使用管理中心部署威胁防御

本章对您适用吗？

要查看所有可用的应用和管理器，请参阅 哪种应用和管理器适合您？ 。本章适用于威胁防御和管理中心。

本章介绍如何管理管理网络上带 威胁防御 的 管理中心 。 对于 管理中心 位于中央总部的远程分支机构部署，请参阅使用远程管理中心部署威胁防御。

关于防火墙

硬件可以运行威胁防御软件或ASA软件。在威胁防御和ASA之间切换需要您对设备进行重新映像。如果您需要不同于当前安装的软件版本，则还应重新映像。请参阅Cisco Secure Firewall ASA 和 Secure Firewall Threat Defense 重新映像指南。

防火墙会运行被称为 Secure Firewall eXtensible 操作系统 (FXOS) 的底层操作系统。防火墙不支持 FXOS Cisco Secure Firewall 机箱管理器；出于故障排除目的，仅支持受限的 CLI。有关详细信息，请参阅适用于具备 Firepower 威胁防御 的 Firepower 1000/2100 和 Cisco Secure Firewall 3100/4200 的思科 FXOS 故障排除指南。

隐私收集声明-防火墙不要求或主动收集个人身份信息。但是，您可以在配置中使用个人身份信息，例如用户名。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。

- 后续步骤, on page 35

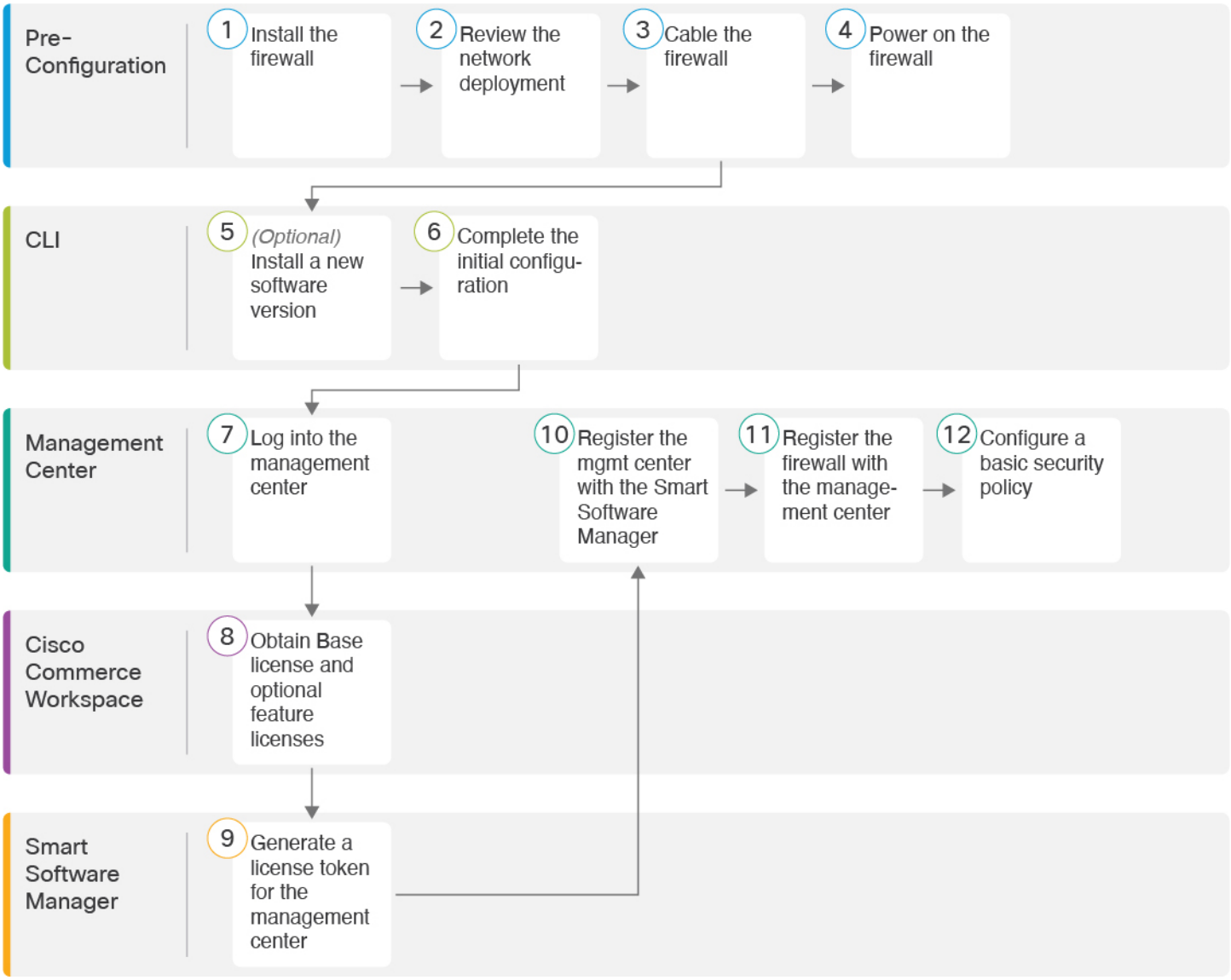
开始之前

部署并执行管理中心的初始配置。《适用于您的型号的入门指南》

端到端任务

请参阅以下任务以部署 威胁防御 和 管理中心。

图 *1:* 端到端任务



1	配置前准备工作	安装防火墙。请参阅硬件安装指南。
2	配置前准备工作	查看网络部署， 第 3 页。
3	配置前准备工作	连接防火墙的电缆， 第 5 页。
