部署 Firepower 威胁防御与 FDM

本章对您适用吗？

本章介绍如何部署使用 Firepower 设备管理器 (FDM) 的独立式 FTD 逻辑设备。要部署高可用性对，请参阅 FDM 配置指南。

FDM可以配置小型网络最常用软件的基本功能。此产品专为包括一台或几台设备的网络而设计，在这种网络中，无需使用高功率多设备管理器来控制包含许多 FDM设备的大型网络。

如果要管理大量设备或要使用FTD支持的更复杂的功能和配置，则使用Firepower管理中心(FMC)。

注释

隐私收集声明 - Firepower 9300 不要求或主动收集个人身份信息。不过，您可以在配置中使用个人身份信息，例如用于用户名。在这种情况下，管理员在执行配置或使用 SNMP 时可能会看到此信息。

关于 Firepower 威胁防御与 FDM

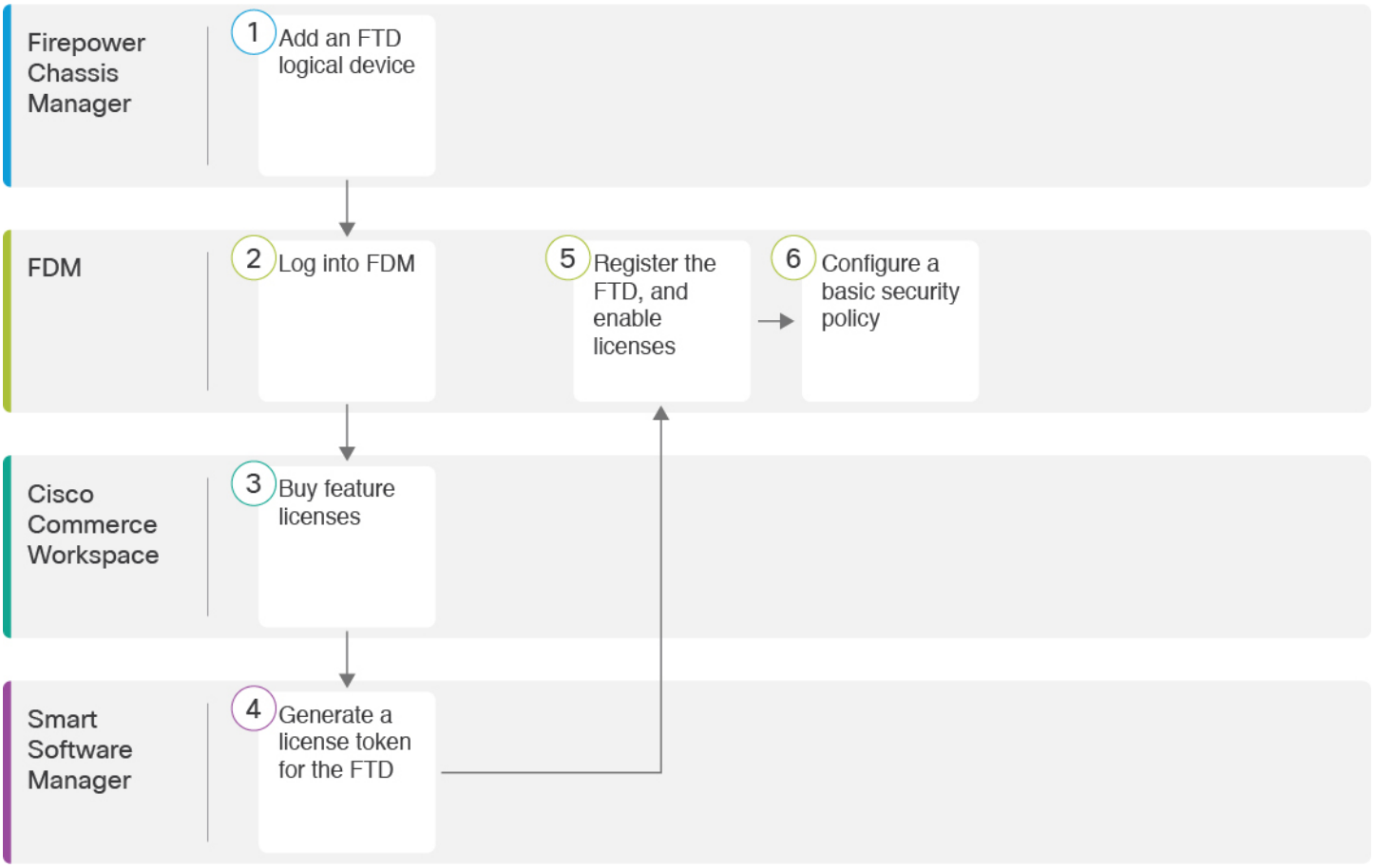
FTD 提供各种下一代防火墙服务，包括状态防火墙、路由、下一代入侵防御系统 (NGIPS)、应用可视性与可控性 (AVC)、URL 过滤，以及高级恶意软件防护 (AMP)。

可以使用 Firepower 设备管理器 (FDM)（设备上的一个简化的设备管理器）管理 FTD。将 HTTPS 用于分配给 FTD 逻辑设备的管理接口。

要进行故障排除，您可以使用管理接口上的 SSH 访问 FTD CLI，也可以从 FXOS CLI 连接到 FTD。

端到端程序

请参阅以下任务以在机箱上部署和配置 FTD。



	工作空间	步骤
1	Firepower 机箱管理器	Firepower 机箱管理器：添加 Firepower 威胁防御逻辑设备， 第 3 页。
2	FDM	登录 FDM， 第 7 页。
3	思科商务工作空间	配置许可， 第 7 页：购买功能许可证。
4	智能软件管理器	配置许可， 第 7 页：为 FTD 生成许可证令牌。
5	FDM	配置许可， 第 7 页：向智能许可服务器注册 FTD，并启用功能许可证。

	工作空间	步骤
6	FDM	配置基本安全策略，第 14 页。

Firepower 机箱管理器：添加 Firepower 威胁防御逻辑设备

可以从 Firepower 9300 将 FTD 部署为本地实例。不支持容器实例。

要添加高可用性对，请参阅 FDM 配置指南。

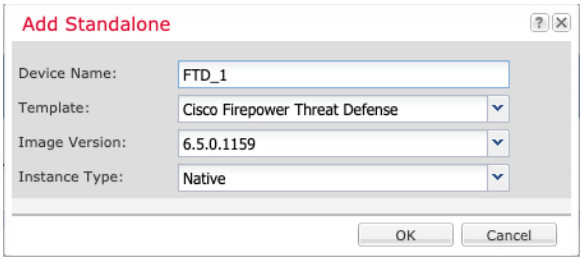
开始之前

- 配置与 FTD一起使用的管理接口；请参阅配置接口。管理接口是必需的。请注意，此管理接口与仅用于机箱管理的机箱管理端口（并且该端口在**接口**选项卡的顶部显示为 **MGMT**）不同。
- 您还必须至少配置一个数据接口。
- 收集以下信息：
  - 此设备的接口 ID
  - 管理接口 IP 地址和网络掩码
  - 网关 IP 地址
  - DNS 服务器 IP 地址
  - FTD 主机名和域名

过程

步骤 1 在 Firepower 机箱管理器中，选择**逻辑设备**。

步骤 2 点击**添加** > **独立设备**，并设置以下参数：



a) 提供**设备名称**。

此名称由机箱管理引擎用于配置管理设置和分配接口；它不是在应用配置中使用的设备名称。

b) 对于**模板 (Template)**，请选择**思科 Firepower 威胁防御 (Cisco Firepower Threat Defense)**。

