



设备管理

本指南适用于作为主要管理器或仅作为分析管理器的本地设备 Cisco Secure Firewall Management Center。在将思科防御协调器(CDO)云交付的防火墙管理中心用作主管理器时，您只能使用本地部署管理中心进行分析。请勿将本指南用于 CDO 管理；请参阅 [使用 Cisco 防御协调器中的云交付防火墙管理中心管理防火墙威胁防御](#)。

本章介绍如何在 Cisco Secure Firewall Management Center 中添加和管理设备。

- [关于设备管理，第 1 页](#)
- [设备管理的要求和必备条件，第 10 页](#)
- [登录 威胁防御 设备上的命令行界面，第 10 页](#)
- [完成 威胁防御 初始配置，第 12 页](#)
- [将设备添加到 管理中心，第 26 页](#)
- [从 管理中心 删除（取消注册）设备，第 30 页](#)
- [添加设备组，第 30 页](#)
- [关闭或重新启动设备，第 31 页](#)
- [配置设备设置，第 32 页](#)
- [更改设备的管理器，第 74 页](#)
- [Cisco Secure Firewall 3100 上的热插拔 SSD，第 82 页](#)
- [设备管理的历史记录基础知识，第 84 页](#)

关于设备管理

使用 管理中心 来管理您的设备。

关于 管理中心 和设备管理

在管理中心管理设备时，它会在自己和设备之间设置双向、SSL 加密的通信信道。管理中心使用此信道向设备发送有关要如何分析和流向设备的网络流量的信息。设备评估流量时，会生成事件并使用同一信道将其发送到管理中心。

通过使用 管理中心管理设备，您可以执行以下操作：

- 从单个位置为所有设备配置策略，从而更轻松地更改配置
- 在设备上安装各种类型的软件更新
- 向受管设备推送运行状况策略并监控其运行状态 管理中心



注释 如果您有 CDO 托管设备，并且仅将本地部署 管理中心 用于分析，则本地部署 管理中心 不支持策略配置或升级。本指南中与设备配置和其他不支持的功能有关的章节和程序不适用于主管理器为 CDO 的设备。

管理中心汇总并关联入侵事件、网络发现信息和设备性能数据，从而能够监控设备报告的相互关联的信息，以及评估网络上出现的整体活动。

可以使用 管理中心来管理设备行为的几乎每个方面。



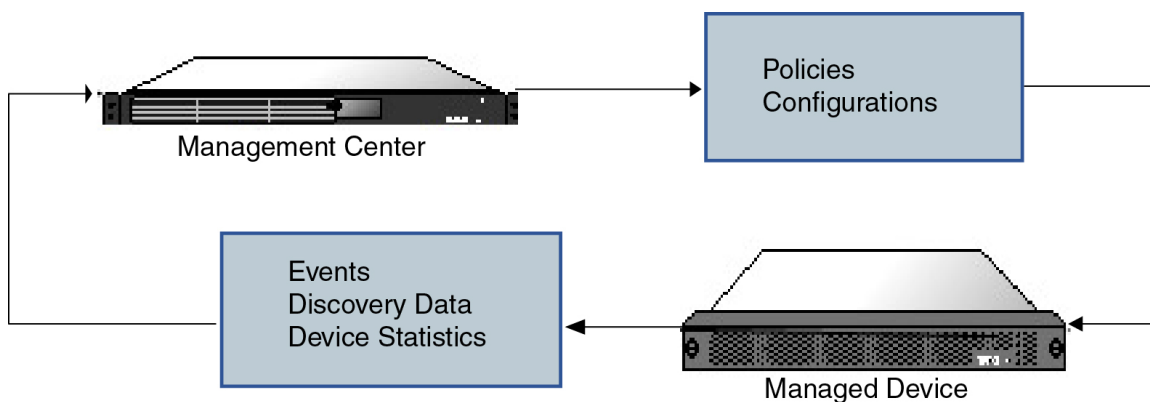
注释 尽管 管理中心 可以按照 <http://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html> 处可用的兼容性矩阵中指定的那样管理运行之前的某些版本的设备，但需要最新版本 威胁防御 软件的新功能不适用于这些以前发布的设备。某些 管理中心 功能可能适用于早期版本。

Cisco Secure Firewall Management Center可以管理哪些内容？

您可以将 Cisco Secure Firewall Management Center 用作集中管理点来管理 威胁防御 设备。

管理设备时，信息通过 SSL 加密的安全 TCP 隧道在 管理中心和该设备之间传输。

下图列出了在管理中心及其托管设备之间传输的内容。请注意，设备间发送的事件和策略的类型基于设备类型。



关于管理连接

使用 管理中心 信息配置设备并将设备添加到 管理中心后，设备或 管理中心 可以建立管理连接。根据初始设置：

- 设备或 管理中心 都可以启动。
- 只有设备可以启动。
- 只有 管理中心 可以发起。

启动始终使用 管理中心 上的 `eth0` 或设备上编号最低的管理接口。如果未建立连接，则会尝试其他管理接口。管理中心上的多个管理接口可让您连接到离散网络或隔离管理和事件流量。但是，发起方不会根据路由表选择最佳接口。



注释 管理连接是信道自身与设备之间的 SSL 加密的安全通信信道。出于安全目的，您不需要通过额外的加密隧道（例如站点间 VPN）运行此流量。例如，如果 VPN 发生故障，您将失去管理连接，因此我们建议使用简单的管理路径。

除策略和事件以外的其他功能

除将策略部署到设备和从其接收事件以外，还可以在 管理中心上执行其他设备相关任务。

备份设备

您无法从 FTD CLI 备份物理受管设备。要备份配置数据和（可选的）统一文件，请使用管理设备 管理中心 执行设备备份。

要备份事件数据，请对管理设备的 管理中心 执行备份。

更新设备

思科会不定期发布 Firepower 系统更新，包括：

- 入侵规则更新，其中可能包含新的和已更新的入侵规则
- 漏洞数据库 (VDB) 更新
- 地理位置更新
- 软件补丁和更新

可以使用 管理中心在其管理的设备上安装更新。

关于设备管理接口

每个设备都包含一个用于与管理中心通信的管理接口。您可以选择将设备配置为使用数据接口进行管理，而不是专用的管理接口。

您可以在管理接口或控制台端口上执行初始设置。

管理接口还用于与智能许可服务器通信、下载更新以及执行其他管理功能。

威胁防御上的管理和事件接口

设置设备时，指定要连接到的管理中心IP地址或主机名称（如已知）。如果设备启动了连接，管理和事件流量都在初始注册时转到此地址。如果管理中心未知，则管理中心建立初始连接。在这种情况下，它最初可能从与威胁防御上指定的不同的管理中心管理接口连接。后续连接应使用具有指定IP地址的管理中心管理接口。

如果管理中心具有单独的仅事件接口，则托管设备会在网络允许的情况下将后续事件流量发送到管理中心仅事件接口。此外，某些托管设备型号包括一个额外的管理接口，您可以为仅事件流量配置该接口。请注意，如果您配置用于管理的数据接口，则不能使用单独的管理接口和事件接口。如果事件网络关闭，则事件流量将恢复到管理中心和/或托管设备上的常规管理接口。

使用威胁防御数据接口进行管理

您可以使用专用的管理接口或常规数据接口与管理中心通信。如果想要从外部接口远程管理威胁防御，或者您没有单独的管理网络，则在数据接口上进行管理器访问非常有用。

管理器访问要求

从数据接口进行管理器访问遵循以下要求。

- 只能在物理数据接口上启用管理器访问。不能使用子接口或 EtherChannel。
- 此接口不能是仅管理接口。
- 仅路由防火墙模式，使用路由接口。
- 不支持 PPPoE。如果您的 ISP 需要 PPPoE，则必须在威胁防御与 WAN 调制解调器之间放入支持 PPPoE 的路由器。
- 接口只能位于全局 VRF 中。
- 默认不对数据接口启用 SSH，因此必须稍后使用管理中心来启用 SSH。由于管理接口网关将更改为数据接口，因此您也无法启动从远程网络到管理接口的 SSH 会话，除非您使用 **configure network static-routes** 命令为管理接口添加静态路由。对于 Amazon Web 服务上的 threat defense virtual，控制台端口不可用，因此您应保持对管理接口的 SSH 访问：在继续配置之前为管理添加静态路由。或者，请确保在配置用于管理器访问的数据接口并断开连接之前完成所有 CLI 配置（包括 **configure manager add** 命令）。
- 您不能使用单独的管理接口和仅事件接口。
- 不支持集群技术。在这种情况下，必须使用管理接口。

- 不支持高可用性。在这种情况下，必须使用管理接口。

每个设备型号的管理接口支持

有关管理接口位置，请参阅您的型号的硬件安装指南。



注释 对于 Firepower 4100/9300，MGMT 接口用于机箱管理，而不是用于威胁防御逻辑设备管理。必须将单独的接口配置为 mgmt（和/或 firepower-eventing）类型，然后将其分配给威胁防御逻辑设备。



注释 对于任何机箱上的威胁防御，物理管理接口在诊断逻辑接口（对 SNMP 或系统日志有用，并且与管理中心中的数据接口一起配置）与管理逻辑接口（用于管理中心通信）之间共享。有关详细信息，请参阅[管理/诊断接口](#)。

有关每个托管设备型号上支持的管理接口，请参阅下表。

表 1: 受管设备上的管理接口支持

型号	管理界面	可选的事件接口
Firepower 1000	management0 注释 management0 是管理 1/1 接口的内部名称。	不支持
Firepower 2100	management0 注释 management0 是管理 1/1 接口的内部名称。	不支持
Secure Firewall 3100	management0 注释 management0 是管理 1/1 接口的内部名称。	不支持
Firepower 4100 和 9300	management0 注释 management0 是此接口的内部名称，与物理接口 ID 无关。	management1 注释 management1 是此接口的内部名称，与物理接口 ID 无关。

型号	管理界面	可选的事件接口
ISA 3000	br1 注释 br1 是管理 1/1 接口的内部名称。	不支持
Cisco Secure Firewall Threat Defense Virtual	eth0	不支持

设备管理接口上的网络路由

管理接口（包括事件专用接口）仅支持通过静态路由到达远程网络。在设置托管设备时，设置进程将为您指定的网关 IP 地址创建一个默认路由。不能删除此路由；只能修改网关地址。



注释 用于管理接口的路由完全独立于您为数据接口配置的路由。如果配置用于管理的数据接口而不是使用专用管理接口，则流量将通过背板路由以使用数据路由表。本节中的信息不适用。

在某些平台上，可以配置多个管理接口（一个管理接口和一个仅事件接口）。默认路由不包括出口接口，因此选择的接口取决于您指定的网关地址以及网关属于哪个接口的网络。如果默认网络上有多个接口，设备将使用编号较低的接口作为出口接口。

如果要访问远程网络，建议为每个管理接口使用至少一个静态路由。我们建议将每个接口放在单独的网络中，以避免潜在的路由问题，包括从其他设备到威胁防御的路由问题。



注释 用于管理连接的接口不由路由表决定。始终首先使用编号最低的接口来进行连接。

NAT 环境

网络地址转换 (NAT) 是一种通过路由器传输和接收网络流量的方法，其中涉及重新分配源或目标 IP 地址。NAT 最常见的用途是允许专用网络与互联网进行通信。静态 NAT 执行 1:1 转换，这不会引发管理中心与设备的通信问题，但端口地址转换 (PAT) 更为常用。PAT 允许您使用单一的公共 IP 地址和独特端口来访问公共网络；这些端口是根据需要动态分配的，因此您无法启动与 PAT 路由器后的设备的连接。

通常，无论是路由目的还是身份验证，都需要两个 IP 地址（连同同一个注册密钥）：管理中心当添加一个设备时，指定设备 IP 地址，设备指定管理中心 IP 地址。但是，如果您只知道其中一个 IP 地址（这是实现路由目的的最低要求），您还必须在连接的两端指定唯一的 NAT ID，以建立对初始通信的信任，并查找正确的注册密钥。管理中心和设备使用注册密钥和 NAT ID（而不是 IP 地址）对初始注册进行身份验证和授权。

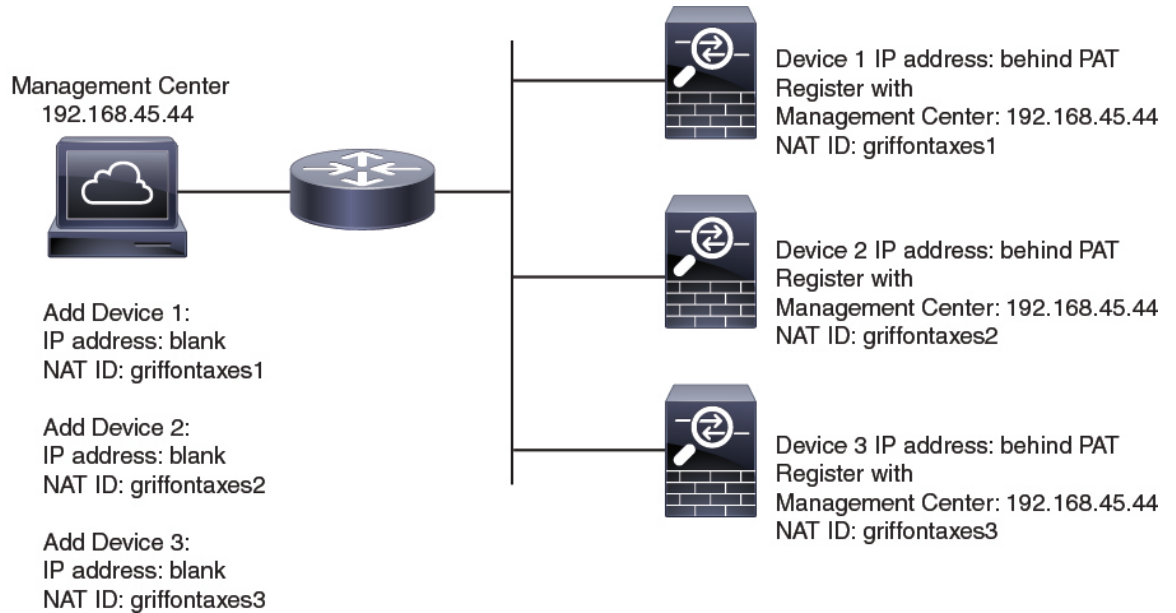
例如，您将设备添加到管理中心，但不知道设备 IP 地址（例如，设备在 PAT 路由器后），因此只需要在管理中心上指定 NAT ID 和注册密钥；将 IP 地址留空。在设备上，指定管理中心 IP 地址、

相同的 NAT ID 和相同的注册密钥。设备将注册到管理中心的 IP 地址。此时，管理中心将使用 NAT ID 而不是 IP 地址对设备进行身份验证。

尽管 NAT ID 最常用于 NAT 环境，但您可以选择使用 NAT ID 来简化向管理中心添加多个设备的过程。在管理中心上，在将 IP 地址留空的同时为要添加的每个设备指定唯一的 NAT ID，然后在每个设备上指定管理中心 IP 地址和 NAT ID。注意：每个设备的 NAT ID 必须是唯一的。

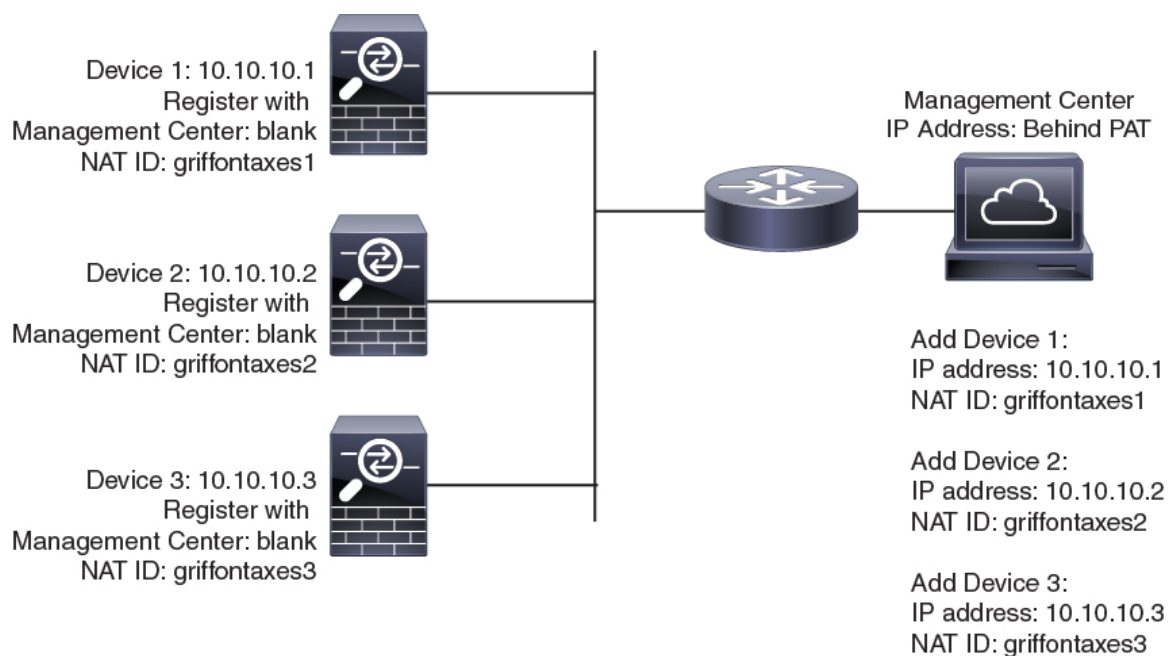
以下示例为 PAT IP 地址后的三个设备。在这种情况下，在管理中心和这些设备上为每个设备指定一个唯一的 NAT ID，并在这些设备上指定管理中心 IP 地址。

图 1: PAT 后的受管设备 NAT ID



以下示例为 PAT IP 地址后的管理中心。在这种情况下，在管理中心和这些设备上为每个设备指定一个唯一的 NAT ID，并在管理中心上指定设备 IP 地址。

图 2: PAT 后的 FMC NAT ID



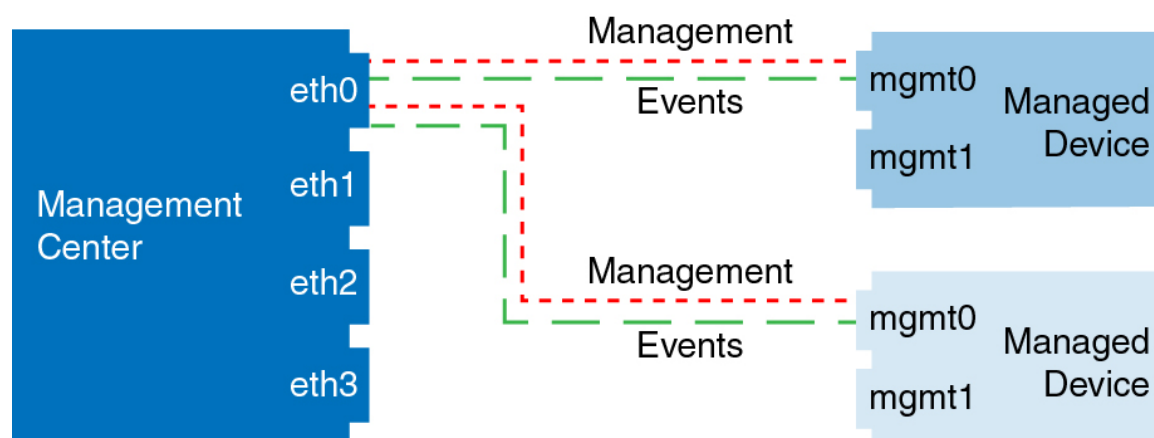
管理和事件流量通道示例



注释 如果在威胁防御上使用数据接口进行管理，则不能对该设备使用单独的管理接口和事件接口。

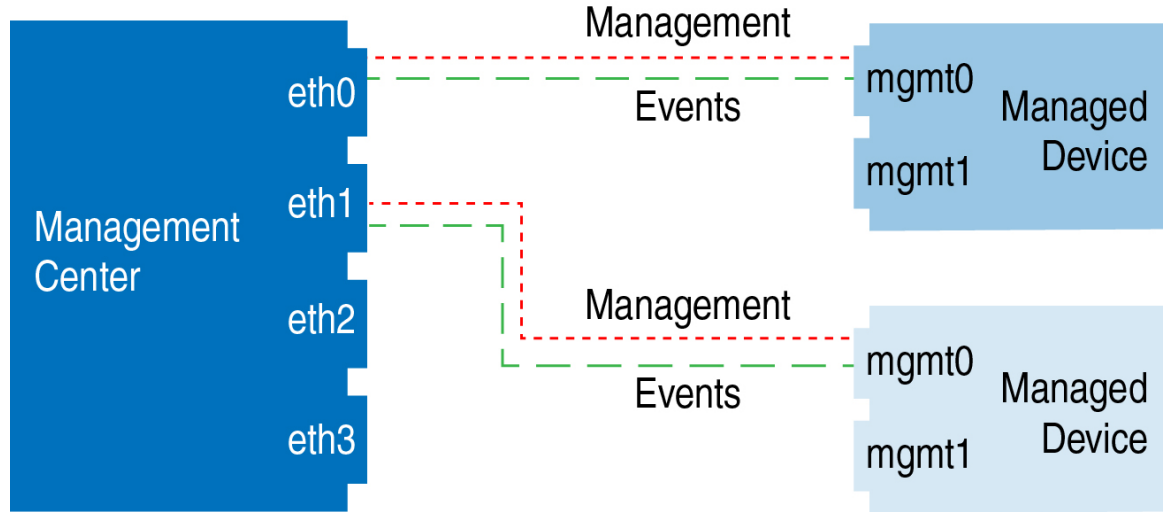
以下示例显示仅使用默认管理接口的管理中心和受管设备。

图 3: Cisco Secure Firewall Management Center 上的单个管理接口



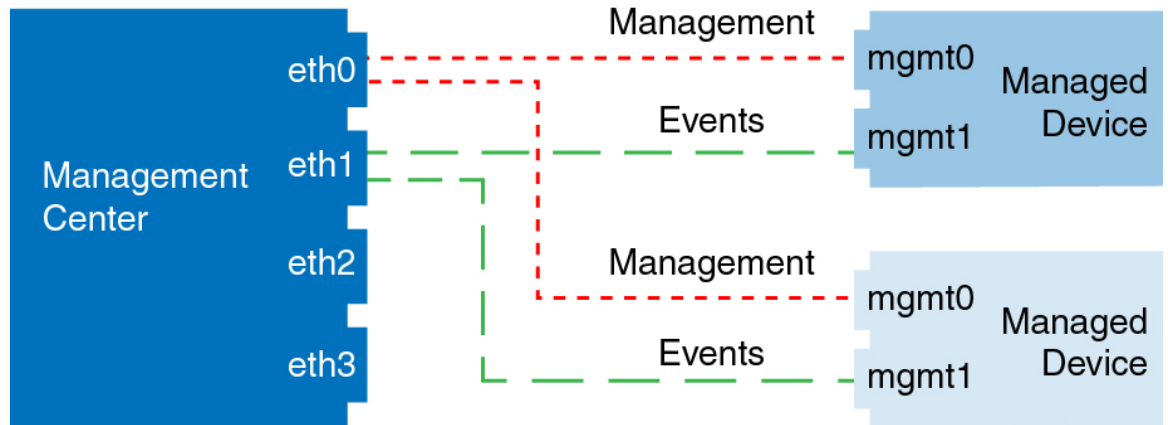
以下示例显示为设备使用单独管理接口的管理中心；每台受管设备均使用 1 管理接口。

