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

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。

- **Cisco Umbrella 连接**

有关详细信息，请参阅Cisco Umbrella 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。

有时托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 Web 分析服务器通信，以向思科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
恶意软件防护	恶意软件云查找。	两个对等体均执行查找。	请参阅正确的 Cisco Secure Endpoint 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
面向终端的AMP集成	从 AMP 云接收由面向终端的 AMP 检测到的恶意软件事件。 显示由面向终端的 AMP 中的系统检测到的恶意软件事件。 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。	两个对等体均接收事件。 您还必须在两个对等体上配置云连接（配置不会同步）。	请参阅正确的 Cisco Secure Endpoint 和恶意软件分析操作所需的服务器地址。
安全情报	下载安全智能源。	活动对等体执行下载，并同步到备用对等体。	intelligence.sourcefire.com

功能	原因	管理中心 高可用性	Resource
URL 筛选	下载 URL 类别和信誉数据。 手动查询（查找）URL类别和信誉数据。 查询未分类的 URL。	活动对等体执行下载，并同步到备用对等体。	URL： • regsvc.sco.cisco.com • est.sco.cisco.com • updates-talos.sco.cisco.com • updates.ironport.com IPV4 块： • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 IPV6 块： • 2a04:e4c7:ffff::/48 • 2a04:e4c7:fffe::/48
思科智能许可	与思科智能软件管理器通信。	活动对等体执行通信。	tools.cisco.com:443 www.cisco.com
思科成功网络	传输使用信息和统计信息。	活动对等体执行通信。	api-sse.cisco.com:8989 dex.sse.itd.cisco.com dex.eu.sse.itd.cisco.com
思科支持诊断结果	接受授权请求并传输使用信息和统计信息。	活动对等体执行通信。	api-sse.cisco.com:8989
系统更新	直接将更新从思科下载到管理中心： • 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。		

功能	原因	管理中心 高可用性	Resource
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： • 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
53/tcp 53/udp	DNS		发送	DNS
67/udp 68/udp	DHCP		发送	DHCP
123/udp	NTP		发送	同步时间。
162/udp	SNMP		发送	发送 SNMP 警报至远程陷阱服务器。

端口	协议/功能	平台	方向	详细信息
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	如果您使用本地安全设备连接器载入 管理中心，则允许端口 443 上的入站连接。
443/tcp	HTPS	管理中心	出站	如果使用云连接器将 管理中心 载入 CDO，则允许来自端口 443 的出站流量。
443/tcp	HTPS	管理中心	出站	如果使用 SecureX 载入管理中心，则允许端口 443 的出站连接。
443/tcp	HTTPS		发送	发送和接收来自互联网的数据。
514/udp	系统日志（警报）		发送	向远程系统日志服务器发送警报。
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。
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。

相关主题

添加 CDO的 LDAP 外部身份验证对象

添加 CDO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。