



防火墙资讯

本章包含以下部分：

- [防火墙资讯，第 1 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。 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 知识库文章（技术说明） 。 |
| 22 | SSH | 输出 | AsyncOS IP | 集中配置管理器配置推送。 也用于备份。 |
| 22 | TCP | 输入 | AsyncOS IP | 通过 SSH 访问 CLI，整合日志文件。 |
| 22 | TCP | 输出 | SCP 服务器 | SCP 推送到日志服务器。 |
| 23 | Telnet | 输入 | AsyncOS IP | 通过 Telnet 访问 CLI。 |
| 23 | Telnet | 输出 | Telnet 服务器 | Telnet 升级 |
| 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 | 服务更新, AsyncOS 升级除外。 |
| 80 | HTTP | 输出 | upgrades.ironport.com | AsyncOS 升级。 |
| 801 | HTTP | 传入和传出 | AsyncOS IP | 使用 trailblazerconfig CLI 命令对 GUI 进行 HTTP 访问。 |
| 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 | update-static.ironport.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 | phonehome.senderbase.org | 接收/发送病毒爆发过滤器。 |
| 443 | TCP | 输出 | <p>在网络安全设备上的“安全服务” (Security Services) > “防恶意软件和信誉” (Anti-Malware and Reputation) 页面的“高级” (Advanced) 部分 > “文件分析高级设置” (Advanced Settings for File Analysis) 配置的文件分析服务器 URL。</p> <p>在邮件安全设备上的“安全服务” (Security Services) > “文件信誉和分析” (File Reputation and Analysis) 页面的“文件分析高级设置” (Advanced Settings for File Analysis) 部分配置的文件分析服务器 URL。</p> | <p>在文件分析服务器上显示详细的文件分析结果。</p> <ul style="list-style-type: none"> 网络安全报告：（云文件分析）确保管理设备可以连接到文件分析服务器 |
| 443 | HTTPS | 传入和传出 | api-sse.cisco.com | 用于向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。 |
| 1024 及更高 | - | — | — | 对于端口 21 (FTP)，请参阅上述信息。 |

| | | | | |
|-------|-------|-------|------------|---|
| 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。 |
| 32137 | TCP | | | |
| 6080 | HTTP | 输入或输出 | | 访问 HTTP 服务器的 API 端口 |
| 6443 | HTTPS | 输入或输出 | | 访问 HTTPS 服务器的 API 端口 |

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。