图 4: Cisco Secure Firewall Management Center 上的多个管理接口



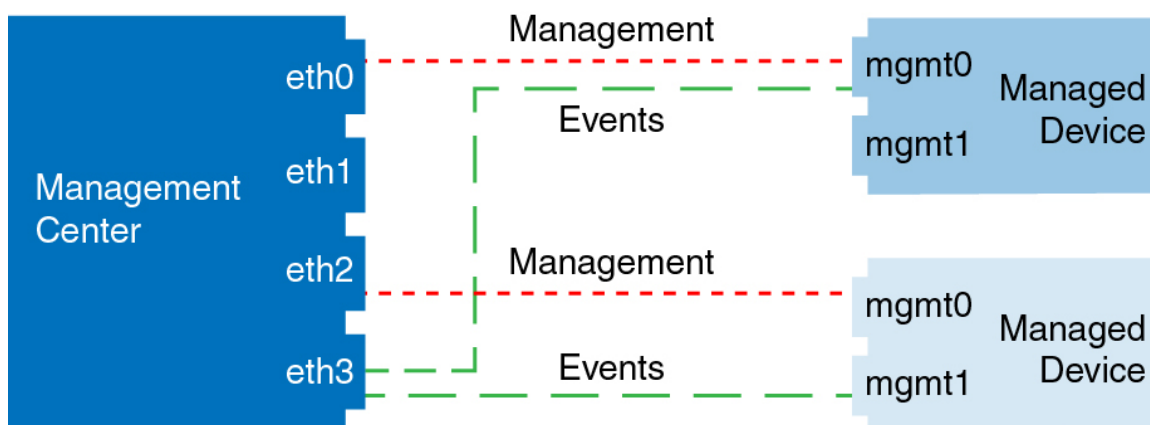
以下示例显示使用单独事件接口的管理中心和受管设备。

图 5: Cisco Secure Firewall Management Center 和受管设备上的单独事件接口



以下示例显示管理中心上多个管理接口与单个事件接口的混合，以及使用单独事件接口或使用单个管理接口的受管设备的混合。

图 6: 混合管理和事件接口用法



设备管理的要求和必备条件

型号支持

任何托管设备；除非在程序中注明。

支持的域

设备所在的域。

用户角色

- 管理员
- 网络管理员

登录 威胁防御 设备上的命令行界面

您可以在 威胁防御 设备上直接登录命令行界面。



注释 当用户连续三次尝试通过 SSH 登录 CLI 失败时，系统会终止 SSH 连接。

开始之前

使用默认 **admin** 用户进行初始登录，完成初始安装过程。创建可以使用 **configure user add** 命令登录 CLI 的其他用户账户。

过程

步骤 1 通过控制台端口或使用 SSH 连接至 威胁防御 CLI。

可以通过 SSH 连接到威胁防御设备的管理接口。如果您为 SSH 连接打开某个数据接口，您也可以连接到该接口上的地址。默认情况下，禁用 SSH 数据接口访问。请参阅[安全外壳 \(Secure Shell\)](#)，以允许与特定数据接口建立 SSH 连接。

对于物理设备，您可以直接连接到设备上的控制台端口。有关控制台电缆的详细信息，请参阅设备的硬件指南。使用以下串行设置：

- 9600 波特率
- 8 个数据位
- 无奇偶校验
- 1 个停止位

在控制台端口上访问的初始 CLI 因设备类型而异。

- ISA 3000-控制台端口上的 CLI 是常规 威胁防御 CLI。
- 其他型号-控制台端口上的 CLI 是 FXOS。您可以使用 **connect ftd** 命令进入 威胁防御 CLI。仅将 FXOS CLI 用于机箱级配置和故障排除。使用 威胁防御 CLI 进行基本配置、监控和正常的系统故障排除。有关 FXOS 命令的信息，请参阅 FXOS 文档。

步骤 2 使用 **admin** 用户名和密码登录。

步骤 3 在 CLI 提示符 (>) 处，使用命令行访问级别所允许的任何命令。

步骤 4 (可选) 访问诊断 CLI：

system support diagnostic-cli

使用此 CLI 可进行高级故障排除。此 CLI 包括额外 **show** 和其他命令。

此 CLI 有两种子模式：用户 EXEC 和特权 EXEC 模式。在特权 EXEC 模式中，有更多命令可用。要进入特权 EXEC 模式，请输入 **enable** 命令；在收到提示时按 Enter 键，无需输入密码。

示例：

```
> system support diagnostic-cli
firepower> enable
Password:
firepower#
```

要返回到常规 CLI，请键入 **Ctrl+a, d**。

完成 威胁防御 初始配置

您可以使用 CLI 完成 威胁防御 初始配置，也可以为除 Firepower 4100/9300 之外的所有 设备管理器 型号完成初始配置。对于 Firepower 4100/9300，部署逻辑设备时，完成所有初始配置。请参阅[Firepower 4100/9300 上的逻辑设备](#)。

使用设备管理器完成威胁防御初始配置

连接到设备管理器以执行威胁防御的初始设置。当您使用设备管理器执行初始设置时，如果您切换到管理中心进行管理，除管理接口和管理器访问设置外，在设备管理器中完成的所有接口配置都将保留。请注意，不会保留其他默认配置设置，例如访问控制策略或安全区。使用 CLI 时，只有管理接口和管理器访问设置会被保留（例如，不保留默认的内部接口配置）。

- 此程序不适用于仅将本地管理中心部署用于分析的 CDO 托管设备。设备管理器配置是为了用于配置主管理器。有关配置设备以便进行分析的详细信息，请参阅[使用 CLI 完成威胁防御初始配置，第 17 页](#)。
- 此程序适用于除 Firepower 4100/9300 和 ISA 3000 以外的所有其他设备。您可以使用设备管理器将这些设备载入管理中心，但由于它们的默认配置不同于其他平台，所以此程序中的详细信息可能会不适用于这些平台。

过程

步骤 1 登录至设备管理器。

- 在浏览器中输入以下 URL。
 - 内部 - <https://192.168.95.1>。
 - 管理 - https://management_ip。管理接口是 DHCP 客户端，因此 IP 地址取决于您的 DHCP 服务器。在此过程中，您必须将管理 IP 地址设置为静态地址，因此我们建议您使用内部接口，以免连接被断开。
- 使用用户名 **admin** 和默认密码 **Admin123** 登录。
- 系统会提示您阅读和接受“最终用户许可协议”并更改管理员密码。

步骤 2 首次登录设备管理器以完成初始配置时，请使用设置向导。您可以选择通过点击页面底部的跳过设备设置 (Skip device setup) 来跳过安装向导。

完成设置向导后，除了内部接口的默认配置外，您还将拥有外部（以太网 1/1）接口的配置，该接口会在您切换到管理中心管理接口时进行维护。

- 为外部接口和管理接口配置以下选项，然后点击下一步 (Next)。
 - 1. 外部接口地址 (Outside Interface Address)** - 此接口通常是互联网网关，并且可用作管理器访问接口。在初始设备设置期间，您不能选择其他外部接口。第一个数据接口是默认的外部接口。

如果要使用与外部（或内部）不同的接口来进行管理器访问，则必须在完成安装向导后手动配置该接口。

配置 IPv4 - 外部接口的 IPv4 地址。可以使用 DHCP，也可以手动输入静态 IP 地址、子网掩码和网关。另外，也可以选择关，不配置 IPv4 地址。您无法使用安装向导配置 PPPoE。如果接口连接到 DSL、电缆调制解调器或 ISP 的其他连接，并且 ISP 使用 PPPoE 来提供 IP 地址，则可能需要使用 PPPoE。您可以在完成向导后配置 PPPoE。

配置 Ipv6 - 外部接口的 Ipv6 地址可以使用 DHCP，也可以手动输入静态 IP 地址、前缀和网关。另外，也可以选择关，不配置 IPv6 地址。

2. 管理接口

如果在 CLI 中执行了初始设置，您将不会看到管理接口设置。

即使您在数据接口上启用管理器访问，也仍会使用管理接口设置。例如，通过数据接口在背板上路由的管理流量将使用管理接口 DNS 服务器解析 FQDN，而非使用数据接口 DNS 服务器。

DNS 服务器 - 系统管理地址的 DNS 服务器。输入 DNS 服务器的一个或多个地址以解析名称。默认值为 OpenDNS 公共 DNS 服务器。如果您编辑字段并想要恢复默认值，请点击使用 **OpenDNS (Use OpenDNS)** 以重新将合适的 IP 地址载入字段。

防火墙主机名 (Firewall Hostname) - 系统管理地址的主机名。

b) 配置时间设置 (NTP) (Time Setting [NTP]) 并点击下一步 (Next)。

1. 时区 - 选择系统时区。

2. NTP 时间服务器 - 选择使用默认 NTP 服务器，还是手动输入 NTP 服务器的地址。可以添加多个服务器来提供备份。

c) 选择启动 90 日评估期而不注册。

不要向智能软件管理器注册威胁防御；所有许可均在管理中心上执行。

d) 点击完成。

e) 系统将提示您选择云管理 (Cloud Management) 或独立 (Standalone)。对于管理中心管理，请选择独立 (Standalone)，然后选择知道了 (Got It)。

步骤 3 （可能需要）配置管理接口。

您可能需要更改管理接口配置，即使您打算使用数据接口访问管理器。如果您使用设备管理器连接的管理接口，则必须重新连接到设备管理器。

- 用于管理器访问的数据接口 - 管理接口必须将网关设置为数据接口。默认情况下，管理接口从 DHCP 接收 IP 地址和网关。如果您没有从 DHCP 接收到网关（例如，您没有将此接口连接到网络），则网关将默认为数据接口，并且您无需进行任何配置。如果您从 DHCP 接收到了网关，则需要使用静态 IP 地址配置此接口，并将该网关设置为数据接口。
- 用于管理器访问的管理接口 - 如果您要配置静态 IP 地址，请确保另将默认网关设置为唯一网关，而不是数据接口。如果您使用 DHCP，则无需进行任何配置，前提是您已成功从 DHCP 获取网关。

步骤 4 如果要配置其他接口，包括要用于管理器访问的外部或内部接口，请选择**设备 (Device)**，然后点击**接口 (Interfaces)** 摘要中的链接。

在向管理中心注册设备时，不会保留其他设备管理器配置。

步骤 5 选择**设备 > 系统设置 > 集中管理**，然后点击**继续**设置管理中心管理。

步骤 6 配置**管理中心/CDO** 详细信息。

图 7:管理中心/CDO 详细信息

Configure Connection to Management Center or CDO

Provide details to register to the management center/CDO.

Management Center/CDO Details

Do you know the Management Center/CDO hostname or IP address?

Yes No

Threat Defense
10.89.5.16
fe80::6a87:c6ff:fea6:4c00/64


→

Management Center/CDO
10.89.5.35

Management Center/CDO Hostname or IP Address

10.89.5.35

Management Center/CDO Registration Key

●●●● 

NAT ID

Required when the management center/CDO hostname or IP address is not provided. We recommend always setting the NAT ID even when you specify the management center/CDO hostname or IP address.

11203

Connectivity Configuration

Threat Defense Hostname

1120-3

DNS Server Group

CustomDNSServerGroup

Management Center/CDO Access Interface

Data Interface

Please select an interface

Management Interface [View details](#)

CANCEL CONNECT

- a) 对于 是否知道管理中心/CDO 主机名或 IP 地址，如果您可以使用 IP 地址或主机名访问 管理中心，请点击 是，如果管理中心 位于 NAT 之后或没有公共 IP 地址或主机名，请点击 否。

必须至少有一个设备（管理中心或威胁防御设备）具有可访问的 IP 地址，才能在两个设备之间建立双向 SSL 加密的通信通道。

- b) 如果您选择是，则输入 **管理中心/CDO 主机名/IP 地址**。
- c) 指定 **管理中心/CDO 注册密钥**。

此密钥是您选择的一次性注册密钥，注册威胁防御设备时也要在管理中心上指定它。注册密钥不得超过 37 个字符。有效字符包括字母数字（A - Z、a - z、0 - 9）和连字符 (-)。此 ID 可用于将多台设备注册到管理中心。

- d) 指定 **NAT ID**。

此 ID 是您选择的唯一一次性字符串，您还需要在管理中心上指定它。如果仅在其中一台设备上指定 IP 地址，则此字段必填；但建议您即使在知道两台设备的 IP 地址时，仍指定 NAT ID。NAT ID 不得超过 37 个字符。有效字符包括字母数字（A - Z、a - z、0 - 9）和连字符 (-)。此 ID 不能用于将任何其他设备注册到管理中心。NAT ID 与 IP 地址结合使用，用于验证连接是否来自正确的设备；只有在对 IP 地址/NAT ID 进行身份验证后，才会检查注册密钥。

步骤 7 配置连接配置。

- a) 指定 **FTD 主机名**。

如果您使用数据接口进行 **管理中心/CDO 访问接口** 访问，则此 FQDN 将用于此接口。

- b) 指定 **DNS 服务器组**。

选择现有组或创建一个新组。默认 DNS 组名为 **CiscoUmbrellaDNSServerGroup**，其中包括 OpenDNS 服务器。

如果要为 **管理中心/CDO 访问接口** 选择数据接口，则此设置会设置数据接口 DNS 服务器。您使用安装向导设置的管理 DNS 服务器用于管理流量。数据 DNS 服务器用于 DDNS（如果已配置）或适用于此接口的安全策略。您可能会选择用于管理的相同 DNS 服务器组，因为管理和数据流量都通过外部接口到达 DNS 服务器。

在管理中心上，数据接口 DNS 服务器在您分配给此威胁防御的平台设置策略中配置。当您威胁防御设备添加到管理中心时，本地设置将保留，并且 DNS 服务器不会添加到平台设置策略。但是，如果稍后将平台设置策略分配给包含 DNS 配置的威胁防御设备，则该配置将覆盖本地设置。我们建议您主动配置与此设置匹配的 DNS 平台设置，以使管理中心和威胁防御设备同步。

此外，仅当在初始注册时发现 DNS 服务器，管理中心才会保留本地 DNS 服务器。

如果要为 **FMC 访问接口** 选择管理接口，则此设置会配置管理 DNS 服务器。

- c) 对于 **管理中心/CDO 访问接口**，请选择任何已配置的接口。

将威胁防御设备注册到管理中心后，您可以将该管理器接口更改为管理接口或另一数据接口。

步骤 8 （可选）如果您选择了数据接口，并且该接口不是外部接口，那么请添加默认路由。

您将看到一条消息，要求您检查是否有通过接口的默认路由。如果您选择了外部接口，那么您已经在安装向导中配置了此路由。如果您选择了其他接口，那么需要在连接到管理中心之前手动配置默认路由。

如果您选择了管理接口，那么需要先将网关配置为唯一网关，然后才能在此屏幕上继续操作。

步骤 9 （可选）如果您选择了数据接口，请点击**添加动态 DNS (DDNS) 方法**。

如果 IP 地址发生变化，DDNS 确保管理中心可接通完全限定域名 (FQDN) 的威胁防御设备。参阅**设备 > 系统设置 > DDNS 服务配置动态 DNS**。

如果您在将威胁防御设备添加到管理中心之前配置 DDNS，则威胁防御设备会自动为 Cisco 受信任根 CA 捆绑包中的所有主要 CA 添加证书，以便威胁防御设备可以验证用于 HTTPS 连接的 DDNS 服务器证书。威胁防御支持任何使用 DynDNS 远程 API 规范的 DDNS 服务器 (<https://help.dyn.com/remote-access-api/>)。

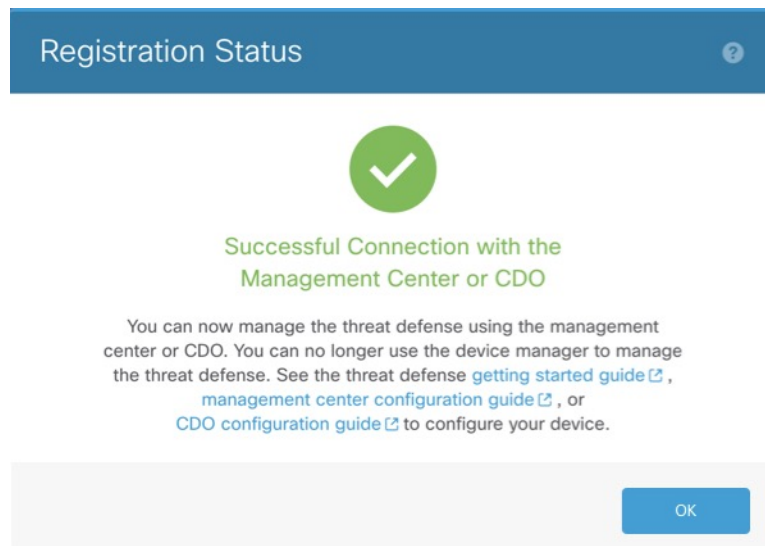
使用管理接口访问管理器时，不支持 DDNS。

步骤 10 点击**连接 (Connect)**。注册状态对话框显示切换到管理中心的当前状态。在**保存管理中心/CDO 注册设置**步骤后，转到管理中心，并添加防火墙。

如果要取消切换到管理中心，请点击**取消注册**。否则，请在**保存管理中心/CDO 注册设置**步骤之后关闭设备管理器浏览器窗口。如果这样做，该过程将暂停，并且只有在您重新连接到设备管理器时才会恢复。

如果您在**保存管理中心/CDO 注册设置**步骤后保持连接到设备管理器，您最终将看到**与管理中心的成功连接或 CDO**对话框。您将断开与设备管理器的连接。

图 8: 成功连接



使用 CLI 完成威胁防御初始配置

连接到威胁防御 CLI 以执行初始设置，包括使用设置向导设置管理 IP 地址、网关和其他基本网络设置。专用管理接口是一种具有自己的网络设置的特殊接口。如果您不想使用管理接口访问管理器，可以使用 CLI 配置数据接口。您还将配置管理中心通信设置。当您使用设备管理器执行初始设置

时，如果您切换到 管理中心 进行管理，除管理接口和管理器访问接口设置外，在 设备管理器 中完成的所有 接口配置都将保留。请注意，不会保留其他默认配置设置，例如访问控制策略。

Before you begin

此过程适用于除 Firepower 4100/9300 之外的所有模式。要在 Firepower 4100/9300 上部署逻辑设备并完成初始配置，请参阅 [Firepower 4100/9300 上的逻辑设备](#)。

Procedure

步骤 1 从控制台端口连接到 威胁防御 CLI，或使用管理接口连接至 SSH，默认情况下其从 DHCP 获取 IP 地址。如果您打算更改网络设置，我们建议使用控制台端口，以免断开连接。

（Firepower 和 Cisco Secure Firewall 硬件型号）控制台端口连接到 FXOS CLI。SSH 会话直接连接到威胁防御 CLI。

步骤 2 使用用户名 **admin** 和密码 **Admin123** 登录。

（Firepower 和 Cisco Secure Firewall 硬件型号）在控制台端口，您可以连接到 FXOS CLI。第一次登录 FXOS 时，系统会提示您更改密码。此密码也用于 SSH 的威胁防御登录。

Note 如果密码已更改，但您不知道，则必须重新映像设备以将密码重置为默认值。对于 Firepower 和 Cisco Secure Firewall 硬件型号：请参阅 [FXOS 故障排除指南](#)，了解 [重新映像程序](#)。对于 ISA 3000：请参阅 [重新映像指南](#) 了解相关说明。

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: *****
Confirm new password: *****
Your password was updated successfully.

