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 Cisco Defense Orchestrator (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 Defense Orchestrator 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

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管理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。

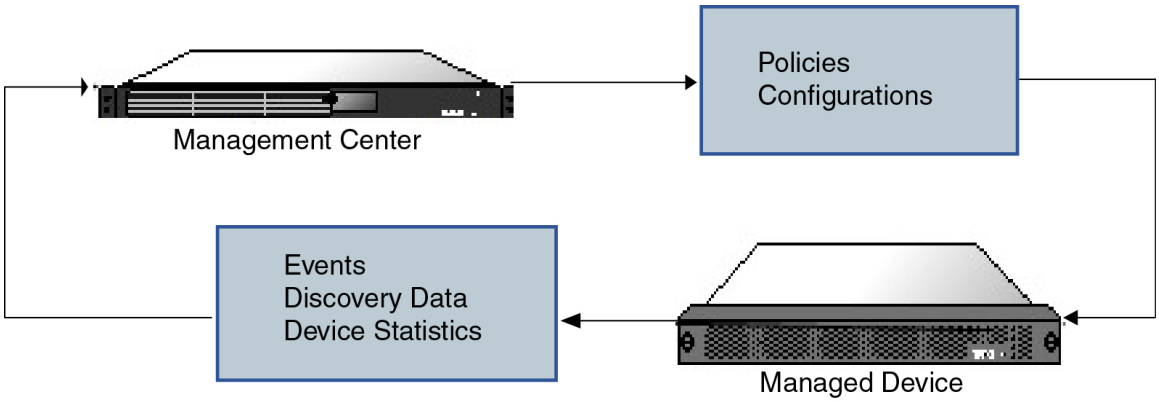
注释 尽管 管理中心 可以按照 http://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html 处可用的兼容性矩阵中指定的那样管理运行之前的某些版本的设备，但需要最新版本 威胁防御 软件的新功能不适用于这些以前发布的设备。某些 管理中心 功能可能适用于早期版本。

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 TLS-1.3-加密的安全隧道在 管理中心和该设备之间传输。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。

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。

确保管理连接稳定，没有过多的丢包，吞吐量至少为 5 Mbps。

注释 管理连接是信道自身与设备之间的 TLS-1.3 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。此外，使用数据接口可以配置冗余辅助接口，以便在主接口发生故障时接管管理功能。

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，也不能在管理器访问接口上创建子接口。 您还可以使用 管理中心 在单个辅助接口上启用管理器访问，以实现冗余。
- 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。

高可用性要求

将数据接口与设备高可用性配合使用时，请参阅以下要求。

- 在两台设备上使用相同的数据接口进行管理器访问。
- 不支持冗余管理器访问数据接口。
- 不能使用 DHCP；仅支持静态 IP 地址。无法使用依赖 DHCP 的功能，包括 DDNS 和零接触调配。
- 在同一子网中有不同的静态 IP 地址。
- 使用 IPv4 或 IPv6；不能同时设置。
- 使用相同的管理器配置（**configure manager add** 命令）确保连接相同。
- 不能将数据接口用作故障转移链路或状态链路。

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。

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
Cisco Secure Firewall 4200	management0 注释 management0 是管理 1/1 接口的内部名称。	management1 注释 management1 是管理 1/2 接口的内部名称。
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。
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。

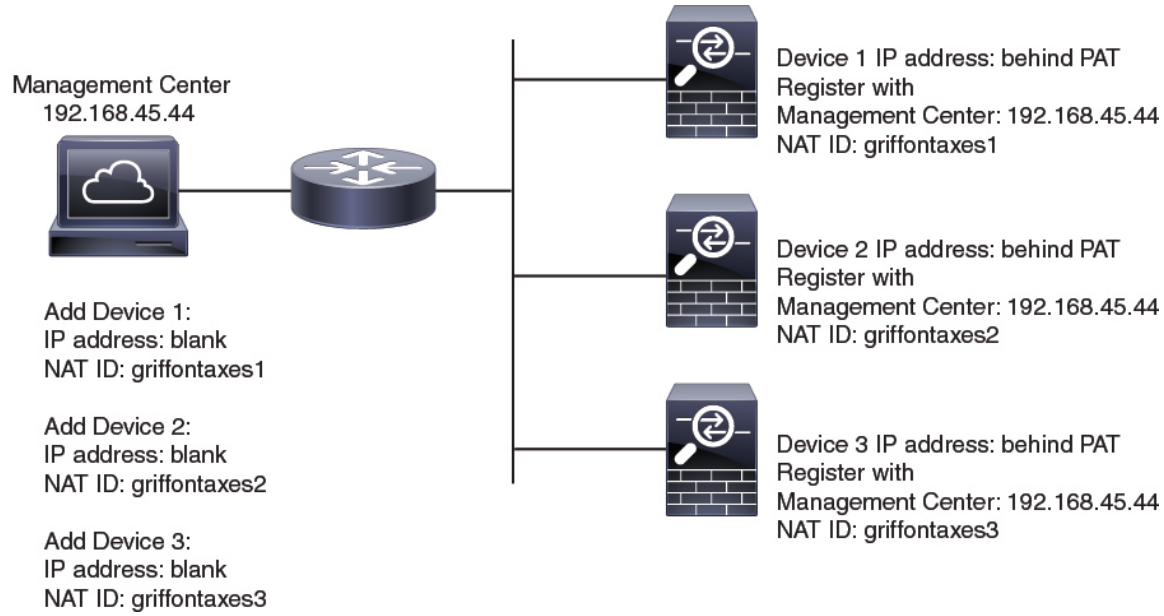
通常，无论是路由目的还是身份验证，都需要两个IP地址（连同一个注册密钥）：管理中心 当添加一个设备时，指定设备 IP 地址，设备指定 管理中心 IP 地址。但是，如果您只知道其中一个 IP 地址（这是实现路由目的的最低要求），您还必须在连接的两端指定唯一的NAT ID，以建立对初始通信的信任，并查找正确的注册密钥。管理中心和设备使用注册密钥和 NAT ID（而不是 IP 地址）对初始注册进行身份验证和授权。

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。

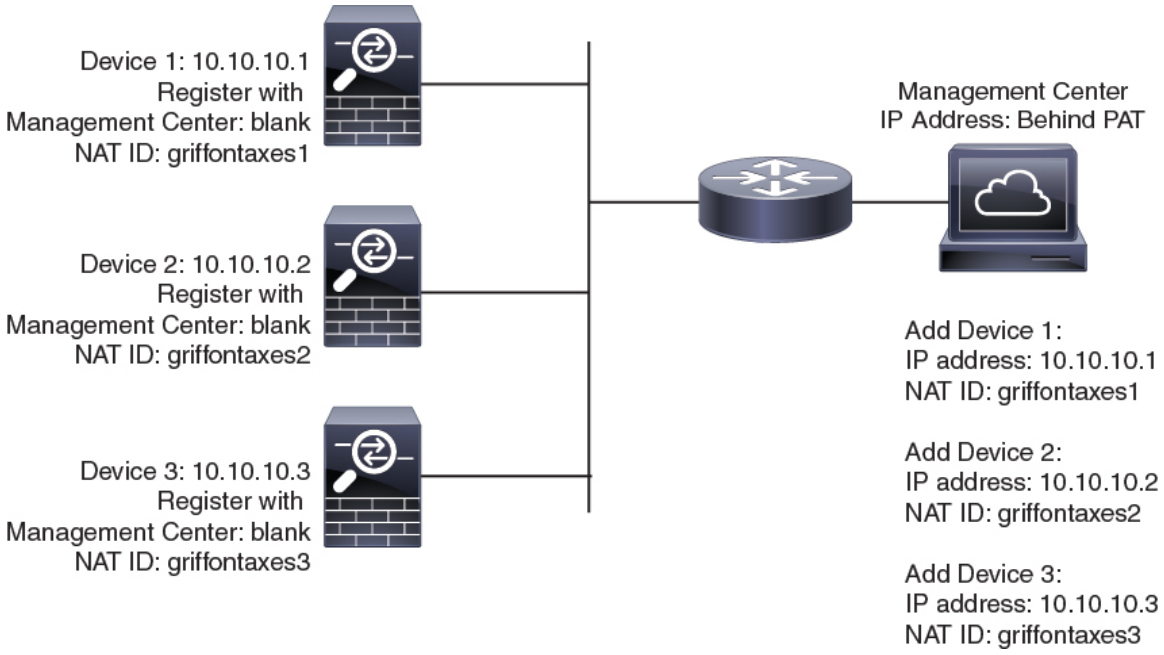
以下示例为 PAT IP 地址后的三个设备。在这种情况下，在 管理中心 和这些设备上为每个设备指定一个唯一的 NAT ID，并在这些设备上指定 管理中心 IP 地址。

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***

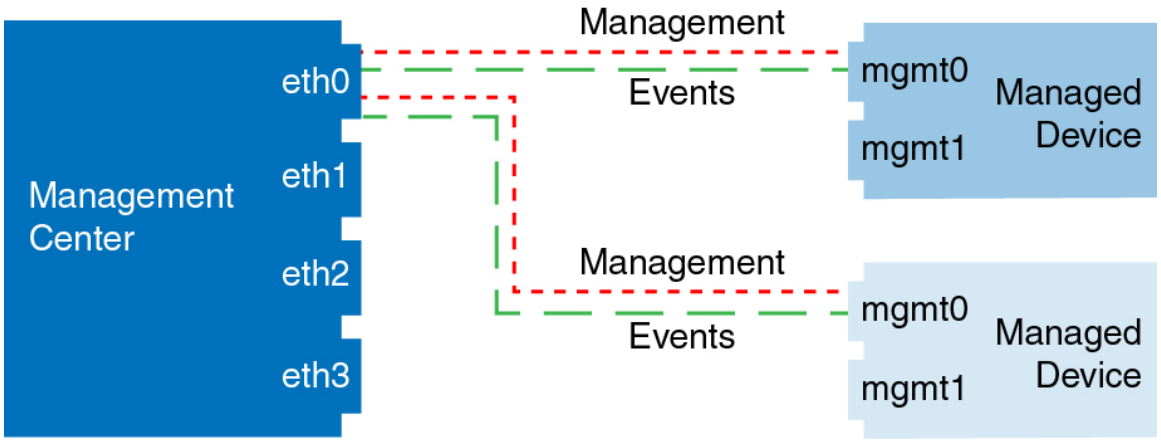


管理和事件流量通道示例

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。

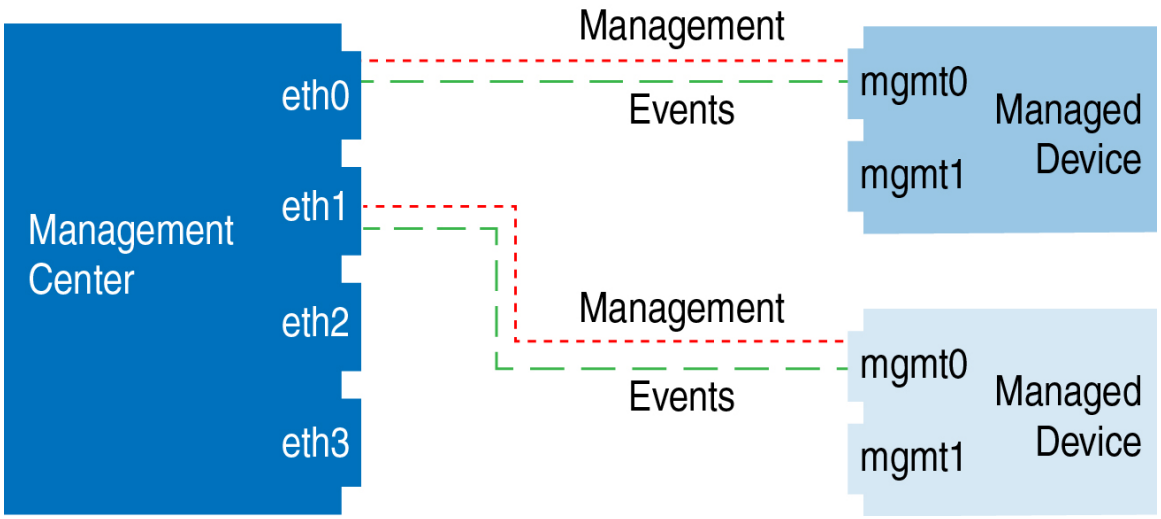
以下示例显示仅使用默认管理接口的 管理中心和受管设备。

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



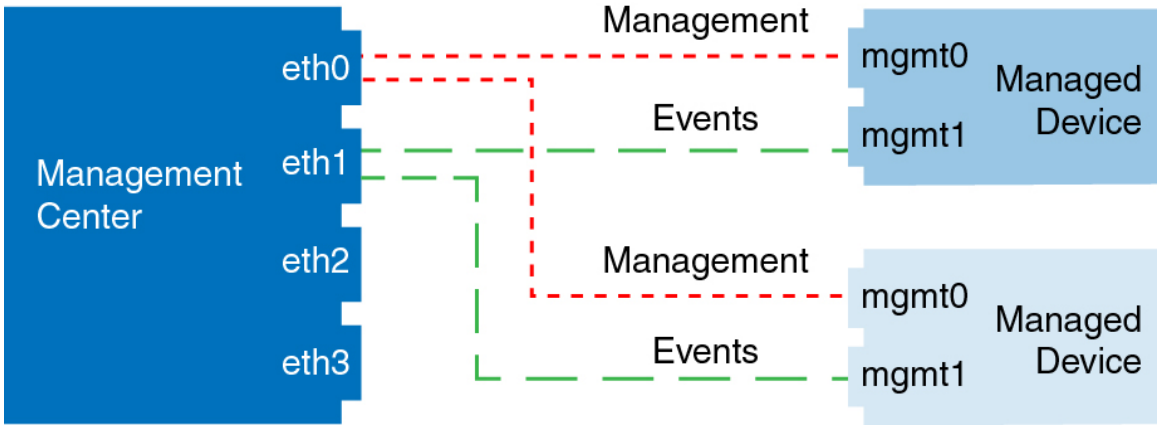
以下示例显示为设备使用单独管理接口的 管理中心；每台受管设备均使用 1 管理接口。

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



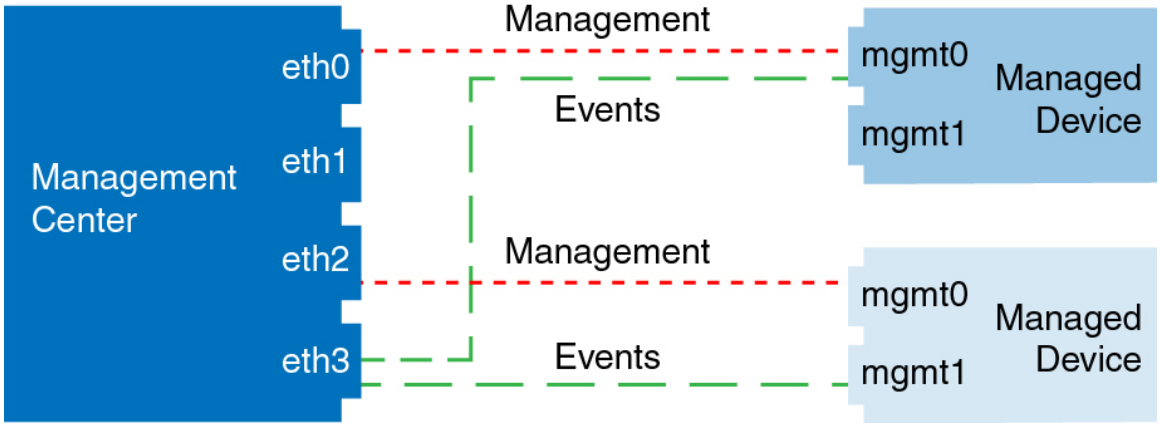
以下示例显示使用单独事件接口的 管理中心和受管设备。

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

支持的域

设备所在的域。

用户角色

- 管理员
- 网络管理员

管理连接

确保管理连接稳定，没有过多的丢包，吞吐量至少为 5 Mbps。

在设备上登录命令行界面

您可以在威胁防御设备上直接登录命令行界面。如果这是您第一次登录，请使用默认**管理员**用户完成初始设置过程；请参阅使用 CLI 完成威胁防御初始配置，第 18 页。

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

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SSH 访问 (SSH Access)，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

控制台端口上的 CLI 是 FXOS（ISA 3000 除外，它是常规 威胁防御 CLI）。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。

对于多实例模式下的机箱，您可以连接到控制台端口上的 FXOS，也可以根据配置 SSH 和 SSH 访问列表为管理接口启用 SSH。默认情况下禁用 SSH。

步骤 2 使用 **admin** 用户名和密码登录。

示例：

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1
```

```
firepower#
```

步骤 3 如果您使用的是控制台端口，请访问 威胁防御 CLI。

connect ftd

多实例模式：

connect ftd *name*

要查看实例名称，请输入不含名称的命令。

注释 此步骤不适用于 ISA 3000。

示例：

```
firepower# connect ftd
>
```

步骤 4 在 CLI 提示符 (>) 处，使用命令行访问级别所允许的任何命令。

要返回到控制台端口上的 FXOS，请输入 **exit**。

步骤 5 （可选） 如果您使用 SSH，则可以连接到 FXOS。

connect fxos

要返回到 威胁防御 CLI，请输入 **exit**。

步骤 6 （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**。

为手动注册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。

对于零接触调配（序列号注册），您不应登录设备或执行初始设置。请参阅使用序列号 (零接触调配) 将设备添加到管理中心，第 31 页。

使用设备管理器完成威胁防御初始配置

当您使用 设备管理器 进行初始设置时，除管理接口和管理器访问设置外，还会预配置以下接口：

- 以太网 1/1—“外部”，IP 地址来自 DHCP、IPv6 自动配置
- 以太网 1/2（或对于 Firepower 1010，为 VLAN1 接口）-“内部”，192.168.95.1/24
- 默认路由 - 通过外部接口上的 DHCP 获取

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。请注意，诸如内部的DHCP服务器、访问控制策略或安全区域等其他设置均未配置。

如果在向 管理中心 注册之前在 设备管理器 中执行其他特定于接口的配置，则会保留该配置。

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）。

- Cisco Secure Firewall 4200 不支持 设备管理器。您需要使用 CLI 程序：使用 CLI 完成威胁防御初始配置，第 18 页
- 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 18 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。

a) 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。

b) 使用用户名 **admin** 和默认密码 **Admin123** 登录。

c) 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。

a) 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。

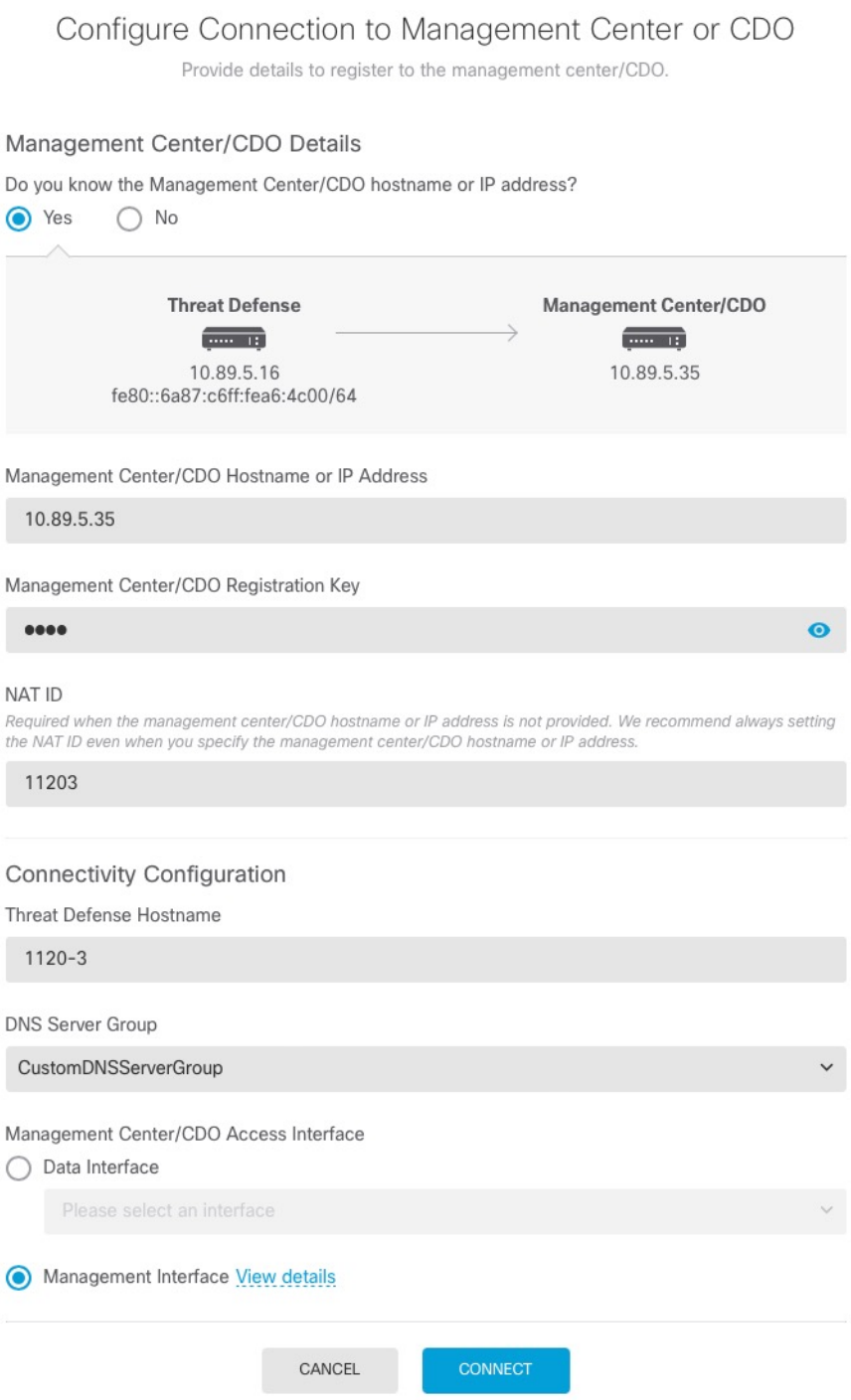
步骤 4 如果要配置其他接口，包括要用于管理器访问的外部或内部接口，请选择**设备 (Device)**，然后点击**接口 (Interfaces)** 摘要中的链接。

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



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 TLS-1.3 加密的通信通道。

b) 如果选择 **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。当您将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 CDO**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/)。

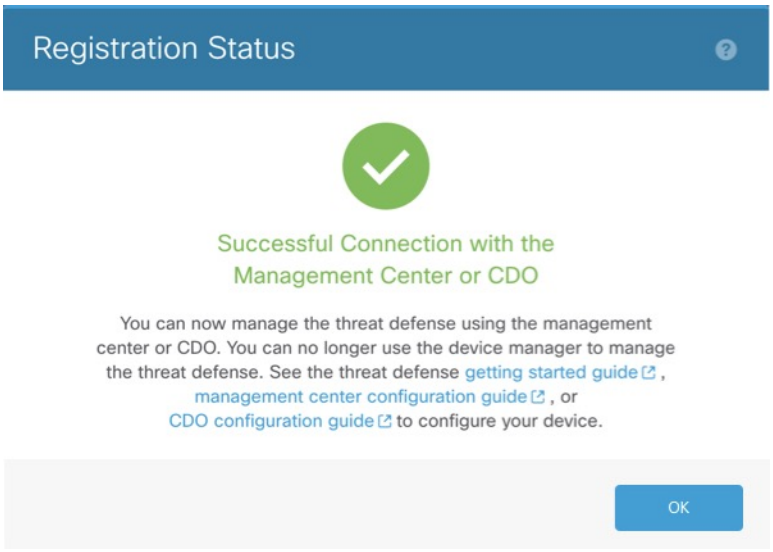
使用管理接口访问管理器时，不支持 DDNS。

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。

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，请参阅《Firepower 1000/2100 和 Cisco Secure Firewall 3100/4200 带威胁防御的 Cisco FXOS 故障排除指南》中的重新映像过程。

对于 ISA 3000，请参阅《Cisco Secure Firewall ASA 和 Secure Firewall Threat Defense 重新映像指南》。

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** 和/或 **输入管理接口的 IPv6 默认网关**-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。确保此接口与管理器访问接口位于不同的子网上，以防止出现路由问题。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** 和/或 **通过 DHCP、路由器或手动方式来配置 IPv6**？ - 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 TLS-1.3 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，也是必需的。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:

以下示例对具有 CDO 生成的显示名称的 CDO使用生成的命令，然后仅使用“分析-FMC”显示名称指定用于分析的本地 管理中心。

