Firepower 7000 and 8000 Series Installation Guide

Version 6.0
August 25, 2020

Cisco Systems, Inc.
www.cisco.com
Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

Introduction to the Firepower System

The Cisco Firepower System combines the security of an industry-leading network intrusion protection system with the power to control access to your network based on detected applications, users, and URLs. You can also use Firepower System appliances to serve in a switched, routed, or hybrid (switched and routed) environment; to perform network address translation (NAT); and to build secure virtual private network (VPN) tunnels between the virtual routers of Firepower managed devices.

The Cisco Firepower Management Center provides a centralized management console and database repository for the Firepower System. Managed devices installed on network segments monitor traffic for analysis.

Devices in a passive deployment monitor traffic flowing across a network, for example, using a switch SPAN, virtual switch, or mirror port. Passive sensing interfaces receive all traffic unconditionally and no traffic received on these interfaces is retransmitted.

Devices in an inline deployment allow you to protect your network from attacks that might affect the availability, integrity, or confidentiality of hosts on the network. Inline interfaces receive all traffic unconditionally, and traffic received on these interfaces is retransmitted unless explicitly dropped by some configuration in your deployment. Inline devices can be deployed as a simple intrusion prevention system. You can also configure inline devices to perform access control as well as manage network traffic in other ways.

This installation guide provides information about deploying, installing, and setting up Firepower System appliances (devices and Management Centers). It also contains hardware specifications and safety and regulatory information for Firepower System appliances.

Tip You can host virtual Firepower Management Centers and devices, which can manage and be managed by physical appliances. However, virtual appliances do not support any of the system's hardware-based features: redundancy, switching, routing, and so on. See the *Firepower NGIPSv for VMware Quick Start Guide* for more information.

The topics that follow introduce you to the Firepower System and describe its key components:

Firepower System Appliances

A Firepower System *appliance* is either a traffic-sensing managed *device* or a managing *Firepower Management Center*:

Physical devices are fault-tolerant, purpose-built network appliances available with a range of throughputs and capabilities. Firepower Management Centers serve as central management points for these devices, and automatically aggregate and correlate the events they generate. There are several *models* of each physical appliance type; these models are further grouped into *series* and *family*. Many Firepower System capabilities are appliance dependent.

Firepower Management Centers

A Firepower Management Center provides a centralized management point and event database for your Firepower System deployment. Firepower Management Centers aggregate and correlate intrusion, file, malware, discovery, connection, and performance data, assessing the impact of events on particular hosts and tagging hosts with indications of compromise. This allows you to monitor the information that your devices report in relation to one another, and to assess and control the overall activity that occurs on your network.

Key features of the Firepower Management Center include:

- device, license, and policy management
- display of event and contextual information using tables, graphs, and charts
- health and performance monitoring
- external notification and alerting
- correlation, indications of compromise, and remediation features for real-time threat response
- custom and template-based reporting

Managed Devices

Devices deployed on network segments within your organization monitor traffic for analysis. Devices deployed passively help you gain insight into your network traffic. Deployed inline, you can use Firepower devices to affect the flow of traffic based on multiple criteria. Depending on model and license, devices:

- gather detailed information about your organization's hosts, operating systems, applications, users, files, networks, and vulnerabilities
- block or allow network traffic based on various network-based criteria, as well as other criteria including applications, users, URLs, IP address reputations, and the results of intrusion or malware inspections
- have switching, routing, DHCP, NAT, and VPN capabilities, as well as configurable bypass interfaces, fast-path rules, and strict TCP enforcement
- have high availability (redundancy) to help you ensure continuity of operations, and stacking to combine resources from multiple devices

You **must** manage Firepower devices with a Firepower Management Center.

Appliance Types

The Firepower System can run on fault-tolerant, purpose-built *physical* network appliances available from Cisco. There are several *models* of each Firepower Management Center and managed device; these models are further grouped into *series* and *family*.

Physical managed devices come in a range of throughputs and have a range of capabilities. Physical Firepower Management Centers also have a range of device management, event storage, and host and user monitoring capabilities.

You can also deploy 64-bit *virtual* Firepower Management Centers and *virtual* Firepower managed devices as ESXi hosts using the VMware vSphere Hypervisor or vCloud Director environment.

Either type of Management Center (physical or virtual) can manage any type of device: physical, virtual, and Cisco ASA with FirePOWER Services. Note, however, that many Firepower System capabilities are appliance dependent.

For more information on Firepower System appliances, including the features and capabilities they support, see:

7000 and 8000 Series Appliances

The 7000 and 8000 Series are Firepower physical appliances. Firepower 8000 Series devices are more powerful and support a few features that Firepower 7000 Series devices do not. For detailed information on 7000 and 8000 Series appliances, see the *Firepower 7000 and 8000 Series Installation Guide*.

Virtual Appliances

You can deploy 64-bit virtual Firepower Management Center and managed devices as ESXi hosts using the VMware vSphere Hypervisor or vCloud Director environments.

Regardless of the licenses installed and applied, virtual appliances do not support any of the system's hardware-based features: redundancy and resource sharing, switching, routing, and so on. Also, virtual devices do not have web interfaces. For detailed information on virtual appliances, see the *Firepower NGIPSv for VMware Quick Start Guide*.

Cisco ASA with FirePOWER Services

Cisco ASA with FirePOWER Services (ASA FirePOWER devices) functions similarly to a managed device. In this deployment, the ASA device provides the first-line system policy and passes traffic to the Firepower System for access control, intrusion detection and prevention, discovery, and advanced malware protection. See the Version 6.0 Firepower System Appliances table for a list of supported ASA models.

Regardless of the licenses installed and applied, ASA FirePOWER devices do not support any of the following Firepower System features:

- ASA FirePOWER devices do not support the Firepower System's hardware-based features: high availability, stacking, switching, routing, VPN, NAT, and so on. However, the ASA platform does provide these features, which you can configure using the ASA CLI and ASDM. See the ASA documentation for more information.
- You cannot use the Firepower Management Center web interface to configure ASA FirePOWER interfaces. The Firepower Management Center does not display ASA interfaces when the ASA FirePOWER device is deployed in SPAN port mode.
- You cannot use the Firepower Management Center to shut down, restart, or otherwise manage ASA FirePOWER processes.

ASA FirePOWER devices have a software and command line interface (CLI) unique to the ASA platform. You use these ASA-specific tools to install the system and to perform other platform-specific administrative tasks.

Note If you edit an ASA FirePOWER device and switch from multiple context mode to single context mode (or visa versa), the device renames all of its interfaces. You must reconfigure all Firepower System security zones, correlation rules, and related configurations to use the updated ASA FirePOWER interface names.

Appliances Delivered with Version 6.0

The following table lists the appliances that Cisco delivers with Version 6.0 of the Firepower System.

Table 1-1 Version 6.0 Firepower System Appliances

Models/Family	Firepower Series	Form	Type
70xx Family: • 7010, 7020, 7030, 7050	7000 Series	hardware	device
71xx Family: • 7110, 7120 • 7115, 7125 • AMP7150	7000 Series	hardware	device
80xx Family: • AMP8050	8000 Series	hardware	device
81xx Family: • 8120, 8130, 8140 • AMP8150	8000 Series	hardware	device
82xx Family: • 8250 • 8260, 8270, 8290	8000 Series	hardware	device

Table 1-1 Version 6.0 Firepower System Appliances (continued)

Models/Family	Firepower Series	Form	Type
83xx Family: • 8350 • 8360, 8370, 8390 • AMP8350 • AMP8360, AMP8370, AMP8390	8000 Series	hardware	device
64-bit virtual NGIPSv	n/a	software	device
ASA FirePOWER: • ASA5585-X-SSP-10, ASA5585-X-SSP-20, ASA5585-X-SSP-40, ASA5585-X-SSP-60	n/a	hardware	device
ASA FirePOWER: • ASA5506-X ASA5506H-X, 5506W-X, 5508-X, ASA5512-X, ASA5515-X, ASA5518-X, ASA5525-X, ASA5545-X, ASA5555-X	n/a	software	device
Firepower Management Centers: • MC750, MC1500, MC2000, MC3500, MC2000, MC4000	n/a	hardware	Management Center
64-bit Firepower Management Center Virtual	n/a	software	Management Center

Note that reimaging results in the loss of **all** configuration and event data on the appliance. See Restoring a Firepower System Appliance to Factory Defaults, page 8-1 for more information.

Tip You can migrate specific configuration and event data from a Version 4.10.3 deployment to a Version 5.2 deployment. Then, you can update through a series of procedures to Version 6.0. For more information, see the *Firepower System Migration Guide* for Version 5.2.

Supported Capabilities by Firepower Management Center Model

When running Version 6.0, all Firepower Management Centers have similar capabilities, with only a few model-based restrictions. The following table matches the major capabilities of the system with the Firepower Management Centers that support those capabilities, assuming you are managing devices that support those features and have the correct licenses installed and applied.

In addition to the capabilities listed in the table, Firepower Management Center models vary in terms of how many devices they can manage, how many events they can store, and how many hosts and users they can monitor. For more information, see the *Firepower Management Center Configuration Guide*.

Also, keep in mind that although you can use any model of Firepower Management Center running Version 6.0 of the system to manage any Version 6.0 device, many system capabilities are limited by the device model. For more information, see Supported Capabilities by Managed Device Model, page 1-7.

Table 1-2 Supported Capabilities by Firepower Management Center Model

Feature or Capability	Management Center	Management Center Virtual
collect discovery data (host, application, and user) reported by managed devices and build a network map for your organization	yes	yes
view geolocation data for your network traffic	yes	yes
manage an intrusion detection and prevention (IPS) deployment	yes	yes
manage devices performing Security Intelligence filtering	yes	yes
manage devices performing simple network-based control, including geolocation-based filtering	yes	yes
manage devices performing application control	yes	yes
manage devices performing user control	yes	yes
manage devices that filter network traffic by literal URL	yes	yes
manage devices performing URL Filtering by category and reputation	yes	yes
manage devices performing simple file control by file type	yes	yes
manage devices performing network-based advanced malware protection (AMP)	yes	yes
receive endpoint-based malware (FireAMP) events from your FireAMP deployment	yes	yes
manage device-based hardware-based features: • fast-path rules • strict TCP enforcement • configurable bypass interfaces • tap mode • switching and routing • NAT policies • VPN	yes	yes
manage device-based redundancy and resource sharing: • device stacks • device high availability • stacks in high-availability pairs	yes	yes
separate and manage internal and external traffic using traffic channels	yes	yes
isolate and manage traffic on different networks using multiple management interfaces	yes	yes
install a malware storage pack	yes	no
connect to an eStreamer, host input, or database client	yes	yes

Supported Capabilities by Managed Device Model

Devices are the appliances that handle network traffic; therefore, many Firepower System capabilities are dependent on the model of your managed devices.

The following table matches the major capabilities of the system with the devices that support those capabilities, assuming you have the correct licenses installed and applied from the managing Firepower Management Center.

Keep in mind that although you can use any model of Firepower Management Center running Version 6.0 of the system to manage any Version 6.0 device, a few system capabilities are limited by the Firepower Management Center model. For more information, see Supported Capabilities by Firepower Management Center Model, page 1-5.

Table 1-3 Supported Capabilities by Managed Device Model

Feature or Capability	7000 and 8000 Series Device	ASA FirePOWER	Virtual Device
network discovery: host, application, and user	yes	yes	yes
intrusion detection and prevention (IPS)	yes	yes	yes
Security Intelligence filtering	yes	yes	yes
access control: basic network control	yes	yes	yes
access control: geolocation-based filtering	yes	yes	yes
access control: application control	yes	yes	yes
access control: user control	yes	yes	yes
access control: literal URLs	yes	yes	yes
access control: URL Filtering by category and reputation	yes	yes	yes
file control: by file type	yes	yes	yes
network-based advanced malware protection (AMP)	yes	yes	yes
Automatic Application Bypass	yes	no	yes
fast-path rules	8000 Series	no	no
strict TCP enforcement	yes	no	no
configurable bypass interfaces	except where hardware limited	no	no
tap mode	yes	no	no
switching and routing	yes	no	no
NAT policies	yes	no	no
VPN	yes	no	no
device stacking	8140 82xx Family 83xx Family	no	no
device high availability	yes	no	no
stacks in high-availability pairs	8140 82xx Family 83xx Family	no	no

Table 1-3 Supported Capabilities by Managed Device Model (continued)

Feature or Capability	7000 and 8000 Series Device	ASA FirePOWER	Virtual Device
traffic channels	yes	no	no
multiple management interfaces	yes	no	no
malware storage pack	yes	no	no
restricted command line interface (CLI)	yes	yes	yes
external authentication	yes	no	no
connect to an eStreamer client	yes	yes	no

7000 and 8000 Series Device Chassis Designations

The following section lists the 7000 Series and 8000 Series devices and their respective chassis hardware codes. The chassis code appears on the regulatory label on the outside of the chassis, and is the official reference code for hardware certifications and safety.

7000 Series Chassis Designations

The following table lists the chassis designations for the 7000 Series models available world-wide.

Table 1-4 7000 Series Chassis Models

Firepower and AMP Device Model	Hardware Chassis Code
7010, 7020, 7030	CHRY-1U-AC
7050	NEME-1U-AC
7110, 7120 (Copper)	GERY-1U-8-C-AC
7110, 7120 (Fiber)	GERY-1U-8-FM-AC
7115, 7125, AMP7150	GERY-1U-4C8S-AC

8000 Series Chassis Designations

The following table lists the chassis designations for the 7000 and 8000 Series models available world-wide.

Table 1-5 8000 Series Chassis Models

Firepower and AMP Device Model	Hardware Chassis Code
AMP8050 (AC or DC power)	CHAS-1U-AC/DC
8120, 8130, 8140, AMP8150 (AC or DC power)	CHAS-1U-AC/DC
8250, 8260, 8270, 8290 (AC or DC power)	CHAS-2U-AC/DC

Table 1-5 8000 Series Chassis Models (continued)

Firepower and AMP Device Model	Hardware Chassis Code
8350, 8360, 8370, 8390 (AC or DC power)	PG35-2U-AC/DC
AMP830, AMP8360, AMP8370, AMP8390 (AC or DC power)	PG35-2U-AC/DC

Firepower System Components

The sections that follow describe some of the key capabilities of the Firepower System that contribute to your organization's security, acceptable use policy, and traffic management strategy.

Tip Many Firepower System capabilities are appliance model, license, and user role dependent. Where needed, Firepower System documentation outlines the requirements for each feature and task.

Redundancy and Resource Sharing

The redundancy and resource-sharing features of the Firepower System allow you to ensure continuity of operations and to combine the processing resources of multiple physical devices:

- Device stacking allows you to increase the amount of traffic inspected on a network segment by connecting two to four physical devices in a stacked configuration.
- Device high availability allows you to establish redundancy of networking functionality and configuration data between two or more 7000 and 8000 Series devices or stacks.

Multiple Management Interfaces

You can use *multiple management interfaces* on a Firepower Management Center, device, or both, to improve performance by separating traffic into two traffic channels: the *management traffic channel* carries inter-device communication and the *event traffic channel* carries high volume event traffic such as intrusion events. Both traffic channels can be carried on the same management interface or split between two management interfaces, each interface carrying one traffic channel.

You can also create a route from a specific management interface on your Firepower Management Center to a different network, allowing your Firepower Management Center to isolate and manage device traffic on one network separately from device traffic on another network.

Additional management interfaces have many of the same capabilities as the default management interface with the following exceptions:

- You can configure DHCP on the default (`eth0`) management interface only. Additional (`eth1` and so on) interfaces require unique static IP addresses and hostnames.
- You must configure both traffic channels to use the same non-default management interface when your Firepower Management Center and managed device are separated by a NAT device.
- You can use Lights-Out Management on the default management interface only.
- On the 70xx Family, you can separate traffic into two channels and configure those channels to send traffic to one or more management interfaces on the Firepower Management Center. However, because the 70xx Family contains only one management interface, the device receives traffic sent from the Firepower Management Center on only one management interface.

After your appliance is installed, use the web browser to configure multiple management interfaces. See Multiple Management Interfaces in the *Firepower Management Center Configuration Guide* for more information.

Network Traffic Management

The Firepower System's network traffic management features allow 7000 and 8000 Series devices to act as part of your organization's network infrastructure. You can:

- configure a Layer 2 deployment to perform packet switching between two or more network segments
- configure a Layer 3 deployment to route traffic between two or more interfaces
- perform network address translation (NAT)
- build secure VPN tunnels from virtual routers on managed devices to remote devices or other third-party VPN endpoints

Discovery and Identity

Cisco's discovery and identity technology collects information about hosts, operating systems, applications, users, files, networks, geolocation information, and vulnerabilities, in order to provide you with a complete view of your network.

You can use the Firepower Management Center's web interface to view and analyze data collected by the system. You can also use discovery and identity to help you perform access control and modify intrusion rule states.

Access Control

Access control is a policy-based feature that allows you to specify, inspect, and log the traffic that traverses your network. As part of access control, the Security Intelligence feature allows you to blacklist—deny traffic to and from—specific IP addresses before the traffic is subjected to deeper analysis.

After Security Intelligence filtering occurs, you can define which and how traffic is handled by targeted devices, from simple IP address matching to complex scenarios involving different users, applications, ports, and URLs. You can trust, monitor, or block traffic, or perform further analysis, such as:

- intrusion detection and prevention
- file control
- file tracking and network-based advanced malware protection (AMP)

Intrusion Detection and Prevention

Intrusion detection and prevention is a policy-based feature, integrated into access control, that allows you to monitor your network traffic for security violations and, in inline deployments, to block or alter malicious traffic. An intrusion policy contains a variety of components, including:

- rules that inspect the protocol header values, payload content, and certain packet size characteristics
- rule state configuration based on FireSIGHT recommendations
- advanced settings, such as preprocessors and other detection and performance features
- preprocessor rules that allow you to generate events for associated preprocessors and preprocessor options

File Tracking, Control, and Network-Based Advanced Malware Protection (AMP)

To help you identify and mitigate the effects of malware, the Firepower System's file control, network file trajectory, and advanced malware protection components can detect, track, capture, analyze, and optionally block the transmission of files (including malware files) in network traffic.

File control is a policy-based feature, integrated into access control, that allows managed devices to detect and block your users from uploading (sending) or downloading (receiving) files of specific types over specific application protocols.

Network-based *advanced malware protection* (AMP) allows the system to inspect network traffic for malware in several types of files. Appliances can store detected files for further analysis, either to their hard drive or (for some models) a malware storage pack.

Regardless of whether you store a detected file, you can submit it to the Cisco cloud for a simple known-disposition lookup using the files SHA-256 hash value. You can also submit files for *dynamic analysis*, which produces a threat score. Using this contextual information, you can configure the system to block or allow specific files.

FireAMP is Cisco's enterprise-class, advanced malware analysis and protection solution that discovers, understands, and blocks advanced malware outbreaks, advanced persistent threats, and targeted attacks. If your organization has a FireAMP subscription, individual users install FireAMP Connectors on their computers and mobile devices (also called endpoints). These lightweight agents communicate with the Cisco cloud, which in turn communicates with the Firepower Management Center.

After you configure the Firepower Management Center to connect to the cloud, you can use the Firepower Management Center web interface to view endpoint-based malware events generated as a result of scans, detections, and quarantines on the endpoints in your organization. The Firepower Management Center also uses FireAMP data to generate and track indications of compromise on hosts, as well as display network file trajectories.

The network file trajectory feature allows you to track a file's transmission path across a network. The system uses SHA-256 hash values to track files. Each file has an associated trajectory map, which contains a visual display of the file's transfers over time as well as additional information about the file.

Application Programming Interfaces

There are several ways to interact with the system using application programming interfaces (APIs):

- The Event Streamer (eStreamer) allows you to stream several kinds of event data from a Firepower System appliance to a custom-developed client application.
- The database access feature allows you to query several database tables on a Firepower Management Center, using a third-party client that supports JDBC SSL connections.
- The host input feature allows you to augment the information in the network map by importing data from third-party sources using scripts or command-line files.
- Remediations are programs that your Firepower Management Center can automatically launch when certain conditions on your network are met. This can not only automatically mitigate attacks when you are not immediately available to address them, but can also ensure that your system remains compliant with your organization's security policy.

Licensing the Firepower System

You can license a variety of features to create an optimal Firepower System deployment for your organization. You use the Firepower Management Center to manage licenses for itself and the devices it manages. The license types offered by the Firepower System depend upon the type of device you want to manage:

- For Firepower, ASA FirePOWER, and NGIPSv devices, you must use Classic Licenses.

By default, your Firepower Management Center can perform domain control, host, application, and user discovery, as well as decrypting and inspecting SSL- and TLS-encrypted traffic.

Feature-specific classic licenses allow your managed devices to perform a variety of functions including:

- intrusion detection and prevention
- Security Intelligence filtering
- file control and AMP for Firepower
- application, user, and URL control
- switching and routing
- device high availability
- network address translation (NAT)
- virtual private network (VPN) deployments

There are a few ways you may lose access to licensed features in the Firepower System. You can remove licenses from the Firepower Management Center, which affects all of its managed devices. You can also disable licensed capabilities on specific managed devices. Finally, some licenses may expire. Though there are some exceptions, you cannot use the features associated with an expired or deleted license.

The following summarizes Firepower System Classic Licenses:

Protection

A Protection license allows managed devices to perform intrusion detection and prevention, file control, and Security Intelligence filtering.

Control

A Control license allows managed devices to perform user and application control, switching and routing (including DHCP relay), and NAT. It also allows configuring devices and stacks into high-availability pairs. A Control license requires a Protection license.

URL Filtering

A URL Filtering license allows managed devices to use regularly updated cloud-based category and reputation data to determine which traffic can traverse your network, based on the URLs requested by monitored hosts. A URL Filtering license requires a Protection license.

Malware

A Malware license allows managed devices to perform network-based advanced malware protection (AMP), that is, to detect and block malware in files transmitted over your network. It also allows you to view trajectories, which track files transmitted over your network. A Malware license requires a Protection license.

VPN

A VPN license allows you to build secure VPN tunnels among the virtual routers on Cisco managed devices, or from managed devices to remote devices or other third-party VPN endpoints. A VPN license requires Protection and Control licenses.

See the *Firepower Management Center Configuration Guide* for complete information about classic license types and restrictions.

Security, Internet Access, and Communication Ports

To safeguard the Firepower Management Center, you should install it on a protected internal network. Although the Firepower Management Center is configured to have only the necessary services and ports available, you must make sure that attacks cannot reach it (or any managed devices) from outside the firewall.

If the Firepower Management Center and its managed devices reside on the same network, you can connect the management interfaces on the devices to the same protected internal network as the Firepower Management Center. This allows you to securely control the devices from the Firepower Management Center. You can also configure multiple management interfaces to allow the Firepower Management Center to manage and isolate traffic from devices on other networks.

Regardless of how you deploy your appliances, intra-appliance communication is encrypted. However, you must still take steps to ensure that communications between appliances cannot be interrupted, blocked, or tampered with; for example, with a distributed denial of service (DDoS) or man-in-the-middle attack.

Also note that specific features of the Firepower System require an Internet connection. By default, all appliances are configured to directly connect to the Internet. Additionally, the system requires certain ports remain open for basic intra-appliance communication, for secure appliance access, and so that specific system features can access the local or Internet resources they need to operate correctly.

Tip With the exception of Cisco ASA with FirePOWER Services, Firepower System appliances support the use of a proxy server. For more information, see the *Firepower Management Center Configuration Guide*.

For more information, see:

- Internet Access Requirements, page 1-13
- Communication Ports Requirements, page 1-14

Internet Access Requirements

Firepower System appliances are configured to directly connect to the Internet on ports 443/tcp (HTTPS) and 80/tcp (HTTP), which are open by default; see Communication Ports Requirements, page 1-14. Note that most Firepower System appliances support use of a proxy server; see the Configuring Network Settings chapter in the *Firepower Management Center Configuration Guide*. Note also that a proxy server cannot be used for whois access.

The following table describes the Internet access requirements of specific features of the Firepower System.

Table 1-6 Firepower System Feature Internet Access Requirements

Feature	Internet access is required to...	Appliances
dynamic analysis: querying	query the Collective Security Intelligence Cloud for threat scores of files previously submitted for dynamic analysis.	Management Center
dynamic analysis: submitting	submit files to the Collective Security Intelligence Cloud for dynamic analysis.	Managed devices

Table 1-6 Firepower System Feature Internet Access Requirements (continued)

Feature	Internet access is required to...	Appliances
FireAMP integration	receive endpoint-based (FireAMP) malware events from the Collective Security Intelligence Cloud cloud.	Management Center
intrusion rule, VDB, and GeoDB updates	download or schedule the download of a intrusion rule, GeoDB, or VDB update directly to an appliance.	Management Center
network-based AMP	perform malware cloud lookups.	Management Center
RSS feed dashboard widget	download RSS feed data from an external source, including Cisco.	Any except virtual devices and ASA FirePOWER
Security Intelligence filtering	download Security Intelligence feed data from an external source, including the Firepower System Intelligence Feed.	Management Center
system software updates	download or schedule the download of a system update directly to an appliance.	Any except virtual devices and ASA FirePOWER
URL Filtering	download cloud-based URL category and reputation data for access control, and perform lookups for uncategorized URLs.	Management Center
whois	request whois information for an external host.	Any except virtual devices and ASA FirePOWER

Communication Ports Requirements

Firepower System appliances communicate using a two-way, SSL-encrypted communication channel, which by default uses port 8305/tcp. The system **requires** this port remain open for basic intra-appliance communication. Other open ports allow:

- access to an appliance's web interface
- secure remote connections to an appliance
- certain features of the system to access the local or Internet resources they need to function correctly

In general, feature-related ports remain closed until you enable or configure the associated feature. For example, until you connect the Firepower Management Center to a User Agent, the agent communications port (3306/tcp) remains closed. As another example, port 623/udp remains closed on 7000 and 8000 Series appliances until you enable LOM.

Caution Do **not** close an open port until you understand how this action will affect your deployment.

For example, closing port 25/tcp (SMTP) outbound on a managed device blocks the device from sending email notifications for individual intrusion events (see the *Firepower Management Center Configuration Guide*). As another example, you can disable access to a physical managed device's web interface by closing port 443/tcp (HTTPS), but this also prevents the device from submitting suspected malware files to the cloud for dynamic analysis.

Note that the system allows you to change some of its communication ports:

- You can specify custom ports for LDAP and RADIUS authentication when you configure a connection between the system and the authentication server; see the *Firepower Management Center Configuration Guide*.
- You can change the management port (8305/tcp); see the *Firepower Management Center Configuration Guide*. However, Cisco **strongly** recommends that you keep the default setting. If you change the management port, you must change it for all appliances in your deployment that need to communicate with each other.
- You can use port 32137/tcp to allow upgraded Firepower Management Centers to communicate with the Collective Security Intelligence Cloud. However, Cisco recommends you switch to port 443, which is the default for fresh installations of Version 6.0 and later. For more information, see the *Firepower Management Center Configuration Guide*.

The following table lists the open ports required by each appliance type so that you can take full advantage of Firepower System features.

Table 1-7 Default Communication Ports for Firepower System Features and Operations

Port	Description	Direction	Is Open on...	To...
22/tcp	SSH/SSL	Bidirectional	Any	allow a secure remote connection to the appliance.
25/tcp	SMTP	Outbound	Any	send email notices and alerts from the appliance.
53/tcp	DNS	Outbound	Any	use DNS.
67/udp 68/udp	DHCP	Outbound	Any	use DHCP. **Note** These ports are **closed** by default.
80/tcp	HTTP	Outbound	Any except virtual devices and ASA FirePOWER	allow the RSS Feed dashboard widget to connect to a remote web server.
		Bidirectional	Management Center	update custom and third-party Security Intelligence feeds via HTTP. download URL category and reputation data (port 443 also required).
161/udp	SNMP	Bidirectional	Any except virtual devices and ASA FirePOWER	allow access to an appliance's MIBs via SNMP polling.
162/udp	SNMP	Outbound	Any	send SNMP alerts to a remote trap server.
389/tcp 636/tcp	LDAP	Outbound	Any except virtual devices	communicate with an LDAP server for external authentication.
389/tcp 636/tcp	LDAP	Outbound	Management Center	obtain metadata for detected LDAP users.
443/tcp	HTTPS	Inbound	Any except virtual devices and ASA FirePOWER	access an appliance's web interface.

Table 1-7 Default Communication Ports for Firepower System Features and Operations (continued)

Port	Description	Direction	Is Open on...	To...
443/tcp	HTTPS AMQP cloud comms.	Bidirectional	Management Center	obtain: • software, intrusion rule, VDB, and GeoDB updates • URL category and reputation data (port 80 also required) • the Cisco Intelligence feed and other secure Security Intelligence feeds • endpoint-based (FireAMP) malware events • malware dispositions for files detected in network traffic • dynamic analysis information on submitted files
			7000 and 8000 Series devices	download software updates using the device's local web interface.
			7000 and 8000 Series, virtual devices, and ASA FirePOWER	submit files to the Cisco cloud for dynamic analysis.
514/udp	syslog	Outbound	Any	send alerts to a remote syslog server.
623/udp	SOL/LOM	Bidirectional	7000 and 8000 Series	allow you to perform Lights-Out Management using a Serial Over LAN (SOL) connection.
1500/tcp 2000/tcp	database access	Inbound	Management Center	allow read-only access to the database by a third-party client.
1812/udp 1813/udp	RADIUS	Bidirectional	Any except virtual devices and ASA FirePOWER	communicate with a RADIUS server for external authentication and accounting.
3306/tcp	User Agent	Inbound	Management Center	communicate with User Agents.
8302/tcp	eStreamer	Bidirectional	Any except virtual devices	communicate with an eStreamer client.
8305/tcp	appliance comms.	Bidirectional	Any	securely communicate between appliances in a deployment. **Required.**
8307/tcp	host input client	Bidirectional	Management Center	communicate with a host input client.
32137/tcp	cloud comms.	Bidirectional	Management Center	allow upgraded Management Centers to communicate with the Cisco cloud.

Preconfiguring Appliances

You can preconfigure multiple appliances and Firepower Management Centers in a central location for later deployment at other sites. For considerations when preconfiguring appliances, see Preconfiguring Firepower Managed Devices, page E-1.

Deploying on a Management Network

The Firepower System can be deployed to accommodate the needs of each unique network architecture. The Management Center provides a centralized management console and database repository for the Firepower System. Devices are installed on network segments to collect traffic connections for analysis.

Management Centers use a management interface to connect to a *trusted management network* (that is, a secure internal network not exposed external traffic). Devices connect to a Management Center using a management interface.

Devices then connect to an external network using sensing interfaces to monitor traffic. For more information on how to use sensing interfaces in your deployment, see Deploying Firepower Managed Devices, page 3-1.

Note See the ASA documentation for more information on deployment scenarios for ASA FirePOWER devices.

Management Deployment Considerations

Your management deployment decisions are based on a variety of factors. Answering these questions can help you understand your deployment options to configure the most efficient and effective system:

- Will you use the default single management interface to connect your device to your Management Center? Will you enable additional management interfaces to improve performance, or to isolate traffic received on the Management Center from different networks? See Understanding Management Interfaces, page 2-2 for more information.
- Do you want to enable traffic channels to create two connections between the Management Center and the managed device to improve performance? Do you want to use multiple management interfaces to further increase throughput capacity between the Management Center and the managed device? See Deploying with Traffic Channels, page 2-3 for more information.
- Do you want to use one Management Center to manage and isolate traffic from devices on different networks? See Deploying with Network Routes, page 2-4 for more information.
- Are you deploying your management interfaces in a protected environment? Is appliance access restricted to specific workstation IP addresses? Security Considerations, page 2-5 describes considerations for deploying your management interfaces securely.
- Are you deploying 8000 Series devices? See Special Case: Connecting 8000 Series Devices, page 2-5 for more information.

Understanding Management Interfaces

Management interfaces provide the means of communication between the Management Center and all devices it manages. Maintaining good traffic control between the appliances is essential to the success of your deployment.

On Management Centers and Firepower devices, you can enable the management interface on the Management Center, device, or both, to sort traffic between the appliances into two separate traffic channels. The *management traffic channel* carries all internal traffic (that is, inter-device traffic specific to the management of the appliance and the system), and the *event traffic channel* carries all event traffic (that is, high volume event traffic, such as intrusion and malware events). Splitting traffic into two channels creates two connection points between the appliances which increases throughput, thus improving performance. You can also enable *multiple management interfaces* to provide still greater throughput between appliances, or to manage and isolate traffic between devices on different networks.

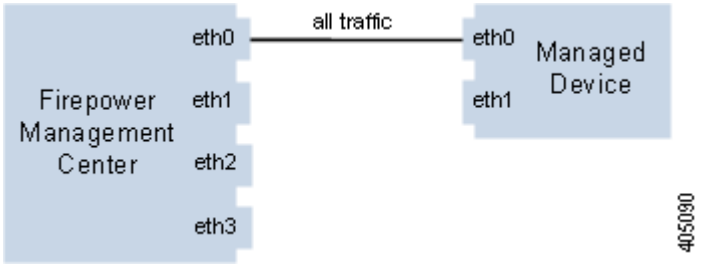
After you register the device to the Management Center, you can change the default configuration to enable traffic channels and multiple management interfaces using the web interface on each appliance. For configuration information, see Configuring Appliance Settings in the *Firepower Management Center Configuration Guide*.

Management interfaces are often located on the back of the appliance. See Identifying the Management Interfaces, page 4-2 for more information.

Single Management Interface

When you register your device to a Management Center, you establish a single communication channel that carries all traffic between the management interface on the Management Center and the management interface on the device.

The following graphic shows the default single communication channel. One interface carries one communication channel that contains both management and event traffic.



Multiple Management Interfaces

You can enable and configure multiple management interfaces, each with a specific IPv4 or IPv6 address and, optionally, a hostname, to provide greater traffic throughput by sending each traffic channel to a different management interface. Configure a smaller interface to carry the lighter management traffic load, and a larger interface to carry the heavier event traffic load. You can register devices to separate management interfaces and configure both traffic channels for the same interface, or use a dedicated management interface to carry the event traffic channels for all devices managed by the Management Center.

You can also create a route from a specific management interface on your Management Center to a different network, allowing your Management Center to isolate and manage device traffic on one network separately from device traffic on another network.

Additional management interfaces function the same as the default management interface with the following exceptions:

- You can configure DHCP on the default (`eth0`) management interface only. Additional (`eth1` and so on) interfaces require unique static IP addresses and hostnames. Cisco recommends that you do not set up DNS entries for additional management interfaces but instead register Management Centers and devices by IP addresses only for these interfaces.
- You must configure both traffic channels to use the same management interface when you use a non-default management interface to connect your Management Center and managed device and those appliances are separated by a NAT device.
- You can use Lights-Out Management on the default management interface only.
- On the 70xx Family, you can separate traffic into two channels and configure those channels to send traffic to one or more management interfaces on the Management Center. However, because the 70xx Family contains only one management interface, the device receives traffic sent from the Management Center on only one management interface.

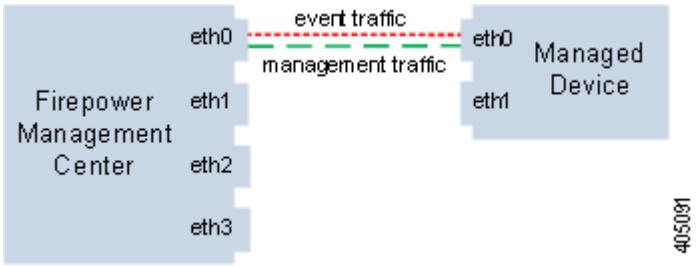
Deployment Options

You can manage traffic flow using traffic channels to improve performance on your system using one or more management interfaces. In addition, you can create a route to a different network using a specific management interface on the Management Center and its managed device, allowing you to isolate traffic between devices on different networks. For more information, see the following sections:

Deploying with Traffic Channels

When you use two traffic channels on one management interface, you create two connections between the Management Center and the managed device. One channel carries management traffic and one carries event traffic, separately and on the same interface.

The following example shows the communication channel with two separate traffic channels on the same interface.

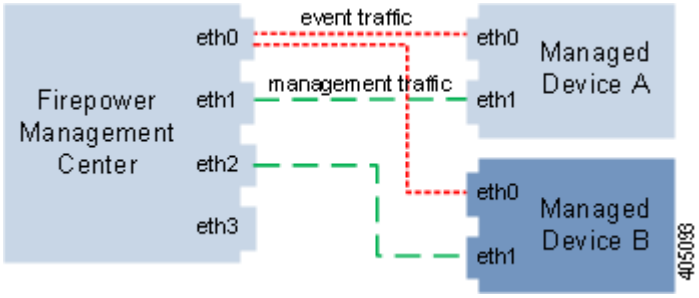


When you use multiple management interfaces, you can improve your performance by dividing the traffic channels over two management interfaces, thus increasing the traffic flow by adding the capacity of both interfaces. One interface carries the management traffic channel and the other carries the event traffic channel. If either interface fails, all traffic reroutes to the active interface and the connection is maintained.

The following graphic shows the management traffic channel and the event traffic channel over two management interfaces.

You can use a dedicated management interface to carry only event traffic from multiple devices. In this configuration, each device is registered to a different management interface to carry the management traffic channel, and one management interface on the Management Center carries all event traffic channels from all devices. If an interface fails, traffic reroutes to the active interface and the connection is maintained. Note that because event traffic for all devices is carried on the same interface, traffic is not isolated between networks.

The following graphic shows two devices using different management channel traffic interfaces sharing the same dedicated interface for event traffic channels.



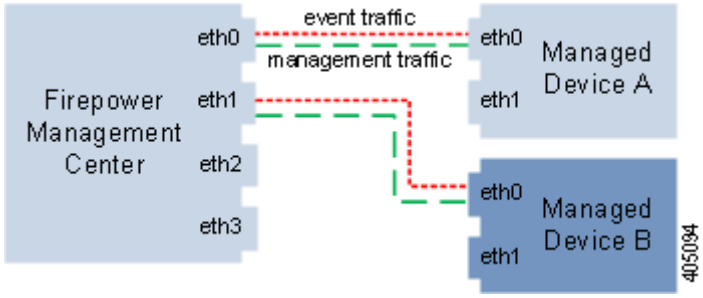
Deploying with Network Routes

You can create a route from a specific management interface on your Management Center to a different network. When you register a device from that network to the specified management interface on the Management Center, you provide an isolated connection between the Management Center and the device on a different network. Configure both traffic channels to use the same management interface to ensure that traffic from that device remains isolated from device traffic on other networks. Because the routed interface is isolated from all other interfaces on the Management Center, if the routed management interface fails, the connection is lost.

Tip You must register a device to the static IP address of any management interface other than the default (`eth0`) management interface. DHCP is supported only on the default management interface.

After you install your Management Center, you configure multiple management interfaces using the web interface. See Configuring Appliance Settings in the *Firepower Management Center Configuration Guide* for more information.

The following graphic shows two devices isolating network traffic by using separate management interfaces for all traffic. You can add more management interfaces to configure separate management and event traffic channel interfaces for each device.



Security Considerations

To deploy your management interfaces in a secure environment, Cisco recommends that you consider the following:

- Always connect the management interface to a trusted internal management network that is protected from unauthorized access.
- Identify the specific workstation IP addresses that can be allowed to access appliances. Restrict access to the appliance to only those specific hosts using Access Lists within the appliance's system policy. For more information, see the *Firepower Management Center Configuration Guide*.

Special Case: Connecting 8000 Series Devices

Supported Devices: 8000 Series

When you register an 8000 Series device to your Management Center, you must either auto-negotiate on both sides of the connection, or set both sides to the same static speed to ensure a stable network link. 8000 Series devices do not support half duplex network links; they also do not support differences in speed or duplex configurations at opposite ends of a connection.

Deploying Firepower Managed Devices

After you register a device to a Firepower Management Center, you deploy the sensing interfaces of the device on a network segment to monitor traffic using an intrusion detection system or protect your network from threats using an intrusion prevention system.

Note See the ASA documentation for more information on deployment scenarios for ASA FirePOWER devices.

For additional information about deployments, consult the *Best Practices Guide*, available from the Cisco sales department.

Sensing Deployment Considerations

Your sensing deployment decisions will be based on a variety of factors. Answering these questions can help you understand the vulnerable areas of your network and clarify your intrusion detection and prevention needs:

- Will you be deploying your managed device with passive or inline interfaces? Does your device support a mix of interfaces, some passive and others inline? See Understanding Sensing Interfaces, page 3-2 for more information.
- How will you connect the managed devices to the network? Hubs? Taps? Spanning ports on switches? Virtual switches? See Connecting Devices to Your Network, page 3-4 for more information.
- Do you want to detect every attack on your network, or do you only want to know about attacks that penetrate your firewall? Do you have specific assets on your network such as financial, accounting, or personnel records, production code, or other sensitive, protected information that require special security policies? See Deployment Options, page 3-7 for more information.
- Will you use multiple sensing interfaces on your managed device to recombine the separate connections from a network tap, or to capture and evaluate traffic from different networks? Do you want to use the multiple sensing interfaces to perform as a virtual router or a virtual switch? See Using Multiple Sensing Interfaces on a Managed Device, page 3-16 for more information.
- Do you provide VPN or modem access for remote workers? Do you have remote offices that also require an intrusion protection deployment? Do you employ contractors or other temporary employees? Are they restricted to specific network segments? Do you integrate your network with the networks of other organizations such as customers, suppliers, or business partners? See Complex Network Deployments, page 3-18 for more information.

Understanding Sensing Interfaces

The sections that follow describe how different sensing interfaces affect the capabilities of the Firepower System. In addition to passive and inline interfaces, you can also have routed, switched, and hybrid interfaces.

Sensing interfaces are located on the front of the device. To identify your sensing interfaces, see Identifying the Sensing Interfaces, page 4-3.

Passive Interfaces

You can configure a passive deployment to monitor traffic flowing across a network using a switch SPAN, virtual switch, or mirror port, allowing traffic to be copied from other ports on the switch. Passive interfaces allow you to inspect traffic within the network without being in the flow of network traffic. When configured in a passive deployment, the system cannot take certain actions such as blocking or shaping traffic. Passive interfaces receive all traffic unconditionally and do not retransmit received traffic.

Inline Interfaces

You configure an inline deployment transparently on a network segment by binding two ports together. Inline interfaces allow you to install a device in any network configuration without the configuration of adjacent network devices. Inline interfaces receive all traffic unconditionally, then retransmit all traffic received on these interfaces except traffic explicitly dropped. You must assign a pair of inline interfaces to an inline set before they can handle traffic in an inline deployment.

Note If you configure an interface as an inline interface, the adjacent port on its NetMod automatically becomes an inline interface as well to complete the pair.

Configurable bypass inline sets allow you to select how your traffic is handled if your hardware fails completely (for example, the device loses power). You may determine that connectivity is critical on one network segment, and, on another network segment, you cannot permit uninspected traffic. Using configurable bypass inline sets, you can manage the traffic flow of your network traffic in one of the following ways:

- *Bypass*: an interface pair configured for bypass allows all traffic to flow if the device fails. The traffic bypasses the device and any inspection or other processing by the device. Bypass allows uninspected traffic across the network segment, but ensures that the network connectivity is maintained.
- *Non-bypass*: an interface pair configured for non-bypass stops all traffic if the device fails. Traffic that reaches the failed device does not enter the device. Non-bypass does not permit traffic to pass uninspected, but the network segment loses connectivity if the device fails. Use non-bypass interfaces in deployment situations where network security is more important than loss of traffic.

Configure the inline set as bypass to ensure that traffic continues to flow if your device fails. Configure the inline set as non-bypass to stop traffic if the device fails. Note that reimaging resets Firepower devices in bypass mode to a non-bypass configuration and disrupts traffic on your network until you reconfigure bypass mode. For more information, see Traffic Flow During the Restore Process, page 8-1.

All Firepower devices can contain configurable bypass interfaces. 8000 Series devices can also contain NetMods with interfaces that cannot be configured for bypass. For more information on NetMods, see Firepower 8000 Series Modules, page 7-32. Other advanced interface options include tap mode, propagate link state, transparent inline mode, and strict TCP mode. For information on how to configure your inline interface sets, see Configuring Inline Sets in the *Firepower Management Center Configuration Guide*. For more information on using inline interfaces, see Connecting Devices to Your Network, page 3-4.

You cannot configure bypass interfaces on an ASA FirePOWER device using the Firepower Management Center. For information on configuring an ASA FirePOWER device in inline mode, see the ASA documentation.

Switched Interfaces

You can configure switched interfaces on a Firepower device in a Layer 2 deployment to provide packet switching between two or more networks. You can also configure virtual switches on Firepower devices to operate as standalone broadcast domains, dividing your network into logical segments. A virtual switch uses the media access control (MAC) address from a host to determine where to send packets.

Switched interfaces can have either a physical or logical configuration:

- *Physical switched interfaces* are physical interfaces with switching configured. Use physical switched interfaces to handle untagged VLAN traffic.
- *Logical switched interfaces* are an association between a physical interface and a VLAN tag. Use logical interfaces to handle traffic with designated VLAN tags.

Virtual switches can operate as standalone broadcast domains, dividing your network into logical segments. A virtual switch uses the media access control (MAC) address from a host to determine where to send packets. When you configure a virtual switch, the switch initially broadcasts packets through every available port on the switch. Over time, the switch uses tagged return traffic to learn which hosts reside on the networks connected to each port.

You can configure your device as a virtual switch and use the remaining interfaces to connect to network segments you want to monitor. To use a virtual switch on your device, create physical switched interfaces and then follow the instructions for Setting Up Virtual Switches in the *Firepower Management Center Configuration Guide*.

Routed Interfaces

You can configure routed interfaces on a Firepower device in a Layer 3 deployment so that it routes traffic between two or more interfaces. You must assign an IP address to each interface and assign the interfaces to a virtual router to route traffic.

You can configure routed interfaces for use with a gateway virtual private network (gateway VPN) or with network address translation (NAT). For more information, see Deploying a Gateway VPN, page 3-10 and Deploying with Policy-Based NAT, page 3-11.

You can also configure the system to route packets by making packet forwarding decisions according to the destination address. Interfaces configured as routed interfaces receive and forward the Layer 3 traffic. Routers obtain the destination from the outgoing interface based on the forwarding criteria, and access control rules designate the security policies to be applied.

Routed interfaces can have either a physical or logical configuration:

- *Physical routed interfaces* are physical interfaces with routing configured. Uses physical routed interfaces to handle untagged VLAN traffic.
- *Logical switched interfaces* are an association between a physical interface and a VLAN tag. Use logical interfaces to handle traffic with designated VLAN tags.

To use routed interfaces in a Layer 3 deployment, you must configure virtual routers and assign routed interfaces to them. A virtual router is a group of routed interfaces that route Layer 3 traffic.

You can configure your device as a virtual router and use the remaining interfaces to connect to network segments you want to monitor. You can also enable strict TCP enforcement for maximum TCP security. To use a virtual router on your device, create physical routed interfaces on your device and then follow the instructions for Setting Up Virtual Routers in the *Firepower Management Center Configuration Guide*.

Hybrid Interfaces

You can configure logical hybrid interfaces on Firepower devices that allow the Firepower System to bridge traffic between virtual routers and virtual switches. If IP traffic received on interfaces in a virtual switch is addressed to the MAC address of an associated hybrid logical interface, the system handles it as Layer 3 traffic and either routes or responds to the traffic depending on the destination IP address. If the system receives any other traffic, it handles it as Layer 2 traffic and switches it appropriately.

To create a hybrid interface, you first configure a virtual switch and virtual router, then add the virtual switch and virtual router to the hybrid interface. A hybrid interface that is not associated with both a virtual switch and a virtual router is not available for routing, and does not generate or respond to traffic.

You can configure hybrid interfaces with network address translation (NAT) to pass traffic between networks. For more information, see Deploying with Policy-Based NAT, page 3-11.

If you want to use hybrid interfaces on your device, define a hybrid interface on the device and then follow the instructions for Setting Up Hybrid Interfaces in the *Firepower Management Center Configuration Guide*.

Connecting Devices to Your Network

You can connect the sensing interfaces on your managed devices to your network in several ways. Configure a hub or network tap using either passive or inline interfaces, or a span port using passive interfaces.