[...]

firepower#
```

步骤 3 （Firepower 和 Cisco Secure Firewall 硬件型号）如果已连接到控制台端口上的 FXOS，请连接到 威胁防御 CLI。

connect ftd

Example:

```
firepower# connect ftd
>
```

步骤 4 第一次登录威胁防御时，系统会提示您接受《最终用户许可协议》(EULA)和，如果使用 SSH 连接，则会提示您更改 admin 密码。然后，系统将显示 CLI 设置脚本。

Note 除非清除配置，否则无法重复 CLI 安装向导（例如，通过重新建立映像）。但是，可以稍后在 CLI 中使用 **configure network** 命令更改所有这些设置。请参阅 [威胁防御命令参考](#)。

默认值或以前输入的值会显示在括号中。要接受之前输入的值，请按 **Enter** 键。

Note 即使您在数据接口上启用管理器访问，也仍会使用管理接口设置。例如，通过数据接口在背板上路由的管理流量将使用管理接口 DNS 服务器解析 FQDN，而非使用数据接口 DNS 服务器。

请参阅以下准则：

- 是否要配置 IPv4？ 和/或是否要配置 IPv6？ - 为至少一种地址类型输入 **y**。
- 输入管理接口的 IPv4 默认网关 (Enter the IPv4 default gateway for the management interface) 和/或输入管理接口的 IPv6 默认网关 (Enter the IPv6 gateway for the management interface) - 如果要使用数据接口而不是使用管理接口来进行管理器访问，请选择**手动**。虽然您不打算使用管理接口，但必须设置 IP 地址，例如专用地址。如果管理接口设置为 DHCP，则无法配置数据接口用于管理，因为默认路由（必须是 **data-interfaces**，请参阅下一个要点）可能会被接收自 DHCP 服务器的路由覆盖。
- 输入管理接口的 IPv4 默认网关 (Enter the IPv4 default gateway for the management interface) 和/或 通过 DHCP、路由器或手动方式来配置 IPv6？ (Configure IPv6 via DHCP, router, or manually?) - 如果想要使用数据接口而非管理接口进行管理器访问，请将网关设置为 **data-interfaces**。此设置将在背板上转发管理流量，因此可路由通过管理器访问数据接口。如果要使用管理接口进行管理器访问，应在管理 1/1 网络上设置网关 IP 地址。
- 如果您的网络信息已更改，需要重新连接 - 如果您已建立 SSH 连接，但在初始设置时更改了 IP 地址，连接将断开。使用新 IP 地址和密码重新进行连接。控制台连接不会受影响。
- 本地管理设备？ - 输入 **否** 以使用 管理中心。回答**是**意味着会改用 Firepower 设备管理器。
- 配置防火墙模式？ - 建议您在初始配置时设置防火墙模式。在初始设置后更改防火墙模式将会清除正在运行的配置。请注意，只有路由防火墙模式支持数据接口管理器访问。

Example:

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress. Please stand by.
You must configure the network to continue.
Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [y]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
```

```

Enter an IPv4 address for the management interface [192.168.45.61]: 10.89.5.17
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.89.5.1
Enter a fully qualified hostname for this system [firepower]: 1010-3
Enter a comma-separated list of DNS servers or 'none'
[208.67.222.222,208.67.220.220,2620:119:35::35]:
Enter a comma-separated list of search domains or 'none' [:] : cisco.com
If your networking information has changed, you will need to reconnect.
Disabling IPv6 configuration: management0
Setting DNS servers: 208.67.222.222,208.67.220.220,2620:119:35::35
Setting DNS domains:cisco.com
Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: 10.89.5.1 on management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
DHCP server is already disabled
DHCP Server Disabled
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...

Device is in OffBox mode - disabling/removing port 443 from iptables.
Update policy deployment information
  - add device configuration
  - add network discovery
  - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required. In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>

```

步骤 5 确定将管理此威胁防御的管理中心。

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} reg_key [nat_id]
[display_name]
```

Note 如果您使用 CDO 进行管理，请在此步骤中使用 CDO 生成的 **configure manager add** 命令。

- {hostname | IPv4_address | IPv6_address | DONTRESOLVE} - 指定管理中心的 FQDN 或 IP 地址。如果管理中心不能直接寻址，请使用 **DONTRESOLVE** 并指定 *nat_id*。必须至少有一个设

备（管理中心 或 威胁防御）具有可访问的 IP 地址，才能在两个设备之间建立双向 SSL 加密的通信通道。如果在此命令中指定 **DONTRESOLVE**，则 FTD 必须有可访问的 IP 地址或主机名。

- *reg_key* - 指定您选择的一次性注册密钥，注册威胁防御时也要在管理中心上指定它。注册密钥不得超过 37 个字符。有效字符包括字母数字（A - Z、a - z、0 - 9）和连字符 (-)。
- *nat_id* - 指定您选择的唯一的一次性字符串，注册威胁防御时若一方没有指定可访问的 IP 地址或主机名，则也要在管理中心上指定它。例如，如果将管理中心设置为 **DONTRESOLVE**，则需要指定它。如果您使用数据接口进行管理，即使您指定了 IP 地址，也必须指定它。NAT ID 不得超过 37 个字符。有效字符包括字母数字（A - Z、a - z、0 - 9）和连字符 (-)。此 ID 不能用于将任何其他设备注册到管理中心。

Note 如果使用数据接口进行管理，即使您同时指定了两个 IP 地址，也必须同时在威胁防御和管理中心上指定 NAT ID。

- *display_name* - 使用 **show managers** 命令提供用于显示此管理器的显示名称。如果您将 CDO 标识为仅用于分析的主用管理器和本地部署管理中心，则此选项非常有用。如果不指定此参数，防火墙将使用以下方法之一自动生成显示名称：

- *hostname* | *IP_address*（如果不使用 **DONTRESOLVE** 关键字）
- *manager-timestamp*

Example:

```
> configure manager add MC.example.com 123456
Manager successfully configured.
```

Example:

如果管理中心位于 NAT 设备之后，请输入唯一的 NAT ID 以及注册密钥，并指定 **DONTRESOLVE** 而非主机名，例如：

```
> configure manager add DONTRESOLVE regk3y78 natid90
Manager successfully configured.
```

Example:

如果威胁防御位于 NAT 设备之后，请输入唯一的 NAT ID 以及管理中心 IP 地址或主机名，例如：

```
> configure manager add 10.70.45.5 regk3y78 natid56
Manager successfully configured.
```

步骤 6 如果您使用 CDO 作为主要管理器，并希望仅将本地部署管理中心用于分析，请确定本地部署管理中心。

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} reg_key [nat_id]
[display_name]
```

Example:

以下示例使用为 CDO 生成的命令，添加显示名称“CDO”，然后指定仅用于分析的本地部署管理中心。

```
> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
LzmlHOynhVUWhXYWz2swmkj2ZWsn3Lb account1.app.us.cdo.cisco.com
Manager successfully configured.
> configure manager add 10.70.45.5 regk3y78 natid56 analytics-FMC
Manager successfully configured.
```

步骤 7 (Optional) 配置用于管理器访问的数据接口。

configure network management-data-interface

然后，系统会提示您为数据接口配置基本网络设置。

Note 使用此命令时，应使用控制台端口。如果使用 SSH 访问管理接口，连接可能会断开，您必须重新连接到控制台端口。有关 SSH 用法的详细信息，请参阅下文。

请参阅以下有关使用此命令的详细信息。另请参阅[使用 威胁防御 数据接口进行管理](#), on page 4。

- 如果您要使用数据接口进行管理，则原始管理接口无法使用 DHCP。如果在初始设置期间没有手动设置 IP 地址，则可以使用 **configure network {ipv4 | ipv6} manual** 命令立即设置它。如果您尚未将管理接口网关设置为 **data-interfaces**，此命令将立即设置它。
- 当您将 威胁防御 添加到 管理中心时，管理中心 会发现并维护接口配置，包括以下设置：接口名称和 IP 地址、网关静态路由、DNS 服务器和 DDNS 服务器。有关 DNS 服务器配置的详细信息，请参阅下文。在管理中心中，您可以稍后对管理器访问接口配置进行更改，但要确保更改不会阻止 威胁防御 或 管理中心 重新建立管理连接。如果管理连接中断，威胁防御 将包含 **configure policy rollback** 命令以恢复以前的部署。
- 如果配置 DDNS 服务器更新 URL，则 威胁防御 会自动添加来自 Cisco 受信任根 CA 捆绑包的所有主要 CA 证书，以便 威胁防御 可以验证用于 HTTPS 连接的 DDNS 服务器证书。威胁防御 支持使用 DynDNS 远程 API 规范 (<https://help.dyn.com/remote-access-api/>) 的任何 DDNS 服务器。
- 此命令设置数据接口 DNS 服务器。使用设置脚本（或使用 **configure network dns servers** 命令）设置的管理 DNS 服务器用于管理流量。数据 DNS 服务器用于 DDNS（如果已配置）或适用于此接口的安全策略。

在管理中心上，数据接口 DNS 服务器在您分配给此 威胁防御 的平台设置策略中配置。当您 将 威胁防御 添加到 管理中心 时，本地设置将保留，并且 DNS 服务器不会添加到平台设置策略。但是，如果稍后将平台设置策略分配给包含 DNS 配置的 威胁防御，则该配置将覆盖本地设置。我们建议您主动配置与此设置匹配的 DNS 平台设置，以使 管理中心 和 威胁防御 同步。

此外，仅当在初始注册时发现 DNS 服务器，管理中心 才会保留本地 DNS 服务器。例如，如果您使用管理接口注册了设备，但随后使用 **configure network management-data-interface** 命令配置数据接口，则必须在 管理中心 中手动配置所有这些设置（包括 DNS 服务器），以便与 FTD 配置匹配。

- 将 威胁防御 注册到 管理中心 后，您可以将该管理接口更改为管理接口或另一数据接口。
- 您在安装向导中设置的 FQDN 将用于此接口。
- 您可以通过命令清除整个设备配置；在恢复场景中可使用此选项，但我们不建议您在初始设置或正常操作中使用它。
- 要禁用数据管理，请输入 **configure network management-data-interface disable** 命令。

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

步骤 8 (Optional) 限制在特定网络上通过数据接口访问管理器。

```
configure network management-data-interface client ip_address netmask
```

默认情况下，允许所有网络。

What to do next

将设备注册到 管理中心。

配置事件接口

您始终需要用于管理通信的管理接口。如果您的设备有第二个管理接口，例如，Firepower4100/9300，则可以为仅事件流量启用该接口。

开始之前

要使用单独的事件接口，您还需要在 管理中心 上启用事件接口。请参阅《[Cisco Secure Firewall Management Center 管理指南](#)》。

过程

步骤 1 启用第二个管理接口作为仅事件的接口。

```
configure network management-interface enable management1
```

```
configure network management-interface disable-management-channel management1
```

您可以选择使用 **configure network management-interface disable-events-channel** 命令禁用主管理接口的事件。不管是哪种情况，设备都会尝试通过事件专属接口发送事件，如果该接口关闭，那么即使您禁用了事件通道，设备也会通过管理接口发送事件。

无法同时禁用接口上的事件通道和管理通道。

示例:

```
> configure network management-interface enable management1  
Configuration updated successfully  
  
> configure network management-interface disable-management-channel management1  
Configuration updated successfully  
  
>
```

步骤 2 配置事件接口的 IP 地址。

事件接口可以与管理接口位于不同的网络中，也可以位于同一网络中。

a) 配置 IPv4 地址:

```
configure network ipv4 manual ip_address netmask gateway_ip management1
```

请注意，此命令中的 *gateway_ip* 用于为设备创建默认路由，因此，您应该输入已经为 `management0` 接口设置的值。它不会为事件接口创建单独的静态路由。如果您在与管理接口不同的网络上使用仅事件接口，我们建议您为仅事件接口创建静态路由。

示例:

```
> configure network ipv4 manual 10.10.10.45 255.255.255.0 10.10.10.1 management1  
Setting IPv4 network configuration.  
Network settings changed.  
  
>
```

b) 配置 IPv6 地址:

- 无状态自动配置:

```
configure network ipv6 router management1
```


示例:

```
> configure network ipv6 router management1
Setting IPv6 network configuration.
Network settings changed.

>
```

- 手动配置:

```
configure network ipv6 manual ip6_address ip6_prefix_length management1
```

示例:

```
> configure network ipv6 manual 2001:0DB8:BA98::3210 64 management1
Setting IPv6 network configuration.
Network settings changed.

>
```

步骤 3 如果管理中心位于远程网络上，则将为仅事件接口添加静态路由；否则，所有流量都将通过管理接口与默认路由匹配。

```
configure network static-routes {ipv4 | ipv6} add management1 destination_ip netmask_or_prefix gateway_ip
```

对于默认路由，请勿使用此命令；当您使用 **configure network ipv4** 或 **ipv6** 命令时，只能更改默认路由网关 IP 地址（请参阅步骤 [步骤 2](#)，第 24 页）。

示例:

```
> configure network static-routes ipv4 add management1 192.168.6.0 255.255.255.0 10.10.10.1
Configuration updated successfully

> configure network static-routes ipv6 add management1 2001:0DB8:AA89::5110 64
2001:0DB8:BA98::3211
Configuration updated successfully

>
```

要显示静态路由，请输入 **show network-static-routes**（不显示默认路由）：

```
> show network-static-routes
-----[ IPv4 Static Routes ]-----
Interface           : management1
Destination         : 192.168.6.0
Gateway             : 10.10.10.1
Netmask             : 255.255.255.0
[...]
```

将设备添加到 管理中心

按照此程序将单个设备添加到 管理中心。如果您计划链接设备以实现高可用性，则仍必须使用此程序；请参阅[添加高可用性对](#)。有关集群，请参阅您的型号的集群章节。

您还可以使用此程序添加由 CDO 交付的云管理 管理中心的设备，并且您希望仅将本地 管理中心 部署用于事件日志记录和分析目的。



注释 如果已建立或将要建立 管理中心高可用性，则仅将设备添加到主用（或预期为主用）管理中心。建立高可用性时，注册到主用 管理中心的设备将自动注册到备用设备。

开始之前

- 将设备设置为由 管理中心管理。请参阅：
 - [完成 威胁防御 初始配置，第 12 页](#)
 - 《适用于您的型号的入门指南》
- 必须注册到智能软件管理器。管理中心有效的评估许可证就足够了，但如果许可证到期，您将无法添加新设备，直到您成功注册。
- 如果注册了一个使用 IPv4 的设备并要将其转换为 IPv6，则必须删除并重新注册该设备。

过程

- 步骤 1** 选择设备 > 设备管理。
- 步骤 2** 从 添加 下拉菜单中，选择 设备。

图 9: 添加设备

Add Device ?

CDO Managed Device

Host:†

Display Name:

Registration Key: *

Group:

Access Control Policy: *

Smart Licensing
Note: All virtual Firewall Threat Defense devices require a performance tier license. Make sure your Smart Licensing account contains the available licenses you need. It's important to choose the tier that matches the license you have in your account. Click [here](#) for information about the Firewall Threat Defense performance-tiered licensing. Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.

Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):

Malware
 Threat
 URL Filtering

Advanced
Unique NAT ID: †

Transfer Packets

步骤 3 如果要将在 CDO 托管设备添加到本地 管理中心 部署仅用于分析，请选中 **CDO 托管设备 (CDO Managed Device)**

系统会隐藏许可和数据包传输设置，因为它们由 CDO 管理。您可以跳过这些步骤。

图 10: 为 CDO 添加设备

步骤 4 在主机字段中，输入要添加的设备的 IP 地址或主机名。

设备的主机名是完全限定域名或通过本地 DNS 解析为有效 IP 地址的名称。如果网络使用 DHCP 来分配 IP 地址，请使用主机名而不是 IP 地址。

在 NAT 环境中，如果在将设备配置为由管理中心管理时已经指定管理中心的 IP 地址或主机名，则可能无需指定设备的 IP 地址或主机名。有关详细信息，请参阅[NAT 环境，第 6 页](#)。

注释 在管理中心高可用性环境中，当两个管理中心都位于 NAT 之后时，要在辅助管理中心上注册威胁防御，必须在**主机 (Host)** 字段中指定一个值。

步骤 5 在显示名称字段中，输入要在管理中心中显示的设备名称。

步骤 6 在注册密钥字段中，输入将设备配置为由管理中心管理时所使用的同一注册密钥。注册密钥是一个一次性的共享密钥。密钥可以包含字母数字字符和连字符 (-)。

步骤 7 在多域部署中，无论当前的域是什么，都将该设备分配给叶域。

如果当前域是叶域，设备会自动添加到当前域。如果当前域不是叶域，则注册后必须切换到叶域才能配置设备。一台设备只能属于一个域。

步骤 8 (可选) 将设备添加到设备组。

步骤 9 选择初始访问控制策略以在注册时部署到设备，或创建一个新策略。

如果设备与所选策略不兼容，部署会失败。这种不兼容有多种可能的原因，包括许可不匹配、型号限制、被动与内联问题和其他配置错误。请在解决导致失败的问题后，手动将配置部署到设备。

步骤 10 选择要应用到设备的许可证。

在添加设备后，您可以从系统 (**System**) > 许可证 (**Licenses**) > 智能许可证 (**Smart Licenses**) 页面应用许可证。

仅对于 **threat defense virtual**，您还必须选择性能层。选择与您账户中的许可证相匹配的级别很重要。在选择级别之前，您的设备默认为 **FTDv50** 选项。有关可用于 **threat defense virtual** 的性能分层许可证授权的详细信息，请参阅《Cisco Secure Firewall Management Center 管理指南》中的 **FTDv** 许可证。

注释 如果要将 **threat defense virtual** 升级到 7.0+ 版，可以选择 **FTDv - 变量 (FTDv - Variable)** 来保持当前的许可证合规性。

步骤 11 如果在设备安装过程中使用了 NAT ID，在高级 (**Advanced**) 部分中，请在唯一 NAT ID (**Unique NAT ID**) 字段中输入相同的 NAT ID。

唯一 NAT ID (Unique NAT ID) 指定您选择的唯一的一次性字符串，若一方未指定可连通的 IP 地址或主机名时，您也可以在初始设置时在威胁防御上指定该字符串。例如，如果您将主机 (**Host**) 字段留空，则为必填项。如果您使用威胁防御数据接口进行管理，即使您指定了 IP 地址，也必须指定它。NAT ID 不得超过 37 个字符。有效字符包括字母数字 (A - Z、a - z、0 - 9) 和连字符 (-)。此 ID 不能用于将任何其他设备注册到管理中心。

注释 如果使用威胁防御上的数据接口进行管理，即使您同时指定了两个 IP 地址，也必须同时在威胁防御和管理中心上指定 NAT ID。

步骤 12 选中传输数据包复选框以允许设备将数据包传输到管理中心。

默认情况下，此选项已启用。如果在启用此选项时触发了 IPS 或 Snort 等事件，设备会将事件元数据信息和数据包数据发送到管理中心进行检测。如果禁用此选项，则仅发送事件信息到管理中心，不发送数据包数据。

步骤 13 点击 **Register**。

管理中心可能需要长达两分钟来验证设备的心跳并建立通信。如果注册成功，设备将添加到列表中。如果注册失败，您会看到一则错误消息。如果设备注册失败，请检查以下项：

- Ping - 访问设备 CLI，然后使用以下命令 ping 管理中心 IP 地址：

```
ping system ip_address
```

如果 ping 不成功，使用 **show network** 命令检查网络设置。如果需要更改设备 IP 地址，使用 **configure network {ipv4 | ipv6} manual** 命令。

- 注册密钥、NAT ID 和管理中心 IP 地址 - 确保在两个设备上使用相同的注册密钥和 NAT ID（如有使用）。可以在设备上使用 **configure manager add** 命令设定注册密钥和 NAT ID。

有关更多故障排除信息，请参阅 <https://cisco.com/go/fmc-reg-error>。

从管理中心删除（取消注册）设备

如果不希望再管理设备，可以将其从管理中心中取消注册。

要取消注册集群、集群节点或高可用性对，请参阅这些部署的章节。

取消注册设备：

- 会切断管理中心和该设备之间的所有通信。
- 从设备管理 (**Device Management**) 页面删除设备。
- 如果设备的平台设置策略配置为使用 NTP 从管理中心接收时间，则将设备返回本地时间管理。
- 让配置保持不变，以便设备继续处理流量。

NAT 和 VPN、ACL 等策略以及接口配置保持不变。

将设备再次注册到相同或不同的管理中心会导致配置被删除，因此设备将在该点停止处理流量。您可以在注册时选择访问控制策略，但必须在注册后重新应用其他策略，然后在再次处理流量之前部署配置。

过程

步骤 1 选择设备 > 设备管理。

步骤 2 在要取消注册的设备旁边，点击删除 (🗑️)。

步骤 3 确认您要取消注册设备。

添加设备组

管理中心允许将设备分组，从而可以在多台设备上轻松部署策略和安装更新。您可以展开和折叠组中的设备列表。

在多域部署中，您可以只在分叶域内创建设备组。当您为多租户配置 Cisco Secure Firewall Management Center 时，现有设备组会被删除；您可以在分叶域级别重新添加这些组。

如果将高可用性对中的主设备添加到某个组，则系统会将两台设备均添加到该组中。如果取消高可用性，则两台设备均会保留在该组中。

过程

步骤 1 选择设备 > 设备管理。

步骤 2 从添加 (**Add**) 下拉菜单中，选择添加组 (**Add Group**)。

要编辑现有的组，请点击要编辑的组的 **编辑** (✎)。

步骤 3 输入 **Name**。

步骤 4 在可用设备 (**Available Devices**) 下，选择一台或多台要添加到设备组的设备。点击的同时使用 **Ctrl** 或 **Shift** 选择多台设备。

步骤 5 点击 **添加 (Add)** 将所选设备包含在设备组中。

步骤 6 或者，要将设备从设备组中删除，请点击要删除的设备旁边的 **删除** (🗑)。

步骤 7 点击 **确定 (OK)** 以添加组。

关闭或重新启动设备

正确关闭系统非常重要。仅拔掉电源或按下电源开关可能会导致文件系统严重损坏。请记住，有许多进程一直在后台运行，拔掉或关闭电源不能正常关闭防火墙。

请参阅以下任务以正确关闭或重启系统。



注释 重新启动设备后，您可能会看到无法重新建立管理连接的错误。在某些情况下，在设备上的管理接口准备就绪之前尝试连接。系统将自动重试连接，并应在 15 分钟内建立连接。

过程

步骤 1 选择 **设备 > 设备管理**。

步骤 2 在要重新启动的设备旁边，点击 **编辑** (✎)。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 点击 **设备 (Device)**。

步骤 4 要重启设备：

- 请点击 **重启设备** (🔄)。
- 出现提示时，确认是否要重启设备。

步骤 5 要关闭设备：

- 在 **系统 (System)** 部分中点击 **关闭设备** (⊗)。
- 出现提示时，确认是否要关闭设备。
- 如果您与防火墙建立了控制台连接，请在防火墙关闭时留意系统提示。您将看到以下提示：

```
System is stopped.  
It is safe to power off now.  
Do you want to reboot instead? [y/N]
```

如果没有控制台连接，请等待大约 3 分钟以确保系统已关闭。

配置设备设置

设备 > 设备管理 页面为您提供一系列信息和选项：

- “查看方式” (View By) - 使用此选项可根据组、许可证、型号、或访问控制策略查看设备。
- “设备状态” (Device State) - 您还可以根据设备的状态来查看设备。您可以点击状态图标查看属于它的设备。括号内为各状态所对应的的设备数量。
- “搜索” (Search) - 您可以通过提供设备名称、主机名或 IP 地址来搜索已配置的设备。
- “添加选项” (Add options) - 您可以添加设备、高可用性对、集群和组。
- “编辑和其他操作” (Edit and other actions) - 针对每个已配置的设备，使用 **编辑** (✎) 图标来编辑设备参数和属性。点击 **更多** (⋮) 图标并执行其他操作：
 - “访问控制策略” (Access Control Policy) - 点击访问控制策略列中的链接以查看部署到设备的策略。
 - “删除” (Delete) - 删除设备。
 - “数据包跟踪器” (Packet Tracer) - 导航至数据包跟踪器页面，以便通过将模型数据包注入系统来检查设备上的策略配置。
 - “数据包捕获” (Packet Capture) - 导航至数据包捕获页面，您可以在其中查看系统在处理数据包时所采取的判定和操作。
 - “恢复升级” (Revert Upgrade) - 恢复上次升级后所做的升级和配置更改。此操作会将设备恢复到升级前的版本。
 - “运行状况监控器” (Health Monitor) - 导航至设备的运行状况监控页面。
 - “故障排除文件” (Troubleshooting Files) - 生成故障排除文件，您可以在其中选择要在报告中包含的数据类型。
 - 对于 Firepower 4100/9300 系列设备，是一个指向 机箱管理器 Web 界面的链接。