c) 选择**映像版本**。

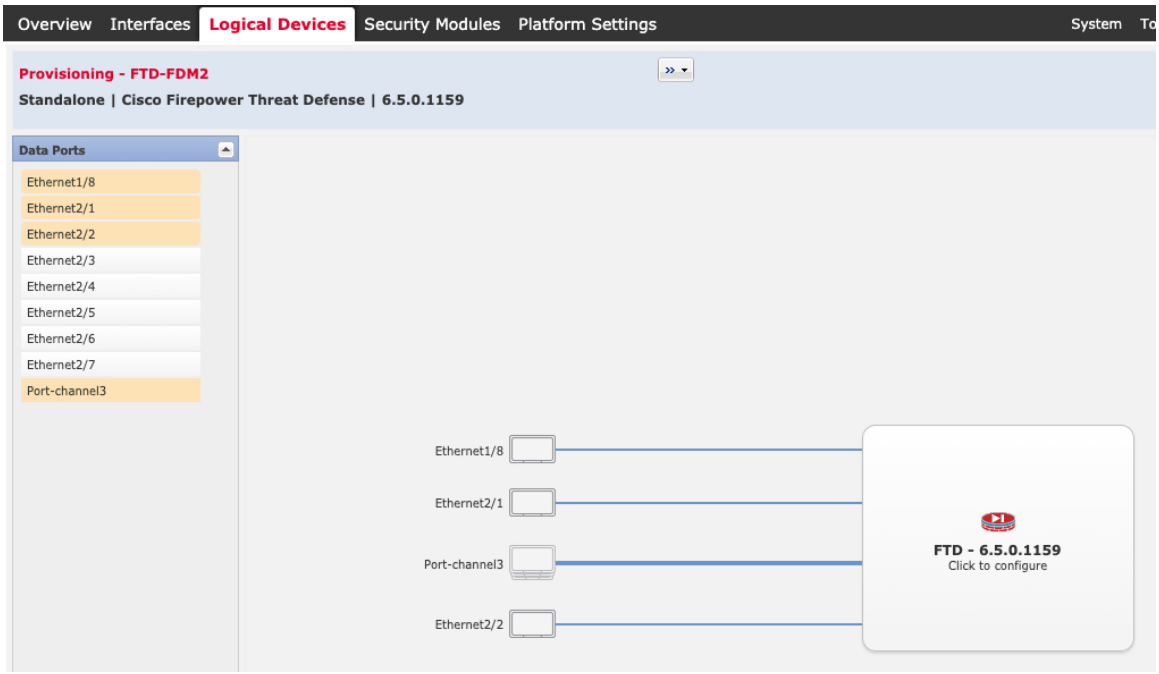
d) 选择**实例类型：本地**。

FDM 不支持容器实例。

e) 点击**确定**。

屏幕会显示调配 - 设备名称 *(Provisioning - device name)* 窗口。

步骤 3 展开**数据端口**区域，然后点击要分配给设备的每个接口。

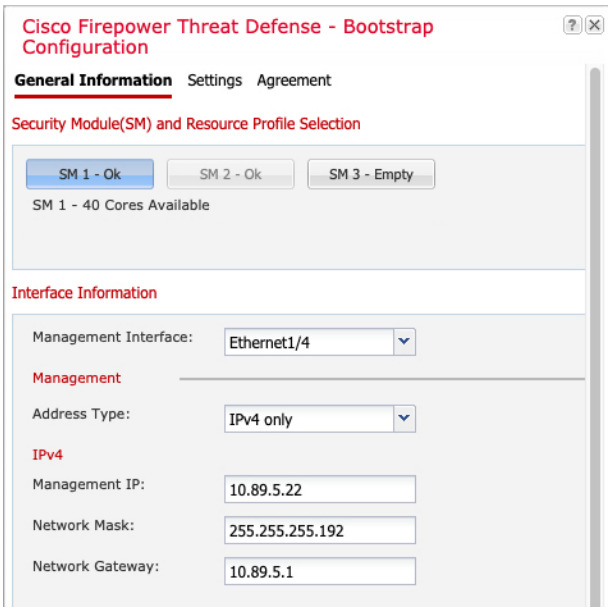


仅可分配先前在**接口**页面上启用的数据接口。稍后需要在 FDM 中启用和配置这些接口，包括设置 IP 地址。

步骤 4 点击屏幕中心的设备图标。

系统将显示对话框，可以在该对话框中配置初始引导程序设置。这些设置仅用于仅初始部署或灾难恢复。为了实现正常运行，稍后可以更改应用 CLI 配置中的大多数值。

步骤 5 在**一般信息**页面上，完成下列操作：



a) （对于 Firepower 9300）在**安全模块选择**下，点击您想用于此逻辑设备的安全模块。

b) 选择**管理接口**。

此接口用于管理逻辑设备。此接口独立于机箱管理端口。

c) 选择管理接口**地址类型**：**仅 IPv4**、**仅 IPv6** 或 **IPv4 和 IPv6**。

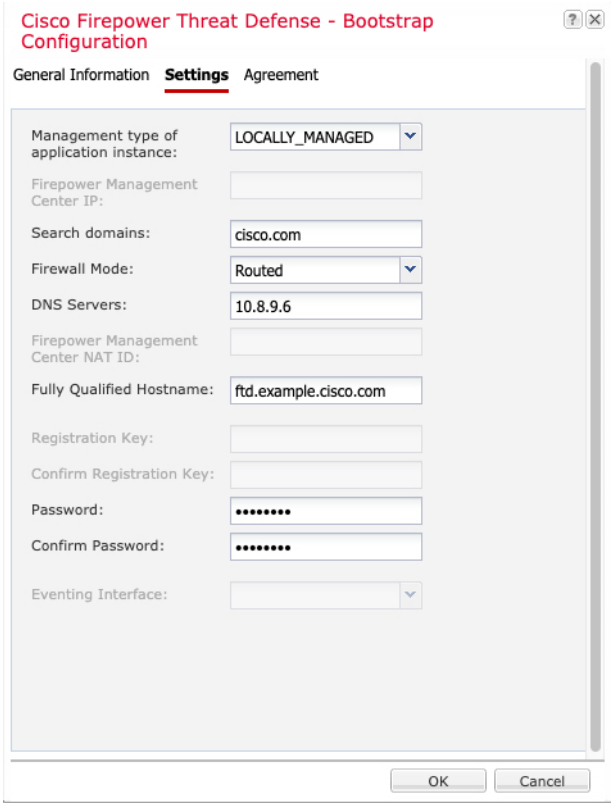
d) 配置**管理 IP** 地址。

设置用于此接口的唯一 IP 地址。

e) 输入**网络掩码 (Network Mask)** 或**前缀长度 (Prefix Length)**。

f) 输入**网络网关 (Network Gateway)** 地址。

步骤 6 在**设置 (Settings)** 选项卡上，完成下列操作：



a) 在**应用实例的管理类型**下拉列表中，选择 **LOCALLY_MANAGED**。

本地实例还支持 FMC 作为管理器。如果在部署逻辑设备后更改管理器，则系统会清除您的配置，并重新初始化设备。

b) 输入逗号分隔列表形式的**搜索域**。

c) **防火墙模式**仅支持**路由式**。

d) 输入逗号分隔列表形式的 **DNS 服务器**。

e) 输入FTD的**完全限定主机名**。

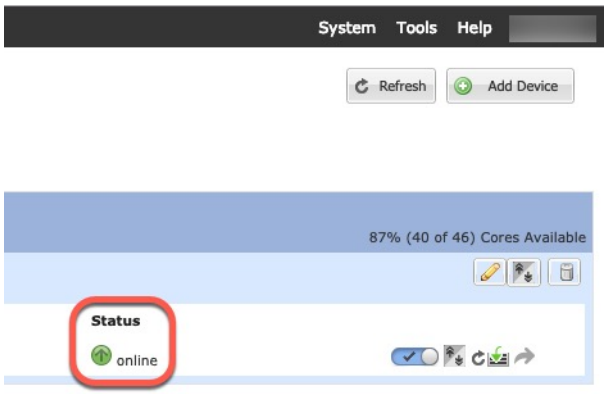
f) 输入供FTD管理员用户用于 CLI 访问的**密码**。

步骤 7 在**协议 (Agreement)** 选项卡上，阅读并接受最终用户许可协议 (EULA)。

步骤 8 点击**确定 (确定)** 关闭配置对话框。

步骤 9 点击**保存**。

机箱通过下载指定软件版本，并将引导程序配置和管理接口设置推送至应用实例来部署逻辑设备。在**逻辑设备**页面中，查看新逻辑设备的状态。当逻辑设备将其**状态**显示为**在线**时，可以开始在应用中配置安全策略。



登录 FDM

登录 FDM 以配置 FTD。

开始之前

- 使用 Firefox、Chrome、Safari、Edge 或 Internet Explorer 的当前版本。
- 确保 Firepower 机箱管理器**逻辑设备**页面上 ASA 逻辑设备**状态**为**在线**。

过程

步骤 1 在浏览器中输入以下 URL。

- **https://***management_ip* - 在引导程序配置中输入的管理接口 IP 地址。

步骤 2 使用用户名 **admin** 和部署 FTD 时设置的密码 登录。

步骤 3 系统会提示您接受 90 天评估许可证。

配置许可

FTD 使用思科智能软件许可，这使得您可以集中购买和管理许可证池。

当您注册机箱时，许可证颁发机构会颁发一张ID证书，用于机箱与许可证颁发机构之间的通信。它还会将机箱分配到相应的虚拟帐户。

基本许可证会自动包含在内。智能许可不会阻止您使用尚未购买的产品功能，但是为了符合要求，您应购买以下可选功能许可证：

- **威胁** - 安全情报和思科 Firepower 下一代 IPS
- **恶意软件** - 适用于网络的高级恶意软件防护 (AMP)
- **URL** - URL 过滤
- **RA VPN** - AnyConnect Plus、AnyConnect Apex 或仅 AnyConnect VPN。

除上述许可证外，您还需要订阅相关内容以获取 1 年、3 年或 5 年的更新。

有关为系统授权许可的完整信息，请参阅《FDM 配置指南》。

开始之前

- 拥有思科智能软件管理器主帐户。

  如果您还没有账户，请单击此链接以设置新账户。通过智能软件管理器，您可以为组织创建一个主账户。

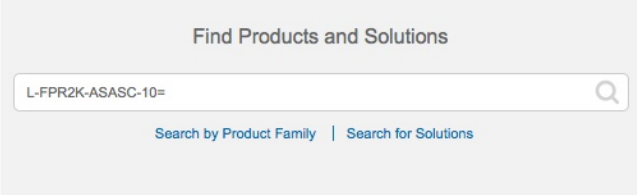
- 您的思科智能软件许可帐户必须符合强加密 (3DES/AES) 许可证的要求，才能使用某些功能（已使用导出合规性标志启用）。

