



## 部署 Firepower 威胁防御与 FMC

本章对您适用吗？

本章介绍如何完成 Firepower 威胁防御(FTD)设备的初始配置以及如何将设备注册到 Firepower 管理中心(FMC)。在大型网络的典型部署中，多个受管设备安装在网段上，监控流量以进行分析，并向负责管理的 FMC 报告，后者有一个使用 Web 界面的集中式管理控制台，您可以用其来执行管控、管理、分析和报告任务。

对于仅包含单个设备或少数设备、无需使用高性能多设备管理器（如 FMC）的网络，您可以使用集成的 Firepower 设备管理器 (FDM)。使用 FDM 基于 Web 的设备设置向导可配置小型网络部署常用的基本软件功能。



注释

思科 Firepower 1010 硬件可以运行 FTD 软件或 ASA 软件。在 FTD 和 ASA 之间切换需要您对设备进行重新映像。请参阅[重新映像思科 ASA 或 Firepower 威胁防御设备](#)。



注释

**隐私收集声明** - Firepower 1010 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。

- [在开始之前](#)，第 2 页
- [端到端程序](#)，第 2 页
- [查看网络部署](#)，第 4 页
- [连接设备电缆（6.5 及更高版本）](#)，第 6 页
- [连接设备电缆 \(6.4\)](#)，第 7 页
- [接通设备电源](#)，第 8 页
- [为 Firepower 管理配置设备](#)，第 9 页
- [登录到 Firepower 管理中心](#)，第 12 页
- [获取 Firepower 管理中心的许可证](#)，第 12 页
- [向 Firepower 管理中心注册 Firepower 威胁防御](#)，第 13 页
- [配置基本安全策略](#)，第 15 页
- [访问 FTD 和 FXOS CLI](#)，第 30 页

- [断开设备电源，第 31 页](#)
- [后续步骤，第 32 页](#)

## 在开始之前

部署并执行 FMC 的初始配置。请参阅 [FMC 入门指南](#)。



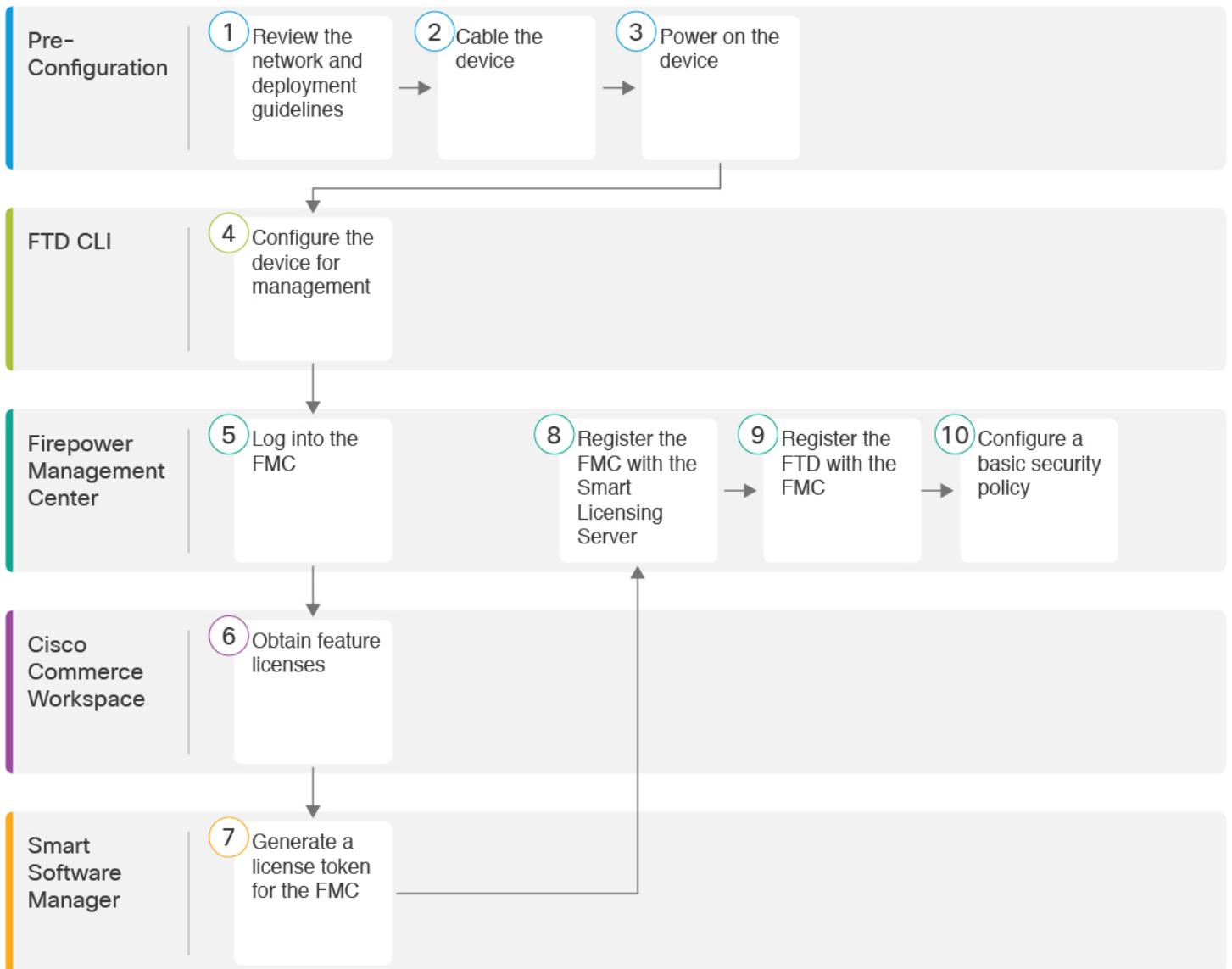
---

**注释** Firepower 设备和 FMC 具有相同的默认管理 IP 地址：192.168.45.45。本指南假设您在初始设置期间将为设备设置不同的 IP 地址。

---

## 端到端程序

请参阅以下任务以在机箱上部署 FTD 和 FMC。



①	配置前准备工作	查看网络部署，第 4 页。
②	配置前准备工作	连接设备电缆（6.5 及更高版本），第 6 页 连接设备电缆 (6.4)，第 7 页。
③	配置前准备工作	接通设备电源。
④	FTD CLI	为 Firepower 管理配置设备，第 9 页。
⑤	Firepower 管理中心	登录到 Firepower 管理中心，第 12 页。

6	思科商务工作空间	获取 Firepower 管理中心的许可证，第 12 页：购买功能许可证。
7	智能软件管理器	获取 Firepower 管理中心的许可证，第 12 页：为 FMC 生成许可证令牌。
8	Firepower 管理中心	获取 Firepower 管理中心的许可证，第 12 页：向智能许可证服务器注册 FMC。
9	Firepower 管理中心	向 Firepower 管理中心注册 Firepower 威胁防御，第 13 页
10	Firepower 管理中心	配置基本安全策略，第 15 页

## 查看网络部署

### 6.5 及更高版本

默认情况下，仅启用管理 1/1 接口并为其配置 IP 地址 (192.168.45.45)。此接口也会最初运行 DHCP 服务器；在初始设置过程中选择 FMC 作为管理器时，DHCP 服务器将被禁用。您可以在将 FTD 连接到 FMC 后配置其他接口。请注意，默认情况下，以交换机端口形式启用了 Ethernet1/2 至 1/8。