点击设备时，系统将显示包含多个选项卡的设备属性页面。您可以使用选项卡来查看设备信息，以及配置路由、接口、内联集和 DHCP。

编辑常规设置

设备 (Device) 页面上的 **常规 (General)** 部分会显示下表所述信息。

表 2: “常规” (General) 部分表字段

字段	说明
名称	管理中心上的设备的显示名称。
传输数据包	显示受管设备是否将数据包数据随事件一起发送到 管理中心。
模式	显示设备的管理接口的模式： 路由 或 透明 。
合规模式	显示设备的安全认证合规性。有效值为 CC、UCAPL 和 None。
TLS 加密加速：	显示 TLS 加密加速是已启用还是已禁用。
设备配置	允许您复制、导出或导入配置。请参阅 将配置复制到另一台设备，第 33 页 和 导出和导入设备配置，第 35 页 。

您可以在此部分编辑其中一些设置。

过程

步骤 1 选择 **设备 > 设备管理**。

步骤 2 在要修改的设备名单旁，点击 **编辑** (✎)。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 点击 **设备 (Device)**。

步骤 4 在 **常规 (General)** 部分中，点击 **编辑** (✎)。

- 输入托管设备的名称 (**Name**)。
- 选择 **转换数据包 (Transfer Packets)** 复选框以允许数据包数据随事件一起存储在 管理中心 上。
- 点击 **强制部署 (Force Deploy)** 以强制将当前策略和设备配置部署到设备。

注释 强制部署比常规部署需要更多时间，因为它涉及要在 威胁防御 上部署的策略规则的完整生成。

步骤 5 有关 **设备配置** 操作，请参阅[将配置复制到另一台设备，第 33 页](#)和[导出和导入设备配置，第 35 页](#)。

步骤 6 点击 **部署 (Deploy)**。

下一步做什么

- 部署配置更改；请参阅[部署配置更改](#)。

将配置复制到另一台设备

在网络中部署新设备时，可以直接复制预配置设备上的配置和策略，而无需手动重新配置新设备。

开始之前

确认：

- 源和目标 威胁防御 设备型号相同并运行同一版本的软件。
- 源设备为独立 Cisco Secure Firewall Threat Defense设备或 Cisco Secure Firewall Threat Defense高可用性对。
- 目标设备为独立 威胁防御设备。
- 源和目标 威胁防御设备具有相同数量的物理接口。
- 源和目标 威胁防御设备的防火墙模式相同 - 路由或透明。
- 源和目标 威胁防御设备的安全认证合规性模式相同。
- 源和目标 威胁防御设备在同一域中。
- 源或目标 威胁防御设备上未在进行配置部署。

过程

步骤 1 选择设备 > 设备管理。

步骤 2 在要修改的设备名单旁，点击 **编辑** (✎)。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 点击 **设备**。

步骤 4 在常规部分中，执行以下操作之一：

- 点击 **获取设备配置** (↓) 以将设备配置从其他设备复制到新设备。在**获取设备配置**页面中，从**选择设备**下拉列表中选择源设备。
- 点击 **推送设备配置** (↑) 以将设备配置从当前设备复制到新设备。在**推送设备配置**页面上，从**目标设备**下拉列表中选择复制配置的目标设备。

步骤 5 (可选) 选中**包括共享策略配置 (Include shared policies configuration)** 复选框以复制策略。

共享策略 (例如访问控制策略、NAT、平台设置和 FlexConfig 策略) 可在多个设备之间共享。

步骤 6 点击**确定**。

您可以在消息中心中的 **任务 (Tasks)** 监控复制设备配置任务的状态。

复制设备配置任务发起后，便会擦除目标设备上的配置，并将源设备的配置复制到目标设备。



警告 完成复制设备配置任务后，无法将目标设备还原为其原始配置。

导出和导入设备配置

您可以导出设备特定的配置：

- 接口
- 内联集
- 路由
- DHCP
- 关联对象

然后，您可以在以下使用案例中为同一设备导入已保存的配置：

- 将设备移动到其他管理中心 - 首先从原始管理中心中删除设备，然后将设备添加到新的管理中心。然后，您可以导入保存的配置。
- 在域之间移动设备 - 在域之间移动设备时，不会保留某些设备特定的配置，因为新域中不存在支持对象（例如安全区域的接口组）。通过在域移动后导入配置，将为该域创建任何必要的对象，并恢复设备配置。
- 恢复旧配置 - 如果部署的更改会对设备的运行产生负面影响，则可以导入已知工作配置的备份副本，以恢复以前的运行状态。
- 重新注册设备 - 如果从管理中心中删除设备，但随后想要重新添加，则可以导入已保存的配置。

请参阅以下准则：

- 您只能将配置导入到同一设备（UUID 必须匹配）。您无法将配置导入到其他设备，即使是同一型号也是如此。
- 请勿在导出和导入的间隙更改设备上运行的版本；版本必须匹配。
- 将设备移至其他管理中心时，目标管理中心版本必须与源版本相同。
- 如果对象不存在，系统将创建该对象。如果对象存在，但值不同，请参阅下文：

表 3: 对象导入操作

场景	导入操作
存在具有相同名称的对象	重用现有对象

场景	导入操作
存在名称相同但值不同的对象	<ul style="list-style-type: none"> 网络和端口对象 - 为此设备创建对象覆盖。请参阅对象覆盖。 接口对象 - 创建新对象。例如，如果类型（安全区域或接口组）和接口类型（例如，路由或交换）不匹配，则会创建新对象。 所有其他对象 - 即使值不同，也可重复使用现有对象。
对象不存在	创建新对象

过程

步骤 1 选择设备 > 设备管理。

步骤 2 在要编辑的设备旁边，点击 **编辑** (✎)。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 点击 **设备**。

步骤 4 导出配置。

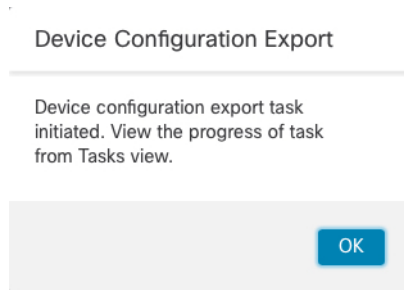
a) 在常规 (**General**) 区域，点击**导出 (Export)**。

图 11: 导出设备配置



系统将提示您确导出；点击**确定 (OK)**。

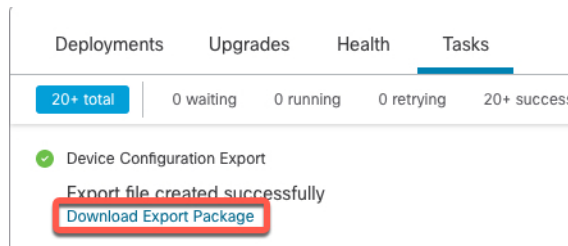
图 12: 确认导出



您可以在任务 (Tasks) 页面中查看导出进度。

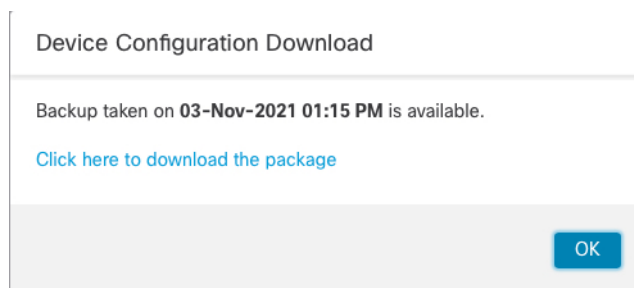
- b) 在通知 (Notifications) > 任务 (Tasks) 页面上, 确保导出已完成; 点击下载导出包 (Download Export Package)。或者, 您可以点击常规 (General) 区域中的下载 (Download) 按钮。

图 13: 导出任务



系统将提示您下载软件包; 点击[点击此处下载软件包 \(Click here to download the package\)](#) 以本地保存文件, 然后点击**确认 (OK)** 以退出对话框。

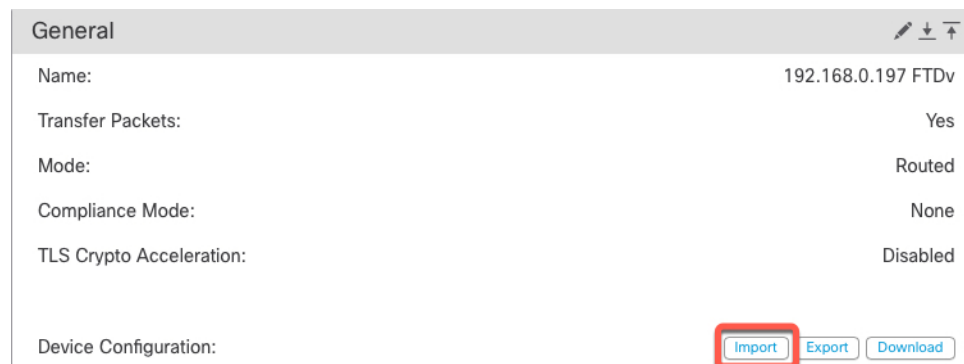
图 14: 下载软件包



步骤 5 导入配置。

- a) 在常规 (General) 区域中, 点击**导入 (Import)**。

图 15: 导入设备配置



系统将提示您确认将替换当前配置。点击是 (**Yes**)，然后导航到配置包（使用后缀 **.sfo**；请注意，此文件与备份/恢复文件不同）。

图 16: 导入软件包

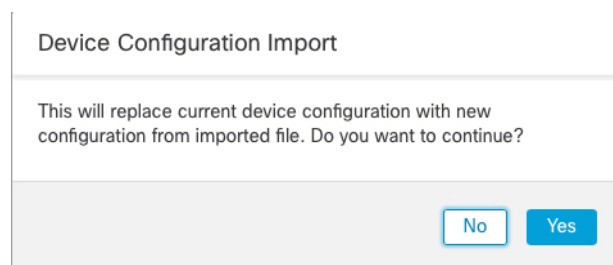
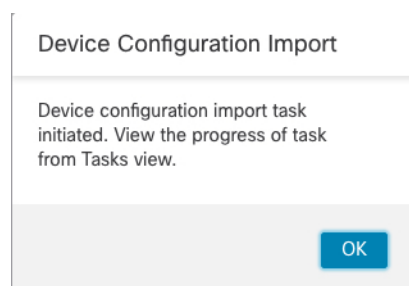


图 17: 导航至软件包



系统将提示您确认导入；点击确认 (**OK**)。

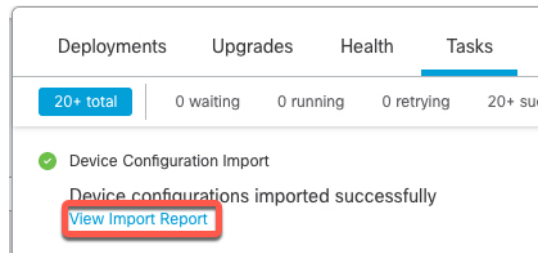
图 18: 确认导入



您可以在任务 (**Tasks**) 页面中查看导入进度。

- b) 查看导入报告，以便查看导入的内容。在导入任务的通知 (**Notifications**) > 任务 (**Tasks**) 页面上，点击查看导入报告 (**View Import Report**)。

图 19: 查看导入报告



设备配置导入报告 (Device Configuration Import Reports) 页面提供可用报告的链接。

Cisco Firepower Management Center

Device Configuration Import Reports

Device	Shared Policies	Device Configurations
0434ef00-15bb-11ec-bb94-93bdde3ad19d	Report does not exist	Device configurations import report

编辑许可证设置

设备 (Device) 页面的许可证 (License) 部分显示为设备启用的许可证。

如果在管理中心上有可用的许可证，则可以启用设备上的许可证。

过程

步骤 1 选择设备 > 设备管理。

步骤 2 在要启用或禁用许可证的设备旁边，点击 **编辑** (✎)。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 单击设备。

步骤 4 在许可证 (License) 部分中，点击 **编辑** (✎)。

步骤 5 选中或取消选中要为受管设备启用或禁用的许可证旁边的复选框。

步骤 6 单击保存。

下一步做什么

- 部署配置更改；请参阅[部署配置更改](#)。

查看系统信息

设备 (**Device**) 页面的“系统” (**System**) 部分显示只读系统信息表，如下表中所述。

也可以关闭或重新启动设备。

表 4: 系统部分表字段

字段	说明
型号	受管设备的型号名称和编号。
序列 (Serial)	受管设备的机箱的序列号。
时间	设备的当前系统时间。
时区	显示时区。
Version	受管设备上当前安装的软件版本。
时间型规则的时区设置:	设备的当前系统时间，以设备平台设置中指定的时区为准。

查看检测引擎

设备 (**Device**) 页面的“检测引擎” (**Inspection Engine**) 部分会显示您的设备是使用 Snort2 还是 Snort3。要切换检测引擎，请参阅 [《Cisco Secure Firewall Management Center Snort 3 配置指南》](#)。

查看运行状况信息

设备 (**Device**) 页面上的运行状况 (**Health**) 部分显示下表所述信息。

表 5: 运行状况部分表字段

字段	说明
状态 (Status)	一个代表设备当前运行状况的图标。点击该图标将显示设备的“运行状况监控器” (Health Monitor)。
策略	一个指向当前部署在设备上的运行状况策略的只读版本的链接。
已排除	一个指向“运行状况排除” (Health Exclude) 页面的链接，您可以在该页面上启用和禁用运行状况排除模块。

编辑管理设置

您可以在管理 (**Management**) 区域中编辑管理设置。

更新管理中心中的主机名或 IP 地址

如果您在将设备的主机名或 IP 地址添加到管理中心后，对其进行编辑（例如使用设备的 CLI），可能需要使用以下操作步骤手动更新管理管理中心上的主机名或 IP 地址。

更改设备管理 IP 地址的步骤，请参阅在 [CLI 中修改威胁防御管理接口](#)，第 52 页。

如果在注册设备时仅使用了 NAT ID，则该 IP 在此页面上将显示为 **NO-IP**，您无需更新 IP 地址/主机名。

过程

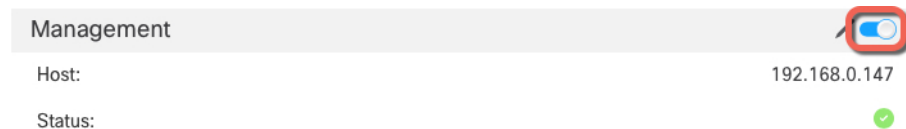
步骤 1 选择 **设备 > 设备管理**。

步骤 2 在要修改管理选项的设备旁边，点击 **编辑** (✎)。

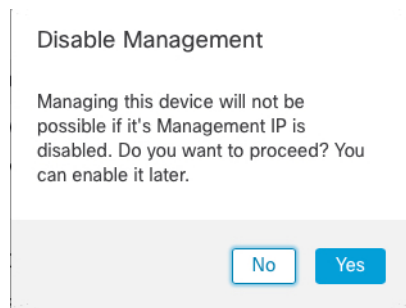
在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 点击 **设备 (Devices)**，并查看 **管理 (Management)** 区域。

步骤 4 点击滑块暂时禁用管理，使其处于禁用状态 (🔴)。

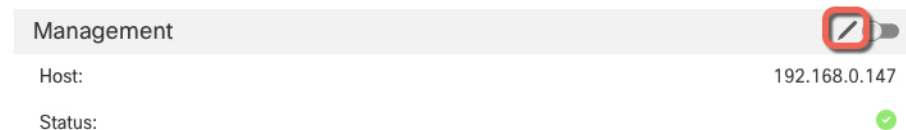


系统将提示您继续禁用管理；点击 **是**。



禁用管理会阻止管理中心和设备之间的连接，但不会从管理中心删除设备。

步骤 5 通过点击 **编辑** (✎) 来编辑主机 IP 地址或主机名。



步骤 6 在 **管理 (Management)** 对话框中，在 **主机 (Host)** 字段中修改名称或 IP 地址，然后点击 **保存 (Save)**。

图 20: 管理 IP 地址


步骤 7 点击滑块重新启用管理，使其处于启用状态（）。

图 21: 启用管理连接

将管理器访问接口从管理更改为数据


你可以从专门的管理界面，或从数据界面管理威胁防御。如果要在添加设备转至管理中心后更改管理器访问接口，请按照以下步骤从管理接口迁移到数据接口。要迁移另一个方向，请参阅[将管理器访问接口从数据更改为管理](#)，第 45 页。

启动从管理到数据的管理器访问迁移会导致管理中心在部署到威胁防御时应用阻止。要删除数据块，请在数据接口上启用管理器访问。

请参阅以下步骤以启用数据接口上的管理器访问，并配置其他所需的设置。

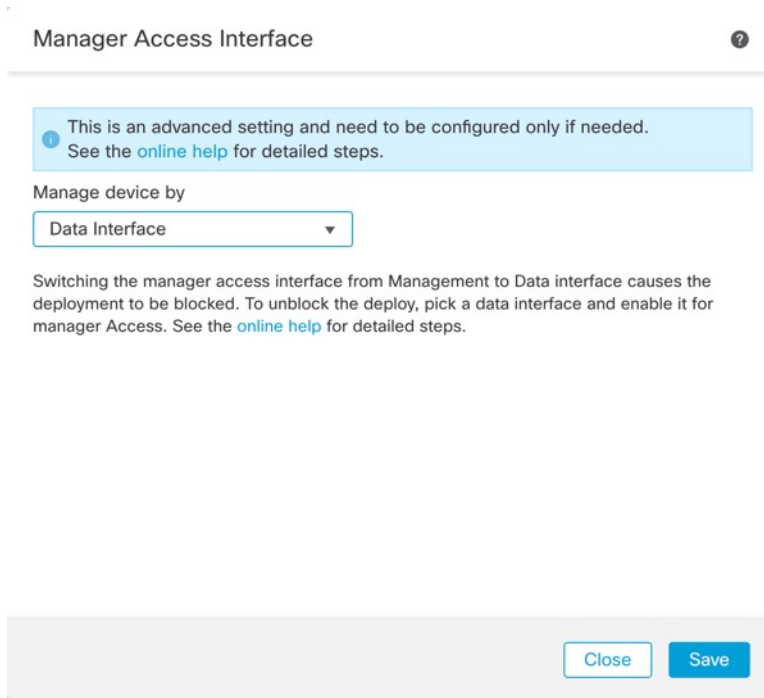
过程

步骤 1 初始化接口迁移。

- 在设备 (Devices) > 设备管理 (Device Management) 页面，然后点击设备的编辑 ()。
- 转到设备 (Device) > 管理 (Management) 部分，然后点击管理器访问接口 (Manager Access Interface) 的链接。

管理器访问接口 (Manager Access Interface) 字段会显示当前管理接口。当您点击链接时，在管理设备依据下拉列表中选择新接口类型 数据接口。

图 22: 管理器访问接口



c) 单击保存。

您现在必须完成此程序中的其余步骤，才能在数据接口上启用管理器访问。管理 (Management) 区域现在会显示管理器访问接口：数据接口 (Manager Access Interface: Data Interface) 以及管理器访问详细信息：配置 (Manager Access Details: Configuration)。

图 23: 管理器访问



如果点击配置 (Configuration)，将打开管理器访问 - 配置详细信息 (Manager Access - Configuration Details) 对话框。管理器访问模式 (Manager Access Mode) 将显示“等待部署” (Deploy pending) 状态。

步骤 2 在设备 (Devices) > 设备管理 (Device Management) > 接口 (Interfaces) > 编辑物理接口 (Edit Physical Interface) > 管理器访问 (Manager Access) 页面上启用数据接口上的管理器访问。

请参阅配置路由模式接口。您可在一个数据接口上启用管理器访问。确保此接口使用名称和 IP 地址进行了充分配置，并且已启用。

步骤 3 (可选) 如果对接口使用DHCP, 请在 **设备 > 设备管理 > DHCP > DDNS** 页面上启用 Web 类型 DDNS 方法。

请参阅 [配置动态 DNS](#)。如果 FTD 的 IP 地址发生变化, DDNS 可确保 管理中心 接通完全限定域名 (FQDN) 内的 威胁防御。

步骤 4 确保 威胁防御 可以通过数据接口路由到 管理中心; 如果需要, 在 **设备 (Devices) > 设备管理 (Device Management) > 路由 (Routing) > 静态路由 (Routing)** 上添加静态路由。

请参阅 [添加静态路由](#)。

步骤 5 (可选) 在平台设置策略中配置 DNS, 并将其应用到位于 **设备 > 平台设置 > DNS** 的此设备。

请参阅 [DNS](#)。如果使用 DDNS, 则需要 DNS。您也可以将 DNS 用于安全策略中的 FQDN。

步骤 6 (可选) 在平台设置策略中为数据接口启用 SSH, 并通过 **设备 > 平台设置 > 安全外壳** 将其应用于此设备。

请参阅 [安全外壳 \(Secure Shell\)](#)。默认情况下, 数据接口上未启用 SSH, 因此, 如果要使用 SSH 管理 威胁防御, 则需要明确允许它。

步骤 7 部署配置更改; 请参阅 [部署配置更改](#)。

管理中心 将通过当前管理接口部署配置更改。部署后, 数据接口现在可供使用, 但与管理的原始管理连接仍处于活动状态。

步骤 8 在 威胁防御 CLI (最好从控制台端口), 将管理接口设置为使用静态 IP 地址, 并将网关设置为使用数据接口。

configure network {ipv4 | ipv6} manual ip_地址网络掩码 data-interfaces

- *ip_address netmask*-虽然您不打算使用管理接口, 但必须设置静态IP地址, 例如专用地址, 以便将网关设置为 **数据接口** (请参阅下一个项目符号)。您无法使用 DHCP, 因为默认路由 (必须是 **数据接口**) 可能会被从 DHCP 服务器收到的路由覆盖。
- **data-interfaces** - 此设置将在背板上转发管理流量, 因此可路由通过管理器访问数据接口。