过程

步骤 1 请确保智能许可帐户包含所需的可用许可证。

当您从思科或经销商那里购买设备时，您的许可证应该已链接到您的智能软件许可证帐户。但是，如果您需要自己添加许可证，则请使用思科商务工作空间上的 **Find Products and Solutions** 搜索字段。搜索以下许可证 PID：

图 *1:* 许可证搜索



注释 如果未找到 PID，您可以手动将 PID 添加到订单中。

- 威胁、恶意软件和 URL 许可证组合：
  - L-FPR9K-24T-TMC=
  - L-FPR9K-36T-TMC=
  - L-FPR9K-40T-TMC=
  - L-FPR9K-44T-TMC=
  - L-FPR9K-48T-TMC=

- L-FPR9K-56T-TMC=

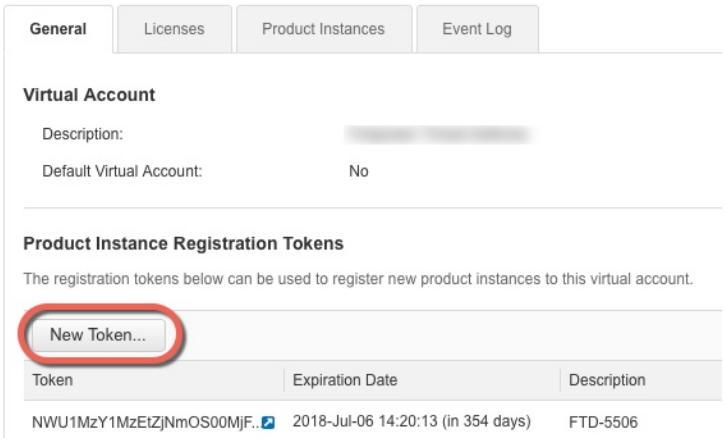
- 威胁、恶意软件和 URL 订阅组合：
  - L-FPR9K-24T-TMC-1Y
  - L-FPR9K-24T-TMC-3Y
  - L-FPR9K-24T-TMC-5Y
  - L-FPR9K-36T-TMC-1Y
  - L-FPR9K-36T-TMC-3Y
  - L-FPR9K-36T-TMC-5Y
  - L-FPR9K-40T-TMC-1Y
  - L-FPR9K-40T-TMC-3Y
  - L-FPR9K-40T-TMC-5Y
  - L-FPR9K-44T-TMC-1Y
  - L-FPR9K-44T-TMC-3Y
  - L-FPR9K-44T-TMC-5Y
  - L-FPR9K-48T-TMC-1Y
  - L-FPR9K-48T-TMC-3Y
  - L-FPR9K-48T-TMC-5Y
  - L-FPR9K-56T-TMC-1Y
  - L-FPR9K-56T-TMC-3Y
  - L-FPR9K-56T-TMC-5Y

- RA VPN - 请参阅思科 AnyConnect 订购指南。

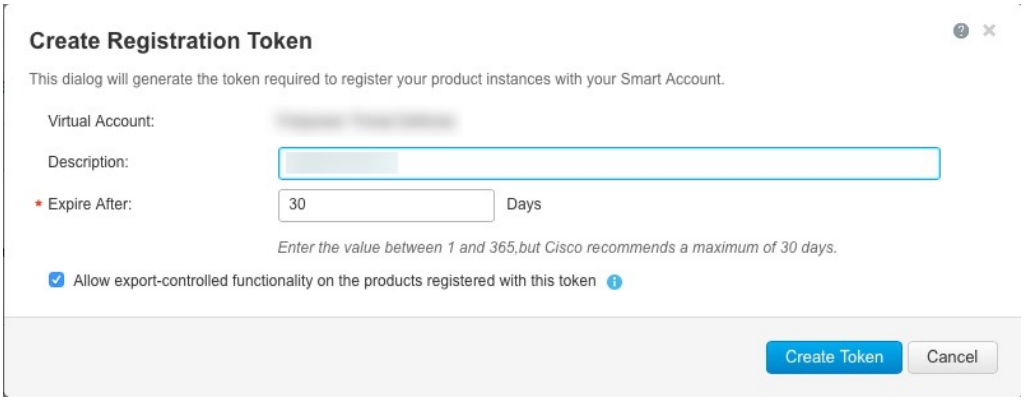
步骤 2 在 Cisco Smart Software Manager 中，为要将此设备添加到的虚拟帐户请求并复制注册令牌。

a) 单击 **Inventory**。

b) 在 **General** 选项卡上，单击 **New Token**。



c) 在 **Create Registration Token** 对话框中，输入以下设置，然后单击 **Create Token**：



- **Description**
- **Expire After** - 思科建议该时间为 30 天。
- **Allow export-controlled functionaility on the products registered with this token**（在使用此令牌注册的产品上允许导出控制的功能）- 在您所在的国家/地区允许进行强加密的情况下启用导出合规性标志。

系统将令牌添加到您的资产中。

d) 单击令牌右侧的箭头图标可以打开 **Token** 对话框，可以从中将令牌 ID 复制到剪贴板。当需要注册 FTD 时，请准备好此令牌，以在该程序后面的部分使用。

图 *2:* 查看令牌

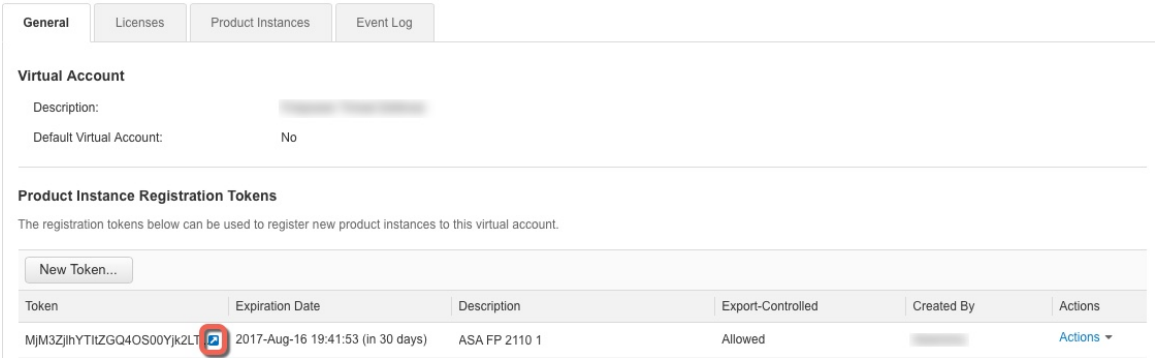
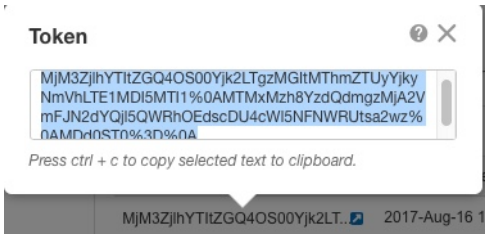


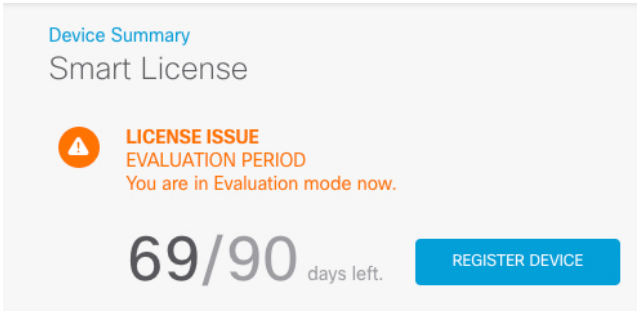
图 *3:* 复制令牌



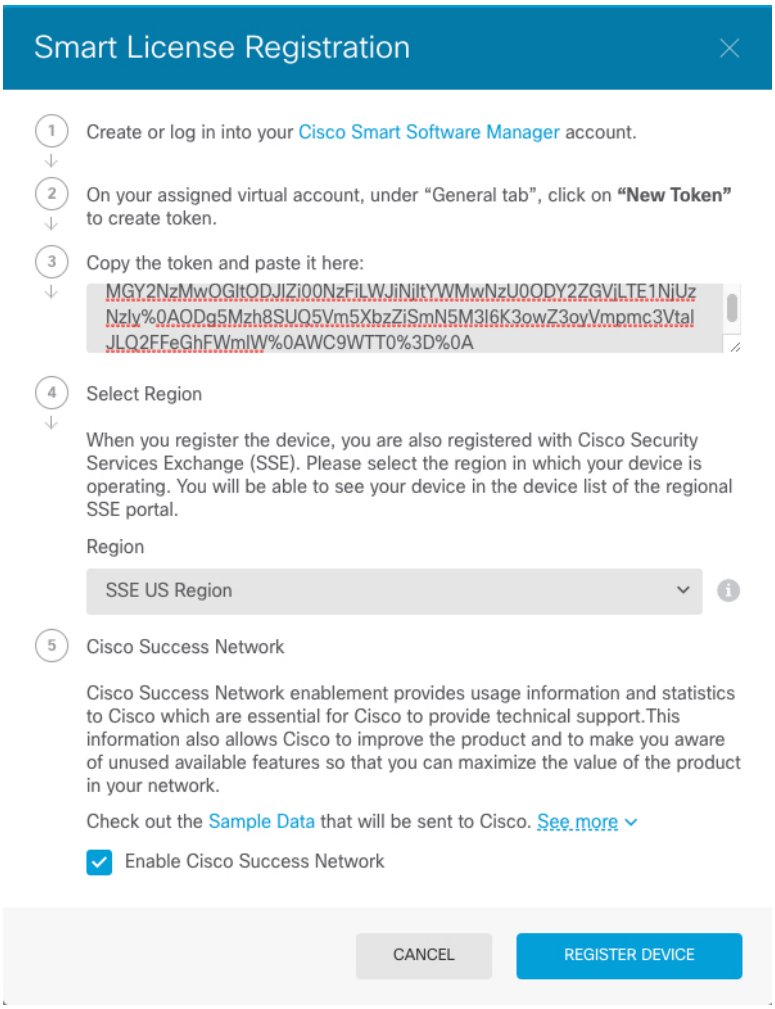
步骤 3 在 FDM 中，单击**设备**，然后在**智能许可证**摘要中，单击**查看配置**。