Using a Hub

An Ethernet hub is a simple way to ensure that the managed device can see all the traffic on a network segment. Most hubs of this type take the IP traffic meant for any of the hosts on the segment and broadcast it to all the devices connected to the hub. Connect the interface set to the hub to monitor all incoming and outgoing traffic on the segment. Using a hub does not guarantee that the detection engine sees every packet on a higher volume network because of the potential of packet collision. For a simple network with low traffic, this is not likely to be a problem. In a high-traffic network, a different option may provide better results. Note that if the hub fails or loses power, the network connection is broken. In a simple network, the network would be down.

Some devices are marketed as hubs but actually function as switches and do not broadcast each packet to every port. If you attach your managed device to a hub, but do not see all the traffic, you may need to purchase a different hub or use a switch with a Span port.

Using a Span Port

Many network switches include a span port that mirrors traffic from one or more ports. By connecting an interface set to the span port, you can monitor the combined traffic from all ports, generally both incoming and outgoing. If you already have a switch that includes this feature on your network, in the proper location, then you can deploy the detection on multiple segments with little extra equipment cost beyond the cost of the managed device. In high-traffic networks, this solution has its limitations. If the span port can handle 200Mbps and each of three mirrored ports can handle up to 100Mbps, then the span port is likely to become oversubscribed and drop packets, lowering the effectiveness of the managed device.

Using a Network Tap

Network taps allow you to passively monitor traffic without interrupting the network flow or changing the network topology. Taps are readily available for different bandwidths and allow you to analyze both incoming and outgoing packets on a network segment. Because you can monitor only a single network segment with most taps, they are not a good solution if you want to monitor the traffic on two of the eight ports on a switch. Instead, you would install the tap between the router and the switch and access the full IP stream to the switch.

By design, network taps divide incoming and outgoing traffic into two different streams over two different cables. Managed devices offer multiple sensing interface options that recombine the two sides of the conversation so that the entire traffic stream is evaluated by the decoders, the preprocessors, and the detection engine.

Cabling Inline Deployments on Copper Interfaces

If you deploy your device inline on your network and you want to use your device's bypass capabilities to maintain network connectivity if the device fails, you must pay special attention to how you cable the connections.

If you deploy a device with fiber bypass capable interfaces, there are no special cabling issues beyond ensuring that the connections are securely fastened and the cables are not kinked. However, if you are deploying devices with copper rather than fiber network interfaces, then you must be aware of the device model that you are using, because different device models use different network cards. Note that some 8000 Series NetMods do not allow bypass configuration.

The network interface cards (NICs) in the device support a feature called Auto-Medium Dependent Interface Crossover (Auto-MDI-X), which allows network interfaces to configure automatically whether you use a straight-through or crossover Ethernet cable to connect to another network device. Firepower devices bypass as crossover connections.

Wire the device as would normally be done without a device deployed. The link should work with power to the device removed. In most cases you should use two straight-through cables to connect the device to the two endpoints.

Figure 3-1 Crossover Bypass Connection Cabling

The following table indicates where you should use crossover or straight-through cables in your hardware bypass configurations. Note that a Layer 2 port functions as a straight-through (MDI) endpoint in the deployment, and a Layer 3 port functions as a crossover (MDIX) endpoint in the deployment. The total crossovers (cables and appliances) should be an odd number for bypass to function properly.

Table 3-1 Valid Configurations for Hardware Bypass

Endpoint 1	Cable	Managed Device	Cable	Endpoint 2
MDIX	straight-through	straight-through	straight-through	MDI
MDI	crossover	straight-through	straight-through	MDI
MDI	straight-through	straight-through	crossover	MDI
MDI	straight-through	straight-through	straight-through	MDIX
MDIX	straight-through	crossover	straight-through	MDIX
MDI	straight-through	crossover	straight-through	MDI
MDI	crossover	crossover	crossover	MDI
MDIX	crossover	crossover	straight-through	MDI

Note that every network environment is likely to be unique, with endpoints that have different combinations of support for Auto-MDI-X. The easiest way to confirm that you are installing your device with the correct cabling is to begin by connecting the device to its two endpoints using one crossover cable and one straight-through cable, but with the device powered down. Ensure that the two endpoints can communicate. If they cannot communicate, then one of the cables is the incorrect type. Switch one (and only one) of the cables to the other type, either straight-through or crossover.

After the two endpoints can successfully communicate with the inline device powered down, power up the device. The Auto-MDI-X feature ensures that the two endpoints will continue to communicate. Note that if you have to replace an inline device, you should repeat the process of ensuring that the endpoints can communicate with the new device powered down to protect against the case where the original device and its replacement have different bypass characteristics.

The Auto-MDI-X setting functions correctly only if you allow the network interfaces to auto-negotiate. If your network environment requires that you turn off the Auto Negotiate option on the Network Interface page, then you must specify the correct MDI/MDIX option for your inline network interfaces. See Configuring Inline Interfaces in the *Firepower Management Center Configuration Guide* for more information.

Special Case: Connecting Firepower 8000 Series Devices

When you register a Firepower 8000 Series managed device to your Firepower Management Center, you must either use auto-negotiation on both sides of the connection, or set both sides to the same static speed to ensure a stable network link. 8000 Series managed devices do not support half duplex network links; they also do not support differences in speed or duplex configurations at opposite ends of a connection.

Deployment Options

When you place your managed device on a network segment, you can monitor traffic using an intrusion detection system or protect your network from threats using an intrusion prevention system.

You can also deploy your managed device to function as a virtual switch, virtual router, or gateway VPN. Additionally, you can use policies to route traffic or control access to traffic on your network.

Deploying with a Virtual Switch

You can create a *virtual switch* on your managed device by configuring inline interfaces as switched interfaces. The virtual switch provides Layer 2 packet switching for your deployment. Advanced options include setting a static MAC address, enabling spanning tree protocol, enabling strict TCP enforcement, and dropping bridge protocol data units (BPDUs) at the domain level. For information on switched interfaces, see Switched Interfaces, page 3-3.

A virtual switch must contain two or more switched interfaces to handle traffic. For each virtual switch, the system switches traffic only to the set of ports configured as switched interfaces. For example, if you configure a virtual switch with four switched interfaces, when the system receives traffic packets through one port it only broadcasts these packets to the remaining three ports on the switch.

To configure a virtual switch to allow traffic, you configure two or more switched interfaces on a physical port, add and configure a virtual switch, and then assign the virtual switch to the switched interfaces. The system drops any traffic received on an external physical interface that does not have a switched interface waiting for it. If the system receives a packet with no VLAN tag and you have not configured a physical switched interface for that port, it drops the packet. If the system receives a VLAN-tagged packet and you have not configured a logical switched interface, it also drops the packet.

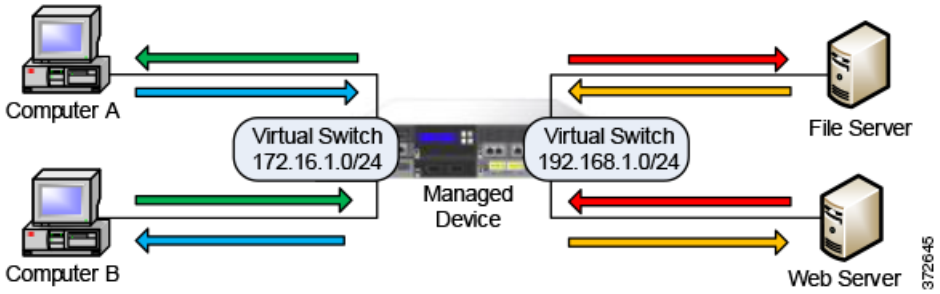
You can define additional logical switched interfaces on the physical port as needed, but you must assign a logical switched interface to a virtual switch to handle traffic.

Virtual switches have the advantage of scalability. When you use a physical switch, you are limited by the number of available ports on the switch. When you replace your physical switch with a virtual switch, you are limited only by your bandwidth and the level of complexity you want to introduce to your deployment.

Use a virtual switch where you would use a Layer 2 switch, such as workgroup connectivity and network segmentation. Layer 2 switches are particularly effective where workers spend most of their time on their local segment. Larger deployments (for example, deployments that contain broadcast traffic, Voice-over-IP, or multiple networks) can use virtual switches on smaller network segments of the deployment.

When you deploy multiple virtual switches on the same managed device, you can maintain separate levels of security as dictated by the needs of each network.

Figure 3-2 Virtual Switches on a Managed Device



In this example, the managed device monitors traffic from two separate networks, 172.16.1.0/20 and 192.168.1.0/24. Although both networks are monitored by the same managed device, the virtual switch passes traffic only to those computers or servers on the same network. Traffic can pass from computer A to computer B through the 172.16.1.0/24 virtual switch (indicated by the blue line) and from computer B to computer A through the same virtual switch (indicated by the green line). Similarly, traffic can pass to and from the file and web servers through the 192.168.1.0/24 virtual switch (indicated by the red and orange lines). However, traffic cannot pass between the computers and the web or file servers because the computers are not on the same virtual switch as the servers.

For more information on configuring switched interfaces and virtual switches, see Setting Up Virtual Switches in the *Firepower Management Center Configuration Guide.*

Deploying with a Virtual Router

You can create a *virtual router* on a managed device to route traffic between two or more networks, or to connect a private network to a public network (for example, the Internet). The virtual router connects two routed interfaces to provide Layer 3 packet forwarding decisions for your deployment according to the destination address. Optionally, you can enable strict TCP enforcement on the virtual router. For more information on routed interfaces, see Routed Interfaces, page 3-3. You must use a virtual router with a gateway VPN. For more information, see Deploying a Gateway VPN, page 3-10.

A virtual router can contain either physical or logical routed configurations from one or more individual devices within the same broadcast domain. You must associate each logical interface with a VLAN tag to handle traffic received by the physical interface with that specific tag. You must assign a logical routed interface to a virtual router to route traffic.

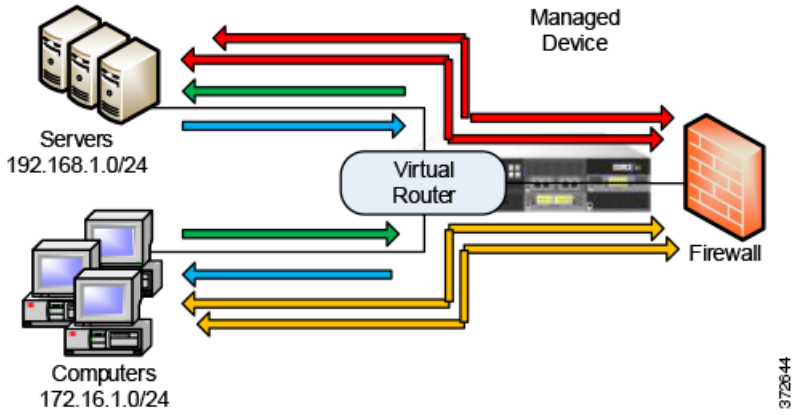
To configure a virtual router, you set up routed interfaces with either physical or logical configurations. You can configure physical routed interfaces for handling untagged VLAN traffic. You can also create logical routed interfaces for handling traffic with designated VLAN tags. The system drops any traffic received on an external physical interface that does not have a routed interface waiting for it. If the system receives a packet with no VLAN tag and you have not configured a physical routed interface for that port, it drops the packet. If the system receives a VLAN-tagged packet and you have not configured a logical routed interface, it also drops the packet.

Virtual routers have the advantage of scalability. Where physical routers limit the number of networks you can connect, multiple virtual routers can be configured on the same managed device. Putting multiple routers on the same device reduces the physical complexity of your deployment, allowing you to monitor and manage multiple routers from one device.

Use a virtual router where you would use a Layer 3 physical router to forward traffic between multiple networks in your deployment, or to connect your private network to a public network. Virtual routers are particularly effective in large deployments where you have many networks or network segments with different security requirements.

When you deploy a virtual router on your managed device, you can use one appliance to connect multiple networks to each other, and to the Internet.

Figure 3-3 Virtual Routers on a Managed Device



In this example, the managed device contains a virtual router to allow traffic to travel between the computers on network 172.16.1.0/20 and the servers on network 192.168.1.0/24 (indicated by the blue and green lines). A third interface on the virtual router allows traffic from each network to pass to the firewall and back (indicated by the red and orange lines).

For more information, see Setting Up Virtual Routers in the *Firepower Management Center Configuration Guide*.

Deploying with Hybrid Interfaces

You can create a *hybrid interface* on a managed device to route traffic between Layer 2 and Layer 3 networks using a virtual switch and a virtual router. This provides one interface that can both route local traffic on the switch and route traffic to and from an external network. For best results, configure policy-based NAT on the interface to provide network address translation on the hybrid interface. See Deploying with Policy-Based NAT, page 3-11.

A hybrid interface must contain one or more switched interfaces and one or more routed interfaces. A common deployment consists of two switched interfaces configured as a virtual switch to pass traffic on a local network and virtual routers to route traffic to networks, either private or public.

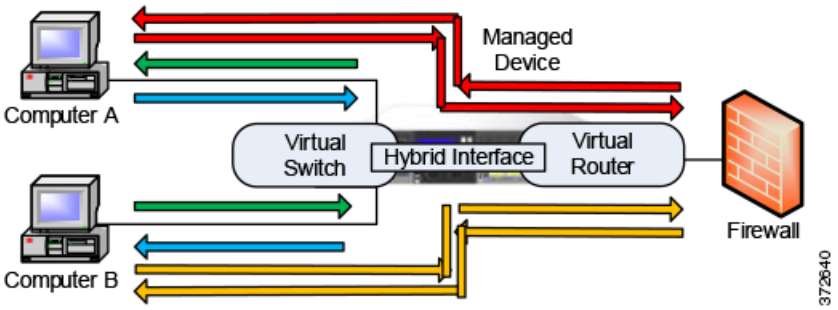
To create a hybrid interface, you first configure a virtual switch and virtual router, then add the virtual switch and virtual router to the hybrid interface. A hybrid interface that is not associated with both a virtual switch and a virtual router is not available for routing, and does not generate or respond to traffic.

Hybrid interfaces have the advantage of compactness and scalability. Using a single hybrid interface combines both Layer 2 and Layer 3 traffic routing functions in a single interface, reducing the number of physical appliances in the deployment and providing a single management interface for the traffic.

Use a hybrid interface where you need both Layer 2 and Layer 3 routing functions. This deployment can be ideal for small segments of your deployment where you have limited space and resources.

When you deploy a hybrid interface, you can allow traffic to pass from your local network to an external or public network, such as the Internet, while addressing separate security considerations for the virtual switch and virtual router in the hybrid interface.

Figure 3-4 Hybrid Interface on a Managed Device



In this example, computer A and computer B are on the same network and communicate using a Layer 2 virtual switch configured on the managed device (indicated by the blue and green lines). A virtual router configured on the managed device provides Layer 3 access to the firewall. A hybrid interface combines the Layer 2 and Layer 3 capabilities of the virtual switch and virtual router to allow traffic to pass from each computer through the hybrid interface to the firewall (indicated by the red and orange lines).

For more information, see Setting Up Hybrid Interfaces in the *Firepower Management Center Configuration Guide*.

Deploying a Gateway VPN

License: VPN

You can create a *gateway virtual private network* (gateway VPN) connection to establish a secure tunnel between a local gateway and a remote gateway. The secure tunnel between the gateways protects communication between them.

You configure the Firepower System to build secure VPN tunnels from the virtual routers of Cisco managed devices to remote devices or other third-party VPN endpoints using the Internet Protocol Security (IPSec) protocol suite. After the VPN connection is established, the hosts behind the local gateway can connect to the hosts behind the remote gateway through the secure VPN tunnel. The VPN endpoints authenticate each other with either the Internet Key Exchange (IKE) version 1 or version 2 protocol to create a security association for the tunnel. The system runs in either IPSec authentication header (AH) mode or the IPSec encapsulating security payload (ESP) mode. Both AH and ESP provide authentication, and ESP also provides encryption.

A gateway VPN can be used in a point-to-point, star, or mesh deployment:

- Point-to-point deployments connect two endpoints with each other in a direct one-to-one relationship. Both endpoints are configured as peer devices, and either device can initiate the secured connection. At least one device must be a VPN-enabled managed device.

  Use a point-to-point deployment to maintain your network security when a host at a remote location uses public networks to connect to a host in your network.

- Star deployments establish a secure connection between a hub and multiple remote endpoints (leaf nodes). Each connection between the hub node and an individual leaf node is a separate VPN tunnel. Typically, the hub node is the VPN-enabled managed device, located at the main office. Leaf nodes are located at branch offices and initiate most of the traffic.

  Use a star deployment to connect an organization's main and branch office locations using secure connections over the Internet or other third-party network to provide all employees with controlled access to the organization's network.

- Mesh deployments connect all endpoints together by means of VPN tunnels. This offers redundancy in that when one endpoint fails, the remaining endpoints can still communicate with each other.

  Use a mesh deployment to connect a group of decentralized branch office locations to ensure that traffic can travel even if one or more VPN tunnels fails. The number of VPN-enabled managed devices you deploy in this configuration controls the level of redundancy.

For more information on gateway VPN configuration and deployments, see Gateway VPN in the *Firepower Management Center Configuration Guide*.

Deploying with Policy-Based NAT

You can use *policy-based network address translation* (NAT) to define policies that specify how you want to perform NAT. You can target your policies to a single interface, one or more devices, or entire networks.

You can configure static (one-to-one) or dynamic (one-to-many) translation. Note that dynamic translations are order-dependent where rules are searched in order until the first matching rule applies.

Policy-based NAT typically operates in the following deployments:

- Hide your private network address.

  When you access a public network from your private network, NAT translates your private network address to your public network address. Your specific private network address is hidden from the public network.

- Allow access to a private network service.

  When a public network accesses your private network, NAT translates your public address to your private network address. The public network can access your specific private network address.

- Redirect traffic between multiple private networks.

  When a server on a private network accesses a server on a connected private network, NAT translates the private addresses between the two private networks to ensure there is no duplication in private addresses and traffic can travel between them.

Using policy-based NAT removes the need for additional hardware and consolidates the configuration of your intrusion detection or prevention system and NAT into a single user interface. For more information, see Using NAT Policies in the *Firepower Management Center Configuration Guide*.

Deploying with Access Control

Access control is a policy-based feature that allows you to specify, inspect, and log the traffic that can enter, exit, or travel within your network. The following section describes how access control can function in your deployment. See the *Firepower Management Center Configuration Guide* for more information on this feature.

An access control policy determines how the system handles traffic on your network. You can add access control rules to your policy to provide more granular control over how you handle and log network traffic.

An access control policy that does not include access control rules uses one of the following default actions to handle traffic:

- block all traffic from entering your network
- trust all traffic to enter your network without further inspection

- allow all traffic to enter your network, and inspect the traffic with a network discovery policy only
- allow all traffic to enter your network, and inspect the traffic with intrusion and network discovery policies

Access control rules further define how traffic is handled by targeted devices, from simple IP address matching to complex scenarios involving different users, applications, ports, and URLs. For each rule, you specify a rule action, that is, whether to trust, monitor, block, or inspect matching traffic with an intrusion or file policy.

Access control can filter traffic based on Security Intelligence data, a feature that allows you to specify the traffic that can traverse your network, per access control policy, based on the source or destination IP address. This feature can create a blacklist of disallowed IP addresses whose traffic is blocked and not inspected.

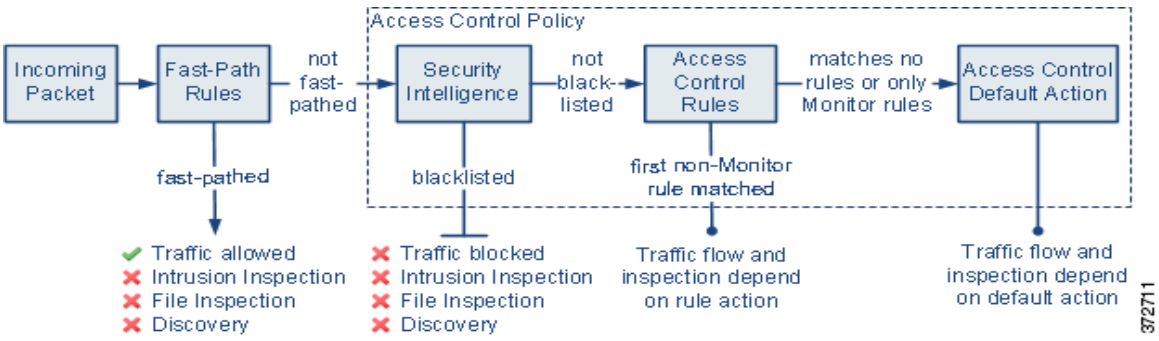
The sample deployment illustrates common network segments. Deploying your managed devices in each of these locations serves different purposes. The following sections describe typical location recommendations:

- Inside the Firewall, page 3-12 explains how access control functions on traffic that passes through the firewall.
- On the DMZ, page 3-13 explains how access control within the DMZ can protect outward-facing servers.
- On the Internal Network, page 3-14 explains how access control can protect your internal network from intentional or accidental attack.
- On the Core Network, page 3-14 explains how an access control policy with strict rules can protect your critical assets.
- On a Remote or Mobile Network, page 3-15 explains how access control can monitor and protect the network from traffic at remote locations or on mobile devices.

Inside the Firewall

Managed devices inside the firewall monitor inbound traffic allowed by the firewall or traffic that passes the firewall due to misconfiguration. Common network segments include the DMZ, the internal network, the core, mobile access, and remote networks.

The diagram below illustrates traffic flow through the Firepower System, and provide some details on the types of inspection performed on that traffic. Note that the system does not inspect fast-pathed or blacklisted traffic. For traffic handled by an access control rule or default action, flow and inspection depend on the rule action. Although rule actions are not shown in the diagram for simplicity, the system does not perform any kind of inspection on trusted or blocked traffic. Additionally, file inspection is not supported with the default action.



An incoming packet is first checked against any fast-path rules. If there is a match, the traffic is fast-pathed. If there is no match, Security Intelligence-based filtering determines if the packet is blacklisted. If not, any access control rules are applied. If the packet meets the conditions of a rule, traffic flow and inspection depend on the rule action. If no rules match the packet, traffic flow and inspection depend on the default policy action. (An exception occurs with Monitor rules, which allow traffic to continue to be evaluated.) The default action on each access control policy manages traffic that has not been fast-pathed or blacklisted, or matched by any non-Monitor rule. Note that fast-path is available only for 8000 Series devices.

You can create access control rules to provide more granular control over how you handle and log network traffic. For each rule, you specify an action (trust, monitor, block, or inspect) to apply to traffic that meets specific criteria.

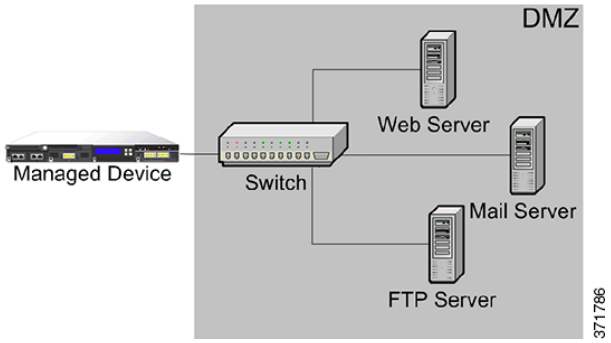
On the DMZ

The DMZ contains outward-facing servers (for example, web, FTP, DNS, and mail), and may also provide services such as mail relay and web proxy to users on the internal network.

Content stored in the DMZ is static, and changes are planned and executed with clear communication and advance notice. Attacks in this segment are typically inbound and become immediately apparent because only planned changes should occur on the servers in the DMZ. An effective access control policy for this segment tightly controls access to services and searches for any new network events.

Servers in the DMZ can contain a database that the DMZ can query via the network. Like the DMZ, there should be no unexpected changes, but the database content is more sensitive and requires greater protection than a web site or other DMZ service. A strong intrusion policy, in addition to the DMZ access control policy, is an effective strategy.

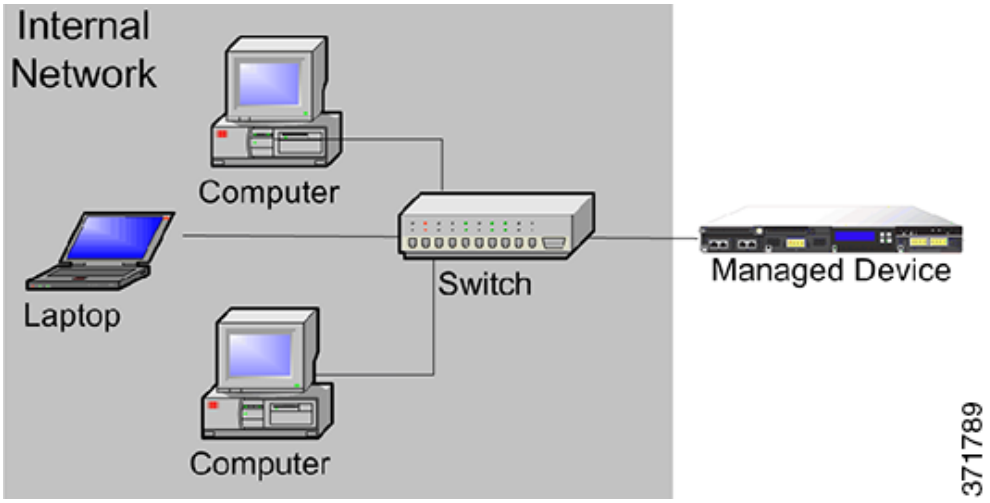
A managed device deployed on this segment can detect attacks directed to the Internet that originate from a compromised server in the DMZ. Monitoring network traffic using Network Discovery can help you monitor these exposed servers for changes (for example, an unexpected service suddenly appearing) that could indicate a compromised server in the DMZ.



On the Internal Network

A malicious attack can originate from a computer on your internal network. This can be a deliberate act (for example, an unknown computer appears unexpectedly on your network), or an accidental infection (for example, a work laptop infected off-site is connected to the network and spreads a virus). Risk on the internal network can also be outbound (for example, a computer sends information to a suspicious external IP address).

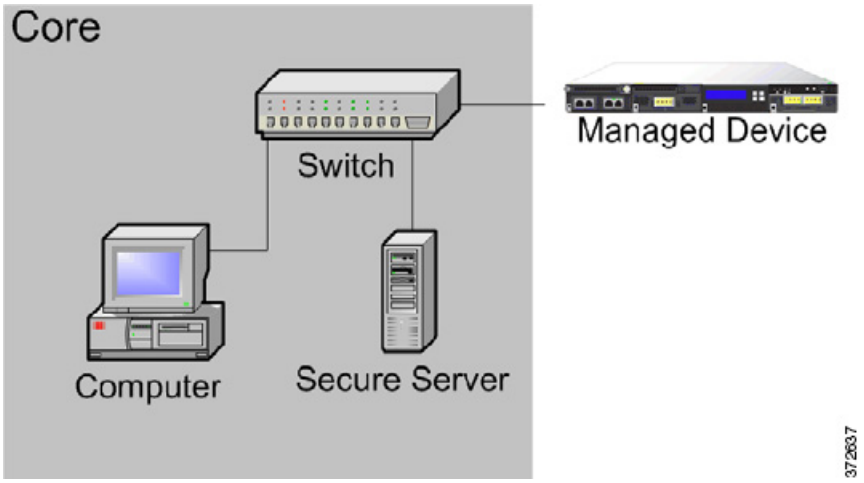
This dynamic network requires a strict access control policy for all internal traffic in addition to outbound traffic. Add access control rules to tightly control traffic between users and applications.



On the Core Network

Core assets are those assets critical to the success of your business that must be protected at all cost. Although core assets vary depending on the nature of your business, typical core assets include financial and management centers or intellectual property repositories. If the security on the core assets is breached, your business can be destroyed.

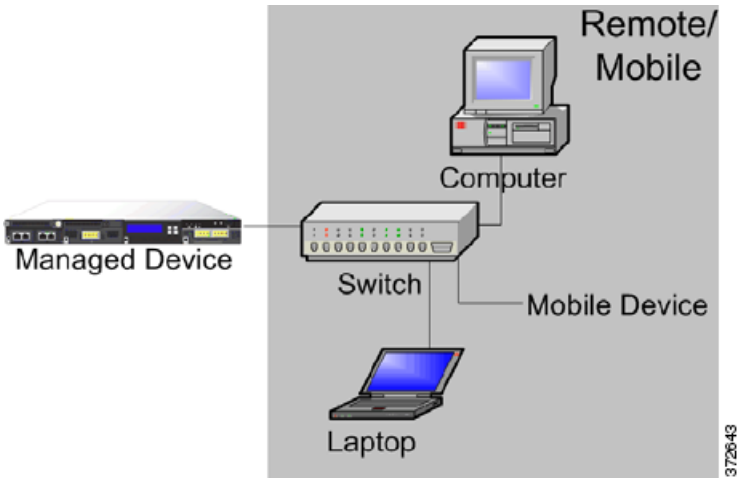
Although this segment must be readily available for your business to function, it must be tightly restricted controlled. Access control should ensure that these assets cannot be reached by those network segments with the highest risk, such as remote networks or mobile devices. Always use the most aggressive control on this segment, with strict rules for user and application access.



On a Remote or Mobile Network

Remote networks, located off-site, often use a virtual private network (VPN) to provide access to the primary network. Mobile devices and the use of personal devices for business purposes (for example, using a “smart phone” to access corporate email) are becoming increasingly common.

These networks can be highly dynamic environments with rapid and continual change. Deploying a managed device on a dedicated mobile or remote network allows you to create a strict access control policy to monitor and manage traffic to and from unknown external sources. Your policy can reduce your risk by rigidly limiting how users, network, and applications access core resources.



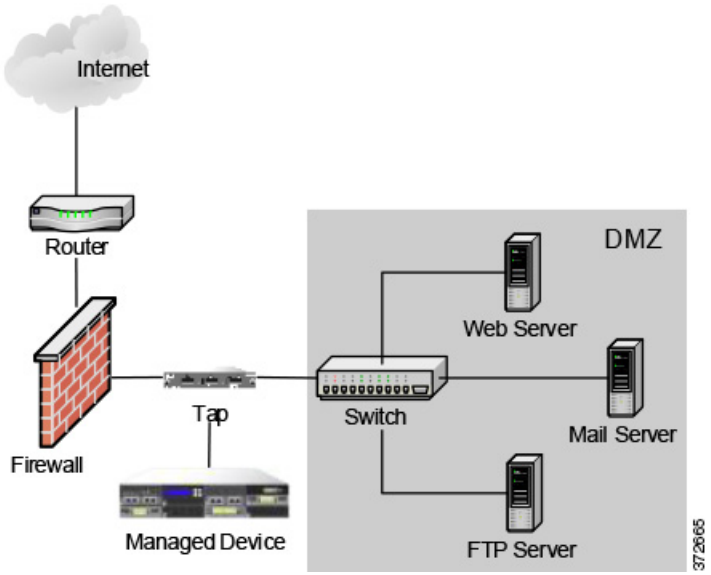
Using Multiple Sensing Interfaces on a Managed Device

The managed device offers multiple sensing interfaces on its network modules. You can use multiple sensing interfaces on managed devices to:

- recombine the separate connections from a network tap
- capture and evaluate traffic from different networks
- perform as a virtual router
- perform as a virtual switch

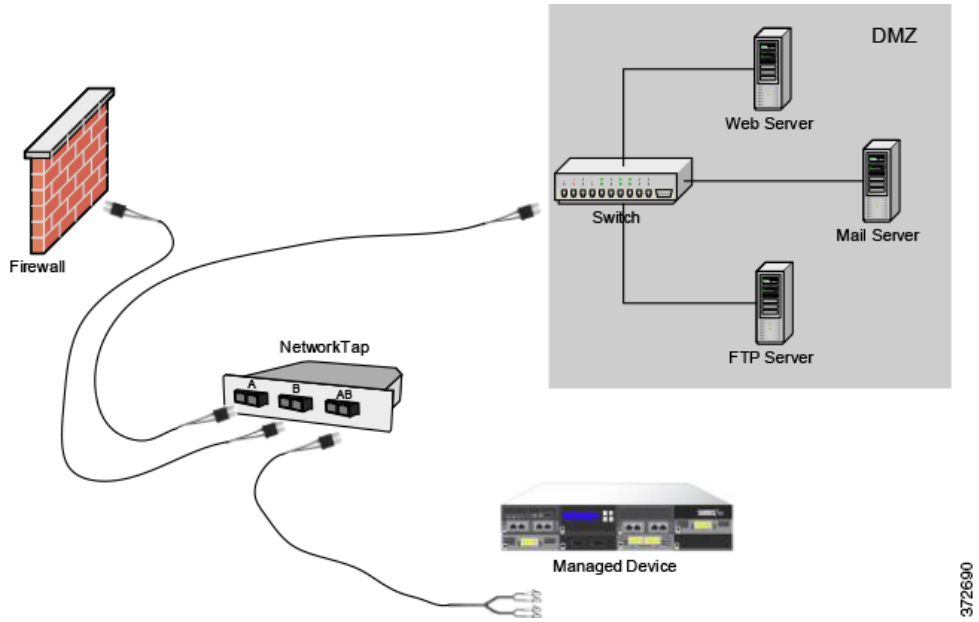
Note Although each sensing interface is capable of receiving the full throughput for which the device is rated, the total traffic on the managed device cannot exceed its bandwidth rating without some packet loss.

Deploying multiple sensing interfaces on a managed device with a network tap is a straightforward process. The following diagram shows a network tap installed on a high-traffic network segment.

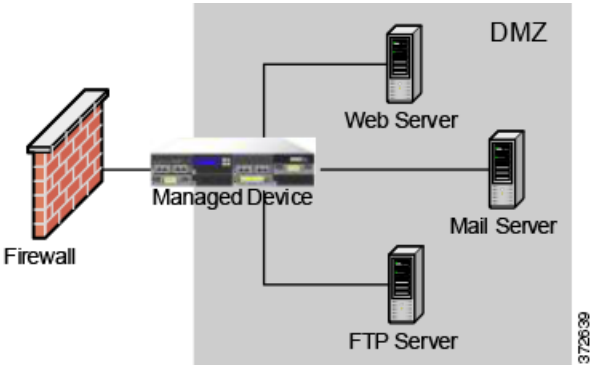


In this scenario, the tap transmits incoming and outgoing traffic through separate sensing interfaces. When you connect the multiple sensing interface adapter card on the managed device to the tap, the managed device is able to combine the traffic into a single data stream so that it can be analyzed.

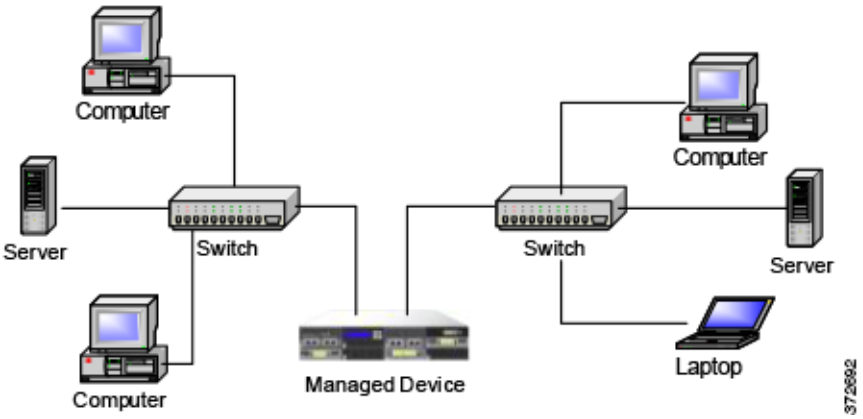
Note that with a gigabit optical tap, as shown in the illustration below, both sets of sensing interfaces on the managed device are used by the connectors from the tap.



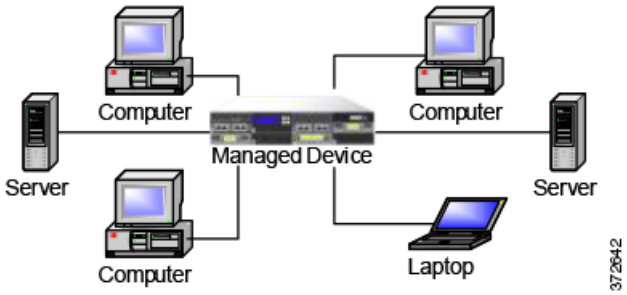
You can use the virtual switch to replace both the tap and the switch in your deployment. Note that if you replace the tap with a virtual switch, you lose the tap packet delivery guarantee.



You can also create interfaces to capture data from separate networks. The following diagram shows a single device with a dual sensing interface adapter and two interfaces connected to two networks.



In addition to using one device to monitor both network segments, you can use the virtual switch capability of the device to replace both switches in your deployment.



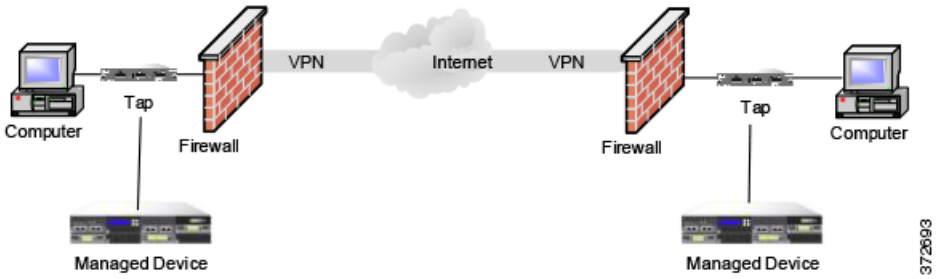
Complex Network Deployments

Your enterprise's network may require remote access, such as using a VPN, or have multiple entry points, such as a business partner or banking connection.

Integrating with VPNs

Virtual private networks, or VPNs, use IP tunneling techniques to provide the security of a local network to remote users over the Internet. In general, VPN solutions encrypt the data payload in an IP packet. The IP header is unencrypted so that the packet can be transmitted over public networks in much the same way as any other packet. When the packet arrives at its destination network, the payload is decrypted and the packet is directed to the proper host.

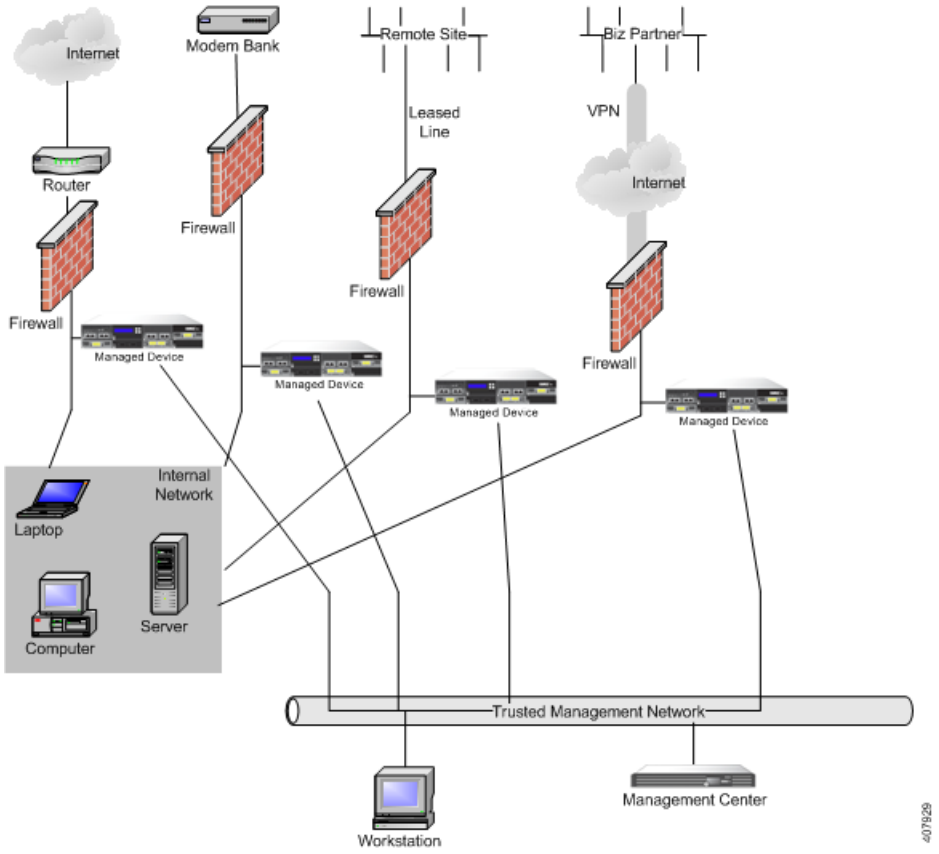
Because network appliances cannot analyze the encrypted payload of a VPN packet, placing managed devices outside the terminating endpoints of the VPN connections ensures that all packet information can be accessed. The following diagram illustrates how managed devices can be deployed in a VPN environment.



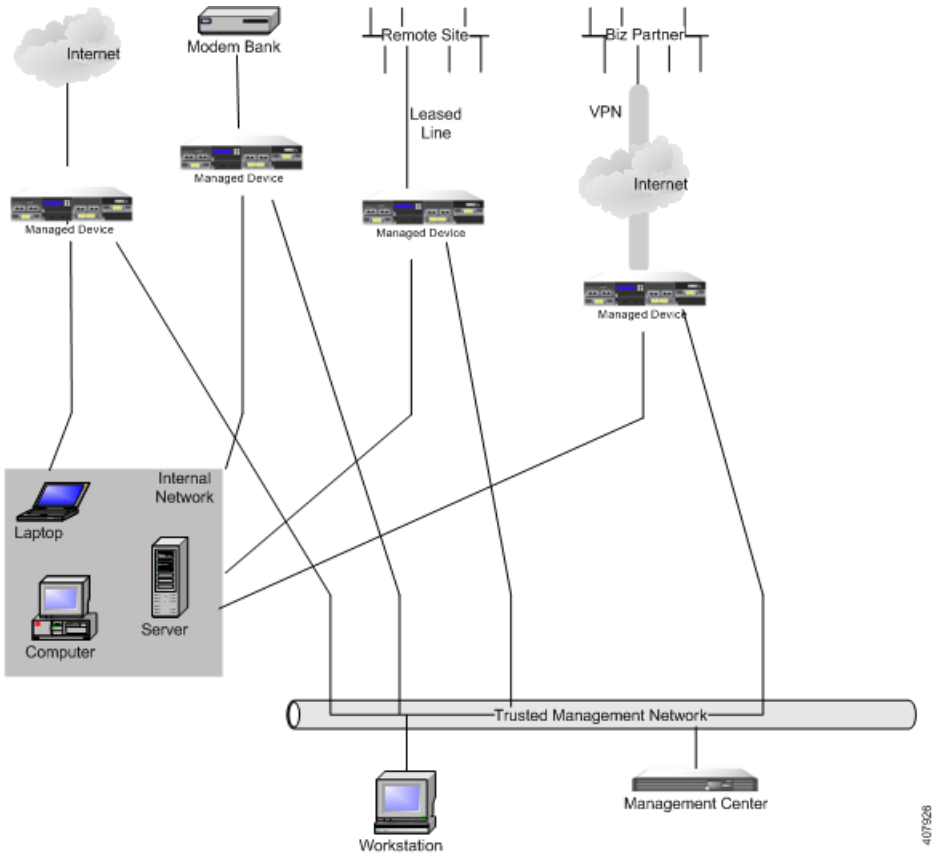
You can replace the firewall and the tap on either side of the VPN connection with the managed device. Note that if you replace the tap with a managed device, you lose the tap packet delivery guarantee.

Detecting Intrusions on Other Points of Entry

Many networks include more than one access point. Instead of a single border router that connects to the Internet, some enterprises use a combination of the Internet, modem banks, and direct links to business partner networks. In general, you should deploy managed devices near firewalls (either inside the firewall, outside the firewall, or both) and on network segments that are important to the integrity and confidentiality of your business data. The following diagram shows how managed devices can be installed at key locations on a complex network with multiple entry points.

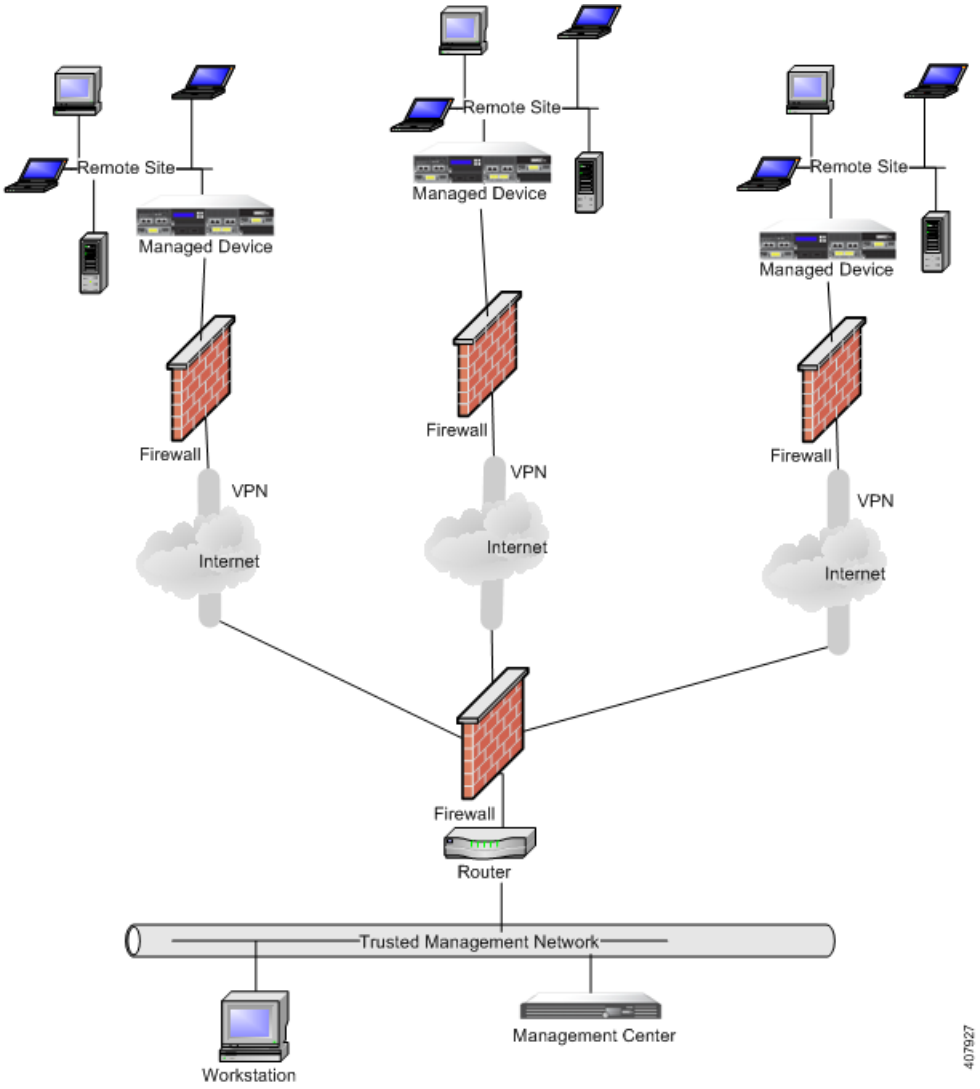


You can replace the firewall and the router with the managed device deployed on that network segment.

