



## 防火墙资讯

本章包含以下部分：

- [防火墙资讯，第 1 页](#)
- [保护邮件网关免遭网络攻击，第 5 页](#)

## 防火墙资讯

下表列出了为了确保思科安全邮件网关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。<br>数据端口 TCP 1024 和更高端口也必须全部打开。<br>有关更多信息，请在知识库中搜索 FTP 端口信息。请参阅 <a href="#">知识库</a> 。 |
| 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。  |
| 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。  |
| 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<br>grpc.talos.cisco.com<br>email-sender-ip-rep-grpc.talos.cisco.com<br>对于基于 IP 的防火墙：<br>146.112.62.0/24<br>146.112.63.0/24<br>146.112.255.0/24<br>146.112.59.0/24<br>2a04:e4c7:ffff::/48<br>2a04:e4c7:ffe::/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<br>sensor-provisioner.ep.prod.agari.com<br>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 | 输出 | 如“安全服务”(Security Services) > “文件信誉和分析”(File Reputation and Analysis) 的“文件信誉”(File Reputation) 部分“高级设置”(Advanced Settings) 的“云服务器池”(Cloud Server Pool) 参数的配置。   | 如果已配置，则为访问云服务获取文件信誉的端口。默认端口为 32137。有关文件分析服务，请参阅端口 443。 |
| 443 | TCP | 输出 | 如“安全服务”(Security Services) > “文件信誉和分析”(File Reputation and Analysis) 的“文件分析”(File Analysis) 部分“高级设置”(Advanced Settings) 的配置。   | 访问云服务以进行文件分析。有关文件信誉服务，请参阅端口 443 或 32137。               |

|     |         |       |  |   |
|-----|---------|-------|--|---|
| 443 | TCP     | 输入和输出 | 如“安全服务” > “文件信誉和分析”的“文件信誉”部分“高级设置”的配置，AMP for Endpoints Console Integration 参数。<br>api.amp.sourcefire.com<br>api.eu.amp.sourcefire.com<br>api.apjc.amp.sourcefire.com<br>api.amp.cisco.com<br>api.eu.amp.cisco.com<br>api.apjc.amp.cisco.com | 对面向终端的 AMP 控制台服务器的访问。                                   |
| 443 | TCP     | 输入和输出 | outlook.office365.com<br>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    | support-ftp.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，在思科安全邮件网关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                                    |

## 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”。

