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.

- **Cisco Umbrella Connection**

  For more information, see Cisco Umbrella DNS Policies.

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 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 Google (google.com) or 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.

Feature	Reason	Management Center High Availability	Resource
Security intelligence	Download security intelligence feeds.	Active peer downloads, syncs to standby.	intelligence.sourcefire.com
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: • regsvc.sco.cisco.com • est.sco.cisco.com • updates-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 Smart Licensing	Communicate with the Cisco Smart Software Manager.	Active peer communicates.	tools.cisco.com:443 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
System updates	Download updates *directly* from Cisco to the management center: • 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.	cisco.com sourcefire.com

Feature	Reason	Management Center High Availability	Resource
SecureX threat response integration	See the appropriate 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.	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.	blog.talosintelligence.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.

Table 2: Communication Port Requirements

Port	Protocol/Feature	Platforms	Direction	Details
53/tcp 53/udp	DNS		Outbound	DNS
67/udp 68/udp	DHCP		Outbound	DHCP
123/udp	NTP		Outbound	Synchronize time.
162/udp	SNMP		Outbound	Send SNMP alerts to a remote trap server.

Port	Protocol/Feature	Platforms	Direction	Details
389/tcp 636/tcp	LDAP		Outbound	Communicate with an LDAP server for external authentication. Obtain metadata for detected LDAP users (Management Center only). Configurable.
443/tcp	HTTPS	Management Center	Inbound	Allow inbound connection to port 443 if you are onboarding the management center with an on-premises Secure Device Connector.
443/tcp	HTPS	Management Center	Outbound	Allow outbound traffic from port 443 if onboarding the management center to CDO using the cloud connector.
443/tcp	HTPS	Management Center	Outbound	Allow outbound connection for port 443 if onboarding the management center using SecureX.
443/tcp	HTTPS		Outbound	Send and receive data from the internet.
514/udp	Syslog (alerts)		Outbound	Send alerts to a remote syslog server.
1812/udp 1813/udp	RADIUS		Outbound	Communicate with a RADIUS server for external authentication and accounting. Configurable.
8305/tcp	Appliance communications		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.

Related Topics

Add an LDAP External Authentication Object for CDO
Add a RADIUS External Authentication Object for CDO