



安全、互联网接入和通信端口

以下主题提供有关系统安全、互联网接入和通信端口的信息：

- [安全要求，第 1 页](#)
- [思科云，第 1 页](#)
- [互联网接入要求，第 2 页](#)
- [通信端口要求，第 4 页](#)

安全要求

为了保护 Cisco Secure Firewall Management Center，应将其安装在受保护的内部网络中。虽然管理中心已配置为仅拥有必需的服务和可用端口，但必须确保无法从防火墙外部攻击它（或任何受管设备）。

如果管理中心及其受管设备位于同一个网络，可以将设备的管理接口连接到与管理中心相同的受保护内部网络。这样，就可以安全地从管理中心控制设备。您还可以配置多个管理接口，使管理中心能够管理和隔离来自其他网络上设备的流量。

无论如何部署设备，内部设备通信将始终加密。但是，您仍需采取措施，确保设备之间的通信不会出现中断、阻塞或受到篡改；例如，遭受分布式拒绝服务 (DDoS) 或中间人攻击。

思科云

管理中心与思科云中的资源进行通信，用于实现以下功能：

- **高级恶意软件防护**
默认配置的是公共云；要进行更改，请参阅 [《Cisco Secure Firewall Management Center 设备配置指南》](#) 中的 [更改 AMP 选项](#)。
- **URL 筛选**
有关详细信息，请参阅 [URL 过滤](#) 一章。
- **集成安全分析和日志记录 (SaaS)**

请参阅[在思科 Cisco Secure Cloud Analytics中的远程数据存储](#)。

- 有关详细信息，请参阅以下链接的集成文档：
 - [与思科 SecureX集成](#)
 - [使用的事件分析 SecureX 威胁响应](#)
- **主动支持功能**
有关信息，请参阅[配置思科支持诊断注册](#)。
- **思科成功网络**
有关信息，请参阅[配置思科成功网络注册](#)。
- **Cisco Umbrella 连接**
有关信息，请参阅《[Cisco Secure Firewall Management Center 设备配置指南](#)》中的 *DNS* 策略。

互联网接入要求

默认情况下，系统配置为通过 443/tcp (HTTPS) 端口和 80/tcp (HTTP) 端口连接到互联网。如果您不希望设备直接接入互联网，则可以配置代理服务器。对于许多功能，您的位置可以确定系统访问哪些资源。

大多数情况下，它是可接入互联网的管理中心。高可用性对中的两个管理中心均应可以接入互联网。根据功能，有时两个对等体均可以接入互联网，而有时只有活动对等体才可以接入互联网。

有时受管设备也可以接入互联网。例如，如果恶意软件防护配置使用动态分析，则受管设备会将文件直接提交到 Secure Secure Malware Analytics 云。或者，您也可以将设备同步到外部 NTP 服务器。

此外，除非您禁用 Web 分析跟踪，否则浏览器可能会与 Google (google.com) 或 Amplitude (amplitude.com) Web 分析服务器通信，以向 Cisco 发送非个人可识别的使用数据。

表 1: 互联网接入要求

功能	原因	管理中心 高可用性	Resource
恶意软件	恶意软件云查找。	两个对等体均执行查找。	请参阅 正确的思科安全终端和恶意软件分析操作所需的服务器地址 。
	下载签名更新以进行文件预分类和本地恶意软件分析。	活动对等体执行下载，并同步到备用对等体。	updates.vrt.sourcefire.com amp.updates.vrt.sourcefire.com
	提交文件以进行动态分析（受管设备）。 查询动态分析结果(管理中心)。	两个对等体均查询动态分析报告。	fmc.api.threatgrid.com fmc.api.threatgrid.eu

功能	原因	管理中心 高可用性	Resource
面向终端的 AMP	<p>从 AMP 云接收由面向终端的 AMP 检测到的恶意软件事件。</p> <p>显示由面向终端的 AMP 中的系统检测到的恶意软件事件。</p> <p>使用在面向终端的 AMP 中创建的集中式文件阻止名单和允许名单覆盖 AMP 云中的处置情况。</p>	<p>两个对等体均接收事件。</p> <p>您还必须在两个对等体上配置云连接（配置不会同步）。</p>	<p>请参阅 正确的思科安全终端和恶意软件分析操作所需的服务器地址。</p>
安全情报	<p>下载安全情报源。</p>	<p>活动对等体执行下载，并同步到备用对等体。</p>	<p>intelligence.sourcefire.com</p>
URL 过滤	<p>下载 URL 类别和信誉数据。</p> <p>手动查询（查找）URL 类别和信誉数据。</p> <p>查询未分类的 URL。</p>	<p>活动对等体执行下载，并同步到备用对等体。</p>	<p>URL:</p> <ul style="list-style-type: none"> • regsvc.sco.cisco.com • est.sco.cisco.com • updates-talos.sco.cisco.com • updates.ironport.com <p>IPV4 块:</p> <ul style="list-style-type: none"> • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 <p>IPV6 块:</p> <ul style="list-style-type: none"> • 2a04:e4c7:ffff:/48 • 2a04:e4c7:fffe:/48
思科智能许可	<p>与思科智能软件管理器通信。</p>	<p>活动对等体执行通信。</p>	<p>tools.cisco.com:443</p> <p>www.cisco.com</p>
思科成功网络	<p>传输使用信息和统计信息。</p>	<p>活动对等体执行通信。</p>	<p>api-sse.cisco.com:8989</p> <p>dex.sse.itd.cisco.com</p> <p>dex.eu.sse.itd.cisco.com</p>
思科支持诊断结果	<p>接受授权请求并传输使用信息和统计信息。</p>	<p>活动对等体执行通信。</p>	<p>api-sse.cisco.com:8989</p>