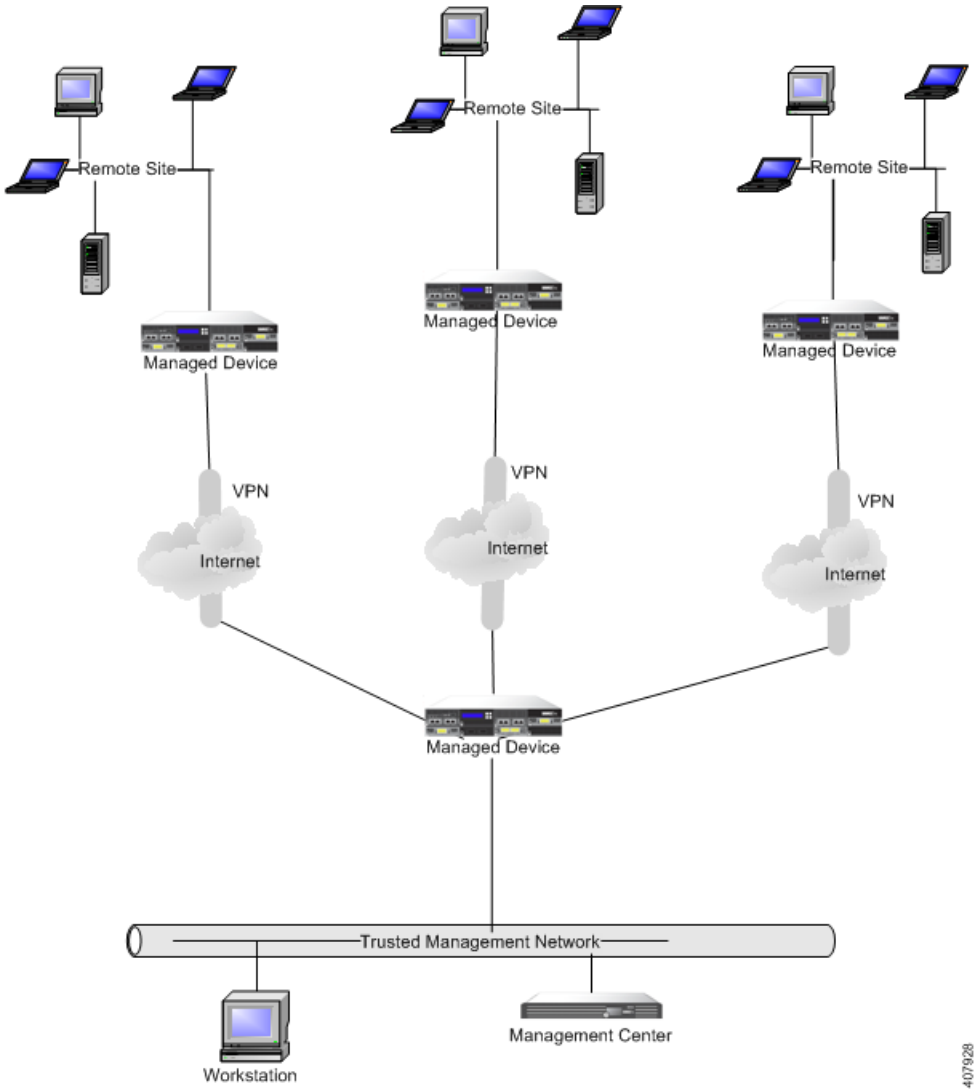


Deploying in Multi-Site Environments

Many organizations want to extend intrusion detection across a geographically disparate enterprise and then analyze all the data from one location. The Firepower System supports this by offering the Firepower Management Center, which aggregates and correlates events from managed devices deployed throughout the organization's many locations. Unlike deploying multiple managed devices and Firepower Management Centers in the same geographic location on the same network, when deploying managed devices in disparate geographic locations, you must take precautions to ensure the security of the managed devices and the data stream. To secure the data, you must isolate the managed devices and Firepower Management Center from unprotected networks. You can do this by transmitting the data stream from the managed devices over a VPN or with some other secure tunneling protocol as shown in the following diagram.



You can replace the firewalls and routers with the managed device deployed in each network segment.



Integrating Multiple Management Interfaces within a Complex Network

You can configure multiple management interfaces in any deployment to isolate traffic from devices that monitor different networks and are managed by the same Firepower Management Center. Multiple management interfaces allow you to add a management interface with a unique IP address (IPv4 or IPv6) to your Firepower Management Center, and create a route from that management interface to a network that contains the device you want to manage. When you register your device to the new management interface, traffic on that device is isolated from traffic on devices registered to the default management interface on the Firepower Management Center.

Tip You must register a device to the static IP address of any management interface other than the default (`eth0`) management interface. DHCP is supported only on the default management interface.

Multiple management interfaces are supported in a NAT environment provided you do not use separate management interfaces for traffic channels. See Deploying on a Management Network, page 2-1 for more information. Note that Lights-Out Management is supported only on the default management interface, not additional management interfaces.

After you install your Firepower Management Center, you configure multiple management interfaces using the web interface. See Configuring Appliance Settings in the*Firepower Management Center Configuration Guide* for more information.

Integrating Managed Devices within Complex Networks

You can deploy managed devices in more complex network topologies than a simple multi-sector network. This section describes the issues surrounding network discovery and vulnerability analysis when deploying in environments where proxy servers, NAT devices, and VPNs exist, in addition to information about using the Firepower Management Center to manage multiple managed devices and the deployment and management of managed devices in a multi-site environment.

Integrating with Proxy Servers and NAT

Network address translation (NAT) devices or software may be employed across a firewall, effectively hiding the IP addresses of internal hosts behind a firewall. If managed devices are placed between these devices or software and the hosts being monitored, the system may incorrectly identify the hosts behind the proxy or NAT device. In this case, Cisco recommends that you position managed devices inside the network segment protected by the proxy or NAT device to ensure that hosts are correctly detected.

Integrating with Load Balancing Methods

In some network environments, “server farm” configurations are used to perform network load balancing for services such as web hosting, FTP storage sites, and so on. In load balancing environments, IP addresses are shared between two or more hosts with unique operating systems. In this case, the system detects the operating system changes and cannot deliver a static operating system identification with a high confidence value. Depending on the number of different operating systems on the affected hosts, the system may generate a large number of operating system change events or present a static operating system identification with a lower confidence value.

Other Detection Considerations

If an alteration has been made to the TCP/IP stack of the host being identified, the system may not be able to accurately identify the host operating system. In some cases, this is done to improve performance. For instance, administrators of Windows hosts running the Internet Information Services (IIS) Web Server are encouraged to increase the TCP window size to allow larger amounts of data to be received, thereby improving performance. In other instances, TCP/IP stack alteration may be used to obfuscate the true operating system to preclude accurate identification and avoid targeted attacks. The likely scenario that this intends to address is where an attacker conducts a reconnaissance scan of a network to identify hosts with a given operating system followed by a targeted attack of those hosts with an exploit specific to that operating system.

Prepare to Installation

This chapter prepares you to install the Cisco Firepower 7000 and 8000 Series appliances and contains the following sections:

Installation Guidelines

When you are installing an appliance, use the following guidelines:

- Ensure that there is adequate space around the appliance to allow for servicing the appliance and for adequate airflow. The airflow in the appliance is from front to back.
- Ensure that the air-conditioning can keep the security appliance at a temperature of 41 to 95°F (5 to 35°C).
- Ensure that the cabinet or rack meets the rack requirements.
- Ensure that the site power meets the power requirements listed in 770 W AC Power Supply. If available, you can use an uninterruptible power supply (UPS) to protect against power failures.

Safety Recommendations

Use the information in the following sections to help ensure your safety and to protect the chassis. This information may not address all potentially hazardous situations in your working environment, so be alert and exercise good judgment at all times.

Observe these safety guidelines:

- Observe good housekeeping in the area of the machines during and after maintenance.
- Keep the area clear and dust-free before, during, and after installation.
- Keep tools away from walkways, where you and others might trip over them.
- Do not wear loose clothing or jewelry, such as earrings, bracelets, chains, or metal fasteners for your clothing that could get caught in the chassis.

Caution Metal objects are good electrical conductors.

- Do not wear loose clothing that can be trapped in the moving parts of a machine. Ensure that your sleeves are fastened or rolled up above your elbows. If your hair is long, fasten it.
- Wear safety glasses if you are working under any conditions that might be hazardous to your eyes.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Never attempt to lift an object that is too heavy for one person.
- When lifting any heavy object:
  - Lifting the chassis may require two people.
  - Do not attempt to lift any objects that weigh more than 16 kg (35 lb) or objects that you think are too heavy for you
  - Ensure you can stand safely without slipping.
  - Distribute the weight of the object equally between your feet.
  - Lift by standing or by pushing up with your leg muscles; this action removes the strain from the muscles in your back.
  - Use a slow lifting force. Never move suddenly or twist when you attempt to lift.
- Do not perform any action that causes hazards or makes the equipment unsafe.
- Before you start the machine, ensure that other service representatives and the customer's personnel are not in a hazardous position.
- Place removed covers and other parts in a safe place, away from all personnel, while you are servicing the machine.
- Insert the ends of your necktie or scarf inside clothing or fasten it with a nonconductive clip, approximately 8 centimeters (3 inches) from the end.
- To avoid electrical shock, do not open or remove chassis covers or metal parts without proper instruction.
- Wear safety glasses when you are: hammering, drilling, soldering, cutting wire, attaching springs, using solvents, or working in any other conditions that might be hazardous to your eyes.
- There must be ample clearance on all sides of the chassis for the cooling air inlet and exhaust ports, as well as for access to the network interface modules (no less than 2 inches).
- Remove all factory packaging before using the appliance.

- Do not cover or block vents, or otherwise enclose the appliance.

Maintain Safety with Electricity

Warning **Before working on a chassis, be sure the power cord is unplugged. Be sure to read the Regulatory and Compliance Safety Information document before installing the security appliance.**

Follow these guidelines when working on equipment powered by electricity:

- Before beginning procedures that require access to the interior of the chassis, locate the emergency power-off switch for the room in which you are working. Then, if an electrical accident occurs, you can act quickly to turn off the power.
- Do not work alone if potentially hazardous conditions exist anywhere in your work space.
- Never assume that power is disconnected; always check.
- Look carefully for possible hazards in your work area, such as moist floors, ungrounded power extension cables, frayed power cords, and missing safety grounds.
- If an electrical accident occurs:
  - Use caution; do not become a victim yourself.
  - Disconnect power from the system.
  - If possible, send another person to get medical aid. Otherwise, assess the condition of the victim, and then call for help.
  - Determine whether the person needs rescue breathing or external cardiac compressions; then take appropriate action.
- Use the chassis within its marked electrical ratings and product usage instructions.
- The Firepower Management Center security appliances are equipped with an AC-input power supply, which is shipped with a three-wire electrical cord with a grounding-type plug that fits into a grounding-type power outlet only. Do not circumvent this safety feature. Equipment grounding should comply with local and national electrical codes.

Prevent Electrostatic Discharge Damage

Electrostatic discharge (ESD) occurs when electronic components are improperly handled, and it can damage equipment and impair electrical circuitry, resulting in intermittent or complete failure.

Always follow ESD-prevention procedures when removing and replacing components. Ensure that the chassis is electrically connected to an earth ground. Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. Connect the grounding clip to an unpainted surface of the chassis frame to safely ground ESD voltages. To properly guard against ESD damage and shocks, the wrist strap and cord must operate effectively. If no wrist strap is available, ground yourself by touching the metal part of the chassis.

For safety, periodically check the resistance value of the anti-static strap, which should be between one and 10 megohms.

Site Environment

When planning the site layout and equipment locations, consider the information in the next section to help avoid equipment failures and reduce the possibility of environmentally caused shutdowns. If you are currently experiencing shutdowns or unusually high error rates with your existing equipment, these considerations may help you isolate the cause of failures and prevent future problems.

Power Supply Considerations

When installing the chassis, consider the following:

- Check the power at the site before installing the chassis to ensure that it is “clean” (free of spikes and noise). Install a power conditioner, if necessary, to ensure proper voltages and power levels in the appliance-input voltage.
- Install proper grounding for the site to avoid damage from lightning and power surges.
- The chassis does not have a user-selectable operating range. Refer to the label on the chassis for the correct appliance input-power requirement.
- Several styles of AC-input power supply cords are available for the appliance; make sure that you have the correct style for your site.
- If you are using dual redundant (1+1) power supplies, we recommend that you use independent electrical circuits for each power supply. The power supplies are hot-swappable.
- Install an uninterruptible power source for your site, if possible.

Equipment Rack Configuration Considerations

Consider the following when planning an equipment-rack configuration:

- If you are mounting a chassis in an open rack, make sure that the rack frame does not block the intake or exhaust ports.
- Be sure enclosed racks have adequate ventilation. Make sure that the rack is not overly congested as each chassis generates heat. An enclosed rack should have louvered sides and a fan to provide cooling air.
- In an enclosed rack with a ventilation fan in the top, heat generated by equipment near the bottom of the rack can be drawn upward and into the intake ports of the equipment above it in the rack. Ensure that you provide adequate ventilation for equipment at the bottom of the rack.
- Baffles can help to isolate exhaust air from intake air, which also helps to draw cooling air through the chassis. The best placement of the baffles depends on the airflow patterns in the rack. Experiment with different arrangements to position the baffles effectively.

Installing a Firepower Managed Device

Firepower System appliances are easily installed on your network as part of a larger Firepower System deployment. You install devices on network segments to inspect traffic and generate intrusion events based on the intrusion policy applied to it. This data is transmitted to a Firepower Management Center, which manages one or more devices to correlate data across your full deployment, and coordinate and respond to threats to your security.

Tip You can use multiple management interfaces to improve performance or to isolate and manage traffic from two different networks. You configure the default management interface (`eth0`) during the initial installation. You can configure additional management interfaces after installation from the user interface. For more information, see *Firepower Management Center Configuration Guide*.

You can pre-configure multiple appliances at one location to be used in different deployment locations. For guidance on pre-configuring, see Preconfiguring Firepower Managed Devices, page E-1.

Note See the ASA documentation for information on installing ASA FirePOWER devices.

Included Items

The following is a list of components that ship with Firepower devices. As you unpack the system and the associated accessories, check that your package contents are complete as follows:

- one appliance
- power cord (two power cords are included with appliances that include redundant power supplies; the power supplies are hot-swappable)
- Category 5e Ethernet straight-through cables: two for a Firepower device
- one rack-mounting kit (required tray and rack-mounting kit available separately for the Firepower 7010, 7020, 7030, and 7050)

Security Considerations

Before you install your appliance, Cisco recommends that you consider the following:

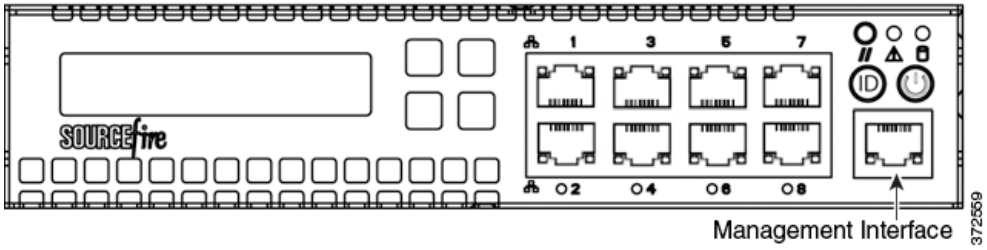
- Locate your appliance in a lockable rack within a secure location that prevents access by unauthorized personnel.
- Allow only trained and qualified personnel to install, replace, administer, or service the appliance.
- Always connect the management interface to a secure internal management network that is protected from unauthorized access.
- Identify the specific workstation IP addresses that can be allowed to access appliances. Restrict access to the appliance to only those specific hosts using Access Lists within the appliance's system policy. For more information, see the *Firepower Management Center Configuration Guide*.

Identifying the Management Interfaces

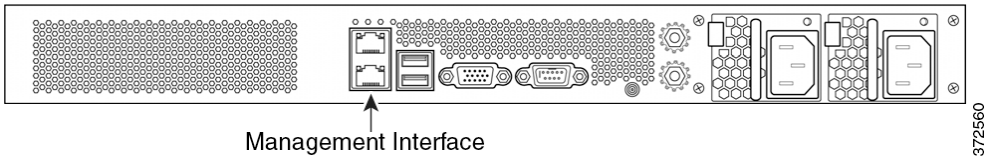
You connect each appliance in your deployment to the network using the management interface. This allows the Firepower Management Center to communicate with and administer the devices it manages. Refer to the correct illustration for your appliance as you follow the installation procedure.

Firepower 7000 Series

The Firepower 7010, 7020, 7030, and 7050 are 1U appliances that are one-half the width of the chassis tray. The following illustration of the front of the chassis indicates the default management interface.

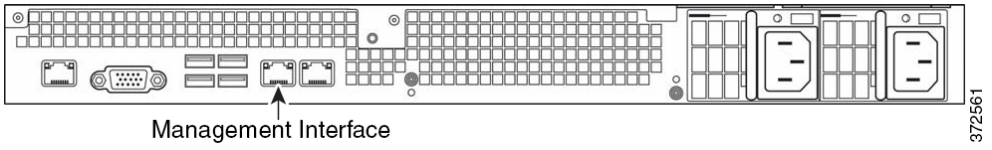


The Firepower 7110/7120, the 7115/7125, and the AMP7150 are available as 1U appliances. The following illustration of the rear of the chassis indicates the location of the default management interface.

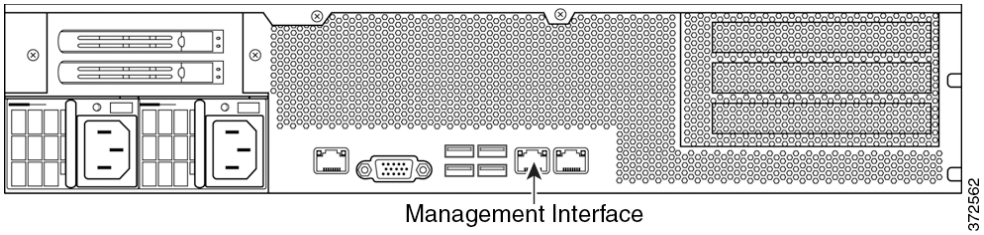


Firepower 8000 Series

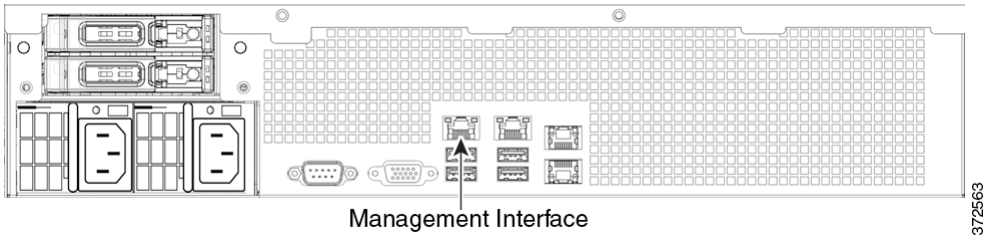
The Firepower 8120, 8130, 8140, and AMP8150 are available as 1U appliances. The following illustration of the rear of the chassis indicates the location of the default management interface.



The Firepower 8250 is available as a 2U appliance. The Firepower 8260, 8270, and 8290 are available as 2U appliances with one, two, or three secondary 2U appliances. The following illustration of the rear of the chassis indicates the location of the default management interface for each 2U appliance.



The Firepower and AMP 8350 is available as a 2U appliance. The Firepower and AMP 8360, 8370, and 8390 are available as 2U appliances with one, two, or three secondary 2U appliances. The following illustration of the rear of the chassis indicates the location of the default management interface for each 2U appliance.



Identifying the Sensing Interfaces

Firepower devices connect to network segments using sensing interfaces. The number of segments each device can monitor depends on the number of sensing interfaces on the device and the type of connection (passive, inline, routed, or switched) that you want to use on the network segment.

The following sections describe the sensing interfaces for each Firepower device:

- To locate the sensing interfaces on the 7000 Series, see Firepower 7000 Series, page 4-3.
- To locate the module slots on the 8000 Series on the Firepower 8000 Series, page 4-7.
- To locate the sensing interfaces on the 8000 Series NetMods, see Firepower 8000 Series Modules, page 4-8.

For information on connection types, see Understanding Sensing Interfaces, page 3-2.

Firepower 7000 Series

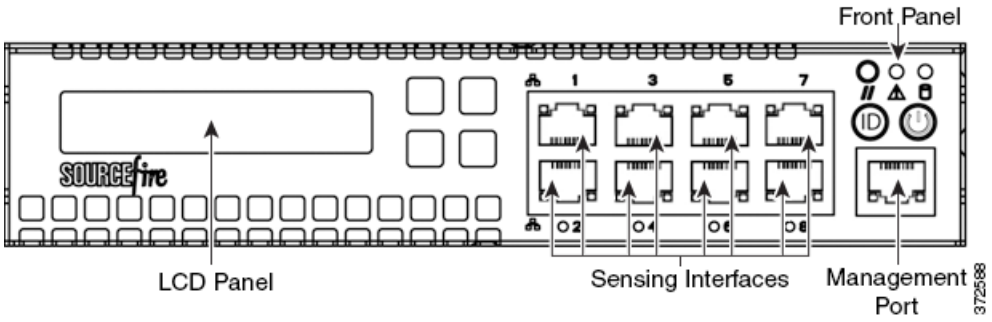
The 7000 Series is available in the following configurations:

- 1U device one-half the width of the rack tray with eight copper interfaces, each with configurable bypass capability.
- 1U device with either eight copper interfaces or eight fiber interfaces, each with configurable bypass capability
- 1U device with four copper interfaces with configurable bypass capability and eight small form-factor pluggable (SFP) ports without bypass capability

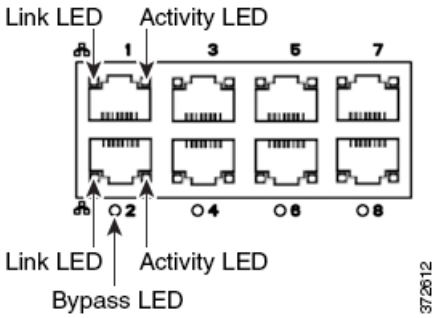
Firepower 7010, 7020, 7030, and 7050

The Firepower 7010, 7020, 7030, and 7050 are delivered with eight copper port sensing interfaces, each with configurable bypass capability. The following illustration of the front of the chassis indicates the location of the sensing interfaces.

Figure 4-1 Eight Port 1000BASE-T Copper Configurable Bypass Interfaces



You can use these connections to passively monitor up to eight separate network segments. You can also use paired interfaces in inline or inline with bypass mode to deploy the device as an intrusion prevention system on up to four networks.



If you want to take advantage of the device's automatic bypass capability, you must connect two interfaces vertically (interfaces 1 and 2, 3 and 4, 5 and 6, or 7 and 8) to a network segment. Automatic bypass capability allows traffic to flow even if the device fails or loses power. After you cable the interfaces, you use the web interface to configure a pair of interfaces as an inline set and enable bypass mode on the inline set.

Firepower 7110 and 7120

The Firepower 7110 and 7120 are delivered with eight copper port sensing interfaces, or eight fiber port sensing interfaces, each with configurable bypass capability. The following illustration of the front of the chassis indicates the location of the sensing interfaces.

Figure 4-2 Firepower 7110 and 7120 Copper Interfaces

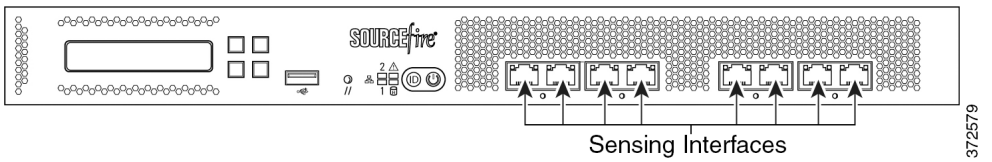
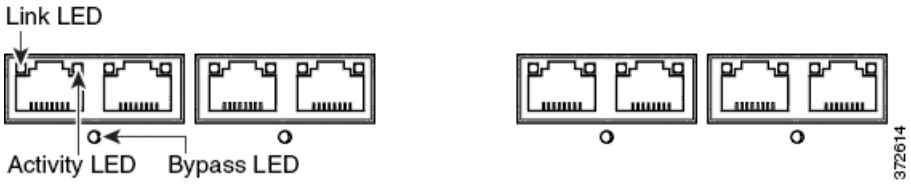


Figure 4-3 Eight-Port 1000BASE-T Copper Interfaces



You can use these connections to passively monitor up to eight separate network segments. You can also use paired interfaces in inline or inline with bypass mode to deploy the device as an intrusion prevention system on up to four networks.

If you want to take advantage of the device's automatic bypass capability, you must connect either the two interfaces on the left or the two interfaces on the right to a network segment. Automatic bypass capability allows traffic to flow even if the device fails or loses power. After you cable the interfaces, you use the web interface to configure a pair of interfaces as an inline set and enable bypass mode on the inline set.

Figure 4-4 Firepower 7110 and 7120 Fiber Interfaces

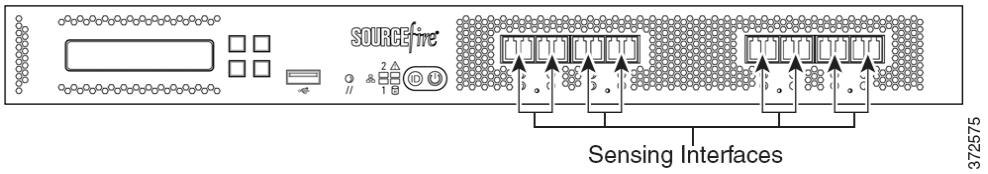


Figure 4-5 Eight-Port 1000BASE-SX Fiber Configurable Bypass

The eight-port 1000BASE-SX fiber configurable bypass configuration uses LC-type (Local Connector) optical transceivers.

You can use these connections to passively monitor up to eight separate network segments. You can also use paired interfaces in inline or inline with bypass mode to deploy the device as an intrusion prevention system on up to four networks.

Tip For best performance, use the interface sets consecutively. If you skip any interfaces, you may experience degraded performance.

If you want to take advantage of the device's automatic bypass capability, you must connect either the two interfaces on the left or the two interfaces on the right to a network segment. Automatic bypass capability allows traffic to flow even if the device fails or loses power. After you cable the interfaces, you use the web interface to configure a pair of interfaces as an inline set and enable bypass mode on the inline set.

Firepower 7115, 7125, and AMP7150

The Firepower 7115, 7125, and AMP7150 devices are delivered with four-port copper interfaces with configurable bypass capability, and eight hot-swappable small form-factor pluggable (SFP) ports without bypass capability. The following illustration of the front of the chassis indicates the location of the sensing interfaces.

Figure 4-6 Firepower 7115, 7125, and AMP7150 Copper and SFP Interfaces

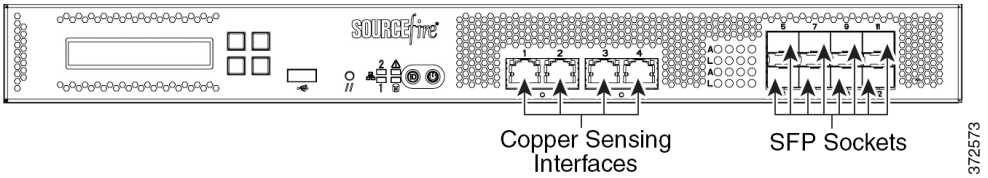
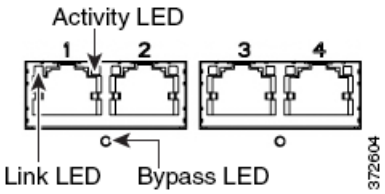


Figure 4-7 Four 1000BASE-T Copper Interfaces



You can use the copper interfaces to passively monitor up to four separate network segments. You can also use paired interfaces in inline or inline with bypass mode to deploy the device as an intrusion prevention system on up to two networks.

If you want to take advantage of the device's automatic bypass capability, you must connect either the two interfaces on the left or the two interfaces on the right to a network segment. Automatic bypass capability allows traffic to flow even if the device fails or loses power. After you cable the interfaces, you use the web interface to configure a pair of interfaces as an inline set and enable bypass mode on the inline set.

SFP Interfaces

When you install Cisco SFP transceivers into the SFP sockets, you can passively monitor up to eight separate network segments. You can also use paired interfaces in inline, non-bypass mode to deploy the device as an intrusion detection system on up to four networks.

Cisco SFP transceivers are available in 1G copper, 1G short range fiber, or 1G long range fiber, and are hot-swappable. You can use any combination of copper or fiber transceivers in your device in either passive or inline configuration. Note that SFP transceivers do not have bypass capability and should not be used in intrusion prevention deployments. To ensure compatibility, use only SFP transceivers available from Cisco. See Using SFP Transceivers in 3D71x5 and AMP7150 Devices, page B-1 for more information.

Figure 4-8 Sample SFP Transceivers

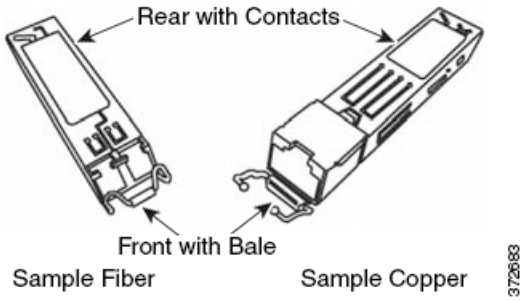
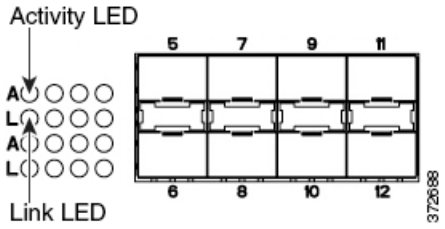


Figure 4-9 SFP Sockets



Firepower 8000 Series

The 8000 Series is available as a 1U device with a 10G network switch or a 2U device with either a 10G or a 40G network switch. This device can be shipped fully assembled, or you can install the network modules (NetMods) that contain the sensing interfaces.

Note If you install a NetMod in an incompatible slot on your device (for example, inserting a 40G NetMod in slots 1 and 4 on a Firepower 8250 or Firepower or AMP 8350) or a NetMod is otherwise incompatible with your system, an error or warning message appears in the web interface of the managing Firepower Management Center when you attempt to configure the NetMod. Contact Support for assistance.

The following modules contain configurable bypass sensing interfaces:

- a quad-port 1000BASE-T copper interface with configurable bypass capability
- a quad-port 1000BASE-SX fiber interface with configurable bypass capability
- a dual-port 10GBASE (MMSR or SMLR) fiber interface with configurable bypass capability
- a dual-port 40GBASE-SR4 fiber interface with configurable bypass capability (2U devices only)

The following modules contain non-bypass sensing interfaces:

- a quad-port 1000BASE-T copper interface without bypass capability
- a quad-port 1000BASE-SX fiber interface without bypass capability
- a dual-port 10GBASE (MMSR or SMLR) fiber interface without bypass capability

In addition, a stacking module combines the resources of two or more identically configured appliances. The stacking module is optional on the Firepower 8140, 8250, and 8350; and is provided in the Firepower 8260, 8270, 8290 and the Firepower and AMP 8360, 8370, 8390 stacked configurations.

Caution Modules are **not** hot-swappable. See Inserting and Removing Firepower 8000 Series Modules, page C-1 for more information.

The following illustrations of the front of the chassis indicates the location of the module slots that contain the sensing interfaces.

Figure 4-10 Firepower 81xx Family Front Chassis View

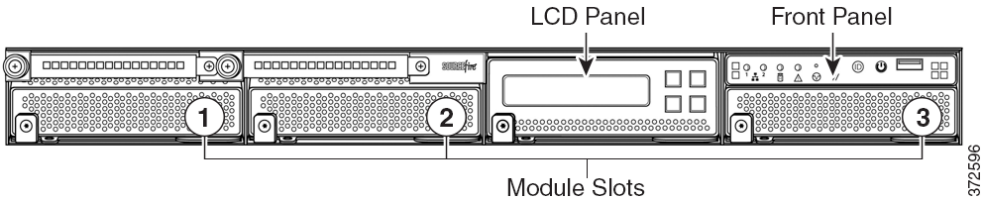
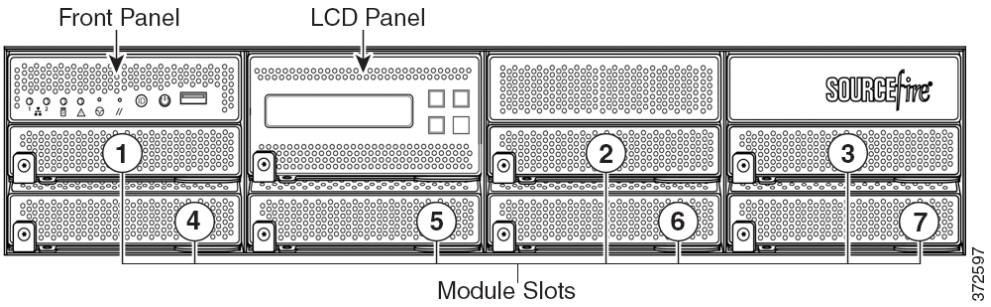


Figure 4-11 Firepower 82xx Family and Firepower and AMP 83xx Family Front Chassis View



Firepower 8000 Series Modules

The Firepower 8000 Series can be delivered with the following modules with configurable bypass capability:

- a quad-port 1000BASE-T copper interface with configurable bypass capability. See Figure 4-12Quad-Port 1000BASE-T Copper Configurable Bypass NetMod, page 4-9 for more information.
- a quad-port 1000BASE-SX fiber interface with configurable bypass capability. See Figure 4-13Quad-Port 1000BASE-SX Fiber Configurable Bypass NetMod, page 4-9 for more information.
- a dual-port 10GBASE (MMSR or SMLR) fiber interface with configurable bypass capability. See Figure 4-14Dual-Port 10GBASE (MMSR or SMLR) Fiber Configurable Bypass NetMod, page 4-10 for more information.
- a dual-port 40GBASE-SR4 fiber interface with configurable bypass capability. See Figure 4-15Dual-Port 40GBASE-SR4 Fiber Configurable Bypass NetMod, page 4-10 for more information.

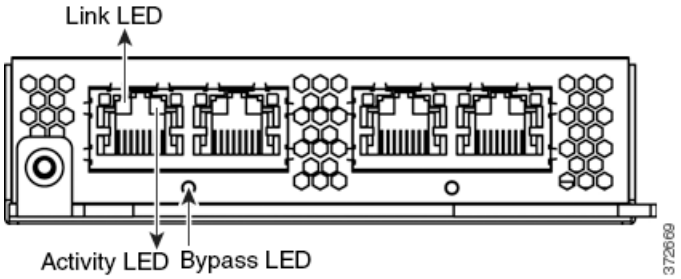
The Firepower 8000 Series can be delivered with the following modules without configurable bypass capability:

- a quad-port 1000BASE-T copper interface without bypass capability. See Figure 4-17Quad-Port 1000BASE-T Copper Non-Bypass NetMod, page 4-11 for more information.

- a quad-port 1000BASE-SX fiber interface without bypass capability. See Figure 4-18Quad-Port 1000BASE-SX Fiber Non-Bypass NetMod, page 4-12 for more information.
- a quad-port 10GBASE (MMSR or SMLR) fiber interface without bypass capability. See Figure 4-19Quad-Port 10GBASE (MMSR or SMLR) Fiber Non-Bypass NetMod, page 4-12 for more information.

A stacking module is optional on the Firepower 8140, 8250, and 8350; and is provided in the Firepower 8260, 8270, 8290 and the Firepower 8360, 8370, 8390 stacked configurations. See Firepower 8000 Series Stacking Module, page 4-12 for more information.

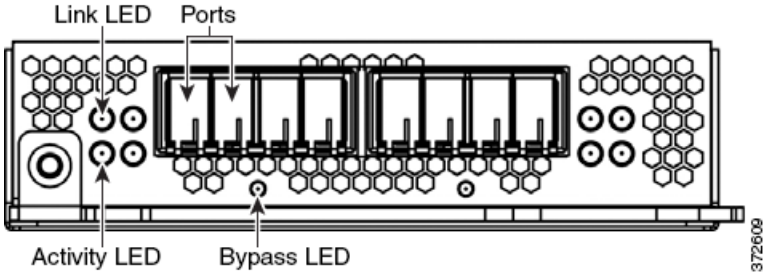
Figure 4-12 Quad-Port 1000BASE-T Copper Configurable Bypass NetMod



You can use these connections to passively monitor up to four separate network segments. You also can use paired interfaces in inline or inline with bypass mode, which allows you to deploy the device as an intrusion prevention system on up to two networks.

If you want to take advantage of the device's automatic bypass capability, you must connect either the two interfaces on the left or the two interfaces on the right to a network segment. This allows traffic to flow even if the device fails or loses power. You must also use the web interface to configure a pair of interfaces as an inline set and enable bypass mode on the inline set.

Figure 4-13 Quad-Port 1000BASE-SX Fiber Configurable Bypass NetMod



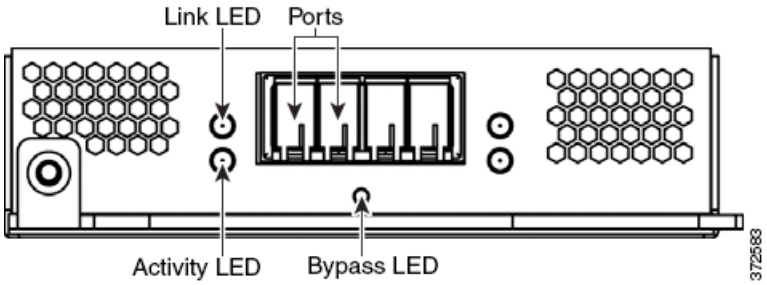
The quad-port 1000BASE-SX fiber configurable bypass configuration uses LC-type (Local Connector) optical transceivers.

You can use this configuration to passively monitor up to four separate network segments. You also can use paired interfaces in inline or inline with bypass mode, which allows you to deploy the managed device as an intrusion prevention system on up to two separate networks.

Tip For best performance, use the interface sets consecutively. If you skip interfaces, you may experience degraded performance.

If you want to take advantage of a device's automatic bypass capability, you must connect the two interfaces on the left or the two interfaces on the right to a network segment. This allows traffic to flow even if the device fails or loses power. You must also use the web interface to configure a pair of interfaces as an inline set and enable bypass mode on the inline set.

Figure 4-14 Dual-Port 10GBASE (MMSR or SMLR) Fiber Configurable Bypass NetMod



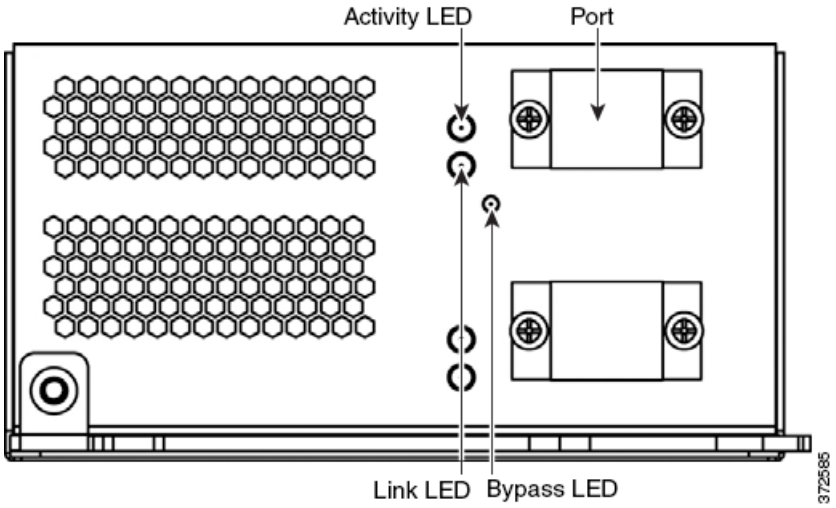
The dual-port 10GBASE fiber configurable bypass configuration uses LC-type (Local Connector) optical transceivers. Note that these can be either MMSR or SMLR interfaces.

You can use this configuration to passively monitor up to two separate network segments. You also can use paired interfaces in inline or inline with bypass mode, which allows you to deploy the managed device as an intrusion prevention system on a single network.

Tip For best performance, use the interface sets consecutively. If you skip interfaces, you may experience degraded performance.

If you want to take advantage of a device's automatic bypass capability, you must connect two interfaces to a network segment. This allows traffic to flow even if the device fails or loses power. You must also use the web interface to configure a pair of interfaces as an inline set and enable bypass mode on the inline set.

Figure 4-15 Dual-Port 40GBASE-SR4 Fiber Configurable Bypass NetMod



The dual-port 40GBASE-SR4 fiber configurable bypass configuration uses MPO (Multiple-Fiber Push On) connector optical transceivers.

You can use the 40G NetMod only in the following 8000 Series models:

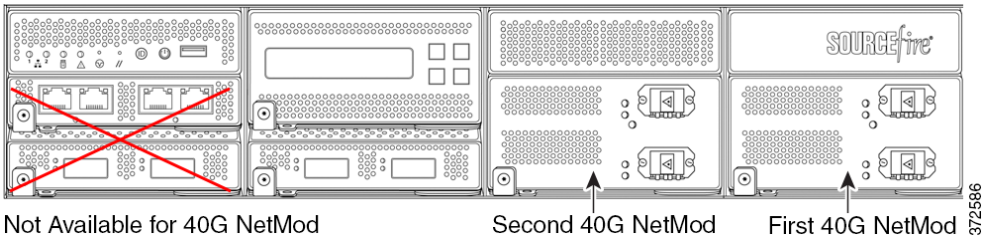
- Firepower 8270 and 8290
- Firepower and AMP 8360, 8370 and 8390
- Firepower 8250 and 8260 (must be 40G-capable)
- Firepower and AMP 8350 (must be 40G-capable)

Caution If you attempt to create a 40G interface on a device that is not 40G-capable, the 40G interface screen on its managing Firepower Management Center web interface displays red. A 40G-capable 8250 displays "8250-40G" on the LCD Panel and a 40G-capable 8350 displays "8350-40G" on the LCD Panel.

You can use this configuration to passively monitor up to two separate network segments. You also can use the paired interface in inline or inline with bypass mode, which allows you to deploy the device as an intrusion prevention system on one network.

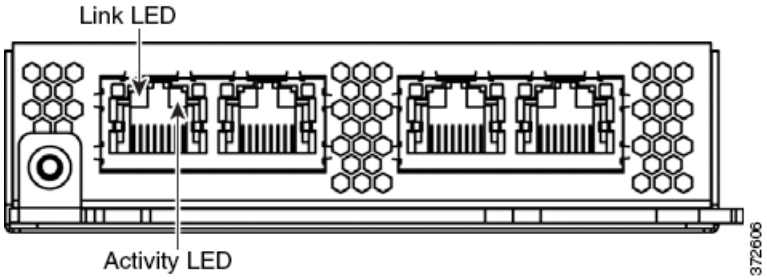
You can use up to two 40G NetMods. Install the first 40G NetMod in slots 3 and 7, and the second in slots 2 and 6. You cannot use a 40G NetMod in slots 1 and 4.

Figure 4-16 40G NetMod Placement



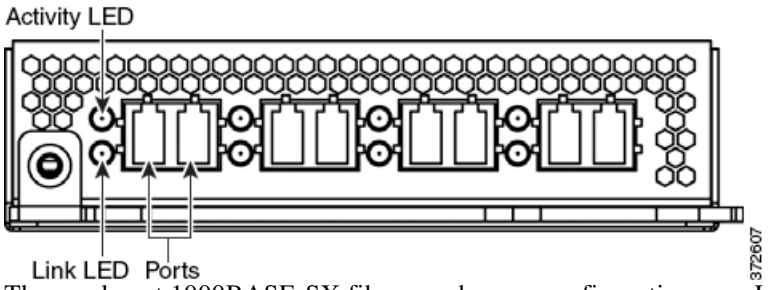
If you want to take advantage of a device's automatic bypass capability, you must use the web interface to configure a pair of interfaces as an inline set and enable bypass mode on the inline set.

Figure 4-17 Quad-Port 1000BASE-T Copper Non-Bypass NetMod



You can use these connections to passively monitor up to four separate network segments. You also can use paired interfaces in inline configuration on up to two network segments.

Figure 4-18 Quad-Port 1000BASE-SX Fiber Non-Bypass NetMod

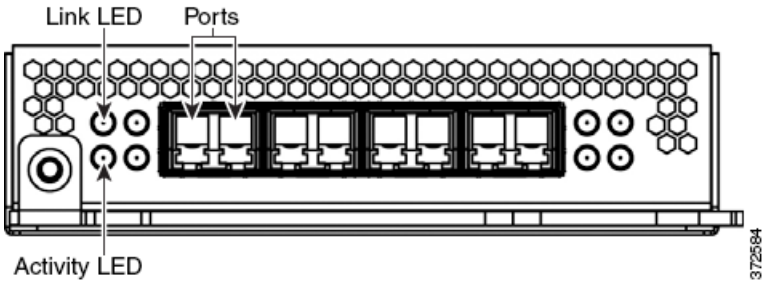


The quad-port 1000BASE-SX fiber non-bypass configuration uses LC-type (Local Connector) optical transceivers.

You can use these connections to passively monitor up to four separate network segments. You also can use paired interfaces in inline configuration on up to two network segments.

Tip For best performance, use the interface sets consecutively. If you skip interfaces, you may experience degraded performance.

Figure 4-19 Quad-Port 10GBASE (MMSR or SMLR) Fiber Non-Bypass NetMod



The quad-port 10GBASE fiber non-bypass configuration uses LC-type (Local Connector) optical transceivers with either MMSR or SMLR interfaces.

Caution The quad-port 10G BASE non-bypass NetMod contains non-removable small form-factor pluggable (SFP) transceivers. Any attempt to remove the SFPs can damage the module.

You can use these connections to passively monitor up to four separate network segments. You also can use paired interfaces in inline configuration on up to two network segments.

Tip For best performance, use the interface sets consecutively. If you skip interfaces, you may experience degraded performance.

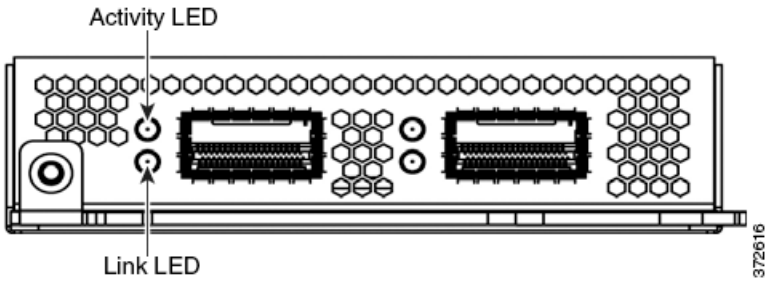
Firepower 8000 Series Stacking Module

A stacking module combines the resources of two or more identically configured appliances. The stacking module is optional on the following 8000 Series models:

- Firepower 8140 and 8250
- Firepower and AMP 8350

The stacking module is included in the following 8000 Series stacked configurations:

- Firepower 8260, 8270, and 8290
- Firepower and AMP 8360, 8370, and 8390



The stacking module allows you to combine the resources of two devices, using one as the primary device and one as the secondary. Only the primary device has sensing interfaces. The following devices can use the stacking module:

- The Firepower 8140, 8250, and 8350 can be delivered with the stacking module.
- The Firepower 8260 stacked configuration is delivered with one stacking module in the primary device and one stacking module in the secondary device.
- The Firepower and AMP 8360 stacked configurations are delivered with one stacking module in the primary device and one stacking module in the secondary device.
- The Firepower 8270 stacked configuration is delivered with two stacking modules in the primary device and one stacking module in each of the two secondary devices.
- The Firepower and AMP 8370 stacked configurations are delivered with two stacking modules in the primary device and one stacking module in each of the two secondary devices.
- The Firepower 8290 stacked configuration is delivered with three stacking modules in the primary device, and one stacking module in each of the three secondary devices.
- The Firepower and AMP 8390 stacked configurations are delivered with three stacking modules in the primary device, and one stacking module in each of the three secondary devices.

For more information on using stacked devices, see Using Devices in a Stacked Configuration.

Using Devices in a Stacked Configuration

You can increase the amount of traffic inspected on network segments by combining the resources of identically configured devices in a stacked configuration. One device is designated as the primary device and is connected to the network segments. All other devices are designated secondary devices, and are used to provide additional resources to the primary device. A Firepower Management Center creates, edits, and manages the stacked configuration.

The primary device contains sensing interfaces and one set of stacking interfaces for each secondary device connected to it. You connect the sensing interfaces on the primary device to the network segments you want to monitor in the same way as a non-stacked device. You connect the stacking interfaces on the primary device to the stacking interfaces on the secondary devices using the stacking cables. Each secondary device is connected directly to the primary device using the stacking interfaces. If a secondary device contains sensing interfaces, they are not used.