```
> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb 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。确保此接口与管理器访问接口位于不同的子网上，以防止出现路由问题。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://dwinchester: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，Firepower 4100/9300 和 Cisco Secure Firewall 4200，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 25 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
```

[…]

管理中心使用注册密钥将设备添加到

按照此程序使用注册密钥将单个设备添加到 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。

您还可以添加云管理设备，并将其用于本地部署 管理中心 的事件日志和分析目的。

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：
  - 为手动注册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》
- 管理中心必须注册到智能软件管理器。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。

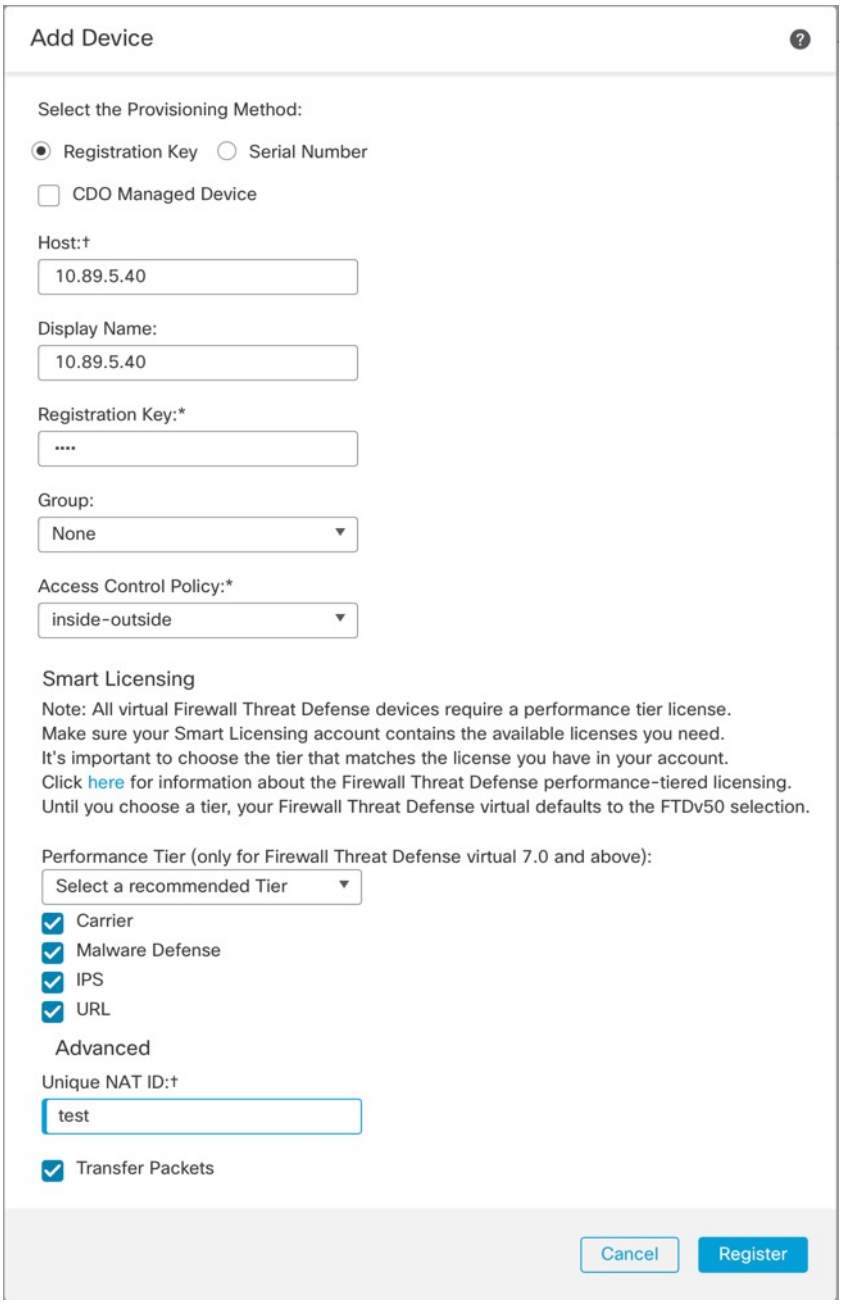
过程

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**。

默认情况下会选择**注册密钥**方法。

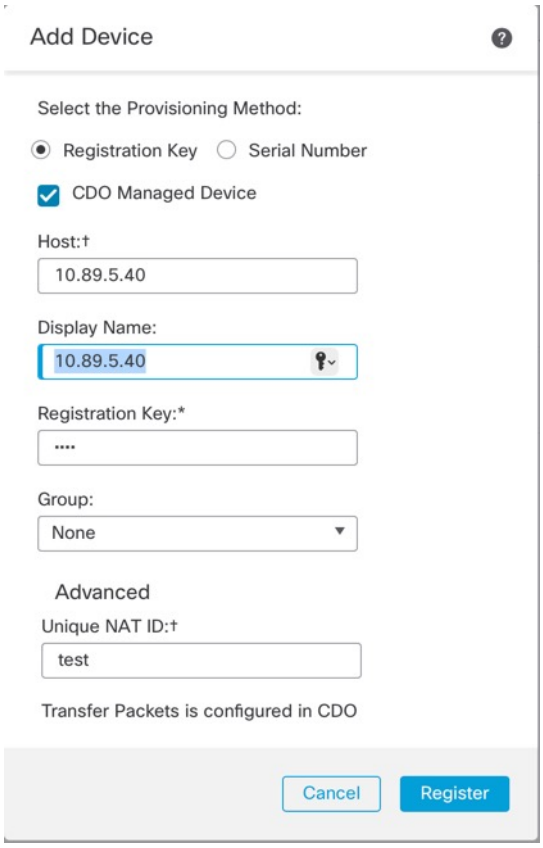
图 *9:* 使用注册密钥添加设备



步骤 3 如果要将云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**。

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 7 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 管理中心上注册设备，则必须在**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 （可选）将设备添加到设备**组**。

步骤 8 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 9 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。

对于 threat defense virtual，您还必须选择**性能层 (Performance Tier)**。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 10 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设备上指定该字符串。例如，如果您将**主机 (Host)** 字段留空，则为必填项。如果您使用设备的数据接口进行管理，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 如果使用设备上的数据接口进行管理，即使您同时指定了两个 IP 地址，也必须同时在设备和 管理中心 上指定 NAT ID。

步骤 11 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 12 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。

使用序列号 (零接触调配) 将设备添加到管理中心

通过零接触调配，您可以按序列号将设备注册到管理中心，而无需在设备上执行任何初始设置。管理中心 与 Cisco Defense Orchestrator (CDO) 集成以实现此功能。

使用 零接触调配时，系统会预配置以下接口：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。请注意，诸如内部的 DHCP 服务器、访问控制策略或安全区域等其他设置均未配置。

- 以太网 1/1—“外部”，IP 地址来自 DHCP、IPv6 自动配置
- 以太网 1/2（或对于 Firepower 1010，为 VLAN1 接口）-“内部”，192.168.95.1/24
- 默认路由 - 通过外部接口上的 DHCP 获取

零接触调配 不支持集群或多实例模式。

仅当使用管理接口时才支持高可用性，因为 零接触调配 使用 DHCP，数据接口和高可用性不支持 DHCP。

零接触调配 仅在以下运行 7.2、7.4 或更高版本的型号上受支持（在 7.2.4 之前， 管理中心 必须可公开访问）：

- Firepower 1010
- Firepower 1100
- Firepower 2100
- Cisco Secure Firewall 3100

开始之前

- 确保设备已取消配置或全新安装。零接触调配仅适用于新设备。预配置可以禁用零接触调配，具体取决于您的设置。
- 连接外部接口或管理接口，使其能够访问互联网。如果您使用外部接口进行零接触调配，请勿同时连接管理接口；如果管理接口从 DHCP 获取 IP 地址，则外部接口的路由将不正确。
- 请确保在 管理中心 上配置了至少一个访问控制策略，以便将其分配给新设备。不能使用 CDO 来添加策略。
- 如果设备没有公共 IP 地址或 FQDN，或者您使用管理接口，请为 管理中心 设置公共 IP 地址/FQDN（如果与 管理中心 管理接口 IP 地址不同；例如，它在 NAT 之后），以便设备可以发起管理连接。请参阅 **系统 (System)** > **配置 (Configuration)** > **管理器远程访问 (Manager Remote Access)**。您还可以在此程序期间在 CDO 中配置公共 IP 地址/FQDN。
- 管理中心必须注册到智能软件管理器。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

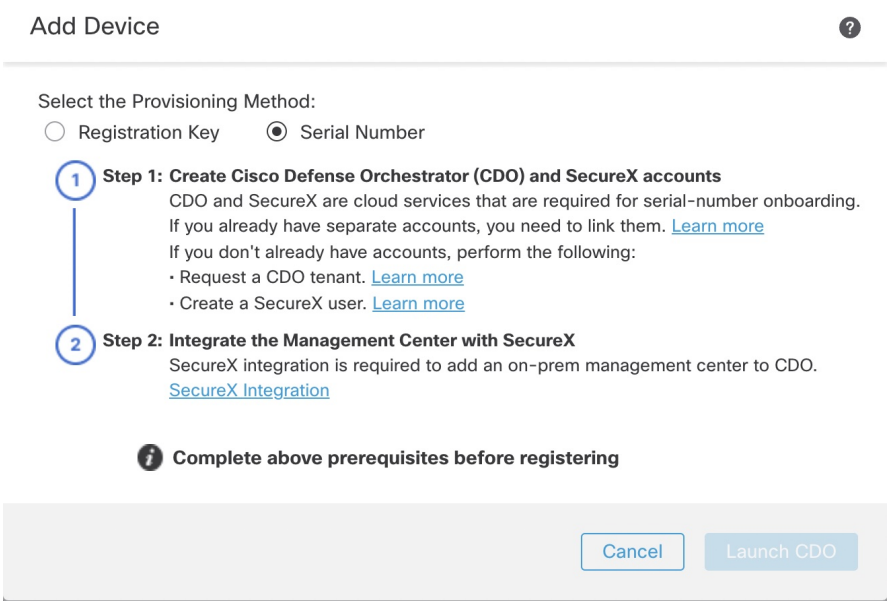
步骤 1 首次使用序列号添加设备时，需要满足以下前提条件。第一次完成后，您可以跳至直接在CDO中添加设备。

a) 在 管理中心上，选择 **设备** > **设备管理**。

b) 从 **添加** 下拉菜单中，选择 **设备**。

c) 点击**序列号 (Serial Number)** 以获取调配方法。

图 *11:* 按序列号添加设备



d) 创建 CDO 帐户。

注释 如果您已有单独的 SecureX 和 CDO 账户，则需要关联这些账户。有关关联帐户的详细信息，请参阅https://cisco.com/go/cdo-securex-link。

如果您还没有账户，请执行以下操作：

- 创建思科安全云（以前称为 SecureX）账户。有关如何创建 CDO 的信息，请参阅 CDO 文档。
- 请求 CDO 租户。有关请求新的 CDO 租户的信息，请参阅 CDO 文档 。

e) 将 管理中心 与思科安全云（以前称为 SecureX）集成。点击链接在 管理中心中打开 **SecureX 集成 (SecureX Integration)** 页面。

点击**启用 SecureX (Enable SecureX)** 打开单独的浏览器选项卡，让您登录思科安全云账户并确认显示的代码。确保此页面未被弹出窗口阻止程序阻止。

关于详细信息，请参阅 《Cisco Secure Firewall Management Center 管理指南》中的“使用外部工具进行事件分析”一章。

CDO 会在您将 管理中心 与思科安全云集成后载入本地 管理中心 。CDO 需要在其清单中添加 管理中心 ，以便进行零接触调配。CDO 的 管理中心 支持仅限于设备激活、查看其托管设备、查看与 管理中心 关联的对象，以及交叉启动 管理中心。

注释　　对于 管理中心 高可用性对，您还需要将辅助 管理中心 与思科安全云集成。

f) 如果尚未打开，请点击**启动** CDO，或在此处登录：https://www.defenseorchestrator.com/。

确保 CDO 未被弹出窗口阻止程序阻止。

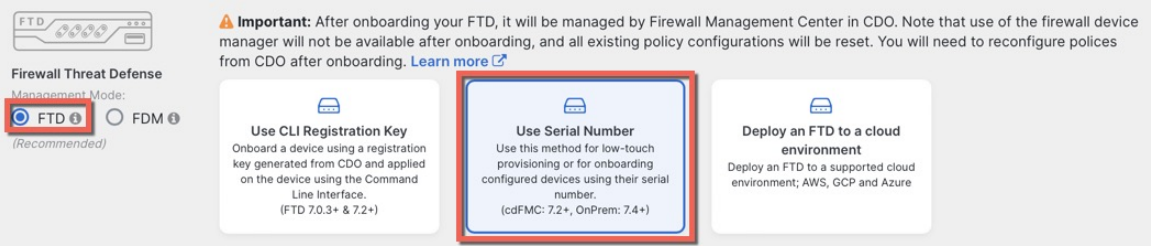
步骤 2　在 CDO**控制面板 (Dashboard)** (https://www.defenseorchestrator.com/) 上，点击**载入 (Onboard)**（ + Onboard ）。

步骤 3　点击 **FTD** 磁贴。

图 *12: FTD* 磁贴

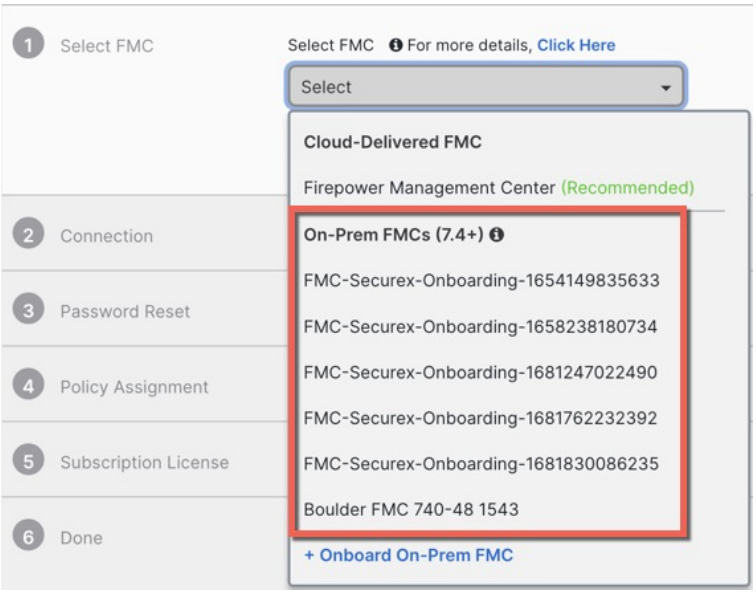
步骤 4　在**载入 FTD 设备 (Onboard FTD Device)** 屏幕上，点击**使用序列号 (Use Serial Number)**。

图 *13:* 使用序列号



步骤 5　在**选择 FMC (Select FMC)** 中，从列表选择**本地 FMC (On-Prem FMC)**，然后点击**下一步 (Next)**。

图 *14:* 选择 ***FMC***



如果 管理中心 设置了公共 IP 地址或 FQDN，则会在您选择后显示。

图 *15:* 公共 ***IP*** 地址***/FQDN***

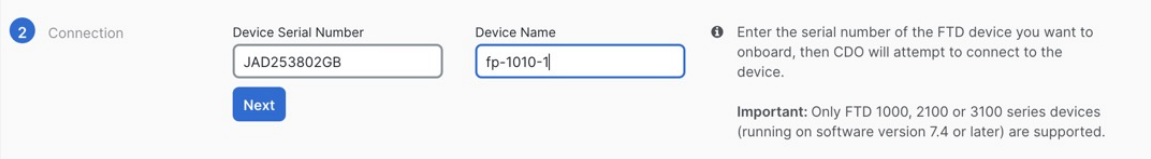
如果设备没有公共 IP 地址/FQDN，或者您使用管理接口进行零接触调配，则 管理中心 需要公共 IP 地址/FQDN。您可以通过点击 **FMC 公共 IP (FMC Public IP)** 链接来设置 管理中心 公共 IP 地址/FQDN。您将看到以下对话框。

图 *16:* 配置 ***FMC*** 公共 ***IP/FQDN***

注释　对于 管理中心 高可用性对，您还需要在辅助 管理中心上设置公共 IP 地址/FQDN。您不能使用 CDO来设置此值；您需要在辅助 管理中心中进行设置。请参阅 **系统 (System)** > > **配置 (Configuration)** > **管理器远程访问 (Manager Remote Access)**。

步骤 6　在**连接 (Connection)** 中，输入设备的序列号和设备名称。点击**下一步**。

图 *17:* 连接

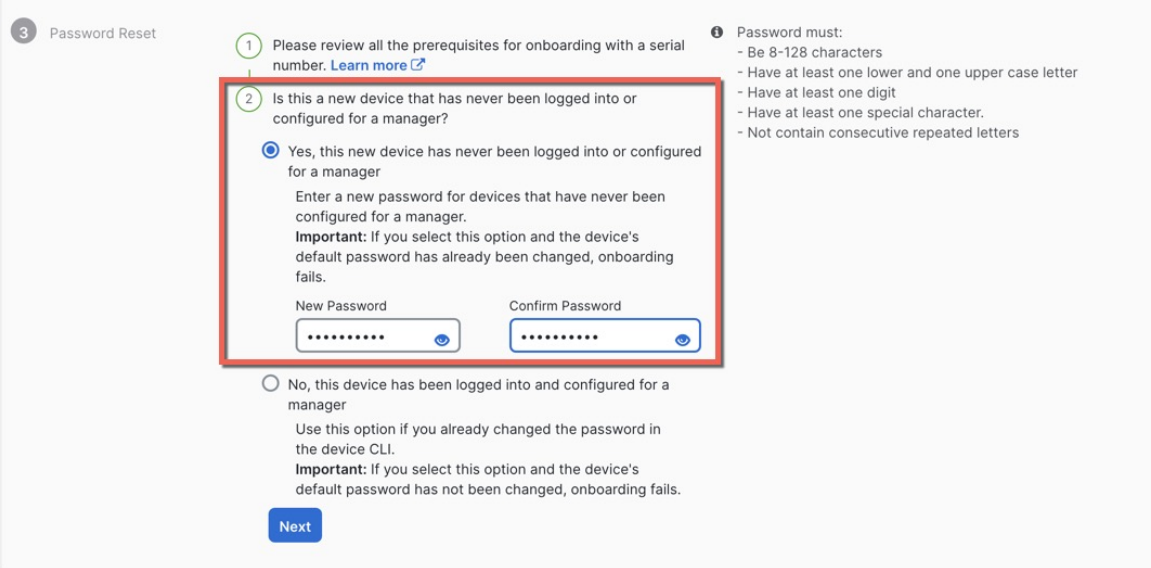


步骤 7　在**密码重置 (Password Reset)** 中，点击**是... (Yes...)** 。输入设备的新密码并确认新密码，然后点击**下一步 (Next)**。

对于零接触调配，设备必须是全新的或已重新映像。

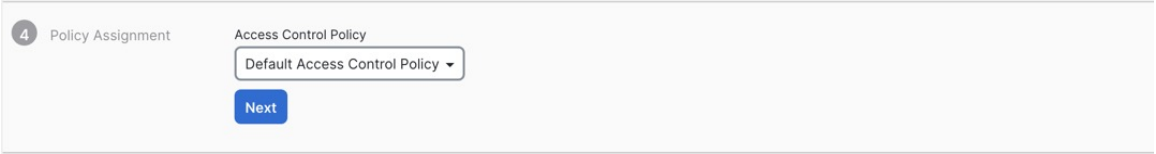
注释　如果您确实登录了设备并重置了密码，并且没有以禁用零接触调配的方式更改配置，则应选择**否... (No...)** 选项。有许多配置会禁用零接触调配，因此我们不建议登录设备，除非您需要这样做，例如执行重新映像。

图 *18:* 密码重设



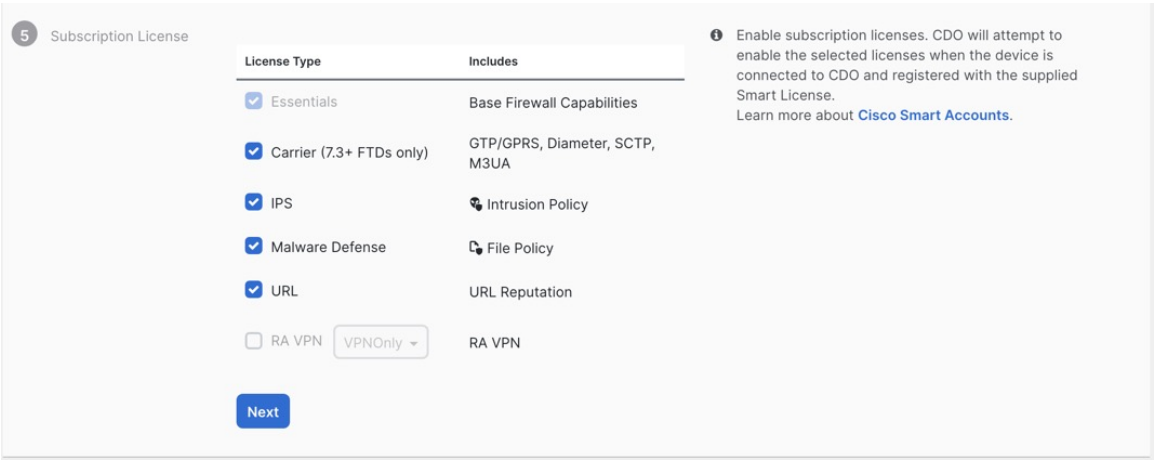
步骤 8　在**策略分配 (Policy Assignment)** 中，请使用下拉菜单为设备选择访问控制策略。如果尚未在 管理中心上添加策略，则应立即转到 管理中心 并添加策略。点击**下一步**。

图 *19:* 策略分配



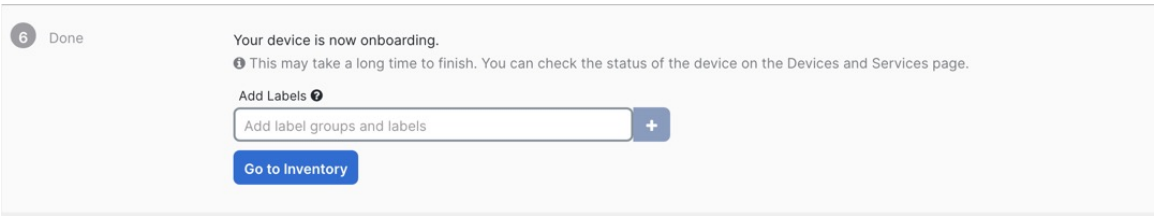
步骤 9 在**订用许可证 (Subscription License)** 中，为设备选择许可证。点击**下一步**。

图 *20:* 订用许可证



步骤 10 在**完成 (Done)** 中，您可以向 CDO中显示的设备添加标签；它们不会用在 管理中心上。

图 *21:* 完成



在 管理中心 中，设备会被添加到**设备管理 (Device Management)** 页面中。您还可以点击**转到清单 (Go to Inventory)** 查看 CDO 中的设备。可在 CDO 清单中查看本地 管理中心 设备，以供参考。

在外部接口上使用零接触调配时，CDO 会充当 DDNS 提供商并执行以下操作：

- 使用 "fmcOnly" 方法在外部启用 DDNS。此方法仅支持零接触调配设备。
- 使用以下主机名映射外部 IP 地址： *serial-number*.**local**。
- 提供到 管理中心 的 IP 地址/主机名映射，以便将主机名解析为正确的 IP 地址。
- 如果 IP 地址发生变化（例如 DHCP 租用更新），则会向 管理中心 发送通知。

如果在管理接口上使用零接触调配，则不支持 DDNS。 管理中心 必须可公开访问，以便设备能够发起管理连接。

您可以继续使用 CDO 作为 DDNS 提供商，也可以稍后将 管理中心 中的 DDNS 配置更改为其他方法。有关详细信息，请参阅配置动态 DNS。

如果设备注册失败，请参阅解决序列号（零接触调配）注册问题，第 114 页。

将机箱添加到管理中心

您可以将 Firepower 4100/9300 添加到管理中心。管理中心和机箱使用机箱 MGMT 接口共享单独的管理连接。 管理中心提供机箱级运行状况警报。对于配置，您仍需要使用 Cisco Secure Firewall 机箱管理器 或 FXOS CLI。

注释 对于 Cisco Secure Firewall 3100，，管理器配置在转换为多实例模式的过程中完成。请参阅启用多实例模式。启用多实例模式后，请参阅 将多实例机箱添加到 管理中心。

过程

步骤 1 通过控制台端口或使用 SSH连接至机箱 FXOS CLI。

步骤 2 配置管理中心。

create device-manager *manager_name* [**hostname** {*hostname* | *ipv4_address* | *ipv6_address*}] [**nat-id** *nat_id*]

系统将提示您输入注册密钥。

您可以从任何范围输入此命令。无需使用 **commit-buffer**即可立即接受此命令。

- **hostname** {*hostname* | *ipv4_address* | *ipv6_address*}—Specifies either the FQDN or IP address of the 管理中心。必须至少有一个设备（管理中心或机箱）具有可访问的IP地址，才能在两个设备之间建立双向 TLS-1.3 加密的通信通道。如果未在此命令中指定 **hostname**，则机箱必须具有可访问的 IP 地址或主机名，并且必须指定 **nat-id**。
- **nat-id** *nat_id*- 指定您选择的唯一的一次性字符串，注册机箱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 机箱上指定它。如果您不指定 **hostname**，则必须设置，但我们建议您始终设置 NAT ID，即使您指定了主机名或 IP 地址。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。
- **Registration Key:** *reg_key*- 系统将提示您输入选择的一次性注册密钥，注册机箱时也要在 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 (-)。

示例：

