防火墙信息

本章包含以下部分：

防火墙信息

下表列出了为了确保 Cisco Secure Email Gateway 正常运行可能需要打开的端口（这些值均为默认值）。

表 *1:* 防火墙端口

默认端口	协议	输入/输出	主机名	目的
20/21	TCP	输入或输出	AsyncOS IP、FTP 服务器	通过 FTP 汇聚日志文件。 数据端口 TCP 1024 和更高端口也必须全部打开。 有关更多信息，请在知识库中搜索 FTP 端口信息。请参阅知识库。
22	TCP	输入	AsyncOS IP	通过 SSH 访问 CLI，整合日志文件。
22	TCP	输出	SSH 服务器	通过 SSH 汇聚日志文件。
22	TCP	输出	SCP 服务器	SCP 推送到日志服务器。
25	TCP	输出	任意	SMTP，用于发送邮件。

防火墙信息

25	TCP	输入	AsyncOS IP	SMTP，用于接收退回的邮件，或者从防火墙外传入的邮件时。
53	UDP/TCP	输出	DNS 服务器	如果配置为使用 Internet 根服务器或防火墙外的其他 DNS 服务器，则使用DNS。也用于 SenderBase 查询。
80	HTTP	输入	AsyncOS IP	通过 HTTP 访问 GUI，进行系统监控。
80	HTTP	输出	downloads.ironport.com	和 McAfee 定义除外。
80	HTTP	输出	updates.ironport.com	AsyncOS 升级和 McAfee 定义。
80	HTTP	输出	TAXII 服务器	用于允许邮件网关使用外部威胁源。
82	HTTP	输入	AsyncOS IP	用于查看垃圾邮件隔离区。
83	HTTPS	输入	AsyncOS IP	用于查看垃圾邮件隔离区。
110	TCP	输出	POP 服务器	垃圾邮件隔离区的最终用户的 POP 身份验证。
123	UDP	输入和输出	NTP 服务器	NTP，如果时间服务器在防火墙外部。
143	TCP	输出	IMAP 服务器	垃圾邮件隔离区的最终用户的 IMAP 身份验证。
161	UDP	输入	AsyncOS IP	SNMP 查询。
162	UDP	输出	管理站	SNMP 陷阱。
389 或 3268	LDAP	输出	LDAP 服务器	LDAP，如果 LDAP 目录服务器在防火墙外部。思科垃圾邮件隔离区的 LDAP 身份验证。
636 或 3269	LDAP	输出	LDAP	LDAPS - ActiveDirectory 的全局目录服务器（使用 SSL）。
443	TCP	输入	AsyncOS IP	到 GUI 的安全 HTTP (https) 访问，以进行系统监控。
443	TCP	输出	res.cisco.com	验证更新服务器的最新文件。

防火墙信息

443	TCP	输出	update-manifests.ironport.com	从更新服务器获得最新文件的列表（适用于物理硬件邮件网关。）
443	TCP	输出	update-manifests.sco.cisco.com	从更新服务器获得最新文件的列表（适用于虚拟邮件网关。）
443	TCP	输出	serviceconfig.talos.cisco.com grpc.talos.cisco.com ~~email-sender-ip-rep-grpc.talos.cisco.com~~ 对于基于 IP 的防火墙： 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	思科 Talos 情报服务 - 获取 IP 信誉、URL 信誉和类别，以及发送服务日志详细信息。
443	TCP	输出	kinesis.us-west-2.amazonaws.com sensor-provisioner.ep.prod .agari.com houston.sensor.prod.agari.com	注册信头详细信息并将其发送到思科高级网络钓鱼防护云服务。
443	TCP	输入和输出	outlook.office365.com login.microsoftonline.com.	访问 Office 365 服务以进行邮箱自动修复。
443	TCP	输入和输出	Microsoft On-Premise 交换服务器的主机名	访问 Microsoft On-Premise 交换服务器以补救邮箱中的邮件。
443	TCP	输出	aggregator.cisco.com	对思科聚合服务器的访问。
443	HTTPS	输出	logapi.ces.cisco.com	上传 Cisco TAC 收集的调试日志。
443	HTTPS	输出	TAXII 服务器	用于允许邮件网关使用外部威胁源。
443	HTTPS	传入和传出	api-sse.cisco.com	用于向思科 SecureX 或 思科威胁响应注册邮件网关。
443	HTTPS	传入和传出	api.eu.sse.itd.cisco.com	用于向思科 SecureX 或 思科威胁响应注册邮件网关。

