Security, Internet Access, and Communication Ports

The following topics provide information on system security, internet access, and communication ports:

Security Requirements

To safeguard the Firepower Management Center, you should install it on a protected internal network. Although the FMC 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 FMC 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 FMC. This allows you to securely control the devices from the FMC. You can also configure multiple management interfaces to allow the FMC to manage and isolate traffic from devices on other networks.

Regardless of how you deploy your appliances, inter-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.

Cisco Clouds

The Firepower System uses Cisco's Collective Security Intelligence (CSI) cloud to obtain the threat intelligence data it uses to assess risk for files and to obtain URL category and reputation. With the correct licenses, you can specify communications options for the AMP for Networks and URL Filtering features.

Additional information:

- **Advanced Malware Protection**

  The public cloud is configured by default; to make changes, see Change AMP Options.

- **URL filtering**

For information, see:

- URL Filtering Options
- Enable URL Filtering Using Category and Reputation

Internet Access Requirements

By default, the system is configured to connect to the internet on ports 443/tcp (HTTPS) and 80/tcp (HTTP). If you do not want your appliances to have direct access to the internet, you can configure a proxy server. For many features, your location can determine which resources the system access.

In most cases, it is the FMC that accesses the internet. Both FMCs in a high availability pair should have internet access. Depending on the feature, sometimes both peers access the internet, and sometimes only the active peer does.

Sometimes, managed devices also access the internet. For example, if your malware protection configuration uses dynamic analysis, managed devices submit files directly to the Threat Grid cloud. Or, you may synchronize a device to an external NTP server.

Table 1: Internet Access Requirements

Feature	Reason	FMC High Availability	Resource
AMP for Networks	Malware cloud lookups.	Both peers perform lookups.	See Required Server Addresses for Proper Cisco Secure Endpoint & Malware Analytics Operations.
	Download signature updates for file preclassification and local malware analysis.	Active peer downloads, syncs to standby.	updates.vrt.sourcefire.com amp.updates.vrt.sourcefire.com
	Submit files for dynamic analysis (managed devices). Query for dynamic analysis results (FMC).	Both peers query for dynamic analysis reports.	fmc.api.threatgrid.com fmc.api.threatgrid.eu
AMP for Endpoints integration	Receive malware events detected by AMP for Endpoints from the AMP cloud. Display malware events detected by the Firepower system in AMP for Endpoints. Use centralized file Block and Allow lists created in AMP for Endpoints to override dispositions from the AMP cloud.	Both peers receive events. You must also configure the cloud connection on both peers (configuration is not synced).	See Required Server Addresses for Proper Cisco Secure Endpoint & Malware Analytics Operations.
Security Intelligence	Download Security Intelligence feeds.	Active peer downloads, syncs to standby.	intelligence.sourcefire.com

Feature	Reason	FMC High Availability	Resource
URL filtering	Download URL category and reputation data. Manually query (look up) URL category and reputation data. Query for uncategorized URLs.	Active FMC downloads, syncs to standby.	database.brightcloud.com service.brightcloud.com
Cisco Smart Licensing	Communicate with the Cisco Smart Software Manager.	Active peer communicates.	tools.cisco.com:443 www.cisco.com
System updates	Download updates *directly* to the FMC: • System software • Intrusion rules • Vulnerability database (VDB) • Geolocation database (GeoDB)	Update intrusion rules, the VDB, and the GeoDB on the active peer, which then syncs to the standby. Upgrade the system software independently on each peer. See the Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0.	cisco.com sourcefire.com
Time synchronization	Synchronize time in your deployment. Not supported with a proxy server.	Any appliance using an external NTP server must have internet access.	0.sourcefire.pool.ntp.org 1.sourcefire.pool.ntp.org 2.sourcefire.pool.ntp.org 3.sourcefire.pool.ntp.org
RSS feeds	Display the Cisco Threat Research Blog on the dashboard.	Any appliance displaying RSS feeds must have internet access.	feeds.feedburner.com
Whois	Request whois information for an external host. Not supported with a proxy server.	Any appliance requesting whois information must have internet access.	The whois client tries to guess the right server to query. If it cannot guess, it uses: • NIC handles: whois.networksolutions.com • IPv4 addresses and network names: whois.arin.net

Communication Port Requirements

Firepower appliances communicate using a two-way, SSL-encrypted communication channel on port 8305/tcp. This port *must* remain open for basic intra-platform communication.