You can stack devices in the following configurations:

- two Firepower 8140s

- up to four Firepower 8250s
- a Firepower 8260 (a 10G-capable primary device and a secondary device)
- a Firepower 8270 (a 40G-capable primary device and two secondary devices)
- a Firepower 8290 (a 40G-capable primary device and three secondary devices)
- up to four Firepower or AMP 8350s
- a Firepower or AMP 8360 (a 40G-capable primary device and a secondary device)
- a Firepower or AMP 8370 (a 40G-capable primary device and two secondary devices)
- a Firepower or AMP 8390 (a 40G-capable primary device and three secondary devices)

For the Firepower 8260 and 8270 devices and Firepower or AMP 8360 and 8370 devices, you can stack additional devices for a total of four devices in the stack.

One device is designated as the primary device and is displayed on the Firepower Management Center's web interface with the primary role. All other devices in the stacked configuration are secondary and displayed in the web interface with the secondary role. You use the combined resources as a single entity except when viewing information from the stacked devices.

Connect the primary device to the network segments you want to analyze in the same way that you would connect a single Firepower 8140, Firepower 8250, and Firepower or AMP 8350. Connect the secondary devices to the primary device as indicated in the stack cabling diagram.

Caution You **must** have management interfaces configured and working for all device stack members. Register all devices as single devices, stack them, and never remove or disable the management interfaces for stacked secondary devices. This allows each stack member to report health and exchange configuration information.

After the devices are physically connected to the network segments and to each other, use a Firepower Management Center to establish and manage the stack.

The following sections provide more information on how to connect and manage stacked devices:

- Connecting the Firepower 8140, page 4-14
- Connecting the Firepower 82xx Family and Firepower and AMP 83xx Family, page 4-15
- Using the 8000 Series Stacking Cable, page 4-18
- Managing Stacked Devices, page 4-19

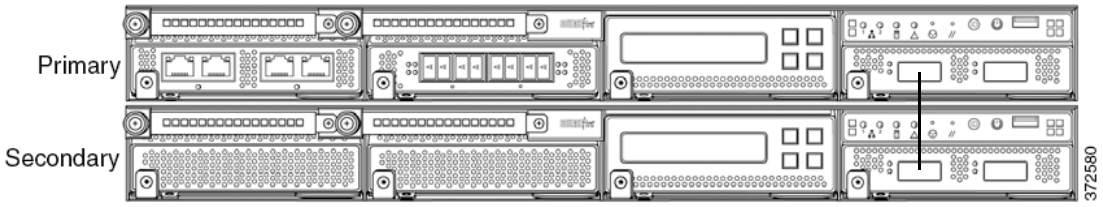
Connecting the Firepower 8140

You can connect two Firepower 8140s in a stacked configuration. You must use one 8000 Series stacking cable to create the physical connection between the primary device and the secondary device. For more information on using the stacking cable, see Using the 8000 Series Stacking Cable, page 4-18.

Install the devices in your rack so you can easily connect the cable between the stacking modules. You can install the secondary device above or below the primary device.

Connect the primary device to the network segments you want to analyze in the same way that you would connect a single Firepower 8140. Connect the secondary device directly to the primary device.

The following graphic shows a primary device with a secondary device installed below the primary device.



To connect a Firepower 8140 secondary device:

Step 1 Use an 8000 Series stacking cable to connect the left stacking interface on the primary device to the left stacking interface on the secondary device, then use the Firepower Management Center that manages the devices to establish the stacked device relationship in the system. Note that the right stacking interface is not connected. See Managing Stacked Devices, page 4-19.

Caution You **must** have management interfaces configured and working for all device stack members. Register all devices as single devices, stack them, and never remove or disable the management interfaces for stacked secondary devices. This allows each stack member to report health and exchange configuration information.

Connecting the Firepower 82xx Family and Firepower and AMP 83xx Family

You can connect any of the following configurations:

- up to four 8250s
- up to four Firepower 8350s or four AMP8350s
- a Firepower 8260 (a 10G-capable primary device and a secondary device)
- a Firepower or AMP 8360 (a 40G-capable primary device and a secondary device)
- a Firepower 8270 (a 40G-capable primary device and two secondary devices)
- a Firepower or AMP 8370 (a 40G-capable primary device and two secondary devices)
- a Firepower 8290 (a 40G-capable primary device and three secondary devices)
- a Firepower or AMP 8390 (a 40G-capable primary device and three secondary devices)

You can stack additional devices for a total of four devices in the stack for the following configurations:

- Firepower 8260 and 8270
- Firepower or AMP 8360
- Firepower or AMP 8370

You must use two 8000 Series stacking cables for each secondary device you want to connect to the primary device. For more information on using the stacking cable, see Using the 8000 Series Stacking Cable, page 4-18.

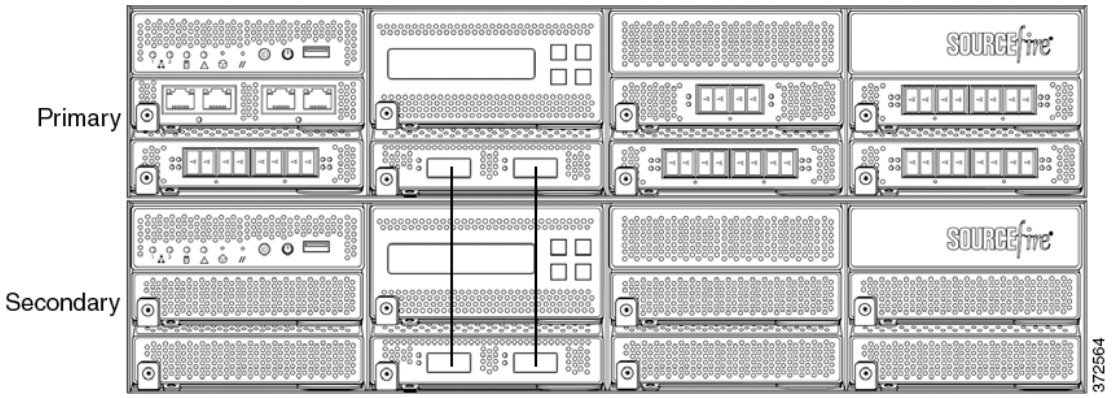
Install the devices in your rack so you can easily connect the cables between the stacking modules. You can install the secondary devices above or below the primary device.

Connect the primary device to the network segments you want to analyze in the same way that you would connect a single Firepower 8250 or 8350 (Firepower or AMP). Connect each secondary device directly to the primary device as required for the number of secondary devices in the configuration.

Caution You **must** have management interfaces configured and working for all device stack members. Register all devices as single devices, stack them, and never remove or disable the management interfaces for stacked secondary devices. This allows each stack member to report health and exchange configuration information.

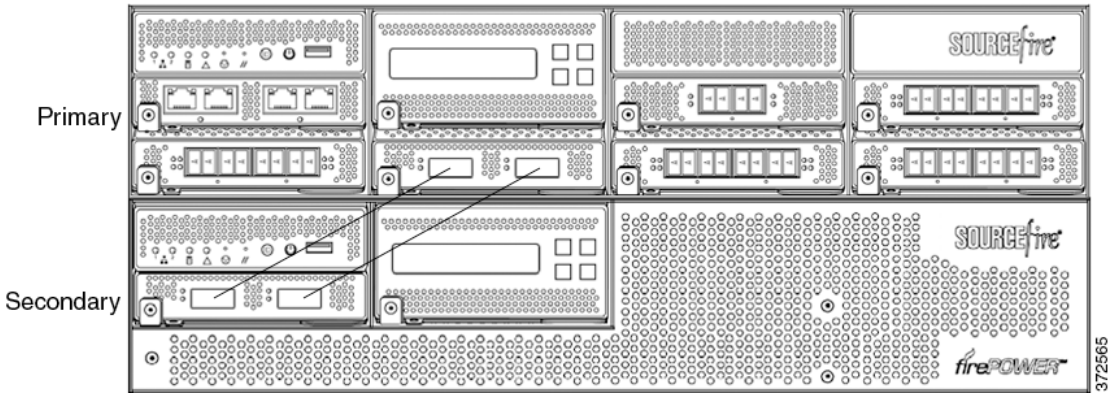
8250 or 8350 Primary Device with One Secondary Device

The following example shows a Firepower 8250 or 8350 (Firepower or AMP) primary device and one secondary device. The secondary device is installed below the primary device. Note that the secondary device contains no sensing interfaces.



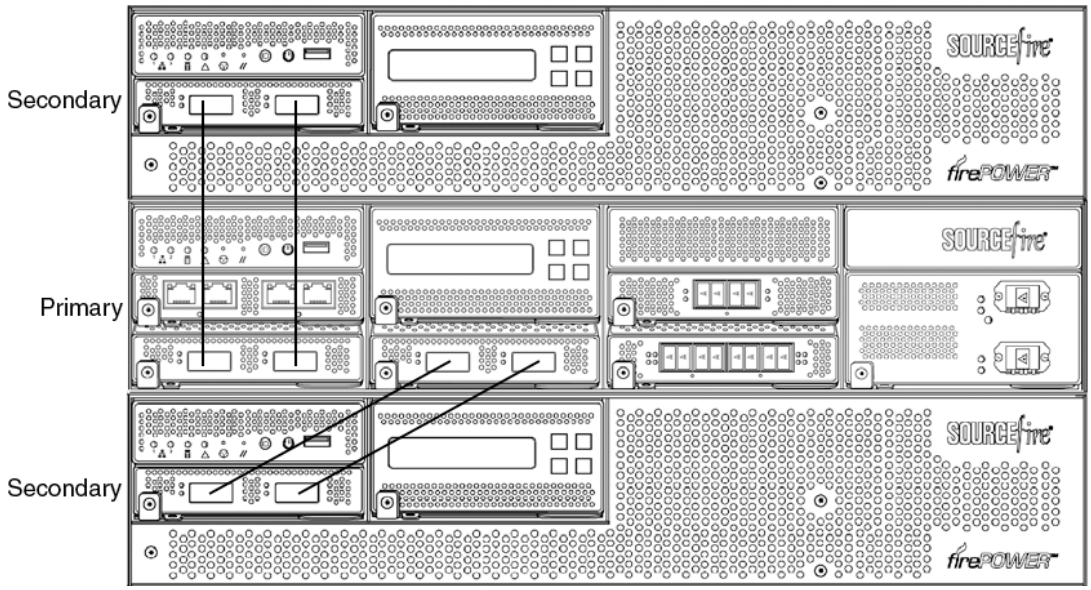
8260 or 8360 Primary Device and One Secondary Device

The following example shows a Firepower 8260 or a 8360 (Firepower or AMP) configuration. The Firepower 8260 includes a 10G-capable 8250 primary device and one dedicated secondary device. The Firepower or AMP 8360 includes a 40G-capable 8350 primary device and one dedicated secondary device. For each configuration (8260 or 8360), the secondary device is installed below the primary device.



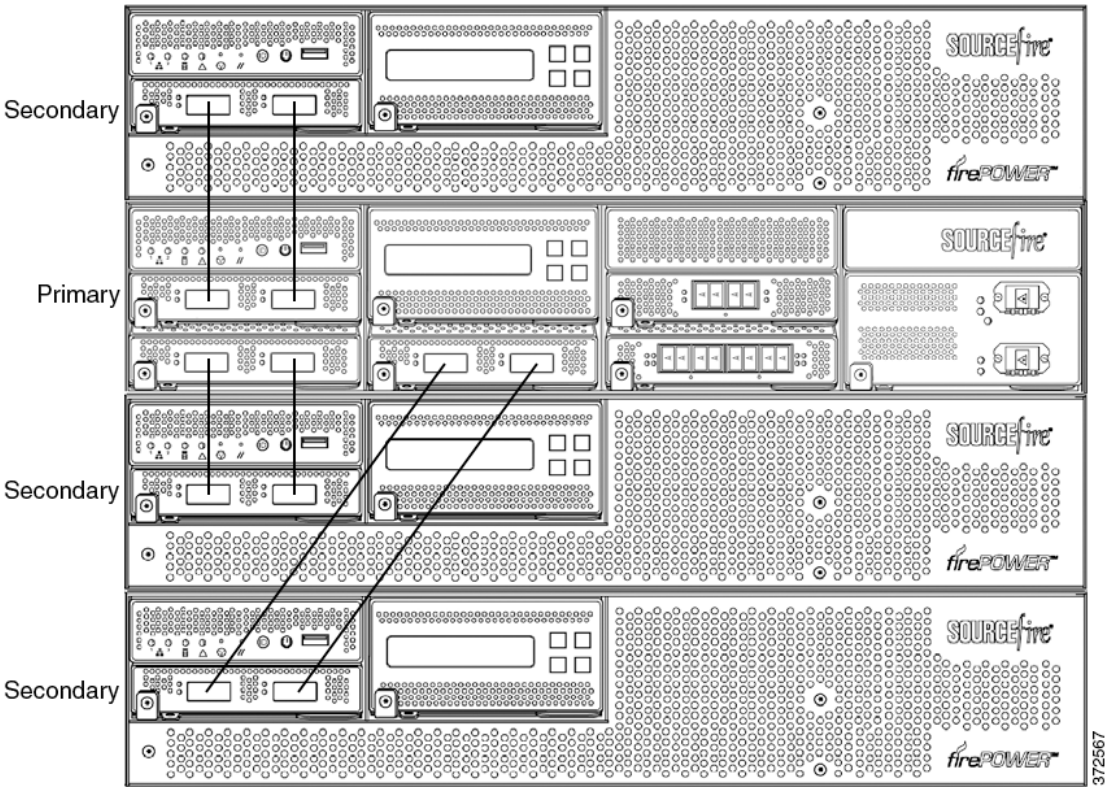
8270 or 8370 Primary Device (40G) and Two Secondary Devices

The following example shows a Firepower 8270 or a 8370 (Firepower or AMP) configuration. The Firepower 8270 includes a 40G-capable 8250 primary device and two dedicated secondary devices. The Firepower or AMP 8370 includes a 40G-capable 8350 primary device and two dedicated secondary devices. For each configuration (8270 or 8370), one secondary device is installed above the primary device and the other is installed below the primary device.



8290 or 8390 Primary Device (40G) and Three Secondary Devices

The following example shows a Firepower 8290 or a 8390 (Firepower or AMP) configuration. The Firepower 8290 includes a 40G-capable 8250 primary device and three dedicated secondary devices. The Firepower or AMP 8370 includes a 40G-capable 8350 primary device and two dedicated secondary devices. For each configuration (8290 or 8390), one secondary device is installed above the primary device and two secondary devices are installed below the primary device.



To connect a 8250 or a 8350 secondary device:

Step 1 Use an 8000 Series stacking cable to connect the left interface on the stacking module on the primary device to the left interface on the stacking module on the secondary device.

Step 2 Use a second 8000 Series stacking cable to connect the right interface on the stacking module on the primary device to the right interface on the stacking module on the secondary device.

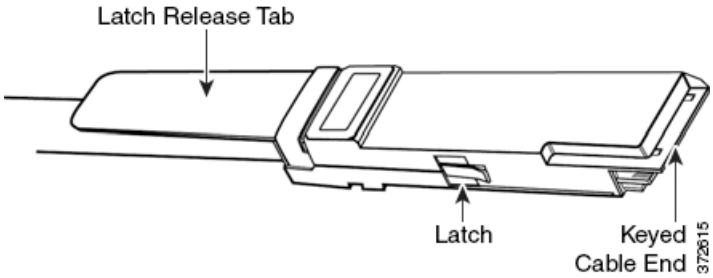
Step 3 Repeat steps 1 and 2 for each secondary device you want to connect.

Step 4 Use the Firepower Management Center that manages the devices to establish the stacked device relationship and manage their joint resources. See Managing Stacked Devices, page 4-19.

Caution You **must** have management interfaces configured and working for all device stack members. Register all devices as single devices, stack them, and never remove or disable the management interfaces for stacked secondary devices. This allows each stack member to report health and exchange configuration information.

Using the 8000 Series Stacking Cable

The 8000 Series stacking cable has identically-keyed ends, each with a latch to secure the cable in the device and a latch release tab.



Use 8000 Series stacking cables to create the physical connection between the primary device and each secondary device as required for each device configuration:

- the Firepower 8250, 8260, 8270, and 8290 require two cables per connection
- the Firepower or AMP 8350, 8360, 8370, and 8390 require two cables per connection
- the Firepower 8140 requires one cable

Devices do not need to be powered down to insert or remove the stacking cable.

Caution Use only the Cisco 8000 Series stacking cable when cabling your devices. Using unsupported cables can create unforeseen errors.

Use the Firepower Management Center to manage the stacked devices after you have physically connected the devices.

To insert an 8000 Series stacking cable:

Step 1 To insert the cable, hold the cable end with release tab facing up, then insert the keyed end into the port on the stacking module until you hear the latch click into place.

To remove an 8000 Series stacking cable:

Step 1 To remove the cable, pull on the release tab to release the latch, then remove the cable end.

Managing Stacked Devices

A Firepower Management Center establishes the stacked relationship between the devices, controls the interface sets of the primary device, and manages the combined resources in the stack. You cannot manage interface sets on the local web interface of a stacked device.

After the stacked relationship is established, each device inspects traffic separately using a single, shared detection configuration. If the primary device fails, traffic is handled according to the configuration of the primary device (that is, as if the stacked relationship did not exist). If the secondary device fails, the primary device continues to sense traffic, generate alerts, and send traffic to the failed secondary device where the traffic is dropped.

For information on establishing and managing stacked devices, see Managing Stacked Devices in the *Firepower Management Center Configuration Guide*.

Rack-Mounting a Firepower Device

You can rack-mount all Firepower devices (with purchase of a 1U mounting kit for Firepower 7010, 7020, 7030, and 7050). When you install an appliance, you must also make sure that you can access its console. To access the console for initial setup, connect to the appliance in one of the following ways:

Keyboard and Monitor/KVM

You can connect a USB keyboard and VGA monitor to a Firepower device, which is useful for rack-mounted appliances connected to a keyboard, video, and mouse (KVM) switch.

Caution Do **not** use a KVM console with USB mass storage to access the appliance for the initial setup because the appliance may attempt to use the mass storage device as a boot device.

Ethernet Connection to Management Interface

Configure a local computer, which must not be connected to the Internet, with the following network settings:

- IP address: `192.168.45.2`
- netmask: `255.255.255.0`
- default gateway: `192.168.45.1`

Using an Ethernet cable, connect the network interface on the local computer to the management interface on the appliance. To interact with the appliance, use terminal emulation software such as HyperTerminal or XModem. The settings for this software are as follows:

- 9600 baud
- 8 data bits
- no parity checking
- 1 stop bit
- no flow control.

Note that the management interface is preconfigured with a default IPv4 address. However, you can reconfigure the management interface with an IPv6 address as part of the setup process.

After initial setup, you can access the console in the following additional ways:

Serial Connection/Laptop

You can connect a computer to a Firepower device using the appliance's serial port. Connect the appropriate rollover serial cable (also known as a NULL modem cable or Cisco console cable) at any time, then configure the remote management console to redirect the default VGA output to the serial port. To interact with the appliance, use terminal emulation software as described above.

A serial port may have an RJ-45 connection or a DB-9 connection, depending on the appliance. See the following table for connectors by appliance.

Table 4-1 Serial Connectors by Model

Firepower Appliance	Connectors
70xx Family	RJ-45

Table 4-1 Serial Connectors by Model

Firepower Appliance	Connectors
71xx Family	DB-9 (female)
8000 Series	RJ-45

After you connect the appropriate rollover cable to your device, redirect the console output as described in Redirecting Console Output, page 4-22. To locate the serial port for each appliance, use the diagrams in Hardware Specifications, page 7-1.

Lights-Out Management Using Serial over LAN

The LOM feature allows you to perform a limited set of actions on a Firepower Management Center or Firepower device using a SOL connection. If you need to restore a LOM-capable appliance to factory defaults and do not have physical access to the appliance, you can use LOM to perform the restore process. After you connect to an appliance using LOM, you issue commands to the restore utility as if you were using a physical serial connection. For more information, see Setting Up Lights-Out Management, page 8-15.

Note You can use Lights-Out Management on the default (`eth0`) management interface only.

To use LOM to restore the appliance to factory settings, do **not** delete network settings. Deleting the network settings also drops the LOM connection. For more information, see Restoring a Firepower System Appliance to Factory Defaults, page 8-1.

To install the appliance:

Step 1 Mount the appliance in your rack using the mounting kit and its supplied instructions.

Step 2 Connect to the appliance using either a keyboard and monitor or Ethernet connection.

Step 3 If you are using a keyboard and monitor to set up the appliance, use an Ethernet cable now to connect the management interface to a protected network segment.

If you plan to perform the initial setup process by connecting a computer directly to the appliance's management interface, you will connect the management interface to the protected network when you finish setup.

Step 4 For a Firepower device, connect the sensing interfaces to the network segments you want to analyze using the appropriate cables for your interfaces:

- Copper Sensing Interfaces: If your device includes copper sensing interfaces, make sure you use the appropriate cables to connect them to your network; see Cabling Inline Deployments on Copper Interfaces, page 3-5.
- Fiber Adapter Card: For devices with a fiber adapter card, connect the LC connectors on the optional multimode fiber cable to two ports on the adapter card in any order. Connect the SC plug to the network segment you want to analyze.
- Fiber Tap: If you are deploying the device with an optional fiber optic tap, connect the SC plug on the optional multimode fiber cable to the "analyzer" port on the tap. Connect the tap to the network segment you want to analyze.

- Copper Tap: If you are deploying the device with an optional copper tap, connect the A and B ports on the left of the tap to the network segment you want to analyze. Connect the A and B ports on the right of the tap (the "analyzer" ports) to two copper ports on the adapter card.

For more information about options for deploying the managed device, see Deploying Firepower Managed Devices, page 3-1.

Note that if you are deploying a device with bypass interfaces, you are taking advantage of your device's ability to maintain network connectivity even if the device fails. See Testing an Inline Bypass Interface Installation, page 4-24 for information on installation and latency testing.

Step 5 Attach the power cord to the appliance and plug into a power source.

If your appliance has redundant power supplies, attach power cords to both power supplies and plug them into separate power sources.

Step 6 Turn on the appliance.

If you are using a direct Ethernet connection to set up the appliance, confirm that the link LED is on for both the network interface on the local computer and the management interface on the appliance. If the management interface and network interface LEDs are not lit, try using a crossover cable. For more information, see Cabling Inline Deployments on Copper Interfaces, page 3-5.

What To Do Next

- Continue with the next chapter, Setting Up Firepower Managed Devices, page 5-1.

Redirecting Console Output

By default, Firepower devices direct initialization status, or *init*, messages to the VGA port. If you restore an appliance to factory defaults and delete its license and network settings, the restore utility also resets the console output to VGA. If you want to use the physical serial port or SOL to access the console, Cisco recommends you redirect console output to the serial port after you complete the initial setup.

To redirect console output using the shell, you run a script from the appliance's shell. Note that while all Firepower devices support LOM, 7000 Series devices do not support LOM and physical serial access at same time. However, the console setting is the same regardless of which access method you want to use.

Using the Shell

You can use the shell to redirect the console output.

To redirect the console output using the shell:

Access: Admin

Step 1 Using your keyboard/monitor or serial connection, log into the appliance's shell using an account with Administrator privileges. The password is the same as the password for the appliance's web interface.

On a Firepower device, you must type `expert` to display the shell prompt.

The prompt for the appliance appears.

Step 2 At the prompt, set the console output by typing one of the following commands:

- To access the appliance using the VGA port:

```
sudo /usr/local/sf/bin/configure_console.sh vga
```

- To access the appliance using the physical serial port:

```
sudo /usr/local/sf/bin/configure_console.sh serial
```

- To access the appliance using LOM via SOL:

```
sudo /usr/local/sf/bin/configure_console.sh sol
```

Step 3 To implement your changes, reboot the appliance by typing `sudo reboot`.

The appliance reboots.

Using the Web Interface

You can also redirect console output through the web interface.

To redirect the console output using the web interface:

Access: Admin

Step 1 Select **System > Configuration.**

Step 2 Select **Console Configuration.**

Step 3 Select a remote console access option:

- Select **VGA** to use the appliance's VGA port. This is the default option.
- Select **Physical Serial Port** to use the appliance's serial port, or to use LOM/SOL on a Firepower 7050 or 8000 Series device.

  The LOM settings appear.
- Select **Lights-Out Management** to use LOM/SOL on a 7000 Series device (except the Firepower 7050).

  On these devices, you cannot use SOL and a regular serial connection at the same time. LOM settings appear.

Step 4 To configure LOM via SOL, enter the appropriate settings:

- **DHCP Configuration** for the appliance (**DHCP** or **Static**).
- **IP Address** to be used for LOM. The LOM IP address must be different from the management interface IP address of the appliance.
- **Netmask** for the appliance.
- **Default Gateway** for the appliance.

Step 5 Click **Save**.

Remote console configuration for the appliance is saved. If you configured Lights-Out Management, you must enable it for at least one user; see Enabling LOM and LOM Users, page 8-16.

Testing an Inline Bypass Interface Installation

Managed devices with bypass interfaces provide the ability to maintain network connectivity even when the device is powered off or inoperative. It is important to ensure that you properly install these devices and quantify any latency introduced by their installation.

Note Your switch's spanning tree discovery protocol can cause a 30-second traffic delay. Cisco recommends that you disable the spanning tree during the following procedure.

The following procedure, applicable only to copper interfaces, describes how to test the installation and ping latency of an inline bypass interface. You will need to connect to the network to run ping tests and connect to the managed device console.

Before You Begin

- Ensure that the interface set type for the Firepower device is configured for inline bypass mode. See Configuring Inline Sets in the *Firepower Management Center Configuration Guide* for instructions on configuring an interface set for inline bypass mode.

To test a device with inline bypass interface installation:

Access: Admin

Step 1 Set all interfaces on the switch, the firewall, and the device sensing interfaces to auto-negotiate.

Note Firepower System devices require auto-negotiate when using auto-MDIX on the device.

Step 2 Power off the device and disconnect all network cables.

Reconnect the device and ensure you have the proper network connections. Check cabling instructions for crossover versus straight-through from the device to the switches and firewalls, see Cabling Inline Deployments on Copper Interfaces, page 3-5.

Step 3 With the device powered off, ensure that you can ping from the firewall through the device to the switch.

If the ping fails, correct the network cabling.

Step 4 Run a continuous ping until you complete step 9.

Step 5 Power the device back on.

Step 6 Using your keyboard/monitor or serial connection, log into the device using an account with Administrator privileges. The password is the same as the password for the device's web interface.

The prompt for the device appears.

Step 7 Shut down the device by typing `system shutdown`.

You can also shut down the device using its web interface; see the Managing Devices chapter in the *Firepower Management Center Configuration Guide.* As most devices power off, they emit an audible click sound. The click is the sound of relays switching and the device going into hardware bypass.

Step 8 Wait 30 seconds.

Verify that your ping traffic resumes.

Step 9 Power the device back on, and verify that your ping traffic continues to pass.

Step 10 For Firepower devices that support tap mode, you can test and record ping latency results under the following sets of conditions:

- device powered off
- device powered on, policy with no rules applied, inline intrusion policy protection mode
- device powered on, policy with no rules applied, inline intrusion policy protection tap mode
- device powered on, policy with tuned rules applied, inline intrusion policy protection mode

Ensure that the latency periods are acceptable for your installation. For information on resolving excessive latency problems, see Configuring Packet Latency Thresholding and Understanding Rule Latency Thresholding in the *Firepower Management Center Configuration Guide*.

Setting Up Firepower Managed Devices

After you deploy and install a Firepower device, you must complete a setup process that allows the new appliance to communicate on your trusted management network. You must also change the administrator password and accept the end user license agreement (EULA).

The setup process also allows you to perform many initial administrative-level tasks, such as setting the time, registering and licensing devices, and scheduling updates. The options you choose during setup and registration determine the default interfaces, inline sets, zones, and policies that the system creates and applies.

The purpose of these initial configurations and policies is to provide an out-of-the-box experience and to help you quickly set up your deployment, not to restrict your options. Regardless of how you initially configure a device, you can change its configuration at any time using the Firepower Management Center. In other words, choosing a detection mode or access control policy during setup, for example, does not lock you into a specific device, zone, or policy configuration.

For more information on each of the steps in the initial setup process, see the following sections:

- Understanding the Setup Process, page 5-2 outlines the setup process.

Note If you are not already familiar with the setup process, Cisco **strongly** recommends you read this section first.

- Performing Initial Setup on a Firepower Device Using the CLI, page 5-3 explains how to use an interactive command line interface (CLI) to perform the setup process on a Firepower device.
- Initial Setup Page: Firepower Devices, page 5-5 explains how to use any device's web interface to complete its initial setup.
- Next Steps, page 5-9 contains guidance on the post-setup tasks you may want to perform as you set up your Firepower System deployment.

Caution The procedures in this chapter explain how to set up an appliance without powering it down. However, if you need to power down for any reason, use the procedure in the Device Management Basics chapter in the *Firepower Management Center Configuration Guide*, the `system shutdown` command from the CLI on a Firepower device, or the `shutdown -h now` command from an appliance's shell (sometimes called expert mode).

Understanding the Setup Process

After you deploy and install a new Firepower device as described in earlier chapters of this guide, you must complete a setup process. Before you begin the setup, make sure that you can meet the following conditions.

Model

You must know which appliance you are setting up. For more information, see Firepower System Appliances, page 1-2.

Access

To set up a new appliance, you must connect using either keyboard and monitor/KVM (keyboard, video, and mouse) or a direct Ethernet connection to the appliance's management interface. After initial setup, you can configure the appliance for serial access. For more information, see Rack-Mounting a Firepower Device, page 4-20.

Note Do **not** use a KVM console with USB mass storage to access the appliance for the initial setup because the appliance may attempt to use the mass storage device as a boot device.

Information

You have, at minimum, the information needed to allow the appliance to communicate on your management network: an IPv4 or IPv6 management IP address, a netmask or prefix length, and a default gateway.

If you know how the appliance is deployed, the setup process is also a good time to perform many initial administrative-level tasks, including registration and licensing.

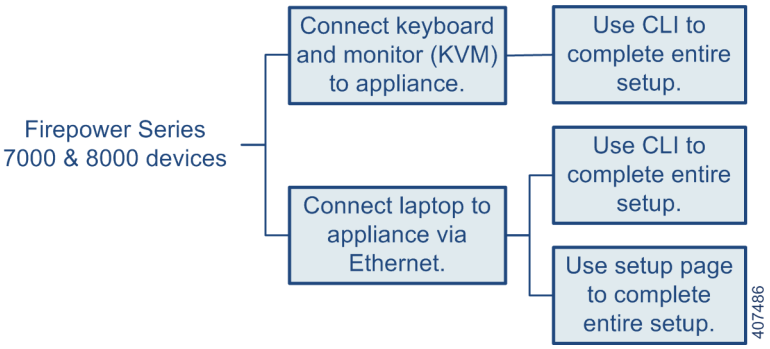
Tip If you are deploying multiple appliances, set up your devices first, then their managing Firepower Management Center. The initial setup process for a device allows you to preregister it to a Firepower Management Center; the setup process for a Firepower Management Center allows you to add and license preregistered managed devices.

After you complete setup, you will use the Firepower Management Center's web interface to perform most management and analysis tasks for your deployment. Firepower devices have a restricted web interface that you can use only to perform basic administration. For more information, see Next Steps, page 5-9.

Tip If you are setting up an appliance after restoring it to factory defaults (see Restoring a Firepower System Appliance to Factory Defaults, page 8-1) and you did not delete the appliance's license and network settings, you can use a computer on your management network to browse directly to the appliance's web interface to perform the setup. Skip to Initial Setup Page: Firepower Devices, page 5-5.

Beginning the Setup

The following diagram illustrates the choices you can make when setting up Firepower devices:



Your access to a Firepower device determines how you set it up. You have the following options:

- Regardless of how you are connected to the device, you can use the CLI to set it up; see Performing Initial Setup on a Firepower Device Using the CLI, page 5-3.
- If you are accessing the appliance via a direct Ethernet connection, you can browse to the appliance's web interface from a local computer; see Initial Setup Page: Firepower Devices, page 5-5.

If you are setting up a reimaged device and you kept your network settings as part of the restore process, you can access the CLI via SSH or a Lights-Out Management (LOM) connection. You can also browse to the device's web interface from a computer on your management network.

Performing Initial Setup on a Firepower Device Using the CLI

Access: Admin

Optionally, you can use the CLI to configure Firepower devices instead of using the device's web interface. When you first log in to a newly configured device using the CLI, you must read and accept the EULA. Then, follow the setup prompts to change the administrator password, configure the device's network settings and detection mode. Finally, register the device to the Firepower Management Center that will manage it.

When following the setup prompts, options are listed in parentheses, such as `(y/n)`. Defaults are listed in square brackets, such as `[y]`. Press Enter to confirm a choice.

Note that the CLI prompts you for much of the same setup information that a device's setup web page does. For detailed information on these options, see Initial Setup Page: Firepower Devices, page 5-5.

To complete the initial setup on a Firepower device using the CLI:

Step 1 Log into the device. Use `admin` as the username and `Admin123` as the password.

- For a device attached to a monitor and keyboard, log in at the console.
- If you connected a computer to the management interface of the device using an Ethernet cable, SSH to the interface's default IPv4 address: 192.168.45.45.

  The device immediately prompts you to read the EULA.

Step 2 Read and accept the EULA.

Step 3 Change the password for the `admin` account. This account has Administrator privileges and cannot be deleted.

This password allows the `admin` user to log into the device's web interface and its CLI; the `admin` user has Configuration CLI access. Changing any user's password for the web interface also changes the password for the CLI, and vice versa.

Cisco recommends that you use strong password that is at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary. For more information, see Change Password, page 5-6.

Step 4 Configure network settings for the device.

First configure (or disable) IPv4 management settings, then IPv6. If you manually specify network settings, you must:

- enter IPv4 addresses, including the netmask, in dotted decimal form. For example, you could specify a netmask of 255.255.0.0.
- enter IPv6 addresses in colon-separated hexadecimal form. For an IPv6 prefix, specify the number of bits; for example, a prefix length of 112.

For more information, see Network Settings, page 5-6. The console may display messages as your settings are implemented.

Step 5 Select whether you want to allow changing of the device's network settings using the LCD panel.

Caution Enabling this option can present a security risk. You need only physical access, not authentication, to configure network settings using the LCD panel. For more information, see Using the LCD Panel on a Firepower Device, page 6-1.

Step 6 Specify the detection mode based on how you deployed the device.

For more information, see Detection Mode, page 5-8. The console may display messages as your settings are implemented. When finished, the device reminds you to register this device to a Firepower Management Center, and displays the CLI prompt.

Step 7 To use the CLI to register the device to the Firepower Management Center that will manage it, continue with the next section, Registering a Firepower Device to a Management Center Using the CLI.

You must manage devices with a Firepower Management Center. If you do not register the device now, you must log in later and register it before you can add it to a Firepower Management Center.

Step 8 Log out of the device.

Registering a Firepower Device to a Management Center Using the CLI

Access: Configuration CLI

If you configured a Firepower device using the CLI, Cisco recommends that you use the CLI to register the device to a Firepower Management Center at the conclusion of the setup script. It is easiest to register a device to its Firepower Management Center during the initial setup process, because you are already logged into the device's CLI.

To register a device, use the `configure manager add` command. A unique alphanumeric registration key is always required to register a device to a Firepower Management Center. This is a simple key that you specify, up to 37 characters in length, and is not the same as a license key.

In most cases, you must provide the Firepower Management Center's hostname or the IP address along with the registration key, for example:

```
configure manager add DC.example.com my_reg_key
```

However, if the device and the Firepower Management Center are separated by a NAT device, enter a unique NAT ID along with the registration key, and specify `DONTRESOLVE` instead of the hostname, for example:

```
configure manager add DONTRESOLVE my_reg_key my_nat_id
```

To register a device to a Firepower Management Center:

Step 1 Log in to the device as a user with Configuration CLI access level:

- If you are performing the initial setup from the console, you are already logged in as the `admin` user, which has the required access level.
- Otherwise, SSH to the device's management IP address or host name.

Step 2 At the prompt, register the device to a Firepower Management Center using the `configure manager add` command, which has the following syntax:

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} reg_key
[nat_id]
```

where:

- `{hostname | IPv4_address | IPv6_address | DONTRESOLVE}` specifies either the fully qualified host name or IP address of the Firepower Management Center. If the Firepower Management Center is not directly addressable, use `DONTRESOLVE`.
- *`reg_key`* is the unique alphanumeric registration key, up to 37 characters in length, required to register a device to the Firepower Management Center.
- *`nat_id`* is an optional alphanumeric string used during the registration process between the Firepower Management Center and the device. It is required if the hostname is set to `DONTRESOLVE`.

Step 3 Log out of the device.

The device is ready to be added to a Firepower Management Center.

Initial Setup Page: Firepower Devices

Access: Admin

In most cases, complete the setup process by logging into the device's web interface and specifying initial configuration options on a setup page. You can skip this step if you already used the CLI to perform initial setup; see Performing Initial Setup on a Firepower Device Using the CLI, page 5-3.

You must change the administrator password, specify network settings if you have not already, and accept the EULA. You can also preregister the device to a Firepower Management Center and specify a detection mode; the detection mode and other options you choose during registration determine the default interfaces, inline sets, and zones that the system creates, as well as the policies that it initially applies to managed devices.

To complete the initial setup on a Firepower device using its web interface:

Step 1 Direct your browser to `https://mgmt_ip/`, where *`mgmt_ip`* is the IP address of the device's management interface.

- For a device connected to a computer with an Ethernet cable, direct the browser on that computer to the default management interface IPv4 address: `https://192.168.45.45/`.
- For a device where network settings are already configured, use a computer on your management network to browse to the IP address of the device's management interface.

Step 2 Log in using `admin` as the username and `Admin123` as the password.

See the following sections for information on completing the setup:

- Change Password, page 5-6
- Network Settings, page 5-6
- Firepower Device LCD Panel Configuration, page 5-7
- Remote Management, page 5-7
- Time Settings, page 5-7
- Detection Mode, page 5-8
- Automatic Backups, page 5-9
- End User License Agreement, page 5-9

Step 3 When you are finished, click **Apply**.

The device is configured according to your selections. You are logged into the web interface as the `admin` user, which has the Administrator role.

Step 4 Log out of the device.

The device is ready to be added to its Firepower Management Center.

Note If you connected directly to the device using an Ethernet cable, disconnect the computer and connect the device's management interface to the management network. If you need to access the device's web interface at any time, direct a browser on a computer on the management network to the IP address or host name that you configured during setup.

Change Password

You must change the password for the `admin` account. This account has Administrator privileges and cannot be deleted.

This password allows the `admin` user to log into the device's web interface and its CLI; the `admin` user has Configuration CLI access. Changing any user's password for the web interface also changes the password for the CLI, and vice versa.

Cisco recommends that you use a strong password that is at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary.

Network Settings

A device's network settings allow it to communicate on your management network. If you already configured the device's network settings, this section of the page may be prepopulated.

The Firepower System provides a dual stack implementation for both IPv4 and IPv6 management environments. You must specify the management network protocol (**IPv4**, **IPv6**, or **Both**). Depending on your choice, the setup page displays various fields where you must set the IPv4 or IPv6 management IP address, netmask or prefix length, and default gateway:

- For IPv4, you must set the address and netmask in dotted decimal form (for example: a netmask of 255.255.0.0).
- For IPv6 networks, you can select the **Assign the IPv6 address using router autoconfiguration** check box to automatically assign IPv6 network settings. Otherwise, you must set the address in colon-separated hexadecimal form and the number of bits in the prefix (for example: a prefix length of 112).

You can also specify up to three DNS servers, as well as the host name and domain for the device.

Firepower Device LCD Panel Configuration

Select whether you want to allow changing of a Firepower device's network settings using the LCD panel.

Caution Enabling this option can represent a security risk. You need only physical access, not authentication, to configure network settings using the LCD panel. For more information, see Using the LCD Panel on a Firepower Device, page 6-1.

Remote Management

You must manage a Cisco device with a Firepower Management Center. In this two-step process, you first configure remote management on the device, then add the device to a Firepower Management Center. For your convenience, the setup page allows you to preregister the device to the Firepower Management Center that will manage it.

Leave the **Register This Device Now** check box enabled, then specify the IP address or fully qualified domain name of the managing Firepower Management Center as the **Management Host**. Also, type the alphanumeric **Registration Key** you will later use to register the device to the Firepower Management Center. Note that this is a simple key that you specify, up to 37 characters in length, and is not the same as the license key.

Note If the device and Firepower Management Center are separated by a network address translation (NAT) device, defer device registration until after you complete the initial setup. See the Managing Devices chapter in the *Firepower Management Center Configuration Guide* for more information.

Time Settings

You can set the time for a device either manually or via network time protocol (NTP) from an NTP server, including the Firepower Management Center. Cisco recommends that you use the Firepower Management Center as the NTP server for its managed devices.

You can also specify the time zone used on the local web interface for the `admin` account. Click the current time zone to change it using a pop-up window.

Detection Mode

The detection mode you choose for a device determines how the system initially configures the device's interfaces, and whether those interfaces belong to an inline set or security zone.

The detection mode is not a setting you can change later; it is simply an option you choose during setup that helps the system tailor the device's initial configurations. In general, you should choose a detection mode based on how your device is deployed:

Passive

Choose this mode if your device is deployed passively, as an intrusion detection system (IDS). In a passive deployment, you can perform file and malware detection, Security Intelligence monitoring, as well as network discovery.

Inline

Choose this mode if your device is deployed inline, as an intrusion prevention system. An intrusion prevention system usually fails *open* and *allows* non-matching traffic.

In an inline deployment, you can also use AMP for Networks, file control, Security Intelligence filtering, and network discovery.

Although you can select the inline mode for any device, keep in mind that inline sets using the following interfaces lack bypass capability:

- non-bypass NetMods on 8000 Series devices
- SFP transceivers on 71xx Family devices

Note Reimaging resets devices in inline deployments to a non-bypass configuration; this disrupts traffic on your network until you reconfigure bypass mode. For more information, see Traffic Flow During the Restore Process, page 8-1.

Access Control

Choose this mode if your device is deployed inline as part of an access control deployment, that is, if you want to perform application, user, and URL control. A device configured to perform access control usually fails *closed* and *blocks* non-matching traffic. Rules explicitly specify the traffic to pass.

You should also choose this mode if you want to take advantage of your device's specific hardware-based capabilities, which include (depending on model): high availability, strict TCP enforcement, fast-path rules, switching, routing, DHCP, NAT, and VPN.

In an access control deployment, you can also perform AMP for Networks, file control, Security Intelligence filtering, and network discovery.

Network Discovery

Choose this mode if your device is deployed passively, to perform host, application, and user discovery only.

The following table lists the interfaces, inline sets, and zones that the system creates depending on the detection mode you choose.

Table 5-1 Initial Configurations Based on Detection Mode

Detection Mode	Security Zones	Inline Sets	Interfaces
Inline	Internal and External	Default Inline Set	first pair added to Default Inline Set—one to the Internal and one to the External zone
Passive	Passive	none	first pair assigned to Passive zone
Access Control	none	none	none
Network Discovery	Passive	none	first pair assigned to Passive zone

Note that security zones are a Firepower Management Center-level configuration which the system does not create until you actually register the device to the Firepower Management Center. Upon registration, if the appropriate zone (Internal, External, or Passive) already exists on the Firepower Management Center, the registration process adds the listed interfaces to the existing zone. If the zone does not exist, the system creates it and adds the interfaces. For detailed information on interfaces, inline sets, and security zones, see the *Firepower Management Center Configuration Guide*.

Automatic Backups

The device provides a mechanism for archiving data so that configuration and event data can be restored in case of failure. As part of the initial setup, you can **Enable Automatic Backups**.

Enabling this setting creates a scheduled task that creates a weekly backup of the configurations on the device.

End User License Agreement

Read the EULA carefully and, if you agree to abide by its provisions, select the check box. Make sure that all the information you provided is correct, and click **Apply**. The device is configured according to your selections and is ready to be added to its managing Firepower Management Center.

Next Steps

After you complete the initial setup process for an appliance and verify its success, Cisco recommends that you complete various administrative tasks that make your deployment easier to manage. You should also complete any tasks you skipped during the initial setup, such as device registration and licensing. For detailed information on any the tasks described in the following sections, as well as information on how you can begin to configure your deployment, see the *Firepower Management Center Configuration Guide*.

Tip If you want to use a serial or LOM/SOL connection to access your appliance's console, you should redirect console output; see Testing an Inline Bypass Interface Installation, page 4-24. If you want to use LOM specifically, you must enable the feature as well as enable at least one LOM user; see Enabling LOM and LOM Users, page 8-16.

Individual User Accounts

After you complete the initial setup, the only user on the system is the `admin` user, which has the Administrator role and access. Users with that role have full menu and configuration access to the system, including via the shell or CLI. Cisco recommends that you limit the use of the `admin` account (and the Administrator role) for security and auditing reasons.

Creating a separate account for each person who will use the system allows your organization not only to audit actions and changes made by each user, but also to limit each person's associated user access role or roles. This is especially important on the Firepower Management Center, where you perform most of your configuration and analysis tasks. For example, an analyst needs access to event data to analyze the security of your network, but may not require access to administrative functions for the deployment.

The system includes ten predefined user roles designed for a variety of administrators and analysts. You can also create custom user roles with specialized access privileges.

Health and System Policies

By default, all appliances have an initial system policy applied. The system policy governs settings that are likely to be similar for multiple appliances in a deployment, such as mail relay host preferences and time synchronization settings. Cisco recommends that you use the Firepower Management Center to apply the same system policy to itself and all the devices it manages.

By default, the Firepower Management Center also has a health policy applied. A health policy, as part of the health monitoring feature, provides the criteria for the system continuously monitoring the performance of the appliances in your deployment. Cisco recommends that you use the Firepower Management Center to apply a health policy to all the devices it manages.

Software and Database Updates

You should update the system software on your appliances before you begin any deployment. Cisco recommends that all the appliances in your deployment run the most recent version of the Firepower System. If you are using them in your deployment, you should also install the latest intrusion rule updates, VDB, and GeoDB.

Caution Before you update any part of the Firepower System, you **must** read the release notes or advisory text that accompanies the update. The release notes provide important information, including supported platforms, compatibility, prerequisites, warnings, and specific installation and uninstallation instructions.

Using the LCD Panel on a Firepower Device

Firepower devices allow you to view device information or configure certain settings using an LCD panel on the front of the device instead of the system's web interface.

The LCD panel has a display and four multi-function keys, and operates in multiple modes that show different information and allow different configurations depending on the state of the device.

For more information, see the following sections:

- Understanding LCD Panel Components, page 6-2 explains how to identify the components of the LCD panel and display the panel's main menu.
- Using the LCD Multi-Function Keys, page 6-3 explains how to use the multi-function keys on the LCD panel.
- Idle Display Mode, page 6-4 describes how the LCD panel displays various system information when the device is idle.
- Network Configuration Mode, page 6-4 explains how to use the LCD panel to configure the network configuration for the device's management interface: the IPv4 or IPv6 address, subnet mask or prefix, and default gateway.

Caution Allowing reconfiguration using the LCD panel may present a security risk. You need only physical access, not authentication, to configure using the LCD panel.

- System Status Mode, page 6-7 explains how you can view monitored system information, such as link state propagation, bypass status, and system resources, as well as change the LCD panel brightness and contrast.
- Information Mode, page 6-8 explains how you can view identifying system information such as the device's chassis serial number, IP address, model, and software and firmware versions.
- Error Alert Mode, page 6-9 describes how the LCD panel communicates error or fault conditions; for example, bypass, fan status, or hardware alerts.

Note The device must be powered on to use the LCD panel. For information on how to safely power on or shut down the device, see the Managing Devices chapter in the *Firepower Management Center Configuration Guide*.

Understanding LCD Panel Components

The LCD panel on the front of a Firepower device has a display and four multi-function keys:

- The display contains two lines of text (up to 17 characters each), as well as the multi-function key map. The map indicates, with symbols, the actions that you can perform with the corresponding multi-function keys.
- The multi-function keys allow you to view system information and complete basic configuration tasks, which vary according to the mode of the LCD panel. For more information, see Using the LCD Multi-Function Keys, page 6-3.

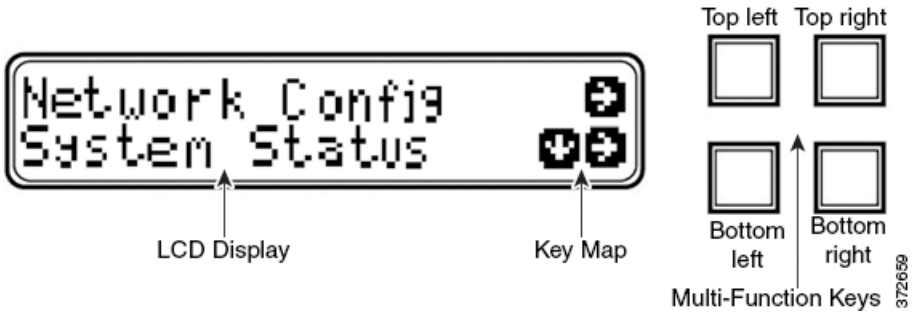
The following graphic shows the panel's default Idle Display mode, which does not include a key map.

Figure 6-1 LCD Panel, Idle Display mode

In Idle Display mode, the panel alternates between displaying the CPU utilization and free memory available, and the chassis serial number. Press any key to interrupt the Idle Display mode and enter the LCD panel's main menu where you can access Network Configuration, System Status, and Information modes.

The following graphic shows the main menu, which has a key map that corresponds to the four multi-function keys (top left, top right, bottom left, and bottom right).

Figure 6-2 LCD Panel, main menu



To access the main menu:

Step 1 In Idle Display mode, press any multi-function key.

The main menu appears:

- To change the device's network configuration, see Network Configuration Mode, page 6-4.
- To view monitored system information or adjust the LCD panel brightness and contrast, see System Status Mode, page 6-7.
- To view identifying system information, see Information Mode, page 6-8.

Note Pressing a multi-function key as the LCD panel enters Idle Display mode can cause the panel to display an unexpected menu.

Using the LCD Multi-Function Keys

Four multi-function keys allow you navigate the menus and options on the LCD panel. You can use the multi-function keys when a key map appears on the display. A symbol's location on the map corresponds to the function and location of the key used to perform that function. If no symbol is displayed, the corresponding key has no function.

Tip The function of a symbol, and therefore the key map, varies according the LCD panel mode. If you do not get the result you expect, check the mode of the LCD panel.

The following table explains the multi-function key functions.

Table 6-1 LCD Panel Multi-Function Keys

Symbol	Description	Function
↑	Up arrow	Scrolls up the list of current menu options.
↓	Down arrow	Scrolls down the list of current menu options.
←	Left arrow	Performs one of the following actions: • Takes no action and displays the LCD panel menu. • Moves the cursor to the left. • Re-enables editing.
→	Right arrow	Performs one of the following actions: • Enters the menu option displayed on that line. • Moves the cursor to the right. • Scrolls through continued text.
X	Cancel	Cancels the action.
+	Add	Increases the selected digit by one.
-	Subtract	Decreases the selected digit by one.
✓	Check mark	Accepts the action.

[Do we want a tip somewhere about returning to the main menu by pressing the left arrow repeatedly?]

Idle Display Mode

The LCD panel enters Idle Display mode after 60 seconds of inactivity (you have not pressed any multi-function keys) with no detected errors. If the system detects an error, the panel enters Error Alert mode (see Error Alert Mode, page 6-9) until the error is resolved. Idle Display mode is also disabled when you are editing your network configuration or running diagnostics.

In Idle Display mode, the panel alternates (at five second intervals) between displaying the CPU utilization and free memory available and the chassis serial number.

A sample of each display might look like this:

