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

Sometimes, managed devices must 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, your browser may contact Amplitude (amplitude.com) web analytics servers to provide non-personally-identifiable usage data to Cisco.

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 1: Inbound Ports for Management Center

Inbound Port	Protocol/Feature	Details
443/tcp	HTTPS	Access the web interface.
443/tcp	HTTPS	Submit queries to Cisco Security Packet Analyzer.
443/tcp	HTTPS	Communicate with integrated and third-party products using the REST API.
443/tcp	HTTPS	Integrate with Secure Endpoint. Outbound also required.
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 2: 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.
123/udp	NTP	Synchronize time.
162/udp	SNMP	Send SNMP alerts to a remote trap server.
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.
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.

Ports for Managed Devices

Table 3: 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.
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.

Table 4: 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.

Outbound Port	Protocol/Feature	Details
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)

Related Topics

Add an LDAP External Authentication Object for the CDO

Add a RADIUS External Authentication Object for CDO