```
firepower# create device-manager boulder_fmc hostname 10.89.5.35 nat-id 93002
(Valid registration key characters: [a-z],[A-Z],[0-9],[-]. Length: [2-36])
```

```
Registration Key: Impala67
```

步骤 3 在 管理中心中，使用机箱管理 IP 地址或主机名添加机箱。

a) 选择 **设备** > **设备管理**，然后选择 **添加** > **添加集群**。

图 *22:* 添加机箱

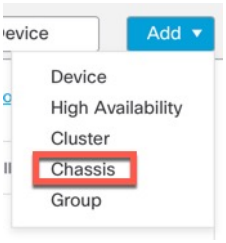
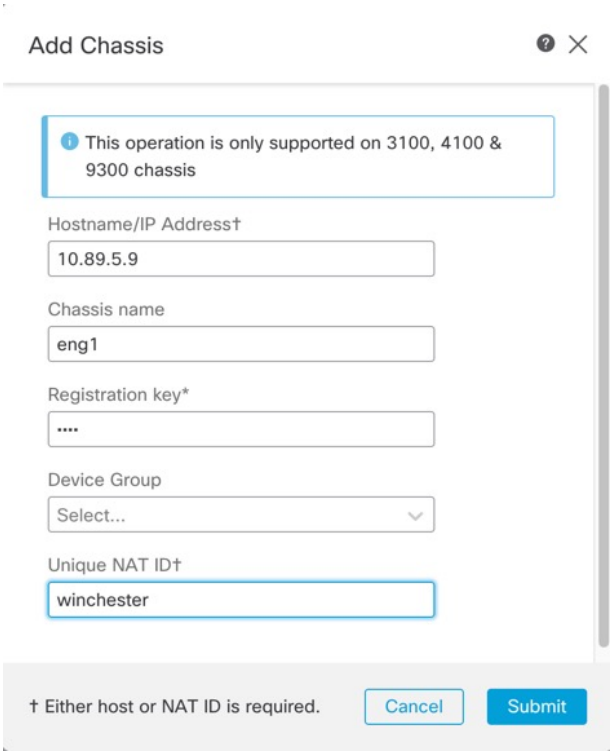


图 *23:* 添加机箱



b) 在 **主机/IP 地址** 字段中，输入要添加的设备的 IP 地址或主机名。

如果您不知道主机名或 IP 地址，可以将此字段留空，指定 **唯一 NAT ID**。

c) 在 **机箱名称** 字段中，输入要在 管理中心中显示的设备名称。

d) 在 **注册密钥** 字段中，输入将机箱配置为由 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（-）。

e) 在多域部署中，无论当前的域是什么，都将该机箱分配给叶 **域**。

如果当前域是叶域，机箱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机箱。一个机箱只能属于一个域。

f) （可选）将机箱添加到 **设备组**。

g) 如果在机箱安装过程中使用了 NAT ID，请展开并在 **唯一 NAT ID** 字段中输入相同的 NAT ID。

NAT ID 可以包含字母数字字符和连字符（-）。

h) 点击 **Submit**。

机箱将添加到 **设备** > **设备管理** 页面。

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** 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。
- 保持配置不变，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。

在删除设备之前，请务必导出配置，以便在重新注册设备时可以重新应用设备级配置（接口、路由等）。如果您没有已保存的配置，则必须重新配置设备设置。

重新添加设备并导入已保存的配置或重新配置设置后，您需要先部署配置，然后才能再次开始传递流量。

开始之前

要重新应用设备级配置（如果您将其重新添加到 管理中心：

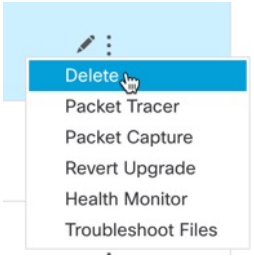
- 导出设备配置。请参阅导出和导入设备配置，第 50 页。

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 **更多**（⋮），然后点击**删除 (Delete)**。

图 *24:* 删除



步骤 3 确认您要取消注册设备。

步骤 4 您现在可以更改管理器。

- 向此 管理中心 重新注册设备 - 如果您知道注册密钥和 NAT ID，则可以 管理中心使用注册密钥将设备添加到 ， 第 27 页。如果您需要重置它们，则可以像新配置一样重新配置管理器。请参阅 识别新的 管理中心 ， 第 107 页。
- 注册到新的 管理中心 - 识别新的 管理中心 ， 第 107 页。
- 更改为 设备管理器 - 从 管理中心 切换到 设备管理器 ， 第 112 页。
- 删除管理器而不指定新管理器 - 要在不识别新管理器的情况下切断 威胁防御 上的管理连接（无管理器模式），请在 威胁防御 CLI 中使用 **configure manager delete** 命令。

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。

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**（ ）。

步骤 3 点击**设备 (Device)**。

步骤 4 要重启设备：

a) 请点击 **重启设备** （ ）。

b) 出现提示时，确认是否要重启设备。

步骤 5 要关闭设备：

a) 在**系统 (System)** 部分中点击 **关闭设备** （ ）。

b) 出现提示时，确认是否要关闭设备。

c) 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。

对于 ISA 3000，完成关闭后，系统 LED 将熄灭。至少等待 10 秒，然后再断开电源。

下载受管设备列表

您可以下载所有受管设备的报告。

开始之前

要执行以下任务，您必须是管理员用户。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 点击 **下载设备列表报告** 链接。

步骤 3 您可以下载 CSV 或 PDF 格式的设备列表。选择 **下载 CSV** 或 **下载 PDF** 以下载报告。

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、版本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-取消注册设备。
  - “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。

图 *25:* 概述

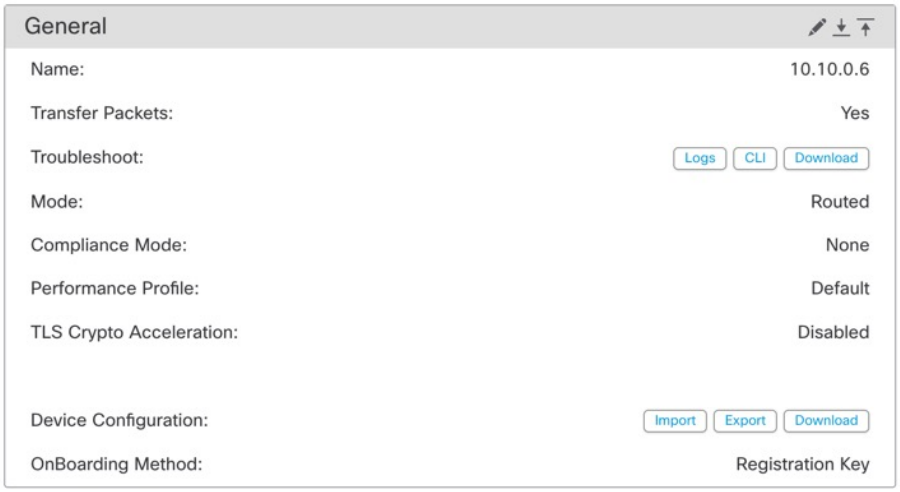


表 *2:*“常规”*(General)*部分表字段

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 。
故障排除	可用于生成和下载故障排除文件，还可查看CLI命令输出。请参阅生成故障排除文件，第 44 页和查看 CLI 输出，第 47 页。
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。
性能配置文件	这将显示设备的核心分配性能配置文件，如平台设置策略中所配置。
TLS 加密加速：	显示 TLS 加密加速是已启用还是已禁用。

字段	说明
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 49 页和导出和导入设备配置，第 50 页。
载入方法	显示设备是使用注册密钥还是使用序列号注册的 (零接触调配)。

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**（✎）。

步骤 3 点击**设备 (Device)**。

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

a) 输入托管设备的**名称 (Name)**。

b) 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。

c) 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 **故障排除** 操作，请参阅 生成故障排除文件，第 44 页 和 查看 CLI 输出，第 47 页。

步骤 6 有关**设备配置** 操作，请参阅将配置复制到另一台设备，第 49 页和导出和导入设备配置，第 50 页。

步骤 7 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。

生成故障排除文件

您可以在每个设备以及所有集群节点生成和下载故障排除文件。对于集群，您可以将所有文件下载为一个压缩文件。您还可以为集群节点添加集群的集群日志。

您也可以从**设备 (Devices)** > **设备管理 (Device Management)** > **更多**（⋮） > **故障排除文件 (Troubleshoot Files)** 菜单中触发文件生成。

过程

步骤 1 选择 **设备** > **设备管理**。

步骤 2 点击要查看的设备旁边的 **编辑**（✎）。

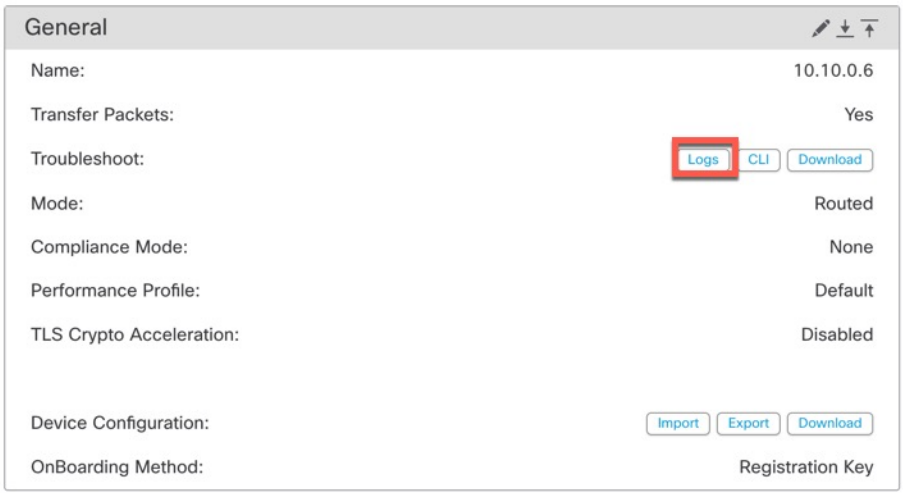
在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 3 点击 **设备** 或 **集群**。

步骤 4 为设备或所有集群节点生成日志。

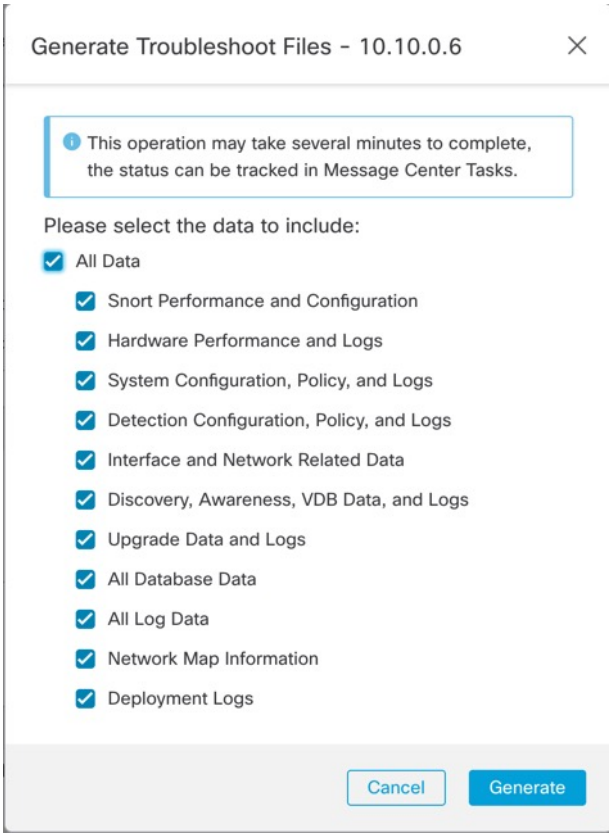
a) 在 **常规** > **故障排除** 部分，点击 **日志**。

图 *26:* 日志



b) 系统会提示您选择要包括的日志。对于集群，在 **设备**下，您可以选择 **所有设备** 或单个节点。集群还具有可用的 **集群日志** 。

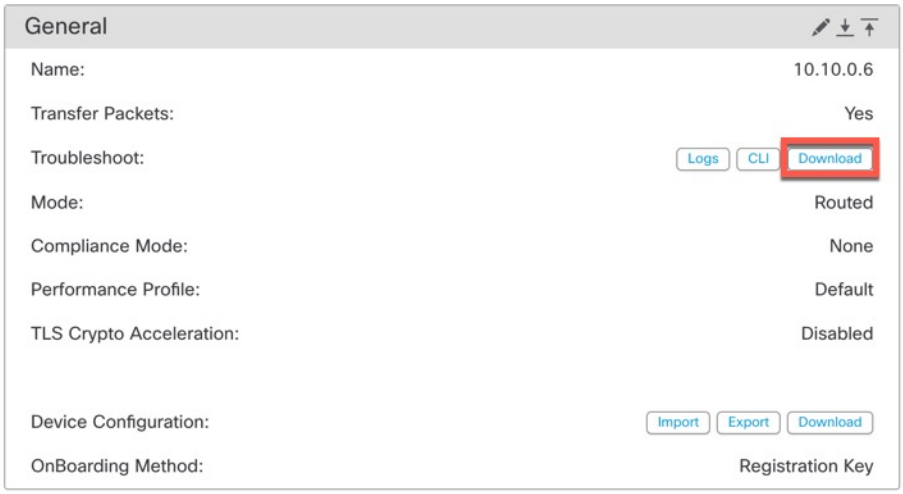
图 *27:* 生成故障排除文件



c) 点击**生成 (Generate)**。

步骤 5 要下载生成的日志，请在 **常规 > 故障排除** 部分，点击 **下载**。

图 *28:* 下载



日志将下载到您的计算机。

查看 CLI 输出

您可以查看一组预定义的 CLI 输出，帮助您排除设备或集群的故障。您还可以输入任何 **show** 命令并查看输出。

对于设备，执行以下命令：

- **show version**
- **show asp drop**
- **show counters**
- **show int ip brief**
- **show blocks**
- **show cpu detailed**

对于集群或集群节点：

- **show running-config cluster**
- **show cluster info**
- **show cluster info health**
- **show cluster info transport cp**
- **show version**
- **show asp drop**
- **show counters**
- **show arp**
- **show int ip brief**
- **show blocks**
- **show cpu detailed**
- **show interface** *ccl_interface*
- **ping** *ccl_ip* **size** *ccl_mtu* **repeat 2**

过程

步骤 1 选择 **设备** > **设备管理**。

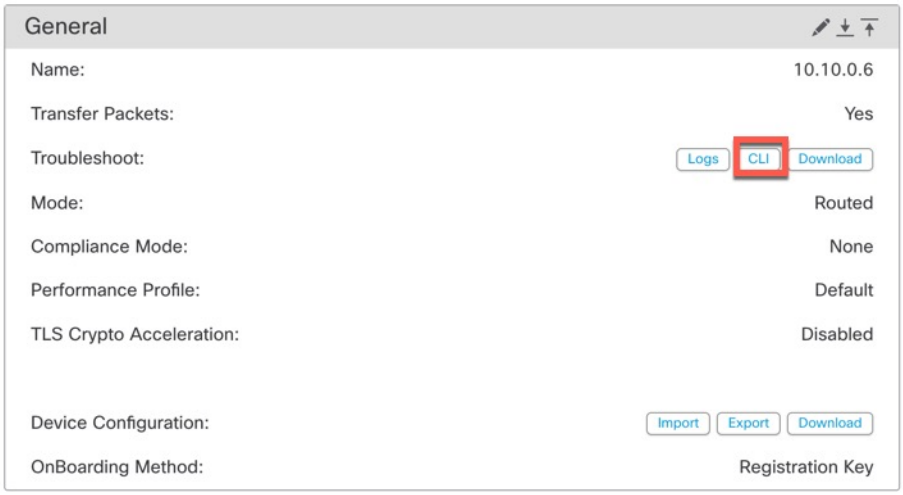
步骤 2 点击要查看的设备旁边的 **编辑**（✎）。

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** 或 **集群**。