我们建议您使用控制台端口而不是 SSH 连接, 因为当您更改管理接口网络设置时, 您的 SSH 会话将断开。

步骤 9 如有必要, 请重新连接 威胁防御, 使其能够到达数据接口上的 管理中心。

步骤 10 在管理中心中, 禁用管理连接, 在 **设备 (Devices) > 设备管理 (Device Management) > 设备 (Device) > 管理 (Management)** 部分中更新 威胁防御 的主机 (Host) IP 地址 (IP address), 然后重新启用连接。

请参阅 [更新管理中心中的主机名或 IP 地址, 第 41 页](#)。如果在将 威胁防御 添加到 管理中心 时使用了 威胁防御 主机名或仅使用了 NAT ID, 则不需要更新该值; 但是, 您需要禁用并重新启用管理连接才能重新启动连接。

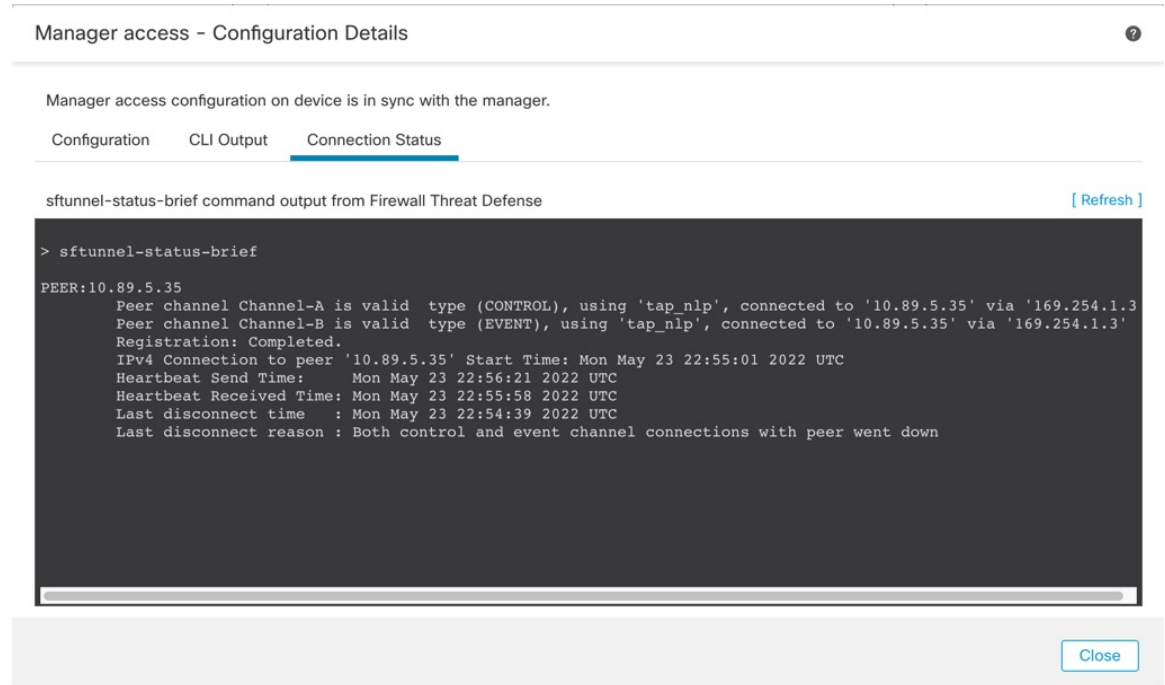
步骤 11 确保管理连接已重新建立。

在管理中心中, 在 **设备 (Devices) > 设备管理 (Device Management) > 设备 (Device) > 管理 (Management) > 管理器访问 - 配置详细信息 (Manager Access - Configuration Details) > 连接状态 (Connection Status)** 页面上检查管理连接状态。

在威胁防御 CLI，输入 `sftunnel-status-brief` 命令以查看管理连接状态。

以下状态显示数据接口成功连接，显示内部“tap_nlp”接口。

图 24: 连接状态



如果重新建立连接需要 10 分钟以上，则应排除连接故障。请参阅[排除数据接口上的管理连接故障](#)，第 61 页。

将管理器访问接口从数据更改为管理

你可以从专门的管理界面，或从数据界面管理威胁防御。如果要在添加设备到管理中心后更改管理器访问接口，请按照以下步骤从数据接口迁移到管理接口。要迁移另一个方向，请参阅[将管理器访问接口从管理更改为数据](#)，第 42 页。

启动从数据到管理的管理器访问迁移会导致管理中心在部署到威胁防御时应用阻止。您必须在数据接口上禁用管理器访问权限才能删除数据块。

请参阅以下步骤以禁用数据接口上的管理器访问，并配置其他所需的设置。

过程

步骤 1 初始化接口迁移。

a) 在 **设备 (Devices) > 设备管理 (Device Management)** 页面，然后点击设备的 **编辑** (✎)。

- b) 转到设备 (**Device**) > 管理 (**Management**) 部分，然后点击管理器访问接口 (**Manager Access Interface**) 的链接。

管理器访问接口 (**Manager Access Interface**) 字段会将当前管理接口显示为数据。点击链接时，在 **管理设备依据** 下拉列表中选择新接口类型，**管理接口**。

图 25: 管理器访问接口

- c) 单击**保存**。

您现在必须完成此程序中的其余步骤，才能在管理接口上启用管理器访问。**管理 (Management)** 区域现在会显示**管理器访问接口：管理接口 (Manager Access Interface: Management Interface)** 以及**管理器访问详细信息：配置 (Manager Access Details: Configuration)**。

图 26: 管理器访问

如果点击**配置 (Configuration)**，将打开**管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** 对话框。**管理器访问模式 (Manager Access Mode)** 将显示“等待部署” (Deploy pending) 状态。

步骤 2 在设备 (Devices) > 设备管理 (Device Management) > 接口 (Interfaces) > 编辑物理接口 (Edit Physical Interface) > 管理器访问 (Manager Access) 页面上禁用数据接口上的管理器访问。

请参阅[配置路由模式接口](#)。此步骤将删除部署时的阻止。

步骤 3 如果尚未执行此操作，请在“平台设置”策略中为数据接口配置 DNS 设置，然后在 设备 > 平台设置 > DNS 上将其应用至设备。

请参阅[DNS](#)。在数据接口上禁用管理器访问的 管理中心 部署将删除任何本地 DNS 配置。如果该 DNS 服务器用于任何安全策略，例如访问规则中的 FQDN，则必须使用 管理中心 重新应用 DNS 配置。

步骤 4 部署配置更改；请参阅[部署配置更改](#)。

将 管理中心 通过当前数据接口部署配置更改。

步骤 5 如有必要，请重新连接 威胁防御，以便它可以到达管理接口上的 管理中心。

步骤 6 在 威胁防御 CLI 中，使用静态 IP 地址或 DHCP 配置管理接口 IP 地址和网关。

当您最初配置用于管理器访问的数据接口时，管理网关设置为 `data-interfaces`，它通过背板转发管理流量，以便可以通过管理器访问数据接口路由。您现在需要为管理网络上的网关设置 IP 地址。

静态 IP 地址：

```
configure network {ipv4 | ipv6} manual ip_address netmask gateway_ip
```

DHCP：

```
configure network {ipv4 | ipv6} dhcp
```

步骤 7 在管理中心中，禁用管理连接，在设备 (Devices) > 设备管理 (Device Management) > 设备 (Device) > 管理 (Management) 部分中更新 威胁防御 的主机 (Host) IP 地址 (IP address)，然后重新启用连接。

请参阅[更新管理中心中的主机名或 IP 地址](#)，第 41 页。如果在将 威胁防御 添加到管理中心时使用了 威胁防御 主机名或仅使用了 NAT ID，则不需要更新该值；但是，您需要禁用并重新启用管理连接才能重新启动连接。

步骤 8 确保管理连接已重新建立。

在管理中心中，检查设备 (Devices) > 设备管理 (Device Management) > 设备 (Device) > 管理 (Management) > 状态 (Status) 字段上的管理连接状态或查看 管理中心 中的通知。

在 威胁防御 CLI，输入 `sftunnel-status-brief` 命令以查看管理连接状态。

如果重新建立连接需要 10 分钟以上，则应排除连接故障。请参阅[排除数据接口上的管理连接故障](#)，第 61 页。

查看数据接口管理的管理器访问详细信息

型号支持-威胁防御

当使用数据接口进行 管理中心 管理而不是使用专用管理接口时，必须注意在 管理中心 中更改设备的接口和网络设置，以免中断连接。您也可以在设备上本地更改数据接口设置，这就要求您在 管理

中心中手动协调这些更改。设备 (Devices) > 设备管理 (Device Management) > 设备 (Device) > 设备管理 (Management) > 管理器访问 + 配置详细信息 (Manager Access - Configuration Details) 对话框可帮助您解决管理中心和威胁防御本地配置之间的任何差异。

通常，在将威胁防御添加到管理中心之前，您可以作为初始威胁防御设置的一部分来配置管理器访问数据接口。当您威胁防御添加到管理中心时，管理中心会发现并维护接口配置，包括以下设置：接口名称和 IP 地址、网关静态路由、DNS 服务器和 DDNS 服务器。对于 DNS 服务器，如果在注册期间发现了它，则在本地维护配置，但不会将其添加到管理中心中的平台设置策略。

将威胁防御添加到管理中心后，如果使用 `configure network management-data-interface` 命令在威胁防御上本地更改数据接口设置，则管理中心会检测到配置更改，并阻止部署到威胁防御。管理中心会使用以下方法之一来检测配置更改：

- 部署到威胁防御。在部署管理中心之前，它将检测配置差异并停止部署。
- 接口 (Interfaces) 页面中的同步 (Sync) 按钮。
- 管理器访问 - 配置详细信息 (Manager Access - Configuration Details) 对话框上的刷新 (Refresh) 按钮

要删除阻止，您必须转到管理器访问 - 配置详细信息 (Manager Access - Configuration Details) 对话框，然后点击确认 (Acknowledge)。下次部署时，管理中心配置将覆盖威胁防御上任何剩余的冲突设置。在您重新部署之前，您有责任在管理中心中手动修复配置。

请参阅此对话框中的以下页面。

配置

查看管理中心和威胁防御上的管理器访问数据接口的配置对比。

以下示例显示了在威胁防御上输入 `configure network management-data-interface` 命令的位置的威胁防御配置详细信息。以粉红色突出显示的内容显示了如果您确认差异但不匹配管理中心中的配置，则威胁防御配置将被删除。以蓝色突出显示的内容显示了将在威胁防御上修改的配置。以绿色突出显示的内容显示了将被添加到威胁防御的配置。

Manager access - Configuration Details

Manager access configuration on device have been updated outside of Manager. Review the differences and update Manager values accordingly.

[Configuration](#) [CLI Output](#) [Connection Status](#)

Last updated: 2022-09-02 at 20:35:58 UTC [\[Refresh \]](#)

	Configuration on Manager	Configuration on Device
4. Ethernet1/1		
Interface Configuration		
FMC Access Enabled	Disabled	Enabled
FMC Access - Allowed Networks		any
Interface Name		outside
IPv4/IPv6 Address		10.89.5.29/26
Static Route Configuration		
IPv4 Gateway		10.89.5.1
IPv6 Gateway		
5. Ethernet1/8		

Legend: Above configurations will be ■ added, ■ modified or ■ disassociated from manager access interface on next deploy to device.

[Close](#) [Acknowledge](#)

以下示例显示在 管理中心中配置接口后的此页面；接口设置匹配，并且已删除粉红色突出显示。

Manager access - Configuration Details

Manager access configuration on device is different from Manager. Review the differences and deploy the changes.

[Configuration](#) [CLI Output](#) [Connection Status](#)

Last updated: 2022-09-09 at 07:10:54 UTC [\[Refresh \]](#)

	Configuration on Manager	Configuration on Device
Web Update Type		
4. GigabitEthernet0/0		
Interface Configuration		
FMC Access Enabled	Enabled	Enabled
FMC Access - Allowed Networks	any	any
Interface Name	outside	outside
IPv4/IPv6 Address	10.89.5.29 255.255.255.192	10.89.5.29 255.255.255.192
Static Route Configuration		
IPv4 Gateway		10.89.5.1
IPv6 Gateway		

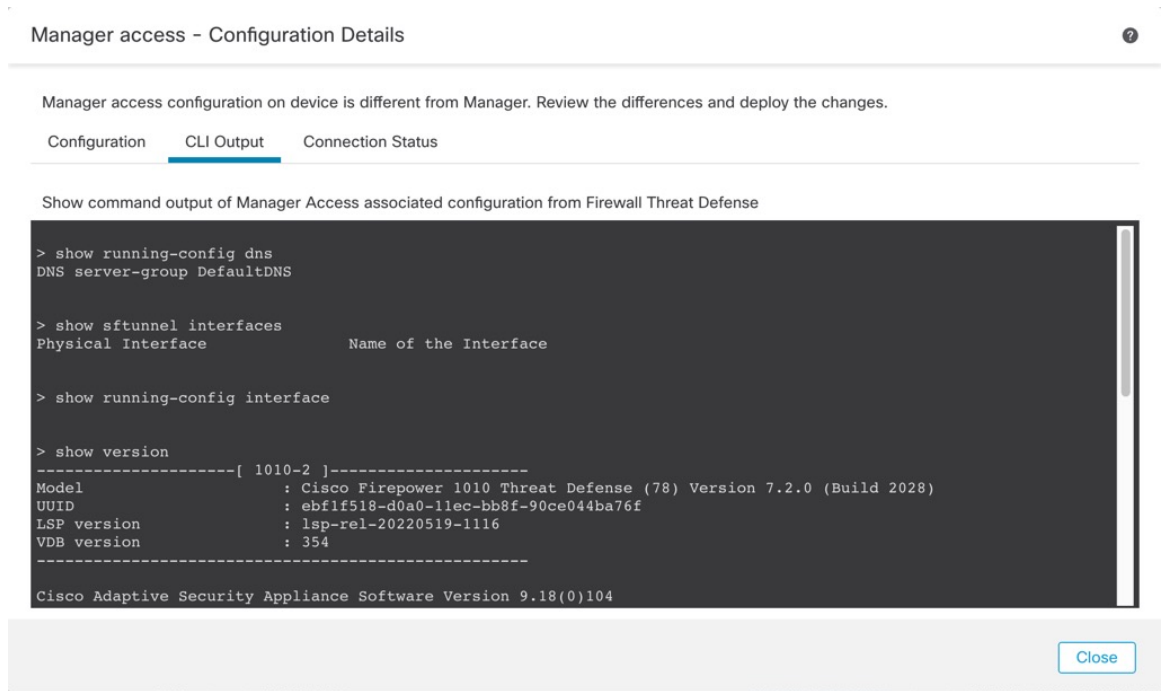
Legend: Above configurations will be ■ added, ■ modified or ■ disassociated from manager access interface on next deploy to device.

[Close](#)

CLI 输出

查看管理器访问数据接口的 CLI 配置，如果您熟悉底层 CLI，这将非常有用。

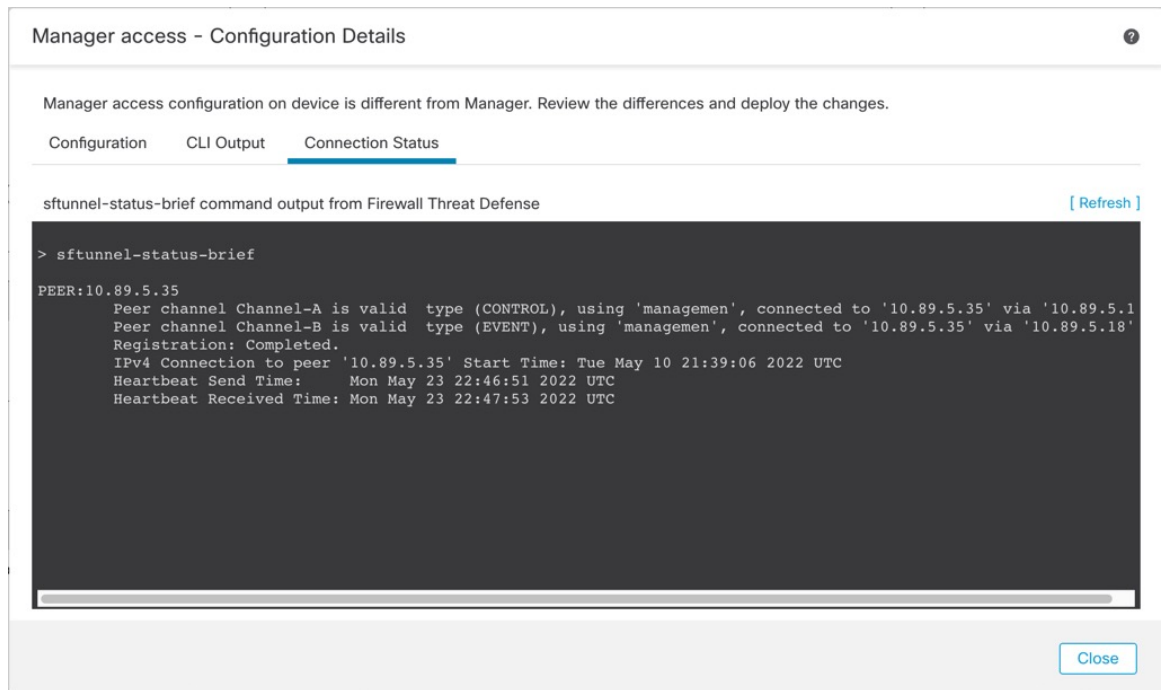
图 27: CLI 输出



连接状态

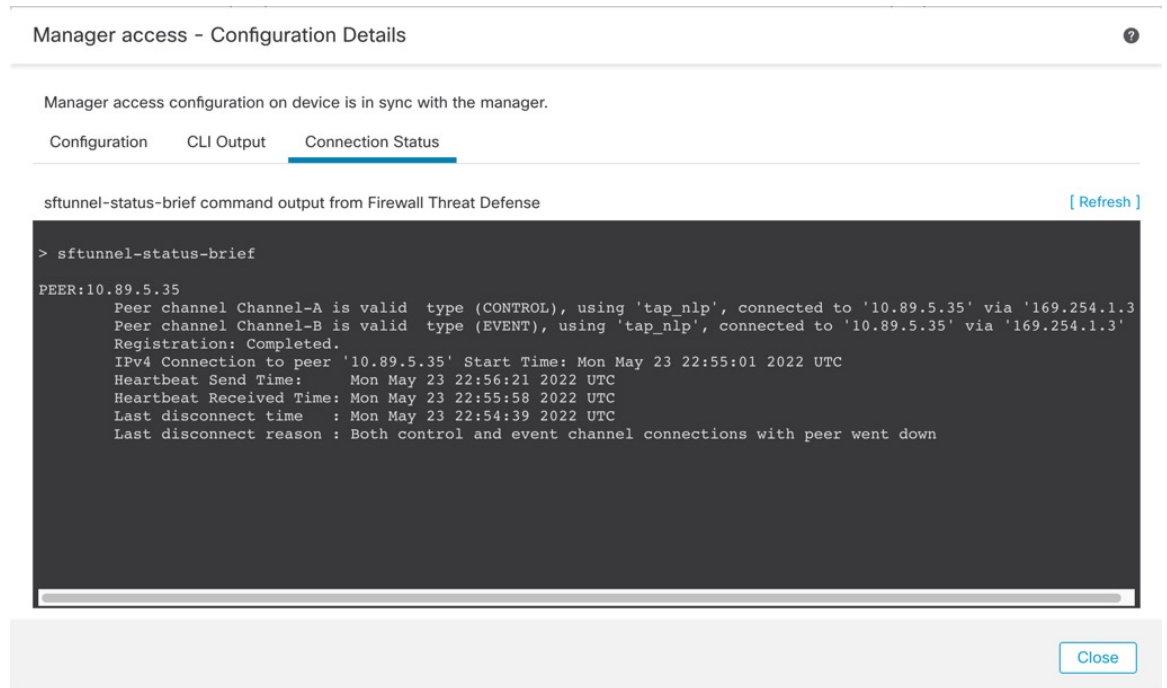
查看管理连接状态。以下示例显示了管理连接仍在管理“management0”接口。

图 28: 连接状态



以下状态显示数据接口成功连接，显示内部“tap_nlp”接口。

图 29: 连接状态



Manager access - Configuration Details

Manager access configuration on device is in sync with the manager.

