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.