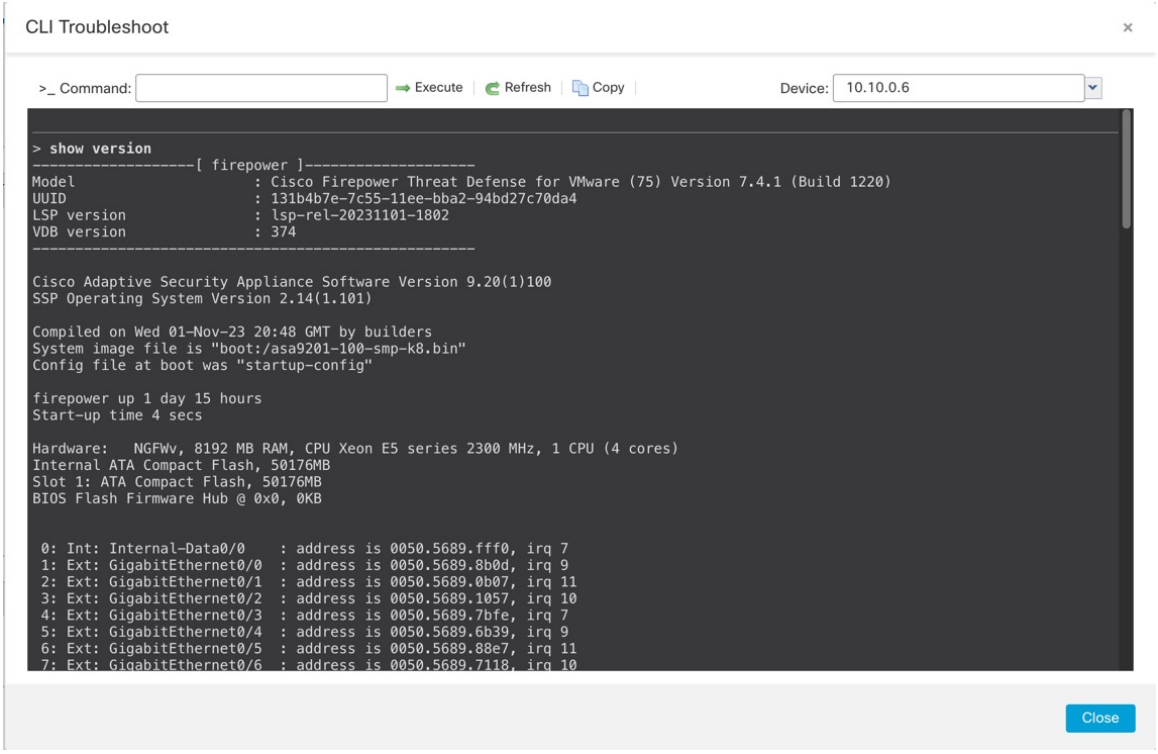
步骤 4 在 **常规 > 故障排除** 部分，点击 **CLI**。

图 *29: CLI*



系统将显示 **CLI 故障排除** 对话框，其中包含已执行的预定义 CLI。

图 *30: CLI* 故障排除



步骤 5 在 **CLI 故障排除** 对话框中，您可以执行以下任务。

- 在 **命令** 字段中输入 **show** 命令，然后点击 **执行**。新的命令输出将添加到窗口中。
- 点击 **刷新** 以重新运行预定义的 CLI。
- 点击 **复制** 以将输出复制到剪贴板上。
- 对于集群，请从 **设备** 下拉列表中选择其他节点。

步骤 6 点击 **Close**。

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**（ ）。

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

您可以导出设备页面上可配置的所有设备特定配置，包括：

- 接口
- 内联集
- 路由

- DHCP
- VTEP
- 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 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。
存在名称相同但值不同的对象。	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**（）。

步骤 3 点击 **设备**。

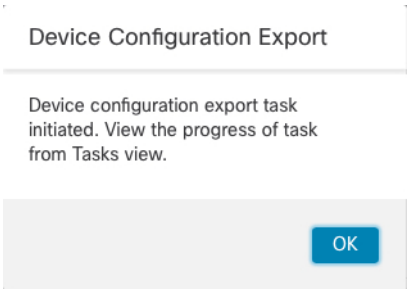
步骤 4 导出配置。

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

图 *31:* 导出设备配置

系统将提示您确认导出；点击**确定 (OK)**。

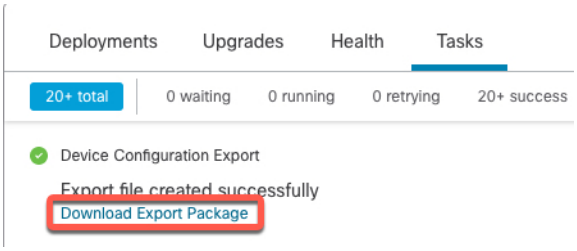
图 *32:* 确认导出



您可以在**任务 (Tasks)** 页面中查看导出进度。

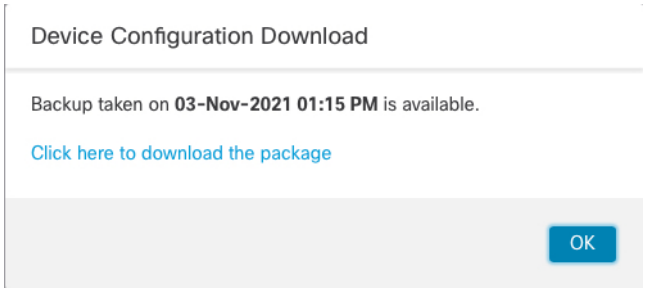
b) 在**通知 (Notifications)** > **任务 (Tasks)** 页面上，确保导出已完成；点击**下载导出包 (Download Export Package)**。或者，您可以点击**常规 (General)** 区域中的**下载 (Download)** 按钮。

图 *33:* 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 *34:* 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 *35:* 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 *36:* 导入软件包

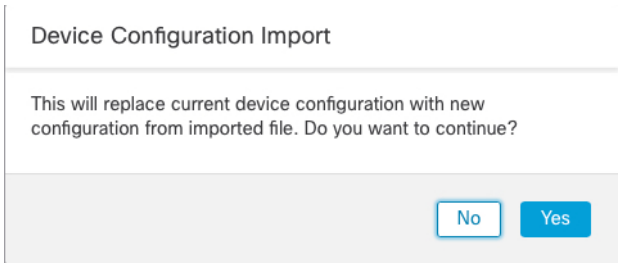
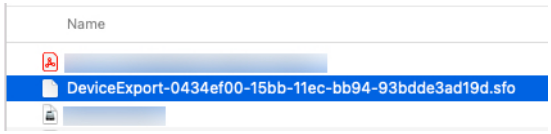
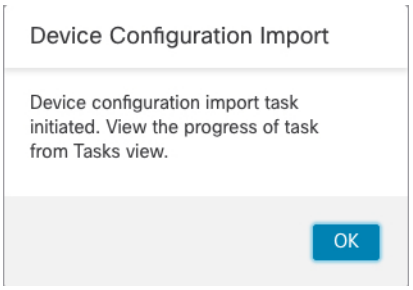


图 *37:* 导航至软件包



系统将提示您确认导入；点击**确认 (OK)**。

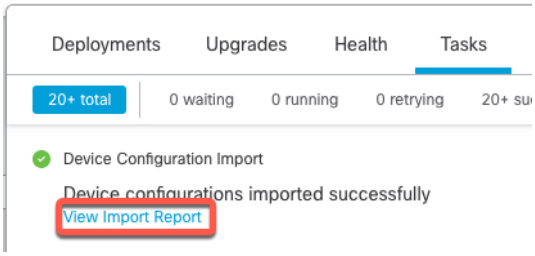
图 *38:* 确认导入



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 *39:* 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**（ ）。

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 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。

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	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 78 页。

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

如果您使用零接触调配在外部接口上注册设备，则会自动生成主机名以及匹配的 DDNS 配置；在这种情况下，您无法编辑主机名。

过程

步骤 1 选择**设备** > **设备管理**。

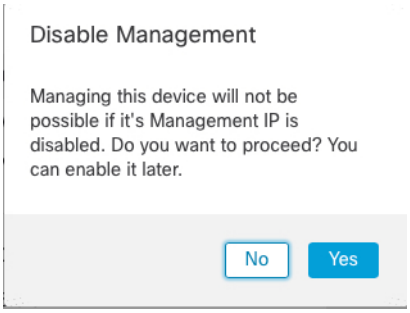
步骤 2 在要修改管理选项的设备旁边，点击 **编辑**（ ）。

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 （ ）。

图 *40:* 禁用管理

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。

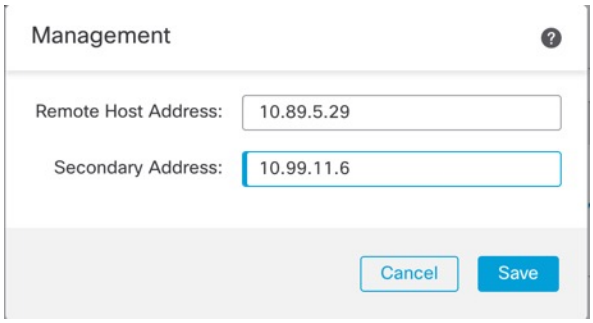
步骤 5 通过点击 **编辑**（ ） 来编辑**远程主机地址** IP 地址和可选**辅助地址**（使用冗余数据接口时）或主机名。

图 *41:* 编辑管理地址

步骤 6 在**管理 (Management)** 对话框中，在**远程主机地址 (Remote Host Address)** 字段和可选的**辅助地址 (Secondary Address)** 字段中修改名称或 IP 地址，然后点击**保存 (Save)**。

有关使用辅助管理器访问数据接口的信息，请参阅配置冗余管理器访问数据接口 ，第 69 页。

图 *42:* 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 *43:* 启用管理连接

更改管理中心和威胁防御 IP 地址

如果需要将 管理中心 和 威胁防御 IP 地址移至新网络，则可能需要同时更改这些地址。

过程

步骤 1 禁用管理连接。

对于高可用性对或集群，在所有设备上执行这些步骤。

a) 选择**设备** > **设备管理**。

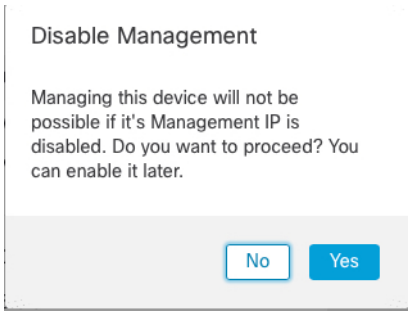
b) 点击设备旁边的 **编辑**（ ）。

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

d) 点击滑块暂时禁用管理，使其处于禁用状态 （ ）。

图 *44:* 禁用管理

系统将提示您继续禁用管理；点击 **是**。



步骤 2 将 管理中心 中的设备 IP 地址更改为新的设备 IP 地址。

稍后您将更改设备上的 IP 地址。

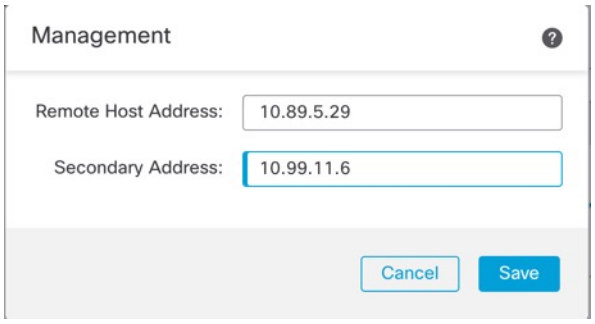
对于高可用性对或集群，在所有设备上执行这些步骤。

a) 通过点击 **编辑**（ ）来编辑**远程主机地址** IP 地址和可选**辅助地址**（使用冗余数据接口时）或主机名。

图 ***45:*** 编辑管理地址

b) 在**管理 (Management)** 对话框中，在**远程主机地址 (Remote Host Address)** 字段和可选的**辅助地址 (Secondary Address)** 字段中修改名称或 IP 地址，然后点击**保存 (Save)**。

图 ***46:*** 管理 ***IP*** 地址



步骤 3 请更改 管理中心 IP 地址。

注意 对所连接的管理中心接口进行更改时要保持谨慎；如果由于配置错误而无法重新连接，则需要访问 管理中心 控制台端口以重新配置 Linux 外壳中的网络设置。您必须与思科 TAC 联系，以获取有关执行此项操作的指导。

a) 选择 **系统**（⚙）> **配置**，然后选择**管理接口**。
b) 在**接口**区域中，点击要配置的接口旁边的**编辑**。
c) 更改 IP 地址，然后点击**保存 (Save)**。

步骤 4 更改设备上的管理器 IP 地址。

对于高可用性对或集群，在所有设备上执行这些步骤。

a) 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
```

b) 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**。

示例：

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

步骤 5 在控制台端口更改管理器访问接口的 IP 地址。

对于高可用性对或集群，在所有设备上执行这些步骤。

如果您使用专用管理接口：

configure network ipv4

configure network ipv6

如果您使用专用管理接口：

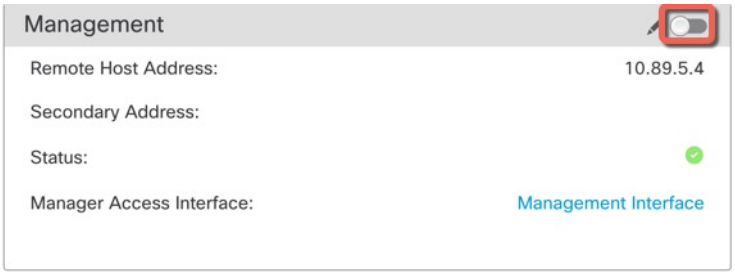
configure network management-data-interface disable

configure network management-data-interface

步骤 6 点击滑块重新启用管理，使其处于启用状态（🔵）。

对于高可用性对或集群，在所有设备上执行这些步骤。

图 *47:* 启用管理连接



步骤 7 （如果使用数据接口进行管理器访问）刷新 管理中心中的数据接口设置。

对于高可用性对，请在两台设备上执行此步骤。

a) 选择**设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **管理 (Management)** > **管理访问权限 - 配置详细信息 (Manager Access - Configuration Details)**，然后点击**刷新 (Refresh)**。

b) 选择**设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)**，然后设置 IP 地址以便与新地址匹配。

c) 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。

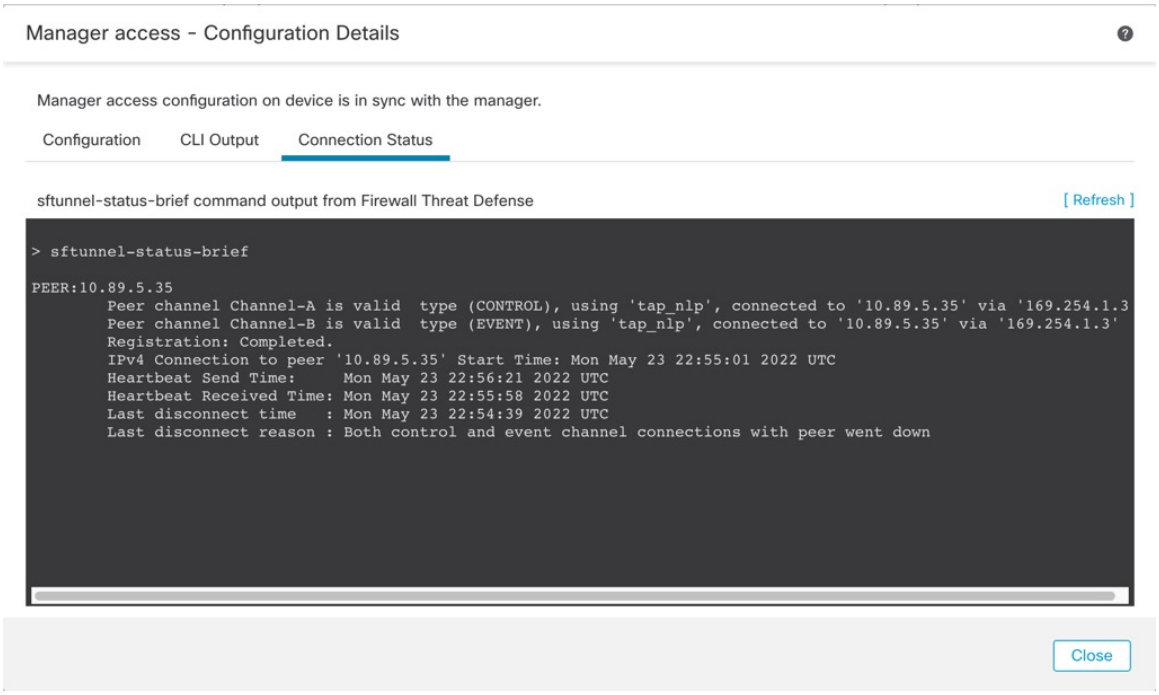
步骤 8 确保管理连接已重新建立。

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 *48:* 连接状态



步骤 9 （对于高可用性 管理中心 对）在辅助 管理中心上重复配置更改。

a) 更改辅助 管理中心 IP 地址。
b) 在两台设备上指定新的对等地址。
c) 将辅助设备设置为主用设备。
d) 禁用设备管理连接。
e) 更改 管理中心 中的设备 IP 地址。
f) 重新启用管理连接。