下图显示了推荐用于 Firepower 1010 的网络部署。

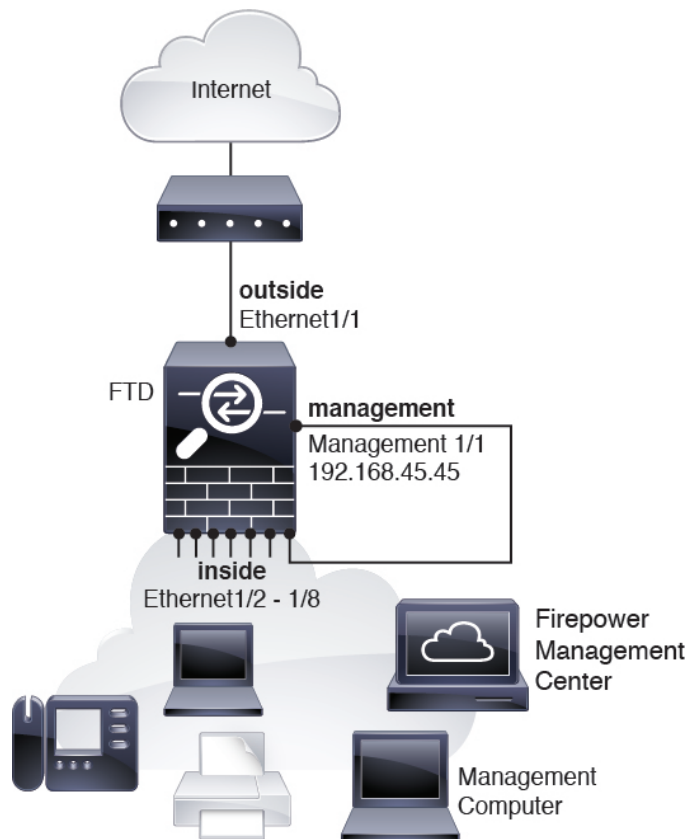
FMC 只能与管理接口上的 FTD 通信。此外，FMC 和 FTD 都需要从管理接口接入互联网以用于许可和更新。

在下图中，通过将管理 1/1 直接连接到内部交换机端口，并将 FMC 和管理计算机连接到其他内部交换机端口，Firepower 1010 充当管理接口和 FMC 的互联网网关。（因为管理接口独立于 FTD 上的其他接口，因此这种直接连接是允许的。）



注释 也可以使用其他拓扑，而部署情况会因要求有所不同。

图 1: 建议的网络部署



## 6.4

默认情况下，仅启用管理1/1 接口并为其配置 IP 地址 (192.168.45.45)。此接口最初也会运行 DHCP 服务器；在初始设置过程中选择 FMC 作为管理器时，会禁用 DHCP 服务器。您可以在将 FTD 连接到 FMC 后配置其他接口。

下图显示了推荐用于 Firepower 1010 的网络部署。

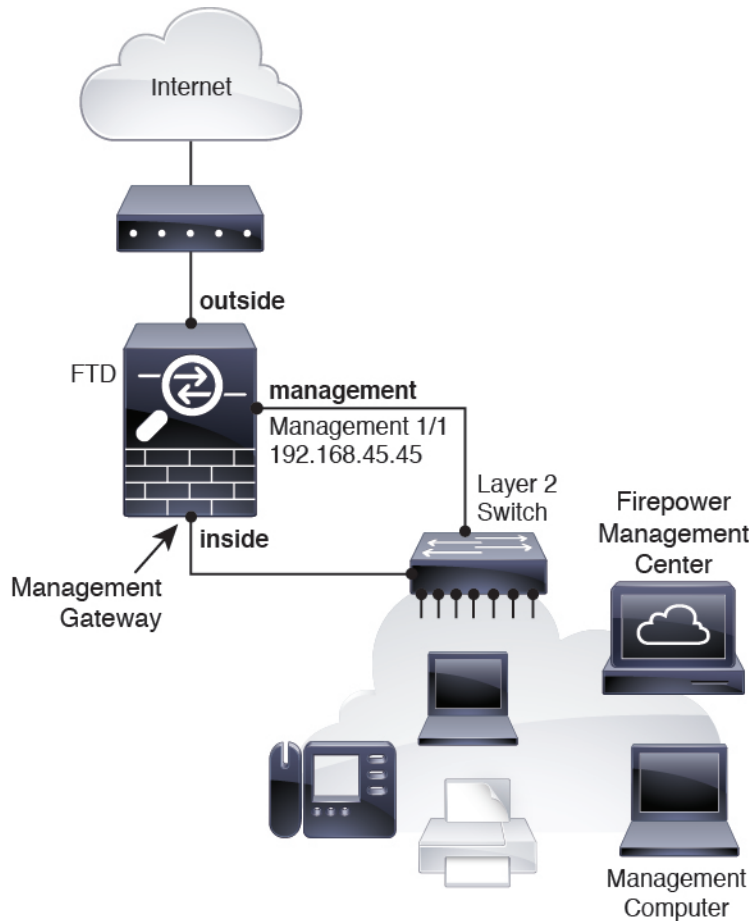
FMC 只能与管理接口上的 FTD 通信。此外，FMC 和 FTD 都需要从管理接口接入互联网以用于许可和更新。

在下图中，通过经第 2 层交换机将管理 1/1 连接到内部接口，并将 FMC 和管理计算机连接到交换机，Firepower 1010 充当管理接口和 FMC 的互联网网关。（因为管理接口独立于 FTD 上的其他接口，因此这种直接连接是允许的。）



**注释** 也可以使用其他拓扑，而部署情况会因要求有所不同。

图 2: 建议的网络部署



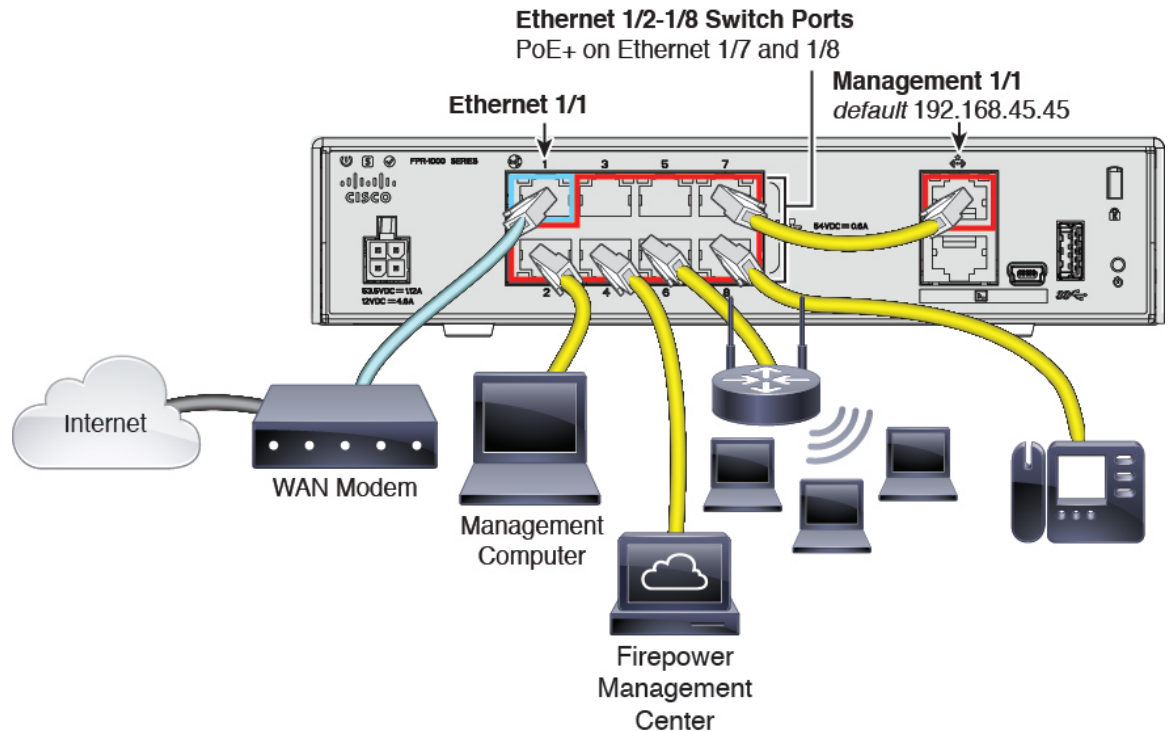
## 连接设备电缆（6.5 及更高版本）

要在 Firepower 1010 上按上述方案进行布线，请参阅下图，其中显示的简单拓扑使用 Ethernet1/1 作为外部接口，并使用其余接口作为内部网络上的交换机端口。