Configuration CLI Output **Connection Status**

sftunnel-status-brief command output from Firewall Threat Defense [\[Refresh \]](#)

```

> sftunnel-status-brief
PEER:10.89.5.35
Peer channel Channel-A is valid type (CONTROL), using 'tap_nlp', connected to '10.89.5.35' via '169.254.1.3'
Peer channel Channel-B is valid type (EVENT), using 'tap_nlp', connected to '10.89.5.35' via '169.254.1.3'
Registration: Completed.
IPv4 Connection to peer '10.89.5.35' Start Time: Mon May 23 22:55:01 2022 UTC
Heartbeat Send Time: Mon May 23 22:56:21 2022 UTC
Heartbeat Received Time: Mon May 23 22:55:58 2022 UTC
Last disconnect time : Mon May 23 22:54:39 2022 UTC
Last disconnect reason : Both control and event channel connections with peer went down

```

[Close](#)

请参阅以下有关关闭连接的输出示例；没有显示“连接至”信息，也没有显示心跳信息：

```

> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down

```

请参阅以下关于已建立连接的输出示例，其中显示了对等信道和心跳信息：

```

> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202' via
'10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC

```

在 CLI 中修改 威胁防御 管理接口

使用 CLI 修改受管设备上的管理接口设置。这些设置中有许多是您在执行初始设置时设置的；此过程允许您更改这些设置，并设置其他设置，例如，启用事件接口（如果您的型号支持）或添加静态路由。



注释 本主题适用于专用管理接口。您也可以为管理配置数据接口。如果要更改该接口的网络设置，则应在管理中心中而不是在 CLI 中执行此操作。如果您需要对中断的管理连接进行故障排除，并且需要直接在威胁防御上进行更改，请参阅 [修改 CLI 中用于管理的 威胁防御 数据接口](#)，第 58 页。

有关威胁防御 CLI 的信息，请参阅 [Cisco Secure Firewall Threat Defense 命令参考](#)。



注释 使用 SSH 时，在对管理接口进行更改时要小心；如果由于配置错误而无法重新连接，您将需要访问设备控制台端口。



注释 如果更改设备管理 IP 地址，请参阅以下有关管理中心连接的任务，具体取决于您在初始设备设置期间使用 **configure manager add command** 命令识别管理中心的方式（请参阅 [识别新的管理中心](#)，第 76 页）：

- **IP 地址一无操作。**如果您使用可访问的 IP 地址识别管理中心，则几分钟后会自动重新建立管理连接。我们还建议您更改管理中心中显示的设备 IP 地址，以保持信息同步；请参阅 [更新管理中心中的主机名或 IP 地址](#)，第 41 页。此操作有助于更快地重新建立连接。**注意：**如果您指定了无法访问的管理中心 IP 地址，请参阅下面的 NAT ID 程序。
- **仅限 NAT ID-手动重新建立连接。**如果仅使用 NAT ID 识别管理中心，则无法自动重新建立连接。在这种情况下，请根据 [更新管理中心中的主机名或 IP 地址](#)，第 41 页更改管理中心中的设备管理 IP 地址。



注释 在高可用性管理中心配置中，当您从设备 CLI 或管理中心修改管理 IP 地址时，即使在 HA 同步后，辅助管理中心也不会反映更改。要确保辅助管理中心也更新，请在两个管理中心之间切换角色，使辅助管理中心成为主用设备。在当前活动的管理中心的管理页面上修改已注册设备的设备管理 IP 地址。

开始之前

- 您可以使用 **configure user add** 命令创建可登录到 CLI 的用户账户；请参阅 [在 CLI 中添加内部用户](#)。您还可以根据 [外部身份验证](#) 配置 AAA 用户。

过程

- 步骤 1** 通过控制台端口或使用 SSH 连接至设备 CLI。
请参阅[登录 威胁防御 设备上的命令行界面](#)，第 10 页。
- 步骤 2** 使用“管理员”(Admin)用户名和密码登录。
- 步骤 3** (仅 Firepower 4100/9300) 启用第二个管理接口作为仅事件的接口。

configure network management-interface enable management1

configure network management-interface disable-management-channel management1

您始终需要用于管理通信的管理接口。如果您的设备有第二个管理接口，则可以为仅事件流量启用该接口。

您可以选择使用 **configure network management-interface disable-events-channel** 命令禁用主管理接口的事件。不管是哪种情况，设备都会尝试通过事件专属接口发送事件，如果该接口关闭，那么即使您禁用了事件通道，设备也会通过管理接口发送事件。

无法同时禁用接口上的事件通道和管理通道。

要使用单独的事件接口，您还需要在 [管理中心](#) 上启用事件接口。请参阅《[Cisco Secure Firewall Management Center 管理指南](#)》。

示例:

```
> configure network management-interface enable management1
Configuration updated successfully

> configure network management-interface disable-management-channel management1
Configuration updated successfully

>
```

- 步骤 4** 配置管理接口和/或事件接口的 IP 地址:

如果未指定 *management_interface* 参数，则更改默认管理接口的网络设置。配置事件接口时，请确保指定 *management_interface* 参数。事件接口可以与管理接口位于不同的网络中，也可以位于同一网络中。如果连接到您正在配置的接口，您将断开连接。您可以重新连接到新 IP 地址。

- a) 配置 IPv4 地址:

- 手动配置:

configure network ipv4 manual ip_address netmask gateway_ip [management_interface]

请注意，此命令中的 *门户_ip* 用于为设备创建默认路由。如果配置仅事件接口，则必须输入 *门户_ip* 作为命令的一部分；但是，此条目只是将默认路由配置为您指定的值，并且不会为事件接口创建单独的静态路由。如果您在与管理接口不同的网络上使用仅事件接口，我们建议您设置 *门户_ip* 以用于管理接口，然后使用 **configure network static-routes** 命令单独为仅事件接口创建静态路由。

示例:

```
> configure network ipv4 manual 10.10.10.45 255.255.255.0 10.10.10.1 management1
Setting IPv4 network configuration.
Network settings changed.
```

```
>
```

- DHCP（只有默认的管理接口上才支持）：

```
configure network ipv4 dhcp
```

b) 配置 IPv6 地址：

- 无状态自动配置：

```
configure network ipv6 router [management_interface]
```

示例：

```
> configure network ipv6 router management0
Setting IPv6 network configuration.
Network settings changed.
```

```
>
```

- 手动配置：

```
configure network ipv6 manual ip6_address ip6_prefix_length [ip6_gateway_ip]
[management_interface]
```

请注意，此命令中的 *ip6_gateway_ip* 用于为设备创建默认路由。如果配置仅事件接口，则必须输入 *ip6_gateway_ip* 作为命令的一部分；但是，此条目只是将默认路由配置为您指定的值，并且不会为事件接口创建单独的静态路由。如果您在与管理接口不同的网络上使用仅事件接口，我们建议您将 *ip6_gateway_ip* 设置为与管理接口配合使用，然后使用 **configure network static-routes** 命令单独为仅事件接口创建静态路由。

示例：

```
> configure network ipv6 manual 2001:0DB8:BA98::3210 64 management1
Setting IPv6 network configuration.
Network settings changed.
```

```
>
```

- DHCPv6（只有默认的管理接口上才支持）：

```
configure network ipv6 dhcp
```

步骤 5 对于 IPv6，启用或禁用 ICMPv6 回应应答和目的地不可达消息。默认情况下，系统会启用这些消息。

```
configure network ipv6 destination-unreachable {enable | disable}
```

```
configure network ipv6 echo-reply {enable | disable}
```

您可能希望禁用这些数据包以防止潜在的拒绝服务攻击。禁用回应应答数据包意味着无法使用 IPv6 ping 到设备管理接口，以进行测试。

示例：

```
> configure network ipv6 destination-unreachable disable
> configure network ipv6 echo-reply disable
```

步骤 6 在默认管理接口上启用 DHCP 服务器，以便向已连接的主机提供 IP 地址：

configure network ipv4 dhcp-server-enable *start_ip_address end_ip_address*

示例：

```
> configure network ipv4 dhcp-server-enable 10.10.10.200 10.10.10.254
DHCP Server Enabled
>
```

只有手动设置管理接口 IP 地址时，才能配置 DHCP 服务器。management center virtual 上不支持此命令。要显示 DHCP 服务器的状态，请输入 **show network-dhcp-server**：

```
> show network-dhcp-server
DHCP Server Enabled
10.10.10.200-10.10.10.254
```

步骤 7 如果管理中心位于远程网络上，则将为仅事件接口添加静态路由；否则，所有流量都将通过管理接口与默认路由匹配。

configure network static-routes {*ipv4 | ipv6*} **add** *management_interface destination_ip netmask_or_prefix gateway_ip*

对于默认路由，请勿使用此命令；当您使用 **configure network ipv4** 或 **ipv6** 命令时，只能更改默认路由网关 IP 地址（请参阅步骤 [步骤 4](#)，第 53 页）。

示例：

```
> configure network static-routes ipv4 add management1 192.168.6.0 255.255.255.0 10.10.10.1
Configuration updated successfully

> configure network static-routes ipv6 add management1 2001:0DB8:AA89::5110 64
2001:0DB8:BA98::3211
Configuration updated successfully

>
```

要显示静态路由，请输入 **show network-static-routes**（不显示默认路由）：

```
> show network-static-routes
-----[ IPv4 Static Routes ]-----
Interface           : management1
Destination         : 192.168.6.0
Gateway             : 10.10.10.1
Netmask             : 255.255.255.0
```

[...]

步骤 8 设置主机名:

configure network hostname *name*

示例:

```
> configure network hostname farscape1.cisco.com
```

在重新启动之后，系统日志消息不会反映新的主机名。

步骤 9 选择搜索域:

configure network dns searchdomains *domain_list*

示例:

```
> configure network dns searchdomains example.com,cisco.com
```

为设备设置搜索域，用逗号隔开。如果没有在命令中指定完全限定域名，例如 **ping system**，则这些域将添加到主机名中。这些域仅用于管理接口，或通过管理接口的命令。

步骤 10 设置多达 3 个 DNS 服务器，用逗号隔开:

configure network dns servers *dns_ip_list*

示例:

```
> configure network dns servers 10.10.6.5,10.20.89.2,10.80.54.3
```

步骤 11 设置与管理中心通信的远程管理端口:

configure network management-interface tcpport *number*

示例:

```
> configure network management-interface tcpport 8555
```

管理中心和受管设备使用双向、SSL 加密的通信通道（默认情况下在端口 8305 上）进行通信。

注释 思科强烈建议保留远程管理端口的默认设置，但如果管理端口与网络中的其他通信冲突，可以选择其他端口。如果更改管理端口，则必须在部署中需要相互通信的所有设备上做出该更改。

步骤 12 （仅限 威胁防御）设置管理或事件接口 MTU。默认 MTU 为 1500 字节。

configure network mtu [字节] [*interface_id*]

- 字节-设置 MTU（以字节为单位）。对于管理接口，如果启用 IPv4，则值可以介于 64 和 1500 之间；如果启用 IPv6，则值可以介于 1280 和 1500 之间。对于事件接口，如果启用 IPv4，该值

可以介于 64 和 9000 之间；如果启用 IPv6，该值可以介于 1280 和 9000 之间。如果同时启用 IPv4 和 IPv6，则最小值为 1280。如果不输入 字节，系统会提示您输入值。

- **interface_id**-指定要设置 MTU 的接口 ID。使用 **show network** 命令查看可用的接口 ID，例如 management0、management1、br1 和 eth0，具体取决于平台。如果未指定接口，则使用管理接口。

示例:

```
> configure network mtu 8192 management1
MTU set successfully to 1500 from 8192 for management1
Refreshing Network Config...
NetworkSettings::refreshNetworkConfig MTU value at start 8192

Interface management1 speed is set to '10000baseT/Full'
NetworkSettings::refreshNetworkConfig MTU value at end 8192
>
```

- 步骤 13** 配置 HTTP 代理。该设备配置为直接连接到互联网上的端口 TCP/443 (HTTPS) 和 TCP/80 (HTTP)。您可以通过 HTTP 摘要对代理服务器进行身份验证。发出命令后，系统将提示您 HTTP 代理地址和端口，是否需要代理身份验证，如果需要，还会提示代理用户名、代理密码和代理密码确认。

注释 对于威胁防御上的代理密码，只能使用 A-Z、a-z 和 0-9 字符。

configure network http-proxy

示例:

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address: 10.100.10.10
Enter HTTP Proxy Port: 80
Use Proxy Authentication? (y/n) [n]: Y
Enter Proxy Username: proxyuser
Enter Proxy Password: proxypassword
Confirm Proxy Password: proxypassword
```

- 步骤 14** 如果更改设备管理 IP 地址，请参阅以下有关管理中心连接的任务，具体取决于您在初始设备设置期间使用 **configure manager add command** 命令识别管理中心的方式（请参阅 [识别新的管理中心](#)，第 76 页）：

- **IP 地址一无操作。**如果您使用可访问的 IP 地址识别管理中心，则几分钟后会自动重新建立管理连接。我们还建议您更改管理中心中显示的设备 IP 地址，以保持信息同步；请参阅 [更新管理中心中的主机名或 IP 地址](#)，第 41 页。此操作有助于更快地重新建立连接。**注意：**如果指定了无法访问的管理中心 IP 地址，则必须使用 [更新管理中心中的主机名或 IP 地址](#)，第 41 页手动重新建立连接。
- **仅限 NAT ID-手动重新建立连接。**如果仅使用 NAT ID 识别管理中心，则无法自动重新建立连接。在这种情况下，请根据 [更新管理中心中的主机名或 IP 地址](#)，第 41 页更改管理中心中的设备管理 IP 地址。

修改 CLI 中用于管理的 威胁防御 数据接口

如果 威胁防御 和 管理中心 之间的管理连接中断，并且您希望指定新的数据接口来替换旧接口，请使用 威胁防御 CLI 配置新接口。此程序假设您要在同一网络上用新接口替换旧接口。如果管理连接处于活动状态，则应使用管理中心对现有数据接口进行任何更改。有关数据管理接口的初始设置，请参阅 [使用 CLI 完成威胁防御初始配置](#)，第 17 页中的 **configure network management-data-interface** 命令。



注释 本主题适用于为管理配置的数据接口，而不是专用的管理接口。如果要更改管理接口的网络设置，请参阅 [在 CLI 中修改 威胁防御 管理接口](#)，第 52 页。

有关 威胁防御 CLI 的信息，请参阅 [Cisco Secure Firewall Threat Defense 命令参考](#)。

开始之前

- 您可以使用 **configure user add** 命令创建可登录到 CLI 的用户账户；请参阅 [在 CLI 中添加内部用户](#)。您还可以根据 [外部身份验证](#) 配置 AAA 用户。

过程

步骤 1 如果要将数据管理接口更改为新接口，请将当前接口电缆移至新接口。

步骤 2 连接到设备 CLI。

使用这些命令时，应使用控制台端口。如果您正在执行初始设置，则可能会断开与管理接口的连接。如果由于管理连接中断而正在编辑配置，并且您具有专用管理接口的 SSH 访问权限，则可以使用该 SSH 连接。

请参阅 [登录 威胁防御 设备上的命令行界面](#)，第 10 页。

步骤 3 使用“管理员”(Admin)用户名和密码登录。

步骤 4 禁用接口，以便您重新配置其设置。

configure network management-data-interface disable

示例:

```
> configure network management-data-interface disable
```

```
Configuration updated successfully..!!
```

```
Configuration disable was successful, please update the default route to point to a gateway on management interface using the command 'configure network'
```

步骤 5 配置用于管理器访问的新数据接口。

configure network management-data-interface

然后，系统会提示您为数据接口配置基本网络设置。

当您将数据管理接口更改为同一网络上的新接口时，请使用与上一个接口相同的设置（接口 ID 除外）。此外，对于 **是否希望在应用之前清除所有设备配置？ (y/n) [n]:** 选项，选择 **y**。此选项将清除旧的数据管理接口配置，以便您可以成功地在新接口上重新使用 IP 地址和接口名称。

```
> configure network management-data-interface
Data interface to use for management: ethernet1/4
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]: y

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

步骤 6 （可选）限制在特定网络上通过数据接口访问 管理中心。

```
configure network management-data-interface client ip_address netmask
```

默认情况下，允许所有网络。

步骤 7 连接将自动重新建立，但在管理中心中禁用和重新启用连接将有助于更快地重新建立连接。请参阅 [更新管理中心中的主机名或 IP 地址，第 41 页](#)。

步骤 8 检查管理连接是否已重新建立。

```
sftunnel-status-brief
```

请参阅以下关于已建立连接的输出示例，其中显示了对等通道和心跳信息：

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202' via
'10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

步骤 9 在管理中心中，选择设备 (**Devices**) > 设备管理 (**Device Management**) > 设备 (**Device**) > 管理 (**Management**) > 管理器访问 - 配置详细信息 (**Manager Access - Configuration Details**)，然后点击刷新 (**Refresh**)。

管理中心检测接口和默认路由配置更改，并阻止部署到威胁防御。当您在设备上本地更改数据接口设置时，必须在管理中心中手动协调这些更改。您可以在配置 (**Configuration**) 选项卡上查看管理中心和威胁防御之间的差异。

步骤 10 选择 **设备 > 设备管理 > 接口**，然后做作一下更改。

- a) 从旧数据管理接口中删除 IP 地址和名称，并禁用此接口的管理器访问。
- b) 使用旧接口（在 CLI 中使用的接口）的配置配置新的数据管理接口，并为其启用管理器访问。

步骤 11 选择 **设备 > 设备管理 > 路由 > 静态路由**，然后将默认路由从旧数据管理接口更改为新路由。

步骤 12 返回**管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** 对话框，然后点击**确认 (Acknowledge)** 以删除部署块。

下次部署时，管理中心配置将覆盖威胁防御上任何剩余的冲突设置。在您重新部署之前，您有责任在管理中心中手动修复配置。

您将看到“配置已清除” (Config was cleared) 和“管理器访问已更改并确认 (Manager/FMC access changed and acknowledged)”的预期消息。

如果管理中心断开连接，则手动回滚配置

如果将威胁防御上的数据接口用于管理器访问，并从管理中心部署影响网络连接的配置更改，则可以将威胁防御上的配置回滚到上次部署的配置，以便恢复管理连接。然后，您可以调整管理中心中的配置设置，以便保持网络连接并重新部署。即使没有丢失连接，也可以使用回滚功能；它不仅限于此故障排除情况。

或者，如果在部署后失去连接，您可以启用配置的自动回滚；请参阅 [编辑部署设置，第 72 页](#)。

请参阅以下准则：

- 只有以前的部署可以在威胁防御上本地提供；您无法回滚到任何较早的部署。
- 支持回滚以实现高可用性，但不支持集群部署。
- 回滚只会影响您可以在管理中心中设置的配置。例如，回滚不会影响与专用管理接口相关的任何本地配置，您只能在威胁防御 CLI 中进行配置。请注意，如果您在上次管理中心部署后使用 **configure network management-data-interface** 命令更改了数据接口设置，然后使用了回滚命令，则这些设置将不会保留；它们将回滚到上次部署的管理中心设置。
- UCAPL/CC 模式无法回滚。
- 无法回滚上一次部署期间更新的带外 SCEP 证书数据。
- 在回滚期间，连接将被丢弃，因为当前配置将被清除。

过程

步骤 1 在威胁防御 CLI 中，回滚到之前的配置。

configure policy rollback

回滚后，威胁防御会通知管理中心已成功完成回滚。在管理中心中，部署屏幕将显示一条横幅，说明配置已回滚。

注释 如果回滚失败且管理中心管理已恢复，请参阅<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html>以了解常见的部署问题。在某些情况下，恢复管理中心管理访问权限后回滚可能会失败；在这种情况下，您可以解决管理中心配置问题，并从管理中心重新部署。

示例:

对于使用数据接口进行管理器访问的威胁防御：

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2020 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
.....
.....
>
```

步骤 2 检查管理连接是否已重新建立。

在管理中心中，在 **设备 (Devices) > 设备管理 (Device Management) > 设备 (Device) > 管理 (Management) > 管理器访问 - 配置详细信息 (Manager Access - Configuration Details) > 连接状态 (Connection Status)** 页面上检查管理连接状态。

在威胁防御 CLI，输入 **sftunnel-status-brief** 命令以查看管理连接状态。

如果重新建立连接需要 10 分钟以上，则应排除连接故障。请参阅[排除数据接口上的管理连接故障，第 61 页](#)。

排除数据接口上的管理连接故障

当使用数据接口进行管理器访问而不是使用专用管理接口时，必须在管理中心中更改威胁防御的接口和网络设置，以免中断连接。如果在将威胁防御添加到管理中心后更改管理接口类型（从数据到管理，或从管理到数据），如果接口和网络设置未正确配置，则可能会丢失管理连接。

本主题可帮助您排除管理连接丢失的问题。

查看管理连接状态

在管理中心中，在 **设备 (Devices) > 设备管理 (Device Management) > 设备 (Device) > 管理 (Management) > 管理器访问 - 配置详细信息 (Manager Access - Configuration Details) > 连接状态 (Connection Status)** 页面上检查管理连接状态。

在威胁防御 CLI，输入 **sftunnel-status-brief** 命令以查看管理连接状态。您还可以使用 **sftunnel-status** 查看更完整的信息。

请参阅以下有关关闭连接的输出示例；没有显示“连接至”信息，也没有显示心跳信息：

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

请参阅以下关于已建立连接的输出示例，其中显示了对等信道和心跳信息：

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

查看 威胁防御 网络信息

在威胁防御 CLI 上，查看管理和管理器访问数据接口网络设置：

show network

```
> show network
===== [ System Information ] =====
Hostname                : 5516X-4
DNS Servers             : 208.67.220.220,208.67.222.222
Management port        : 8305
IPv4 Default route
  Gateway               : data-interfaces
IPv6 Default route
  Gateway               : data-interfaces

===== [ br1 ] =====
State                   : Enabled
Link                   : Up
Channels               : Management & Events
Mode                   : Non-Autonegotiation
MDI/MDIX               : Auto/MDIX
MTU                    : 1500
MAC Address            : 28:6F:7F:D3:CB:8D
----- [ IPv4 ] -----
Configuration          : Manual
Address                : 10.99.10.4
Netmask                : 255.255.255.0
Gateway                : 10.99.10.1
----- [ IPv6 ] -----
Configuration          : Disabled

===== [ Proxy Information ] =====
State                  : Disabled
Authentication        : Disabled

===== [ System Information - Data Interfaces ] =====
DNS Servers           :
Interfaces            : GigabitEthernet1/1
```

```

===== [ GigabitEthernet1/1 ] =====
State           : Enabled
Link            : Up
Name            : outside
MTU             : 1500
MAC Address     : 28:6F:7F:D3:CB:8F
----- [ IPv4 ] -----
Configuration   : Manual
Address         : 10.89.5.29
Netmask         : 255.255.255.192
Gateway        : 10.89.5.1
----- [ IPv6 ] -----
Configuration   : Disabled

```

检查向 管理中心注册 威胁防御

在 威胁防御 CLI 中，检查 管理中心 注册是否已完成。请注意，此命令不会显示管理连接的 当前 状态。

show managers

```

> show managers
Type           : Manager
Host           : 10.10.1.4
Display name   : 10.10.1.4
Identifier     : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration   : Completed
Management type : Configuration

```

Ping the 管理中心

在 威胁防御 CLI 上，使用以下命令从数据接口对 管理中心 执行 ping 操作：

ping *fmc_ip*

在 威胁防御 CLI 上，使用以下命令从管理接口对 管理中心 执行 ping 操作，该接口应通过背板路由到数据接口：

ping system *fmc_ip*

捕获 威胁防御 内部接口上的数据包

在 威胁防御 CLI 上，捕获内部背板接口 (nlp_int_tap) 上的数据包，以查看是否发送了管理数据包：

capture 名称 interface nlp_int_tap trace detail match ip any any

show capture *name* trace detail

检查内部接口状态，统计信息和数据包计数

在 威胁防御 CLI 上，查看有关内部背板接口 nlp_int_tap 的信息：

show interace detail