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 66 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。

开始之前

对于高可用性对，除非另有说明，否则请仅在主用设备上执行所有步骤。一旦配置更改被部署，备用设备会同步主用设备的配置和其他状态信息。

过程

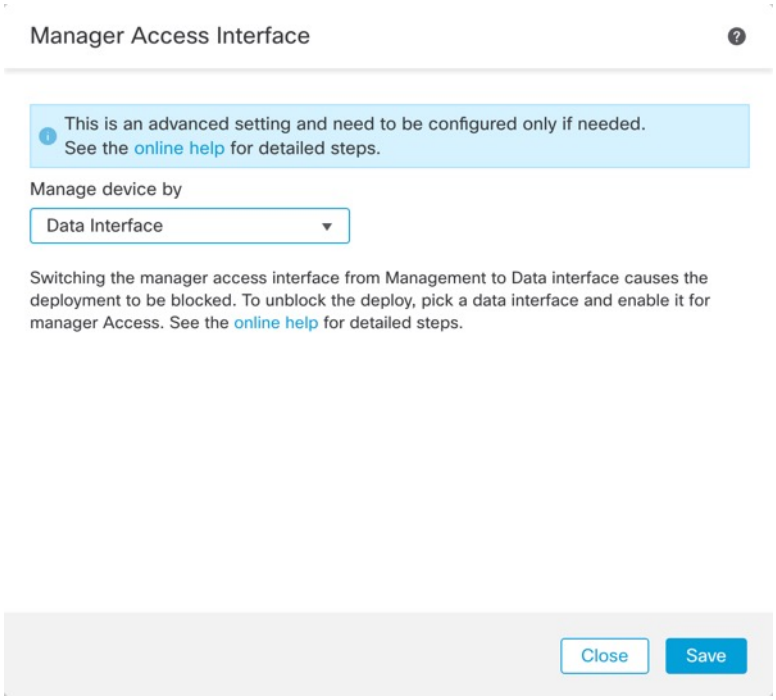
步骤 1 初始化接口迁移。

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 *49:* 管理器访问接口



c) 点击**保存 (Save)**。

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 *50:* 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以及一个可选的辅助接口上启用管理器访问。确保这些接口使用名称和 IP 地址进行了充分配置，并且已启用。

如果使用辅助接口实现冗余，请参阅配置冗余管理器访问数据接口，第 69 页以了解其他所需的配置。

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SSH 访问 (SSH Access)。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。 对于高可用性，请在两台设备上执行此步骤。

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。 对于高可用性，请在两台设备上执行此步骤。

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**远程主机地址 (Remote Host Address)**IP 地址 (IP address) 和可选**辅助地址 (Secondary 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 56 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。

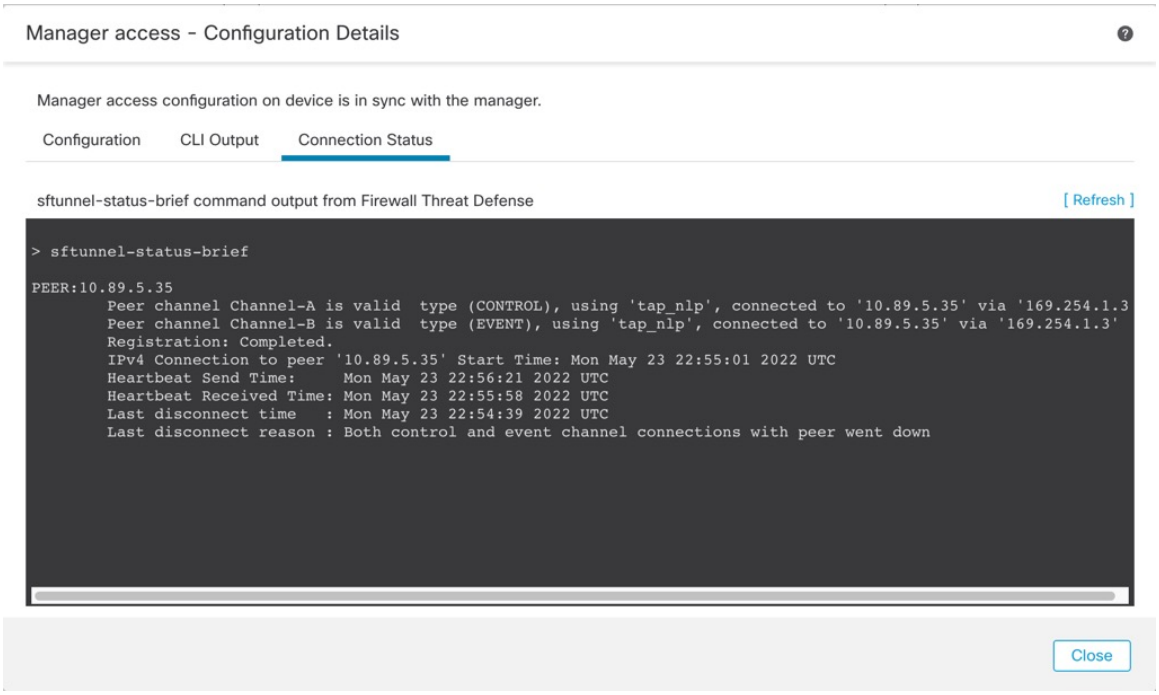
步骤 11 确保管理连接已重新建立。

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 *51:* 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 87 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 62 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。

开始之前

对于高可用性对，除非另有说明，否则请仅在主用设备上执行所有步骤。一旦配置更改被部署，备用设备会同步主用设备的配置和其他状态信息。

过程

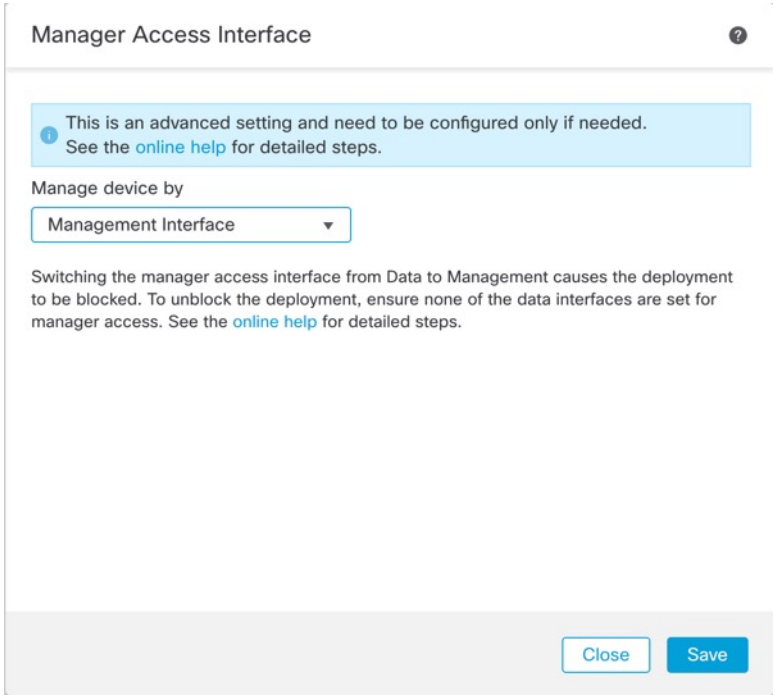
步骤 1 初始化接口迁移。

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 *52:* 管理器访问接口



c) 点击**保存 (Save)**。

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 *53:* 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。 对于高可用性，请在两台设备上执行此步骤。

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。 对于高可用性，请在两台设备上执行此步骤。

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**远程主机地址 (Remote Host Address)**IP 地址 (IP address) 并删除**辅助地址 (Secondary 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 56 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 87 页。

配置冗余管理器访问数据接口

在使用数据接口进行管理器访问时，您可以配置辅助数据接口，以便在主接口发生故障时接管管理功能。您只能配置一个辅助接口。设备会使用SLA监控来跟踪包含两个接口的静态路由和ECMP区域的可行性，以便管理流量可以使用这两个接口。

不支持高可用性。

开始之前

- 辅助接口需要与主接口位于不同的安全区域。
- 适用于辅助接口的所有要求与适用于主接口的要求相同。请参阅使用威胁防御数据接口进行管理，第4页。

过程

步骤1 在 **设备 (Devices)** > **设备管理 (Device Management)** 页面，然后点击设备的 **编辑**（ ）。

步骤2 启用对辅助接口的管理器访问。

此设置是标准接口设置（例如启用接口、设置名称、设置安全区域和设置静态IPv4地址）的补充。

a) 选择**接口 (Interfaces)** > **编辑物理接口 (Edit Physical Interface)** > **管理器访问 (Manager Access)**。

b) 选中**在此接口上为管理器启用管理 (Enable management on this interface for the Manager)**。

c) 点击**确定 (OK)**。

两个接口都会在列表中显示（**管理器访问**）。

图 ***54:*** 接口列表

Interface	Logical Name	Type	Security Zones
Diagnostic1/1	diagnostic	Physical	
Ethernet1/1 (Manager Access)	outside	Physical	outside
Ethernet1/2		Physical	
Ethernet1/3		Physical	
Ethernet1/4		Physical	
Ethernet1/5		Physical	
Ethernet1/6		Physical	
Ethernet1/7		Physical	
Ethernet1/8 (Manager Access)	redundant	Physical	mgmt

步骤3 将辅助地址添加到**管理 (Management)** 设置。

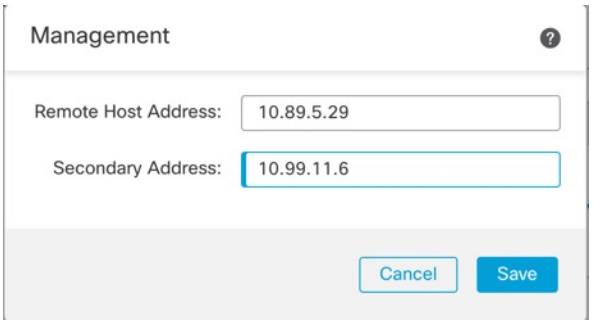
a) 点击**设备 (Devices)**，并查看**管理 (Management)** 区域。

b) 点击**编辑**（）。

图 *55:* 编辑管理地址

c) 在**管理 (Management)** 对话框中，在**辅助地址 (Secondary Address)** 字段中修改名称或 IP 地址

图 *56:* 管理 *IP* 地址

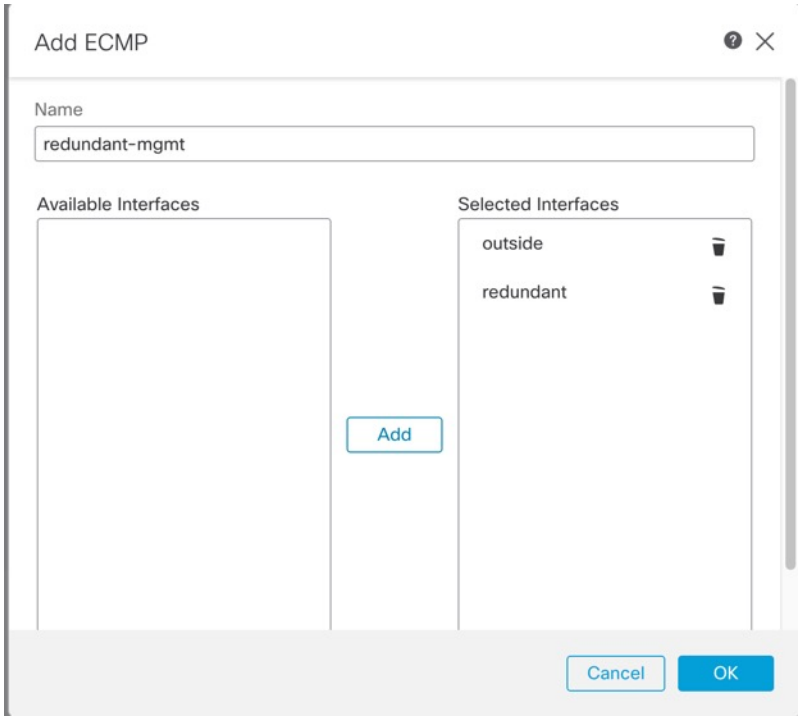


d) 点击**保存 (Save)**。

步骤 4 通过两个接口创建 ECMP 区域。

a) 点击**路由**。
b) 从虚拟路由器下拉列表中，选择主接口和辅助接口所在的虚拟路由器。
c) 点击 **ECMP**，然后点击**添加 (Add)**。
d) 为 ECMP 区域输入一个**名称**。
e) 在**可用接口 (Available Interfaces)** 框下选择主和辅助接口，然后点击**添加 (Add)**。

图 *57:* 添加 ***ECMP*** 区域

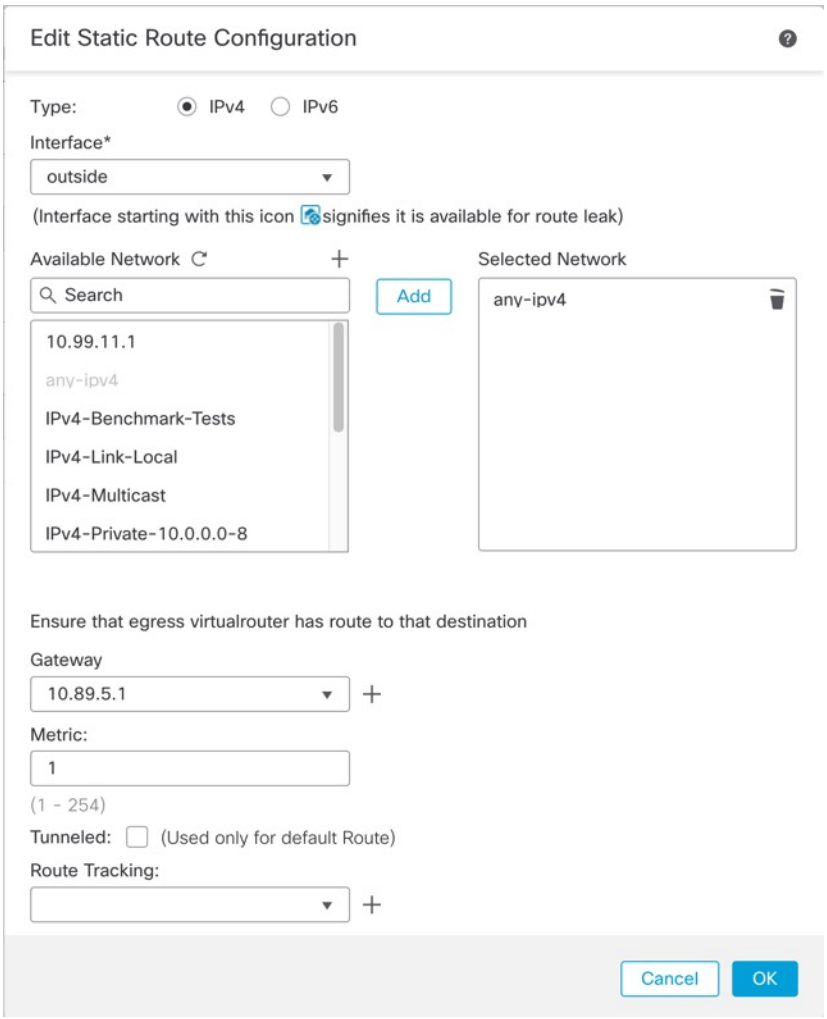


f) 点击**确定 (OK)**，然后点击**保存 (Save)**。

步骤 5 为两个接口添加等价默认静态路由，并在两个接口上启用 SLA 跟踪。

除网关外，路由应完全相同，并且都应具有指标 1。主接口应已具有您可以编辑的默认路由。

图 *58:* 添加/编辑静态路由

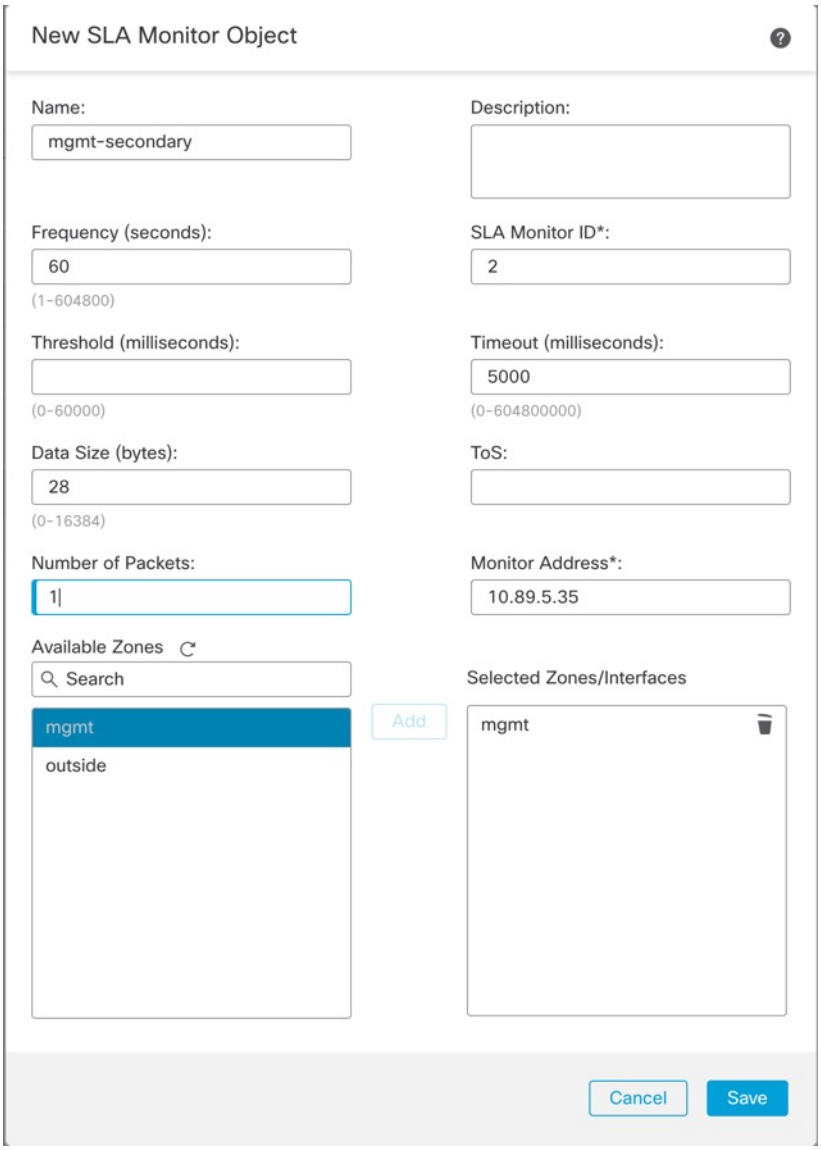


a) 点击**静态路由 (Static Route)**。
b) 点击**添加路由 (Add Route)** 以添加新路由，或点击现有路由的 **编辑**（）。
c) 从**接口 (Interface)** 下拉列表中选择接口。
d) 对于目标网络，从**可用网络 (Available Networks)** 框中选择 **any-ipv4**，然后点击**添加 (Add)**。
e) 输入默认**网关**。
f) 对于**路由跟踪 (Route Tracking)**，请点击 **添加**（）以添加新的 SLA 监控器对象。
g) 输入以下必需参数：

- 作为 管理中心 IP 地址的**监控地址**。
- **可用区域 (Available Zones)** 中的主要或辅助管理接口的区域；例如，为主接口对象选择外部区域，为辅助接口对象选择管理区域。

有关详细信息，请参阅SLA 监控器。

图 *59:* 添加 ***SLA*** 监控



h) 点击**保存 (Save)**，然后在**路由跟踪 (Route Tracking)** 下拉列表中选择您刚创建的 SLA 对象。

i) 点击**确定 (OK)**，然后点击**保存 (Save)**。

j) 对另一个管理接口的默认路由重复此操作。

步骤 6 部署配置更改；请参阅 部署配置更改。

作为此功能部署的一部分，管理中心 会为管理流量启用辅助接口，包括用于管理流量的自动生成的策略型路由配置，以到达正确的数据接口。管理中心 还会部署 **configure network management-data-interface** 命令的第二个实例。请注意，如果在 CLI 中编辑辅助接口，您将无法配置网关或以其他方式更改默认路由，因为只能在 管理中心 中编辑此接口的静态路由。

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。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