注释 也可以使用其他拓扑，而部署情况会因要求有所不同。例如，可以将交换机端口转换为防火墙接口。

图 3: Firepower 1010 的布线



## 过程

**步骤 1** 将 Management1/1 直接连接到 Ethernet1/2 至 1/8 中的一个交换机端口。

**步骤 2** 使用电缆将以下各项连接到交换机端口 Ethernet1/2 至 1/8:

- Firepower 管理中心
- 管理计算机
- 其他端点

**注释** Firepower 1010 和 FMC 具有相同的默认管理 IP 地址: 192.168.45.45。本指南假设您在初始设置期间将为设备设置不同的 IP 地址。

**步骤 3** 将以太网1/1 连接到外部路由器。

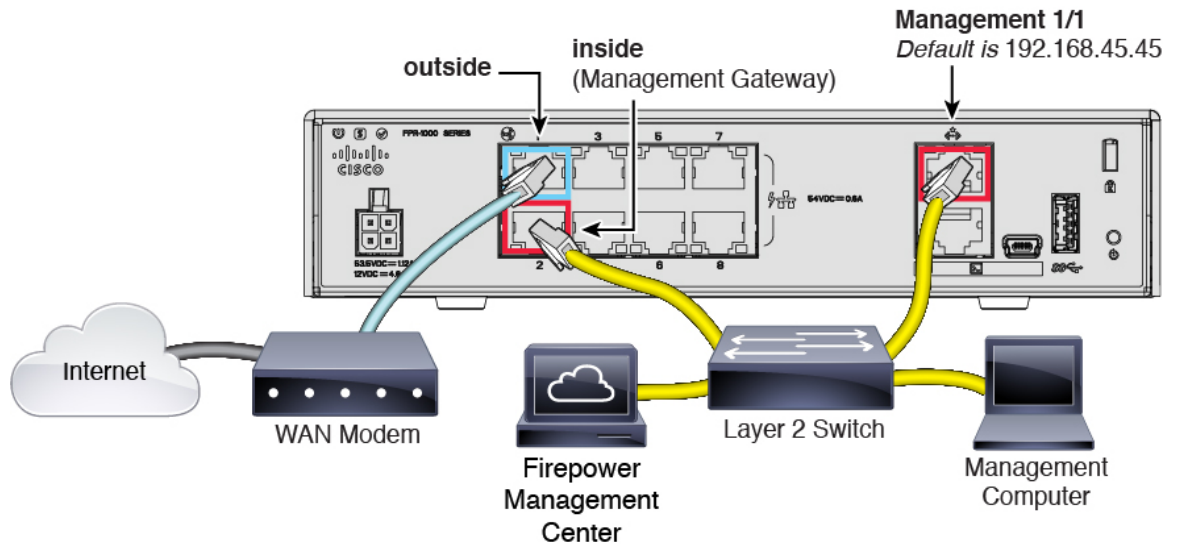
## 连接设备电缆 (6.4)

要在 Firepower 1010 上按上述方案进行布线, 请参阅下图, 其中显示了使用第 2 层交换机的简单拓扑。



注释 也可以使用其他拓扑，而部署情况会因要求有所不同。

图 4. Firepower 1010 的布线



## 过程

**步骤 1** 将以下各项布线到第 2 层以太网交换机：

- 内部接口（例如，以太网 1/2）
- 管理 1/1 接口
- Firepower 管理中心
- 管理计算机

注释 Firepower 1010 和 FMC 具有相同的默认管理 IP 地址：192.168.45.45。本指南假设您在初始设置期间将为设备设置不同的 IP 地址。

**步骤 2** 将外部接口（例如，以太网 1/1）连接到外部路由器。

**步骤 3** 将其他网络连接到其余接口。

## 接通设备电源

系统电源由电源线控制；没有电源按钮。

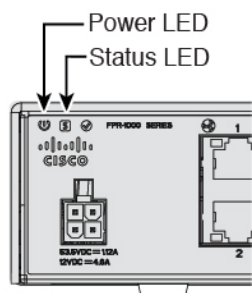


## 过程

**步骤 1** 将电源线一端连接到设备，另一端连接到电源插座。

插上电源线插头时，自动接通电源。

**步骤 2** 检查设备背面或顶部的电源 LED；如果该 LED 呈绿色稳定亮起，表示设备已接通电源。



**步骤 3** 检查设备背面或顶部的状态 LED；其呈绿色稳定亮起之后，系统已通过通电诊断。

# 为 Firepower 管理配置设备

首次访问 CLI 时，设置向导会提示您提供设置 Firepower 威胁防御设备和注册 Firepower 管理中心 (FMC) 所需的基本网络配置参数。请注意，以后无法在 FMC 中配置这些设置；只能在 CLI 中更改它们。

## 过程

**步骤 1** 通过控制台端口或使用 SSH 连接至管理接口 192.168.45.45，从而连接至 FTD CLI。

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

**步骤 3** 当 Firepower 威胁防御系统启动时，设置向导会提示您输入 FTD 管理接口的网络信息，以便与 FMC 通信。

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。

请参阅以下准则：

- 输入管理接口 [数据接口] 的 IPv4 默认网关 - 默认数据接口仅适用于 Firepower 设备管理器管理；使用 FMC 时，应为管理 1/1 设置网关 IP 地址。
- 如果网络信息已更改则需要重新连接 - 如果您已通过 SSH 连接到默认 IP 地址，但在初始设置时更改了 IP 地址，则会断开连接。使用新 IP 地址和密码重新进行连接。另请注意，如果更改 IP 地址，则会禁用管理 1/1 上的 DHCP 服务器。
- **Manage the device locally?** (是/否) [是] - 输入否以使用 FMC。回答是意味着会改用 Firepower 设备管理器。另请注意，如果尚未禁用管理 1/1 上的 DHCP 服务器，则会禁用该服务器。

- **Configure firewall mode? (路由/透明) [路由]** - 我们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。有关详细信息，请参阅以下指南中的“适用于 Firepower 威胁防御的透明或路由防火墙模式”：[《Firepower 管理中心配置指南》](#)

#### 示例:

```

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 change the password for 'admin' to continue.
Enter new password: *****
Confirm new password: *****
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
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]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: 5516X-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
DHCP Server Disabled
The DHCP server has been disabled. You may re-enable with configure network ipv4
dhcp-server-enable
For HTTP Proxy configuration, run 'configure network http-proxy'

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

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 4** 将 Firepower 威胁防御设备注册到负责管理的 FMC。

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

- {hostname | IPv4\_address | IPv6\_address | DONTRESOLVE} 指定 FMC 的完全限定主机名或 IP 地址。如果 FMC 不是直接可寻址的，请使用 DONTRESOLVE。
- reg\_key 是向 FMC 注册设备所需的唯一字母数字注册密钥。

**注释** 注册密钥是由用户生成的一次性使用密钥，长度不超过 37 个字符。有效字符包括字母数字 (A - Z、a - z、0 - 9) 和连字符 (-)。当您将设备添加到 FMC 时，需要记住此注册密钥。

- nat\_id 是当一方未指定 IP 地址时，在 FMC 与设备之间的注册流程中使用的可选字母数字字符串。如果主机名设置为 DONTRESOLVE，此项为必填项。在 FMC 上输入相同的 NAT ID。

**注释** NAT ID 是由用户生成的一次性使用密钥，长度不超过 37 个字符。有效字符包括字母数字 (A - Z、a - z、0 - 9) 和连字符 (-)。当您将设备添加到 FMC 时，需要记住此 NAT ID。

**示例：**

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

如果 Firepower 威胁防御设备和 FMC 由一台 NAT 设备隔开，请随注册密钥一起输入一个唯一的 NAT ID，并指定 DONTRESOLVE 而非主机名，例如：

**示例：**

