Security, Internet Access, and Communication Ports

Tip If you are using AMP for Networks or AMP for Endpoints, your location can determine which AMP cloud resources the FMC accesses. The Required Server Addresses for Proper AMP Operations Troubleshooting TechNote lists the internet resources (including static IP addresses) required not only by Firepower appliances, but also by Cisco AMP components like connectors and private cloud appliances.

Table 1: Firepower Internet Access Requirements

Feature	Reason	Resource
AMP for Networks	Malware cloud lookups.	cloud-sa.amp.sourcefire.com cloud-sa.eu.amp.sourcefire.com cloud-sa.apjc.amp.sourcefire.com cloud-sa-589592150.us-east-1.elb.amazonaws.com
	Download signature updates for file preclassification and local malware analysis.	updates.vrt.sourcefire.com amp.updates.vrt.sourcefire.com
	Submit files for dynamic analysis (managed devices). Query for dynamic analysis results (FMC).	panacea.threatgrid.com
AMP for Endpoints integration	Receive malware events detected by AMP for Endpoints from the AMP cloud.	api.amp.sourcefire.com api.eu.amp.sourcefire.com api.apjc.amp.sourcefire.com export.amp.sourcefire.com export.eu.amp.sourcefire.com export.apjc.amp.sourcefire.com
Security Intelligence	Download Security Intelligence feeds.	intelligence.sourcefire.com
URL filtering	Download URL category and reputation data. Manually query URL category and reputation data. Query for uncategorized URLs.	database.brightcloud.com service.brightcloud.com
System updates	Download updates *directly* from Cisco to the appliance: • System software • Intrusion rules • Vulnerability database (VDB) • Geolocation database (GeoDB)	cisco.com sourcefire.com

Feature	Reason	Resource
Time synchronization	Synchronize time in your deployment. Not supported with a proxy server.	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.	blogs.cisco.com/talos cloud.google.com
Whois	Request whois information for an external host. Not supported with a proxy server.	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.

Table 2: Firepower Communication Port Requirements

Port	Protocol/Feature	Platforms	Direction	Details
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).

Security, Internet Access, and Communication Ports

Port	Protocol/Feature	Platforms	Direction	Details
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 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	HTTPS	FMC Any device	Outbound	Send and receive data from the internet. For details, see Internet Access Requirements, on page 1.
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 7000 & 8000 Series	Outbound	Communicate with a RADIUS server for external authentication and accounting. Configurable.

Security, Internet Access, and Communication Ports

Port	Protocol/Feature	Platforms	Direction	Details
3306/tcp	User Agent	FMC	Inbound	Communicate with User Agents.
5222/tcp	ISE	FMC	Outbound	Communicate with an ISE identity source.
8302/tcp	eStreamer	FMC 7000 & 8000 Series	Inbound	Communicate with an eStreamer client.
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