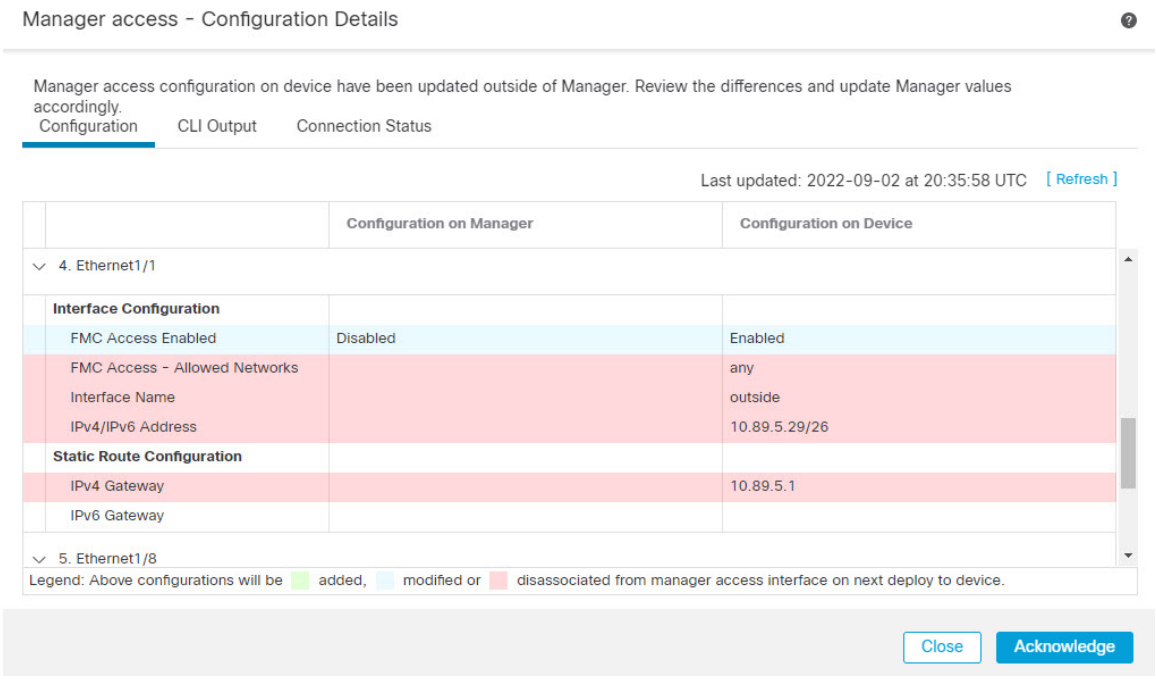
要删除阻止，您必须转到**管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** 对话框，然后点击**确认 (Acknowledge)**. 下次部署时，管理中心 配置将覆盖 威胁防御 上任何剩余的冲突设置。在您重新部署之前，您有责任在 管理中心 中手动修复配置。

请参阅此对话框中的以下页面。

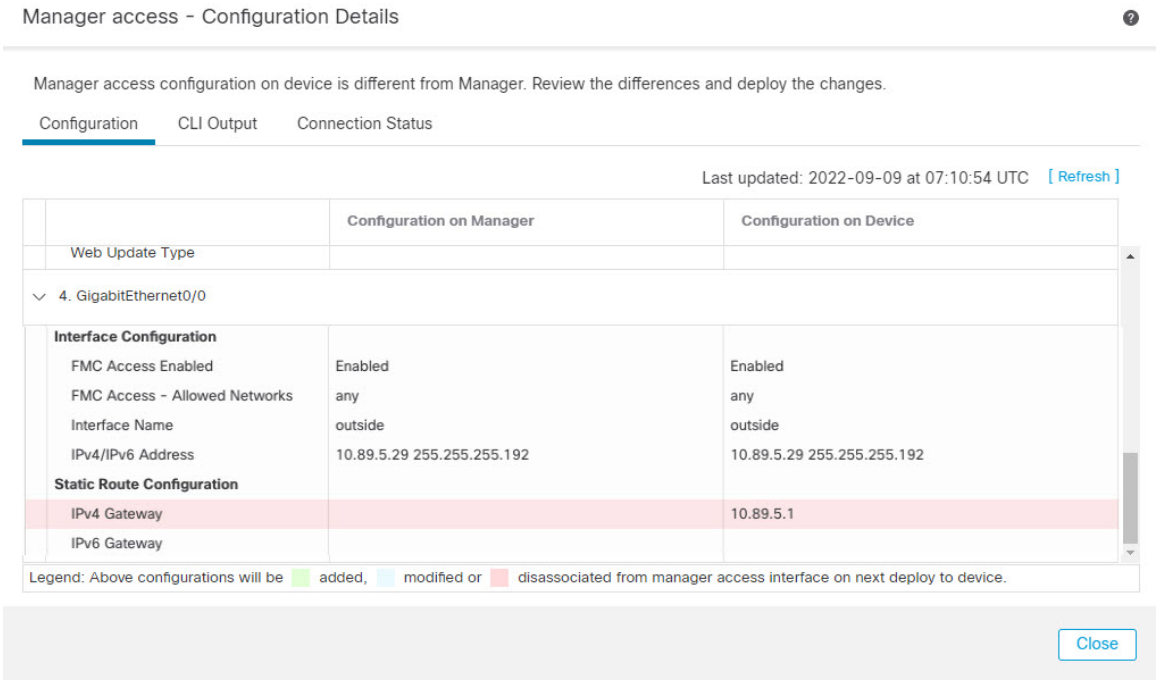
配置

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。



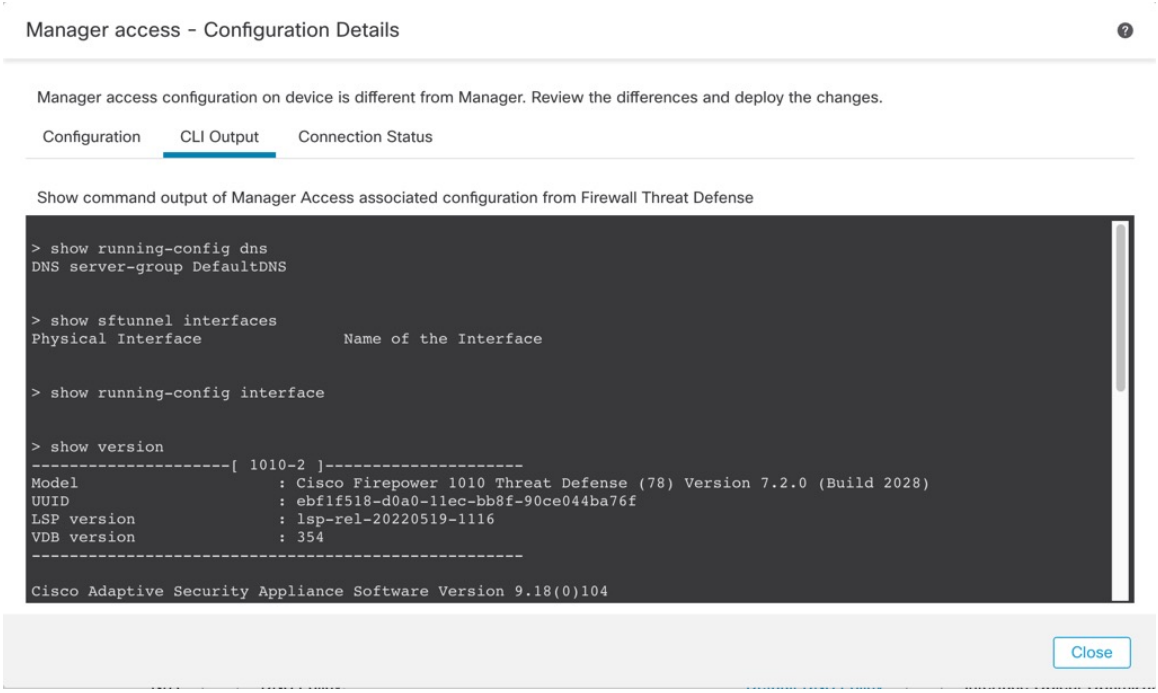
以下示例显示在 管理中心中配置接口后的此页面；接口设置匹配，并且已删除粉红色突出显示。



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。

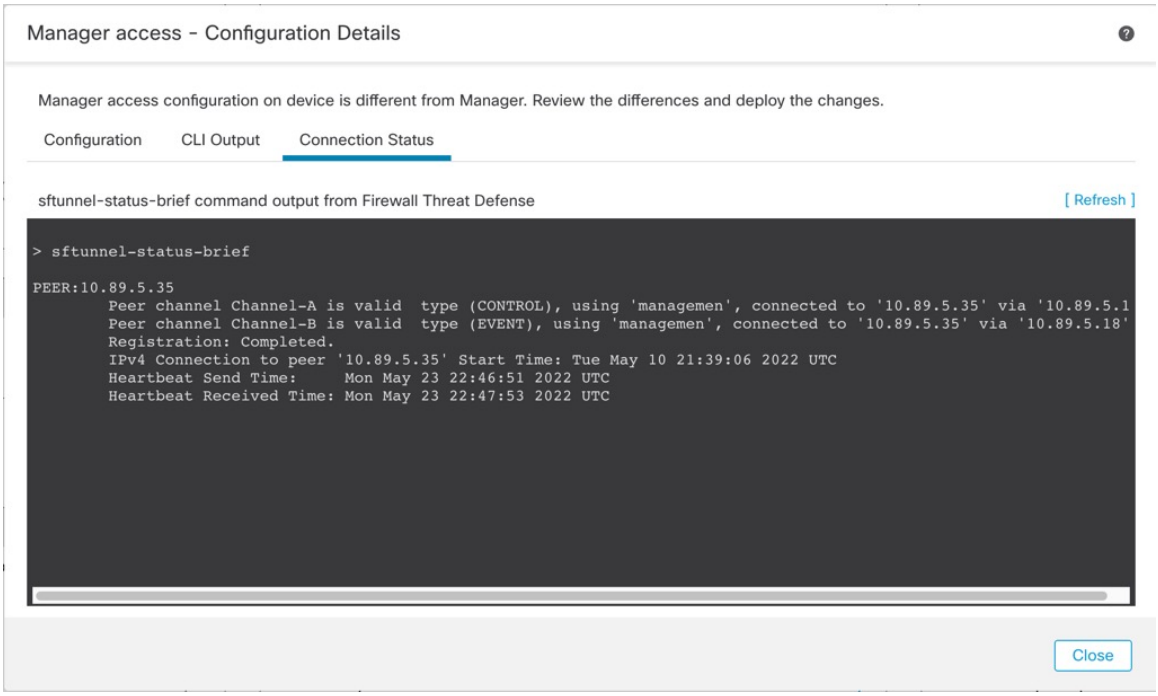
图 *60: CLI* 输出



连接状态

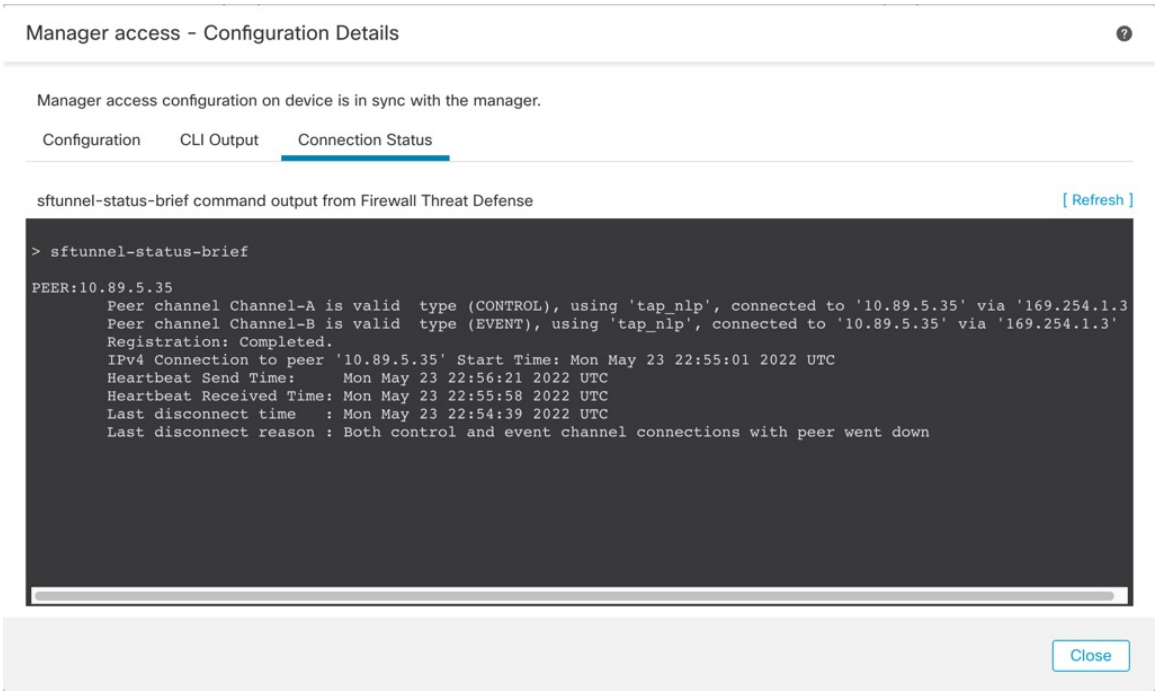
查看管理连接状态。以下示例显示了管理连接仍在使用管理“management0”接口。

图 *61:* 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 *62:* 连接状态



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 84 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 107 页）：

- **IP 地址—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 56 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 56 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 管理中心的设备管理页面上修改已注册设备的管理 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。

请参阅在设备上登录命令行界面，第 11 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/Cisco Secure Firewall 4200））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 *ipv6_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 *ipv6_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 *ipv6_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 79 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
```

管理中心和托管设备使用双向、TLS-1.3 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，是否需要进行代理身份验证，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 107 页）：

- **IP 地址—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 56 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 56 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 56 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 18 页中的 **configure network management-data-interface** 命令 。

对于高可用性对，在两台设备上执行所有 CLI 步骤。在 管理中心中，仅对主用设备执行以下步骤。一旦配置更改被部署，备用设备会同步主用设备的配置和其他状态信息。

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 78 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。

请参阅在设备上登录命令行界面，第 11 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 56 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 98 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 87 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，必须注意在 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                  : FTD-4
Domains                   : cisco.com
DNS Servers               : 72.163.47.11
DNS from router           : enabled
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces

==================[ management0 ]===================
Admin State               : enabled
Admin Speed               : 1gbps
Operation Speed           : 1gbps
Link                      : up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 68:87:C6:A6:54:80
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.89.5.4
Netmask                   : 255.255.255.192
Gateway                   : 169.254.1.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled
```

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

======[ System Information - Data Interfaces ]======
DNS Servers                 : 72.163.47.11
Interfaces                  : Ethernet1/1

==================[ Ethernet1/1 ]===================
State                       : Enabled
Link                        : Up
Name                        : outside
MTU                         : 1500
MAC Address                 : 68:87:C6:A6:54:A4
----------------------[ IPv4 ]----------------------
Configuration               : Manual
Address                     : 10.89.5.6
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 interface 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。

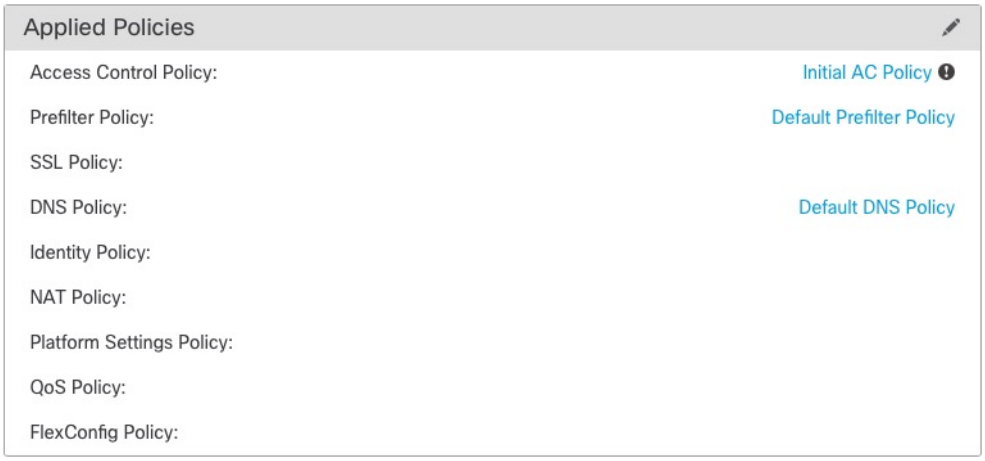
图 *63*: 设备清单详细信息

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 ***64:*** 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 *65:* 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

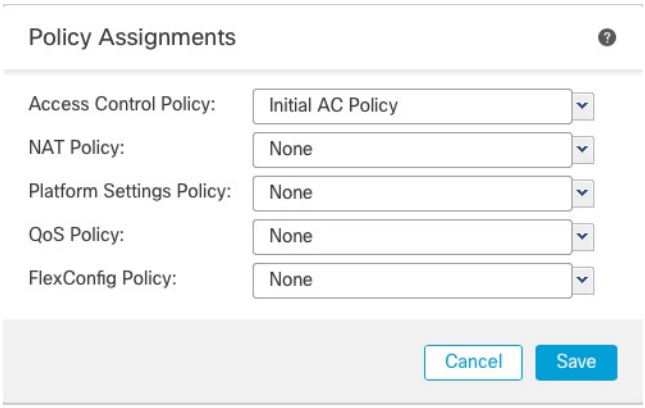
步骤 1 选择**设备** > **设备管理**。

步骤 2 在要为其分配策略的设备旁边，点击 **编辑**（）。

步骤 3 点击 **设备**。

步骤 4 在 **应用的策略** 部分中，点击 **编辑**（）。

图 *66:* 策略分配



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 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。

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）。
对象组搜索	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。 **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)**。
接口对象优化	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，则系统将转而为每个访问控制/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。

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 43 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：

威胁防御 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**（✎）。

步骤 3 点击**设备 (Device)**，然后点击**高级设置 (Advanced Settings)** 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。
- 可以使用 **object-group-search threshold** 命令启用阈值，以有助于防止性能下降。使用阈值运行时，对于每个连接，将根据网络对象匹配源和目标IP地址。如果将源地址匹配的对象数乘以目标地址匹配的对象数结果超过 10,000，则丢弃连接。配置规则以防止过多的匹配项。

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 点击保存 **(Save)**。

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，则系统将转而为每个访问控制/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。

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 点击保存 **(Save)**。

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 *67:* 部署设置

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 86 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

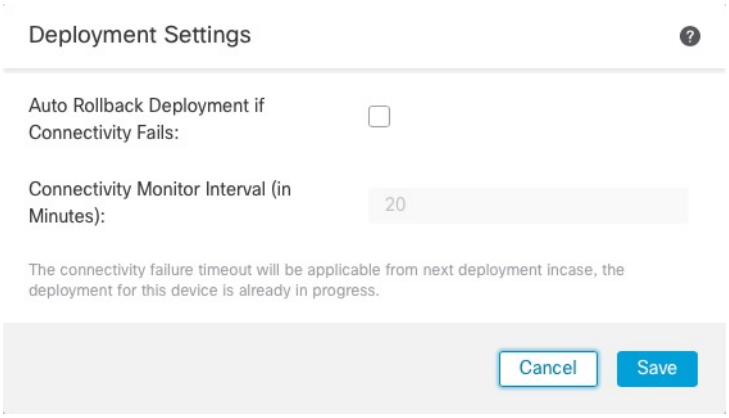
步骤 1 选择**设备** > **设备管理**。

步骤 2 在要为其分配策略的设备旁边，点击 **编辑**（）。

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 *68:* 部署设置



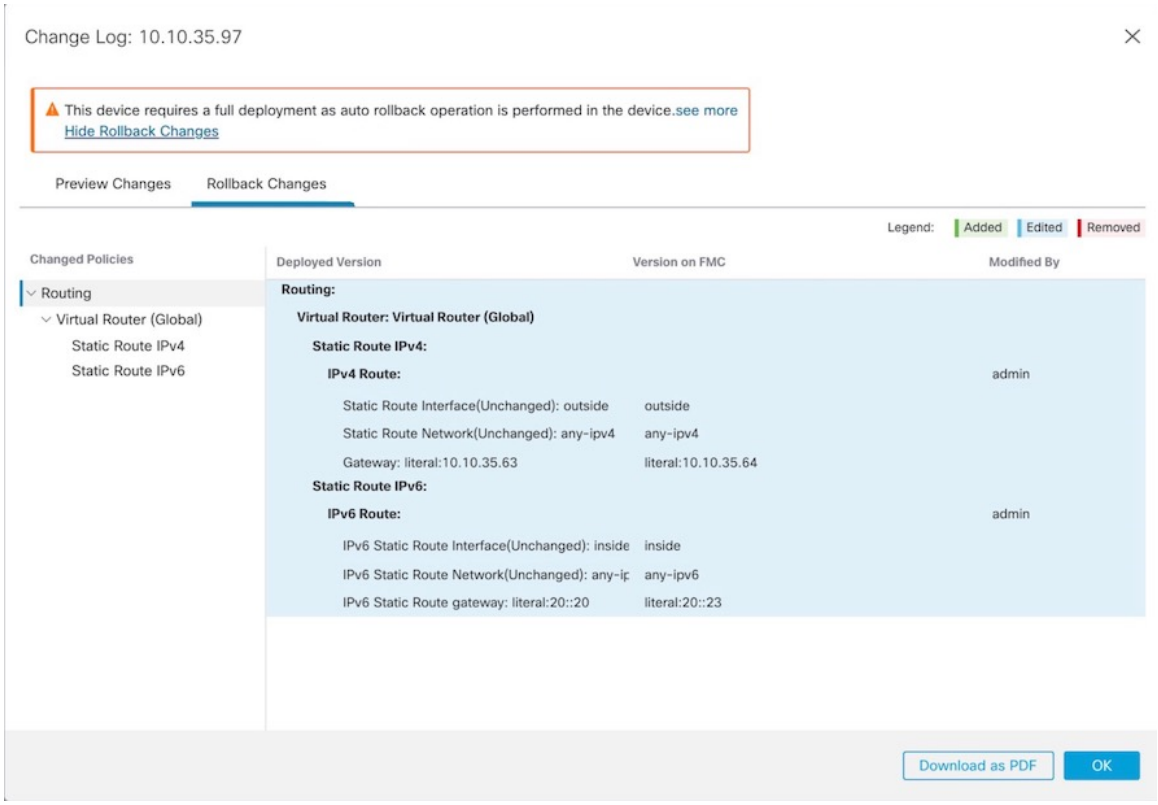
步骤 5 选中**连接失败时自动回滚部署 (Auto Rollback Deployment if Connectivity Fails)** 以启用自动回滚。