您会看到**智能许可证**页面。

步骤 4 单击 **Register Device**。

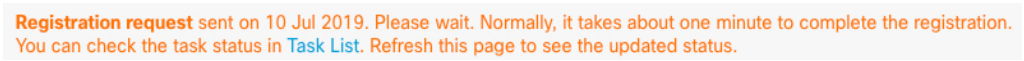


然后，按照**智能许可证注册**对话框中的说明粘贴令牌：

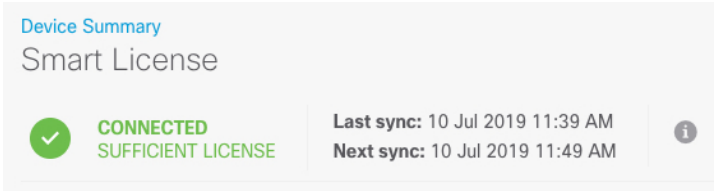


步骤 5 单击**注册设备**。

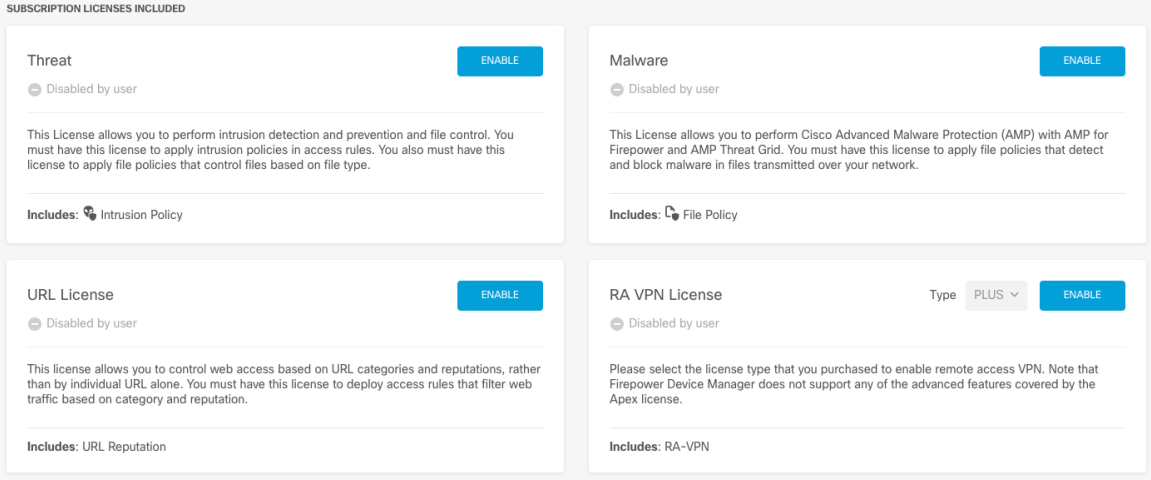
您会返回到**智能许可证**页面。在设备注册时，您会看到以下消息：



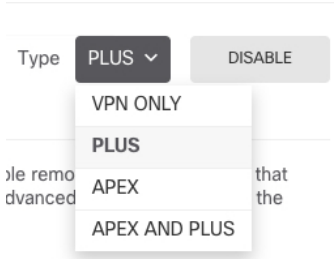
在设备成功注册并刷新页面后，您会看到以下内容：



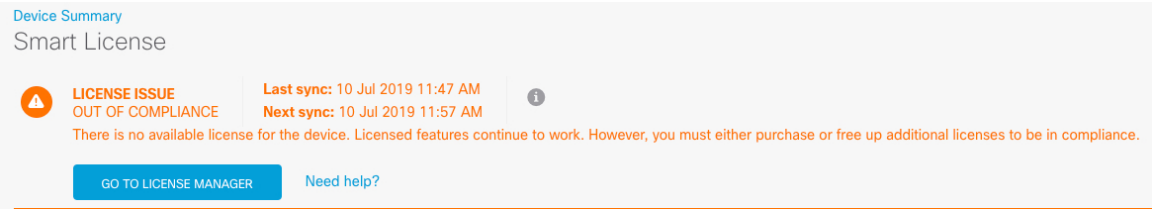
步骤 6 根据需要，点击每个可选许可证的**启用/禁用**控件。



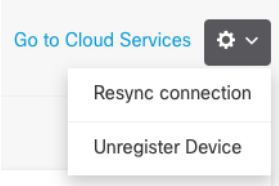
- **启用** - 将许可证注册到您的思科智能软件管理器账户，并启用控制的功能。现在，您可以配置和部署该许可证控制的策略了。
- **禁用** - 取消许可证向思科智能软件管理器账户的注册，并禁用控制的功能。新策略中无法配置这些功能，也不能再部署使用该功能的策略。
- 如果启用了 **RA VPN** 许可证，请选择要使用的许可证类型：**Plus**、**Apex**、**仅 VPN**或 **Plus 和 Apex**。



启用功能后，如果帐户中没有许可证，则在刷新页面后，您会看到以下不合规消息：



步骤 7 从齿轮下拉列表中选择**Resync Connection**（再同步连接），将许可证信息与思科智能软件管理器同步。



配置基本安全策略

要配置基本安全策略，需完成以下任务。

1	配置接口，第 14 页。 为内部接口分配静态 IP 地址，并将 DHCP 用于外部接口。
2	将接口添加到安全区域，第 17 页。 将内部和外部接口添加到访问控制所需的内部和外部安全区域。
3	添加默认路由，第 18 页。 如果没有收到来自外部 DHCP 服务器的默认路由，则需要手动添加它。
4	配置 NAT，第 20 页。 在外部接口上使用接口 PAT。
5	允许流量从内部传到外部，第 22 页。 允许流量从内部传到外部。
6	（可选）配置 DHCP 服务器，第 23 页。 在内部接口上为客户端使用 DHCP 服务器。
7	（可选）配置管理网关并允许在数据接口上进行管理，第 24 页。 更改管理网关和/或允许从数据接口进行管理。
8	部署配置，第 26 页。

配置接口

启用 FTD 接口并设置 IP 地址。通常，您必须至少配置两个接口才能让系统传递有意义的流量。通常，您将拥有面向上游路由器或互联网的外部接口，以及组织网络的一个或多个内部接口。其中一些接口可能是“隔离区”(DMZ)，您可以在其中放置可公开访问的资产，例如 Web 服务器。

