Security, Internet Access, and Communication Ports

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

Security Requirements

To safeguard the Secure Firewall Management Center, you should install it on a protected internal network. Although the 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 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 management center. This allows you to securely control the devices from the management center. You can also configure multiple management interfaces to allow the management center 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 management center communicates with resources in the Cisco cloud for the following features:

- **Advanced Malware Protection**

  The public cloud is configured by default; to make changes, see *Change AMP Options* in the Cisco Secure Firewall Management Center Device Configuration Guide.

- **URL filtering**

  For more information, see the *URL filtering* chapter in the Cisco Secure Firewall Management Center Device Configuration Guide.

- **Integration with Security Analytics and Logging (SaaS)**

  See Remote Data Storage in Cisco Secure Cloud Analytics.

- **Integration with Cisco XDR**

  For details, see the Cisco Secure Firewall Threat Defense and Cisco XDR Integration Guide

- **The proactive support feature**

  For information, see Configure Cisco Support Diagnostics Enrollment.

- **Cisco Success Network**

  For information, see Configure Management Center to Share Usage Metrics and Statistics with Cisco.

- **Cisco Umbrella Connection**

  For information, see *DNS Policies* in the Cisco Secure Firewall Management Center Device Configuration Guide.

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 can access.

In most cases, it is the management center that accesses the internet. Both management centers 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 Secure Malware Analytics cloud. Or, you may synchronize a device to an external NTP server.

Additionally, unless you disable web analytics tracking, your browser may contact Amplitude (amplitude.com) web analytics servers to provide non-personally-identifiable usage data to Cisco.

Table 1: Internet Access Requirements

Feature	Reason	Management Center High Availability	Resource
Malware defense	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 (management center).	Both peers query for dynamic analysis reports.	fmc.api.threatgrid.com fmc.api.threatgrid.eu
AMP for Endpoints	Receive malware events detected by AMP for Endpoints from the AMP cloud. Display malware events detected by the 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.
Event enrichment	Download Talos taxonomy. Query Talos Cloud Services for event enrichment.	Both peers communicate independently with Talos Cloud Services.	URL: • *.talos.cisco.com IPv4 blocks: • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 IPv6 blocks: • 2a04:e4c7:ffff::/48 • 2a04:e4c7:fffe::/48
Security intelligence	Download security intelligence feeds.	Active peer downloads, syncs to standby.	intelligence.sourcefire.com

Feature	Reason	Management Center 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 peer downloads, syncs to standby.	URLs: • *.talos.cisco.com • updates-talos.sco.cisco.com • updates-dyn-talos.sco.cisco.com • updates.ironport.com IPv4 blocks: • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 IPv6 blocks: • 2a04:e4c7:ffff::/48 • 2a04:e4c7:fffe::/48
Cisco Secure Dynamic Attributes Connector	Get packages from the Amazon Elastic Container Registry (Amazon ECR)	Both peers communicate.	public.ecr.aws csdac-cosign.s3.us-west-1.amazonaws.com
Cisco Smart Licensing	Communicate with the Cisco Smart Software Manager.	Active peer communicates.	smartreceiver.cisco.com www.cisco.com
Cisco Success Network	Transmit usage information and statistics.	Active peer communicates.	api-sse.cisco.com:8989 dex.sse.itd.cisco.com dex.eu.sse.itd.cisco.com
Cisco Support Diagnostics	Accepts authorized requests and transmits usage information and statistics.	Active peer communicates.	api-sse.cisco.com:8989
Cisco XDR integration	See Cisco Secure Firewall Threat Defense and Cisco XDR Integration Guide.		
Time synchronization	Synchronize time in your deployment. Not supported with a proxy server.	Any appliance using an external NTP server must have internet access.	time.cisco.com
RSS feeds	Display the Cisco Threat Research Blog on the dashboard.	Any appliance displaying RSS feeds must have internet access.	blog.talosintelligence.com

Feature	Reason	Management Center High Availability	Resource
Updates	Download updates *directly* from Cisco to the management center: • System software • Intrusion rules (SRU/LSP) • 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.	amazonaws.com cisco.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

The management center communicates with managed devices using a two-way, SSL-encrypted communication channel on port 8305/tcp. This port *must* remain open for basic 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.

For information on internet resources the system may contact over these ports, see Internet Access Requirements, on page 2.

Ports for Management Center

Table 2: Inbound Ports for Management Center

Inbound Port	Protocol/Feature	Details
22/tcp	SSH	Secure remote connections to the appliance.
161/udp	SNMP	Allow access to MIBs via SNMP polling.
443/tcp	HTTPS	Access the web interface.
443/tcp	HTTPS	Onboard an on-prem management center to CDO with Secure Device Connector (on-prem).
443/tcp	HTTPS	Submit queries to Cisco Security Packet Analyzer.

