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.

Table 1: 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.
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.

Port	Protocol/Feature	Platforms	Direction	Details
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 the CDO
Add a RADIUS External Authentication Object for CDO