典型的边缘路由情况是通过 DHCP 从 ISP 获取外部接口地址，同时在内部接口上定义静态地址。

以下示例配置了一个具有静态地址的内部接口，以及一个使用 DHCP 的外部接口。

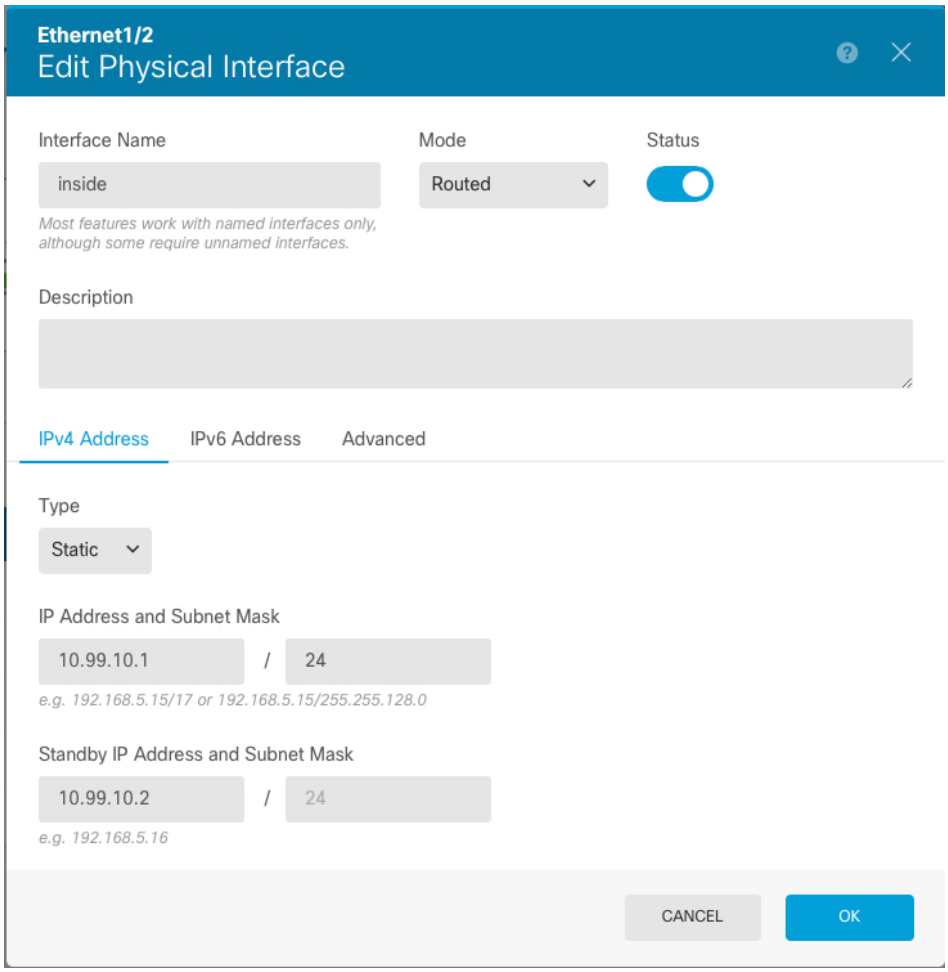
过程

步骤 1 点击**设备**，然后点击**接口**摘要中的链路。

系统默认选择**接口**页面。接口列表显示可用物理接口、物理接口名称、地址和状态。

步骤 2 单击要用于内部的接口的编辑图标 ( )。

步骤 3 进行以下设置：



a) 设置**接口名称**。

设置接口名称，最多 48 个字符。字母字符必须为小写。例如 **inside** 或 **outside**。如果没有名称，将忽略其余的接口配置。除非配置子接口，否则接口应有名称。