```

> show interface detail
[...]
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec

```

```

(Full-duplex), (1000 Mbps)
Input flow control is unsupported, output flow control is unsupported
MAC address 0000.0100.0001, MTU 1500
IP address 169.254.1.1, subnet mask 255.255.255.248
37 packets input, 2822 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 pause input, 0 resume input
0 L2 decode drops
5 packets output, 370 bytes, 0 underruns
0 pause output, 0 resume output
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
input queue (blocks free curr/low): hardware (0/0)
output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
37 packets input, 2304 bytes
5 packets output, 300 bytes
37 packets dropped
   1 minute input rate 0 pkts/sec,  0 bytes/sec
   1 minute output rate 0 pkts/sec,  0 bytes/sec
   1 minute drop rate, 0 pkts/sec
   5 minute input rate 0 pkts/sec,  0 bytes/sec
   5 minute output rate 0 pkts/sec,  0 bytes/sec
   5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
Interface number is 14
Interface config status is active
Interface state is active

```

检查路由和 NAT

在威胁防御 CLI 中，检查是否已添加默认路由 (S*)，以及管理接口 (nlp_int_tap) 是否存在内部 NAT 规则。

show route

```

> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*      0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C       10.89.5.0 255.255.255.192 is directly connected, outside
L       10.89.5.29 255.255.255.255 is directly connected, outside

>

```

show nat

```

> show nat

```



```

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface service
  tcp 8305 8305
  translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface service
  tcp ssh ssh
  translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
  ipv6 service tcp 8305 8305
  translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
  translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
  translate_hits = 0, untranslate_hits = 0
>

```

检查其他设置

请参阅以下命令以检查是否存在所有其他设置。您还可以在 管理中心的 **设备 (Devices) > 设备管理 (Device Management) > 设备 (Device) > 管理 (Management) > 管理器访问 - 配置详细信息 (Manager Access - Configuration Details) > CLI 输出 (CLI Output)** 页面上看到许多这些命令。

show running-config sftunnel

```

> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305

```

show running-config ip-client

```

> show running-config ip-client
ip-client outside

```

show conn address fmc_ip

```

> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
  preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap 10.89.5.29(169.254.1.2):51231 outside 10.89.5.35:8305, idle 0:00:04,
  bytes 86684, flags UxIO
TCP nlp_int_tap 10.89.5.29(169.254.1.2):8305 outside 10.89.5.35:52019, idle 0:00:02,
  bytes 1630834, flags UIO
>

```

检查 DDNS 更新是否成功

在 威胁防御 CLI 中，检查 DDNS 更新是否成功：

debug ddns

```

> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfully updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
DDNS: IDB SB total = 0

```

如果更新失败，请使用 **debug http** 和 **debug ssl** 命令。对于证书验证失败，请检查是否已在设备上安装根证书：

show crypto ca certificates trustpoint_name

要检查 DDNS 操作，请执行以下操作：

show ddns update interface fmc_访问_ifc_name

```
> show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name Update Destination
  RBD_DDNS not available

Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```


检查 管理中心 日志文件


请参阅 <https://cisco.com/go/fmc-reg-error>。

查看清单详细信息

设备 (**Device**) 页面上的库存详细信息 (**Inventory Details**) 部分会显示机箱详细信息，例如 CPU 和内存。

图 30: 设备清单详细信息

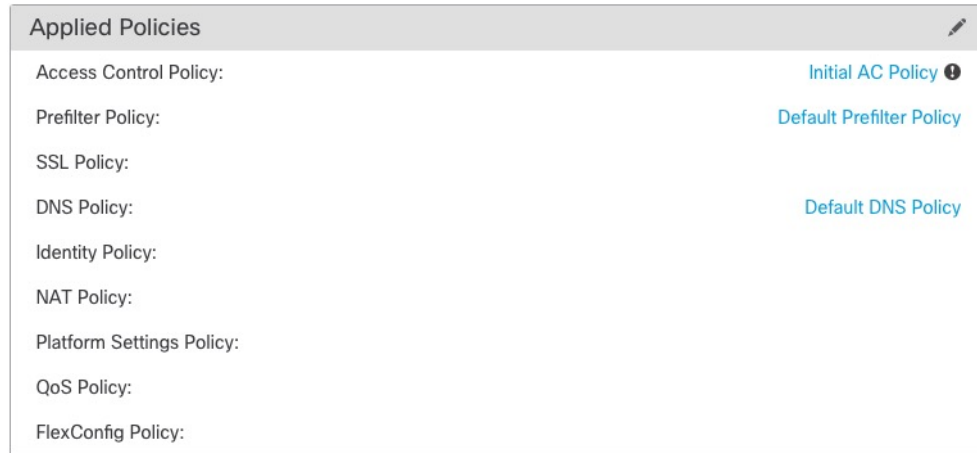
Inventory Details 	
CPU Type:	CPU Xeon E5 series 2300 MHz
CPU Cores:	1 CPU (4 cores)
Memory:	8192 MB RAM
Storage:	N/A
Chassis URL:	N/A
Chassis Serial Number:	N/A
Chassis Module Number:	N/A
Chassis Module Serial Number:	N/A

要更新信息，请点击 **刷新** ()。

编辑应用的策略

设备 (**Device**) 页面的应用的策略 (**Applied Policies**) 部分显示了应用于防火墙的以下策略：

图 31: 应用的策略



对于包含链接的策略，您可以点击链接以查看策略。

对于访问控制策略，请点击感叹号（ⓘ）图标以查看用于故障排除的访问策略信息（**Access Policy Information for Troubleshooting**）对话框。该对话框显示了如何将访问规则扩展为访问控制条目（ACE）。

图 32: 用于故障排除的访问策略信息



您可以从设备管理（**Device Management**）页面将策略分配给单个设备。

过程

步骤 1 选择设备 > 设备管理。

步骤 2 在要为其分配策略的设备旁边，点击 **编辑** (✎)。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 点击 **设备**。

步骤 4 在应用的策略 (**Applied Policies**) 部分中，点击 **编辑** (✎)。

图 33: 策略分配

The screenshot shows a dialog box titled "Policy Assignments" with a help icon. It contains five rows, each with a label and a dropdown menu:

- Access Control Policy: Initial AC Policy
- NAT Policy: None
- Platform Settings Policy: None
- QoS Policy: None
- FlexConfig Policy: None

At the bottom of the dialog, there are two buttons: "Cancel" and "Save".

步骤 5 对于每种策略类型，请从下拉菜单选择一个策略。只有现有的策略会被列出。

步骤 6 单击保存。

下一步做什么

- 部署配置更改；请参阅 [部署配置更改](#)。

编辑高级设置

设备 (Device) 页面的高级设置 (**Advanced Settings**) 部分会显示高级配置设置表，如下所述。您可以编辑任何这些设置。

表 6: “高级” (**Advanced**) 部分表字段

字段	说明
应用绕行 (Application Bypass)	设备上“自动应用绕行” (Automatic Application Bypass) 的状态。
旁路阈值	“自动应用绕行” (Automatic Application Bypass) 阈值（以毫秒为单位）。

字段	说明
对象组搜索	<p>设备上对象组搜索的状态。运行时，FTD 设备会根据访问规则中使用的任何网络或接口对象的内容，将访问控制规则扩展为多个访问控制列表条目。您可以通过启用对象组搜索来减少搜索访问规则所需的内存。启用对象组搜索后，系统不会扩展网络或接口对象，而是根据这些组定义在访问规则中搜索匹配项。对象组搜索不会影响访问规则的定义方式或它们在 Firepower 管理中心中的显示方式，而只会影响将连接与访问控制规则匹配时设备如何对其进行解释和处理。</p> <p>注释 默认情况下，当您首次在管理中心添加威胁防御时，将启用对象组搜索 (Object Group Search)。</p>
接口对象优化	<p>设备上的接口对象优化状态。部署期间，访问控制策略和预过滤器策略中使用的接口组和安全区域生成用于每个源/目的接口对的单独规则。如果启用接口对象优化，则系统将转而每个访问控制/预过滤器规则部署一个规则，这可简化设备配置并提高部署性能。如果选择此选项，则还需选择对象组搜索 (Object Group Search) 选项以降低设备上的内存使用。</p>

以下主题介绍如何编辑高级设备设置。



注释 有关“传输数据包” (Transfer Packets) 设置的信息，请参阅[编辑常规设置](#)，第 32 页。

配置自动应用旁路

自动应用绕行 (AAB) 允许数据包在 Snort 关闭或时绕过检测，或者对于经典设备，如果数据包处理时间过长，则。AAB 会导致 Snort 在故障发生后的十分钟内重新启动，并生成可用于分析 Snort 故障原因的故障排除数据。



注意 部分激活 AAB 会重启 Snort 进程，这会暂时中断对几个数据包的检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅[Snort 重启流量行为](#)。

请参阅以下行为：

FTD 行为：如果 Snort 关闭，则在指定的计时器持续时间后触发 AAB。如果 Snort 已启用，则即使数据包处理超过配置的计时器，也不会触发 AAB。

经典设备行为：AAB 限制通过接口处理数据包所允许的时间。通过网络的数据包延迟容限来平衡数据包处理时延。

该功能适用于任何部署；但在内联部署中最有价值。

通常，在超过延迟阈值后使用入侵策略中的“规则延迟阈值”通过快速路径传送数据包。“规则延迟阈值”不关闭引擎或生成故障排除数据。

如果绕过了检测，则设备会生成运行状况监控警报。

AAB 默认为禁用；要启用 AAB，请按照所述步骤进行操作。

过程

步骤 1 选择设备 > 设备管理。

步骤 2 在要编辑高级设备设置的设备旁边，点击 **编辑** (✎)。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 点击 **设备**，然后点击 **高级设置** 部分的 **编辑** (✎)。

步骤 4 选中 **自动应用旁路**。

步骤 5 输入介于 250 毫秒到 60,000 毫秒之间的 **旁路阈值**。默认设置为 3000 毫秒 (ms)。

步骤 6 点击 **保存 (Save)**。

下一步做什么

- 部署配置更改；请参阅 [部署配置更改](#)。

配置对象组搜索

运行时，威胁防御设备会根据访问规则中使用的任何网络或接口对象的内容，将访问控制规则扩展为多个访问控制列表条目。您可以通过启用对象组搜索来减少搜索访问规则所需的内存。启用对象组搜索后，系统不会扩展网络或接口对象，而是根据这些组定义在访问规则中搜索匹配项。对象组搜索不会影响访问规则的定义方式或它们在管理中心中的显示方式，而只会影响将连接与访问控制规则匹配时设备如何对其进行解释和处理。

启用对象组搜索可以降低包含网络或接口对象的访问控制策略的内存要求。但是，请务必注意，对象组搜索还可能会降低规则查找性能，从而提高 CPU 利用率。您应该在 CPU 影响与降低特定访问控制策略的内存要求之间取得平衡。在大多数情况下，启用对象组搜索可提高网络运营性能。

默认情况下会为在管理中心中首次添加的威胁防御设备启用对象组搜索。对于升级的设备，如果设备配置了禁用的对象组搜索，则需要手动将其启用。一次只能在一台设备上启用；您无法将其全局启用。我们建议您在部署使用网络或接口对象的访问规则的任何设备上将其启用。



注释

如果您启用对象组搜索，然后配置并操作设备一段时间，请注意，随后禁用该功能可能会导致不良结果。如果禁用对象组搜索，现有访问控制规则将按照设备的运行配置进行扩展。如果扩展所需的内存超过设备上的可用内存，设备可能会处于不一致状态，并且可能会影响性能。如果设备运行正常，则在启用对象组搜索后不应将其禁用。

开始之前

- 型号支持-威胁防御
- 我们建议您同时在每台设备上启用事务提交。在设备 CLI 中，输入 **asp rule-engine transactional-commit access-group** 命令。
- 更改此设置可能会在设备重新编译 ACL 时中断系统操作。我们建议您在维护窗口期间更改此设置。

过程

步骤 1 选择设备 > 设备管理。

步骤 2 在要配置规则的 威胁防御设备旁，点击 **编辑** (✎)。

步骤 3 点击设备 (Device) 选项卡，然后点击高级设置 (Advanced Settings) 部分的 **编辑** (✎)。

步骤 4 选中对象组搜索 (Object Group Search)。

步骤 5 要使对象组搜索除网络对象外还适用于接口对象，请选中接口对象优化 (Interface Object Optimization)。

如果不选择接口对象优化 (Interface Object Optimization)，则系统会为每个源/接口对部署单独的规则，而不是使用规则中使用的安全区域和接口组。这意味着接口组不可用于对象组搜索处理。

步骤 6 单击保存。

配置接口对象优化

部署期间，访问控制策略和预过滤器策略中使用的接口组和安全区域生成用于每个源/目的接口对的单独规则。如果启用接口对象优化，则系统将转而部署一个规则，这可简化设备配置并提高部署性能。如果选择此选项，则还需选择**对象组搜索 (Object Group Search)** 选项以降低设备上的内存使用。

默认情况下，接口对象优化处于禁用状态。一次只能在一台设备上启用；您无法将其全局启用。



注释 如果禁用接口对象优化，则现有访问控制规则将在不使用接口对象的情况下进行部署，但这样可能会延长部署时间。此外，如果启用了对象组搜索，则其优势将不会应用于接口对象，并且您可能会在设备的运行配置中看到访问控制规则的扩展。如果扩展所需的内存超过设备上的可用内存，设备可能会处于不一致状态，并且可能会影响性能。

开始之前

型号支持-威胁防御

过程

- 步骤 1 选择设备 > 设备管理。
- 步骤 2 在要配置规则的 FTD 设备旁，点击 **编辑** (✎)。
- 步骤 3 点击设备 (**Device**) 选项卡，然后点击高级设置 (**Advanced Settings**) 部分的 **编辑** (✎)。
- 步骤 4 选中接口对象优化 (**Interface Object Optimization**)。
- 步骤 5 单击保存。

编辑部署设置

设备 (**Device**) 页面上的运行状况 (**Deployment Settings**) 部分显示下表所述信息。

图 34: 部署设置



Deployment Settings 	
Auto Rollback Deployment if Connectivity fails	Disabled
Connectivity Monitor Interval (in Minutes) 	20 Mins.

表 7: 部署设置

字段	说明
连接失败时自动回滚部署	“启用” (Enabled) 或 “禁用” (Disabled)。 您可以在管理连接因部署而失败时启用自动回滚；特别是如果您将数据用于管理中心访问，然后又错误地配置了数据接口。
连接监控间隔（分钟）	显示在回滚配置之前等待的时间。

您可以从**设备管理 (Device Management)** 页面设置部署设置。部署设置包括在管理连接因部署而失败时启用部署自动回滚；特别是如果您将数据用于管理中心访问，然后又错误地配置了数据接口。您也可以使用 **configure policy rollback** 命令手动回滚配置（请参阅[如果管理中心断开连接，则手动回滚配置，第 60 页](#)）。

请参阅以下准则：

- 只有以前的部署可以在 **威胁防御** 上本地提供；您无法回滚到任何较早的部署。
- 支持回滚以实现高可用性，但不支持集群部署。
- 回滚只会影响您可以在管理中心中设置的配置。例如，回滚不会影响与专用管理接口相关的任何本地配置，您只能在 **威胁防御 CLI** 中进行配置。请注意，如果您在上次管理中心部署后使用 **configure network management-data-interface** 命令更改了数据接口设置，然后使用了回滚命令，则这些设置将不会保留；它们将回滚到上次部署的 **管理中心** 设置。
- UCAPL/CC 模式无法回滚。

- 无法回滚上一次部署期间更新的带外 SCEP 证书数据。
- 在回滚期间，连接将被丢弃，因为当前配置将被清除。

过程

步骤 1 选择设备 > 设备管理。

步骤 2 在要为其分配策略的设备旁边，点击 **编辑** (✎)。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 点击 **设备**。

步骤 4 在部署设置 (**Deployment Settings**) 部分中，点击 **编辑** (✎)。

图 35: 部署设置

Deployment Settings

Auto Rollback Deployment if Connectivity Fails:

Connectivity Monitor Interval (in Minutes): 20

The connectivity failure timeout will be applicable from next deployment incase, the deployment for this device is already in progress.

Cancel Save

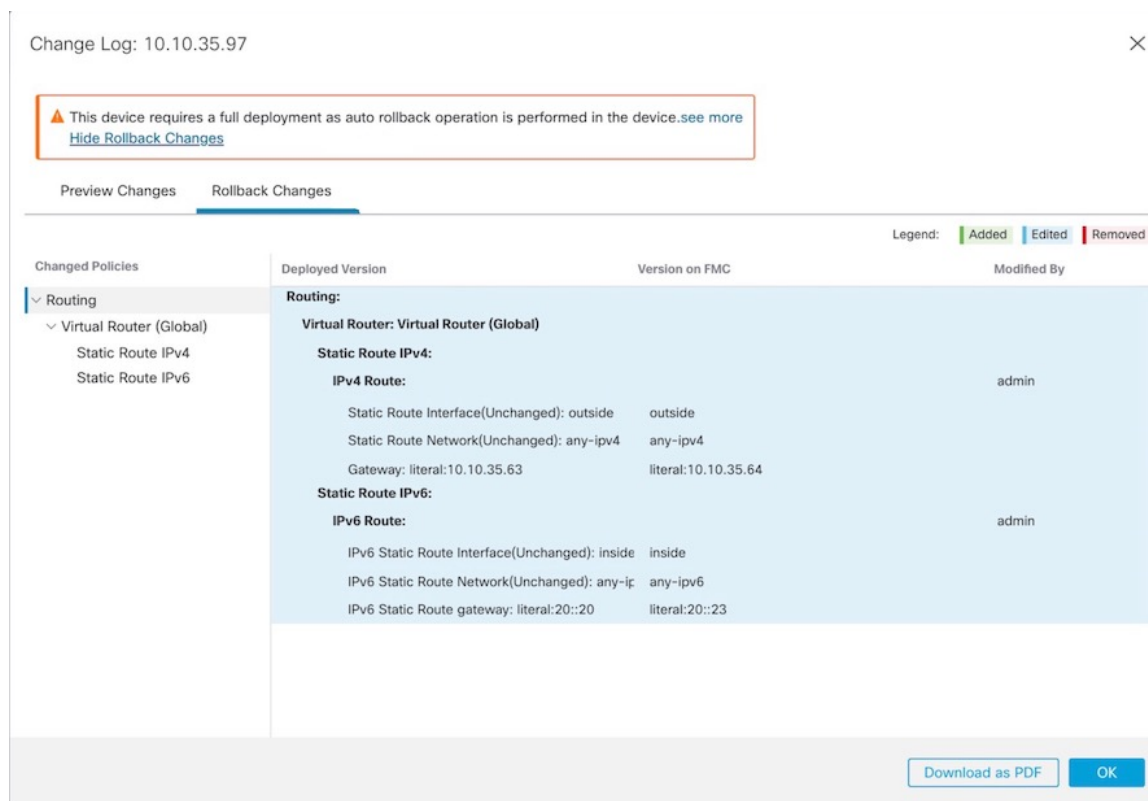
步骤 5 选中连接失败时自动回滚部署 (**Auto Rollback Deployment if Connectivity Fails**) 以启用自动回滚。

步骤 6 设置连接监控间隔 (分钟) (**Connectivity Monitor Interval [in Minutes]**) 以设置在回滚配置之前要等待的时间。默认值为 20 分钟。

步骤 7 如果发生回滚，请参阅以下内容以了解后续步骤。

- 如果自动回滚成功，您会看到一条成功消息，指示您执行完整部署。
- 您还可以转到部署 (**Deployment**) 屏幕，然后点击预览 (**Preview**) (👁️) 图标以查看已回滚的配置部分 (请参阅部署预览)。点击显示回滚更改 (**Show Rollback Changes**) 以查看更改，然后点击隐藏回滚更改 (**Hide Rollback Changes**) 以隐藏更改。

图 36: 回滚更改



- 在部署历史记录预览中，您可以查看回滚更改。请参阅[查看部署历史记录预览](#)。

步骤 8 检查管理连接是否已重新建立。

在管理中心中，在 **设备 > 设备管理 > 设备 > 管理 > FMC 访问详细信息 > 连接状态** 页面上检查管理连接状态。

在威胁防御 CLI，输入 **sftunnel-status-brief** 命令以查看管理连接状态。

如果重新建立连接需要 10 分钟以上，则应排除连接故障。请参阅[排除数据接口上的管理连接故障](#)，第 61 页。

更改设备的管理器

在以下情况时，您可能需要更改设备上的管理器：

- [编辑设备上的管理中心 IP 地址或主机名](#)，第 75 页 - 如果更改 FMC IP 地址或主机名，建议您匹配设备上的新 IP 地址或主机名。

- [识别新的管理中心，第 76 页](#) - 从旧 FMC 中删除设备（如果有）后，您可以为新 FMC 配置设备，然后将其添加到 FMC。
- [从设备管理器切换到管理中心，第 77 页](#) - 不能对同一设备同时使用 FDM 和 FMC。如果您从 FDM 更改为 FMC，则 FTD 配置将被清除，并且您将需要重新开始。
- [从管理中心切换到设备管理器，第 80 页](#) - 不能对同一设备同时使用 FDM 和 FMC。如果您从 FMC 更改为 FDM，则 FTD 配置将被清除，并且您将需要重新开始。

编辑设备上的 管理中心 IP 地址或主机名

如果更改 管理中心 IP 地址或主机名，还应在设备 CLI 中更改值，以便配置匹配。虽然在大多数情况下，无需更改设备上的管理中心 IP 地址或主机名即可重新建立管理连接，但在至少一种情况下，必须执行此任务才能重新建立连接：将设备添加到管理中心并指定仅 NAT ID。即使在其他情况下，我们也建议保持 管理中心 IP 地址或主机名为最新状态，以实现额外的网络恢复能力。

过程

步骤 1 在威胁防御 CLI 中，查看 管理中心 标识符。

show managers

示例:

```
> show managers
Type                : Manager
Host                : 10.10.1.4
Display name       : 10.10.1.4
Identifier          : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration       : Completed
Management type    : Configuration
```

步骤 2 在威胁防御 CLI 中，编辑 管理中心 IP 地址或主机名。

configure manager edit 标识符 {hostname {ip_address | hostname} | **displayname** display_name}

