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。

- **集成 Security Analytics and Logging (SaaS)**

请参阅在思科 Cisco Secure Cloud Analytics中的远程数据存储。

- **集成 思科 XDR**

  有关详细信息，请参阅《Cisco Secure Firewall Threat Defense 和 Cisco XDR 集成指南》。

- **主动支持功能**

  有关信息，请参阅配置思科支持诊断注册。

- **Cisco Success Network**

  有关信息，请参阅配置 管理中心 以与思科共享使用情况指标和统计信息。

- **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可以访问哪些资源。

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，用于动态分析提交与外部 NTP 服务器同步。

此外，除非您禁用 Web 分析跟踪，否则浏览器可能会与 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 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

功能	原因	管理中心 高可用性	Resource
面向终端的 AMP	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。
事件扩充	下载 Talos 分类法。 查询 Talos 云服务以扩充事件。	两个对等体与 Talos 云服务独立通信。	URL： • *.talos.cisco.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
安全智能	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 过滤	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： • *.talos.cisco.com • updates-talos.sco.cisco.com • updates-dyn-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
Cisco Secure Dynamic Attributes Connector	从 Amazon Elastic Container Registry (Amazon ECR) 获取软件包	两个对等体进行通信。	public.ecr.aws csdac-cosign.s3.us-west-1.amazonaws.com
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。	smartreceiver.cisco.com www.cisco.com
Cisco Success Network	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
思科 XDR 集成	请参阅《Cisco Secure Firewall Threat Defense 和 Cisco XDR 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。	可配置。
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

功能	原因	管理中心 高可用性	Resource
更新：内容更新	直接向管理中心下载内容更新： • 入侵规则 (SRU/LSP) • 漏洞数据库 (VDB) • 地理位置数据库 (GeoDB)	更新活动对等体，然后同步到备用设备。	对于轻量级安全软件包 (LSP)： talosintelligence.com 对于其他内容更新： support.sourcefire.com
更新：产品升级	将产品升级直接下载到管理中心。 请注意，直接下载到受管设备需要版本 7.6.1+ 的管理中心。	在一个对等体上下载管理中心升级包会尝试在两个对等体上下载。如果只有一个对等体访问了互联网，您可以在升级过程中同步软件包。 威胁防御升级包不会同步，但也不需要同步。	cdo-ftd-images.s3-us-west-2.amazonaws.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。

有关系统可能通过这些端口联系的互联网资源的信息，请参阅 互联网接入要求，第 2 页。

管理中心 的端口

表 2: 管理中心 的入站端口

入站端口	协议/功能	详细信息
22/tcp	SSH	与设备的安全远程连接。
161/udp	SNMP	允许通过 SNMP 轮询访问 MIB。

入站端口	协议/功能	详细信息
443/tcp	HTTPS	访问 Web 界面。
443/tcp	HTTPS	使用 安全设备连接器 （本地部署）将本地部署 管理中心 载入 [CDO 。
443/tcp	HTTPS	提交查询至思科安全数据包分析器。
443/tcp	HTTPS	使用 REST API 与集成产品和第三方产品通信。
443/tcp	HTTPS	与 Cisco Secure Endpoint集成。还需要出站。
623/udp	SOL/LOM	使用 LAN 上串行 (SOL) 连接执行无人值守管理 (LOM)。
1500/tcp 2000/tcp	数据库访问	允许第三方客户端对事件数据库进行只读访问。
8302/tcp	eStreamer	与 eStreamer 客户端通信。
8305/tcp	设备通信	在同一部署中的设备之间安全地进行通信。还需要出站。 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	与主机输入客户端通信。
8989/tcp	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。还需要出站。

表 *3:* 管理中心的出站端口

出站端口	协议/功能	详细信息
7/udp 514/udp 6514/tcp	系统日志（审核日志记录）	在配置审核日志记录时，验证与系统日志服务器的连接 (7/udp)。 未配置 TLS 时，将审核日志发送到远程系统日志服务器 (514/udp)。 配置 TLS 后，将审核日志发送到远程系统日志服务器 (6514/tcp)。
25/tcp	SMTP	发送邮件通知和警报。
53/tcp 53/udp	DNS	DNS
67/udp 68/udp	DHCP	DHCP
80/tcp	HTTP	通过 HTTP 下载自定义安全情报源。
80/tcp	HTTP	下载或查询 URL 类别和信誉数据。还需要出站 443/tcp。
80/tcp	HTTP	在控制面板中显示 RSS 源。

出站端口	协议/功能	详细信息
123/udp	NTP	同步时间。
162/udp	SNMP	发送 SNMP 警报至远程陷阱服务器。
389/tcp 636/tcp	LDAP	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。 可配置。
443/tcp	HTTPS	与 Cisco Secure Malware Analytics 云（公共或私有）通信。
443/tcp	HTTPS	发送和接收来自互联网的数据。
443/tcp	HTTPS	与面向终端的 AMP 集成。入站也需要。
443/tcp	HTTPS	使用 思科安全云 或 安全设备连接器（云）将本地 管理中心 载入 CDO。
1812/udp 1813/udp	RADIUS	与 RADIUS 服务器通信以进行外部身份验证和记账。 可配置。
5222/tcp	ISE	与 ISE 身份源通信。
8305/tcp	设备通信	在同一部署中的设备之间安全地进行通信。入站也需要。 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。
8989/tcp	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。入站也需要。
8989/tcp	Cisco Success Network	传输使用信息和统计信息。

受管设备的端口

表 *4:* 受管设备的入站端口

入站端口	协议/功能	详细信息
22/tcp	SSH	与设备的安全远程连接。
161/udp	SNMP	允许通过 SNMP 轮询访问 MIB。
443/tcp	HTTPS	使用 REST API 与集成产品和第三方产品通信。
443/tcp	远程访问 VPN (SSL/IPSec)	允许远程用户与您的网络建立安全的 VPN 连接。
500/udp 4500/udp	远程访问 VPN (IKEv2)	允许远程用户与您的网络建立安全的 VPN 连接。

入站端口	协议/功能	详细信息
885/tcp	强制网络门户	与强制网络门户身份源通信。
8305/tcp	设备通信	在同一部署中的设备之间安全地进行通信。还需要出站。 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。
8989/tcp	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。还需要出站。

表 5: 受管设备的出站端口

出站端口	协议/功能	详细信息
53/tcp 53/udp	DNS	DNS
67/udp 68/udp	DHCP	DHCP
123/udp	NTP	同步时间。
162/udp	SNMP	发送 SNMP 警报至远程陷阱服务器。
1812/udp 1813/udp	RADIUS	与 RADIUS 服务器通信以进行外部身份验证和记账。 可配置。
389/tcp 636/tcp	LDAP	与 LDAP 服务器通信以进行外部身份验证。 可配置。
443/tcp	HTTPS	发送和接收来自互联网的数据。
514/udp	系统日志（审核日志记录）	未配置 TLS 时，将审核日志发送到远程系统日志服务器。
8305/tcp	设备通信	在同一部署中的设备之间安全地进行通信。入站也需要。 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。
8514 / UDP	Cisco Secure Network Analytics 管理器	使用 Security Analytics and Logging（本地部署）将系统日志消息发送到 Secure Network Analytics
8989/tcp	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。入站也需要。

相关主题

添加 管理中心 的 LDAP 外部身份验证对象

为 管理中心 添加 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。