b) 将**模式**设置为**路由**。

如果要使用被动接口，请参阅《 FDM 配置指南》 。

c) 将**状态**滑块设置为已启用设置 ( )。

重要事项 还必须在 FXOS 中启用该接口。

d) （可选） 设置**说明**。

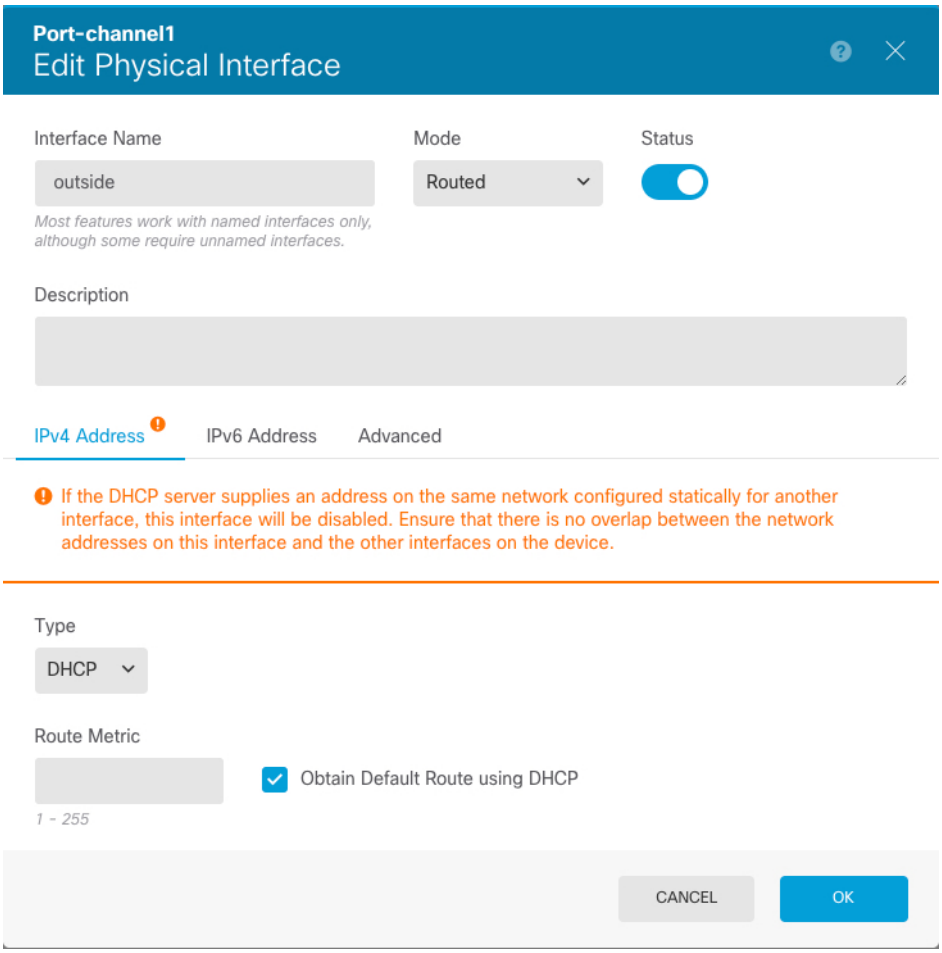
一行说明最多可包含 200 个字符（不包括回车符）。

e) 在 **IPv4 地址**页面上，配置静态 IP 地址。

f) （可选） 单击 **IPv6 地址**，并配置 IPv6。

步骤 4 点击**点击**。

步骤 5 单击要用于外部的接口的编辑图标 ( )，并设置适用于内部的相同字段；对于此接口，请为 IPv4 地址选择**DHCP** 。



注释 如果使用静态 IP 地址或不接收来自 DHCP 的默认路由，则需要手动设置默认路由；请参阅《 FDM 配置指南》。

将接口添加到安全区域

安全区是一组接口。区域将网络划分网段，帮助您管理流量以及对流量进行分类。您可以定义多个区域，但一个给定接口只能位于一个区域中。

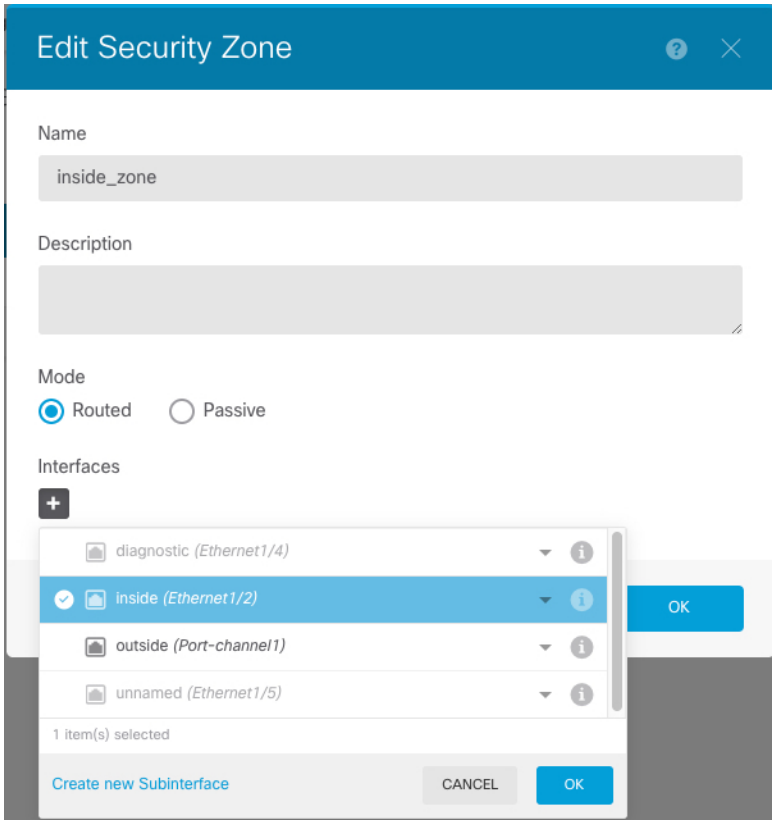
此程序介绍如何将接口添加到以下预配置的区域：

- **inside_zone** - 此区域用于表示内部网络。
- **outside_zone** - 此区域用于表示在您控制之外的网络，例如互联网。

过程

步骤 1 选择**对象**，然后从目录中选择**安全区**。

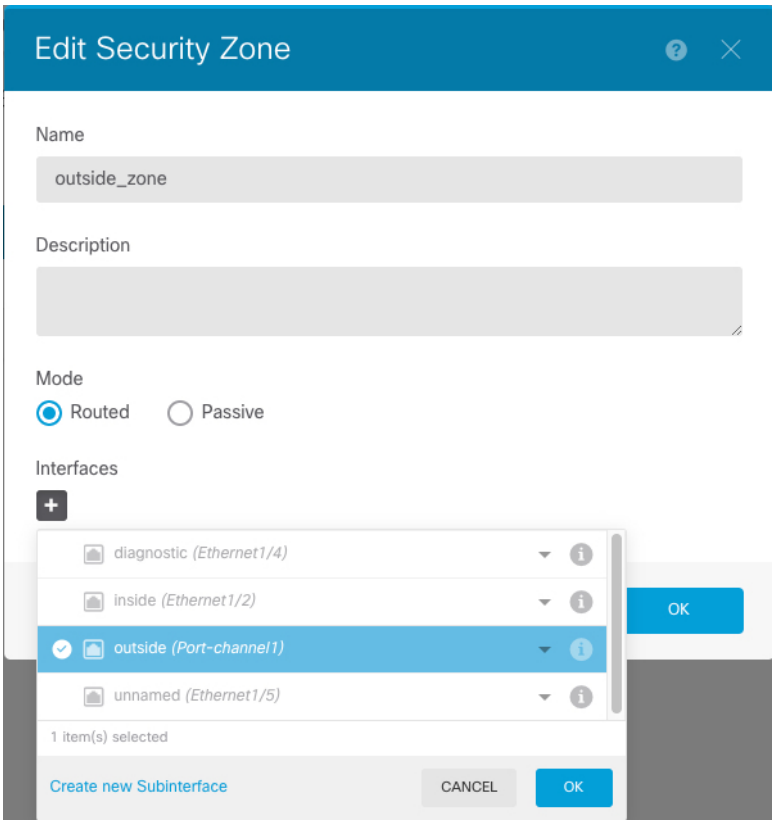
步骤 2 点击 **inside_zone** 的编辑图标 ( )。



步骤 3 在**接口**列表中，点击 + 并选择要添加到该区域的内部接口。

步骤 4 点击 **确定**，保存更改。

步骤 5 重复这些步骤以将外部接口添加到 **outside_zone** 中。



添加默认路由

默认路由通常指向可从外部接口访问的上游路由器。如果您将 DHCP 用作外部接口，则您的设备可能已经收到了默认路由。如果需要手动添加路由，则遵照此程序执行。如果收到来自 DHCP 服务器的默认路由，那么它将显示在**设备摘要** > **静态路由**页面上。

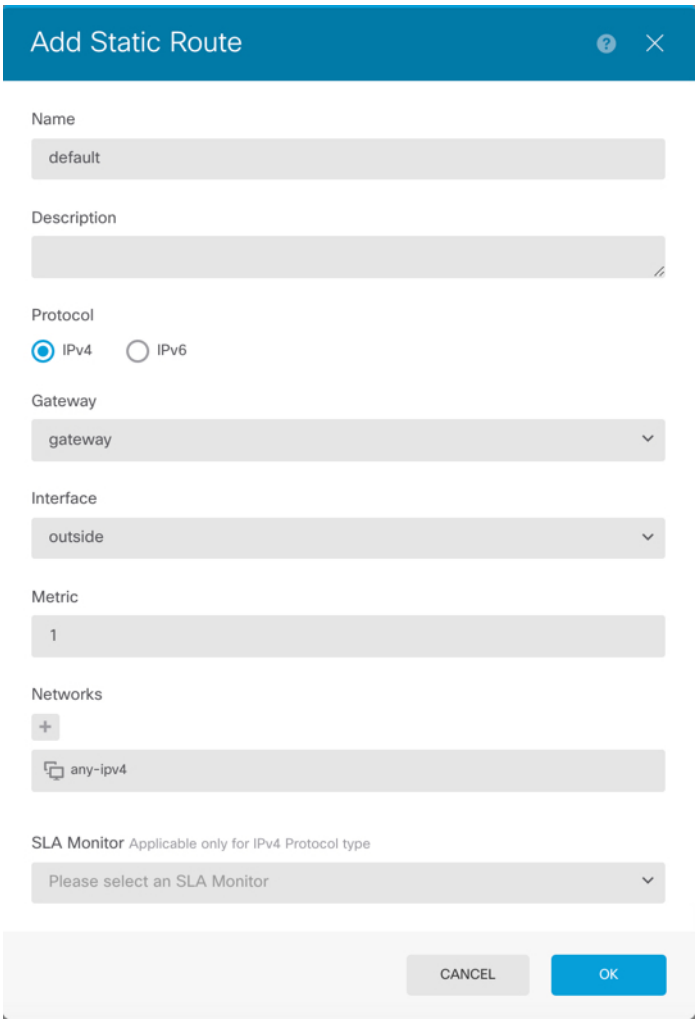
过程

步骤 1 点击**设备**，然后点击**路由**摘要中的链接。

系统将显示**静态路由**页面。

步骤 2 单击 + 或**添加静态路由**。

步骤 3 配置默认路由属性。

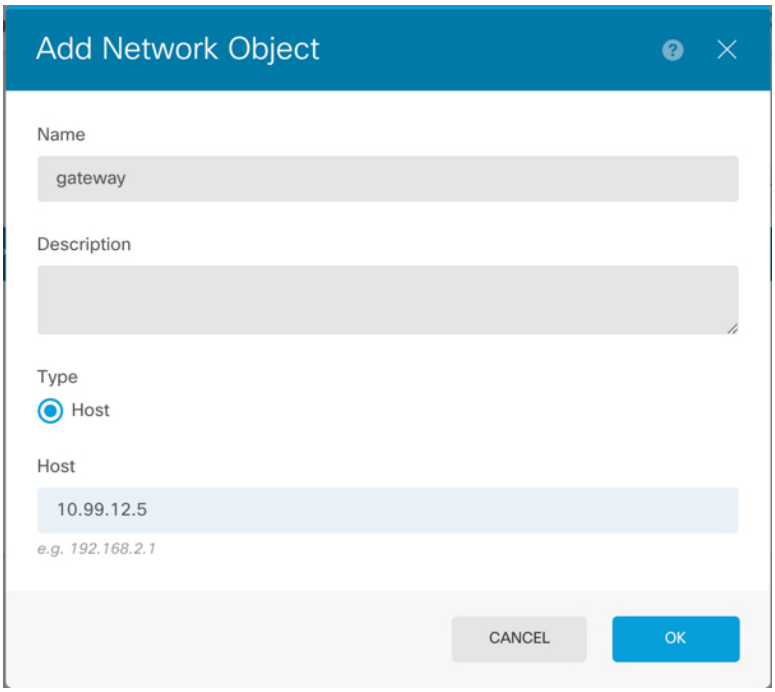


a) 输入**名称**，例如，**默认值**。

b) 单击 **IPv4** 或 **IPv6** 单选按钮。

需要为 IPv4 和 IPv6 创建单独的默认路由。

c) 单击**网关**，然后单击**创建新网络**以将网关 IP 地址添加为主机对象。



d) 选择网关**接口**，例如**外部**。

e) 单击**网络** + 图标，为 IPv4 默认路由选择 **any-ipv4**，为 IPv6 默认路由选择 **any-ipv6**。

步骤 4 点击**确定**。

配置 NAT

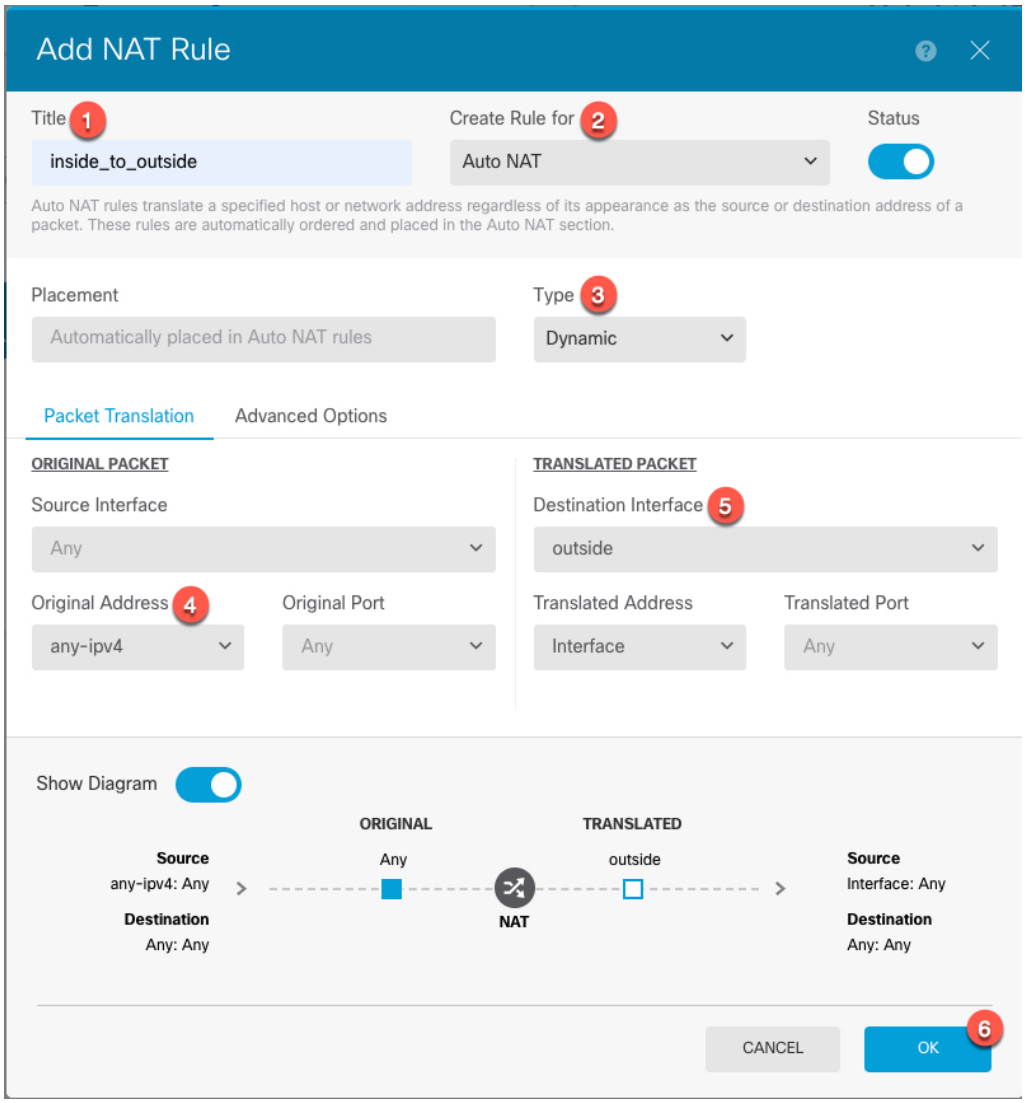
典型的 NAT 规则会将内部地址转换为外部接口 IP 地址上的端口。这类 NAT 规则称为接口端口地址转换 *(PAT)*。您不能将接口 PAT 用于 IPv6。