```
> configure manager add DONTRESOLVE my_reg_key my_nat_id  
Manager successfully configured.
```

FMC 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。NAT ID 必须在用于注册受管理设备的所有 NAT ID 中唯一，以便为初始通信建立信任并查找正确的注册密钥。

**注释** 至少一个安全设备（FMC 或 Firepower 威胁防御）必须有公共 IP 地址，以便在两个设备之间建立双向 SSL 加密通信通道。

---

**下一步做什么**

将设备注册到 FMC。

## 登录到 Firepower 管理中心

使用 FMC 配置并监控 FTD。

### 开始之前

有关受支持浏览器的信息，请参阅您所用版本的发行说明（参阅<https://www.cisco.com/go/firepower-notes>）。

### 过程

---

**步骤 1** 使用支持的浏览器输入以下 URL。

**https://fmc\_ip\_address**

**步骤 2** 输入您的用户名和密码。

**步骤 3** 单击 **Log In**。

---

## 获取 Firepower 管理中心的许可证

所有许可证都由 FMC 提供给 FTD。您可以选择购买以下功能许可证：

- **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。

### 开始之前

- 拥有 [思科智能软件管理器](#) 主帐户。

如果您还没有帐户，请单击此链接以 [设置新帐户](#)。通过智能软件管理器，您可以为组织创建一个主帐户。

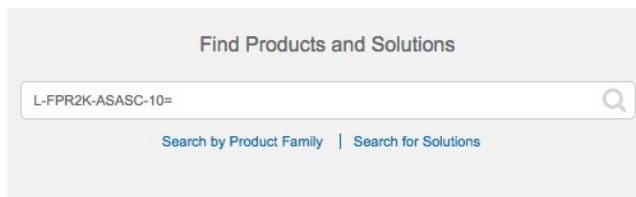
- 您的思科智能软件许可帐户必须符合强加密 (3DES/AES) 许可证的要求，才能使用某些功能（已使用导出合规性标志启用）。

## 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 5: 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-FPR1010T-TMC=
- 威胁、恶意软件和 URL 订阅组合：
  - L-FPR1010T-TMC-1Y
  - L-FPR1010T-TMC-3Y
  - L-FPR1010T-TMC-5Y
- RA VPN - 请参阅[思科 AnyConnect 订购指南](#)。

**步骤 2** 如果尚未执行此操作，请向智能许可服务器注册 FMC。

注册需要您在智能软件管理器中生成注册令牌。有关详细指示，请参阅[FMC配置指南](#)。

## 向 Firepower 管理中心注册 Firepower 威胁防御

将 FTD 注册到 FMC。

### 开始之前

- 收集您在 FTD 初始配置中设置的以下信息：
  - FTD 管理 IP 地址和/或 NAT ID
  - FMC 注册密钥

## 过程

步骤 1 在 FMC 中，选择 **Devices > Device Management**。

步骤 2 从 **Add** 下拉列表选择 **Add Device**，然后输入以下参数。

**Add Device** ? x

Host:† 192.168.101.10

Display Name: 192.168.101.10

Registration Key:\* 1a2b3c4d5e

Group: None

Access Control Policy:\* initial ac

**Smart Licensing**

Malware:

Threat:

URL Filtering:

**Advanced**

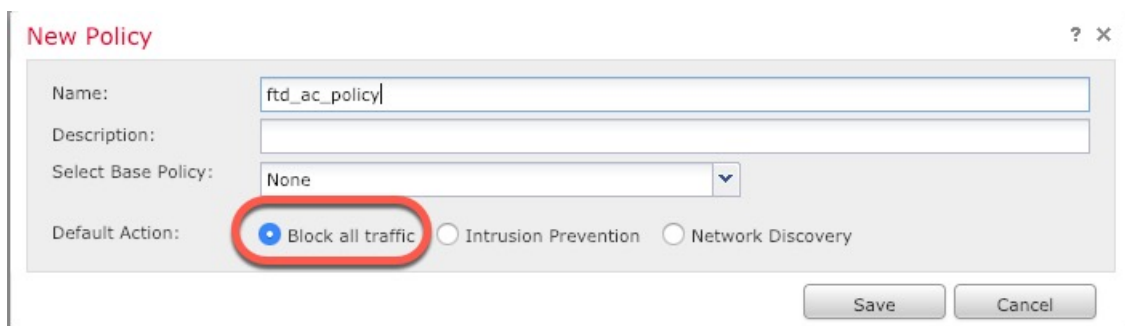
Unique NAT ID:†

Transfer Packets:

On Firepower Threat Defense devices version 6.2.1 onwards, AnyConnect VPN licenses can be enabled from [smart license page](#)

Register Cancel

- **Host** - 输入要添加 FTD 的 IP 地址。如果在 FTD 初始配置中同时指定了 FMC IP 地址和 NAT ID，可以将此字段留空。
- **Display Name** - 输入要在 FMC 中显示的 FTD 的名称。
- **Registration Key** - 输入您在 FTD 初始配置中指定的注册密钥。
- **Domain** - 如果有多域环境，请将设备分配给分叶域。
- **Group** - 如果在使用组，则将其分配给设备组。
- **Access Control Policy** - 选择初始策略。除非已经拥有您知道自己需要使用的自定义策略，否则选择 **Create new policy**，然后选择 **Block all traffic**。之后您可以更改此设置以允许流量通过；请参阅 [允许流量从内部传到外部](#)，第 28 页。



- **Smart Licensing** - 为要部署的功能分配所需的智能许可证：**Malware**（如果您打算使用 AMP 恶意软件检查）、**Threat**（如果您打算使用入侵防御）、**URL**（如果您打算实施基于类别的 URL 过滤）。
- **Unique NAT ID** - 指定您在 FTD 初始配置中指定的 NAT ID。
- **Transfer Packets** - 可让设备将数据包传输至 FMC。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 FMC 进行检测。如果禁用此选项，只有事件信息会发送到 FMC，数据包数据不发送。

**步骤 3** 单击 **Register**，并确认注册成功。

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 FTD 注册失败，请检查以下项：

- Ping - 访问 FTDCLI，然后使用以下命令 ping FMC 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 FTDIP 地址，使用 **configure network {ipv4 | ipv6} manual** 命令。

- 注册密钥、NAT ID 和 FMCIP 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 FTD 上使用 **configure manager add** 命令设定注册密钥和 NAT ID。也可以使用此命令更改 FMCIP 地址。

## 配置基本安全策略

本部分介绍如何使用以下设置配置基本安全策略：

- 内部和外部接口 - 为内部接口分配静态 IP 地址，并将 DHCP 用作外部接口。
- DHCP 服务器 - 在内部接口上为客户端使用 DHCP 服务器。
- 默认路由 - 通过外部接口添加默认路由。
- NAT - 在外部接口上使用接口 PAT。