```
CPU: 50%
FREE MEM: 1024 MB
```

or:

```
Serial Number:
3D99-101089108-BA0Z
```

In Idle Display mode, press any multi-function key to enter the main menu; see Understanding LCD Panel Components, page 6-2.

Note Pressing a multi-function key as the LCD panel enters Idle Display mode can cause the panel to display an unexpected menu.

Network Configuration Mode

The Firepower System provides a dual stack implementation for both IPv4 and IPv6 management environments. In Network Configuration mode, you can use the LCD panel to configure the network settings for a Firepower device's management interface: the IP address, subnet mask or prefix, and default gateway.

If you edit the IP address of a Firepower device using the LCD panel, confirm that the changes are reflected on the managing Management Center. In some cases, you may need to edit the device management settings manually. See the for more information.

By default, the ability to change network configuration using the LCD panel is disabled. You can enable it during the initial setup process, or using the device's web interface. For more information, see Allowing Network Reconfiguration Using the LCD Panel, page 6-6.

Caution Enabling this option may present a security risk. You need only physical access, not authentication, to configure network settings using the LCD panel.

To configure network settings using Network Configuration mode:

Step 1 In Idle Display mode, press any multi-function key to enter the main menu.

The main menu appears:

```
Network Config          →
System Status        ↓  →
```

[Need to figure out what happens if you don't have permissions. Refer them to system status mode to view network settings?]

Step 2 Press the right arrow (à) key on the top row to access Network Configuration mode.

The LCD panel displays the following:

```
IPv4                ↓ →
IPv6                  →
```

Step 3 Press the right arrow key to select the IP address you want to configure:

- For IPv4, the LCD panel might display the following:

```
IPv4 set to DHCP.   ←
Enable Manual?      →
```

- For IPv6, the LCD panel might display the following:

```
IPv6 Disabled.      ←
Enable Manual?      →
```

Step 4 Press the right arrow key to manually configure the network:

- For IPv4, the LCD panel displays the IPv4 address. For example:

```
IPv4 Address:     - +
194.170.001.001   X →
```

- For IPv6, the LCD panel displays a blank IPv6 address. For example:

```
IPv6 Address:     - +
0000:0000:0000:00 X →
```

The first line on the panel indicates whether you are editing the IPv4 or IPv6 address. The second line displays the IP address you are editing. A cursor underlines the first digit, and represents the digit you are editing. The two symbols correspond with the multi-function keys to the right of each row.

Note that the IPv6 address does not fit completely on the display. As you edit each digit and move the cursor to the right, the IPv6 address scrolls to the right.

Step 5 Edit the digit underlined by the cursor, if needed, and move to the next digit in the IP address:

- To edit the digit, press the minus (-) or plus (+) keys on the top row to decrease or increase the digit by one.
- To move to the next digit in the IP address, press the right arrow key on the bottom row to move the cursor to the next digit to the right.

With the cursor on the first digit, the LCD panel displays the cancel and right arrow symbols at the end of the IP address. With the cursor on any other digit, the LCD panel displays the left and right arrow symbols.

Step 6 When you finish editing the IPv4 or IPv6 address, press the right arrow key again to display the check mark (✓) key to accept the changes.

Before you press the right arrow key, the function symbols on the display looks like the following sample:

```
IPv4 Address:     - +
194.170.001.001   X →
```

After you press the right arrow key, the function symbols on the display looks like the following sample:

```
IPv4 Address:     X ✓
194.170.001.001   ←
```

Step 7 Press the check mark key to accept the changes to the IP address.

For IPv4, the LCD panel displays the following:

```
Subnet Mask:       - +
000.000.000.000    X →
```

For IPv6, the LCD panel displays the following:

```
Prefix:            - +
000.000.000.000    X →
```

Step 8 Edit the subnet mask or prefix the same way you edited the IP address, and press the check mark key to accept the changes.

The LCD panel displays the following:

```
Default Gateway    - +
000.000.000.000    X →
```

Step 9 Edit the default gateway the same way you edited the IP address, and press the check mark key to accept the changes.

The LCD panel displays the following:

```
Save?              ✓
                   X
```

Step 10 Press the check mark key to save your changes.

Allowing Network Reconfiguration Using the LCD Panel

Because it presents a security risk, the ability to change network configuration using the LCD panel is disabled by default. You can enable it during the initial setup process (see Understanding the Setup Process, page 5-2), or using the device's web interface as described in the following procedure.

To allow network reconfiguration using a device's LCD panel:

Access: Admin

Step 1 After you complete the initial setup of the device, log into the device's web interface using an account with Administrator privileges.

Step 2 Select **System > Local > Configuration**.

The Information page appears.

Step 3 Click **Network**.

The Network Settings page appears.

Step 4 Under LCD Panel, select the **Allow reconfiguration of network configuration** check box. When the security warning appears, confirm that you want to enable this option.

Tip For information on the other options on this page, see the *Firepower Management Center Configuration Guide*.

Step 5 Click **Save**.

The network settings are changed.

System Status Mode

The LCD panel's System Status mode displays monitored system information, such as link state propagation, bypass status, and system resources. You can also change the LCD panel's brightness and contrast in System Status mode.

The following table describes the information and options available in this mode.

Table 6-2 System Status Mode Options

Option	Description
Resources	Displays the CPU utilization and free memory available. Note that Idle Display mode also shows this information.

Link State	Displays a list of any inline sets currently in use and the link state status for that set. The first line identifies the inline set, and the second line displays its status (normal or tripped). For example:
	`eth2-eth3:`
	`normal`

Fail Open	Displays a list of the bypass inline sets in use and the status of those pairs, either normal or in bypass.
Fan Status	Displays a list and the status of the fans in the device.
Diagnostics	Accessible after pressing a specific key sequence available from Support. **Caution** Do **not** access the diagnostics menu without the guidance of Support. Accessing the diagnostics menu without specific instructions from Support can damage your system.
LCD Brightness	Allows you to adjust the brightness of the LCD display.
LCD Contrast	Allows you to adjust the contrast of the LCD display.

To enter System Status mode and view monitored system information:

Step 1 In Idle Display mode, press any multi-function key to enter the main menu.

The main menu appears:

```
Network Config          →
System Status        ↓  →
```

Step 2 Press the right arrow (→) key on the bottom row to access System Status mode.

The LCD panel displays the following:

```
Resources            ↓  →
Link State           ↓  →
```

Step 3 Scroll through the options by pressing the down arrow (â) key. Press the right arrow key in the row next to the status you want to view.

Depending on the option you chose, the LCD panel displays the information listed in Table 6-2 on page 6-7. To change the LCD panel brightness or contrast, see the next procedure.

Do we need a step here talking about how to get back?

To adjust the LCD panel brightness or contrast:

Step 1 In System Status mode, scroll through the options by pressing the down arrow (â) key until the LCD panel displays the LCD Brightness and LCD Contrast options:

```
LCD Brightness      ↓ →
LCD Contrast        ↓ →
```

Step 2 Press the right arrow key in the row next to the LCD display feature (brightness or contrast) you want to adjust.

The LCD panel displays the following:

```
Increase              →
Decrease            ↓ →
```

Step 3 Press the right arrow key to increase or decrease the display feature you have selected.

The LCD display changes as you press the keys.

Step 4 Press the down arrow to display the Exit option:

```
Decrease            ↓ →
Exit                  →
```

Step 5 Press the right arrow key in the Exit row to save the setting and return to the main menu.

Information Mode

The LCD panel's Information mode displays identifying system information such as the device's chassis serial number, IP address, model, and software and firmware versions. Support may require this information if you call for assistance.

The following table describes the information available in this mode.

Table 6-3 Information Mode Options

Option	Description
IP address	Displays the IP address of the device's management interface.
Model	Displays the device's model.

Table 6-3 Information Mode Options (continued)

Option	Description
Serial number	Displays the device's chassis serial number.
Versions	Displays the device's system software and firmware versions. Use the multi-function keys to scroll through the following information: • Product version • NFE version • Micro Engine version • Flash version • GerChr version

To enter Information mode and view identifying system information:

Step 1 In Idle Display mode, press any multi-function key to enter the main menu.

The main menu appears:

```
Network Config          →
System Status       ↓ →
```

Step 2 Scroll through the modes by pressing the down arrow (â) key until the LCD panel displays Information mode:

```
System Status       ↓ →
Information         ↓ →
```

Step 3 Press the right arrow (→) key on the bottom row to access Information mode.

Step 4 Scroll through the options by pressing the down arrow (â) key. Press the right arrow key in the row next to the information you want to view.

Depending on the option you chose, the LCD panel displays the information listed in Table 6-3 on page 6-8.

Do we need a step here talking about how to get back?

Error Alert Mode

When a hardware error or fault condition occurs, Error Alert mode interrupts Idle Display mode. In Error Alert mode, the LCD display flashes and displays one or more of the errors listed in the following table.

Table 6-4 LCD Panel Error Alerts

Error	Description
Hardware alarm	Alerts on hardware alarms
Link state propagation	Displays the link state of paired interfaces
Bypass	Displays the status of inline sets configured in bypass mode
Fan status	Alerts when a fan reaches a critical condition

When a hardware error alert occurs, the LCD displays the main hardware alert menu, as follows:

```
HARDWARE ERROR!          →
Exit                     →
```

You can use the multi-function keys to scroll through the list of error alerts or exit Error Alert mode. Note that the LCD display continues to flash and display an alert message until all error conditions are resolved.

The LCD panel always displays the platform daemon error message first, followed by a list of other hardware error messages. The following table provides basic information on Firepower device error messages, where *X* indicates the NFE accelerator card (`0` or `1`) that generated the alert.

Table 6-5 Hardware Alarm Error Messages

Error Message	Condition Monitored	Description
NFE_platformd*X*	platform daemon	Alerts when the platform daemon fails.
`NFE_temp`*X*	temperature status	Alerts when the temperature of the accelerator card exceeds acceptable limits: • `WARNING`: greater than 80°C/176°F (7000 Series) or 97°C/206°F (8000 Series). • `CRITICAL`: greater than 90°C/194°F (7000 Series) or 102°C/215°F (8000 Series).
`HeartBeat`*X*	heartbeat	Alerts when the system cannot detect the heartbeat.
`frag`*X*	`nfe_ipfragd` (host frag) daemon	Alerts when the `ipfragd` daemon fails.
`rules`*X*	`Rulesd` (host rules) daemon	Alerts when the `Rulesd` daemon fails.
`TCAM`*X*	TCAM daemon	Alerts when the `TCAM` daemon fails.
`NFEMessD`*X*	message daemon	Alerts when the message daemon fails.
NFEHardware	hardware status	Alerts when one or more accelerator cards is not communicating.
NFEcount	cards detected	Alerts when the number of accelerator cards detected on the device does not match the expected accelerator card count for the platform.
7000 Series only: GerChr_comm 8000 Series only: NMSB_comm	communications	Alerts when the media assembly is not present or not communicating.
7000 Series only: `gerd` 8000 Series only: `scmd`	`scmd` daemon status	Alerts when the `scmd daemon` fails.
7000 Series only: `gpsl` 8000 Series only: `psls`	`psls` daemon status	Alerts when the `psls daemon` fails.

Table 6-5 Hardware Alarm Error Messages (continued)

Error Message	Condition Monitored	Description
7000 Series only: `gftw` 8000 Series only: `ftwo`	`ftwo` daemon status	Alerts when the `ftwo daemon` fails.

`NFE_port18`
`NFE_port19`
`NFE_port20`
`NFE_port21`
	internal link status	Alerts when the link between the network module switch board and the accelerator card fails:
		• 7000 Series
		All families: `NFE_port18` only
		• 8000 Series
		81xx Family: `NFE_port18` and `NFE_port19` only
		82xx Family and 83xx Family: `NFE_port18`, `NFE_port19`, `NFE_port20`, and `NFE_port21`

Use the following procedure to view hardware alert error messages on the LCD display.

To view the hardware alert error messages:

Step 1 In Error Alert mode, on the HARDWARE ERROR! line, press the right arrow (→) key to view the hardware errors that triggered the Error Alert mode.

The LCD panel lists the error alert messages starting with the `NFE platform` daemon failure followed by a list of error messages.

`NFEplatformd`*X*
`NFEtemp`*X* ↓
where *X* indicates the accelerator card (either `0` or `1`) that generated the alert.

Step 2 On the error message line, press the down arrow (â) key to view additional errors. When there are no additional errors, the Exit row appears.

`Exit` →

Step 3 Press the right arrow (→) key to exit Error Alert mode.

If you exit Error Alert mode before you resolve the error that triggered the alert, the LCD panel returns to Error Alert mode. Contact Support for assistance.

Hardware Specifications

Firepower 7000 and 8000 Series devices are delivered on a variety of platforms to meet the needs of your organization.

Rack and Cabinet Mounting Options

You can mount Firepower devices in racks and server cabinets. The appliance comes with a rack-mounting kit except for the Firepower 7010, 7020, 7030, and 7050. For information on mounting the appliance in a rack, refer to the instructions delivered with the rack-mounting kit.

The Firepower 7010, 7020, 7030, and 7050 require a tray and rack-mounting kit, available separately. You can purchase rack and cabinet mounting kits for other appliances separately.

Firepower 7000 Series Devices

All Firepower 7000 Series devices have an LCD panel on the front of the appliance where you can view and, if enabled, configure your appliance. See the following sections for information:

- Firepower 7010, 7020, 7030, and 7050, page 7-1
- Firepower 7110 and 7120, page 7-6
- Firepower 7115, 7125, and AMP7150, page 7-13

Firepower 7010, 7020, 7030, and 7050

The Firepower 7010, 7020, 7030, and 7050 devices, also called the 70xx Family, are 1U appliances, one-half the width of the rack tray and delivered with eight copper interfaces, each with configurable bypass capability. See the *Regulatory Compliance and Safety Information for FirePOWER and FireSIGHT Appliances* document for safety considerations for Firepower 70xx Family appliances.

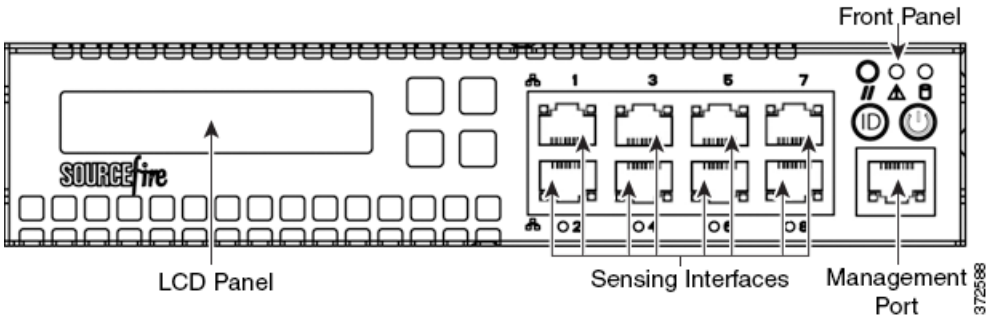
See the following sections for more information:

- Firepower 70xx Family Front View, page 7-2
- Firepower 70xx Family Rear View, page 7-5
- Firepower 70xx Family Physical and Environmental Parameters, page 7-5

Firepower 70xx Family Front View

The front of the chassis contains the LCD panel, sensing interfaces, front panel, and management interface.

Figure 7-1 Firepower 70xx Family (Chassis: CHRY-1U-AC; NEME-1U-AC) Front View



The following table describes the features on the front of the appliance.

Table 7-1 Firepower 70xx Family System Components: Front View

Feature	Description
LCD panel	Operates in multiple modes to configure the device, display error messages, and view system status. For more information, see Using the LCD Panel on a Firepower Device, page 6-1.
Sensing interfaces	Contain the sensing interfaces that connect to the network. For information, see Sensing Interfaces, page 7-4.
10/100/1000 Ethernet management interface	Provides for an out-of-band management network connection. The management interface is used for maintenance and configuration purposes **only** and is not intended to carry service traffic.
Front panel	Houses LEDs that display the system's operating state, as well as various controls, such as the power button. For more information, see Table 7-11Firepower 7110 and 7120 Front Panel Components, page 7-8.

Figure 7-2 Firepower 70xx Family Front Panel

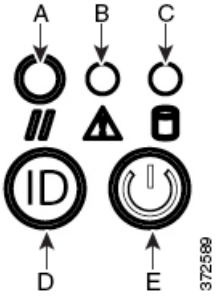


Table 7-2 Front Panel Components

A	Reset button	D	System ID button
B	System status LED	E	Power button and LED
C	Hard drive activity LED		

The front panel of the chassis houses LEDs, which display the system's operating state. The following table describes the LEDs on the front panel.

Table 7-3 Firepower 70xx Family Front Panel LEDs

LED	Description
Reset button	Allows you to reboot the appliance without disconnecting it from the power supply.
System status	Indicates the system status: • A green light indicates the system is powered up and operating normally, or powered down and attached to AC power. • An amber light indicates a system fault. See Table 7-4 on page 7-3 for more information.
Hard drive activity	Indicates the hard drive status: • A blinking green light indicates the fixed disk drive is active. • If the light is off, there is no drive activity or the system is powered off.
System ID	When pressed, the ID button displays a blue light, and a blue light is visible at the rear of the chassis.
Power button and LED	Indicates whether the appliance has power: • A green light indicates that the appliance has power and the system is on. • No light indicates the system is shut down or does not have power.

The following table describes the conditions under which the system status LEDs might be lit.

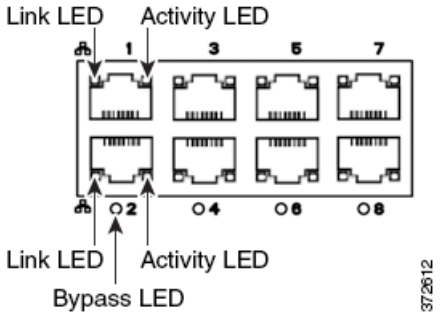
Table 7-4 Firepower 70xx Family System Status

Condition	Description
Critical	Any critical or non-recoverable threshold crossing associated with the following events: • temperature, voltage, or fan critical threshold crossing • power subsystem failure • system inability to power up due to incorrectly installed processors or processor incompatibility • critical event logging errors, including System Memory Uncorrectable ECC error and fatal/uncorrectable bus errors, such as PCI SERR and PERR
Non-critical	A non-critical condition is a threshold crossing associated with the following events: • temperature, voltage, or fan non-critical threshold crossing • Set Fault Indication command from system BIOS; the BIOS may use the command to indicate additional, non-critical status such as system memory or CPU configuration changes
Degraded	A degraded condition is associated with the following events: • one or more processors are disabled by Fault Resilient Boot (FRB) or BIOS • some system memory disabled or mapped out by BIOS • one of the power supplies unplugged or not functional

Sensing Interfaces

The Firepower 70xx Family appliances are delivered with eight copper interfaces, each with configurable bypass capability.

Figure 7-3 Eight-Port 1000BASE-T Copper Interfaces



Use the following table to understand the activity and link LEDs on the copper interfaces.

Table 7-5 Firepower 70xx Family Copper Link/Activity LEDs

Status	Description
Both LEDs off	The interface does not have link.
Link amber	The speed of the traffic on the interface is 10Mb or 100Mb.
Link green	The speed of the traffic on the interface is 1Gb.
Activity blinking green	The interface has link and is passing traffic.

Use the following table to understand bypass LEDs on the copper interfaces.

Table 7-6 Firepower 70xx Family Copper Bypass LEDs

Status	Description
Off	The interface pair is not in bypass mode or has no power.
Steady green	The interface pair is ready to enter bypass mode.
Steady amber	The interface pair has been placed in bypass mode intentionally, or has entered bypass mode gracefully, and is not inspecting traffic.
Blinking amber	The interface pair has unexpectedly entered bypass mode; that is, it has failed open.

The 10/100/1000 management interface is located on the front of the appliance. The following table describes the LEDs associated with the management interface.

Table 7-7 Firepower 70xx Family Management Interface LEDs

LED	Description	
Left (link)	7010/20/30	Indicates whether the link is up. If the light is on, the link is up. If the light is off, there is no link.
	7050	For 10Mbps links, the link light does not illuminate. Link status is shared with the right (activity) LED.

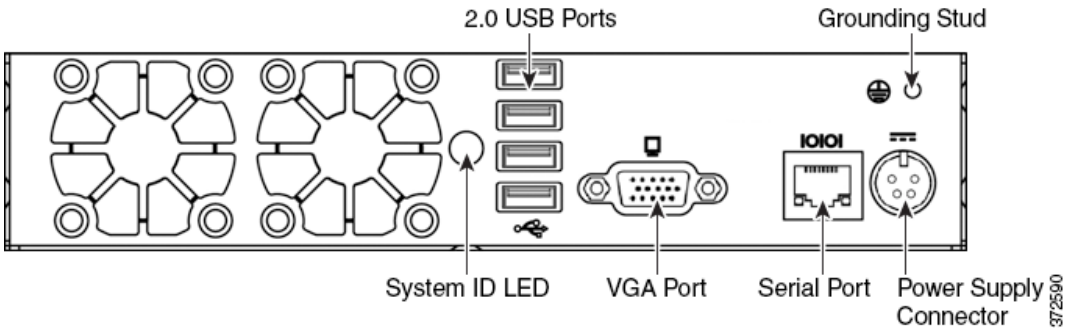
Table 7-7 Firepower 70xx Family Management Interface LEDs (continued)

LED	Description	
Right (activity)	7010/20/30	Indicates activity on the port. If the light is blinking, there is activity. If the light is off, there is no activity.
	7050	For 10Mbps links, if the light is on, there is link and activity. If the light is off, there is no link or activity.

Firepower 70xx Family Rear View

The rear of the chassis contains the system ID LED, connection ports, grounding stud, and power supply connector.

Figure 7-4 Firepower 70xx Family (Chassis: CHRY-1U-AC) Rear View



The following table describes the features that appear on the rear of the appliance.

Table 7-8 Firepower 70xx Family System Components: Rear View

Feature	Description
System ID LED	Helps identify a system installed in a high-density rack with other similar systems. The blue LED indicates that the ID button is pressed.
2.0 USB ports VGA port Serial port	Allows you to attach a monitor and keyboard to the device to establish a direct workstation-to-appliance connection.
Grounding stud	Allows you to connect the appliance to the common bonding network. See the Power Requirements for Firepower Devices, page A-1 for more information.
12V Power supply connector	Provides a power connection to the device through an AC power source.

Firepower 70xx Family Physical and Environmental Parameters

The following table describes the physical attributes and the environmental parameters for the appliance.

Table 7-9 Firepower 70xx Family Physical and Environmental Parameters

Parameter	Description	
Form factor	1U, half rack width	
Dimensions (D x W x H)	Single chassis: 12.49 in. x 7.89 in. x 1.66 in. (31.74 cm x 20.04 cm x 4.21 cm) 2-Chassis Tray: 25.05 in. x 17.24 in. x 1.73 in. (63.62 cm x 43.8 cm x 4.44 cm)	
Chassis weight maximum installed	Chassis: 7 lbs (3.17 kg) Single chassis and power supply in tray: 17.7 lbs (8.03 kg) Double chassis and power supplies in single tray: 24.7 lbs (11.2 kg)	
Copper 1000BASE-T	Gigabit copper Ethernet bypass-capable interfaces in a paired configuration Cable and distance: Cat5E at 50 m	
Power supply	200 W AC power supply Voltage: 100 VAC to 240 VAC nominal (90 VAC to 264 VAC maximum) Current: 2A maximum over the full range Frequency range: 50/60 Hz nominal (47 Hz to 63 Hz maximum)	
Operating temperature	7010/20/30	32°F to 104°F (0°C to 40°C)
	7050	23°F to 104°F (-5°C to 40°C)
Non-operating temperature	7010/20/30	-4°F to 158°F (-20°C to 70°C)
	7050	14°F to 140°F (-10°C to 60°C)
Operating humidity	7010/20/30	5% to 95%, non-condensing Operation beyond these limits is not guaranteed and not recommended.
	7050	5% to 85%, non-condensing Operation beyond these limits is not guaranteed and not recommended.
Non-operating humidity	7010/20/30	0% to 95%, non-condensing
	7050	0% to 85%, non-condensing
	Store the unit below the maximum non-condensing relative humidity. Acclimate below maximum operating humidity at least 48 hours prior to placing the unit in service.	
Altitude	0 ft (sea level) to 5905 ft (0 m to 1800 m)	
Cooling requirements	682 BTU/hour You must provide sufficient cooling to maintain the appliance within its required operating temperature range. Failure to do this may cause a malfunction or damage to the appliance.	
Acoustic noise	53 dBA when idle. 62 dBA at full processor load	
Operating shock	No errors with half a sine wave shock of 5G (with 11 ms duration)	
Airflow	20 ft^3 (0.57 m^3) per minute Airflow through the appliance enters at the front and sides and exits at the rear.	

Firepower 7110 and 7120

The Firepower 7110 and 7120 devices, part of the 71xx Family, are 1U appliances, and are delivered with eight copper or eight fiber interfaces, each with configurable bypass capability. See the *Regulatory Compliance and Safety Information for FirePOWER and FireSIGHT Appliances* document for safety considerations for 71xx Family appliances.

See the following sections for more information:

- Firepower 7110 and 7120 Chassis Front View, page 7-7
- Firepower 7110 and 7120 Chassis Rear View, page 7-11
- Firepower 7110 and 7120 Physical and Environmental Parameters, page 7-12

Firepower 7110 and 7120 Chassis Front View

The front of the chassis contains the LCD panel, USB port, front panel, and either copper or fiber sensing interfaces.

Figure 7-5 Firepower 7110 and 7120 with Copper Interfaces (Chassis: GERY-1U-8-C-AC)

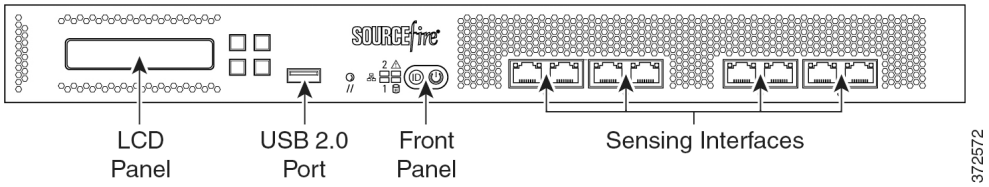
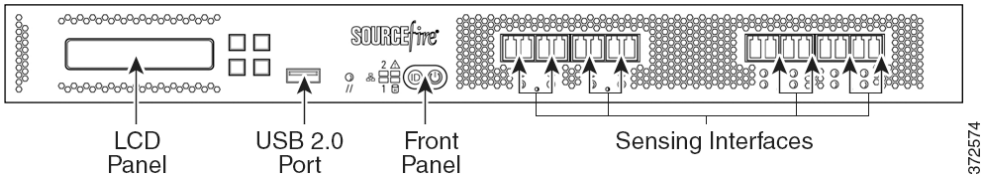


Figure 7-6 Firepower 7110 and 7120 with Fiber Interfaces (Chassis: GERY-1U-8-FM-AC)



The following table describes the features on the front of the appliance.

Table 7-10 Firepower 7110 and 7120 System Components: Front View

Feature	Description
LCD panel	Operates in multiple modes to configure the device, display error messages, and view system status. For more information, see Using the LCD Panel on a Firepower Device, page 6-1.
Front panel USB 2.0 port	Allows you to attach a keyboard to the device.
Front panel	Houses LEDs that display the system's operating state, as well as various controls, such as the power button. For more information, see Figure 7-7Firepower 7110 and 7120 Front Panel, page 7-8.
Sensing interfaces	Contain the sensing interfaces that connect to the network. For more information, see Firepower 7110 and 7120 Sensing Interfaces, page 7-9.

Figure 7-7 Firepower 7110 and 7120 Front Panel

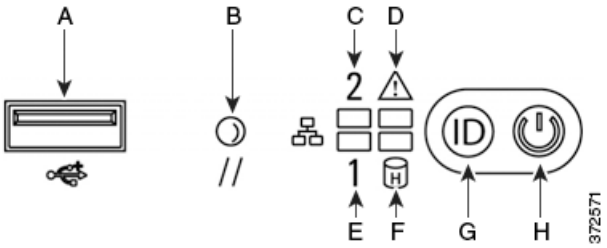


Table 7-11 Firepower 7110 and 7120 Front Panel Components

A	USB 2.0 connector	E	NIC1 activity LED
B	Reset button	F	Hard drive activity LED
C	NIC2 activity LED	G	ID button
D	System status LED	H	Power button and LED

The front panel of the chassis houses LEDs, which display the system's operating state. The following table describes the LEDs on the front panel.

Table 7-12 Firepower 7110 and 7120 Front Panel LEDs

LED	Description
NIC activity (1 and 2)	Indicates whether there is any network activity: • A green light indicates there is network activity. • No light indicates there is no network activity.
System status	Indicates the system status: • No light indicates the system is operating normally, or is powered off. • A red light indicates a system error. See the Table 7-13Firepower 7110 and 7120 System Status, page 7-9 for more information.
Reset button	Allows you to reboot the appliance without disconnecting it from the power supply.
Hard drive activity	Indicates the hard drive status: • A blinking green light indicates the fixed disk drive is active. • An amber light indicates a fixed disk drive fault. • If the light is off, there is no drive activity or the system is powered off.
System ID	Helps identify a system installed in a high-density rack with other similar systems: • A blue light indicates the ID button is pressed and a blue light is on at the rear of the appliance. • No light indicates the ID button is not pressed.
Power button and LED	Indicates whether the appliance has power: • A green light indicates that the appliance has power and the system is on. • A blinking green light indicates that the appliance has power and is shut down. • If the light is off, the system does not have power.

The following table describes the conditions under which the system status LEDs might be lit.

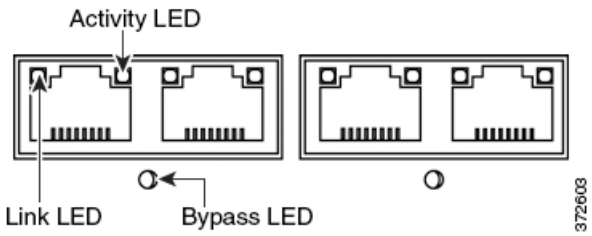
Table 7-13 Firepower 7110 and 7120 System Status

Condition	Description
Critical	Any critical or non-recoverable threshold crossing associated with the following events: • temperature, voltage, or fan critical threshold crossing • power subsystem failure • system inability to power up due to incorrectly installed processors or processor incompatibility • critical event logging errors, including System Memory Uncorrectable ECC error and fatal/uncorrectable bus errors, such as PCI SERR and PERR
Non-critical	A non-critical condition is a threshold crossing associated with the following events: • temperature, voltage, or fan non-critical threshold crossing • chassis intrusion • Set fault indication command from system BIOS; the BIOS may use the command to indicate additional non-critical status such as system memory or CPU configuration changes
Degraded	Any degraded condition is associated with the following events: • one or more processors are disabled by Fault Resilient Boot (FRB) or BIOS • some system memory disabled or mapped out by BIOS • one of the power supplies unplugged or not functional **Tip** If you observe a degraded condition indication, check your power supply connections first. Power down the device, disconnect both power cords, reconnect the power cords to reseat them, then restart the device. ⚠ **Caution** To power down safely, use the procedure in the Managing Devices chapter in the *Firepower Management Center Configuration Guide*, or the `system shutdown` command from the CLI.

Firepower 7110 and 7120 Sensing Interfaces

The Firepower 7110 and 7120 devices are delivered with eight-port copper or eight-port fiber interfaces, each with configurable bypass capability.

Figure 7-8 Eight-Port 1000BASE-T Copper Interfaces



Use the following table to understand the activity and link LEDs on the copper interfaces.

Table 7-14 Firepower 7110 and 7120 Copper Link/Activity LEDs

Status	Description
Both LEDs off	The interface does not have link.
Link amber	The speed of the traffic on the interface is 10Mb or 100Mb.
Link green	The speed of the traffic on the interface is 1Gb.
Activity blinking green	The interface has link and is passing traffic.

Use the following table to understand the bypass LED on the copper interfaces.

Table 7-15 Firepower 7110 and 7120 Copper Bypass LED

Status	Description
Off	The interface pair is not in bypass mode or has no power.
Steady green	The interface pair is ready to enter bypass mode.
Steady amber	The interface pair has been placed in bypass mode and is not inspecting traffic.
Blinking amber	The interface pair is in bypass mode; that is, it has failed open.

Figure 7-9 Eight-Port 1000BASE-SX Fiber Configurable Bypass Interfaces

Use the following table to understand the link and activity LEDs on the fiber interfaces.

Table 7-16 Firepower 7110 and 7120 Fiber Link/Activity LEDs

Status	Description
Top (activity)	For an inline interface: the light is on when the interface has activity. If dark, there is no activity. For a passive interface: the light is non-functional.
Bottom (link)	For an inline or passive interface: the light is on when the interface has link. If dark, there is no link.

Use the following table to understand the activity and link LEDs on the fiber interfaces.

Table 7-17 Firepower 7110 and 7120 Fiber Bypass LEDs

Status	Description
Off	The interface pair is not in bypass mode or has no power.
Steady green	The interface pair is ready to enter bypass mode.

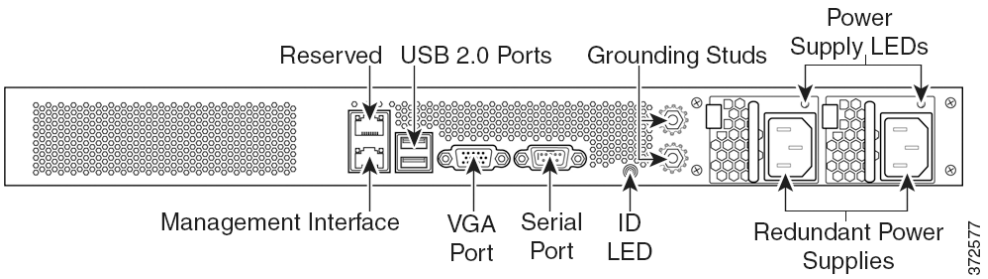
Table 7-17 Firepower 7110 and 7120 Fiber Bypass LEDs (continued)

Status	Description
Steady amber	The interface pair has been placed in bypass mode and is not inspecting traffic.
Blinking amber	The interface pair is in bypass mode; that is, it has failed open.

Firepower 7110 and 7120 Chassis Rear View

The rear of the chassis contains the management interface, connection ports, grounding studs, and power supplies.

Figure 7-10 Firepower 7110 and 7120 (Chassis: GERY-1U-8-C-AC or GERY-1U-8-FM-AC) Rear View



The following table describes the features that appear on the rear of the appliance.

Table 7-18 Firepower 7110 and 7120 System Components: Rear View

Features	Description
VGA port USB port	Allows you to attach a monitor, keyboard, and mouse to the device to establish a direct workstation-to-appliance connection.
10/100/1000 Ethernet management interface	Provides for an out-of-band management network connection. The management interface is used for maintenance and configuration purposed **only** and is not intended to carry service traffic.
System ID LED	Helps identify a system installed in a high-density rack with other similar systems. The blue light indicates that the ID button is pressed.
Grounding studs	Allows you to connect the appliance to the Common Bonding Network. See the Power Requirements for Firepower Devices, page A-1 for more information.
Redundant power supplies	Provides power to the device through an AC power source. Looking at the rear of the chassis, power supply #1 is on the left and power supply #2 is on the right. The power supplies are hot-swappable.
Power supply LEDs	Indicates the status of the power supply. See Table 7-20Firepower 7110 and 7120 Power Supply LED, page 7-12.

The 10/100/1000 management interface is located on the rear of the appliance. The following table describes the LEDs associated with the management interface.

Table 7-19 Firepower 7110 and 7120 Management Interface LEDs

LED	Description
Left (activity)	Indicates activity on the port: • A blinking light indicates activity. • No light indicates there is no activity.
Right (link)	Indicates whether the link is up: • A light indicates the link is up. • No light indicates there is no link.

The power supply modules are located on the rear of the appliance. The following table describes the LED associated with the power supply.

Table 7-20 Firepower 7110 and 7120 Power Supply LED

LED	Description
Off	The power cord is not plugged in.
Red	No power supplied to this module. or A power supply critical event, such as module failure, a blown fuse, or a fan failure; the power supply shuts down.
Blinking red	A power supply warning event, such as high temperature or a slow fan; the power supply continues to operate.
Blinking green	AC input is present; volts on standby, the power supply is switched off.
Green	The power supply is plugged in and on.

Firepower 7110 and 7120 Physical and Environmental Parameters

The following table describes the physical attributes and the environmental parameters for the appliance.

Table 7-21 Firepower 7110 and 7120 Physical and Environmental Parameters

Parameter	Description
Form factor	1U
Dimensions (D x W x H)	21.6 in. x 19.0 in. x 1.73 in. (54.9 cm x 48.3 cm x 4.4 cm)
Weight maximum installed	27.5 lbs (12.5 kg)
Copper 1000BASE-T	Gigabit copper Ethernet bypass-capable interfaces in a paired configuration Cable and distance: Cat5E at 50 m
Fiber 1000BASE-SX	Fiber bypass-capable interfaces with LC connectors Cable and distance: SX is multimode fiber (850 nm) at 550 m (standard)

Table 7-21 Firepower 7110 and 7120 Physical and Environmental Parameters (continued)

Parameter	Description
Power supply	450 W dual redundant (1+1) AC power supplies Voltage: 100 VAC to 240 VAC nominal (85 VAC to 264 VAC maximum) Current: 3A maximum for 90 VAC to 132 VAC, per supply 1.5A maximum for 187 VAC to 264 VAC, per supply Frequency range: 47 Hz to 63 Hz **Note** The power supplies are hot-swappable.
Operating temperature	41°F to 104°F (5°C to 40°C)
Non-operating temperature	-29°F to 158°F (-20°C to 70°C)
Operating humidity	5% to 85% non-condensing
Non-operating humidity	5% to 90%, non-condensing with a maximum wet bulb of 82°F (28°C) at temperatures from 77°F to 95°F (25°C to 35°C) Store the unit below 95% non-condensing relative humidity. Acclimate below maximum operating humidity at least 48 hours before placing the unit in service.
Altitude	0ft (sea level) to 5905 ft (0 m to 1800 m)
Cooling requirements	900 BTU/hour You must provide sufficient cooling to maintain the appliance within its required operating temperature range. Failure to do this may cause a malfunction or damage to the appliance.
Acoustic noise	64 dBA at full processor load, normal fan operation Meets GR-63-CORE 4.6 Acoustic Noise
Operating shock	Complies with Bellecore GR-63-CORE standards
Airflow	140 ft^3 (3.9 m^3) per minute Airflow through the appliance enters at the front and exits at the rear with no side ventilation.

Firepower 7115, 7125, and AMP7150

The Firepower 7115, 7125, and AMP7150 devices, part of the 71xx Family, are delivered with four-port copper interfaces with configurable bypass capability, and eight hot-swappable small form-factor pluggable (SFP) ports without bypass capability. To ensure compatibility, use only Cisco SFP transceivers.

Note The Firepower AMP7150 has many of the same form factors as the Firepower 7115 and 7125, but has been optimized to take advantage of the Firepower System's AMP for Networks capabilities.

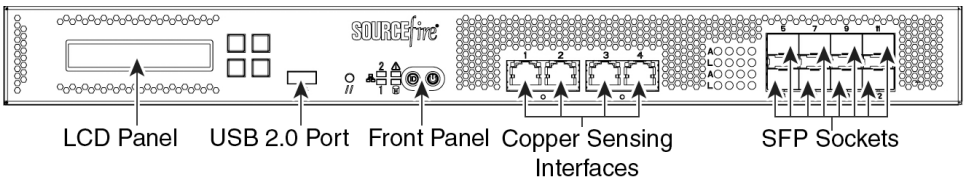
See the following sections for more information:

- Firepower 7115, 7125, and AMP7150 Chassis Front View, page 7-14
- Firepower 7115, 7125, and AMP7150 Chassis Rear View, page 7-18
- Firepower 7115, 7125, and AMP7150 Physical and Environmental Parameters, page 7-20

Firepower 7115, 7125, and AMP7150 Chassis Front View

The front of the chassis contains the LCD panel, USB port, front panel, copper sensing interfaces, and SFP sockets.

Figure 7-11 Firepower 7115, 7125, and AMP7150 (Chassis: GERY-1U-8-4C8S-AC) Front View



The following table describes the features on the front of the appliance.

Table 7-22 Firepower 7115, 7125, and AMP7150 System Components: Front View

Feature	Description
LCD panel	Operates in multiple modes to configure the device, display error messages, and view system status. For more information, see Using the LCD Panel on a Firepower Device, page 6-1.
Front panel USB 2.0 port	Allows you to attach a keyboard to the device.
Front panel	Houses LEDs that display the system's operating state, as well as various controls, such as the power button. For more information, see Figure 7-12Firepower 7115, 7125, and AMP7150 Front Panel, page 7-14.
Sensing interfaces	Contain the sensing interfaces that connect to the network. For more information, see Firepower 7115, 7125, and AMP7150 Sensing Interfaces, page 7-16.

Figure 7-12 Firepower 7115, 7125, and AMP7150 Front Panel

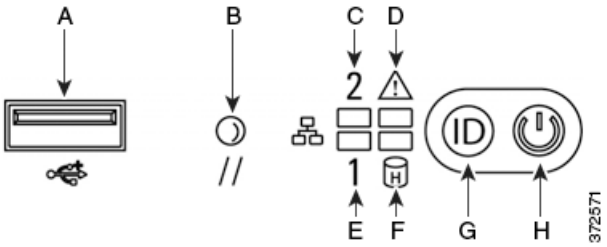


Table 7-23 Firepower 7115, 7125, and AMP7150 Front Panel Components

A	USB 2.0 connector	E	NIC1 activity LED
B	Reset button	F	Hard drive activity LED
C	NIC2 activity LED	G	ID button
D	System status LED	H	Power button and LED

The front panel of the chassis houses LEDs, which display the system's operating state. The following table describes the LEDs on the front panel.

Table 7-24 Firepower 7115, 7125, and AMP7150 Front Panel LEDs

LED	Description
NIC activity (1 and 2)	Indicates whether there is any network activity: • A green light indicates there is network activity. • No light indicates there is no network activity.
System status	Indicates the system status: • No light indicates the system is operating normally, or is powered off. • A red light indicates a system error. See the Table 7-25Firepower 7115, 7125, and AMP7150 System Status, page 7-16 for more information.
Reset button	Allows you to reboot the appliance without disconnecting it from the power supply.
Hard drive activity	Indicates the hard drive status: • A blinking green light indicates the fixed disk drive is active. • An amber light indicates a fixed disk drive fault. • If the light is off, there is no drive activity or the system is powered off.
System ID	Helps identify a system installed in a high-density rack with other similar systems: • A blue light indicates the ID button is pressed and a blue light is on at the rear of the appliance. • No light indicates the ID button is not pressed.
Power button and LED	Indicates whether the appliance has power: • A green light indicates that the appliance has power and the system is on. • A blinking green light indicates that the appliance has power and is shut down. • No light indicates the system does not have power.

The following table describes the conditions under which the system status LEDs might be lit.

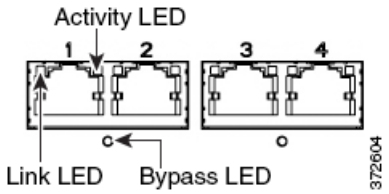
Table 7-25 Firepower 7115, 7125, and AMP7150 System Status

Condition	Description
Critical	Any critical or non-recoverable threshold crossing associated with the following events: • temperature, voltage, or fan critical threshold crossing • power subsystem failure • system inability to power up due to incorrectly installed processors or processor incompatibility • critical event logging errors, including System Memory Uncorrectable ECC error and fatal/uncorrectable bus errors, such as PCI SERR and PERR
Non-critical	A non-critical condition is a threshold crossing associated with the following events: • temperature, voltage, or fan non-critical threshold crossing • chassis intrusion • Set Fault Indication command from system BIOS; the BIOS may use the command to indicate additional non-critical status such as system memory or CPU configuration changes
Degraded	Any degraded condition is associated with the following events: • one or more processors are disabled by Fault Resilient Boot (FRB) or BIOS • some system memory disabled or mapped out by BIOS • one of the power supplies unplugged or not functional **Tip** If you observe a degraded condition indication, check your power supply connections first. Power down the device, disconnect both power cords, reconnect the power cords to reseat them, then restart the device. **Caution** To power down safely, use the procedure in the Managing Devices chapter in the *Firepower Management Center Configuration Guide*, or the `system shutdown` command from the CLI.

Firepower 7115, 7125, and AMP7150 Sensing Interfaces

The Firepower 7115, 7125, and AMP7150 devices are delivered with four-port copper interfaces with configurable bypass capability, and eight hot-swappable small form-factor pluggable (SFP) ports without bypass capability.

Figure 7-13 Four 1000BASE-T Copper Interfaces



Use the following table to understand the link and activity LEDs on copper interfaces.

Table 7-26 Firepower 7115, 7125, and AMP7150 Copper Link/Activity LEDs

Status	Description
Both LEDs off	The interface does not have link.
Link amber	The speed of the traffic on the interface is 10Mb or 100Mb.
Link green	The speed of the traffic on the interface is 1Gb.
Activity blinking green	The interface has link and is passing traffic.

Use the following table to understand the bypass LED on copper interfaces.

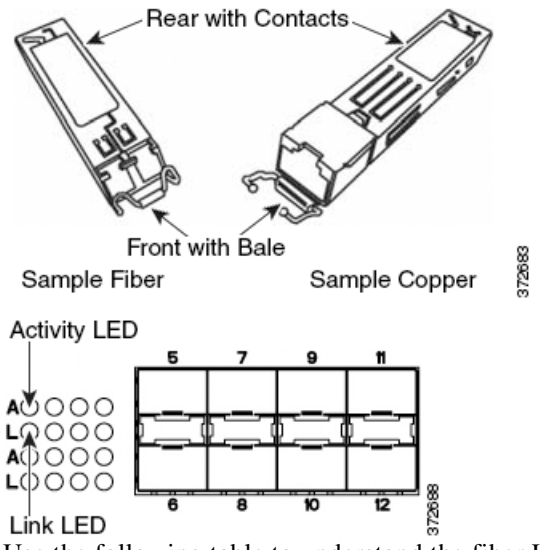
Table 7-27 Firepower 7115, 7125, and AMP7150 Copper Bypass LED

Status	Description
Off	The interface pair is not in bypass mode or has no power.
Steady green	The interface pair is ready to enter bypass mode.
Steady amber	The interface pair has been placed in bypass mode and is not inspecting traffic.
Blinking amber	The interface pair is in bypass mode; that is, it has failed open.

SFP Interfaces

You can install up to eight hot-swappable Cisco SFP transceivers, available in 1G copper, 1G short range fiber, or 1G long range fiber. SFP transceivers do not have bypass capability and should not be used in intrusion prevention deployments. See Using SFP Transceivers in 3D71x5 and AMP7150 Devices, page B-1 for more information.

Figure 7-14 Sample SFP Transceivers



Use the following table to understand the fiber LEDs.

Table 7-28 Firepower 7115, 7125, and AMP7150 SFP Socket Activity/Link LEDs

Status	Description
Top (activity)	For an inline interface: the light is on when the interface has activity. If dark, there is no activity. For a passive interface: the light is non-functional.
Bottom (link)	For an inline or passive interface: the light is on when the interface has link. If dark, there is no link.

Use the following table to understand the specifications of the SFP optical transceivers.

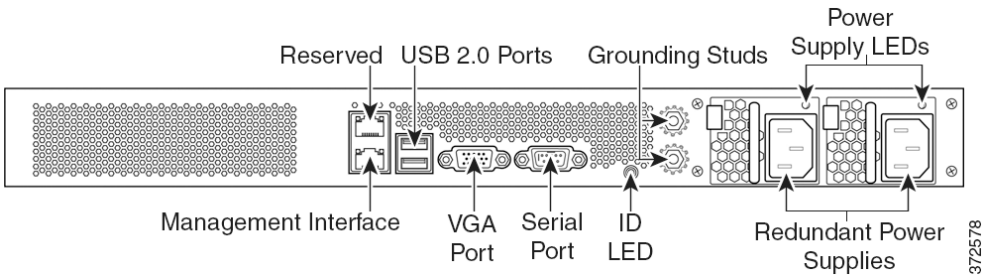
Table 7-29 Firepower 7115, 7125, and AMP7150 SFP Optical Parameters

Parameter	1000BASE-SX	1000BASE-LX
Optical connectors	LC duplex	LC duplex
Bit rate	1000Mbps	1000Mbps
Baud rate/encoding/tolerance	1250Mbps 8b/10b encoding	1250Mbps 8b/10b encoding
Optical interface	Multimode	Single mode only
Operating distances	656 ft (200 m) for 62.5 µm/125 µm fiber 1640 ft (500 m) for 50 µm/125 µm fiber	6.2 miles (10 km) for 9 µm/125 µm fiber
Transmitter wavelength	770-860 nm (850 nm typical)	1270-1355 nm (1310 nm typical)
Maximum average launch power	0 dBm	-3 dBm
Minimum average launch power	-9.5 dBm	-11.5 dBm
Maximum average power at receiver	0 dBm	-3 dBm
Receiver sensitivity	-17 dBm	-19 dBm

Firepower 7115, 7125, and AMP7150 Chassis Rear View

The rear of the chassis contains the management interface, connection ports, grounding studs, and power supplies.

Figure 7-15 Firepower 7115, 7125, and AMP7150 (Chassis: GERY-1U-8-4C8S-AC) Rear View



The following table describes the features that appear on the rear of the appliance.

Table 7-30 Firepower 7115, 7125 and AMP7150 System Components: Rear View

Features	Description
VGA port USB port	Allows you to attach a monitor, keyboard, and mouse to the device to establish a direct workstation-to-appliance connection.
10/100/1000 Ethernet management interface	Provides for an out-of-band management network connection. The management interface is used for maintenance and configuration purposed **only** and is not intended to carry service traffic.
System ID LED	Helps identify a system installed in a high-density rack with other similar systems. The blue light indicates that the ID button is pressed.
Grounding studs	Allows you to connect the appliance to the Common Bonding Network. See the Power Requirements for Firepower Devices, page A-1 for more information.
Redundant power supplies	Provides power to the device through an AC power source. Looking at the rear of the chassis, power supply #1 is on the left and power supply #2 is on the right. **Note** The power supplies are hot-swappable.
Power supply LEDs	Indicates the status of the power supply. See Table 7-32Firepower 7115, 7125, and AMP7150 Power Supply LED, page 7-19.

The 10/100/1000 management interface is located on the rear of the appliance. The following table describes the LEDs associated with the management interface.

Table 7-31 Firepower 7115, 7125, and AMP7150 Management Interface LEDs

LED	Description
Left (activity)	Indicates activity on the port: • A blinking light indicates activity. • No light indicates there is no activity.
Right (link)	Indicates whether the link is up: • A light indicates the link is up. • No light indicates there is no link.

The power supply modules are located on the rear of the appliance. The following table describes the LED associated with the power supply.

Table 7-32 Firepower 7115, 7125, and AMP7150 Power Supply LED

LED	Description
Off	The power cord is not plugged in.
Red	No power supplied to this module. or A power supply critical event, such as module failure, a blown fuse, or a fan failure; the power supply shuts down.
Blinking red	A power supply warning event, such as high temperature or a slow fan; the power supply continues to operate.

Table 7-32 Firepower 7115, 7125, and AMP7150 Power Supply LED (continued)

LED	Description
Blinking green	AC input is present; volts on standby, the power supply is switched off.
Green	The power supply is plugged in and on.

Firepower 7115, 7125, and AMP7150 Physical and Environmental Parameters

The following table describes the physical attributes and the environmental parameters for the appliance.

Table 7-33 Firepower 7115, 7125, and AMP7150 Physical and Environmental Parameters

Parameter	Description
Form factor	1U
Dimensions (D x W x H)	21.6 in. x 19.0 in. x 1.73 in. (54.9 cm x 48.3 cm x 4.4 cm)
Weight maximum installed	29.0 lbs (13.2 kg)
Copper 1000BASE-T	Gigabit copper Ethernet bypass-capable interfaces in a paired configuration Cable and distance: Cat5E at 50 m
Copper 1000BASE-T SFP	Gigabit copper Ethernet non-bypass capable interfaces in a paired configuration Cable and distance: Cat5E at 50 m
Fiber 1000BASE-SX SFP	Fiber non-bypass capable interfaces with LC connectors Cable and distance: SX is multimode fiber (850 nm) at 550 m (standard) 656 ft (200 m) for 62.5 µm/125 µm fiber 1640 ft (500 m) for 50 µm/125 µm fiber
Fiber 1000BASE-LX SFP	Fiber non-bypass capable interfaces with LC connectors Cable and distance: LX is single mode fiber (1310 nm) at 10 km for 9 µm/125 µm fiber (standard)
Power supply	450 W dual redundant (1+1) AC power supplies Voltage: 100 VAC to 240 VAC nominal (85 VAC to 264 VAC maximum) Current: 3A maximum for 90 VAC to 132 VAC, per supply 1.5A maximum for 187 VAC to 264 VAC, per supply Frequency range: 47 Hz to 63 Hz **Note** The power supplies are hot-swappable.
Operating temperature	41ºF to 104ºF (5ºC to 40ºC)
Non-operating temperature	-29ºF to 158ºF (-20ºC to 70ºC)
Operating humidity	5% to 85% non-condensing
Non-operating humidity	5% to 90%, non-condensing with a maximum wet bulb of 82ºF (28ºC) at temperatures from 77ºF to 95ºF (25ºC to 35ºC) Store the unit below 95% non-condensing relative humidity. Acclimate below maximum operating humidity at least 48 hours before placing the unit in service.
Altitude	0ft (sea level) to 5905 ft (0 m to 1800 m)

Table 7-33 Firepower 7115, 7125, and AMP7150 Physical and Environmental Parameters (continued)

Parameter	Description
Cooling requirements	900 BTU/hour You must provide sufficient cooling to maintain the appliance within its required operating temperature range. Failure to do this may cause a malfunction or damage to the appliance.
Acoustic noise	64 dBA at full processor load, normal fan operation Meets GR-63-CORE 4.6 Acoustic Noise
Operating shock	Complies with Bellecore GR-63-CORE standards
Airflow	140 ft^3 (3.9 m^3) per minute Airflow through the appliance enters at the front and exits at the rear with no side ventilation.

Firepower 8000 Series Devices

The Firepower 8000 Series devices use network modules (NetMods) that contain either copper or fiber sensing interfaces. The devices can be shipped fully assembled or you can install the modules. Assemble your device before installing the Firepower System. See the assembly instructions shipped with your modules.

Some 8000 Series devices can be stacked to increase the capability of the system. For each stacking kit, you replace a NetMod with a stacking module and cable the devices together using the 8000 Series stacking cable. See Using Devices in a Stacked Configuration, page 4-13 for more information.

The Firepower 8000 Series device can be delivered on a variety of chassis:

- AMP8050 is a 1U chassis and can contain up to three modules.
- Firepower 8120, 8130, 8140, and AMP8150, also known as the 81xx Family, is a 1U chassis and can contain up to three modules. For the Firepower 8140 only, you can add a stacking kit for a total 2U configuration.
- Firepower 8250, part of the 82xx Family, is a 2U chassis and can contain up to seven modules. You can add up to three stacking kits for a total 8U configuration.
- Firepower 8260, part of the 82xx Family, is a 4U configuration with two 2U chassis. The primary chassis contains one stacking module and up to six sensing modules. The secondary chassis contains one stacking module. You can add up to two stacking kits for a total 8U configuration.
- Firepower 8270, part of the 82xx Family, is a 6U configuration with three 2U chassis. The primary chassis contains two stacking modules and up to five sensing modules. Each secondary chassis contains one stacking module. You can add one stacking kit for a total 8U configuration.
- Firepower 8290, part of the 82xx Family, is an 8U configuration with four 2U chassis. The primary chassis contains three stacking modules and up to four sensing modules. Each secondary chassis contains one stacking module. This model is fully configured and does not accept a stacking kit.
- Firepower 8350 and AMP8350, part of the 83xx Family, is a 2U chassis and can contain up to seven modules. You can add up to three stacking kits for a total 8U configuration.
- Firepower 8360 and AMP8360, part of the 83xx Family, is a 4U configuration with two 2U chassis. The primary chassis contains one stacking module and up to six sensing modules. The secondary chassis contains one stacking module. You can add up to two stacking kits for a total 8U configuration.

- Firepower 8370 and AMP8370, part of the 83xx Family, is a 6U configuration with three 2U chassis. The primary chassis contains two stacking modules and up to five sensing modules. Each secondary chassis contains one stacking module. You can add one stacking kit for a total 8U configuration.
- Firepower 8390 and AMP8390, part of the 83xx Family, is an 8U configuration with four 2U chassis. The primary chassis contains three stacking modules and up to four sensing modules. Each secondary chassis contains one stacking module. This model is fully configured and does not accept a stacking kit.

Note The AMP models have many of the same form factors as their Firepower counterparts, but have been optimized to take advantage of the Firepower System's network-based advanced malware protection (AMP) capabilities.

See the following sections for more information:

- Firepower 8000 Series Chassis Front View, page 7-22
- Firepower 8000 Series Chassis Rear View, page 7-26
- Firepower 8000 Series Physical and Environmental Parameters, page 7-29
- Firepower 8000 Series Modules, page 7-32

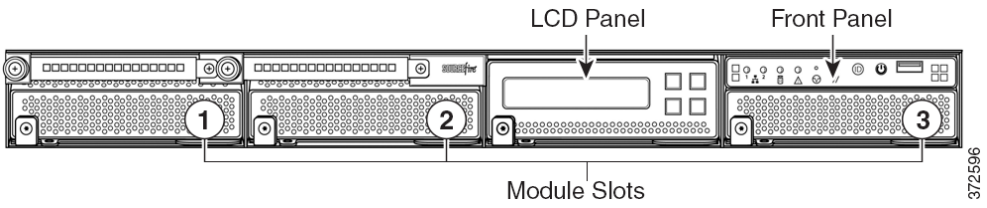
Firepower 8000 Series Chassis Front View

The Firepower 8000 Series chassis can be in the AMP8x50, 81xx Family, the 82xx Family, or the 83xx Family. See the *Regulatory Compliance and Safety Information for FirePOWER and FireSIGHT Appliances* document for safety considerations for AMP8x50, 81xx Family, 82xx Family, and 83xx Family appliances.

AMP8x50 and Firepower 81xx Family Chassis Front View

The front view of the chassis contains the LCD panel, front panel, and three module slots.

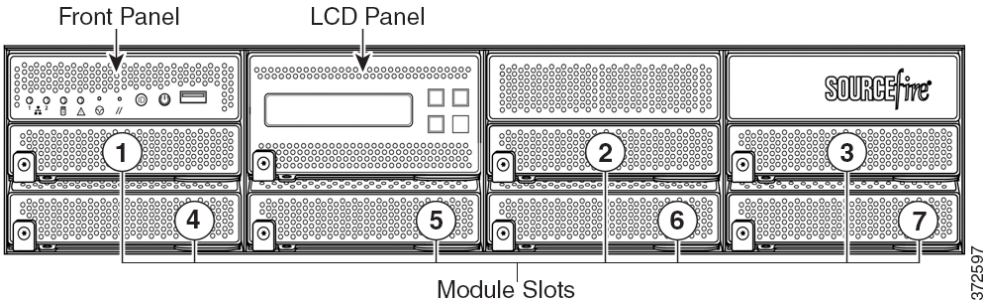
Figure 7-16 AMP8x50 and Firepower 81xx Family (Chassis: CHAS-1U-AC/DC) Front View



Firepower 82xx Family and Firepower and AMP 83xx Family Chassis Front View

The front view of the chassis contains the LCD panel, front panel, and seven module slots.

Figure 7-17 Firepower 82xx Family (Chassis: CHAS-2U-AC/DC) and Firepower and AMP 83xx Family (PG35-2U-AC/DC) Front View



The following table describes the features on the front of the appliance.

Table 7-34 Firepower 8000 Series System Components: Front View

Feature	Description
Module slots	Contain the modules. For information on available modules, see Firepower 8000 Series Modules, page 7-32.
LCD panel	Operates in multiple modes to configure the device, display error messages, and view system status. For more information, see Using the LCD Panel on a Firepower Device, page 6-1.
Front panel controls	Houses LEDs that display the system's operating state, as well as various controls, such as the power button. For more information, see Figure 7-19Firepower 82xx Family and Firepower and AMP 83xx Family Front Panel, page 7-24.
Front panel USB port	The USB 2.0 port allows you to attach a keyboard to the device.

See the following sections for more information:

- Firepower 8000 Series Front Panel, page 7-23
- Firepower 8000 Series Chassis Rear View, page 7-26

Firepower 8000 Series Front Panel

The front panel for the Firepower and AMP 81xx Family, 82xx Family, and 83xx Family contain the same components.

Figure 7-18 Firepower 81xx Family Front Panel

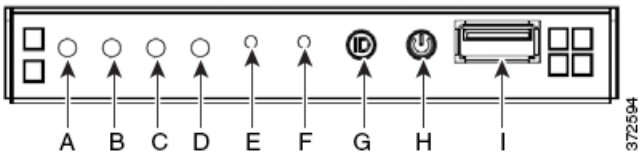


Figure 7-19 Firepower 82xx Family and Firepower and AMP 83xx Family Front Panel

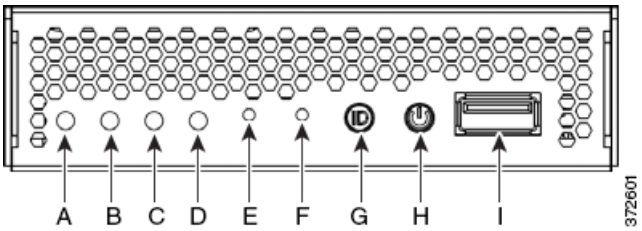


Table 7-35 Firepower 8000 Series Front Panel Components

A	NIC activity LED	F	Reset button
B	Reserved	G	ID button
C	Hard drive activity LED	H	Power button and LED
D	System status LED	I	USB 2.0 connector
E	Non-maskable interrupt button		

The front panel of the chassis houses LEDs, which display the system's operating state. The following table describes the LEDs on the front panel

Table 7-36 Firepower 8000 Series Front Panel LEDs

LED	Description
NIC activity	Indicates whether there is any network activity: • Green indicates there is network activity. • If the light is off, there is no network activity.
Hard drive activity	Indicates the hard drive status: • Blinking green indicates the fixed disk drive is active. • Amber indicates a fixed disk drive fault. • If the light is off, there is no drive activity or the system is powered off.
System status	Indicates the system status: • Green indicates the system is operating normally. • Blinking green indicates the system is operating in a degraded condition. • Blinking amber indicates the system is in a non-critical condition. • Amber indicates the system is in a critical or non-recoverable condition, or the system is starting up. • If the light is off, the system is starting up or off. **Note** The amber status light takes precedence over the green status light. When the amber light is on or blinking, the green light is off. See Table 7-37 on page 7-25 for more information.

Table 7-36 Firepower 8000 Series Front Panel LEDs (continued)

LED	Description
System ID	Helps identify a system installed in a high-density rack with other similar systems: • A blue light indicates the ID button is pressed and a blue light is on at the rear of the appliance. • No light indicates the ID button is not pressed.
Power button and LED	Indicates whether the system has power: • Green indicates that the system has power. • If the light is off, the system does not have power.

The following table describes the conditions under which the system status LEDs might be lit.

Table 7-37 Firepower 8000 Series System Status

Condition	Description
Critical	Any critical or non-recoverable threshold crossing associated with the following events: • temperature, voltage, or fan critical threshold crossing • power subsystem failure • system inability to power up due to incorrectly installed processors or processor incompatibility • critical event logging errors, including System Memory Uncorrectable ECC error and fatal/uncorrectable bus errors, such as PCI SERR and PERR
Non-critical	A non-critical condition is a threshold crossing associated with the following events: • temperature, voltage, or fan non-critical threshold crossing • chassis intrusion • Set Fault Indication command from system BIOS; the BIOS may use the command to indicate additional, non-critical status such as system memory or CPU configuration changes
Degraded	A degraded condition is associated with the following events: • one or more processors are disabled by Fault Resilient Boot (FRB) or BIOS • some system memory disabled or mapped out by BIOS • one of the power supplies unplugged or not functional **Tip** If you observe a degraded condition indication, check your power supply connections first. Power down the device, disconnect both power cords, reconnect the power cords to reseat them, and then restart the device. ⚠ **Caution** To power down safely, use the procedure in the Managing Devices chapter in the *Firepower Management Center Configuration Guide*, or the `system shutdown` command from the CLI.

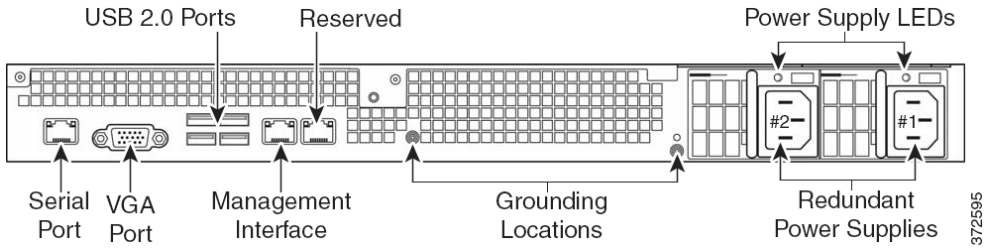
Firepower 8000 Series Chassis Rear View

The Firepower 8000 Series chassis can be in the 81xx Family, 82xx Family, or 83xx Family.

AMP8x50 and Firepower 81xx Family Chassis Rear View

The rear view of the chassis contains connection ports, the management interface, and the power supplies.

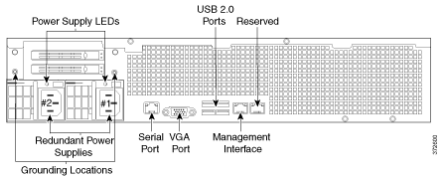
Figure 7-20 AMP8x50 and Firepower 81xx Family (Chassis: CHAS-1U-AC/DC) Rear View



Firepower 82xx Family Chassis Rear View

The rear view of the chassis contains power supplies, connection ports, and the management interface.

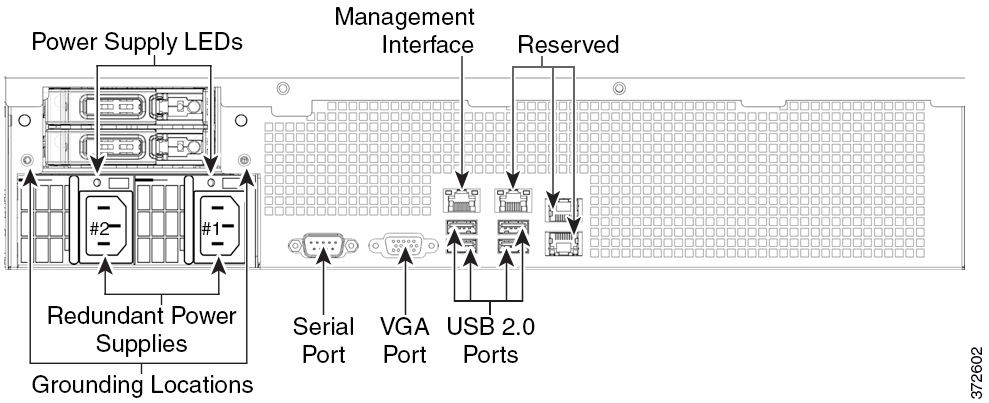
Figure 7-21 Firepower 82xx Family (Chassis: CHAS-2U-AC/DC) Rear View



Firepower and AMP 83xx Family Chassis Rear View

The rear view of the chassis contains power supplies, connection ports, and the management interface.

Figure 7-22 Firepower and AMP 83xx Family (Chassis: PG35-2U-AC/DC) Rear View



The following table describes the features that appear on the rear of the appliance.

Table 7-38 Firepower 8000 Series System Components: Rear View

Feature	Description
VGA port USB 2.0 ports	Allows you to attach a monitor, keyboard, and mouse to the device, as an alternative to using the serial port, to establish a direct workstation-to-appliance connection.
RJ45 serial port (81xx Family and 82xx Family)	Allows you to establish a direct workstation-to-appliance connection (using an RJ45 to DB-9 adapter) for direct access to all of the management services on the device. The RJ45 serial port is used for maintenance and configuration purposes **only** and is not intended to carry service traffic.
RS232 serial port (83xx Family)	Allows you to establish a direct workstation-to-appliance connection for direct access to all of the management services on the device. The RJ232 serial port is used for maintenance and configuration purposes **only** and is not intended to carry service traffic.
10/100/1000 Ethernet management interface	Provides for an out-of-band management network connection. The management interface is used for maintenance and configuration purposes **only** and is not intended to carry service traffic.
Redundant power supplies	Provides power to the device through an AC power source. Looking at the rear of the chassis, power supply #1 is on the right and power supply #2 is on the left.
Grounding locations	Allows you to connect the appliance to the Common Bonding Network. See the Power Requirements for Firepower Devices, page A-1 for more information.

The 10/100/1000 management interface is located on the rear of the appliance. The following table describes the LEDs associated with the management interface.

Table 7-39 Firepower 8000 Series Management Interface LEDs

LED	Description
Left (activity)	Indicates activity on the port: • A blinking light indicates activity. • No light indicates there is no activity.
Right (link)	Indicates whether the link is up: • A light indicates the link is up. • No light indicates there is no link.

The power supply modules are located on the rear of the appliance. The following table describes the LEDs associated with the management interface.

Table 7-40 Firepower 8000 Series Power Supply LEDs

LED	Description
Off	The power supply is not plugged in.
Amber	No power supplied to this module. or A power supply critical event such as module failure, a blown fuse, or a fan failure; the power supply shuts down.
Blinking amber	A power supply warning event, such as high temperature or a slow fan; the power supply continues to operate.
Blinking green	AC input is present; volts on standby, the power supply is switched off.
Green	The power supply is plugged in and on.

The following table lists the signals on a typical DB-9 serial connector and the corresponding pins on the device's RJ45 serial connectors. You can use this table to construct an adapter for serial connections.

Table 7-41 Firepower 8000 Series RJ45 to DB-9 Adapter Pin-Out

DB-9 Pin	Signal	Description	RJ45 Pin
1	DCD/DSR	Data carrier detect/data set ready	7
2	RD	Receive data	6
3	TD	Transmit data	3
4	DTR	Data terminal ready	2
5	GND	Ground	4 & 5
6		No connection	
7	RTS	Request to send	1
8	CTS	Clear to send	8
9		No connection	

Firepower 8000 Series Physical and Environmental Parameters

The following table describes the physical attributes and environmental parameters for AMP8x50 and 81xx Family devices.

Table 7-42 AMP8x50 and 81xx Family Physical and Environmental Parameters

Parameter	Description
Form factor	1U
Dimensions (D x W x H)	28.7 in. x 17.2 in. x 1.73 in. (72.8 cm x 43.3 cm x 4.4 cm)
Weight maximum installed	43.5 lbs (19.8 kg)
Copper 1000BASE-T configurable bypass NetMod	Quad-port Gigabit copper Ethernet configurable bypass interfaces in a paired configuration Cable and distance: Cat5E at 50 m
Fiber 10GBASE configurable bypass MMSR or SMLR NetMod	Dual-port fiber configurable bypass interfaces with LC connectors Cable and distance: LR is single-mode at 5000 m (available) SR is multimode fiber (850 nm) at 550 m (standard)
Fiber 1000BASE-SX configurable bypass NetMod	Quad-port fiber configurable bypass interfaces 1000BASE-SX with LC connectors Cable and distance: SX is multimode fiber (850 nm) at 550 m (standard)
Copper 1000BASE-T non-bypass NetMod	Quad-port Gigabit copper Ethernet non-bypass interfaces in a paired configuration Cable and distance: Cat5E at 50 m
Fiber 10GBASE non-bypass MMSR or SMLR NetMod	Quad-port fiber non-bypass interfaces with LC connectors Cable and distance: LR is single-mode at 5000 m (available) SR is multimode fiber (850 nm) at 550 m (standard)
Fiber 1000BASE-SX non-bypass NetMod	Quad-port fiber non-bypass interfaces 1000BASE-SX with LC connectors Cable and distance: SX is multimode fiber (850 nm) at 550 m (standard)
Power supply	Dual 650 W redundant power supplies designed for AC or DC. AC Voltage: 100 VAC to 240 VAC nominal (85 VAC to 264 VAC maximum) AC Current: 5.2A maximum over the full range, per supply 2.6A maximum for 187 VAC to 264 VAC, per supply AC Frequency range: 47 Hz to 63 Hz DC Voltage: -48 VDC nominal referenced to RTN -40 VDC to -72 VDC maximum DC Current: 11A maximum, per supply **Note** The power supplies are hot-swappable.
Operating temperature	50°F to 95°F (10°C to 35°C)
Non-operating temperature	-29°F to 158°F (-20°C to 70°C)
Operating humidity	5% to 85% non-condensing
Non-operating humidity	5% to 90%, non-condensing with a maximum wet bulb of 82ºF (28ºC) at temperatures from 77°F to 95°F (25°C to 35°C)
Altitude	0ft (sea level) to 6000 ft (0 to 1800 m)

Table 7-42 AMP8x50 and 81xx Family Physical and Environmental Parameters (continued)

Parameter	Description
Cooling requirements	1725 BTU/hour You must provide sufficient cooling to maintain the appliance within its required operating temperature range. Failure to do this may cause a malfunction or damage to the appliance.
Acoustic noise	Max normal operating noise is 87.6 dB LWAd (high temperature). Typical normal operating noise is 80 dB LWAd.
Operating shock	No errors with half a sine wave shock of 2G (with 11 ms duration)
Airflow	160 ft^3 (4.5 m^3) per minute Restriction of the airflow such as blocking the front or back or enclosing the unit in a cabinet without sufficient clearance may cause the unit to overheat, even if the ambient temperature is in the operating range. Airflow through the appliance enters at the front and exits at the rear. The minimum recommended clearance in the front and back is 7.9 in. (20 cm). This minimum can only be used if you can ensure a supply of low temperature air at the front of the appliance.

The following table describes the physical attributes and environmental parameters for Firepower 82xx Family and the Firepower and AMP 83xx Family devices.

Table 7-43 Firepower 82xx Family and Firepower and AMP 83xx Family Physical and Environmental Parameters

Parameter	Description	
Form factor	2U	
Dimensions (D x W x H)	29.0 in. x 17.2 in. x 3.48 in. (73.5 cm x 43.3 cm x 88.2 cm)	
Weight maximum installed	82xx Family:	58 lbs (25.3 kg)
	83xx Family:	67 lbs (30.5 kg)
Copper 1000BASE-T configurable bypass NetMod	Quad-port Gigabit copper Ethernet configurable bypass interfaces in a paired configuration Cable and distance: Cat5E at 50 m	
Fiber 10GBASE MMSR or SMLR configurable bypass NetMod	Dual-port fiber configurable bypass interfaces with LC connectors Cable and distance: LR is single-mode at 5000 m (available) SR is multimode fiber (850 nm) at 550 m (standard)	
Fiber 1000BASE-SX configurable bypass NetMod	Quad-port fiber configurable bypass interfaces1000BASE-SX with LC connectors Cable and distance: SX is multimode fiber (850 nm) at 550 m (standard)	
Fiber 40GBASE-SR4 configurable bypass NetMod	Dual-port fiber configurable bypass interfaces with OTP/MTP connectors Cable and distance: OM3: 100 m at 850 nm Multimode OM4: 150 m at 850 nm Multimode	
Copper 1000BASE-T non-bypass NetMod	Quad-port Gigabit copper Ethernet non-bypass interfaces in a paired configuration Cable and distance: Cat5E at 50 m	

Table 7-43 Firepower 82xx Family and Firepower and AMP 83xx Family Physical and Environmental Parameters

Parameter	Description	
Fiber 10GBASE non-bypass MMSR or SMLR NetMod	Quad-port fiber non-bypass interfaces with LC connectors Cable and distance: LR is single-mode at 5000 m (available) SR is multimode fiber (850 nm) at 550 m (standard)	
Fiber 1000BASE-SX non-bypass NetMod	Quad-port fiber non-bypass interfaces 1000BASE-SX with LC connectors Cable and distance: SX is multimode fiber (850 nm) at 550 m (standard)	
Power supply	82xx Family:	Dual 750 W redundant power supplies designed for AC or DC. AC Voltage: 100 VAC to 240 VAC nominal (85 VAC to 264 VAC maximum) AC Current: 8A maximum over the full range, per supply 4A maximum for 187 VAC to 264 VAC, per supply AC Frequency range: 47 Hz to 63 Hz DC Voltage: -48 VDC nominal referenced to RTN -40 VDC to -72 VDC maximum DC Current: 18A maximum, per supply **Note** The power supplies are hot-swappable.
	83xx Family:	Dual 1000 W redundant power supplies designed for AC or DC. AC Voltage: 100 VAC to 240 VAC nominal (85 VAC to 264 VAC maximum) AC Current: 11A maximum over the full range, per supply 5.5A maximum for 187 VAC to 264 VAC, per supply AC Frequency range: 47 Hz to 63 Hz DC Voltage: -48 VDC nominal referenced to RTN -40 VDC to -72 VDC maximum DC Current: 25A maximum, per supply **Note** The power supplies are hot-swappable.
Operating temperature	82xx Family:	50°F to 95°F (10°C to 35°C)
	83xx Family:	41°F to 104°F (5°C to 40°C)
Non-operating temperature	-29°F to 158°F (-20°C to 70°C)	
Operating humidity	5% to 85% non-condensing	
Non-operating humidity	5% to 90%, non-condensing with a maximum wet bulb of 82°F (28°C) at temperatures from 77°F to 95°F (25°C to 35°C)	
Altitude	0 ft (sea level) to 6000 ft (0 to 1800 m)	

Table 7-43 Firepower 82xx Family and Firepower and AMP 83xx Family Physical and Environmental Parameters

Parameter	Description
Cooling requirements	up to 2900 BTU/hour You must provide sufficient cooling to maintain the appliance within its required operating temperature range. Failure to do this may cause a malfunction or damage to the appliance.
Acoustic noise	Max normal operating noise is 81.6 dB LWAd (high temperature). Typical normal operating noise is 81.4 dB LWAd.
Operating shock	No errors with half a sine wave shock of 2G (with 11 ms duration)
Airflow	Front to back, 210 ft^3 (6 m^3) per minute Restriction of the airflow such as blocking the front or back or enclosing the unit in a cabinet without sufficient clearance may cause the unit to overheat, even if the ambient temperature is in the operating range. Airflow through the appliance enters at the front and exits at the rear. The minimum recommended clearance in the front and back is 7.9 in. (20cm). This minimum can only be used if you can ensure a supply of low temperature air at the front of the appliance.

Firepower 8000 Series Modules

The sensing interfaces for the Firepower 8000 Series appliances can be delivered with copper or fiber interfaces.

Caution Modules are **not** hot-swappable. See Inserting and Removing Firepower 8000 Series Modules, page C-1 for more information.

The following modules contain configurable bypass sensing interfaces:

- a quad-port 1000BASE-T copper interface with configurable bypass capability. See Quad-Port 1000BASE-T Copper Configurable Bypass NetMod, page 7-33.
- a quad-port 1000BASE-SX fiber interface with configurable bypass capability. See Quad-Port 1000BASE-SX Fiber Configurable Bypass NetMod, page 7-33 for more information.
- a dual-port 10GBASE (MMSR or SMLR) fiber interface with configurable bypass capability. See Dual-Port 10GBASE (MMSR or SMLR) Fiber Configurable Bypass NetMod, page 7-35 for more information.
- a dual-port 40GBASE-SR4 fiber interface with configurable bypass capability (2U devices only). See Dual-Port 40GBASE-SR4 Fiber Configurable Bypass NetMod, page 7-36 for more information.

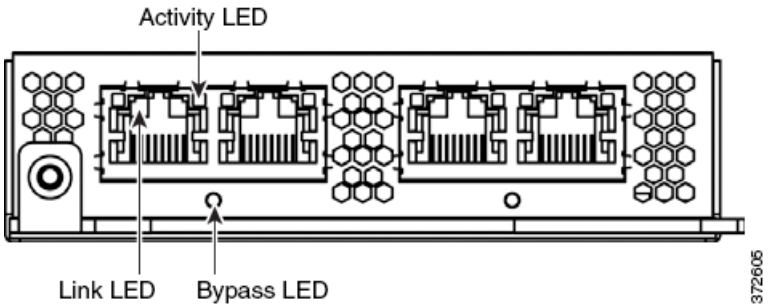
The following modules contain non-bypass sensing interfaces:

- a quad-port 1000BASE-T copper interface without bypass capability. See Quad-Port 1000BASE-T Copper Non-Bypass NetMod, page 7-38 for more information.
- a quad-port 1000BASE-SX fiber interface without bypass capability. See Quad-Port 1000BASE-SX Fiber Non-Bypass NetMod, page 7-39 for more information.
- a quad-port 10GBASE (MMSR or SMLR) fiber interface without bypass capability. See Quad-Port 10GBASE (MMSR or SMLR) Fiber Non-Bypass NetMod, page 7-39 for more information.

In addition, you can use a stacking module to connect two Firepower 8140, up to four Firepower 8250, or up to four Firepower or AMP 8350 devices to combine their processing power and increase throughput. See Stacking Module, page 7-41 for more information.

Quad-Port 1000BASE-T Copper Configurable Bypass NetMod

The quad-port 1000BASE-T copper configurable bypass NetMod contains four copper ports and link, activity, and bypass LEDs.



Use the following table to understand the link and activity LEDs on copper interfaces.

Table 7-44 Copper Link/Activity LEDs

Status	Description
Both LEDs off	The interface does not have link and is not in bypass mode.
Link amber	The speed of the traffic on the interface is 10Mb or 100Mb.
Link green	The speed of the traffic on the interface is 1Gb.
Activity blinking green	The interface has link and is passing traffic.

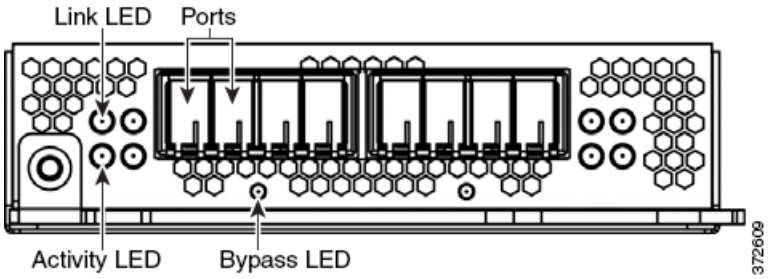
Use the following table to understand the bypass LEDs on copper interfaces.

Table 7-45 Copper Bypass LEDs

Status	Description
Off	The interface does not have link and is not in bypass mode.
Steady green	The interface has link and is passing traffic.
Steady amber	The interface has been intentionally brought down.
Blinking amber	The interface is in bypass mode; that is, it has failed open.

Quad-Port 1000BASE-SX Fiber Configurable Bypass NetMod

The quad-port 1000BASE-SX fiber configurable bypass NetMod contains four fiber ports and link, activity, and bypass LEDs.



Use the following table to understand link and activity LEDs of the fiber interfaces.

Table 7-46 Fiber Link/Activity LEDs

Status	Description
Top	For an inline or passive interface: • A blinking light indicates the interface has activity. • No light indicates there is no activity.
Bottom	For an inline interface: • A light indicates the interface has activity. • No light indicates there is no activity. For a passive interface, the light is always on.

Use the following table to understand bypass LEDs on the fiber interfaces.

Table 7-47 Fiber Bypass LEDs

Status	Description
Off	The interface does not have link and is not in bypass mode.
Steady green	The interface has link and is passing traffic.
Steady amber	The interface has been intentionally brought down.
Blinking amber	The interface is in bypass mode; that is, it has failed open.

Use the following table to understand the optical specifications of the fiber interfaces.

Table 7-48 1000BASE-SX NetMod Optical Parameters

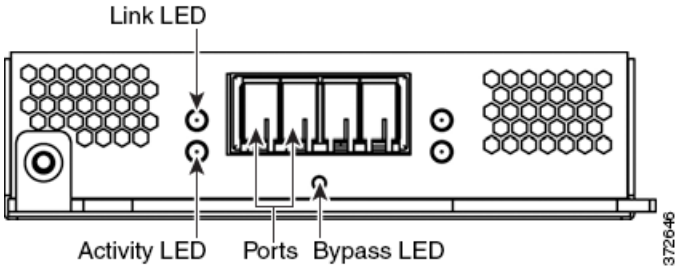
Parameter	1000BASE-SX
Optical connectors	LC duplex
Bit rate	1000Mbps
Baud rate/encoding/tolerance	1250Mbps 8b/10b encoding
Optical interface	Multimode
Operating distances	656 ft (200 m) for 62.5 µm/125 µm fiber 1640 ft (500 m) for 50 µm/125 µm fiber
Transmitter wavelength	770-860 nm (850 nm typical)

Table 7-48 1000BASE-SX NetMod Optical Parameters (continued)

Parameter	1000BASE-SX
Maximum average launch power	0 dBm
Minimum average launch power	-9.5 dBm
Maximum average power at receiver	0 dBm
Receiver sensitivity	-17 dBm

Dual-Port 10GBASE (MMSR or SMLR) Fiber Configurable Bypass NetMod

The dual-port 10GBASE (MMSR or SMLR) fiber configurable bypass NetMod contains two fiber ports and link, activity, and bypass LEDs.



Use the following table to understand link and activity LEDs of the fiber interfaces.

Table 7-49 Fiber Link/Activity LEDs

Status	Description
Top	For an inline or passive interface: • A blinking light indicates the interface has activity. • No light indicates there is no activity.
Bottom	For an inline interface: • A light indicates the interface has activity. • No light indicates there is no activity. For a passive interface, the light is always on.

Use the following tables to understand the bypass LEDs on the fiber interfaces.

Table 7-50 Fiber Bypass LEDs

Status	Description
Off	The interface does not have link and is not in bypass mode.
Steady green	The interface has link and is passing traffic.
Steady amber	The interface has been intentionally brought down.
Blinking amber	The interface is in bypass mode; that is, it has failed open.

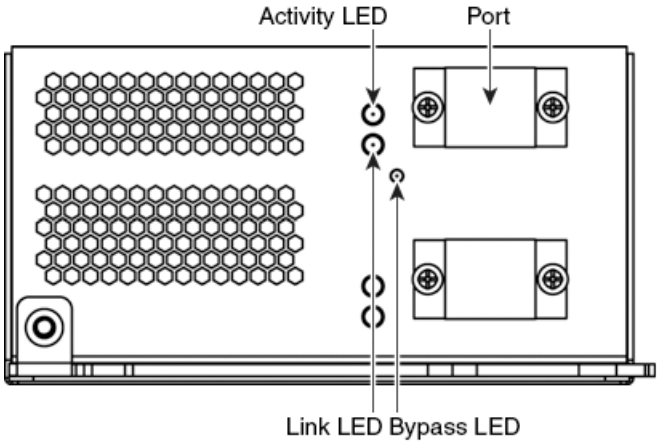
Use the following table to understand the optical parameters of the fiber interfaces.

Table 7-51 10GBASE MMSR and SMLR NetMod Optical Parameters

Parameter	10GBASE MMSR	10GBASE SMLR
Optical connectors	LC duplex	LC duplex
Bit rate	10.000Gbps	10.000Gbps
Baud rate/encoding/tolerance	10.3125Gbps 64/66b encoding +/- 100 ppm	10.3125Gbps 64/166b encoding +/- 100 ppm
Optical interface	Multimode	Single mode only
Operating distance	840-860 nm (850 nm typical) 85 ft (26 m) to 108 ft (33 m) for 62.5 µm/125 µm fiber (modal BW 160 to 200 respectively) 216 ft (66 m) to 269 ft (82 m) for 50 µm/125 µm fiber (modal BW 400 to 500 respectively) Distances to 980 ft (300 m) are available with higher quality (OM3) fiber. Minimum distances (all): 6ft (2 m)	1270-1355 nm (1310 nm typical) 6 ft to 6.2 miles (2 m to 10 km) for 9 µm/125 µm fiber
Transmitter wavelength	840-860 nm (850 nm typical)	1270-1355 nm (1310 nm typical)
Maximum average launch power	-1 dBm	-0.5 dBm
Minimum average launch power	-7.3 dBm	-8.2 dBm
Maximum average power at receiver	-1 dBm	-0.5 dBm
Receiver sensitivity	-9.9 dBm	-14.4 dBm

Dual-Port 40GBASE-SR4 Fiber Configurable Bypass NetMod

The dual-port 40GBASE-SR4 fiber configurable bypass NetMod contains two fiber ports and link, activity, and bypass LEDs.



You can use the 40G NetMod in the following 8000 Series models:

- Firepower 8270 and 8290
- Firepower and AMP 8360, 8370 and 8390
- Firepower 8250 and 8260 (must be 40G-capable)
- Firepower and AMP 8350 (must be 40G-capable)

Caution If you attempt to create a 40G interface on a device that is not 40G-capable, the 40G interface screen on its managing Firepower Management Center web interface displays red. A 40G-capable 8250 displays "8250-40G" on the LCD Panel and a 40G-capable 8350 displays "8350-40G" on the LCD Panel. See Firepower 8000 Series Modules, page 4-8 for placement information.

Use the following table to understand link and activity LEDs of the fiber interfaces.

Table 7-52 Fiber Link/Activity LEDs

Status	Description
Top (activity)	The light flashes when the interface has activity. If dark, there is no activity.
Bottom (link)	The light is on when the interface has link. If dark, there is no link.

Use the following table to understand bypass LED of the fiber interfaces.

Table 7-53 Fiber Bypass LED

Status	Description
Off	The interface pair does not have link and is not in bypass mode, or has no power.
Steady green	The interface pair has link and is passing traffic.
Steady amber	The interface has been intentionally brought down.
Blinking amber	The interface is in bypass mode; that is, it has failed open.

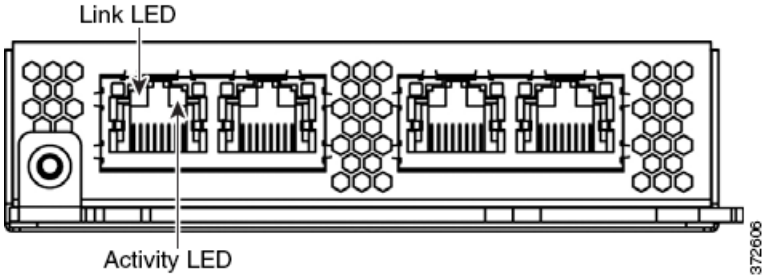
Use the following table to understand optical parameters of the fiber interfaces.

Table 7-54 40GBASE-SR4 NetMod Optical Parameters

Parameter	40GBASE-SR4
Optical connectors	OTP/MTP single row twelve fiber positions. Only the outer eight fibers are used.
Bit rate	40.000Gbps
Baud rate/encoding/tolerance	10.3125Gbps 64/66b encoding +/- 100 ppm
Optical interface	Multimode
Operating distances	320 ft (100 m) for 50 µm/125 µm fiber (OM3) Minimum distance: 2 ft (0.5 m) 40G optics are carried on eight fiber cables utilizing MPO connectors.
Transmitter wavelength	840-860 nm (850 nm typical)
Maximum average launch power	2.4 dBm
Minimum average launch power	-7.8 dBm
Maximum average power at receiver	2.4 dBm
Receiver sensitivity	-9.5 dBm

Quad-Port 1000BASE-T Copper Non-Bypass NetMod

The quad-port 1000BASE-T copper non-bypass NetMod contains four copper ports, and link and activity LEDs.



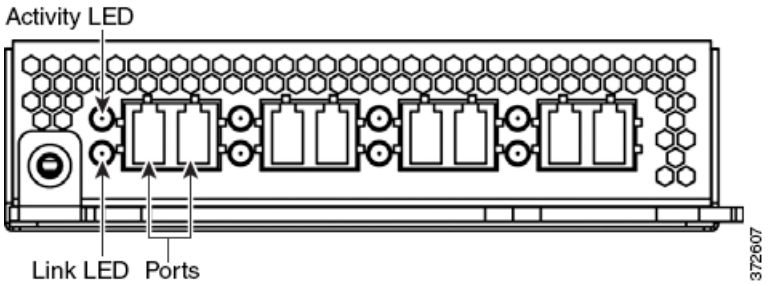
Use the following table to understand copper LEDs.

Table 7-55 Non-Bypass Copper Link/Activity LEDs

Status	Description
Both LEDs Off	The interface does not have link.
Link Amber	The speed of the traffic on the interface is 10Mb or 100Mb.
Link Green	The speed of the traffic on the interface is 1Gb.
Activity Blinking Green	The interface has link and is passing traffic.

Quad-Port 1000BASE-SX Fiber Non-Bypass NetMod

The quad-port 1000BASE-SX fiber non-bypass NetMod contains four fiber ports, and link and activity LEDs.



Use the following table to understand the link and activity LEDs on the fiber interfaces.

Table 7-56 Non-Bypass Fiber Link/Activity LEDs

Status	Description
Top (Activity)	For an inline or passive interface: the light flashes when the interface has activity. If dark, there is no activity.
Bottom (Link)	For an inline interface: the light is on when the interface has link. If dark, there is no link. For a passive interface: the light is always on.

Use the following table to understand the optical parameters of the fiber interfaces.

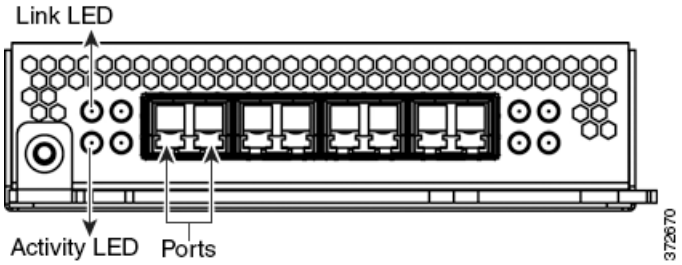
Table 7-57 1000BASE-SX NetMod Optical Parameters

Parameter	1000BASE-SX
Optical connectors	LC duplex
Bit rate	1000Mbps
Baud rate/encoding/tolerance	1250Mbps 8b/10b encoding
Optical interface	Multimode
Operating distances	656 ft (200 m) for 62.5 µm/125 µm fiber 1640 ft (500 m) for 50 µm/125 µm fiber
Transmitter wavelength	770-860 nm (850 nm typical)
Maximum average launch power	0 dBm
Minimum average launch power	-9.5 dBm
Maximum average power at receiver	0 dBm
Receiver sensitivity	-17 dBm

Quad-Port 10GBASE (MMSR or SMLR) Fiber Non-Bypass NetMod

The quad-port 10GBASE (MMSR or SMLR) fiber non-bypass NetMod contains four fiber ports, and link and activity LEDs.

Caution The quad-port 10GBASE non-bypass NetMod contains non-removable SFPs. Any attempt to remove the SFP may damage the module.



Use the following table to understand the link and activity LEDs on fiber interfaces.

Table 7-58 Fiber Link/Activity LEDs

Status	Description
Top	For an inline or passive interface: the light flashes when the interface has activity. If dark, there is no activity.
Bottom	For an inline interface: the light is on when the interface has link. If dark, there is no link. For a passive interface: the light is always on.

Use the following table to understand the optical parameters of the fiber interfaces.

Table 7-59 10GBASE MMSR and SMLR NetMod Optical Parameters

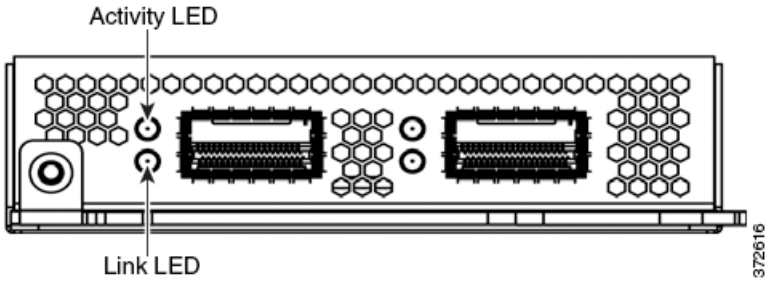
Parameter	10GBASE MMSR	10GBASE SMLR
Optical connectors	LC duplex	LC duplex
Bit rate	10.000Gbps	10.000Gbps
Baud rate/ encoding/tolerance	10.3125Gbps 64/66b encoding +/- 100 ppm	10.3125Gbps 64/66b encoding +/- 100 ppm
Optical interface	Multimode	Single mode only
Operating distance	840-860 nm (850 nm typical) 85 ft (26 m) to 108 ft (33 m) for 62.5 µm/125 µm fiber (modal BW 160 to 200 respectively) 216 ft (66 m) to 269 ft (82 m) for 50 µm/125 µm fiber (modal BW 400 to 500 respectively) Distances to 980 ft (300 m) are available with higher quality (OM3) fiber. Minimum distances (all): 6ft (2 m)	1270-1355 nm (1310 nm typical) 6 ft to 6.2 miles (2 m to 10 km) for 9 µm/125 µm fiber

Table 7-59 10GBASE MMSR and SMLR NetMod Optical Parameters (continued)

Parameter	10GBASE MMSR	10GBASE SMLR
Transmitter wavelength	840-860 nm (850 nm typical)	1270-1355 nm (1310 nm typical)
Maximum average launch power	-1 dBm	-0.5 dBm
Minimum average launch power	-7.3 dBm	-8.2 dBm
Maximum average power at receiver	-1 dBm	-0.5 dBm
Receiver sensitivity	-9.9 dBm	-14.4 dBm

Stacking Module

The stacking module contains two connection ports for the 8000 Series stacking cable, and activity and link LEDs.



You can use the stacking module optionally in the following 8000 Series models:

- Firepower 8140 and 8250
- Firepower and AMP 8350

The stacking module is included in the following 8000 Series stacked configurations:

- Firepower 8260, 8270, and 8290
- Firepower and AMP 8360, 8370, and 8390

You can use the following table to understand the stacking LEDs.

Table 7-60 Stacking LEDs

Status	Description
Top	Indicates activity on the interface: • A blinking light indicates there is activity on the interface. • No light indicates there is no activity.
Bottom	Indicates whether the interface has link: • A light indicates the interface has link. • No light indicates there is no link.

Restoring a Firepower System Appliance to Factory Defaults

Cisco provides ISO images on its Support Site for restoring, or reimaging, Firepower managed devices to their original factory settings.

For more information, see the following sections:

Before You Begin

Before you begin restoring your appliances to factory defaults, you should familiarize yourself with the expected behavior of the system during the restore process.

Configuration and Event Backup Guidelines

Before you begin the restore process, Cisco recommends that you delete or move any backup files that reside on your appliance, then back up current event and configuration data to an external location.

Restoring your appliance to factory defaults results in the loss of almost **all** configuration and event data on the appliance. Although the restore utility can retain the appliance's license, network, console, and Lights-Out Management (LOM) settings, you must perform all other setup tasks after the restore process completes.

Traffic Flow During the Restore Process

To avoid disruptions in traffic flow on your network, Cisco recommends restoring your appliances during a maintenance window or at a time when the interruption will have the least impact on your deployment.

Restoring a Firepower device that is deployed inline resets the device to a non-bypass (fail closed) configuration, disrupting traffic on your network. Traffic is blocked until you configure bypass-enabled inline sets on the device. For more information about editing your device configuration to configure bypass, see the Managing Devices chapter of the *Firepower Management Center Configuration Guide*.

Understanding the Restore Process

Access: Admin

To restore a Firepower device, you boot from the appliance's internal flash drive and use an interactive menu to download and install the ISO image on the appliance. For your convenience, you can install system software and intrusion rule updates as part of the restore process.

Only reimage your appliances during a maintenance window. Reimaging resets appliances in bypass mode to a non-bypass configuration and disrupts traffic on your network until you reconfigure bypass mode. For more information, see Traffic Flow During the Restore Process, page 8-1.

Note that you **cannot** restore an appliance using its web interface. To restore an appliance, you must connect to it in one of the following ways:

Keyboard and Monitor/KVM

You can connect a USB keyboard and VGA monitor to the appliance, which is useful for rack-mounted appliances connected to a KVM (keyboard, video, and mouse) switch. If you have a KVM that is remote-accessible, you can restore appliances without having physical access.

Serial Connection/Laptop

You can use a rollover serial cable (also known as a NULL modem cable or a Cisco console cable) to connect a computer to the appliance. See the hardware specifications for your appliance to locate the serial port. To interact with the appliance, use terminal emulation software such as HyperTerminal or XModem. For more information, including a table of serial port connectors by appliance, see Serial Connection/Laptop, page 4-20.

Lights-Out Management Using Serial over LAN

You can perform a limited set of actions on Management Centers and Firepower devices using Lights-Out Management (LOM) with a Serial over LAN (SOL) connection. If you do not have physical access to an appliance, you can use LOM to perform the restore process. After you connect to an appliance using LOM, you issue commands to the restore utility as if you were using a physical serial connection. Note that you can use Lights-Out Management on the default (`eth0`) management interface only. For more information, see Setting Up Lights-Out Management, page 8-15.

Before You Begin

- Obtain the restore ISO image for the appliance from the Support Site. See To obtain the restore ISO and other update files:, page 8-3

To restore a Firepower device:

Step 1 Copy the image to an appropriate storage medium.

Step 2 Connect to the appliance.

Step 3 Reboot the appliance and invoke the restore utility.

What to Do Next

- Install the ISO image using the procedure in To restore a Firepower device:, page 8-2.

Obtaining the Restore ISO and Update Files

Access: Any

Cisco provides ISO images for restoring appliances to their original factory settings. Before you restore an appliance, obtain the correct ISO image from the Support Site.

The ISO image you should use to restore an appliance depends on when Cisco introduced support for that appliance model. Unless the ISO image was released with a minor version to accommodate a new appliance model, ISO images are usually associated with major versions of the system software (for example, 5.2 or 5.3). To avoid installing an incompatible version of the system, Cisco recommends that you always use the most recent ISO image available for your appliance.

Firepower devices use an internal flash drive to boot the appliance so you can run the restore utility.

Cisco also recommends that you always run the latest version of the system software supported by your appliance. After you restore an appliance to the latest supported major version, you should update its system software, intrusion rules, and Vulnerability Database (VDB). For more information, see the release notes for the update you want to apply, as well as the *Firepower Management Center Configuration Guide*.

For your convenience, you can install system software and intrusion rule updates as part of the restore process. For example, you could restore a device to Version 6.0, and also update the device to Version 6.0.0.1 as part of that process. Keep in mind that only Management Centers require rule updates.

To obtain the restore ISO and other update files:

Step 1 Using the user name and password for your support account, log into the Support Site (https://sso.cisco.com/autho/forms/CDClogin.html).

Step 2 Browse to the software download section (https://software.cisco.com/download/navigator.html).

Step 3 Enter a search string in the **Find** area on the page that appears for the system software you want to download and install.

For example, to find software downloads for Firepower, you would enter **Firepower.**

Step 4 Find the image (ISO image) that you want to download.

You can click one of the links on the left side of the page to view the appropriate section of the page. For example, you would click **5.4.1 Images** to view the images and release notes for Version 5.4.1 of the Firepower System.

Step 5 Click the ISO image you want to download.

The file begins downloading.

Step 6 Copy the files to an HTTP (web) server, FTP server, or SCP-enabled host that the appliance can access on its management network.

If using FTP, the user name and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept the FTP write request from the user. Refer to the documentation for your FTP server for more information.

Caution Do **not** transfer ISO or update files via email; the files can become corrupted. Also, do **not** change the names of the files; the restore utility requires that they be named as they are on the Support Site.

Beginning the Restore Process

Begin the restore process by booting the appliance from an internal flash drive.

After you make sure that you have the appropriate level of access and connection to an appliance, as well the correct ISO image, use one of the following procedures to restore your appliance:

- Starting the Restore Utility Using KVM or Physical Serial Port, page 8-4 explains how to start the restore process for an appliance where you do not have LOM access.
- Starting the Restore Utility Using Lights-Out Management, page 8-5 explains how use LOM to start the restore process via an SOL connection.

Caution The procedures in this chapter explain how to restore an appliance without powering it down. However, if you need to power down for any reason, use the appliance's web interface, the `system shutdown` command from the CLI on a Firepower device, or the `shutdown -h now` command from an appliance's shell (sometimes called expert mode).

Starting the Restore Utility Using KVM or Physical Serial Port

Access: Admin

For Firepower devices, Cisco provides a restore utility on an internal flash drive.

Note Do **not** use a KVM console with USB mass storage to access the appliance for the initial setup because the appliance may attempt to use the mass storage device as a boot device.

If you need to restore an appliance to factory defaults and do not have physical access, you can use LOM to perform the restore process; see Starting the Restore Utility Using Lights-Out Management, page 8-5.

To start the restore utility:

Step 1 Using your keyboard/monitor or serial connection, log into the appliance using an account with Administrator privileges. The password is the same as the password for the appliance's web interface.

Step 2 Reboot the appliance:

- On a Firepower device, type `system reboot`.

The appliance reboots.

Step 3 Monitor the reboot status:

- If the system is performing a database check, you may see the following message: `The system is not operational yet. Checking and repairing database are in progress. This may take a long time to finish.`
- For a keyboard and monitor connection, quickly press one of the arrow keys to prevent the appliance from booting the currently installed version of the system.
- For a serial connection, when you see the BIOS boot options, press Tab slowly and repeatedly (to prevent the appliance from booting the currently installed version of the system). The LILO boot prompt appears. For example:

```
LILO 22.8 boot:
System-5.4 System_Restore
```

Step 4 Indicate that you want to restore the system:

- For a keyboard and monitor connection, use the arrow keys to select `System_Restore` and press Enter.
- For a serial connection, type `System_Restore` at the prompt and press Enter.

The `boot` prompt appears after the following choices:

```
0. Load with standard console
1. Load with serial console
```

Step 5 Select a display mode for the restore utility's interactive menu:

- For a keyboard and monitor connection, type `0` and press Enter.
- For a serial connection, type `1` and press Enter.

If you do not select a display mode, the restore utility defaults to the standard console after 30 seconds.

Unless this is the first time you have restored the appliance to this major version, the utility automatically loads the last restore configuration you used. To continue, confirm the settings in a series of pages.

Step 6 Press Enter to confirm the copyright notice.

What to Do Next

- Continue with Using the Interactive Menu to Restore an Appliance, page 8-6.

Starting the Restore Utility Using Lights-Out Management

Access: Admin

If you need to restore an appliance to factory defaults and do not have physical access to the appliance, you can use LOM to perform the restore process. Note that if you want to use LOM to configure the initial setup, you **must** preserve the network settings during the initial setup. Note also that you can use Lights-Out Management on the default (`eth0`) management interface only.

Note Before you can restore an appliance using LOM, you must enable the feature; see Setting Up Lights-Out Management, page 8-15.

To start the restore utility using Lights-Out Management:

Step 1 At your computer's command prompt, enter the IPMI command to start the SOL session:

- For IPMItool, type:

  ```
  sudo ipmitool -I lanplus -H IP_address -U username sol activate
  ```

- For ipmiutil, type:

  ```
  sudo ipmiutil sol -a -V4 -J3 -N IP_address -U username -P password
  ```

Where *IP_address* is the IP address of the management interface on the appliance, *username* is user name of an authorized LOM account, and *password* is the password for that account. Note that IPMItool prompts you for the password after you issue the `sol activate` command.

If you are using a Firepower device, type `expert` to display the shell prompt.

Step 2 Reboot the appliance as root user:

- For a Firepower device, type `system reboot`.

The appliance reboots.

Step 3 Monitor the reboot status.

If the system is performing a database check, you may see the following message: `The system is not operational yet. Checking and repairing database are in progress. This may take a long time to finish.`

When you see the BIOS boot options, press Tab slowly and repeatedly (to prevent the appliance from booting the currently installed version of the system) until the LILO boot prompt appears. For example:

```
LILO 22.8 boot:
System-5.4 System_Restore
```

Step 4 At the `boot` prompt, start the restore utility by typing `System_Restore`.

The `boot` prompt appears after the following choices:

```
0. Load with standard console
1. Load with serial console
```

Step 5 Type `1` and press Enter to load the interactive restore menu via the appliance's serial connection.

Note If you do not select a display mode, the restore utility defaults to the standard console after 30 seconds.

Unless this is the first time you have restored the appliance to this major version, the utility automatically loads the last restore configuration you used. To continue, confirm the settings in a series of pages.

Step 6 Press Enter to confirm the copyright notice.

What to Do Next

- Continue with Using the Interactive Menu to Restore an Appliance, page 8-6.

Using the Interactive Menu to Restore an Appliance

The restore utility for Firepower devices uses an interactive menu to guide you through the restoration.

Note Only reimage your appliances during a maintenance window. Reimaging resets appliances in bypass mode to a non-bypass configuration and disrupts traffic on your network until you reconfigure bypass mode. For more information, see Traffic Flow During the Restore Process, page 8-1.

The menu displays the options listed in the following table.

Table 8-1 Restore Menu Options

Option	Description	For more information, see...
1 IP Configuration	Specify network information about the management interface on the appliance you want to restore, so that the appliance can communicate with the server where you placed the ISO and any update files.	Identifying the Appliance's Management Interface, page 8-8
2 Choose the transport protocol	Specify the location of the ISO image you will use to restore the appliance, as well as any credentials the appliance needs to download the file.	Specifying ISO Image Location and Transport Method, page 8-9
3 Select Patches/Rule Updates	Specify a system software and intrusion rules update to be applied after the appliance is restored to the base version in the ISO image.	Updating System Software and Intrusion Rules During Restore, page 8-10
4 Download and Mount ISO	Download the appropriate ISO image and any system software or intrusion rule updates. Mount the ISO image.	Downloading the ISO and Update Files and Mounting the Image, page 8-11
5 Run the Install	Invoke the restore process.	Invoking the Restore Process, page 8-11
6 Save Configuration 7 Load Configuration	Save any set of restore configurations for later use, or load a saved set.	Saving and Loading Restore Configurations, page 8-13
8 Wipe Contents of Disk	Securely scrub the hard drive to ensure that its contents can no longer be accessed.	Scrubbing the Hard Drive, page D-1

Navigate the menu using your arrow keys. To select a menu option, use the up and down arrows. Use the right and left arrow keys to toggle between the **OK** and **Cancel** buttons at the bottom of the page.

The menu presents two different kinds of options:

- To select a numbered option, first highlight the correct option using the up and down arrows, then press Enter while the **OK** button at the bottom of the page is highlighted.
- To select a multiple-choice (radio button) option, first highlight the correct option using the up and down keys, then press the space bar to mark that option with an x. To accept your selection, press Enter while the **OK** button is highlighted.

In most cases, complete menu options **1**, **2**, **4**, and **5**, in order. Optionally, add menu option **3** to install system software and intrusion rule updates during the restore process.

If you are restoring an appliance to a different major version from the version currently installed on the appliance, a two-pass restore process is required. The first pass updates the operating system, and the second pass installs the new version of the system software.

If this is your second pass, or if the restore utility automatically loaded the restore configuration you want to use, you can start with menu option **4**: Downloading the ISO and Update Files and Mounting the Image, page 8-11. However, Cisco recommends you double-check the settings in the restore configuration before proceeding.

Tip To use a previously saved configuration, start with menu option **6**: Saving and Loading Restore Configurations, page 8-13. After you load the configuration, skip to menu option **4**: Downloading the ISO and Update Files and Mounting the Image, page 8-11.

To restore an appliance using the interactive menu, use the following steps:

Step 1 **1 IP Configuration** — see Identifying the Appliance's Management Interface, page 8-8.

Step 2 **2 Choose the transport protocol** — see Specifying ISO Image Location and Transport Method, page 8-9.

Step 3 **3 Select Patches/Rule Updates** (optional) — Updating System Software and Intrusion Rules During Restore, page 8-10.

Step 4 **4 Download and Mount ISO** — see Downloading the ISO and Update Files and Mounting the Image, page 8-11.

Step 5 **5 Run the Install** — see Invoking the Restore Process, page 8-11.

Identifying the Appliance's Management Interface

Access: Admin

The first step in running the restore utility is to identify the management interface on the appliance you want to restore, so that the appliance can communicate with the server where you copied the ISO and any update files. If you are using LOM, remember that the management IP address for the appliance is **not** the LOM IP address.

To identify the appliance's management interface:

Step 1 From the main menu, select **1 IP Configuration**.

Step 2 Select the appliance's management interface (generally **eth0**).

Step 3 Select the protocol you are using for your management network: **IPv4** or **IPv6**.

Options for assigning an IP address to the management interface appear.

Step 4 Select a method to assign an IP address to the management interface: **Static** or **DHCP**:

- If you select **Static**, a series of pages prompts you to manually enter the IP address, network mask or prefix length, and default gateway for the management interface.
- If you select **DHCP**, the appliance automatically detects the IP address, network mask or prefix length, and default gateway for the management interface, then displays the IP address.

Step 5 When prompted, confirm your settings.

If prompted, confirm the IP address assigned to the appliance's management interface.

What to Do Next

- Continue with the next section, Specifying ISO Image Location and Transport Method.

Specifying ISO Image Location and Transport Method

Access: Admin

After you configure the management IP address that the restore process will use to download files it needs, you must identify which ISO image you will use to restore the appliance. This is the ISO image that you downloaded from the Support Site (see Obtaining the Restore ISO and Update Files, page 8-3), and stored on a web server, FTP server, or SCP-enabled host.

The interactive menu prompts you to enter any necessary information to complete the download, as listed in the following table.

Table 8-2 Information Needed to Download Restore Files

To use...	You must provide...
HTTP	• IP address for the web server • full path to the ISO image directory (for example, `/downloads/ISOs/`)
FTP	• IP address for the FTP server • path to the ISO image directory, relative to the home directory of the user whose credentials you want to use (for example, `mydownloads/ISOs/`) • authorized user name and password for the FTP server **Note** The FTP protocol requires a client to send a remote user name and password on each FTP request to a server. The user name and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept the FTP write request from the user. Refer to the documentation for your FTP server for more information.
SCP	• IP address for the SCP server • authorized user name for the SCP server • full path to the ISO image directory • password for the user name you entered earlier **Note** Note that before you enter your password, the appliance may ask you to add the SCP server to its list of trusted hosts. You must accept to continue.

Note that the restore utility will also look for update files in the ISO image directory.

To specify the restore files' location and transport method:

Step 1 From the main menu, select **2 Choose the transport protocol**.

Step 2 On the page that appears, select either **HTTP**, **FTP**, or **SCP**.

If using FTP, the user name and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept the FTP write request from the user. Refer to the documentation for your FTP server for more information.

Step 3 Use the series of pages presented by the restore utility to provide the necessary information for the protocol you chose, as described in Table 8-2 on page 8-9.

If your information was correct, the appliance connects to the server and displays a list of the Cisco ISO images in the location you specified.

Step 4 Select the ISO image you want to use.

Step 5 When prompted, confirm your settings.

Step 6 Do you want to install a system software or intrusion rule update as a part of the restore process?

- If yes, continue with the next section, Updating System Software and Intrusion Rules During Restore.
- If no, continue with Downloading the ISO and Update Files and Mounting the Image, page 8-11. Note that you can use the system's web interface to manually install updates after the restore process completes.

Updating System Software and Intrusion Rules During Restore

Access: Admin

Optionally, you can use the restore utility to update the system software and intrusion rules after the appliance is restored to the base version in the ISO image. Note that only Management Centers require rule updates.

The restore utility can only use one system software update and one rule update. However, system updates are cumulative back to the last major version; rule updates are also cumulative. Cisco recommends that you obtain the latest updates available for your appliance; see Obtaining the Restore ISO and Update Files, page 8-3.

If you choose not to update the appliance during the restore process, you can update later using the system's web interface. For more information, see the release notes for the update you want to install, as well as the Updating System Software chapter in the *Firepower Management Center Configuration Guide*.

To install updates as part of the restore process:

Step 1 From the main menu, select **3 Select Patches/Rule Updates**.

The restore utility uses the protocol and location you specified in the previous procedure (see Specifying ISO Image Location and Transport Method, page 8-9) to retrieve and display a list of any system software update files in that location. If you are using SCP, enter your password when prompted to display the list of update files.

Step 2 Select the system software update, if any, you want to use.

You do not have to select an update; press Enter without selecting an update to continue. If there are no system software updates in the appropriate location, the system prompts you to press Enter to continue.

The restore utility retrieves and displays a list of rule update files. If you are using SCP, enter your password when prompted to display the list.

Step 3 Select the rule update, if any, you want to use.

You do not have to select an update; press Enter without selecting an update to continue. If there are no rule updates in the appropriate location, the system prompts you to press Enter to continue.

What to Do Next

- Continue with the next section, Downloading the ISO and Update Files and Mounting the Image.

Downloading the ISO and Update Files and Mounting the Image

Access: Admin

The final step before you invoke the restore process is to download the necessary files and mount the ISO image.

Before You Begin

- Before you begin this step, you may want to save your restore configuration for later use. For more information, see Saving and Loading Restore Configurations, page 8-13.

To download and mount the ISO image:

Step 1 From the main menu, select **4 Download and Mount ISO**.

Step 2 When prompted, confirm your choice. If you are downloading from an SCP server, enter your password when prompted.

The appropriate files are downloaded and mounted.

What to Do Next

- Continue with the next section, Invoking the Restore Process.

Invoking the Restore Process

Access: Admin

After you download and mount the ISO image, you are ready to invoke the restore process. If you are restoring an appliance to a different major version from the version currently installed on the appliance, a two-pass restore process is required. The first pass updates the operating system, and the second pass installs the new version of the system software.

First Pass of Two (Changing Major Versions Only)

When restoring an appliance to a different major version, a first pass by the restore utility updates the appliance's operating system, and, if necessary, the restore utility itself.

Note If you are restoring an appliance to the same major version, or if this is your second pass through the process, skip to the next procedure: Second or Only Pass, page 8-12.

To perform the first pass of a two-pass restore process:

Step 1 From the main menu, select **5 Run the Install**.

Step 2 When prompted (twice), confirm that you want to reboot the appliance.

Step 3 Monitor the reboot and invoke the restore process again:

- If the system is performing a database check, you may see the following message: `The system is not operational yet. Checking and repairing database are in progress. This may take a long time to finish.`

- For a keyboard and monitor connection, quickly press one of the arrow keys to prevent the appliance from booting the currently installed version of the system.
- For a serial or SOL/LOM connection, when you see the BIOS boot options, press Tab slowly and repeatedly until the LILO boot prompt appears. For example:

```
LILO 22.8 boot:
System-5.4 System_Restore
```

Step 4 Indicate that you want to restore the system:

- For a keyboard and monitor connection, use the arrow keys to select `Serial_Restore` and press Enter.
- For a serial or SOL/LOM connection, type `Serial_Restore` at the prompt and press Enter.

In either case, the `boot` prompt appears after the following choices:

```
0. Load with standard console
1. Load with serial console
```

Step 5 Select a display mode for the restore utility's interactive menu:

- For a keyboard and monitor connection, type `0` and press Enter.
- For a serial or SOL/LOM connection, type `1` and press Enter.

If you do not select a display mode, the restore utility defaults to the standard console after 30 seconds.

Unless this is the first time you have restored the appliance to this major version, the utility automatically loads the last restore configuration you used. To continue, confirm the settings in a series of pages.

Step 6 Press Enter to confirm the copyright notice.

What to do Next

- Begin the second pass of the process, starting with Using the Interactive Menu to Restore an Appliance, page 8-6.

Second or Only Pass

Use the following procedure to perform the second or only pass through the restore process.

To perform the second or only pass through the restore process:

Step 1 From the main menu, select **5 Run the Install**.

Step 2 Confirm that you want to restore the appliance and continue with the next step.

Step 3 Choose whether you want to delete the appliance's license and network settings. Deleting these settings also resets display (console) and LOM settings.

In most cases, you do not want to delete these settings, because it can make the initial setup process shorter. Changing settings after the restore and subsequent initial setup is often less time consuming than trying to reset them now. For more information, see Next Steps, page 8-14.

Caution Do **not** delete the network settings if you are restoring the appliance using a LOM connection. After you reboot the appliance, you will be unable to reconnect via LOM.

Step 4 Type your final confirmation that you want to restore the appliance.

The final stage of the restore process begins. When it completes, if prompted, confirm that you want to reboot the appliance.

Caution Make sure you allow sufficient time for the restore process to complete. On appliances with internal flash drives, the utility first updates the flash drive, which is then used to perform other restore tasks. If you quit (by pressing Ctrl + C, for example) during the flash update, you could cause an unrecoverable error. If you think the restore is taking too long or you experience any other issues with the process, do **not** quit. Instead, contact Support.

Note Reimaging resets appliances in bypass mode to a non-bypass configuration and disrupts traffic on your network until you reconfigure bypass mode. For more information, see Traffic Flow During the Restore Process, page 8-1.

What to Do Next

- Continue with Next Steps, page 8-14.

Saving and Loading Restore Configurations

Access: Admin

You can use the restore utility to save a restore configuration to use if you need to restore a Firepower device again. Although the restore utility automatically saves the last configuration used, you can save multiple configurations, which include:

- network information about the management interface on the appliance; see Identifying the Appliance's Management Interface, page 8-8
- the location of the restore ISO image, as well as the transport protocol and any credentials the appliance needs to download the file; see Specifying ISO Image Location and Transport Method, page 8-9
- the system software and intrusion rules updates, if any, that you want to apply after the appliance is restored to the base version in the ISO image; see Updating System Software and Intrusion Rules During Restore, page 8-10

SCP passwords are not saved. If the configuration specifies that the utility must use SCP to transfer ISO and other files to the appliance, you will have to re-authenticate to the server to complete the restore process.

The best time to save a restore configuration is after you provide the information listed above, but before you download and mount the ISO image.

To save a restore configuration:

Step 1 From the restore utility's main menu, select **6 Save Configuration**.

The utility displays the settings in the configuration you are saving.

Step 2 When prompted, confirm that you want to save the configuration.

Step 3 When prompted, enter a name for the configuration.

What to Do Next

- To use the configuration you just saved to restore the appliance, continue with Downloading the ISO and Update Files and Mounting the Image, page 8-11.

To load a saved restore configuration:

Step 1 From the main menu, select **7 Load Configuration**.

The utility presents a list of saved restore configurations. The first option, **default_config**, is the configuration you last used to restore the appliance. The other options are restore configurations that you have saved.

Step 2 Select the configuration you want to use.

The utility displays the settings in the configuration you are loading.

Step 3 When prompted, confirm that you want to load the configuration.

The configuration is loaded. If prompted, confirm the IP address assigned to the appliance's management interface.

What to Do Next

- To use the configuration you just loaded to restore the appliance, continue with Downloading the ISO and Update Files and Mounting the Image, page 8-11.

Next Steps

Restoring your appliance to factory default settings results in the loss of almost **all** configuration and event data on the appliance, including bypass configurations for devices deployed inline. For more information, see Traffic Flow During the Restore Process, page 8-1.

After you restore an appliance, you must complete an initial setup process:

- If you did not delete the appliance's license and network settings, you can use a computer on your management network to browse directly to the appliance's web interface to perform the setup. For more information, see Initial Setup Page: Firepower Devices, page 5-5.
- If you deleted license and network settings, you must configure the appliance as if it were new, beginning with configuring it to communicate on your management network. See Setting Up Firepower Managed Devices, page 5-1.

Note that deleting license and network settings also resets display (console) and LOM settings=. After you complete the initial setup process:

- If you want to use a serial or SOL/LOM connection to access your appliance's console, you should redirect console output; see Testing an Inline Bypass Interface Installation, page 4-24.
- If you want to use LOM, you must re-enable the feature as well as enable at least one LOM user; see Enabling LOM and LOM Users, page 8-16.

Setting Up Lights-Out Management

If you need to restore a Firepower device to factory defaults and do not have physical access to the appliance, you can use Lights-Out Management (LOM) to perform the restore process. Note that you can use Lights-Out Management on the default (`eth0`) management interface only.

Note The baseboard management controller (BMC) for a Firepower 71xx, Firepower 82xx, or a Firepower or AMP 83xx device is only accessible via 1Gbps link speeds when the host is powered on. When the device is powered down the BMC can only establish Ethernet link at 10 and 100Mbps. Therefore if LOM is being used to remotely power the device, connect the device to the network using 10 and 100Mbps link speeds only.

The LOM feature allows you to perform a limited set of actions on a Firepower device, using a Serial over LAN (SOL) connection. With LOM, you use a command line interface on an out-of-band management connection to perform tasks such as viewing the chassis serial number, or monitoring conditions such as fan speed and temperature.

The syntax of LOM commands depends on the utility you are using, but LOM commands generally contain the elements listed in the following table.

Table 8-3 LOM Command Syntax

IPMItool (Linux/Mac)	ipmiutil (Windows)	Description
`ipmitool`	`ipmiutil`	Invokes the IPMI utility.
n/a	`-V4`	For ipmiutil only, enables admin privileges for the LOM session.
`-I lanplus`	`-J3`	Enables encryption for the LOM session.
`-H` *`IP_address`*	`-N` *`IP_address`*	Specifies the IP address of the management interface on the appliance.
`-U` *`username`*	`-U` *`username`*	Specifies the user name of an authorized LOM account.
n/a (prompted on login)	-P *`password`*	For ipmiutil only, specifies the password for an authorized LOM account.
`command`	*`command`*	The command you want to issue to the appliance. Note that where you issue the command depends on the utility: • For IPMItool, type the command last. • For ipmiutil, type the command first.

Therefore, for IPMItool:

```
ipmitool -I lanplus -H IP_address -U username command
```

Or, for ipmiutil:

```
ipmiutil command -V4 -J3 -N IP_address -U username -P password
```

Note that the `chassis power off` and `chassis power cycle` commands are not valid on 70xx Family appliances. For a full list of LOM commands supported by the Firepower System, see the Configuring Appliance Settings chapter in the *Firepower Management Center Configuration Guide*.

Note Before you can connect to a 7000 Series device using SOL, you must disable Spanning Tree Protocol (STP) on any third-party switching equipment connected to the device's management interface.

Note In some power cycle scenarios, the baseboard management controller (BMC) of a Firepower 7050 connected to the network via the management interface could lose the IP address assigned to it by the DHCP server. Because of this, Cisco recommends you configure the Firepower 7050 BMC with a static IP address. Alternately, you can disconnect the network cable and reconnect it, or remove and restore power to the device to force renegotiation of the link.

Before you can restore an appliance using LOM, you must enable LOM for both the appliance and the user who will perform the restore. Then, use a third-party Intelligent Platform Management Interface (IPMI) utility to access the appliance. You must also make sure you redirect the appliance's console output to the serial port.

For more information, see the following sections:

- Enabling LOM and LOM Users, page 8-16
- Installing an IPMI Utility, page 8-17

Enabling LOM and LOM Users

Access: Admin

Before you can use LOM to restore an appliance, you must enable and configure the feature. You must also explicitly grant LOM permissions to users who will use the feature.

You configure LOM and LOM users on a per-appliance basis using each appliance's local web interface. That is, you cannot use the Management Center to configure LOM on a Firepower device. Similarly, because users are managed independently per appliance, enabling or creating a LOM-enabled user on the Management Center does not transfer that capability to users on Firepower devices.

LOM users also have the following restrictions:

- You must assign the Administrator role to the user.
- The user name may have up to 16 alphanumeric characters. Hyphens and longer user names are not supported for LOM users.
- The password may have up to 20 alphanumeric characters. Longer passwords are not supported for LOM users. A user's LOM password is the same as that user's system password.
- Management Centers and 8000 Series devices can have up to 13 LOM users. 7000 Series devices can have up to eight LOM users.

Tip For detailed instructions on the following tasks, see the Configuring Appliance Settings chapter in the *Firepower Management Center Configuration Guide*.

To enable LOM:

Step 1 Select **System > Configuration**, then click **Console Configuration**.

Step 2 Your next step depends on your appliance model:

- To enable LOM on Firepower 8000 Series devices, you must enable remote access using the **Physical Serial Port** before you can specify the LOM IP address, netmask, and default gateway (or use DHCP to have these values automatically assigned).
- On Firepower 7000 Series devices, select **Lights Out Management** to configure LOM settings. 7000 Series devices do not support LOM and physical serial access at the same time.

Note The LOM IP address must be different from the management interface IP address of the appliance.

To enable LOM capabilities for a Firepower System user:

Step 1 Select **System > User Management**, then either edit an existing user to add LOM permissions, or create a new user that you will use for LOM access to the appliance.

Step 2 On the User Configuration page, enable the **Administrator** role if it is not already enabled.

Step 3 Enable the **Allow Lights-Out Management Access** check box and save your changes.

Installing an IPMI Utility

You use a third-party IPMI utility on your computer to create an SOL connection to the appliance.

If your computer is running Linux or Mac OS, use IPMItool. Although IPMItool is standard with many Linux distributions, you must install IPMItool on a Mac. First, confirm that your Mac has Apple's xCode developer tools package installed. Also, make sure the optional components for command line development are installed ("UNIX Development" and "System Tools" in newer versions, or "Command Line Support" in older versions). Finally, install MacPorts and IPMItool. For more information, use your favorite search engine or see these sites:

```
https://developer.apple.com/technologies/tools/
http://www.macports.org/
```

For Windows environments, use ipmiutil, which you must compile yourself. If you do not have access to a compiler, you can use ipmiutil itself to compile. For more information, use your favorite search engine or see this site:

```
http://ipmiutil.sourceforge.net/
```

Power Requirements for Firepower Devices

Warnings and Cautions

This document contains both warnings and cautions. Warnings are safety related. Failure to follow warnings may lead to injury or equipment damage. Cautions are requirements for proper function. Failure to follow cautions may result in improper operation.

Caution The intra-building ports of the equipment or subassembly are suitable for connection to intra-building or exposed wiring or cabling only. The intra-building ports of the equipment or subassembly **must not** be metallically connected to interfaces that connect outside the plant (OSP) or its wiring. These interfaces are designed for use as intra-building 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 the primary protectors is not sufficient protection to connect these interfaces metallically to OSP wiring.

Static Control

Caution Electrostatic discharge control procedures, such as using grounded wrist straps and an ESD work surface, must be in place before unpacking, installing, or moving the appliance. Excessive electrostatic discharges can damage the appliance or cause unintended operation.

Firepower 70xx Family Appliances

This section describes the power requirements for:

- Firepower 7010, 7020, and 7030 (CHRY-1U-AC)
- Firepower 7050 (NEME-1U-AC)

These appliances are suitable for installation by qualified personnel in network telecommunication facilities and locations where the National Electric Code applies. Note that each is available only as an AC appliance.

Cisco recommends that you save the packing materials in case a return is necessary.

For more information, see the following sections:

- See Installation, page A-2 for circuit installation, voltage, current, frequency range, and power cord information.
- See Grounding/Earthing Requirements, page A-2 for bonding locations, recommended terminals, and ground wire requirements.

Installation

This appliance must be installed in accordance with the requirements of Article 250 of NFPA 70, National Electric Code (NEC) Handbook, and local electrical codes.

The appliance uses a single power supply. An external surge protection device must be used at the input of the network equipment where the Firepower System is to be installed.

The circuit must be rated for the full rating of the appliance.

Voltage

The power supply works with 100VAC to 240VAC nominal (90VAC to 264VAC maximum). Use of voltages outside this range may cause damage to the appliance.

Current

The labeled current rating is 2A maximum over the full range. Appropriate wire and breakers must be used to reduce the potential for fire.

Frequency Range

The frequency range of the AC power supply is 47 Hz to 63 Hz. Frequencies outside this range may cause the appliance to not operate or to operate incorrectly.

Power Cord

The power connection on the power supply is an IEC C14 connector and accepts IEC C13 connectors. A UL-recognized power cord must be used. The minimum wire gauge is 16 AWG. The cord supplied with the appliance is a 16 AWG, UL-recognized cord with NEMA 515P plug. Contact the factory about other power cords.

Note Do **not** cut the cord on the power supply.

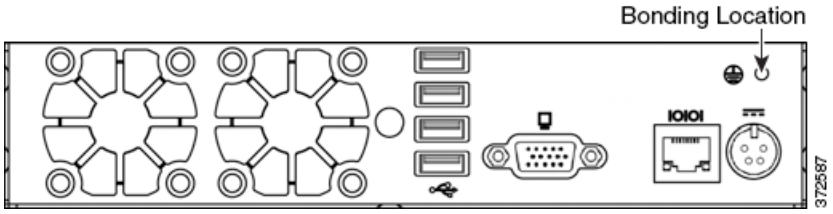
Grounding/Earthing Requirements

The appliance must be grounded to the common bonding network.

Bonding Location

A ground bonding location is provided on the rear of the chassis. An M4 stud is provided. An outside-toothed lock washer is provided for attaching a ring terminal. A standard ground symbol is available by each stud.

The following illustration indicates the bonding location on the chassis.



Recommended Terminals

You must use a UL-Approved terminal for the ground connection. A ring terminal with a clearance hole for #6 (M3.5) stud may be used. For 16 AWG wire, AMP/Tyco 36151 is recommended. This is a UL-approved ring terminal with a hole for a #6 stud.

Ground Wire Requirements

The ground wire must be sized sufficiently to handle the current of the circuit in case of a single fault. The size of the ground wire should be equal to the current of the breaker used to protect the circuit. See Current, page A-2.

Bare conductors must be coated with antioxidant before crimp connections are made. Only copper cables can be used for grounding purposes.

Firepower 71xx Family Appliances

This section describes the power requirements for:

- Firepower 7110 and 7120 (GERY-1U-8-AC)
- Firepower 7115 and 7125 (GERY-1U-4C8S-AC)

These appliances are suitable for installation by qualified personnel in network telecommunication facilities and locations where the National Electric Code applies. Note that each is available only as an AC appliance.

Cisco recommends that you save the packing materials in case a return is necessary.

For more information, see the following sections:

- See Installation, page A-4 for circuit installation, voltage, current, and frequency range, and power cord information.
- See Grounding/Earthing Requirements, page A-5 for bonding locations, recommended terminals, and ground wire requirements.

Installation

The Firepower System must be installed in accordance with the requirements of Article 250 of NFPA 70, National Electric Code (NEC) Handbook, and local electrical codes.

Separate circuits are required to create redundant power sources. Use an uninterruptible or battery-backed power source to prevent power status issues or power loss due to input line power glitches. The power supplies are hot-swappable.

Supply sufficient power to each power supply to run the entire appliance. The voltage and current ratings for each supply are listed on the label on the appliance.

Use an external Surge Protection Device at the input of the network equipment where the Firepower System is to be installed.

Separate Circuit Installation

If separate circuits are used, each one must be rated the full rating of the appliance. This configuration provides for circuit failure and power supply failure.

Example: Each supply is attached to a different 220V circuit. Each circuit must be capable of supplying 5A, as stated on the label.

Same Circuit Installation

If the same circuit is used to feed both supplies, then the power rating of one supply applies to the whole box. This configuration only provides protection from a power supply failure.

Example: Both supplies are attached to the same 220V circuit. The maximum draw from this circuit would be 5A, as stated on the label.

Voltage

The power supplies will work with these voltages: 100VAC to 240VAC nominal (85VAC to 264VAC maximum). Use of voltages outside this range may cause damage to the appliance.

Current

The labeled current rating for each supply is: 10A maximum over the full range, per supply 5A maximum for 187VAC to 264VAC, per supply. Appropriate wire and breakers must be used to reduce the potential for fire.

Frequency Range

The frequency range of the AC power supply is 47 Hz to 63 Hz. Frequencies outside this range may cause the appliance to not operate or to operate incorrectly.

Power Cords

The power connections on the power supplies are IEC C14 connectors and they will accept IEC C13 connectors. A UL-recognized power cord must be used. The minimum wire gauge is 16 AWG. The cords supplied with the appliances are 16 AWG, UL-recognized cords with NEMA 515P plug. Contact the factory about other power cords.

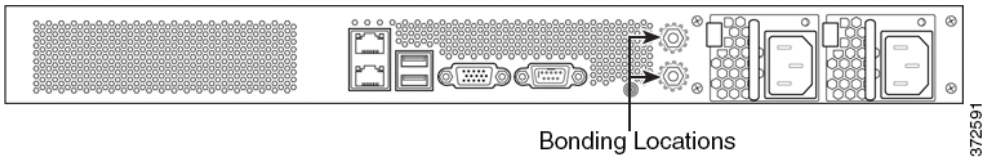
Grounding/Earthing Requirements

The Firepower System must be grounded to the Common Bonding Network.

Bonding Locations

Ground bonding locations are provided on the rear of the chassis. M4 studs are provided. Outside-toothed lock washers are provided for attaching ring terminals. A standard ground symbol is available by each stud.

The following illustration indicates the bonding locations on the chassis.



Recommended Terminals

You must use UL-Approved terminals for the ground connection. Ring terminals with a clearance hole for 4mm or #8 studs may be used. For 10-12 AWG wire, Tyco 34853 is recommended. This is a UL-approved, ring terminal with a hole for a #8 stud.

Ground Wire Requirements

The ground wire must be sized sufficiently to handle the current of the circuit in case of a single fault. The size of the ground wire should be equal to the current of the breaker used to protect the circuit. See Current, page A-4.

Bare conductors must be coated with antioxidant before crimp connections are made. Only copper cables can be used for grounding purposes.

Firepower 81xx Family Appliances

This section describes the power requirements for:

- Firepower 8120, 8130, and 8140 (CHAS-1U-AC, CHAS-1U-DC, or CHAS-1U-AC/DC)

These appliances are suitable for installation by qualified personnel in network telecommunication facilities and locations where the National Electric Code applies.

Cisco recommends that you save the packing materials in case a return is necessary.

For more information, see the following sections:

- See AC Installation, page A-6 for circuit installation, voltage, current, and frequency range, and power cord information.
- See DC Installation, page A-7 for circuit installation, voltage, current, ground references, terminals, breaker requirements, and minimum wire size.
- See Grounding/Earthing Requirements, page A-8 for bonding locations, recommended terminals, ground wire requirements, and DC supplies.

AC Installation

The Firepower System must be installed in accordance with the requirements of Article 250 of NFPA 70, National Electric Code (NEC) Handbook, and local electrical codes.

Caution Do **not** connect DC power to AC supplies.

Separate circuits are required to create redundant power sources. Use an uninterruptible or battery-backed power source to prevent power status issues or power loss due to input line power glitches. The power supplies are hot-swappable.

Supply sufficient power to each power supply to run the entire appliance. The voltage and current ratings for each supply are listed on the label on the appliance.

Use an external Surge Protection Device at the input of the network equipment where the Firepower System is to be installed.

Separate Circuit Installation

If separate circuits are used, each one must be rated the full rating of the appliance. This configuration provides for circuit failure and power supply failure.

Example: Each supply is attached to a different 220V circuit. Each circuit must be capable of supplying 5A, as stated on the label.

Same Circuit Installation

If the same circuit is used to feed both supplies, then the power rating of one supply applies to the whole box. This configuration only provides protection from a power supply failure.

Example: Both supplies are attached to the same 220V circuit. The maximum draw from this circuit would be 5A, as stated on the label.

AC Voltage

The power supplies will work with these voltages: 100VAC to 240VAC nominal (85VAC to 264VAC maximum). Use of voltages outside this range may cause damage to the appliance.

AC Current

The labeled current rating for each supply is: 5.2A maximum over the full range, per supply 2.6A maximum for 187VAC to 264VAC, per supply. Appropriate wire and breakers must be used to reduce the potential for fire.

Frequency Range

The frequency range of the AC power supply is 47 Hz to 63 Hz. Frequencies outside this range may cause the appliance to not operate or to operate incorrectly.

Power Cords

The power connections on the power supplies are IEC C14 connectors and they will accept IEC C13 connectors. A UL-recognized power cord must be used. The minimum wire gauge is 16 AWG. The cords supplied with the appliances are 16 AWG, UL-recognized cords with NEMA 515P plug. Contact the factory about other power cords.

DC Installation

Separate circuits are required to create redundant power sources. Use an uninterruptible or battery-backed power source to prevent power status issues or power loss due to input line power glitches. The power supplies are hot-swappable.

Caution Do **not** connect AC power to DC supplies.

Supply sufficient power to each power supply to run the entire appliance. The voltage and current ratings for each supply are listed on the label on the appliance.

Use an external Surge Protection Device at the input of the network equipment where the Firepower System is to be installed.

Separate Circuit Installation

If separate circuits are used, each circuit must be rated to the full rating of the appliance. This configuration provides for circuit failure and power supply failure.

Example: Each supply is attached to a different –48VDC circuit. Each circuit must be capable of supplying 20A, as stated on the label.

Same Circuit Installation

If the same circuit is used to feed both supplies, then the power rating of one supply applies to the whole box. This configuration only provides protection from a power supply failure.

Example: Both supplies are attached to the same –48VDC circuit. The maximum draw from this circuit would be 20A, as stated on the label.

Caution Use of this optimization requires that the power cords are rated for the full rating for each supply.

DC Voltage

The power supplies will work with these voltages:

- -48VDC nominal referenced to RTN

- -40VDC to -72VDC maximum

Use of voltages outside this range may cause damage to the appliance.

DC Current

11A maximum, per supply

Ground Reference

The DC power supplies are fully isolated from the ground reference.

Recommended Terminals

Power is connected to the DC supplies through screw terminals. Terminals must be UL approved. Terminals must have a hole supporting an M4 or a #8 screw. The maximum width of the terminal is 8.1mm (0.320”). A representative spade terminal for 10-12 gauge wire is Tyco 325197.

Breaker Requirements

A breaker sufficient to carry the rated current at the rated voltage must be provided. The circuit breaker must meet the following requirements:

- UL Recognized
- CSA Approved (Recommended)
- VDE Approved (Recommended)
- Support the maximum load (20A)
- Support the installation voltage (-40V to -72VDC, as required by the power supply)
- Rated for DC use

A recommended breaker is: Airpax IELK1-1-72-20.0-01-V. The terminal option used will depend on the installation. This breaker is a single pole, 20A breaker with a DC rating of 80V. It is listed as having a *long delay*. Information about this breaker can be found at http://www.airpax.net/site/utilities/eliterature/pdfs/ial.pdf.

Minimum Wire Size Requirements

Power feeds with three wires (one circuit) per raceway may use 12 AWG wire. Power feeds with more than one circuit per raceway must use 10 AWG wire. Note that the two separate feeds for the redundant supplies are two circuits and must use 10 AWG wire.

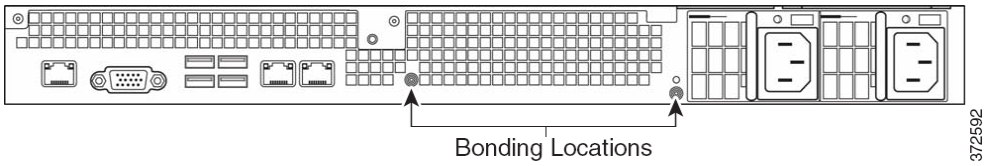
Grounding/Earthing Requirements

The Firepower System must be grounded to the Common Bonding Network.

Bonding Locations

Ground bonding locations are provided on the rear of the chassis. M4 studs are provided. Outside-toothed lock washers are provided for attaching ring terminals. A standard ground symbol is available by each stud.

The following illustration indicates the bonding locations on the 1U chassis.



Recommended Terminals

You must use UL-Approved terminals for the ground connection. Ring terminals with a clearance hole for 4mm or #8 studs may be used. For 10-12 AWG wire, Tyco 34853 is recommended. This is a UL-approved, ring terminal with a hole for a #8 stud.

Ground Wire Requirements

The ground wire must be sized sufficiently to handle the current of the circuit in case of a single fault. The size of the ground wire should be equal to the current of the breaker used to protect the circuit. For AC circuits, see AC Current, page A-6. For DC currents, see DC Current, page A-8.

Bare conductors must be coated with antioxidant before crimp connections are made. Only copper cables can be used for grounding purposes.

DC Supplies

The DC power supplies have additional ground connections on each supply. This allows the hot-swappable supply to be connected to power, return and ground so that it may be safely inserted. This ground lug must be attached.

It is a M4 screw with an outside-toothed lock washer screw.

The ground wire should be sized to match the breaker for the circuit.

Firepower 82xx Family Appliances

This section describes the power requirements for:

- Firepower 8250, 8260, 8270, and 8290 (CHAS-2U-AC, CHAS-2U-DC, or CHAS-2U-AC/DC)

These appliances are suitable for installation by qualified personnel in network telecommunication facilities and locations where the National Electric Code applies.

Cisco recommends that you save the packing materials in case a return is necessary.

For more information, see the following sections:

- See AC Installation, page A-10 for circuit installation, voltage, current, and frequency range, and power cord information.

- See DC Installation, page A-11 for circuit installation, voltage, current, ground references, terminals, breaker requirements, and minimum wire size.
- See Grounding/Earthing Requirements, page A-12 for bonding locations, recommended terminals, ground wire requirements, and DC supplies.

AC Installation

The Firepower System must be installed in accordance with the requirements of Article 250 of NFPA 70, National Electric Code (NEC) Handbook, and local electrical codes.

Caution Do **not** connect DC power to AC supplies.

Separate circuits are required to create redundant power sources. Use an uninterruptible or battery-backed power source to prevent power status issues or power loss due to input line power glitches. The power supplies are hot-swappable.

Supply sufficient power to each power supply to run the entire appliance. The voltage and current ratings for each supply are listed on the label on the appliance.

Use an external Surge Protection Device at the input of the network equipment where the Firepower System is to be installed.

Separate Circuit Installation

If separate circuits are used, each one must be rated the full rating of the appliance. This configuration provides for circuit failure and power supply failure.

Example: Each supply is attached to a different 220V circuit. Each circuit must be capable of supplying 5A, as stated on the label.

Same Circuit Installation

If the same circuit is used to feed both supplies, then the power rating of one supply applies to the whole box. This configuration only provides protection from a power supply failure.

Example: Both supplies are attached to the same 220V circuit. The maximum draw from this circuit would be 5A, as stated on the label.

AC Voltage

The power supplies will work with these voltages: 100VAC to 240VAC nominal (85VAC to 264VAC maximum). Use of voltages outside this range may cause damage to the appliance.

AC Current

The labeled current rating for each supply is: 8A maximum over the full range, per supply 4A maximum for 187VAC to 264VAC, per supply. Appropriate wire and breakers must be used to reduce the potential for fire.

Frequency Range

The frequency range of the AC power supply is 47 Hz to 63 Hz. Frequencies outside this range may cause the appliance to not operate or to operate incorrectly.

Power Cords

The power connections on the power supplies are IEC C14 connectors and they will accept IEC C13 connectors. A UL-recognized power cord must be used. The minimum wire gauge is 16 AWG. The cords supplied with the appliances are 16 AWG, UL-recognized cords with NEMA 515P plug. Contact the factory about other power cords.

DC Installation

Separate circuits are required to create redundant power sources. Use an uninterruptible or battery-backed power source to prevent power status issues or power loss due to input line power glitches. The power supplies are hot-swappable.

Caution Do **not** connect AC power to DC supplies.

Supply sufficient power to each power supply to run the entire appliance. The voltage and current ratings for each supply are listed on the label on the appliance.

Use an external Surge Protection Device at the input of the network equipment where the Firepower System is to be installed.

Separate Circuit Installation

If separate circuits are used, each circuit must be rated to the full rating of the appliance. This configuration provides for circuit failure and power supply failure.

Example: Each supply is attached to a different –48VDC circuit. Each circuit must be capable of supplying 20A, as stated on the label.

Same Circuit Installation

If the same circuit is used to feed both supplies, then the power rating of one supply applies to the whole box. This configuration only provides protection from a power supply failure.

Example: Both supplies are attached to the same –48VDC circuit. The maximum draw from this circuit would be 20A, as stated on the label.

Caution Use of this optimization requires that the power cords are rated for the full rating for each supply.

DC Voltage

The power supplies will work with these voltages:

- -48VDC nominal referenced to RTN

- -40VDC to -72VDC maximum

Use of voltages outside this range may cause damage to the appliance.

DC Current

18A maximum, per supply

Ground Reference

The DC power supplies are fully isolated from the ground reference.

Recommended Terminals

Power is connected to the DC supplies through screw terminals. Terminals must be UL approved. Terminals must have a hole supporting an M4 or a #8 screw. The maximum width of the terminal is 8.1mm (0.320”). A representative spade terminal for 10-12 gauge wire is Tyco 325197.

Breaker Requirements

A breaker sufficient to carry the rated current at the rated voltage must be provided. The circuit breaker must meet the following requirements:

- UL Recognized
- CSA Approved (Recommended)
- VDE Approved (Recommended)
- Support the maximum load (20A)
- Support the installation voltage (-40V to -72VDC, as required by the power supply)
- Rated for DC use

A recommended breaker is: Airpax IELK1-1-72-20.0-01-V. The terminal option used will depend on the installation. This breaker is a single pole, 20A breaker with a DC rating of 80V. It is listed as having a *long delay*. Information about this breaker can be found at http://www.airpax.net/site/utilities/eliterature/pdfs/ial.pdf.

Minimum Wire Size Requirements

Power feeds with three wires (one circuit) per raceway may use 12 AWG wire. Power feeds with more than one circuit per raceway must use 10 AWG wire. Note that the two separate feeds for the redundant supplies are two circuits and must use 10 AWG wire.

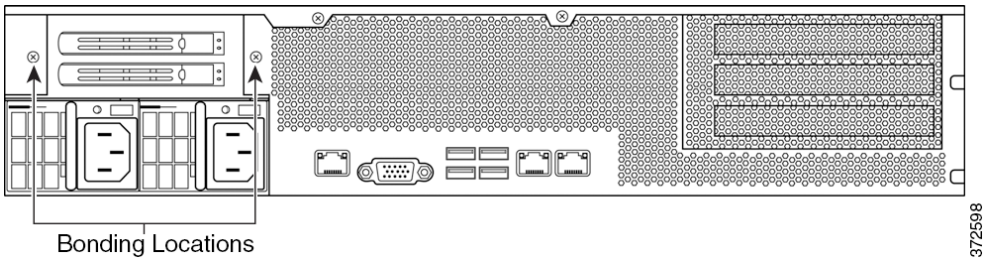
Grounding/Earthing Requirements

The Firepower System must be grounded to the Common Bonding Network.

Bonding Locations

Ground bonding locations are provided on the rear of the chassis. M4 studs are provided. Outside-toothed lock washers are provided for attaching ring terminals. A standard ground symbol is available by each stud.

The following illustration indicates the bonding locations on the 2U chassis.



Recommended Terminals

You must use UL-Approved terminals for the ground connection. Ring terminals with a clearance hole for 4mm or #8 studs may be used. For 10-12 AWG wire, Tyco 34853 is recommended. This is a UL-approved, ring terminal with a hole for a #8 stud.

Ground Wire Requirements

The ground wire must be sized sufficiently to handle the current of the circuit in case of a single fault. The size of the ground wire should be equal to the current of the breaker used to protect the circuit. For AC circuits, see AC Current, page A-6. For DC currents, see DC Current, page A-8.

Bare conductors must be coated with antioxidant before crimp connections are made. Only copper cables can be used for grounding purposes.

DC Supplies

The DC power supplies have additional ground connections on each supply. This allows the hot-swappable supply to be connected to power, return and ground so that it may be safely inserted. This ground lug must be attached.

It is a M4 screw with an outside-toothed lock washer screw.

The ground wire should be sized to match the breaker for the circuit.

Firepower and AMP 83xx Family Appliances

This section describes the power requirements for:

- Firepower and AMP 8350, 8360, 8370, and 8390 (PG35-2U-AC/DC)

These appliances are suitable for installation by qualified personnel in network telecommunication facilities and locations where the National Electric Code applies.

Cisco recommends that you save the packing materials in case a return is necessary.

For more information, see the following sections:

- See AC Installation, page A-14 for circuit installation, voltage, current, and frequency range, and power cord information.
- See DC Installation, page A-15 for circuit installation, voltage, current, ground references, terminals, breaker requirements, and minimum wire size.
- See Grounding/Earthing Requirements, page A-16 for bonding locations, recommended terminals, ground wire requirements, and DC supplies.

AC Installation

The Firepower System must be installed in accordance with the requirements of Article 250 of NFPA 70, National Electric Code (NEC) Handbook, and local electrical codes.

Caution Do **not** connect DC power to AC supplies.

Separate circuits are required to create redundant power sources. Use an uninterruptible or battery-backed power source to prevent power status issues or power loss due to input line power glitches. The power supplies are hot-swappable.

Supply sufficient power to each power supply to run the entire appliance. The voltage and current ratings for each supply are listed on the label on the appliance.

Use an external Surge Protection Device at the input of the network equipment where the Firepower System is to be installed.

Separate Circuit Installation

If separate circuits are used, each one must be rated the full rating of the appliance. This configuration provides for circuit failure and power supply failure.

Example: Each supply is attached to a different 220V circuit. Each circuit must be capable of supplying 10A, as stated on the label.

Same Circuit Installation

If the same circuit is used to feed both supplies, then the power rating of one supply applies to the whole box. This configuration only provides protection from a power supply failure.

Example: Both supplies are attached to the same 220V circuit. The maximum draw from this circuit would be 10A, as stated on the label.

AC Voltage

The power supplies will work with these voltages: 100VAC to 240VAC nominal (85VAC to 264VAC maximum). Use of voltages outside this range may cause damage to the appliance.

AC Current

The labeled current rating for each supply is: 11A maximum over the full range, per supply 5.5A maximum for 187VAC to 264VAC, per supply. Appropriate wire and breakers must be used to reduce the potential for fire.

Frequency Range

The frequency range of the AC power supply is 47 Hz to 63 Hz. Frequencies outside this range may cause the appliance to not operate or to operate incorrectly.

Power Cords

The power connections on the power supplies are IEC C14 connectors and they will accept IEC C13 connectors. A UL-recognized power cord must be used. The minimum wire gauge is 16 AWG. The cords supplied with the appliances are 16 AWG, UL-recognized cords with NEMA 515P plug. Contact the factory about other power cords.

DC Installation

Separate circuits are required to create redundant power sources. Use an uninterruptible or battery-backed power source to prevent power status issues or power loss due to input line power glitches. The power supplies are hot-swappable.

Caution Do **not** connect AC power to DC supplies.

Supply sufficient power to each power supply to run the entire appliance. The voltage and current ratings for each supply are listed on the label on the appliance.

Use an external Surge Protection Device at the input of the network equipment where the Firepower System is to be installed.

Separate Circuit Installation

If separate circuits are used, each circuit must be rated to the full rating of the appliance. This configuration provides for circuit failure and power supply failure.

Example: Each supply is attached to a different –48VDC circuit. Each circuit must be capable of supplying 25A, as stated on the label.

Same Circuit Installation

If the same circuit is used to feed both supplies, then the power rating of one supply applies to the whole box. This configuration only provides protection from a power supply failure.

Example: Both supplies are attached to the same –48VDC circuit. The maximum draw from this circuit would be 25A, as stated on the label.

Caution Use of this optimization requires that the power cords are rated for the full rating for each supply.

DC Voltage

The power supplies will work with these voltages:

- -48VDC nominal referenced to RTN

- -40VDC to -72VDC maximum

Use of voltages outside this range may cause damage to the appliance.

DC Current

25A maximum, per supply

Ground Reference

The DC power supplies are fully isolated from the ground reference.

Recommended Terminals

Power is connected to the DC supplies through screw terminals. Terminals must be UL approved. Terminals must have a hole supporting an M4 or a #8 screw. The maximum width of the terminal is 8.1mm (0.320”). A representative spade terminal for 10-12 gauge wire is Tyco 325197.

Breaker Requirements

A breaker sufficient to carry the rated current at the rated voltage must be provided. The circuit breaker must meet the following requirements:

- UL Recognized
- CSA Approved (Recommended)
- VDE Approved (Recommended)
- Support the maximum load (20A)
- Support the installation voltage (-40V to -72VDC, as required by the power supply)
- Rated for DC use

A recommended breaker is: Airpax IELK1-1-72-20.0-01-V. The terminal option used will depend on the installation. This breaker is a single pole, 20A breaker with a DC rating of 80V. It is listed as having a *long delay*. Information about this breaker can be found at http://www.airpax.net/site/utilities/eliterature/pdfs/ial.pdf.

Minimum Wire Size Requirements

Power feeds with three wires (one circuit) per raceway may use 12 AWG wire. Power feeds with more than one circuit per raceway must use 10 AWG wire. Note that the two separate feeds for the redundant supplies are two circuits and must use 10 AWG wire.

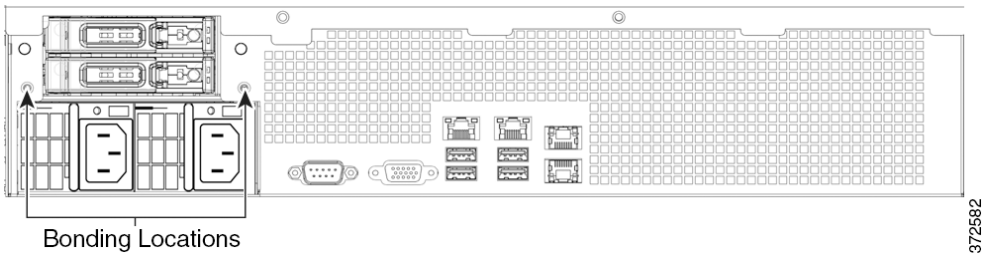
Grounding/Earthing Requirements

The Firepower System must be grounded to the Common Bonding Network.

Bonding Locations

Ground bonding locations are provided on the rear of the chassis. M4 studs are provided. Outside-toothed lock washers are provided for attaching ring terminals. A standard ground symbol is available by each stud.

The following illustration indicates the bonding locations on the 83xx Family 2U chassis.



Recommended Terminals

You must use UL-Approved terminals for the ground connection. Ring terminals with a clearance hole for 4mm or #8 studs may be used. For 10-12 AWG wire, Tyco 34853 is recommended. This is a UL-approved, ring terminal with a hole for a #8 stud.

Ground Wire Requirements

The ground wire must be sized sufficiently to handle the current of the circuit in case of a single fault. The size of the ground wire should be equal to the current of the breaker used to protect the circuit. For AC circuits, see AC Current, page A-14. For DC currents, see DC Current, page A-16.

Bare conductors must be coated with antioxidant before crimp connections are made. Only copper cables can be used for grounding purposes.

DC Supplies

The DC power supplies have additional ground connections on each supply. This allows the hot-swappable supply to be connected to power, return and ground so that it may be safely inserted. This ground lug must be attached.

It is a M4 screw with an outside-toothed lock washer screw.

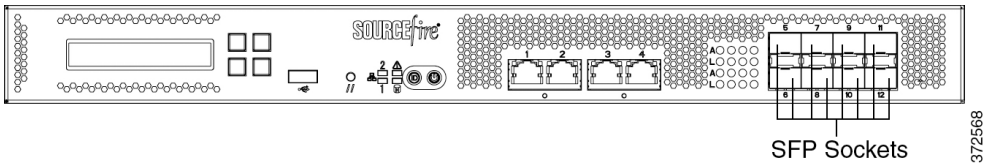
The ground wire should be sized to match the breaker for the circuit.

Using SFP Transceivers in 3D71x5 and AMP7150 Devices

3D71x5 and AMP7150 SFP Sockets and Transceivers

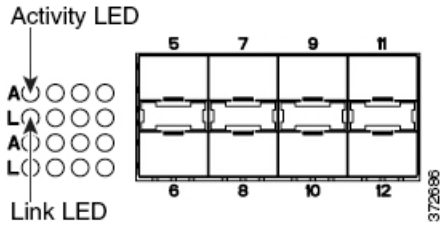
The 3D71x5 and AMP7150 appliances contain eight small form-factor pluggable (SFP) sockets and can house up to eight SFP transceivers.

Figure B-1 3D71x5 and AMP7150 Front View



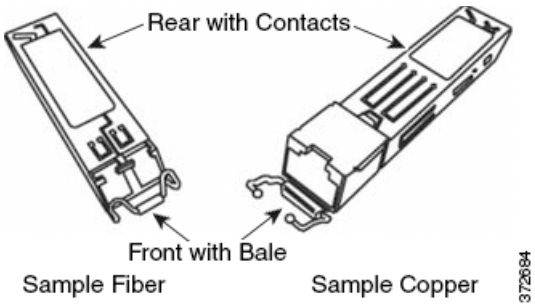
3D71x5 and AMP7150 SFP Sockets

The eight SFP sockets are numbered from 5 through 12 in a vertical pattern, and oriented in a tab-to-center configuration (the upper row faces up and the lower row faces down).



The accompanying LEDs to the left of the sockets display information on activity and link for each interface. See Firepower 7115, 7125, and AMP7150 SFP Socket Activity/Link LEDs for more information.

Sample SFP Transceivers



The 3D71x5 and AMP7150 can support up to eight SFP transceivers in any combination of three formats:

- SFP-C-1: copper transceiver
- SFP-F-1-SR: short range fiber transceiver
- SFP-F-1-LR: long range fiber transceiver

Use only Cisco SFP transceivers in the 3D71x5 and AMP7150. Non-Cisco SFP transceivers can jam in the socket and can cause permanent damage to the transceiver, the chassis, or both.

You can insert or remove transceivers while the device remains functioning. Refresh the user interface on the Management Center to see the change in configuration.

SFP transceivers do not have bypass capability. Use these transceivers in a passive deployment or an inline deployment where you want your device to stop all traffic if the device fails or loses power (for example, virtual switches, virtual routers, and some access control policies).

For a passive deployment, you can use any combination of transceivers in up to eight sockets to monitor up to eight network segments. For an inline deployment, you can use any combination (copper, fiber, or mixed) of transceivers in vertically sequential sockets (5 and 6, 7 and 8, 9 and 10, or 11 and 12) to monitor up to four network segments.

Use the Management Center that manages your device to configure the ports on the transceivers.

Inserting an SFP Transceiver

Use appropriate electrostatic discharge (ESD) procedures when inserting the transceiver. Avoid touching the contacts at the rear, and keep the contacts and ports free of dust and dirt.

Caution Do not force an SFP transceiver into a socket as this can jam the transceiver and can cause permanent damage to the transceiver, the chassis, or both.

To insert an SFP transceiver:

Step 1 Taking care not to touch the contacts in the rear, use your fingers to grasp the sides of the bale and slide the rear of the transceiver into a socket on the chassis. Note that sockets on the upper row face up and sockets on the lower row face down.

Step 2 Gently push the bale toward the transceiver to close the bale and engage the locking mechanism, securing the transceiver in place.

Step 3 Follow the procedure in Installing a Firepower Managed Device, page 4-1 to configure the port on the transceiver.

Note that if you insert a transceiver into a device currently in operation, you must refresh the user interface on the Management Center to view the change.

Removing an SFP Transceiver

Use appropriate electrostatic discharge (ESD) procedures when removing the transceiver. Avoid touching the contacts at the rear, and keep the contacts and ports free of dust and dirt.

To remove an SFP transceiver:

Step 1 Disconnect all cables from the transceiver you want to remove from the device.

Step 2 Using your fingers, gently pull the bale of the transceiver away from the chassis to disengage the connecting mechanism.

For transceivers in the upper row, pull down. For transceivers in the lower row, lift up.

Step 3 Using your fingers, grasp the sides of the bale and use the bale as a handle to gently pull the transceiver out of the chassis, taking care not to touch the contacts at the back of the transceiver.

Inserting and Removing Firepower 8000 Series Modules

Firepower 8000 Series devices allow for modular flexibility in your deployment. Use the steps in this section to:

- insert a new module
- remove or replace a preinstalled module

Module Slots on the Firepower 8000 Series Devices

Firepower 8000 Series devices can use the modules in the following slots:

- Firepower 81xx Family, page C-1
- Firepower 82xx Family and 83xx Family, page C-2

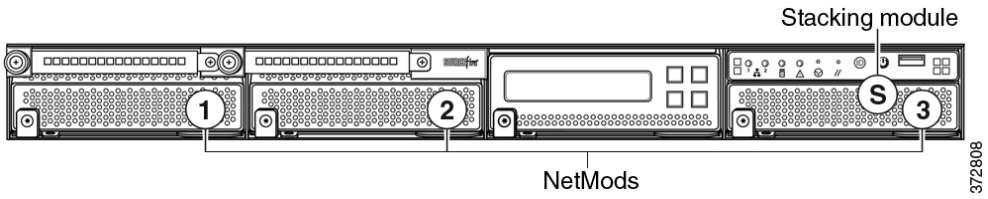
After you insert the modules into your device, see the following sections for more information on using the modules:

- For information on configuring the sensing interfaces, see Identifying the Sensing Interfaces, page 4-3.
- For information on using the stacking module, see Using Devices in a Stacked Configuration, page 4-13.

Firepower 81xx Family

Firepower 81xx Family devices can use the modules in the following slots:

Figure C-1 Firepower 81xx Family Primary Device



Stacking Configuration Considerations

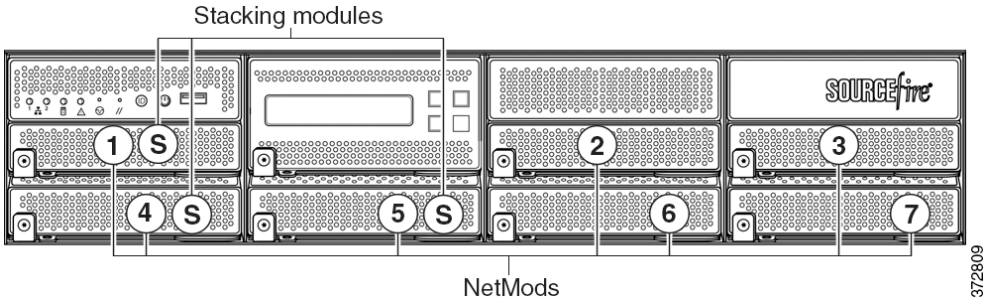
Configure the modules as follows for stacked devices:

- Install NetMods on the primary device only.
- Install one stacking module on the primary device and one stacking module on the secondary device.

Firepower 82xx Family and 83xx Family

Firepower 82xx Family and 83xx Family devices can use the modules in the following slots:

Figure C-2 Firepower 82xx Family and 83xx Family Primary Device

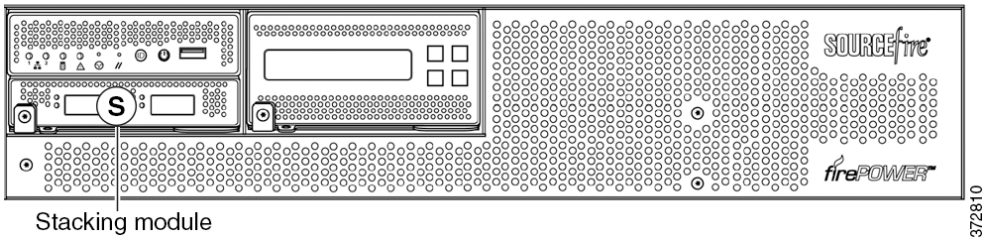


Stacking Configuration Considerations

Configure the modules as follows for stacked devices:

- Install NetMods on the primary device only.
- Install one stacking module on the primary device for each stacked secondary device, and one stacking module on each secondary device.

Figure C-3 Firepower 82xx Family and 83xx Family Secondary Device



Included Items

Your module assembly kit includes a T8 Torx screwdriver and one or more of the following modules:

- quad-port 1000BASE-T copper configurable bypass NetMod. For more information, see Quad-Port 1000BASE-T Copper Configurable Bypass NetMod, page 7-33.
- quad-port 1000BASE-SX fiber configurable bypass NetMod. For more information, see Quad-Port 1000BASE-SX Fiber Configurable Bypass NetMod, page 7-33.

- dual-port 10GBASE (MMSR or SMLR) fiber configurable bypass NetMod. For more information, see Dual-Port 10GBASE (MMSR or SMLR) Fiber Configurable Bypass NetMod, page 7-35.
- dual-port 40GBASE-SR4 fiber configurable bypass NetMod. For more information, see Dual-Port 40GBASE-SR4 Fiber Configurable Bypass NetMod, page 7-36.

Note Use this dual-slot NetMod only on the 40G-capacity Firepower 8250 or Firepower or AMP 8350. If you need to upgrade your device, see the *Cisco 8000 Series Device 40G Capacity Upgrade Guide*.

- quad-port 1000BASE-T copper non-bypass NetMod. For more information, see Quad-Port 1000BASE-T Copper Non-Bypass NetMod, page 7-38.
- quad-port 1000BASE-SX fiber non-bypass NetMod.quad-port 1000BASE-SX fiber non-bypass NetMod. For more information, see Quad-Port 1000BASE-SX Fiber Non-Bypass NetMod, page 7-39.
- quad-port 10GBASE (MMSR or SMLR) fiber non-bypass NetMod. For more information, see Quad-Port 10GBASE (MMSR or SMLR) Fiber Non-Bypass NetMod, page 7-39.

Caution The quad-port 10GBASE fiber non-bypass NetMod contains non-removable small form factor pluggable (SFP) transceivers. Any attempt to remove the SFPs can damage the module.

- stacking module. For more information, see Stacking Module, page 7-41.

If you install a NetMod in an incompatible slot on your Firepower device or a NetMod is otherwise incompatible with your system, an error or warning message appears in the web interface on the managing Management Center when you attempt to configure the NetMod. Contact support for assistance.

Note Replacing a NetMod can alter the configuration of a fully configured Korean-certified (KCC mark) Firepower device. For more information, see the original configuration documentation for your appliance and the *Regulatory Compliance and Safety Information for FirePOWER and FireSIGHT Appliances* document.

Identifying the Module Parts

All modules contain the same parts, regardless of sensing interface, speed, or size of the module.

Figure C-4 Sample Module or Slot Cover (open)

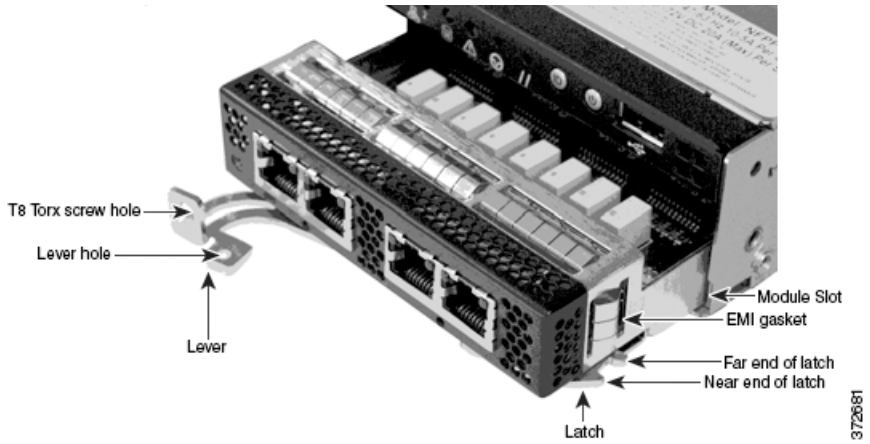
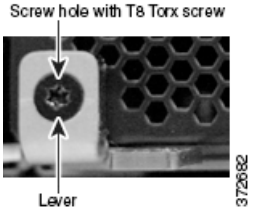


Figure C-5 Sample Module Lever (closed with screw in hole)



Before You Begin

Prepare to insert or remove your module using the following guidelines:

- Identify all appliance and module parts.
- Identify the slots where you want to install your NetMods.

Tip You can insert the NetMod into any available, compatible slot.

- Identify the correct slots for your stacking modules. See Using Devices in a Stacked Configuration, page 4-13.
- Firepower 8140: slot 3
- Firepower 8250, 8260 and 8350, 8360 primary slot: slot 5
- Firepower 8270 and 8370 primary slots: slots 5 and 1
- Firepower 8290 and 8390 primary slots: slots 5, 1, and 4
- Firepower 82xx and 83xx secondary: slot S
- Confirm that the EMI gaskets are in place.
- Unplug all power cords from the appliance.

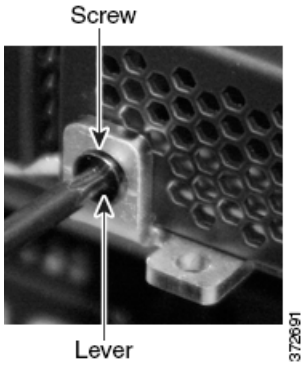
Caution You **cannot** hot-swap modules. You must power down and unplug **both** power cords from the appliance before inserting or removing modules.

Removing a Module or Slot Cover

Use proper electrostatic discharge (ESD) practices such as wearing wrist straps and using an ESD work surface when handling the modules. Store unused modules in an ESD bag or box to prevent damage.

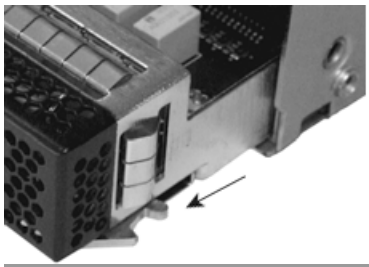
To remove a module or slot cover:

Step 1 Remove and reserve the T8 Torx screw from the lever of the module using the included screwdriver.



Step 2 Pull the lever away from the module to release the latch.

Step 3 Slide the module out of the slot.



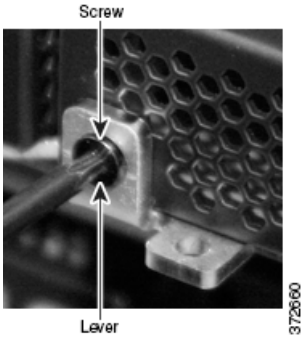
Inserting a Module or Slot Cover

Before You Begin

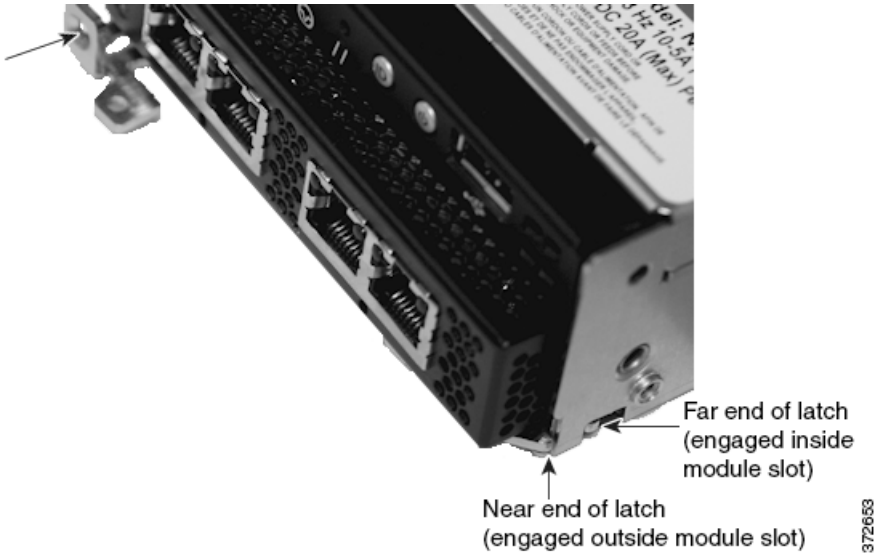
- Remove the existing module or slot cover to prepare the slot for a new module. See Removing a Module or Slot Cover, page C-5 for more information.

To insert a module or slot cover:

Step 1 Remove and reserve the T8 Torx screw from the lever of the module using the included screwdriver.

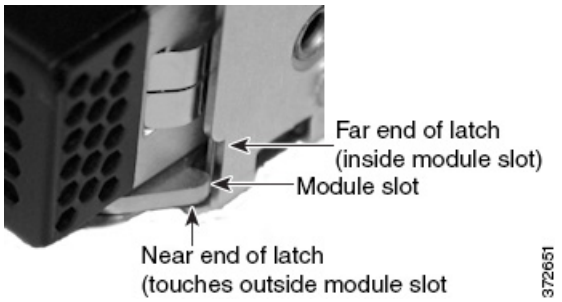


Step 2 Pull the lever away from the module to open the latch. The near end of the latch is visible. The far end of the latch is inside the module.

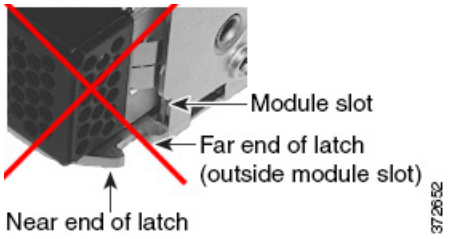


Step 3 Insert the module into the slot until the far end of the latch is inside the slot and the near end of the latch touches the outside of the module slot.

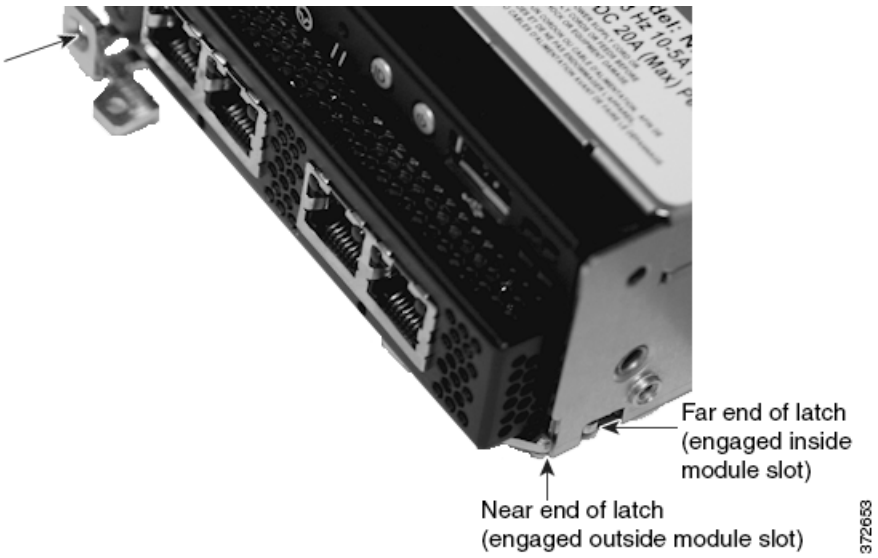
Correct module alignment



Incorrect module alignment



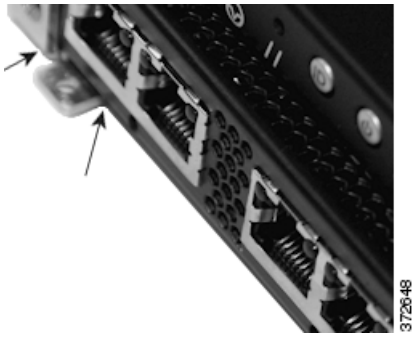
Step 4 Push the lever toward the module so that the latch engages and pulls the module into the slot.



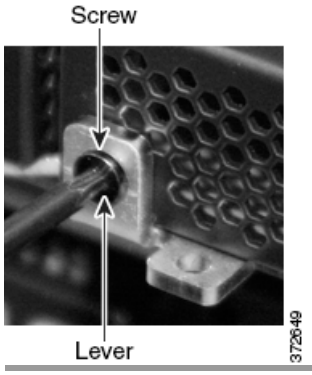
Caution Do **not** use excessive force. If the latch does not engage, remove and realign the module, then try again.

Step 5 Press firmly on the screw hole to push the lever fully against the module to secure the latch.

The lever is fully against the module, and the module is flush with the chassis.



Step 6 Insert and tighten the reserved T8 Torx screw into the lever.



Scrubbing the Hard Drive

You can securely scrub the hard drive on Management Centers and Firepower devices to ensure that its contents can no longer be accessed. For example, if you need to return a defective appliance that contains sensitive data, you can use this feature to overwrite the data.

Scrubbing the Contents of the Hard Drive

This mode of scrubbing the disk meets the following military standard:

STANDARDS

The DoD scrub sequence is compliant with the DoD 5220.22-M procedure for sanitizing removable and non-removable rigid disks which requires overwriting all addressable locations with a character, its complement, then a random character, and verify. Please refer to the DoD document for additional constraints.

Caution Scrubbing your hard drive results in the loss of all data on the appliance, which is rendered inoperable.

You scrub the hard drive using an option in the interactive menu described in Using the Interactive Menu to Restore an Appliance, page 8-6.

To scrub the hard drive:

Access: Admin

Step 1 Follow the instructions in one of the following sections to display the restore utility's interactive menu, depending on how you are accessing the appliance:

- Starting the Restore Utility Using KVM or Physical Serial Port, page 8-4
- Starting the Restore Utility Using Lights-Out Management, page 8-5

Step 2 From the main menu, select **8 Wipe Contents of Disk**.

Step 3 When prompted, confirm that you want to scrub the hard drive.

The hard drive is scrubbed. The scrub process may take several hours to complete; larger drives take longer.

Preconfiguring Firepower Managed Devices

You can preconfigure your Firepower devices at a *staging* location (a central location to preconfigure or stage multiple appliances) to be deployed at a *target* location (any location other than the staging location).

To preconfigure and deploy an appliance to a target location, perform the following steps:

- install the system on the device at the staging location
- optionally, register the device to a Management Center
- optionally, push any updates from the managing Management Center to the device
- optionally, unregister the device from the Management Center
- shut down and ship the appliance to the target location
- deploy the appliances in the target locations

Tip Save all packing materials and include all reference material and power cords when repackaging the appliance.

Before You Begin

Before preconfiguring the appliance, collect the network settings, licenses, and other pertinent information for the staging location and the target location.

Tip It can be helpful to create a spreadsheet to manage this information at the staging location and the target location.

During the initial setup, you configure your appliance with enough information to connect the appliance to the network and install the system. Optionally, you can connect a device to a Management Center to push any updates from the Management Center to the device. You can also enable other features that are not required for initial setup but can be useful to preconfigure.

Required Preconfiguration Information

At a minimum, you need the following information to preconfigure your appliance:

- the new password (initial setup requires changing the password)

- the hostname of the appliance
- the domain name of the appliance
- the IP management address of the appliance
- the network mask of the appliance at the target location
- the default gateway of the appliance at the target location
- the IP address of the DNS server at the staging location, or, if accessible, the target location
- the IP address of the NTP server at the staging location, or, if accessible, the target location
- the detection mode for the target location

Optional Preconfiguration Information

You can change some default configurations, such as:

- allow access to the LCD panel to configure Firepower devices
- set the time zone if you choose to manually set the time for your appliances
- set the remote storage location for automatic backups
- set the Lights-Out Management (LOM) IP address to enable LOM

Note In some power cycle scenarios, the baseboard management controller (BMC) of a Firepower 7050 connected to the network via the management interface could lose the IP address assigned to it by the DHCP server. Because of this, Cisco recommends you configure the Firepower 7050 BMC with a static IP address. Alternately, you can disconnect the network cable and reconnect it, or remove and restore power to the device to force renegotiation of the link.

If you want to register a device to a Management Center, you need the following information:

- the name or IP address of the managed device
- the name of the management host (the Management Center)
- the registration key (a personally created unique alphanumeric key up to 37 characters in length)

Preconfiguring Time Management

Keep in mind the following considerations:

- Cisco recommends that you synchronize time to a physical NTP server. Do not synchronize managed devices to a virtual Management Center. Performance optimization on a virtual appliance can affect the real time clock.
- If the network at your staging location can access the DNS and NTP servers at the target location, use the IP addresses for the DNS and NTP servers at the target location. If not, use the staging location information and reset at the target location.
- Use the time zone for the target deployment if you set the time on the appliance to the manually instead of using NTP. See Time Settings, page 5-7.

Installing the System

Use the installation procedures described in Installing a Firepower Managed Device, page 4-1 and Setting Up Firepower Managed Devices, page 5-1. When preconfiguring the system, keep the following in mind:

- If you allow access to a Firepower device's network settings using the LCD panel, you introduce a security risk where unauthorized changes can be made by physically accessing the device. See Firepower Device LCD Panel Configuration, page 5-7.
- Pre-register a device using the host name or IP address of the Management Center in the target deployment. Note the registration key for later in completing the registration. See Remote Management, page 5-7.
- If you change the default detection mode, be sure to notify the appropriate personnel at the target deployment. Configuring interfaces differently from the detection mode can cause the system to incorrectly assign interfaces. See Detection Mode, page 5-8.
- If you need to configure Network Address Translation (NAT) for your device, provide the NAT ID of the device when registering the device using either the CLI on the device or the web interface on its managing Management Center. See Registering a Firepower Device to a Management Center Using the CLI, page 5-4 and Working In NAT Environments in the *Firepower Management Center Configuration Guide*.
- Add licenses during the initial setup. If you do not add licenses at that time, any devices you register during initial setup are added to the Firepower Management Center as unlicensed; you must license each of them individually after the initial setup process is over. See *Firepower Management Center Installation Guide* for more information.

Registering a Device

Access: Admin

You can register a device to a Management Center to push policies and updates to the managed device if your Management Center is running a software version equal to or greater than the software version on the device.

Note If you deploy the Management Center and its managed device in different target locations, you must delete the device from the Management Center before shutting down the appliances. See Deleting Devices from a Management Center, page E-4.

To register a device to a Management Center:

Step 1 On the device, configure remote management using the host name or IP address of the Management Center in the target deployment. Note the registration key for later use in completing the registration. See Remote Management, page 5-7.

Note You must configure remote management on the device before you can register the device to a Management Center.

What to Do Next

- On the Management Center, register the device using the registration information from your remote management configuration. See the *Firepower Management Center Installation Guide* for more information.

Preparing the Appliance for Shipment

To prepare the appliance for shipment, you must safely power down and repackage the appliance:

- If your managed device will not be used in the same configuration at the target location, you must delete the device from the Management Center, then power down and repackage the appliances. See Deleting Devices from a Management Center, page E-4.
- To safely power down the appliance, see Powering Down the Appliance, page E-5.
- To ensure that your appliance is safely prepared for shipping, see Shipping Considerations, page E-5.

Deleting Devices from a Management Center

Access: Admin

Unless you deploy the Management Center and its managed device at the same target location, you must delete the device from the Management Center. This prevents the device from looking for the UUID of the original Management Center when you register the device to a different Management Center at the target location.

To delete a device from the Management Center:

Step 1 On the Management Center, Select **Devices > Device Management**.

Step 2 Next to the device you want to delete, click the delete icon ().

When prompted, confirm that you want to delete the device. Communication between the device and the Management Center is discontinued and the device is deleted from the Device Management page. If the device has a system policy that causes it to receive time from the Management Center via NTP, the device reverts to local time management.

After deleting the device from the Management Center, verify that the device is not remotely managed by the Management Center.

To verify that a Firepower device is not managed by a Management Center:

Step 1 On the Firepower device, you can use either the web interface or the CLI:

- On the web interface of the Firepower device, go to **System > Registration > Remote Management** and confirm that the Host list on the Remote Management screen is empty.
- On the CLI of the Firepower device, run the command `show manager` and confirm that no host is displayed.

Deleting a License from a Management Center

Access: Admin

Use the following procedure if you need to delete a license for any reason. Keep in mind that, because Cisco generates licenses based on each Management Center's unique license key, you cannot delete a license from one Management Center and reuse it on a different Management Center. For more information, see See Licensing the Firepower System in the *Firepower Management Center Configuration Guide*.

To delete a license:

Step 1 Select **Systems > Licenses**.

Step 2 Next to the license you want to delete, click the delete icon ( ).

Deleting a license removes the licensed capability from all devices using that license. For example, if your Protection license is valid and enabled for 100 managed devices, deleting the license removes protection capabilities from all 100 devices.

Step 3 Confirm that you want to delete the license.

The license is deleted.

Powering Down the Appliance

Access: Admin

Use the following procedures to power down the appliance safely before disconnecting the power supply.

To power down a Firepower device:

Step 1 On the device, enter the following at the command line:

```
system shutdown
```

The device shuts down safely.

Shipping Considerations

To prepare the appliance for shipment to the target location, you must safely power down and repackage the appliance. Keep in mind the following considerations:

- Use the original packaging to repack the appliance.
- Include all reference material and power cords with the appliance.
- Protect the NetMods and SFPs from damage caused by improper handling or undue pressure.
- Provide all setting and configuration information to the target location, including the new password and the detection mode.

Troubleshooting the Appliance Preconfiguration

If your appliance is correctly preconfigured for target deployment, you can install and deploy the appliance without further configuration.

If you have difficulty logging into the appliance, the preconfiguration may have an error. Try the following troubleshooting procedures:

- Confirm that all power cables and communication cables are connected properly to the appliance.
- Confirm that you have the current password for your appliance. The initial setup at the staging location prompts you to change your password. See the configuration information provided by the staging location for the new password.
- Confirm that the network settings are correct. See Initial Setup Page: Firepower Devices, page 5-5 .
- Confirm that the correct communication ports are functioning properly. See the documentation for your firewall for information on managing firewall ports. See Communication Ports Requirements, page 1-14 for required open ports.
- If you use a Network Address Translation (NAT) appliance in your deployment, confirm that NAT is configured correctly. See Working in NAT Environments in the *Firepower Management Center Configuration Guide*.

If you continue to experience difficulty, contact your IT department.