过程

步骤 1 单击**策略**，然后单击 **NAT**。

步骤 2 单击 + 或**创建 NAT 规则**。

步骤 3 配置基本规则选项：



a) 设置**标题**。
b) 选择**创建规则用于** > **自动 NAT**。
c) 选择**类型** > **动态**。

步骤 4 配置以下数据包转换选项：

a) 对于**原始数据包**，请将**原始地址**设置为**任意 ipv4**。

此规则将转换源自任何接口的所有 IPv4 流量。如果要限制接口或地址，可以选择特定的**源接口**，并为**原始地址**指定 IP 地址。

b) 对于**转换后的数据包**，请将**目标接口**设置为外部接口。

默认情况下，接口 IP 地址用于转换后的地址。

步骤 5 （可选）单击**显示图表**以查看规则的直观示意图。

步骤 6 点击**确定**。

允许流量从内部传到外部

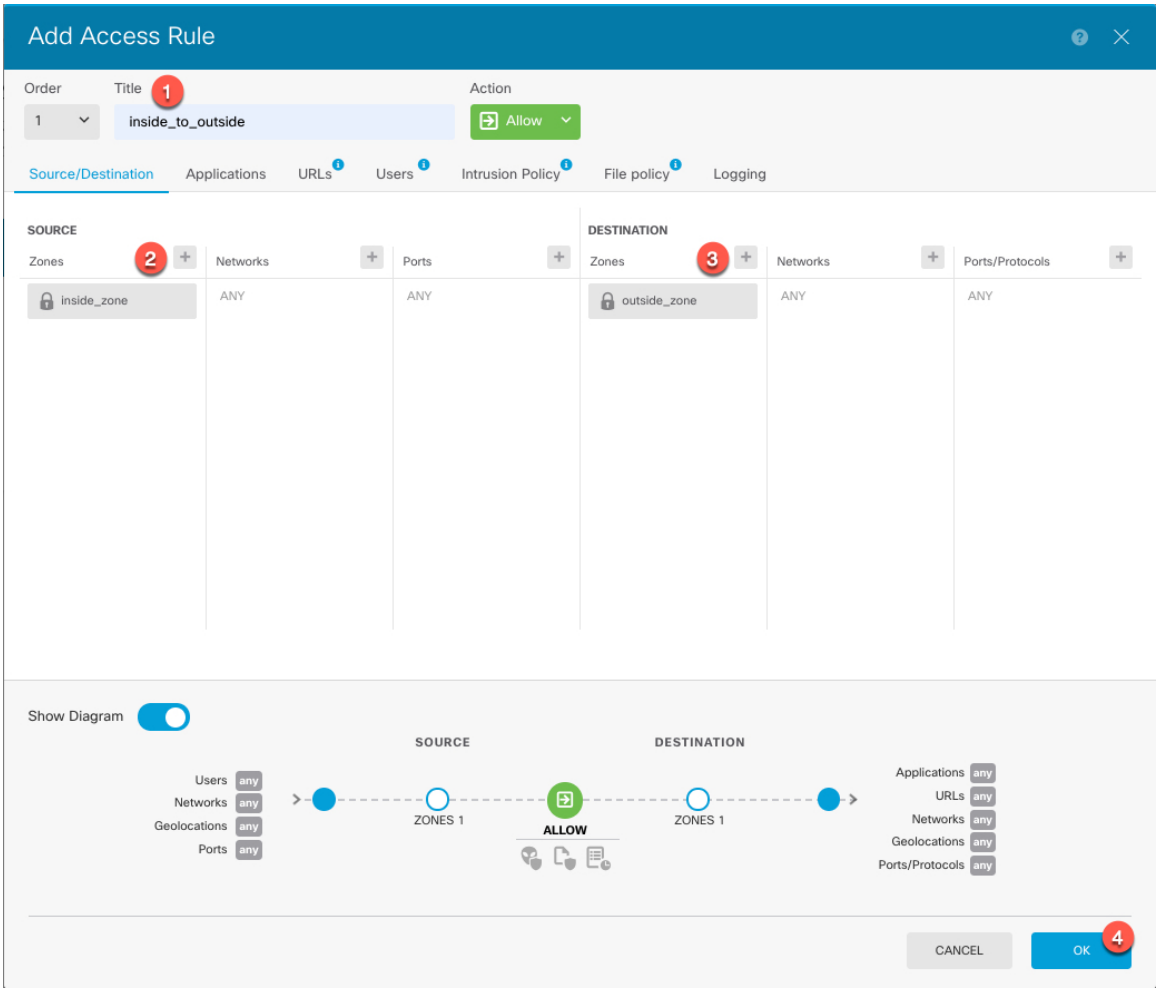
默认情况下，会在安全区域之间阻止流量。此程序介绍如何允许流量从内部传到外部。

过程

步骤 1 选择**策略** > **访问控制**。

步骤 2 单击 **+** 或**创建访问规则**。

步骤 3 配置基本规则选项：



a) 设置**标题**。

b) 对于**源**，请单击**区域** **+** 图标，然后选择内部区域。

c) 对于**目标**，请单击**区域** + 图标，然后选择外部区域。
d) （可选） 单击**显示图表**以查看规则的直观示意图。
e) 点击**确定**。

（可选）配置 DHCP 服务器

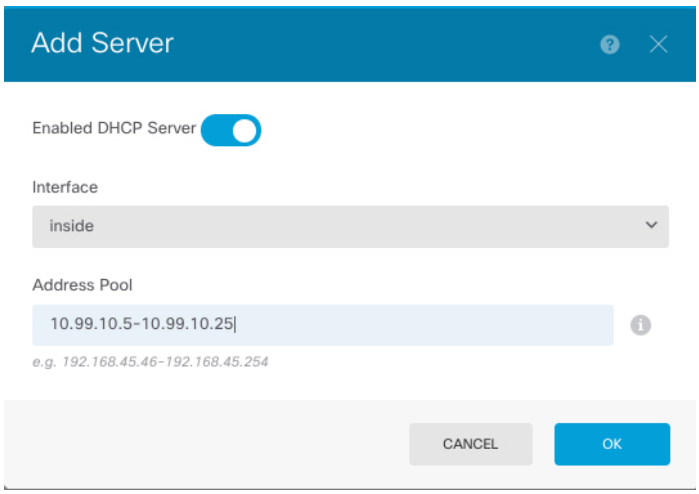
如果希望客户端使用 DHCP 从 FTD处获取 IP 地址，请启用 DHCP 服务器。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **DHCP 服务器**链接。

步骤 2 单击 + 或**创建 DHCP 服务器**。

步骤 3 配置服务器属性。



a) 点击**启用 DHCP 服务器**滑块，使其显示为已启用状态 ( )。
b) 选择要在其上启用 DHCP 服务器的**接口**。

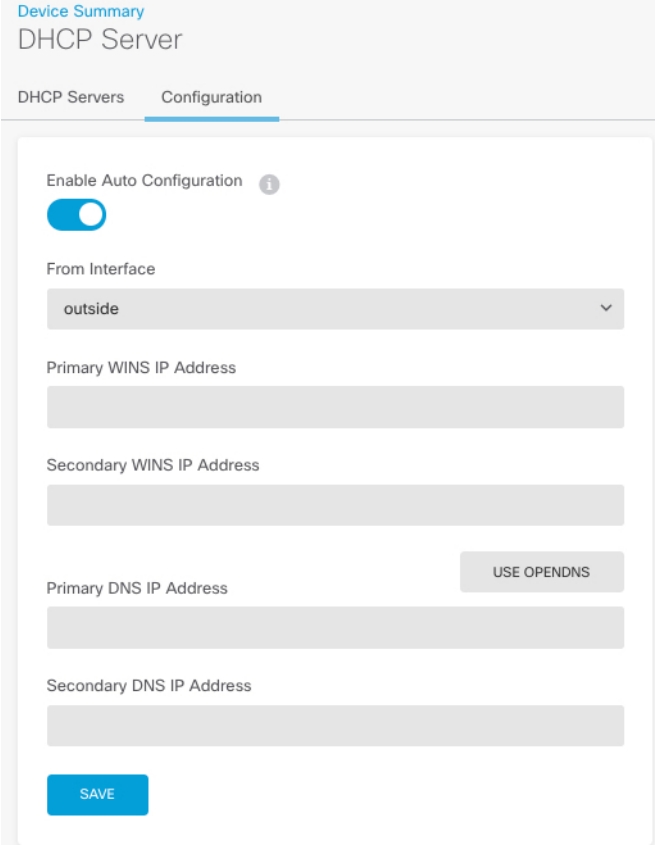
接口必须拥有静态 IP 地址；如果要在接口上运行 DHCP 服务器，则不能使用 DHCP 获取接口。