- 访问控制 - 允许流量从内部传到外部。

要配置基本安全策略，需完成以下任务。

①	配置接口（6.5 及更高版本），第 16 页 配置接口 (6.4)，第 20 页。
②	配置 DHCP 服务器，第 23 页。
③	添加默认路由，第 24 页。
④	配置 NAT，第 25 页。
⑤	允许流量从内部传到外部，第 28 页。
⑥	部署配置，第 29 页。

## 配置接口（6.5 及更高版本）

为交换机端口添加 VLAN1 接口或将交换机端口转换为防火墙接口，将接口分配到安全区域，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。默认情况下，以太网 1/1 接口是可用于外部的常规防火墙接口，其余接口是 VLAN 1 上的交换机端口；添加 VLAN1 接口后，可以将其设置为内部接口。或者，可以将交换机端口分配给其他 VLAN，或将交换机端口转换为防火墙接口。

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。

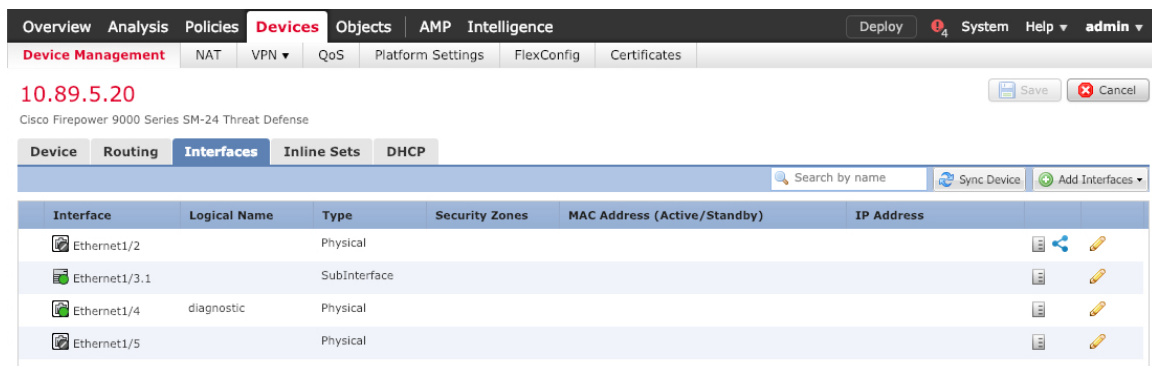
以下示例配置了一个含静态地址的路由模式内部接口 (VLAN1)，以及一个使用 DHCP 的路由模式外部接口（以太网 1/1）。


### 过程

**步骤 1** 选择 **Devices > Device Management**，然后单击设备的编辑图标（）。

**步骤 2** 单击 **Interfaces**。

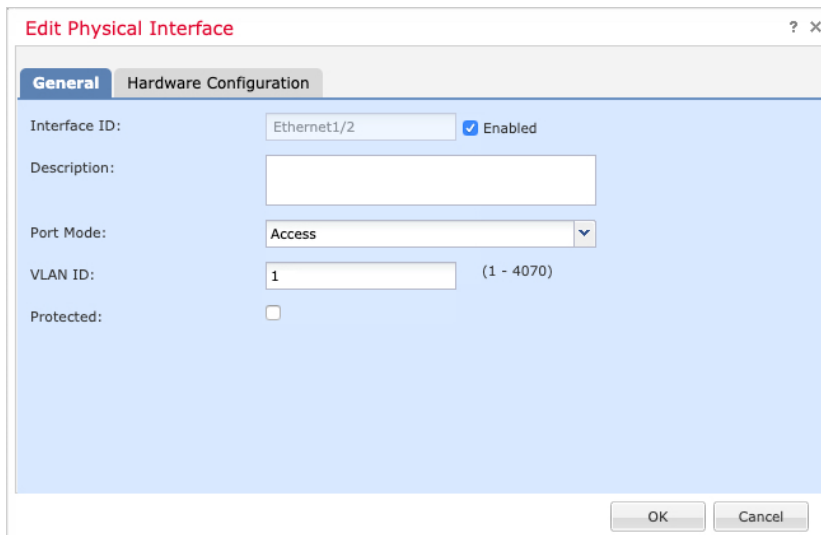




**步骤 3**（可选）单击交换机端口列表中的滑块，为任何交换机端口（以太网 1/2 至 1/8）禁用交换机端口模式，使其显示为“禁用”（）。

**步骤 4** 启用交换机端口。

a) 单击与交换机端口相对应的编辑图标（）。



b) 选中启用复选框以启用此接口。

c)（可选）更改 VLAN ID；默认值为 1。接下来，您将添加一个 VLAN 接口来匹配此 ID。

d) 点击点。

**步骤 5** 添加内部 VLAN 接口。

a) 单击添加接口 > VLAN 接口。

**General** 选项卡将显示。

The screenshot shows the 'Add VLAN Interface' configuration window with the following settings:

- Name:** inside (with an 'Enabled' checkbox checked)
- Description:** (empty text box)
- Mode:** None (dropdown menu)
- Security Zone:** inside\_zone (dropdown menu)
- MTU:** 1500 (range: 64 - 9198)
- VLAN ID \*:** 1 (range: 1 - 4070)
- Disable Forwarding on Interface:** None (dropdown menu)

The 'Associated Interface' table is empty, displaying 'No records to display'. 'OK' and 'Cancel' buttons are located at the bottom right of the window.

- b) 输入长度最大为 48 个字符的 **Name**。  
例如，将接口命名为 **inside**。
- c) 选中 **Enabled** 复选框。
- d) 将 **Mode** 保留为 **None**。
- e) 从 **Security Zone** 下拉列表中选择一个现有的内部安全区域，或者单击 **New** 添加一个新的安全区域。

例如，添加一个名为 **inside\_zone** 的区域。必须将每个接口分配给安全区域和/或接口组。每个接口只能属于一个安全区域，但可以同时属于多个接口组。您可以根据区域或组应用安全策略。例如，您可以将内部接口分配到内部区域，而将外部接口分配到外部区域。然后可以配置访问控制策略，允许流量从内部传到外部，但不允许从外部传入内部。大多数策略仅支持安全区域；您可以在 NAT 策略、预过滤器策略和 QoS 策略中使用区域或接口组。

- f) 将 **VLAN ID** 设置为 **1**。

默认情况下，所有交换机端口都设置为 VLAN 1；如果在此处选择不同的 VLAN ID，还需要编辑每个交换机端口，使其位于新 VLAN ID 所对应的 VLAN 上。

保存接口后，无法更改 VLAN ID；VLAN ID 既是使用的 VLAN 标记，也是您的配置中的接口 ID。

- g) 单击 **IPv4** 和/或 **IPv6** 选项卡。

- **IPv4** - 从下拉列表中选择 **Use Static IP**，然后以斜杠表示法输入 IP 地址和子网掩码。

例如，输入 **192.168.1.1/24**

- IPv6 - 为无状态自动配置选中 **Autoconfiguration** 复选框。

h) 单击 **OK**。

**步骤 6** 单击要用于外部的以太网 1/1 的编辑图标（✎）。

**General** 选项卡将显示。

a) 输入长度最大为 48 个字符的 **Name**。

例如，将接口命名为 **outside**。

b) 选中 **Enabled** 复选框。

c) 将 **Mode** 保留为 **None**。

d) 从 **Security Zone** 下拉列表中选择现有的外部安全区域，或者单击 **New** 添加一个新的安全区域。

例如，添加一个名为 **outside\_zone** 的区域。

e) 单击 **IPv4** 和/或 **IPv6** 选项卡。

- **IPv4** - 选择 **Use DHCP**，然后配置以下选填参数：

- **Obtain default route using DHCP** - 从 DHCP 服务器获取默认路由。
- **DHCP route metric** - 分配到所获悉路由的管理距离，介于 1 和 255 之间。获悉的路由的默认管理距离为 1。

The screenshot shows the 'Edit Physical Interface' configuration window with the 'IPv4' tab selected. The 'IP Type' dropdown is set to 'Use DHCP'. Below it, the 'Obtain default route using DHCP' checkbox is checked. The 'DHCP route metric' is set to '1' in a text input field, with '(1 - 255)' indicating the valid range.

- **IPv6** - 为无状态自动配置选中 **Autoconfiguration** 复选框。

f) 点击确定。

步骤 7 点击保存。

## 配置接口 (6.4)

启用 FTD 接口，为其分配安全区域并设置 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。