如果 管理中心 最初由 **DONTRESOLVE** 和 NAT ID 标识，则可以使用此命令将该值更改为主机名或 IP 地址。不能将 IP 地址或主机名更改为 **DONTRESOLVE**。

管理连接将关闭，然后重新建立。您可以使用 **sftunnel-status** 命令监控连接状态。

示例:

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 hostname 10.10.5.1
```

识别新的 管理中心

此程序介绍如何为受管设备识别新的 管理中心。即使新的 管理中心 使用旧的 管理中心的 IP 地址，也应执行这些步骤。

过程

步骤 1 在旧 管理中心 上，如果存在，请删除受管设备。请参阅[从 管理中心 删除（取消注册）设备](#)，第 30 页。

如果您有与 管理中心的活动连接，则无法更改 管理中心 IP 地址。

步骤 2 连接到设备 CLI，例如使用 SSH。

步骤 3 配置新的 管理中心。

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE } regkey [nat_id] [display_name]
```

- {hostname | IPv4_address | IPv6_address}-设置主机名，IPv4地址或IPv6地址。管理中心
- **DONTRESOLVE**-如果 管理中心 不可直接寻址，请使用 **DONTRESOLVE** 而不是主机名或 IP 地址。如果使用 **DONTRESOLVE**，则需要使用 *nat_id*。当您将此设备添加到 管理中心时，请确保同时指定设备 IP 地址和 *nat_id*；连接的一端需要指定 IP 地址，两端需要指定相同的唯一 NAT ID。
- *regkey*-输入注册期间要在 管理中心 和设备之间共享的注册密钥。可以为此密钥选择介于 1 至 37 个字符之间的任何文本字符串；添加威胁防御时，需要在管理中心上输入相同的密钥。
- *nat_id*-当一方未指定 IP 地址时，在 管理中心 与设备之间的注册流程中使用的字母数字字符串，介于 1 至 37 个字符。此 NAT ID 是仅在注册期间使用的一次性密码。确保 NAT ID 是唯一的，不会被等待注册的任何其他设备使用。添加 威胁防御 时，在 管理中心 上指定相同的 NAT ID。
- *display_name* - 使用 **show managers** 命令提供用于显示此管理器的显示名称。如果您将 CDO 标识为仅用于分析的主用管理器和本地部署管理中心，则此选项非常有用。如果不指定此参数，防火墙将使用以下方法之一自动生成显示名称：

- *hostname* | *IP_address*（如果不使用 **DONTRESOLVE** 关键字）
- **manager-timestamp**

示例:

```
> configure manager add DONTRESOLVE abc123 efg456
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
>
```

步骤 4 将此设备添加到管理中心。请参阅[将设备添加到管理中心](#)，第 26 页。

从设备管理器切换到管理中心

当您从设备管理器切换到管理中心时，除管理接口和管理器访问设置外，所有接口配置会被保留。请注意，不会保留其他配置设置，例如访问控制策略或安全区。

切换到管理中心后，您将无法再使用设备管理器管理威胁防御设备。

开始之前

如果防火墙已配置为高可用性，您必须首先使用设备管理器（如果可能）或 **configure high-availability disable** 命令中断高可用性配置。理想情况下，应从主用设备中断高可用性。

过程

步骤 1 在设备管理器中，从 Cisco 智能软件管理器中取消注册设备。

步骤 2 （可能需要）配置管理接口。

您可能需要更改管理接口配置，即使您打算使用数据接口访问管理器。如果您使用设备管理器连接的管理接口，则必须重新连接到设备管理器。

- 用于管理器访问的数据接口 - 管理接口必须将网关设置为数据接口。默认情况下，管理接口从 DHCP 接收 IP 地址和网关。如果您没有从 DHCP 接收到网关（例如，您没有将此接口连接到网络），则网关将默认为数据接口，并且您无需进行任何配置。如果您从 DHCP 接收到了网关，则需要使用静态 IP 地址配置此接口，并将该网关设置为数据接口。
- 用于管理器访问的管理接口 - 如果您要配置静态 IP 地址，请确保另将默认网关设置为唯一网关，而不是数据接口。如果您使用 DHCP，则无需进行任何配置，前提是您已成功从 DHCP 获取网关。

步骤 3 选择 **设备 > 系统设置 > 集中管理**，然后点击 **继续** 设置管理中心管理。

步骤 4 配置 **管理中心/CDO** 详细信息。

图 37: 管理中心/CDO 详细信息

Configure Connection to Management Center or CDO


Provide details to register to the management center/CDO.

Management Center/CDO Details

Do you know the Management Center/CDO hostname or IP address?

Yes No


Threat Defense



10.89.5.16
fe80::6a87:c6ff:fea6:4c00/64

→

Management Center/CDO



10.89.5.35

Management Center/CDO Hostname or IP Address

10.89.5.35

Management Center/CDO Registration Key

●●●● 👁

NAT ID

Required when the management center/CDO hostname or IP address is not provided. We recommend always setting the NAT ID even when you specify the management center/CDO hostname or IP address.

11203

Connectivity Configuration

Threat Defense Hostname

1120-3

DNS Server Group

CustomDNSServerGroup ▼

Management Center/CDO Access Interface

Data Interface

Please select an interface ▼

Management Interface [View details](#)

CANCEL
CONNECT

- a) 对于 **是否知道管理中心/CDO 主机名或 IP 地址**，如果您可以使用 IP 地址或主机名访问管理中心，请点击 **是**，如果管理中心位于 NAT 之后或没有公共 IP 地址或主机名，请点击 **否**。

必须至少有一个设备（管理中心或威胁防御设备）具有可访问的 IP 地址，才能在两个设备之间建立双向 SSL 加密的通信通道。

- b) 如果您选择是，则输入 **管理中心/CDO 主机名/IP 地址**。
- c) 指定 **管理中心/CDO 注册密钥**。

此密钥是您选择的一次性注册密钥，注册威胁防御设备时也要在管理中心上指定它。注册密钥不得超过 37 个字符。有效字符包括字母数字（A - Z、a - z、0 - 9）和连字符 (-)。此 ID 可用于将多台设备注册到管理中心。

- d) 指定 **NAT ID**。

此 ID 是您选择的唯一一次性字符串，您还需要在管理中心上指定它。如果仅在其中一台设备上指定 IP 地址，则此字段必填；但建议您即使在知道两台设备的 IP 地址时，仍指定 NAT ID。NAT ID 不得超过 37 个字符。有效字符包括字母数字（A - Z、a - z、0 - 9）和连字符 (-)。此 ID 不能用于将任何其他设备注册到管理中心。NAT ID 与 IP 地址结合使用，用于验证连接是否来自正确的设备；只有在对 IP 地址/NAT ID 进行身份验证后，才会检查注册密钥。

步骤 5 配置连接配置。

- a) 指定 **FTD 主机名**。

如果您使用数据接口进行 **管理中心/CDO 访问接口** 访问，则此 FQDN 将用于此接口。

- b) 指定 **DNS 服务器组**。

选择现有组或创建一个新组。默认 DNS 组名为 **CiscoUmbrellaDNSServerGroup**，其中包括 OpenDNS 服务器。

如果要为 **管理中心/CDO 访问接口** 选择数据接口，则此设置会设置数据接口 DNS 服务器。您使用安装向导设置的管理 DNS 服务器用于管理流量。数据 DNS 服务器用于 DDNS（如果已配置）或适用于此接口的安全策略。您可能会选择用于管理的相同 DNS 服务器组，因为管理和数据流量都通过外部接口到达 DNS 服务器。

在管理中心上，数据接口 DNS 服务器在您分配给此威胁防御的平台设置策略中配置。当您威胁防御设备添加到管理中心时，本地设置将保留，并且 DNS 服务器不会添加到平台设置策略。但是，如果稍后将平台设置策略分配给包含 DNS 配置的威胁防御设备，则该配置将覆盖本地设置。我们建议您主动配置与此设置匹配的 DNS 平台设置，以使管理中心和威胁防御设备同步。

此外，仅当在初始注册时发现 DNS 服务器，管理中心才会保留本地 DNS 服务器。

如果要为 **FMC 访问接口** 选择管理接口，则此设置会配置管理 DNS 服务器。

- c) 对于 **管理中心/CDO 访问接口**，请选择任何已配置的接口。

将威胁防御设备注册到管理中心后，您可以将该管理器接口更改为管理接口或另一数据接口。

步骤 6（可选）如果您选择了数据接口，并且该接口不是外部接口，那么请添加默认路由。

您将看到一条消息，要求您检查是否有通过接口的默认路由。如果您选择了外部接口，那么您已经在安装向导中配置了此路由。如果您选择了其他接口，那么需要在连接到管理中心之前手动配置默认路由。

如果您选择了管理接口，那么需要先将网关配置为唯一网关，然后才能在此屏幕上继续操作。

步骤 7（可选）如果您选择了数据接口，请点击**添加动态 DNS (DDNS) 方法**。

如果 IP 地址发生变化，DDNS 确保 管理中心 可接通完全限定域名 (FQDN) 的 威胁防御 设备。参阅 **设备 > 系统设置 > DDNS 服务配置动态 DNS**。

如果您在将威胁防御设备添加到管理中心之前配置 DDNS，则威胁防御设备会自动为 Cisco 受信任根 CA 捆绑包中的所有主要 CA 添加证书，以便威胁防御设备可以验证用于 HTTPS 连接的 DDNS 服务器证书。威胁防御支持任何使用 DynDNS 远程 API 规范的 DDNS 服务器 (<https://help.dyn.com/remote-access-api/>)。

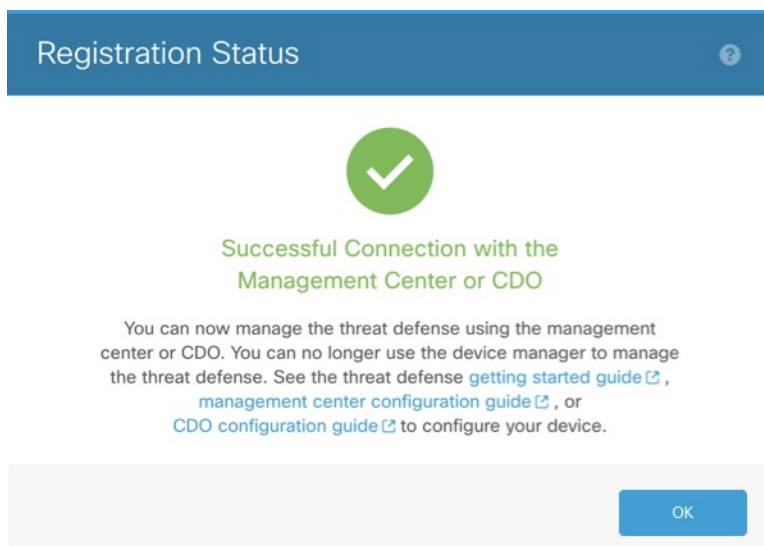
使用管理接口访问管理器时，不支持 DDNS。

步骤 8 点击**连接 (Connect)**。注册状态 对话框显示切换到管理中心的当前状态。在 **保存管理中心/CDO 注册设置** 步骤后，转到管理中心，并添加防火墙。

如果要取消切换到管理中心，请点击 **取消注册**。否则，请在 **保存管理中心/CDO 注册设置** 步骤之后关闭 设备管理器 浏览器窗口。如果这样做，该过程将暂停，并且只有在您重新连接到设备管理器时才会恢复。

如果您在 **保存管理中心/CDO 注册设置** 步骤后保持连接到设备管理器，您最终将看到与**管理中心的成功连接或 CDO** 对话框。您将断开与设备管理器的连接。

图 38: 成功连接



从管理中心 切换到 设备管理器

您可以将当前由本地部署或云交付的管理中心管理的威胁防御设备配置为使用设备管理器设备。

您可以从管理中心切换到设备管理器，而无需重新安装软件。在从管理中心切换到设备管理器之前，请确认设备管理器满足您的所有配置要求。如果要从设备管理器切换到管理中心，请参阅 [从设备管理器切换到管理中心](#)，第 77 页。



注意 切换到设备管理器会清除设备配置，并会使系统恢复默认配置。但是，管理 IP 地址和主机名保留不变。

过程

步骤 1 在管理中心中，从设备 (**Devices**) > 设备管理 (**Device Management**) 页面删除防火墙。

步骤 2 使用 SSH 或控制台端口连接到威胁防御 CLI。如果使用 SSH，请打开与 **管理 IP 地址** 的连接，并使用 **admin** 用户名（或具有管理员权限的任何其他用户）登录威胁防御 CLI。

控制台端口默认为 FXOS CLI。使用 **connect ftd** 命令连接到威胁防御 CLI。SSH 会话直接连接到威胁防御 CLI。

如果无法连接到管理 IP 地址，请解决以下问题：

- 确保管理物理端口连接到正常运行的网络。
- 确保为管理网络配置了管理 IP 地址和网关。使用 **configure network ipv4/ipv6 manual** 命令。

步骤 3 验证您当前处于远程管理模式之下。

show managers

示例：

```
> show managers
Type                : Manager
Host                : 10.89.5.35
Display name       : 10.89.5.35
Identifier          : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration       : Completed
```

步骤 4 删除远程管理器，进入无管理器模式。

configure manager delete uuid

无法直接从远程管理转至本地管理。如果定义了多个管理器，则需要指定标识符（也称为 UUID；请参阅 **show managers** 命令）。单独删除每个管理器条目。

示例：

```
> configure manager delete
Deleting task list
Manager successfully deleted.

>
> show managers
```

```
No managers configured.
```

步骤 5 配置本地管理器。

configure manager local

现在，您可以使用 Web 浏览器在 <https://management-IP-address> 位置打开本地管理器。

示例：

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

Cisco Secure Firewall 3100上的热插拔 SSD

如果您有两个 SSD，它们会在您启动时形成 RAID。防火墙启动时，您可以在 CLI 上执行以下任务：威胁防御

- 热插拔其中一个 SSD - 如果 SSD 出现故障，您可以更换它。请注意，如果您只有一个 SSD，则无法在防火墙开启时将其删除。
- 删除一个 SSD - 如果您有两个 SSD，可以删除一个。
- 添加第二个 SSD - 如果您有一个 SSD，可以添加第二个 SSD 并形成 RAID。



注意 请勿在未使用此程序从 RAID 中移除 SSD 的情况下将其移除。可能会导致数据丢失。

过程

步骤 1 删除其中一个 SSD。

a) 从 RAID 中删除 SSD。

```
configure raid remove-secure local-disk {1 | 2}
```

remove-secure 关键字将从 RAID 中删除 SSD，禁用自加密磁盘功能，并对 SSD 执行安全擦除。如果您只想从 RAID 中删除 SSD 并保持数据不变，可以使用 **remove** 关键字。

示例：

```
> configure raid remove-secure local-disk 2
```

b) 监控 RAID 状态，直到 SSD 不再显示在清单中。

show raid

从 RAID 中删除 SSD 后，可操作性和驱动器状态将显示为降级。第二个驱动器将不再列为成员磁盘。

示例：

```
> show raid
Virtual Drive
ID: 1
Size (MB): 858306
Operability: operable
Presence: equipped
Lifecycle: available
Drive State: optimal
Type: raid
Level: raid1
Max Disks: 2
Meta Version: 1.0
Array State: active
Sync Action: idle
Sync Completed: unknown
Degraded: 0
Sync Speed: none

RAID member Disk:
Device Name: nvme0n1
Disk State: in-sync
Disk Slot: 1
Read Errors: 0
Recovery Start: none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name: nvme1n1
Disk State: in-sync
Disk Slot: 2
Read Errors: 0
Recovery Start: none
Bad Blocks:
Unacknowledged Bad Blocks:

> show raid
Virtual Drive
ID: 1
Size (MB): 858306
Operability: degraded
Presence: equipped
Lifecycle: available
Drive State: degraded
Type: raid
Level: raid1
Max Disks: 2
Meta Version: 1.0
Array State: active
Sync Action: idle
Sync Completed: unknown
Degraded: 1
Sync Speed: none

RAID member Disk:
Device Name: nvme0n1
Disk State: in-sync
```

```
Disk Slot:          1
Read Errors:       0
Recovery Start:    none
Bad Blocks:
Unacknowledged Bad Blocks:
```

- c) 从机箱中取出 SSD。

步骤 2 添加 SSD。

- a) 将 SSD 物理添加到空插槽。
- b) 将 SSD 添加到 RAID。

configure raid add local-disk {1 | 2}

将新 SSD 同步到 RAID 可能需要几个小时，在此期间防火墙完全正常运行。您甚至可以重新启动，同步将在启动后继续。使用 **show raid** 命令显示状态。

如果您安装的 SSD 以前在另一个系统上使用过，并且仍处于锁定状态，请输入以下命令：

configure raid add local-disk {1 | 2} psid

*Psid*印在 SSD 背面的标签上。或者，您可以重新启动系统，SSD 将被重新格式化并添加到 RAID。

设备管理的历史记录基础知识

功能	版本	详细信息
策略支持回滚以实现高可用性	7.2	configure policy rollback 命令支持高可用性。
多管理器支持	7.2	<p>我们引入了云交付的管理中心。云交付的管理中心使用思科防御协调器 (CDO) 平台，并会跨多个思科安全解决方案统一管理。我们负责管理器的更新。</p> <p>运行版本 7.2+ 的硬件或虚拟管理中心可以“共同管理”云托管设备，但仅限于事件日志记录和分析目的。您无法从硬件或虚拟管理中心将策略部署到这些设备。</p> <p>新增/修改的威胁防御命令：configure manager add、configure manager delete、configure manager edit 和 show managers</p> <p>新增/修改的屏幕：</p> <ul style="list-style-type: none"> • 将云托管设备添加到硬件或虚拟管理中心时，请使用新的 CDO 托管设备 (CDO Managed Device) 复选框将其指定为仅用于分析。 • 在设备 (Devices) > 设备管理 (Device Management) 中查看哪些设备仅用于分析。 <p>有关详细信息，请参阅 CDO 文档。</p>

功能	版本	详细信息
默认情况下会为访问控制规则启用对象组搜索。	7.2	从版本 7.2.0 开始，托管设备默认启用 对象组搜索 (Object Group Search) 设置。在 设备管理 (Device Management) 页面上编辑设备设置时，此选项位于 高级设置 (Advanced Settings) 部分中。
导致管理连接丢失的部署的自动回滚。	7.2	如果部署导致管理中心和威胁防御之间的管理连接断开，您现在就可以启用配置的自动回滚。之前，您只能使用 configure policy rollback 命令来手动回滚配置。 新增/修改的菜单项： <ul style="list-style-type: none"> • 设备 (Devices) > 设备管理 (Device Management) > 设备 (Device) > 部署设置 (Deployment Settings) • 部署 (Deploy) > 高级部署 (Advanced Deploy) > 预览 (Preview) • 部署 (Deploy) > 部署历史 (Deployment History) > 预览 (Preview)
Cisco Secure Firewall 3100 上的 SSD 支持 RAID。	7.1	SSD 是自加密驱动器 (SED)，如果您有 2 个 SSD，则它们会组成软件 RAID。 新增/经修改的命令： configure raid, show raid, show ssd
导入和导出设备配置	7.1	您可以导出设备特定的配置，然后可以在以下使用案例中为同一设备导入已保存的配置： <ul style="list-style-type: none"> • 将设备移至其他 FMC。 • 恢复老旧配置。 • 重新注册设备。 新增/修改的屏幕： 设备 (Devices) > 设备管理 (Device Management) > 设备 (Device) > 常规 (General)
使用 设备管理器 来配置威胁防御，以便由管理中心管理。	7.1.	当您使用 设备管理器 执行初始设置时，如果您切换到 管理中心 进行管理，除管理和管理器访问设置外，在 设备管理器 中完成的所有接口配置都将保留。请注意，不会保留其他默认配置设置，例如访问控制策略或安全区。使用 管理中心 CLI 时，仅保留管理和管理器访问设置（例如，不保留默认的内部接口配置）。 切换到 管理中心 后，您将无法再使用 设备管理器 来管理 管理中心。 新增/修改 设备管理器 屏幕： 系统设置 (System Settings) > 管理中心 (Management Center)
按升级状态过滤设备。	6.7	设备管理 (Device Management) 页面现在提供有关托管设备的升级信息，包括设备是否正在升级（及其升级路径），以及上次升级是成功还是失败。 新增/修改的屏幕： 设备 (Devices) > 设备管理 (Device Management)

功能	版本	详细信息
更新 威胁防御 上的 管理中心 IP 地址	6.7	<p>如果更改 管理中心 IP 地址，现在可以使用 威胁防御 CLI 更新设备。</p> <p>新增/修改的 威胁防御 CLI 命令：configure manager edit</p>
在数据接口上管理 威胁防御	6.7	<p>现在可以在数据接口上配置 威胁防御 的 管理中心 管理，而不是使用专用的管理接口。</p> <p>当您想要从总部的 管理中心 管理分支机构的 FTD 并需要在外部接口上管理 威胁防御 时，此功能对于远程部署非常有用。如果 威胁防御 通过 DHCP 方式接收到公共 IP 地址，则可以选择通过 web 更新方式为接口配置动态 DNS (DDNS)。如果 威胁防御 的 IP 地址发生变化，DDNS 可确保 管理中心 接通完全限定域名 (FQDN) 内的 威胁防御。</p> <p>注释 在集群或高可用性中，不支持从数据接口进行 管理中心 访问。</p> <p>新增/修改的屏幕：</p> <ul style="list-style-type: none"> • 设备 (Devices) > 设备管理 (Device Management) > 设备 (Device) > 管理 (Management) • 设备 > 设备管理 > 接口 > FMC 访问 • 设备 > 设备管理 > DHCP > DDNS > DDNS 更新方法 页面 <p>新增/修改的 威胁防御 CLI 命令：configure network management-data-interface、configure policy rollback</p> <p>支持的平台： 威胁防御</p>
一键访问 机箱管理器。	6.4	<p>对于 Firepower 4100/9300 系列设备，“设备管理” (Device Management) 页面会提供指向 机箱管理器 Web 界面的链接。</p> <p>新增/修改的屏幕： 设备 (Devices) > 设备管理 (Device Management)</p>
按运行状况和部署状态过滤设备；查看版本信息。	6.2.3	<p>“设备管理” (Device Management) 页面现在提供受管设备的版本信息，并且能够按运行状况和部署状态过滤设备。</p> <p>新增/修改的屏幕： 设备 (Devices) > 设备管理 (Device Management)</p>

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。