443	HTTPS	传入和传出	api.apj.sse.itd.cisco.com	用于向思科 SecureX 或 思科威胁响应注册邮件网关。
443	HTTPS	传入和传出	est.sco.cisco.com	用于在向思科 SecureX 或 思科威胁响应注册时，用于下载证书，以验证您的邮件网关是否正在访问已验证的站点。
443	HTTPS	传入和传出	AsyncOS IP	使用`trailblazerconfig` CLI 命令对 GUI 进行 HTTPS 访问。
514	UDP/TCP	输出	系统日志服务器	系统日志记录。
628	TCP	输入/输入	AsyncOS IP	QMQP，如果从外部防火墙注入邮件。
990	TCP/FTP	输出	cxd.cisco.com	上传 Cisco TAC 收集的调试日志。
1024 及更高	-	—	—	对于端口 21 (FTP)，请参阅上述信息。
2222	CCS	输入/输入	AsyncOS IP	集群通信服务（用于集中管理）。
	TCP	输出	AsyncOS IP	思科垃圾邮件隔离区。
7025	TCP	输入和输出	AsyncOS IP	当此集中功能时，在 Cisco Secure Email Gateway 与思科安全管理器邮件和 Web 网关之间传递策略、病毒和病毒爆发隔离区数据。
6080	HTTP	输入或输出	AsyncOS IP	访问 HTTP 服务器的 API 端口
6443	HTTPS	输入或输出	AsyncOS IP	访问 HTTPS 服务器的 API 端口

文件信誉和文件分析服务的防火墙信息

下表列出了邮件网关中配置的文件信誉和文件分析服务正常运行可能需要打开的端口（这些均为默认值）。

表 *2:* 防火墙端口

地区	目的	主机名	默认端口	协议	输入/输出

防火墙信息

美国和 北美地区	文件信誉	cloud-esa-asn.amp.cisco.com cloud-esa-est.amp.cisco.com	443	TCP	输出。
	文件分析	panacea.threatgrid.com	443	TCP	输出
	API	api.amp.cisco.com	443	TCP	输出
	事件服务器	intake.amp.cisco.com	443	TCP	输出
	管理服务器	mgmt.amp.cisco.com	443	TCP	输出
加拿大	文件分析 (File Analysis)	panacea.threatgrid.ca	443	TCP	输出
欧洲	文件信誉	cloud-esa-asn.eu.amp.cisco.com cloud-esa-est.eu.amp.cisco.com	443	TCP	输出
	文件分析	panacea.threatgrid.eu	443	TCP	输出
	API	api.eu.amp.cisco.com	443	TCP	输出
	事件服务器	intake.eu.amp.cisco.com	443	TCP	输出
	管理服务器	mgmt.eu.amp.cisco.com	443	TCP	输出
澳大利亚	文件分析 (File Analysis)	panacea.threatgrid.com.au	443	TCP	输出
亚太地区、日本和中国	文件信誉	cloud-esa-asn.apjc.amp.cisco.com cloud-esa-est.apjc.amp.cisco.com	443	TCP	输出
	文件分析	使用欧洲或北美主机名	443	TCP	输出
	API	api.apjc.amp.cisco.com	443	TCP	输出
	事件服务器	intake.apjc.amp.cisco.com	443	TCP	输出
	管理服务器	mgmt.apjc.amp.cisco.com	443	TCP	输出

保护邮件网关免遭网络攻击

确保执行以下前提条件以保护邮件网关免受网络攻击：

- 不要将端口 22 (SSH) 暴露给邮件网关外部 IP 地址。
- 仅启用特定 IP 地址以使用 Web 界面和 CLI 配置设置来管理邮件网关。
- [如果需要]使用 `adminaccessconfig` CLI 命令来启用主机信头保护。
- 使用 `adminaccessconfig` CLI 命令来启用交叉脚本保护。
- 不要在公共侦听程序上配置中继规则。

注释 如果需要外部侦听程序上配置中继规则，可在普通公共侦听程序上配置“SMTP AUTH”。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。