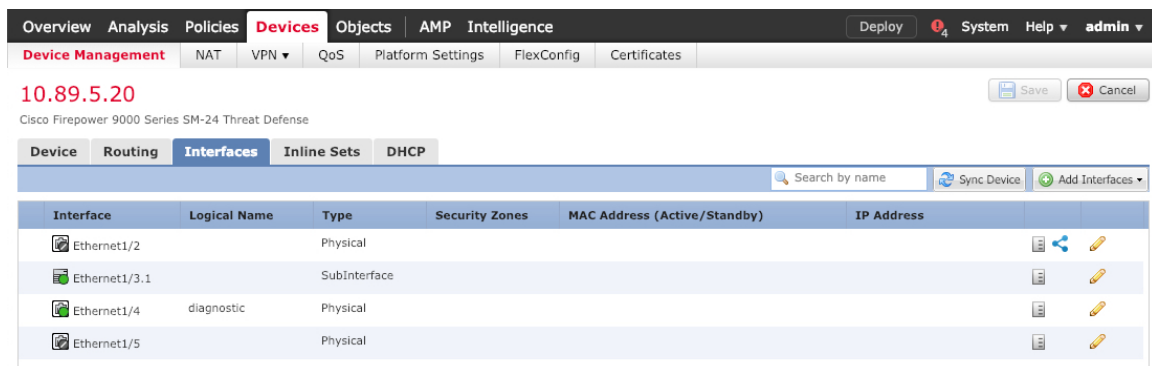
典型的边缘路由情况是通过 DHCP 从 ISP 获取外部接口地址，同时在内部接口上定义静态地址。

以下示例使用 DHCP 在接口内部配置了一个路由模式（含静态地址），并在接口外部配置了一个路由模式。

### 过程

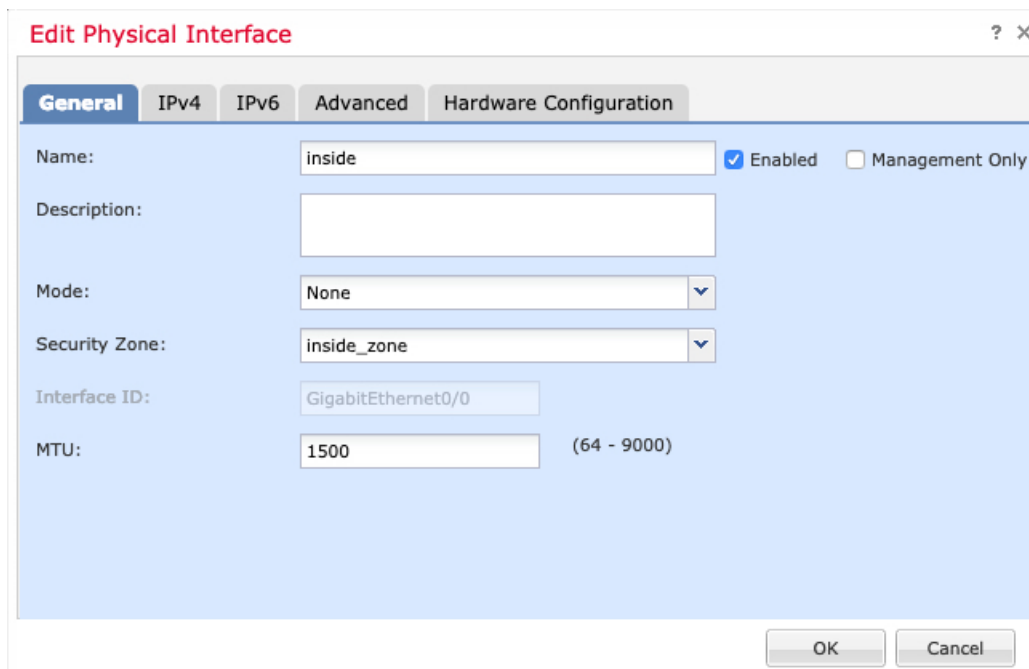
步骤 1 选择 **Devices > Device Management**，然后单击设备的编辑图标（✎）。

步骤 2 单击 **Interfaces**。



步骤 3 单击要用于内部的接口的编辑图标 (✎)。

**General** 选项卡将显示。



- 输入长度最大为 48 个字符的 **Name**。  
例如，将接口命名为 **inside**。
- 选中 **Enabled** 复选框。
- 将 **Mode** 保留为 **None**。
- 从 **Security Zone** 下拉列表选择一个现有的内部安全区域，或者单击 **New** 添加一个新的安全区域。

例如，添加一个名为 **inside\_zone** 的区域。必须将每个接口分配给安全区域和/或接口组。每个接口只能属于一个安全区域，但可以同时属于多个接口组。您可以根据区域或组应用安全策略。例如，您可以将内部接口分配到内部区域，而将外部接口分配到外部区域。然后可以配置访问控制策略，允许流量从内部传到外部，但不允许从外部传入内部。大多数策略仅支持安全区域；您可以在 NAT 策略、预过滤器策略和 QoS 策略中使用区域或接口组。

e) 单击 **IPv4** 和/或 **IPv6** 选项卡。

- **IPv4** - 从下拉列表中选择 **Use Static IP**，然后以斜杠表示法输入 IP 地址和子网掩码。  
例如，输入 **192.168.1.1/24**

- **IPv6** - 为无状态自动配置选中 **Autoconfiguration** 复选框。

f) 单击 **OK**。

**步骤 4** 单击要用于外部的接口的编辑图标 (✎)。

**General** 选项卡将显示。

a) 输入长度最大为 48 个字符的 **Name**。

例如，将接口命名为 **outside**。

b) 选中 **Enabled** 复选框。

c) 将 **Mode** 保留为 **None**。

d) 从 **Security Zone** 下拉列表中选择 一个现有的外部安全区域，或者单击 **New** 添加一个新的安全区域。

例如，添加一个名为 `outside_zone` 的区域。

e) 单击 **IPv4** 和/或 **IPv6** 选项卡。

- **IPv4** - 选择 **Use DHCP**，然后配置以下选填参数：

- **Obtain default route using DHCP** - 从 DHCP 服务器获取默认路由。

- **DHCP route metric** - 分配到所获悉路由的管理距离，介于 1 和 255 之间。获悉的路由的默认管理距离为 1。

The screenshot shows the 'Edit Physical Interface' configuration window with the 'IPv4' tab selected. The 'IP Type' dropdown menu is set to 'Use DHCP'. Below it, the 'Obtain default route using DHCP' checkbox is checked. The 'DHCP route metric' is set to '1', with a range of '(1 - 255)' shown to the right.

- **IPv6** - 为无状态自动配置选中 **Autoconfiguration** 复选框。

f) 点击确定。

**步骤 5** 点击保存。

## 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** 选择 **Devices > Device Management**，然后单击设备的编辑图标（）。

**步骤 2** 选择 **DHCP > DHCP Server**。

**步骤 3** 在 **Server** 页面上单击 **Add**，然后配置以下选项：

The screenshot shows the 'Add Server' dialog box. The 'Interface\*' dropdown menu is set to 'inside'. The 'Address Pool\*' is set to '10.9.7.9-10.9.7.25', with a range of '(2.2.2.10-2.2.2.20)' shown to the right. The 'Enable DHCP Server' checkbox is checked. 'OK' and 'Cancel' buttons are at the bottom.

- **Interface** -- 从下拉列表中选择接口。

- **Address Pool** - DHCP 服务器使用的 IP 地址的范围（从最低到最高）。IP 地址范围必须与选定接口位于相同的子网上，且不能包括接口自身的 IP 地址。
- **Enable DHCP Server** - 在所选接口上启用 DHCP 服务器。

步骤 4 点击确定。

步骤 5 点击保存。

## 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，其将显示在 **Devices > Device Management > Routing > Static Route** 页面上的 **IPv4 Routes** 或 **IPv6 Routes** 表中。

### 过程

步骤 1 选择 **Devices > Device Management**，然后单击设备的编辑图标（✎）。

步骤 2 选择 **Route > Static Route**，单击 **Add Route**，然后设置以下项：

- **Type** - 根据要添加静态路由的类型，单击 **IPv4** 或 **IPv6** 单选按钮。
- **Interface** - 选择出口接口；通常是外部接口。



- **Available Network** - 为 IPv4 默认路由选择 **any-ipv4**，为 IPv6 默认路由选择 **any-ipv6**，然后单击 **Add** 将其移至 **Selected Network** 列表。
- **Gateway** 或 **IPv6 Gateway** - 输入或选择作为此路由的下一个跃点的网关路由器。您可以提供 IP 地址或网络/主机对象。
- **Metric** - 输入到目标网络的跃点数。有效值范围为 1 到 255；默认值为 1。

**步骤 3** 单击 **OK**。

路由即已添加至静态路由表。