功能	原因	管理中心 高可用性	Resource
系统更新	直接将更新从思科下载到管理中心： <ul style="list-style-type: none"> • 系统软件 • 入侵规则 • 漏洞数据库 (VDB) • 地理位置数据库 (GeoDB) 	更新活动对等体上的入侵规则、VDB 和 GeoDB，然后再同步到备用对等体。 在每个对等体上单独升级系统软件。	cisco.com sourcefire.com
SecureX 威胁响应集成	请参阅相应的 集成指南 。		
时间同步	同步部署中的时间。 代理服务器不支持。	使用外部 NTP 服务器的任何设备均必须接入互联网。	0.sourcefire.pool.ntp.org 1.sourcefire.pool.ntp.org 2.sourcefire.pool.ntp.org 3.sourcefire.pool.ntp.org
RSS 源	在控制面板上显示思科威胁研究博客。	显示 RSS 源的任何设备均必须接入互联网。	blog.talosintelligence.com blogs.cisco.com feeds.feedburner.com
Whois	请求外部主机的 whois 信息。 代理服务器不支持。	请求 whois 信息的任何设备均必须接入互联网。	whois 客户端会尝试猜出要查询的正确服务器。如果猜不出，则使用： <ul style="list-style-type: none"> • NIC 句柄： whois.networksolutions.com • IPv4 地址和网络名称： whois.arin.net

通信端口要求

管理中心 和托管设备在 8305/tcp 端口上使用双向、SSL 加密的通信通道进行通信。此端口 必须 保持开放，以进行基本通信。

其他端口允许安全管理，并访问特定功能所需的外部资源。一般来说，除非启用或配置相关功能，否则，功能相关的端口会保持关闭。在了解此操作对部署的影响之前，请勿更改或关闭已打开的端口。

表 2: 通信端口要求

端口	协议/功能	平台	方向	详细信息
22/tcp	SSH	管理中心 威胁防御	进站	与安全设备的远程连接。
53/tcp 53/udp	DNS		出站	DNS
67/udp 68/udp	DHCP		发送	DHCP
123/udp	NTP		发送	同步时间。
161/udp	SNMP	管理中心 威胁防御	进站	允许通过 SNMP 轮询访问 MIB。
162/udp	SNMP		发送	发送 SNMP 警报至远程陷阱服务器。
389/tcp 636/tcp	LDAP		发送	与 LDAP 服务器通信以进行外部身份验证。 获取检测到的 LDAP 用户元数据（仅限管理中心）。 可配置。
443/tcp	HTTPS	管理中心	接收	访问 Web 界面。
443/tcp	远程接入 VPN (SSL/IPSec)	威胁防御	进站	允许远程用户与您的网络建立安全的 VPN 连接。
500/udp 4500/udp	远程接入 VPN (IKEv2)	威胁防御	进站	允许远程用户与您的网络建立安全的 VPN 连接。
443/tcp	HTTPS	管理中心 威胁防御	接收	使用 Firepower REST API（包括思科终端服务(TS)代理）与第三方集成产品通信。
443/tcp	HTTPS		发送	发送和接收来自互联网的数据。 有关详细信息，请参阅 互联网接入要求 ，第 2 页。
443	HTTPS	管理中心	both	与面向终端的 AMP 集成
514/udp	系统日志（警报）		发送	向远程系统日志服务器发送警报。
623/udp	SOL/LOM	管理中心	进站	使用 LAN 上串行 (SOL) 连接执行无人值守管理 (LOM)。

端口	协议/功能	平台	方向	详细信息
885/tcp	强制网络门户	威胁防御	入站	与强制网络门户身份源通信。
1500/tcp 2000/tcp	数据库访问	管理中心	入站	允许第三方客户端对事件数据库进行只读访问。
1812/udp 1813/udp	RADIUS		发送	与 RADIUS 服务器通信以进行外部身份验证和记账。 可配置。
8302/tcp	eStreamer	管理中心	入站	与 eStreamer 客户端通信。
8305/tcp	设备通信		双向	在同一部署中的设备之间安全地进行通信。 可配置。如果更改此端口，必须为部署中的所有设备更改此端口。建议保留默认值。
8307/tcp	主机输入客户端	管理中心	入站	与主机输入客户端通信。
8989/tcp	思科支持诊断结果		两者	接受授权请求并传输使用信息和统计信息。

相关主题

[添加 管理中心的 LDAP 外部身份验证对象](#)

[添加 管理中心的 RADIUS 外部身份验证对象](#)

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。