Firewall Information

This chapter contains the following sections:

Firewall Information

The following table lists the possible ports that may need to be opened for proper operation of Cisco Secure Email Gateway (these are the default values).

Table 1: Firewall Ports

Default Port	Protocol	In/Out	Hostname	Purpose
20/21	TCP	In or out	AsyncOS IPs, FTP server	FTP for aggregation of log files. Data ports TCP 1024 and higher must also all be open. For more information, search for FTP port information in the Knowledge Base. See Knowledge Base.
22	TCP	In	AsyncOS IPs	SSH access to the CLI, aggregation of log files.
22	TCP	Out	SSH Server	SSH aggregation of log files.
22	TCP	Out	SCP server	SCP push to log server.
25	TCP	Out	Any	SMTP to send email.
25	TCP	In	AsyncOS IPs	SMTP to receive bounced email or if injecting email from outside firewall.

Firewall Information

53	UDP/TCP	Out	DNS servers	DNS if configured to use Internet root servers or other DNS servers outside the firewall. Also for SenderBase queries.
80	HTTP	In	AsyncOS IPs	HTTP access to the GUI for system monitoring.
80	HTTP	Out	downloads.ironport.com	and McAfee definitions.
80	HTTP	Out	updates.ironport.com	AsyncOS upgradesand McAfee definitions.
80	HTTP	Out	TAXII servers	Used to allow your email gateway to consume external threat feeds.
82	HTTP	In	AsyncOS IPs	Used for viewing the spam quarantine.
83	HTTPS	In	AsyncOS IPs	Used for viewing the spam quarantine.
110	TCP	Out	POP server	POP authentication for end users for spam quarantine.
123	UDP	In & Out	NTP server	NTP if time servers are outside firewall.
143	TCP	Out	IMAP server	IMAP authentication for end users for spam quarantine.
161	UDP	In	AsyncOS IPs	SNMP Queries.
162	UDP	Out	Management station	SNMP Traps.
389 or 3268	LDAP	Out	LDAP servers	LDAP if LDAP directory servers are outside firewall. LDAP authentication for Cisco Spam Quarantine.
636 or 3269	LDAPS	Out	LDAPS	LDAPS — ActiveDirectory's global catalog server (uses SSL).
443	TCP	In	AsyncOS IPs	Secure HTTP (https) access to the GUI for system monitoring.
443	TCP	Out	res.cisco.com	Verify the latest files for the update server.
443	TCP	Out	update-manifests.ironport.com	Obtain the list of the latest files from the update server (for physical hardware email gateways.)

443	TCP	Out	update-manifests.sco.cisco.com	Obtain the list of the latest files from the update server (for virtual email gateways.)
443	TCP	Out	serviceconfig.talos.cisco.com grpc.talos.cisco.com email-sender-ip-rep-grpc.talos.cisco.com For IP -based firewall: 146.112.62.0/24 146.112.63.0/24 146.112.255.0/24 146.112.59.0/24 2a04:e4c7:ffff::/48 2a04:e4c7:fffe::/48	Cisco Talos Intelligence Services - to obtain IP reputation, URL reputation and category, and to send Service Logs details.
443	TCP	Out	kinesis.us-west-2.amazonaws.com sensor-provisioner.ep.prod .agari.com houston.sensor.prod.agari.com	Register and send header details to Cisco Advanced Phishing Protection cloud service.
443	TCP	Out	As configured in Security Services > File Reputation and Analysis, Advanced Settings for File Reputation section, Cloud Server Pool parameter.	If configured, the port for access to cloud services for obtaining file reputation. The default port is 32137. For file analysis services, see port 443.
443	TCP	Out	As configured in Security Services > File Reputation and Analysis, Advanced Settings for File Analysis section.	Access to cloud services for file analysis. For file reputation services, see port 443 or 32137.
443	TCP	In & Out	As configured in Security Services > File Reputation and Analysis, Advanced Settings for File Reputation section, AMP for Endpoints Console Integration parameter. api.amp.sourcefire.com api.eu.amp.sourcefire.com api.apjc.amp.sourcefire.com api.amp.cisco.com api.eu.amp.cisco.com api.apjc.amp.cisco.com	Access to AMP for Endpoints console servers.

443	TCP	In & Out	outlook.office365.com login.microsoftonline.com.	Access to Office 365 services for mailbox auto remediation.
443	TCP	In & Out	Hostname of the Microsoft On-premise exchange server	Access to Microsoft On-premise exchange servers for remedating messages from the mailbox.
443	TCP	Out	aggregator.cisco.com	Access to the Cisco Aggregator server.
443	HTTPS	Out	logapi.ces.cisco.com	To upload the debug logs that are collected by Cisco TAC.
443	HTTPS	Out	TAXII servers	Used to allow your email gateway to consume external threat feeds.
443	HTTPS	In and Out	api-sse.cisco.com	Used to register your email gateway with Cisco SecureX or Cisco Threat Response.
443	HTTPS	In and Out	api.eu.sse.itd.cisco.com	Used to register your email gateway with Cisco SecureX or Cisco Threat Response.
443	HTTPS	In and Out	api.apj.sse.itd.cisco.com	Used to register your email gateway with Cisco SecureX or Cisco Threat Response.
443	HTTPS	In and Out	est.sco.cisco.com	Used to download a certificate to verify whether your email gateway is accessing a verified site when registering to Cisco SecureX or Cisco Threat Response.
443	HTTPS	In and Out	AsyncOS IPs	HTTPS access to the GUI using `trailblazerconfig` CLI command.
514	UDP/TCP	Out	Syslog server	Syslog logging.
628	TCP	In & In	AsyncOS IPs	QMQP if injecting email from outside firewall.
990	TCP/FTP	Out	support-ftp.cisco.com	To upload the debug logs that are collected by Cisco TAC.
1024 and higher	—	—	—	See information above for Port 21 (FTP.)
2222	CCS	In & In	AsyncOS IPs	Cluster Communication Service (for Centralized Management).

	TCP	Out	AsyncOS IPs	Cisco Spam Quarantine.
7025	TCP	In and out	AsyncOS IPs	Pass policy, virus, and outbreak quarantine data between Cisco Secure Email Gateways and Cisco Secure Manager Email and Web Gateways when this feature is centralized.
6080	HTTP	In or Out	AsyncOS IPs	Access to API ports for HTTP Server
6443	HTTPS	In or Out	AsyncOS IPs	Access to API ports for HTTPS Server

Protecting Email Gateway from Network Attacks

Make sure that you perform the following prerequisites to protect your email gateway from network attacks:

- Do not expose port 22 (SSH) to your email gateway external IP address.
- Enable only specific IP addresses to manage your email gateway using the web interface and CLI configuration settings.
- [If required] Enable Host Header protection using the `adminaccessconfig` CLI command.
- Enable Cross Scripting protection using the `adminaccessconfig` CLI command.
- Do not configure a Relay rule on a public listener.

Note If you require a relay rule on an external listener, configure ‘SMTP AUTH’ on a normal public listener.