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：

- 安全性和强化，第 1 页
- 通信端口，第 1 页
- 访问的互联网资源，第 5 页

安全性和强化

为了保护防火墙管理中心，应将其安装在受保护的内部网络中。虽然 防火墙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）。

如果防火墙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防火墙管理中心相同的受保护内部网络。这样，就可以安全地从 防火墙管理中心控制设备。您还可以配置多个管理接口，使 防火墙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。

通信端口

对于网络屏障（如边缘防火墙）后的部署，请确保允许在所需端口上的流量。请注意，非基本或默认操作所需的端口在配置或功能需要之前保持关闭。

防火墙管理中心 的端口

管理中心使用这些端口进行通信。

表 *1:* 防火墙管理中心 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。

入站端口	协议/功能	详细信息
161/udp	SNMP	允许通过 SNMP 轮询访问 MIB。
443/tcp	HTTPS	**Required.** 访问管理中心 Web 界面。
443/tcp	HTTPS	使用 安全设备连接器 （本地部署）将本地部署 防火墙管理中心 载入 [安全云控制 。
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。
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	**Required.** 与托管设备安全通信。也会在此端口上发起连接。 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。也会在此端口上发起连接。

表 *2:* 防火墙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	**Required.** DNS
67/udp 68/udp	DHCP	DHCP
80/tcp	HTTP	发送和接收来自互联网的数据。请参阅访问的互联网资源 ， 第 5 页。

出站端口	协议/功能	详细信息
80/tcp	HTTP	通过 HTTP 下载自定义安全智能源。
80/tcp	HTTP	下载或查询 URL 类别和信誉数据。此功能也使用 443/tcp。
80/tcp	HTTP	在控制面板中显示 RSS 源。
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	发送和接收来自互联网的数据。请参阅访问的互联网资源，第 5 页。
443/tcp	HTTPS	与 Cisco Secure Malware Analytics 云（公共或私有）通信。
443/tcp	HTTPS	与 Cisco Secure Endpoint集成。也会在此端口上接受连接。
443/tcp	HTTPS	使用 或 安全设备连接器（云）将本地 防火墙管理中心 载入 安全云控制。
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	**Required.** 与托管设备安全通信。也会在此端口上接受连接。 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。也会在此端口上接受连接。
8989/tcp	Cisco Success Network	传输使用信息和统计信息。

托管设备的端口

托管设备使用这些端口进行通信。

表 *3:* 托管设备的入站端口

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。

入站端口	协议/功能	详细信息
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。
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	**Required.** 与 防火墙管理中心 安全通信。也会在此端口上发起连接。 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	接受授权的请求。也会在此端口上发起连接。

表 *4:* 托管设备的出站端口

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	从互联网发送和接收数据；请参阅访问的互联网资源 ， 第 5 页。
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。

出站端口	协议/功能	详细信息
8305/tcp	设备通信	**Required.** 与 防火墙管理中心 安全通信。也会在此端口上接受连接。 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 Cisco Secure Network Analytics。
8989/tcp	思科支持诊断结果	传输使用信息和统计信息。也会在此端口上接受连接。

访问的互联网资源

除系统访问互联网外，您的浏览器可能还会与 Amplitude (amplitude.com) 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。

防火墙管理中心 访问的互联网资源

管理中心通过 443/tcp 端口 (HTTPS) 和 80/tcp 端口 (HTTP) 连接至互联网。您可以配置代理服务器，但 NTP 和 whois 除外。对于某些功能，您的位置决定了可访问的资源。某些功能还需访问设备；请参阅下表。

表 *5:* 防火墙管理中心 访问的互联网资源

功能	原因	高可用性	Resource
CA 证书捆绑包	每天在系统定义的时间查询新的 CA 证书。本地 CA 捆绑包包含用于访问多项思科服务的证书。	每个对等体都会下载其自己的证书。	cisco.com/security/pki
恶意软件防护	Cisco Secure Malware Analytics 云 查找。	两个对等体均执行查找。	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
	查询动态分析结果。	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	高可用性	Resource
事件扩充	下载 Talos 分类法。 查询 Talos 云服务以扩充事件。	两个对等体进行通信。	URL： • *.talos.cisco.com • est.sco.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
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 • est.sco.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

功能	原因	高可用性	Resource
Cisco Secure Dynamic Attributes Connector	从 Amazon Elastic Container Registry (Amazon ECR) 获取软件包。	每个对等体会下载自己的软件包。	public.ecr.aws csdac-cosign.s3.us-west-1.amazonaws.com
Cisco Secure Endpoint	从云接收由Cisco Secure Endpoint检测到的恶意软件事件。 显示由Cisco Secure Endpoint中的系统检测到的恶意软件事件。 使用在Cisco Secure Endpoint中创建的集中式文件阻止名单和允许名单覆盖云中的处置情况。	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）。	正确的 Cisco Secure Endpoint 和恶意软件分析操作所需的服务器地址
思科 智能软件管理器	与 智能软件管理器通信。	活动对等体执行通信。	www.cisco.com smartreceiver.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	配置设备以便将事件发送到 。	活动对等体执行通信。	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。	两个对等体都与 NTP 服务器通信。	用户已配置
RSS 源	在控制面板上显示思科威胁研究博客。	两个对等体进行通信。	blog.talosintelligence.com
升级	下载产品（管理中心和设备/机箱）升级。	在一个对等体上下载防火墙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。 存储在防火墙管理中心上的设备升级包不会同步，但它们也不需要同步。	cdo-ftd-images-us-west-2.amazonaws.com

功能	原因	高可用性	Resource
入侵规则	下载入侵规则 (SRU/LSP)。	活动对等体执行下载，并同步到备用对等体。	est.sco.cisco.com updates-talos.sco.cisco.com updates-dyn-talos.sco.cisco.com updates.ironport.com
漏洞数据库	下载 VDB 更新。	活动对等体执行下载，并同步到备用对等体。	support.sourcefire.com
地理位置数据库	下载 GeoDB 更新。	活动对等体执行下载，并同步到备用对等体。	support.sourcefire.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

托管设备访问的互联网资源

托管设备通过 443/tcp 端口 (HTTPS) 和 80/tcp 端口 (HTTP) 连接至互联网。您可以配置代理服务器，但 NTP 除外。对于某些功能，您的位置决定了可访问的资源。

表 *6:* 托管设备访问的互联网资源

特性	原因	高可用性/集群	资源
CA 证书捆绑包	每天在系统定义的时间查询新的 CA 证书。本地 CA 捆绑包包含用于访问多项思科服务的证书。	每个设备都会下载自己的证书。	cisco.com/security/pki
恶意软件防护	提交文件以供动态分析。	所有设备提交文件。	fmc.api.threatgrid.com fmc.api.threatgrid.eu
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。	所有设备都会通信。	api-sse.cisco.com:8989
时间同步	同步部署中的时间。 代理服务器不支持。	所有设备都会与 NTP 服务器通信。	用户已配置。

特性	原因	高可用性/集群	资源
升级	将升级直接下载到托管设备。 每周测试一次连接。	升级包不会同步。每个设备必须从互联网、主用 防火墙管理中心 或内部服务器获取其自身的数据。	cdo-ftdimages.s3-us-west-2.amazonaws.com
思科 XDR 集成	将事件发送至 。	所有设备都会发送事件。	Cisco Secure Firewall Threat Defense 和 Cisco XDR 集成指南

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。