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)** > **高级部署 (Advanced Deploy)** 屏幕，然后点击**预览 (Preview)** (图标以查看已回滚的配置部分（请参阅部署配置更改）。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 *69:* 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。

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 87 页。

编辑集群运行状况监控设置

集群 (Cluster) 页面的**集群运行状况监控设置 (Cluster Health Monitor Settings)** 部分会显示下表所述信息。

图 *70:* 集群运行状况监控设置

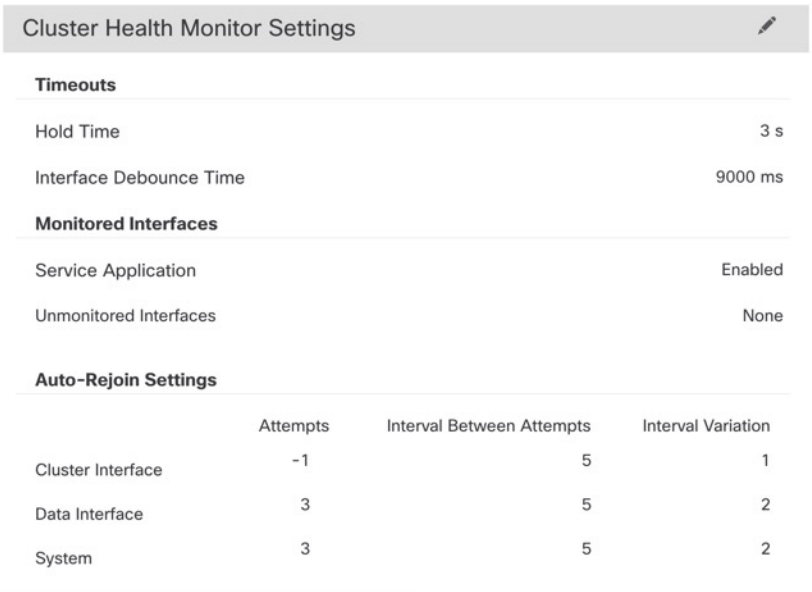


表 *8:* 集群运行状况监控设置部分表格字段

字段	说明
超时	
保持时间	0.3 到 45 秒之间；默认值为 3 秒。为了确定节点系统运行状况，集群节点会在集群控制链路上将 heartbeat 消息发送到其他节点。如果节点在保持期内未接收到来自对等节点的任何 heartbeat 消息，则对等节点被视为无响应或无法工作。
接口防退回时间	介于 300 和 9000 毫秒之间。默认值为 500 毫秒。接口防退回时间是节点将接口视为发生故障并将节点从集群中删除之前经过的时间。
受监控接口	接口运行状态检查将监控链路故障。如果特定逻辑接口的所有物理端口在特定节点上发生故障，但在其他节点上的同一逻辑接口下仍有活动端口，则会从集群中删除该节点。节点在多长时间后从集群中删除成员取决于接口的类型以及该节点是既定节点还是正在加入集群的设备。
服务应用	显示是否对 Snort 和磁盘已满进程进行监控。
不受监控的接口	显示不受监控的接口。
自动重新加入设置	
集群接口	显示集群控制链路故障的自动重新加入设置。
尝试次数	介于 1 和 65535 之间。默认值为 1（不受限制）。设置尝试重新加入的次数。

字段	说明
尝试之间的间隔	介于 2 和 60 之间。默认值为 5 分钟。定义两次重新加入尝试之间的间隔持续时间（以分钟为单位）。
间隔变化	介于 1 和 3 之间。默认值为间隔持续时间的 1 倍。定义是否增加每次尝试的间隔持续时间。
数据接口	显示数据接口故障的自动重新加入设置。
尝试次数	介于 1 和 65535 之间。默认值为 3。设置尝试重新加入的次数。
尝试之间的间隔	介于 2 和 60 之间。默认值为 5 分钟。定义两次重新加入尝试之间的间隔持续时间（以分钟为单位）。
间隔变化	介于 1 和 3 之间。默认值为间隔持续时间的 2 倍。定义是否增加每次尝试的间隔持续时间。
System	显示内部错误的自动重新加入设置。内部故障包括：应用程序同步超时、不一致的应用程序状态等。
尝试次数	介于 1 和 65535 之间。默认值为 3。设置尝试重新加入的次数。
尝试之间的间隔	介于 2 和 60 之间。默认值为 5 分钟。定义两次重新加入尝试之间的间隔持续时间（以分钟为单位）。
间隔变化	介于 1 和 3 之间。默认值为间隔持续时间的 2 倍。定义是否增加每次尝试的间隔持续时间。

注释 如果禁用系统运行状况检查，则在禁用系统运行状况检查时不适用的字段将不会显示。

您可以从此部分更改这些设置。

您可以监控任何端口通道 ID、单个物理接口 ID，以及 Snort 和磁盘已满进程。运行状况监控不在 VLAN 子接口或虚拟接口（例如，VNI 或 BVI）上执行。您不能为集群控制链路配置监控；它始终处于被监控状态。

过程

步骤 1 选择 **设备** > **设备管理**。

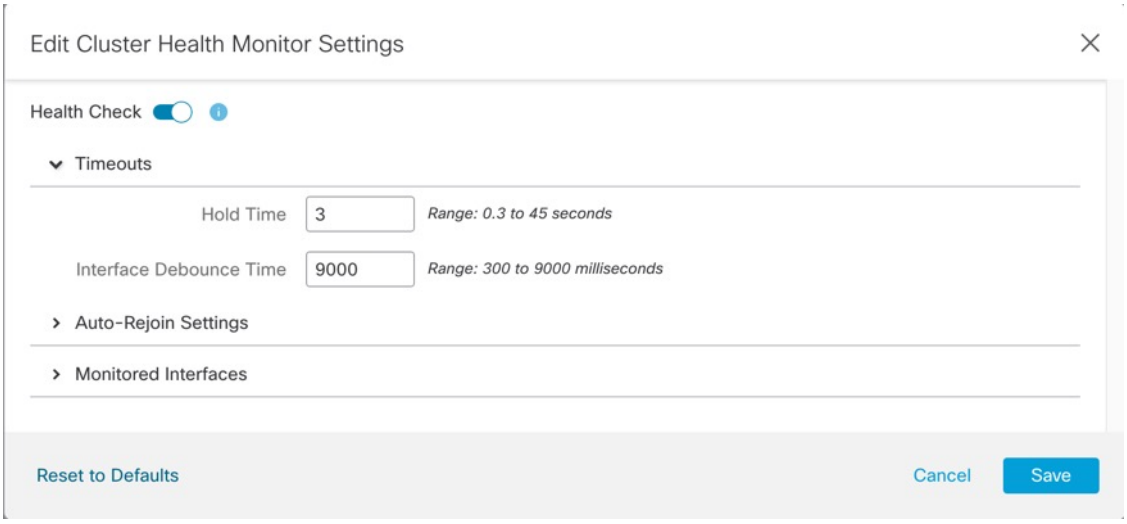
步骤 2 在要修改的集群旁边，点击 **编辑**（✎）。

步骤 3 点击**集群 (Cluster)**。

步骤 4 在**集群运行状况监控器设置 (Cluster Health Monitor Settings)** 部分，点击 **编辑**（✎）。

步骤 5 通过点击**运行状况检查 (Health Check)** 滑块禁用系统运行状况检查。

图 *71:* 禁用系统运行状况检查



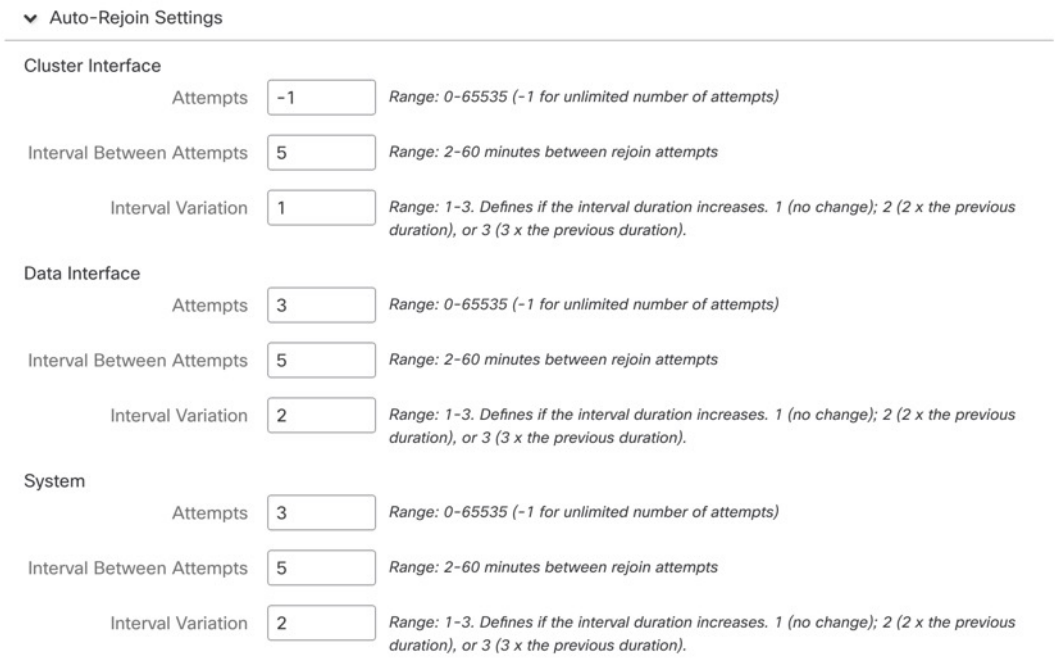
当拓扑发生任何更改时（例如添加或删除数据接口、启用或禁用节点、或交换机上的接口、或者添加额外的交换机形成 VSS 或 vPC），您应禁用系统运行状态检查功能，还要禁用对已禁用接口的接口监控。当拓扑结构更改完成且配置更改已同步到所有节点后，您可以重新启用系统运行状况检查功能和被监控的接口。

步骤 6 配置保持时间和接口防反跳时间。

- **保持时间 (Hold Time)** - 设置保持时间以确定两次节点心跳状态消息之间的时间间隔，其值介于 0.3 到 45 秒；默认值为 3 秒。
- **接口防反跳时间 (Interface Debounce Time)** - 将防反跳时间设置为 300 到 9000 毫秒之间。默认值为 500 毫秒。较小的值可以加快检测接口故障的速度。请注意，如果配置的防反跳时间较低，会增加误报几率。在发生接口状态更新时，节点会等待指定的毫秒数，然后才将接口标记为发生故障，并将节点从集群中删除。对于从故障状态转换为正常运行状态的 EtherChannel（例如，交换机重新加载或交换机启用 EtherChannel）而言，更长的防反跳时间可以防止集群节点上的接口仅仅因为另一个集群节点在绑定端口时的速度更快便显示为故障状态。

步骤 7 自定义在运行状况检查发生故障后的自动重新加入集群设置。

图 *72:* 配置自动重新加入设置

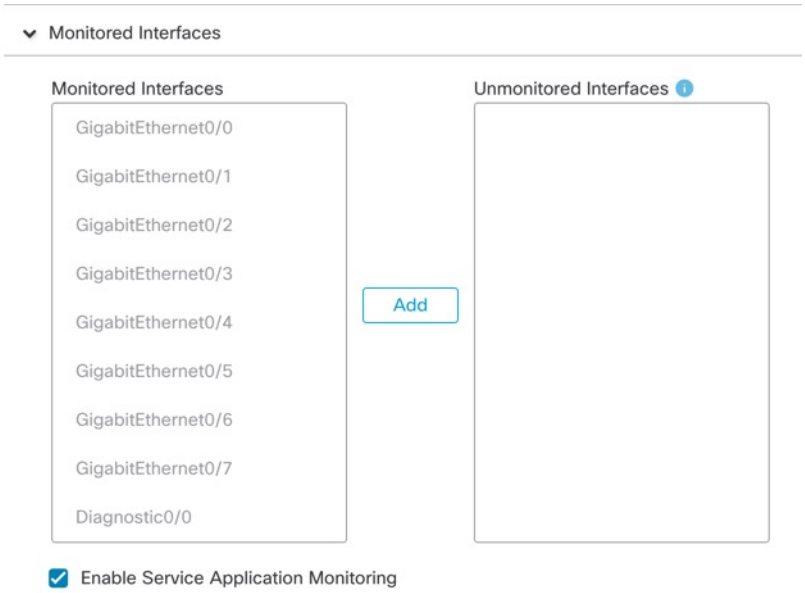


为**集群接口 (Cluster Interface)**、**数据接口 (Data Interface)** 和**系统 (System)** 设置以下值（内部故障包括：应用同步超时、应用状态不一致等）：

- **尝试次数 (Attempts)** - 设置重新加入尝试次数，介于 -1 和 65535 之间。**0** 将禁用自动重新加入。**集群接口 (Cluster Interface)** 的默认值为 -1（无限制）。**数据接口 (Data Interface)** 和**系统 (System)** 的默认值为 3。
- **尝试之间的间隔 (Interval Between Attempts)** - 定义两次重新加入尝试之间的间隔持续时间（以分钟为单位），介于 2 和 60 之间。默认值为 5 分钟。节点尝试重新加入集群的最大总时间限制为自上次失败之时起 14400 分钟（10 天）。
- **间隔变化 (Interval Variation)** - 定义是否增加间隔持续时间。设置介于 1 和 3 之间的值：**1**（无更改）；**2**（2 倍于上一次持续时间）或 **3**（3 倍于上一次持续时间）。例如，如果您将间隔持续时间设置为 5 分钟，并将变化设置为 2，则在 5 分钟后进行第 1 次尝试；在 10 分钟 (2 x 5) 后进行第 2 次尝试；在 20 分钟 (2 x 10) 后进行第 3 次尝试。**集群接口 (Cluster Interface)** 的默认值为 **1**，**数据接口 (Data Interface)** 和**系统 (System)** 的默认值为 **2**。

步骤 8 通过移动**受监控接口 (Monitored Interfaces)**或**不受监控接口 (Unmonitored Interfaces)** 窗口中的接口来配置受监控接口。您还可以选中或取消选中**启用服务应用监控 (Enable Service Application Monitoring)**，以启用或禁用对 Snort 和磁盘已满进程的监控。

图 *73:* 配置受监控的接口



接口运行状态检查将监控链路故障。如果特定逻辑接口的所有物理端口在特定节点上发生故障，但在其他节点上的同一逻辑接口下仍有活动端口，则会从集群中删除该节点。节点在多长时间后从集群中删除成员取决于接口的类型以及该节点是既定节点还是正在加入集群的设备。默认情况下，为所有接口以及 Snort 和磁盘已满进程启用运行状况检查。

您可能想禁用不重要的接口的运行状况检查。

当拓扑发生任何更改时（例如添加或删除数据接口、启用或禁用节点、或交换机上的接口、或者添加额外的交换机形成 VSS 或 vPC），您应禁用系统运行状态检查功能，还要禁用对已禁用接口的接口监控。当拓扑结构更改完成且配置更改已同步到所有节点后，您可以重新启用系统运行状况检查功能和被监控的接口。

步骤 9 点击**保存 (Save)**。

步骤 10 部署配置更改；请参阅 部署配置更改。

更改设备的管理设置

您可能需要更改管理器、更改管理器 IP 地址或执行其他管理任务。

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，请删除托管设备。请参阅删除（取消注册）设备，第 39 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。请参阅管理中心使用注册密钥将设备添加到 ， 第 27 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。

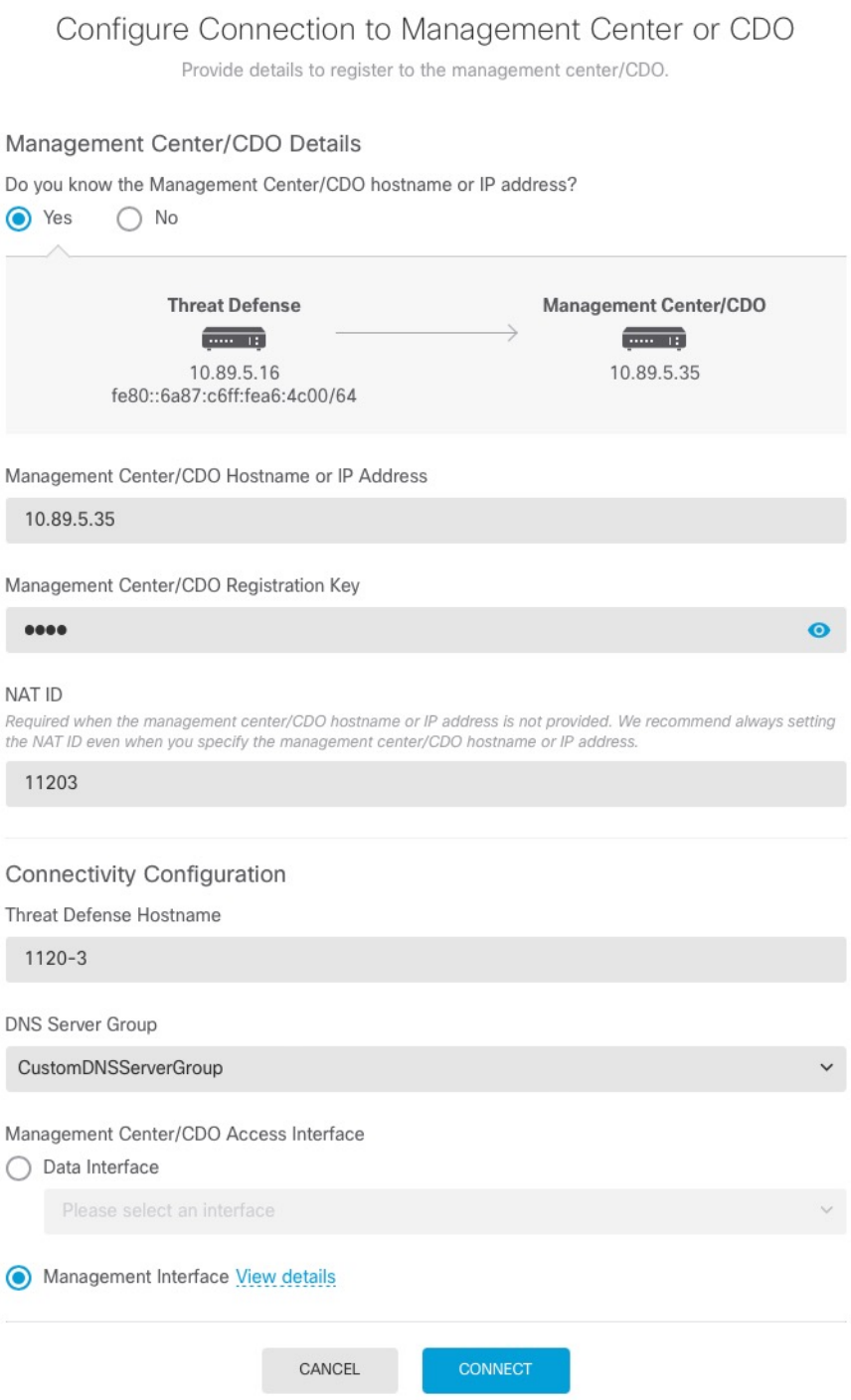
您可能需要更改管理接口配置，即使您打算使用数据接口访问管理器。如果您使用 设备管理器连接的管理接口，则必须重新连接到 设备管理器 。