Inbound Port	Protocol/Feature	Details
443/tcp	HTTPS	Communicate with integrated and third-party products using the REST API.
443/tcp	HTTPS	Integrate with Secure Endpoint. Outbound also required.
623/udp	SOL/LOM	Lights-Out Management (LOM) using a Serial Over LAN (SOL) connection.
1500/tcp 2000/tcp	Database access	Allow read-only access to the event database by a third-party client.
8302/tcp	eStreamer	Communicate with an eStreamer client.
8305/tcp	Appliance communications	Securely communicate between appliances in a deployment. Outbound also required. 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	Communicate with a host input client.
8989/tcp	Cisco Support Diagnostics	Accepts authorized requests and transmits usage information and statistics. Outbound also required.

Table 3: Outbound Ports for Management Center

Outbound Port	Protocol/Feature	Details
7/udp 514/udp 6514/tcp	Syslog (audit logging)	Verify connectivity with the syslog server when configuring audit logging (7/udp). Send audit logs to a remote syslog server, when TLS is not configured (514/udp). Send audit logs to a remote syslog server, when TLS is configured (6514/tcp).
25/tcp	SMTP	Send email notices and alerts.
53/tcp 53/udp	DNS	DNS
67/udp 68/udp	DHCP	DHCP
80/tcp	HTTP	Download custom Security Intelligence feeds over HTTP.
80/tcp	HTTP	Download or query URL category and reputation data. Outbound 443/tcp also required.
80/tcp	HTTP	Display RSS feeds in the dashboard.
123/udp	NTP	Synchronize time.
162/udp	SNMP	Send SNMP alerts to a remote trap server.

Outbound Port	Protocol/Feature	Details
389/tcp 636/tcp	LDAP	Communicate with an LDAP server for external authentication. Obtain metadata for detected LDAP users. Configurable.
443/tcp	HTTPS	Communicate with the Secure Malware Analytics Cloud (public or private).
443/tcp	HTTPS	Send and receive data from the internet.
443/tcp	HTTPS	Integrate with AMP for Endpoints. Inbound also required.
443/tcp	HTTPS	Onboard an on-prem management center to CDO with Cisco Security Cloud or Secure Device Connector (cloud).
1812/udp 1813/udp	RADIUS	Communicate with a RADIUS server for external authentication and accounting. Configurable.
5222/tcp	ISE	Communicate with an ISE identity source.
8305/tcp	Appliance communications	Securely communicate between appliances in a deployment. Inbound also required. Configurable. If you change this port, you must change it for *all* appliances in the deployment. We recommend you keep the default.
8989/tcp	Cisco Support Diagnostics	Accepts authorized requests and transmits usage information and statistics. Inbound also required.
8989/tcp	Cisco Success Network	Transmit usage information and statistics.

Ports for Managed Devices

Table 4: Inbound Ports for Managed Devices

Inbound Port	Protocol/Feature	Details
22/tcp	SSH	Secure remote connections to the appliance.
161/udp	SNMP	Allow access to MIBs via SNMP polling.
443/tcp	HTTPS	Communicate with integrated and third-party products using the REST API.
443/tcp	Remote access VPN (SSL/IPSec)	Allow secure VPN connections to your network from remote users.
500/udp 4500/udp	Remote access VPN (IKEv2)	Allow secure VPN connections to your network from remote users.
885/tcp	Captive portal	Communicate with a captive portal identity source.

Inbound Port	Protocol/Feature	Details
8305/tcp	Appliance communications	Securely communicate between appliances in a deployment. Outbound also required. Configurable. If you change this port, you must change it for *all* appliances in the deployment. We recommend you keep the default.
8989/tcp	Cisco Support Diagnostics	Accepts authorized requests and transmits usage information and statistics. Outbound also required.

Table 5: Outbound Ports for Managed Devices

Outbound Port	Protocol/Feature	Details
53/tcp 53/udp	DNS	DNS
67/udp 68/udp	DHCP	DHCP
123/udp	NTP	Synchronize time.
162/udp	SNMP	Send SNMP alerts to a remote trap server.
1812/udp 1813/udp	RADIUS	Communicate with a RADIUS server for external authentication and accounting. Configurable.
389/tcp 636/tcp	LDAP	Communicate with an LDAP server for external authentication. Configurable.
443/tcp	HTTPS	Send and receive data from the internet.
514/udp	Syslog (audit logging)	Send audit logs to a remote syslog server, when TLS is not configured.
8305/tcp	Appliance communications	Securely communicate between appliances in a deployment. Inbound also required. Configurable. If you change this port, you must change it for *all* appliances in the deployment. We recommend you keep the default.
8514/UDP	Secure Network Analytics Manager	Send syslog messages to Secure Network Analytics using Security Analytics and Logging (On Premises)
8989/tcp	Cisco Support Diagnostics	Accepts authorized requests and transmits usage information and statistics. Inbound also required.

Related Topics

Add an LDAP External Authentication Object for the Management Center
Add a RADIUS External Authentication Object for Management Center