The screenshot shows the configuration page for a Static Route on a Cisco Firepower 9000 Series SM-24 Threat Defense device. The interface includes a navigation menu at the top with tabs for Overview, Analysis, Policies, Devices (selected), Objects, AMP, and Intelligence. Below the navigation is a breadcrumb trail: Device Management > NAT > VPN > QoS > Platform Settings > FlexConfig > Certificates. The main content area shows the IP address 10.89.5.20 and a warning: "You have unsaved changes" with Save and Cancel buttons. The left sidebar shows a tree view of routing options, with "Static Route" selected. The main table displays the configuration for the static route:

Network	Interface	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes					
any-ipv4	outside	10.99.10.1	false	1	
▼ IPv6 Routes					

**步骤 4** 点击保存。

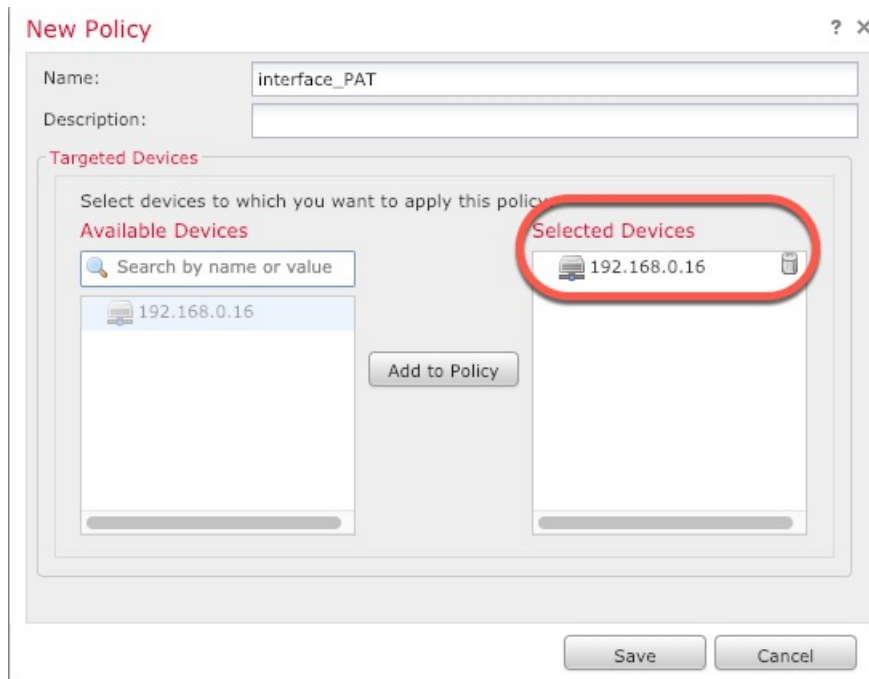
## 配置 NAT

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)。

### 过程

**步骤 1** 选择 **Devices > NAT**，然后单击 **New Policy > Threat Defense NAT**。

**步骤 2** 为策略命名，选择要使用策略的设备，然后单击 **Save**。

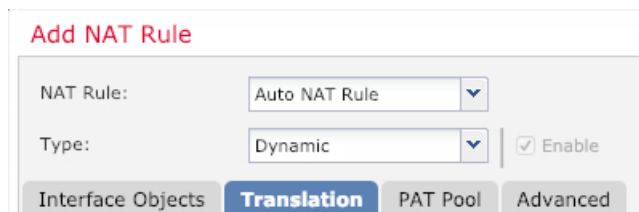


策略即已添加 FMC。您仍然需要为策略添加规则。

**步骤 3** 单击 **Add Rule**。

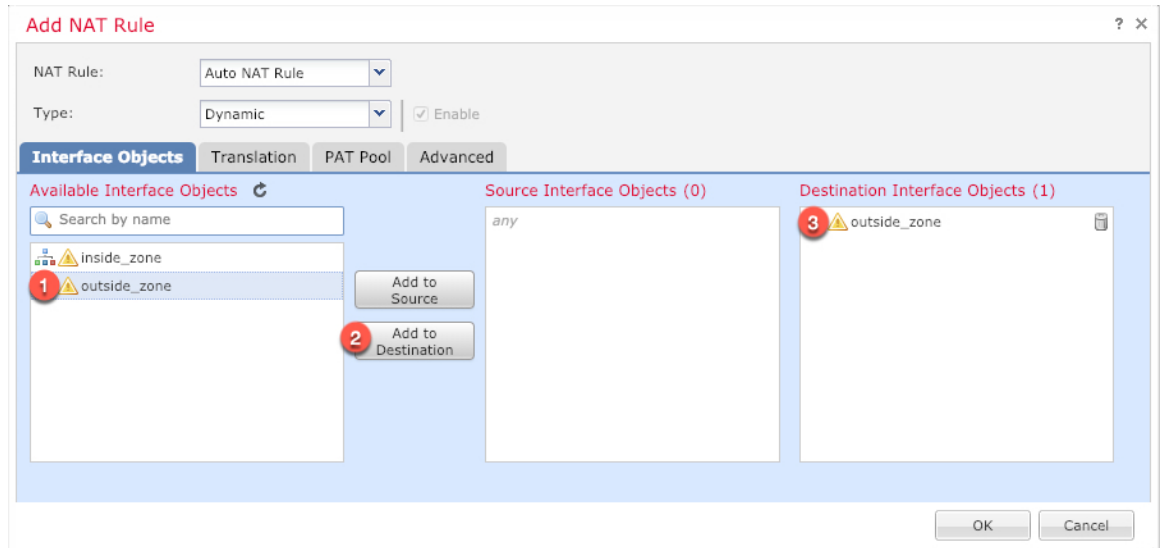
**Add NAT Rule** 对话框将显示。

**步骤 4** 配置基本规则选项：

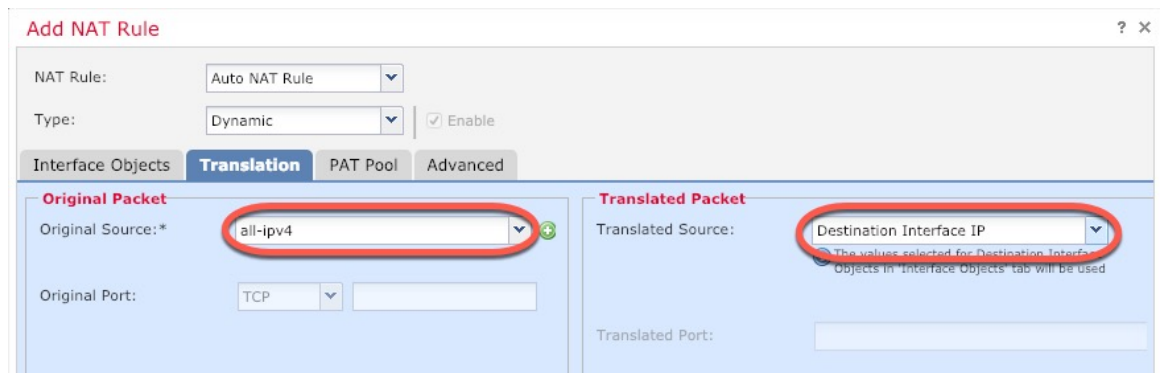


- **NAT Rule** - 选择 **Auto NAT Rule**。
- **Type** - 选择 **Dynamic**。

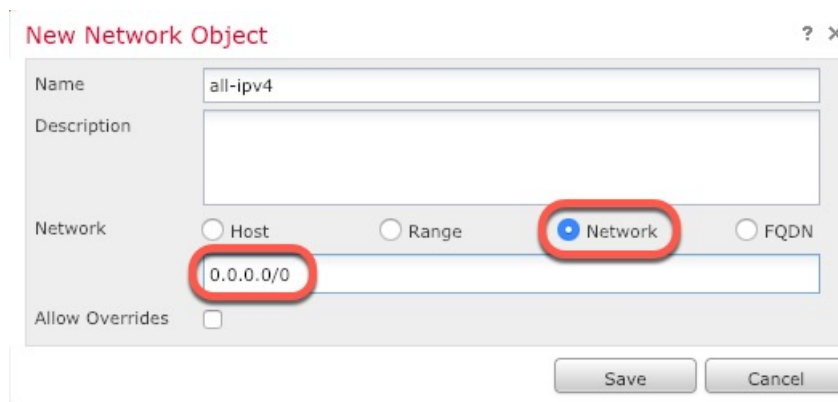
**步骤 5** 在 **Interface Objects** 页面，将 **Available Interface Objects** 区域中的外部区域添加到 **Destination Interface Objects** 区域。



步骤 6 在 **Translation** 页面上配置以下选项：



- **Original Source** - 单击添加图标 (+) 为所有 IPv4 流量添加网络对象 (0.0.0.0/0)。

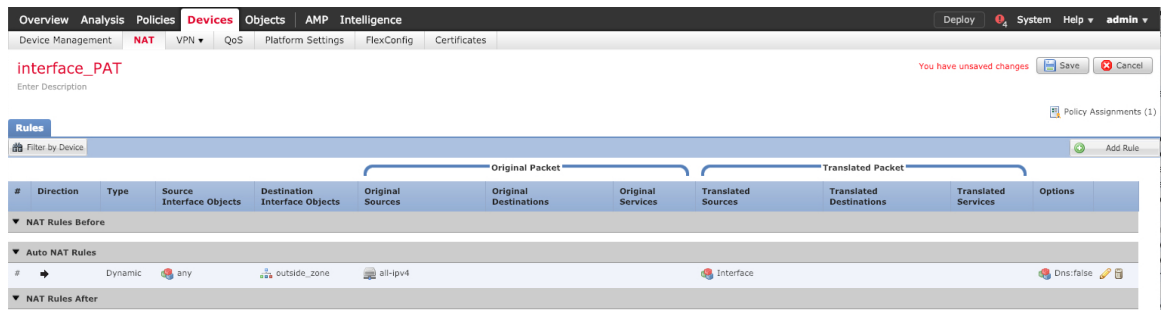


注释 您不能使用系统定义的 **any-ipv4** 对象，因为自动 NAT 规则将 NAT 添加为对象定义的一部分，您无法编辑系统定义的对象。

- **Translated Source** - 选择 **Destination Interface IP**。

步骤 7 单击 **Save** 以添加规则。

规则即已保存至 **Rules** 表。




步骤 8 单击 **NAT** 页面上的 **Save** 以保存更改。

## 允许流量从内部传到外部

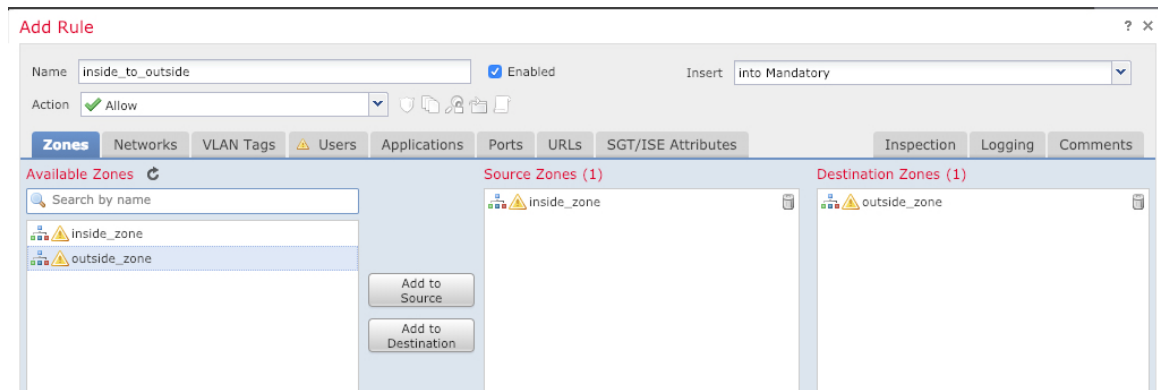
如果您在使用 FMC 注册 FTD 时创建了基本的封锁所有流量访问控制策略，则需要向策略添加规则以允许流量通过设备。以下程序可添加规则以允许从内部区域到外部区域的流量。如有其他区域，请务必添加允许流量到适当网络的规则。

请参阅 [FMC 配置指南](#) 以配置更高级的安全设置和规则。

### 过程

步骤 1 选择 **Policy > Access Policy > Access Policy**，然后单击分配给 FTD 的访问控制策略的编辑图标（）。

步骤 2 单击 **Add Rule** 并设置以下参数：

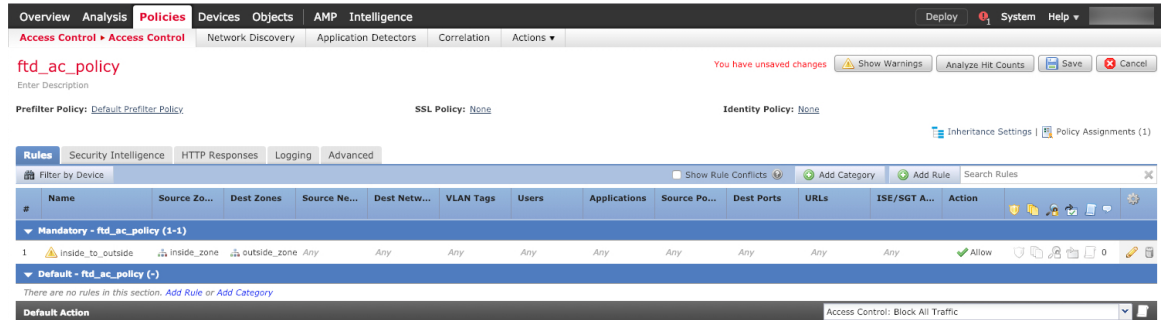


- **Name** - 为此规则命名，例如 **inside\_to\_outside**。
- **Source Zones** - 从 **Available Zones** 中选择内部区域，然后单击 **Add to Source**。
- **Destination Zones** - 从 **Available Zones** 中选择外部区域，然后单击 **Add to Destination**。

其他设置保留原样。

**步骤 3** 单击 **Add**。

规则即已添加至 **Rules** 表。



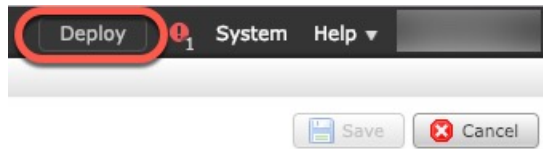
**步骤 4** 点击保存。

## 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

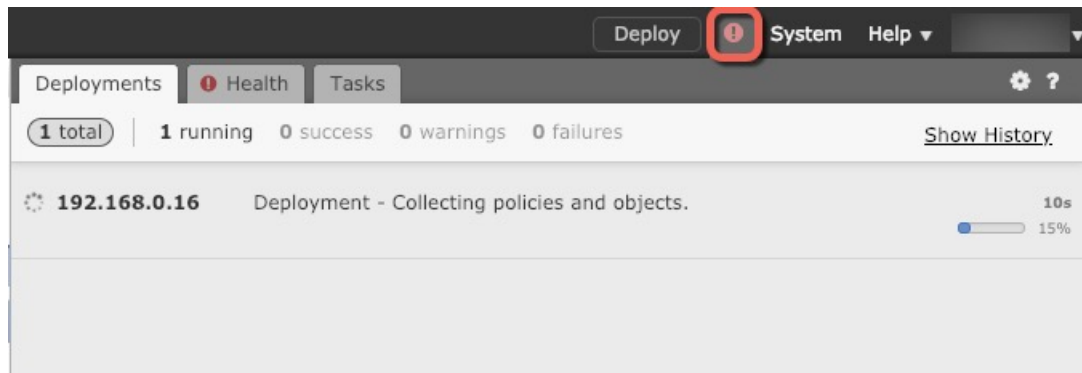
**步骤 1** 单击右上方的 **Deploy**。



**步骤 2** 选择 **Deploy Policies** 对话框中的设备，然后单击 **Deploy**。



**步骤 3** 确保部署成功。单击菜单栏中 **Deploy** 按钮右侧的图标可以查看部署状态。



## 访问 FTD 和 FXOS CLI

使用命令行界面 (CLI) 可设置系统以及对系统进行基本的故障排除。无法通过 CLI 会话配置策略。可以连接到控制台端口以访问 CLI。

可以通过 SSH 连接到 FTD 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。

也可以从 FTD CLI 访问 FXOS CLI，以便进行故障排除。

### 过程

**步骤 1** 要登录 CLI，请将管理计算机连接到控制台端口。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

**注意** 控制台端口上的 CLI 是 FXOS。

**步骤 2** 在出现提示时，登录 FXOS CLI。

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** 访问 FTD CLI。

**connect ftd**

示例:

```
firepower# connect ftd
>
```

登录后，如需了解 CLI 中可用命令的相关信息，请输入 **help** 或 **?**。有关使用信息，请参阅 [Firepower 威胁防御命令参考](#)。

**步骤 4** 要退出 FTD CLI，请输入 **exit** 或 **logout** 命令。

示例:

```
> exit
firepower#
```

**注释** 此时系统会将您重新导向至 FXOS CLI 提示。有关 CLI 中可用命令的相关信息，请输入 **?**。有关使用信息，请参阅 [思科 Firepower FXOS 命令参考](#)。

---

## 断开设备电源

使用 FMC 正确关闭系统非常重要。仅拔掉电源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 Firepower 系统。Firepower 1010 机箱没有外部电源开关。

### 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，点击编辑图标 (✎)。

**步骤 3** 点击设备 (Device) 选项卡。

**步骤 4** 单击系统部分中的关闭设备图标 (🔴)。

**步骤 5** 出现提示时，确认是否要关闭设备。

**步骤 6** 观察电源 LED 和状态 LED 以验证机箱是否已断电 (不亮)。

**步骤 7** 在机箱成功关闭电源后，您可以在必要时拔下电源插头以物理方式断开机箱的电源。

## 后续步骤

要继续配置 FTD，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 FMC 的信息，请参阅 [《Firepower 管理中心配置指南》](#)。