- 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 *74:* 管理中心*/CDO* 详细信息



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 TLS-1.3 加密的通信通道。

b) 如果选择 **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。当您将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 CDO**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/)。

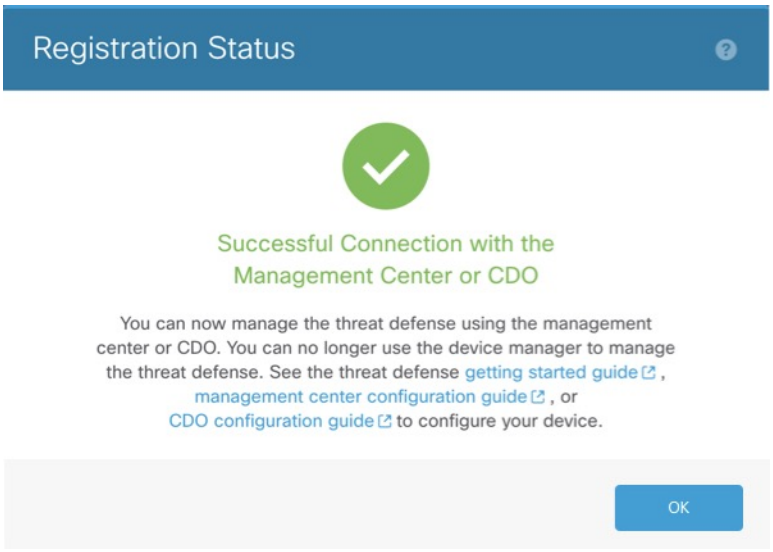
使用管理接口访问管理器时，不支持 DDNS。

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 *75:* 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 108 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，请执行以下操作之一：

- 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.
```

解决序列号（零接触调配）注册问题

如果设备无法使用序列号进行注册，则设备可能未成功连接到云。要确认云连接，请检查托管状态 LED 是否呈绿色闪烁。如果它没有呈绿色闪烁，则可能是由于以下原因导致的：

- 您在 CLI 或 设备管理器 中执行了初始配置，并禁用了低接触调配
- 序列号已被其他管理器申领

有关序列号注册的其他要求，请参阅使用序列号 (零接触调配) 将设备添加到管理中心，第 31 页。

要解决注册失败问题，请执行以下任务之一。

重置设备

在以下型号上支持：

- Firepower 1010
- Firepower 1100
- Cisco Secure Firewall 3100

如果您无权访问 CLI，并希望确保您的设备已取消配置并为 零接触调配做好准备，请按住凹进的小重置按钮五秒钟以上，将设备重置为默认状态。有关详细信息，请参阅硬件安装指南。

使用手动注册和注册密钥

如果低接触调配失败，完成注册的最简单方法是使用注册密钥方法。

1. 请参阅为手动注册完成威胁防御初始配置，第 12 页或使用设备管理器完成威胁防御初始配置，第 13 页。
2. 如果系统未显示初始设置任务，则可能是您的设备已成功注册到另一个 管理中心。您必须先删除管理连接，然后再向正确的管理器重新注册。

1. 首先，检查注册是否已完成：

```
> 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
```

2. 如果**注册 (Registration)** 显示**已完成 (Completed)**，则需要删除管理器：

   configure manager delete

3. 然后，您可以使用 **configure manager add**在 CLI 上注册设备。

在 CLI 中重新启动低接触调配

如果设备之前使用低接触调配进行了注册，则注册将失败，您将在CDO中看到**序列号已申领**错误。

您可以取消注册序列号，清除配置和任何现有管理连接，然后重新开始该过程。

1. 使用 SSH 或控制台端口连接到 FXOS CLI。

   如果使用 SSH，则连接到 威胁防御 CLI。在这种情况下，请输入 **connect fxos**。如果使用控制台端口，则直接连接到 FXOS。

```
> connect fxos
firepower#
```

2. 进入本地管理模式。

   connect local-mgmt

```
firepower# connect local-mgmt
firepower(local-mgmt)#
```

3. 从思科云取消注册设备。

   cloud deregister

```
firepower(local-mgmt)# cloud deregister
Release Image Detected RESULT=success MESSAGE=SUCCESS 10, X-Flow-Id:
2b3c9e8b-76c3-4764-91e4-cfd9828e73f9
```

4. 清除配置以恢复云连接。

   erase configuration

```
firepower(local-mgmt)# erase configuration
All configurations will be erased and system will reboot. Are you sure? (yes/no):yes
Removing all the configuration. Please wait....
Configurations are cleaned up. Rebooting....
```

5. 使用序列号 (零接触调配) 将设备添加到管理中心，第 31 页

使用 设备管理器 重新启动低接触调配

如果您登录 设备管理器，可能会意外禁用低接触调配。在这种情况下，您可以在 设备管理器 中重新启动低接触调配。

注释 如果序列号已被申领，请参阅在 CLI 中重新启动低接触调配，第 115 页。

1. 在 设备管理器 中，点击**设备 (Device)**，然后点击**系统设置 (System Settings)** > **云服务 (Cloud Services)**。
2. 选中**自动注册**Cisco Defense Orchestrator或 **Cisco Secure Firewall Management Center**。
3. 点击**注册**。
4. 使用序列号 (零接触调配) 将设备添加到管理中心，第 31 页

Cisco Secure Firewall 3100/4200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。

将配置迁移到新型号

通过防火墙威胁防御型号迁移向导，您可以将配置从旧的威胁防御型号迁移到新型号。您可以将源设备接口映射到目标设备接口。在迁移之前，源设备和目标设备已锁定。

支持进行迁移的设备

支持的源设备

- Cisco Firepower 1120
- Cisco Firepower 1140
- Cisco Firepower 1150
- Cisco Firepower 2110
- 思科 Firepower 2120
- 思科 Firepower 2130

- 思科 Firepower 2140

注释 源设备必须为 7.0 或更高版本。

支持的目标设备

- Cisco Secure Firewall 3105
- Cisco Secure 防火墙 3110
- Cisco Secure Firewall 3120
- Cisco Secure Firewall 3130
- Cisco Secure Firewall 3140

注释 Cisco Secure Firewall 3110、3120、3130 和 3140 设备必须为 7.1 或更高版本。Cisco Secure Firewall 3105 必须为 7.3 或更高版本。

迁移许可证

您必须使用智能许可帐户注册和注册设备。迁移会将源设备许可证复制到目标设备。

迁移的前提条件

- 您必须将源设备和目标设备注册到管理中心。
- 您的智能许可帐户必须具有目标设备的许可证授权。
- 我们建议目标设备是没有任何配置的新注册设备。
- 源设备和目标设备必须处于同一：
  - 域
  - 防火墙模式：路由或透明
  - 合规模式
- 目标设备不得：
  - 在多实例模式下
  - 是集群的一部分
- 用户必须在设备上具有修改权限。

- 源设备上的配置必须有效且没有错误。
- 源设备可以有待处理的部署。但在迁移期间，不得在任何设备上运行部署、导入或导出任务。
- 如果源设备是 HA 对的一部分，目标设备不需要是 HA 对的一部分，反之亦然。迁移不会形成或破坏 HA 对。

向导可以迁移哪些配置？

迁移向导会将以下配置从源设备复制到目标设备：

- 许可证
- 接口配置
- 内联集配置
- 路由配置
- DHCP 和 DDNS 配置
- 虚拟路由器配置
- Policies
- 关联的对象和对象覆盖
- 平台设置
- 远程分支机构部署配置

迁移向导会将以下策略配置从源设备复制到目标设备：

- 运行状况策略
- NAT 策略
- QoS 策略
- 远程访问 VPN 策略
- FlexConfig 策略
- 访问控制策略
- 预过滤策略
- IPS 策略
- DNS 策略
- SSL 策略
- 恶意软件和文件策略

- 身份策略

迁移向导会将以下路由配置从源设备复制到目标设备：

- ECMP
- BFD
- OSPFv2/v3
- EIGRP
- RIP
- BGP
- 基于策略的路由
- Static Route
- 组播路由
- 虚拟路由器

迁移向导会将以下接口从源设备复制到目标设备：

- 物理接口
- 子接口
- Etherchannel 接口
- 网桥组接口
- VTI 接口
- VNI 接口
- 环回接口

迁移的限制

- 向导不会迁移：
  - 站点间 VPN
  - SNMP 配置

    在迁移后，您可以使用设备的平台设置来配置 SNMP。
- 一次只能执行一个迁移。
- 如果源接口的速度、自动协商和双工设置对于目标设备的映射接口有效，则会复制这些值。否则，这些参数将被设置为默认值。

- 远程访问 VPN 信任点证书不会被注册。您必须在部署之前手动注册这些证书。
- 在迁移后，默认情况下，目标设备会使用 Snort 3 而不是 Snort 2，即使源设备使用的是 Snort 2。
- 对于 HA 设备：
  - 目标设备：您不能映射属于故障转移配置的接口。这些接口会在向导中被禁用。
  - 源和目标设备：被监控的接口、故障转移触发条件和接口 MAC 地址等 HA 配置不会被向导迁移。如果需要，您必须在迁移后手动配置这些参数。

迁移 Cisco Secure Firewall Threat Defense

开始之前

查看迁移的前提条件和限制。

过程

步骤 1 选择**设备 > 设备管理**。

步骤 2 点击页面右上角的**迁移 (Migrate)**。

步骤 3 点击欢迎屏幕上的**开始 (Start)**。

步骤 4 从**源设备 (Source Device)** 下拉列表中选择设备。

如果设备是 HA 对的一部分，则仅显示 HA 对的容器名称。

步骤 5 点击**下一步**。

步骤 6 从**源设备 (Source Device)** 下拉列表中选择设备。

如果设备是 HA 对的一部分，则仅显示 HA 对的容器名称。

步骤 7 点击**下一步**。

步骤 8 在**配置接口 (Configure Interfaces)** 步骤中，将源设备的物理接口映射到目标设备的物理接口。

并非强制映射所有接口。您必须映射所有已命名的接口和属于其他接口的接口。您不能映射属于 HA 故障转移配置的接口。这些接口会在向导中被禁用。向导会根据用户提供的接口映射来创建逻辑接口。

- 点击**映射默认值 (Map Default)** 以配置默认的接口映射。

  例如，源设备中的以太网接口 1/1 会被映射到目标设备中的以太网接口 1/1。

- 点击**全部清除 (Clear All)** 可清除所有映射。

步骤 9 点击**下一步**。

步骤 10 点击**查看映射 (View Mappings)** 以验证接口映射。

步骤 11 点击**提交 (Submit)** 开始迁移。

步骤 12 在通知 (Notifications) > 任务 (Tasks) 页面中查看迁移状态。

下一步做什么

在成功迁移后，您可以部署设备。

部署并非强制性的，您可以验证配置并根据需要进行部署。但是，在部署之前，请确保执行 迁移最佳实践，第 123 页中提到的操作。

迁移最佳实践

成功迁移后，我们建议您在部署之前执行以下操作：

- 如果源设备处于活动状态，请更改接口的 IP 地址，因为它们会从源设备复制到目标设备。
- 确保使用修改后的 IP 地址来更新 NAT 策略。
- 如果在迁移后将接口速度设置为默认值，请配置接口速度。
- 在目标设备上重新注册设备证书（如有）。
- 如果您有 HA 设置，请配置 HA 参数，例如被监控的接口、故障转移触发条件和接口 MAC 地址。
- 配置迁移后重置的诊断接口。
- （可选）使用设备的平台设置来配置 SNMP。
- （可选）配置远程分支机构部署配置。

  如果源或目标设备具有通过数据接口的管理器访问权限，则在迁移后，管理器访问权限将丢失。更新目标设备上的管理器访问配置。有关详细信息，请参阅 *Cisco Secure Firewall Management Center* 设备配置指南 或联机帮助中的将管理器访问接口从“管理”更改为“数据 ”主题。
- （可选）根据需要配置站点间 VPN。这些配置不会从源设备迁移。
- 在部署之前查看部署预览。选择 **部署 > 高级部署**，然后点击设备的 **预览** （ ） 图标。

设备管理的历史记录基础知识

功能	最低 管理中心	最低 威胁防御	详细信息
Firepower 4100/9300 的机箱级运行状况警报。	7.4.1	7.4.1	**升级影响。升级后启用新的运行状况模块并应用设备运行状况策略。** 现在，只要将机箱作为只读设备注册到管理中心，您就可以查看Firepower 4100/9300 的机箱级运行状况警报。您还必须启用防火墙威胁防御平台故障运行状况模块并应用运行状况策略。警报会出现在信息中心、运行状况监控器（在左窗格的“设备”(Devices)下选择机箱）和运行状况事件视图中。 您还可以在多实例模式下为 Cisco Secure Firewall 3100 添加机箱（并查看运行状况警报）。对于这些设备，您可以使用管理中心来管理机箱。但对于 Firepower 4100/9300 机箱，您仍必须使用机箱管理器或 FXOS CLI。 新增/修改的屏幕：**设备 (Devices)** > **设备管理 (Device Management)** > **添加 (Add)** > **机箱 (Chassis)** 请参阅：将机箱添加到管理中心
查看设备或设备集群的 CLI 输出。	7.4.1	任意	您可以查看一组预定义的 CLI 输出，帮助您排除设备或集群的故障。您还可以输入任何 **show** 命令并查看输出。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** > **常规 (General)**
故障排除文件生成和下载可从“设备”(Device) 和“集群”(Cluster) 页面获取。	7.4.1	7.4.1	您可以在“设备”(Device) 页面上为每个设备以及在“集群”(Cluster) 页面上为所有集群节点生成和下载故障排除文件。对于集群，您可以将所有文件下载为一个压缩文件。您还可以为集群节点添加集群的集群日志。您也可以从**设备 (Devices)** > **设备管理 (Device Management)** > **更多**（⋮） > **故障排除文件 (Troubleshoot Files)** 菜单中触发文件生成。 新增/修改的菜单项： • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **常规 (General)** • **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** > **常规 (General)**

功能	最低 管理中心	最低 威胁防御	详细信息
使用序列号将设备注册 Firepower 1000/2100 和 Cisco Secure Firewall 3100 到管理中心的零接触调配。	7.4.0	管理中心可公开访问：7.2.0 管理中心不可公开访问：7.2.4/7.4.0	通过零接触调配（也称为低接触调配），您可以按序列号将 Firepower 1000/2100 和 Cisco Secure Firewall 3100 设备注册到管理中心，而无需在设备上执行任何初始设置。管理中心与 SecureX 和思科防御协调器集成以实现此功能。 新增/修改的屏幕：**设备 (Devices)** > **设备管理 (Device Management)** > **添加 (Add)** > **设备 (Device)** > **序列号 (Serial Number)** 其他版本限制：当管理中心无法公开访问时，7.3.x 或 7.4.0 版威胁防御设备不支持此功能。支持在版本 7.4.1 中返回。
合并的管理接口和诊断接口。	7.4.0	7.4.0	**升级影响。升级后合并接口。** 对于使用 7.4 及更高版本的新设备，您不能使用旧诊断接口。仅合并的管理接口可用。 如果您已升级到 7.4 或更高版本，并且： • 您没有为诊断接口进行任何配置，则接口将自动合并。 • 您已为诊断接口进行了配置，则可以选择手动合并接口，也可以继续使用单独的诊断接口。请注意，在更高版本中将删除对诊断接口的支持，因此您应计划尽快合并接口。 合并模式还会将 AAA 流量的行为更改为默认使用数据路由表。现在，只有在配置中指定管理专用接口（包括管理接口）时，才可以使用管理专用路由表。 对于平台设置，这意味着： • 您无法再启用 HTTP、ICMP 或 SMTP 进行诊断。 • 对于 SNMP，可以允许“管理”而不是“诊断”上的主机。 • 对于系统日志服务器，您可以通过“管理”而不是“诊断”来访问它们。 • 如果系统日志服务器或 SNMP 主机的平台设置按名称指定诊断接口，则必须为合并设备和非合并设备使用单独的平台设置策略。 • 如果不指定接口，DNS 查找不会再回退到管理专用路由表。 新增/修改的屏幕：**设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** 新增/经修改的命令： **show management-interface convergence**

功能	最低 管理中心	最低 威胁防御	详细信息
从 Firepower 1000/2100 迁移到 Cisco Secure Firewall 3100。	7.4.0	任意	您现在可以将配置从 Firepower 1000/2100 轻松迁移到 Cisco Secure Firewall 3100。 新增/修改的屏幕：**设备 (Devices)** > **设备管理 (Device Management)** > **迁移 (Migrate)** 平台限制：不支持从 Firepower 1010 或 1010E 迁移。
下载所有已注册设备的报告。	7.4.0	任意	现在您可以下载所有已注册设备的报告。在**设备 (Devices)** > **设备管理 (Device Management)**中，点击页面右上角新的**下载设备列表报告 (Download Device List Report)** 链接。
使用数据接口管理威胁防御高可用性对。	7.4.0	7.4.0	威胁防御高可用性现在支持使用常规数据接口与管理中心通信。以前，只有独立设备才支持这一功能。 请参阅：使用威胁防御数据接口进行管理
集群运行状况监控设置。	7.3.0	任意	您现在可以编辑集群运行状况监控设置。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** > **集群运行状况监控设置 (Cluster Health Monitor Settings)** **注释** 如果您之前使用 FlexConfig 配置了这些设置，务必要在部署之前删除 FlexConfig 配置。否则，FlexConfig 配置将覆盖管理中心配置。
冗余管理器访问数据接口。	7.3.0	7.3.0	在使用数据接口进行管理器访问时，您可以配置辅助数据接口，以便在主接口发生故障时接管管理功能。设备会使用 SLA 监控来跟踪包含两个接口的静态路由和 ECMP 区域的可行性，以便管理流量可以使用这两个接口。 新增/修改的菜单项： • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **管理 (Management)** • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **接口 (Interfaces)** > **管理器访问 (Manager Access)**
ISA 3000 系统 LED 支持关闭。	7.0.5/7.3.0	7.0.5/7.3.0	关闭 ISA 3000 时，系统 LED 会熄灭。至少等待 10 秒，然后再断开电源。
ISA 3000 支持关闭。	7.0.2/7.2.0	7.0.2/7.2.0	您现在可以关闭 ISA 3000；以前，您只能重新启动设备。
策略支持回滚以实现高可用性设备。	7.2.0	7.2.0	**configure policy rollback** 命令支持高可用性设备。

功能	最低 管理中心	最低 威胁防御	详细信息
多管理器支持	7.2.0	7.2.0	我们引入了云交付的管理中心。云交付的管理中心使用 Cisco Defense Orchestrator (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。 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。 新增/修改的命令： **configure manager add**, **configure manager delete**, **configure manager edit**, **show managers** 新增/修改的屏幕： • 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** 复选框将其指定为仅用于分析。 • 在 **设备** > **设备管理**中查看哪些设备仅用于分析。 有关详细信息，请参阅 CDO文档。
默认情况下会为访问控制规则启用对象组搜索。	7.2.0	7.2.0	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”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。	7.2.0	7.2.0	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。以前，您只能使用 **configure policy rollback** 命令手动回滚配置。 新增/修改的菜单项： • **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。	7.1.0	7.1.0	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**
管理连接支持 TLS 1.3。	7.1.0	7.1.0	FMC 设备管理连接现在使用 TLS 1.3。以前支持 TLS 1.2。

功能	最低 管理中心	最低 威胁防御	详细信息
导入和导出设备配置。	7.1.0	7.1.0	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： • 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** > **设备管理** > **设备** > **常规**
使用 FDM 将 FTD 配置为由 FMC 进行管理。	7.1.0	7.1.0	如果使用 FDM 执行初始设置，那么在切换到 FMC 进行管理时，除管理和 FMC 访问设置外，会保留在 FDM 中完成的所有接口配置。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 FMC 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 FMC 后，您将无法再使用 FDM 管理 FTD。 新增/修改 FDM 屏幕：**系统设置 (System Settings)** > **管理中心 (Management Center)**
按升级状态过滤设备。	6.7.0	6.7.0	**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)**
更新 FTD 上的 FMC IP 地址。	6.7.0	6.7.0	如果更改 FMC IP 地址，现在可以使用 FTD CLI 更新设备。 新增/经修改的命令： **configure manager edit**
一键访问 Firepower 机箱管理器。	6.4.0	6.4.0	对于 Firepower 4100/9300 系列设备，“设备管理”(Device Management) 页面会提供指向 Firepower 机箱管理器 Web 界面的链接。 新增/修改的屏幕：**设备 (Devices)** > **设备管理 (Device Management)**
按运行状况和部署状态过滤设备；查看版本信息。	6.2.3	6.2.3	“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。 新增/修改的屏幕：**设备 (Devices)** > **设备管理 (Device Management)**

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。