c) 输入**地址池**

该 IP 地址范围必须与所选接口位于同一子网上，并且不能包括接口本身的 IP 地址、广播地址或子网地址。

d) 点击**点击**。

步骤 4 （可选） 点击**配置**以配置自动配置和全局设置。



DHCP 自动配置使 DHCP 服务器能为 DHCP 客户端提供从运行于指定接口上的 DHCP 客户端获得的 DNS 服务器、域名和 WINS 服务器信息。通常，如果您是在使用 DHCP 获取地址，则会使用自动配置，但您可以选择通过 DHCP 获取其地址的任何接口。如果无法使用自动配置，可以手动定义所需的选项。

a) 点击**启用自动配置**滑块，使其显示为已启用状态 ( )。
b) 在 **From Interface**（从接口）下拉菜单中，选择希望客户端继承其服务器设置的接口。
c) 如果未启用自动配置，或者如果要覆盖任何一个自动配置的设置，请配置一个或多个全局选项。这些设置将发送到运行 DHCP 服务器的所有接口上的 DHCP 客户端。
d) 点击**保存**。

（可选）配置管理网关并允许在数据接口上进行管理

部署 FTD 时，配置了管理地址和外部网关。通过以下程序，可以将 FTD 配置为通过数据接口（而不是管理接口）在背板上发送管理流量。在这种情况下，如果位于直接连接的管理网络上，则仍可以管理 FTD，但发往任何其他网络的管理流量将在数据接口之外路由，而不是通过管理接口进行路由。

此外，默认情况下，只能通过管理接口（FDM或CLI访问）来管理FTD。通过以下程序，还可以在一个或多个数据接口上启用管理。请注意，管理接口网关不会影响数据接口上的FDM管理流量；在这种情况下，FTD 会使用常规路由表。

开始之前

根据配置接口，第 14 页配置数据接口。

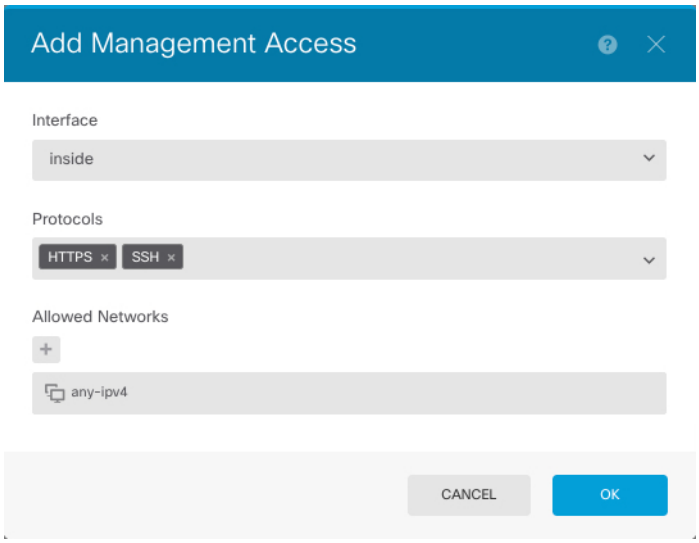
过程

步骤 1 允许从数据接口进行管理。

a) 点击**设备**，然后依次点击**系统设置** > **管理访问**链接。

b) 单击**数据接口**。

c) 单击 + 或**创建数据接口**，并为每个接口创建一个规则：



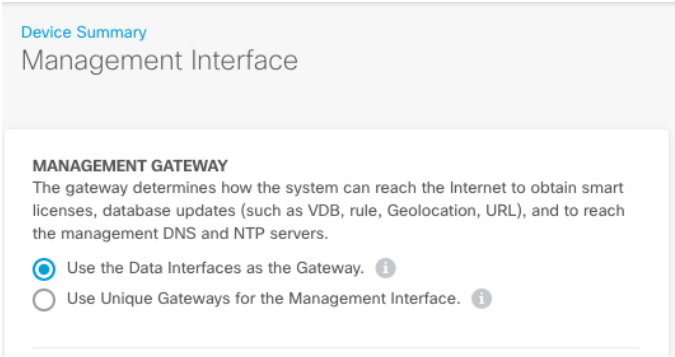
- **接口** - 选择要在其上允许管理访问的接口。
- **协议** - 选择规则是用于 HTTPS（端口 443）、SSH（端口 22）还是二者。
- **允许的网络** - 选择定义应该能够访问系统的IPv4或IPv6网络或主机的网络对象。要指定“任何”地址，请选择 **any-ipv4** (0.0.0.0/0) 和 **any-ipv6** (::/0)。

d) 点击**确定**。

步骤 2 将管理网关设置为使用数据接口。

a) 点击**设备**，然后依次点击**系统设置** > **管理接口**链接。

b) 选择**使用数据接口作为网关**。



c) 点击**保存**，阅读警告，然后点击**确定**。

部署配置

将配置更改部署到 FTD；在部署之前，您的所有更改都不会在设备上生效。

过程

步骤 1 点击网页右上角的**部署更改**图标。

若有未部署的更改，系统会用圆点高亮显示。

“待处理更改”窗口显示配置的部署版本与待处理更改之间的对比信息。这些更改进行了颜色编码，表示出删除、添加或编辑的元素。有关每种颜色的解释，请参阅窗口中的说明。

步骤 2 如果您对所做的更改比较满意，可以点击**立即部署**立即启动作业。

窗口将显示部署正在进行。您可以关闭窗口，或等待部署完成。如果您在部署过程中关闭窗口，作业不会停止。您可以在任务列表或审核日志中查看结果。如果将窗口保持打开状态，请点击**部署历史记录**链接查看结果。

访问 Firepower 威胁防御 CLI

您可以使用FTDCLI更改管理接口参数并进行故障排除。要访问CLI，可以使用管理接口上的SSH，也可以从 FXOS CLI 连接。

过程

步骤 1 （选项 1）通过 SSH 直接连接到 FTD管理接口的 IP 地址。

在部署逻辑设备时，您需要设置管理IP地址。使用admin帐户和初始部署期间设定的密码登录FTD。如果忘记密码，可以编辑 Firepower 机箱管理器中的逻辑设备以更改密码。

步骤 2 （选项 2）从 FXOS CLI，使用控制台连接或 Telnet 连接以连接到模块 CLI。

a) 连接到 安全模块。

connect module *slot_number* {**console** | **telnet**}

使用 Telnet 连接的优点在于，您可以同时对模块开展多个会话，并且连接速度更快。

示例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) 连接到 FTD控制台。

connect ftd *name*

如果您有多个应用程序实例，则必须指定实例名称。要查看实例名称，请输入不含名称的命令。

示例：

```
Firepower-module1> connect ftd FTD_Instance1

============================ ATTENTION ==============================
You are connecting to ftd from a serial console. Please avoid
executing any commands which may produce large amount of output.
Otherwise, data cached along the pipe may take up to 12 minutes to be
drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use
'connect module <slot> telnet' to connect to the security module.
=====================================================================

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to bootCLI
>
```

c) 输入 **exit** 使应用程序控制台返回到 FXOS 模块 CLI。

注释 对于 6.3 之前的版本，输入 **Ctrl-a, d**。

d) 返回 FXOS CLI的管理引擎层。

要退出控制台：

1. 输入 ~

   您将退出至 Telnet 应用。

2. 要退出 Telnet 应用，请输入：

   telnet>**quit**

要退出 Telnet 会话：

输入 **Ctrl-], .**

示例

以下示例连接至安全模块 1FTD上的 ，然后退回到 FXOS CLI 的管理引擎层。

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect ftd FTD_Instance1

============================ ATTENTION ==============================
You are connecting to ftd from a serial console. Please avoid
executing any commands which may produce large amount of output.
Otherwise, data cached along the pipe may take up to 12 minutes to be
drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use
'connect module <slot> telnet' to connect to the security module.
=====================================================================

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to bootCLI
> ~
telnet> quit
Connection closed.
Firepower#
```

后续步骤

要继续配置 FTD 设备，请参阅适用于您的软件版本的文档：导航思科 Firepower 文档。

有关使用 FDM 的信息，请参阅 《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》 。

FTD 与 FDM 的历史记录

功能名称	版本	功能信息
支持具有本地实例的 FDM	6.5.0	现在，可以使用 FDM 部署本地实例。 新增/修改的屏幕： **逻辑设备** > **添加设备** **注释** 需要 FXOS 2.7.1。