Other ports allow secure management, as well as access to external resources required by specific features. In general, feature-related ports remain closed until you enable or configure the associated feature. Do *not* change or close an open port until you understand how this action will affect your deployment.

Security, Internet Access, and Communication Ports

Table 2: Firepower Communication Port Requirements

Port	Protocol/Feature	Platforms	Direction	Details
7/UDP	UDP/audit logging	FMC, classic	Outbound	Verify connectivity with the syslog server when configuring audit logging.
22/tcp	SSH	FMC Any device	Inbound	Secure remote connections to the appliance.
25/tcp	SMTP	FMC	Outbound	Send email notices and alerts.
53/tcp 53/udp	DNS	FMC Any device	Outbound	DNS
67/udp 68/udp	DHCP	FMC Any device	Outbound	DHCP
80/tcp	HTTP	FMC 7000/8000 series	Outbound	Display RSS feeds in the dashboard.
80/tcp	HTTP	FMC	Outbound	Download or query URL category and reputation data (port 443 also required).
80/tcp	HTTP	FMC	Outbound	Download custom Security Intelligence feeds over HTTP.
123/udp	NTP	FMC Any device	Outbound	Synchronize time.
161/udp	SNMP	FMC Any device	Inbound	Allow access to MIBs via SNMP polling.
162/udp	SNMP	FMC Any device	Outbound	Send SNMP alerts to a remote trap server.
389/tcp 636/tcp	LDAP	FMC FTD 7000/8000 series	Outbound	Communicate with an LDAP server for external authentication. Obtain metadata for detected LDAP users (FMC only). Configurable.
443/tcp	HTTPS	FMC 7000/8000 series	Inbound	Access the web interface.
443/tcp	Remote access VPN (SSL/IPSec)	FTD	Inbound	Allow secure VPN connections to your network from remote users.

Port	Protocol/Feature	Platforms	Direction	Details
500/udp 4500/udp	Remote access VPN (IKEv2)	FTD	Inbound	Allow secure VPN connections to your network from remote users.
443/tcp	HTTPS	FMC FTD	Inbound	Communicate with integrated and third-party products using the Firepower REST API, including Cisco Terminal Services (TS) Agent.
443/tcp	HTTPS	FMC Any device	Outbound	Send and receive data from the internet. For details, see Internet Access Requirements, on page 2.
443	HTTPS	FMC	Outbound	Communicate with the AMP cloud (public or private) See also information for port 32137.
443	HTTPS	FMC	Inbound and Outbound	Integrate with AMP for Endpoints
514/udp	Syslog (alerts)	FMC Any device	Outbound	Send alerts to a remote syslog server.
623/udp	SOL/LOM	FMC 7000/8000 series	Inbound	Lights-Out Management (LOM) using a Serial Over LAN (SOL) connection.
885/tcp	Captive portal	Any device	Inbound	Communicate with a captive portal identity source.
1500/tcp 2000/tcp	Database access	FMC	Inbound	Allow read-only access to the event database by a third-party client.
1812/udp 1813/udp	RADIUS	FMC FTD 7000/8000 series	Outbound	Communicate with a RADIUS server for external authentication and accounting. Configurable.
3306/tcp	User Agent	FMC	Inbound	Communicate with User Agents.
5222/tcp	ISE	FMC	Outbound	Communicate with an ISE identity source.
6514/tcp	Syslog (audit events)	FMC 7000/8000 series NGIPSv ASA FirePOWER	Outbound	Send audit logs to a remote syslog server, when TLS is configured.
8302/tcp	eStreamer	FMC 7000/8000 series	Inbound	Communicate with an eStreamer client.

Security, Internet Access, and Communication Ports

Port	Protocol/Feature	Platforms	Direction	Details
8305/tcp	Appliance communications	FMC Any device	Both	Securely communicate between appliances in a deployment. Configurable. If you change this port, you must change it for *all* appliances in the deployment. We recommend you keep the default.
8307/tcp	Host input client	FMC	Inbound	Communicate with a host input client.
32137/tcp	AMP for Networks	FMC	Outbound	Communicate with the Cisco AMP cloud. This is a legacy configuration. We recommend you use the default (443).

Related Topics

Identifying the LDAP Authentication Server
Configuring RADIUS Connection Settings