4	配置前准备工作	打开防火墙电源， 第 7 页。
5	CLI	（可选）检查软件并安装新版本， 第 8 页。
6	CLI	使用 CLI 完成威胁防御初始配置， 第 10 页。
7	管理中心	登录管理中心， 第 13 页。
8	Cisco Commerce Workspace	购买基本许可证和可选功能许可证 (获取管理中心的许可证， 第 13 页)。
9	智能软件管理器	为 管理中心 (获取管理中心的许可证， 第 13 页) 生成许可证令牌。
10	管理中心	向智能许可证服务器 (获取管理中心的许可证， 第 13 页) 注册管理中心。
11	管理中心	向管理中心注册威胁防御， 第 15 页。
12	管理中心	配置基本安全策略， 第 18 页。

查看网络部署

管理接口

管理中心 只能在管理接口上与 威胁防御 通信。

专用管理接口是一种具有自己的网络设置的特殊接口：

- 默认情况下，管理 1/1 接口已启用并配置为 DHCP 客户端。如果您的网络不包括 DHCP 服务器，您可以在控制台端口的初始设置期间，将管理接口设置为使用静态 IP 地址。
- 威胁防御和 管理中心 都需要从管理接口接入互联网以用于许可和更新。

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。

数据接口

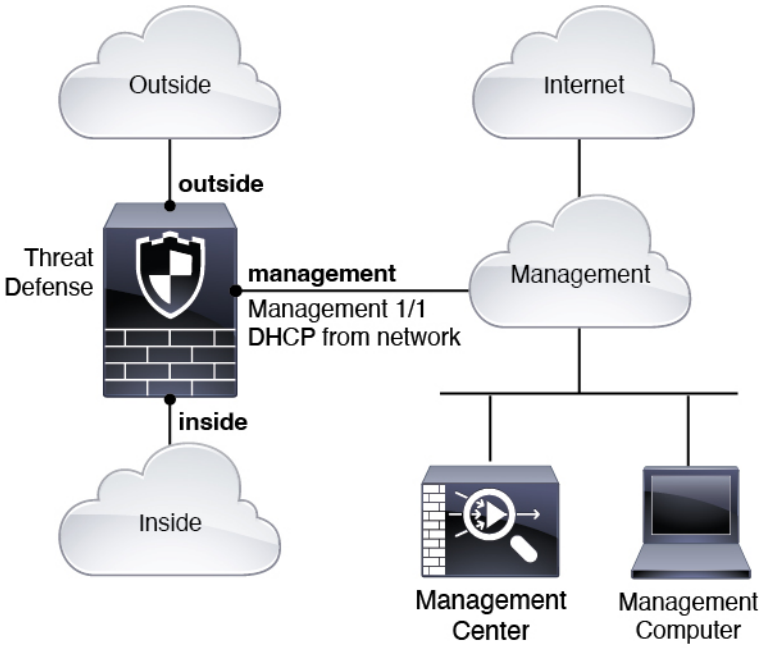
您可以在将 威胁防御 连接到 管理中心 后配置其他接口。

典型的单独管理网络部署

下图显示防火墙的一种典型网络部署，其中 威胁防御、管理中心 和管理计算机连接到管理网络。

管理网络具有互联网接入路径以用于许可和更新。

图 *2:* 单独的管理网络



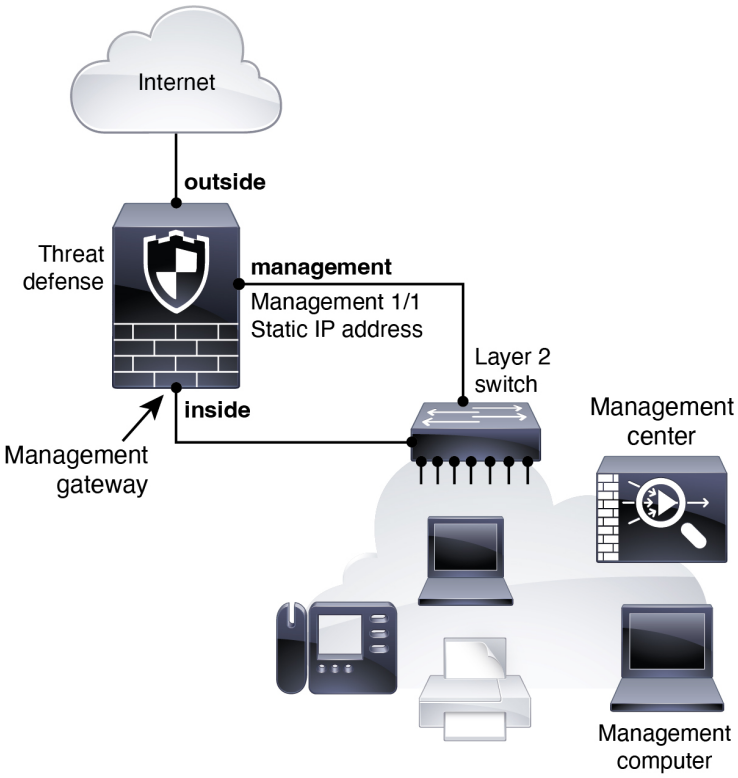
典型边缘网络部署

下图显示了防火墙的典型网络部署，其中：

- 内部充当管理和 管理中心 的互联网网关。
- 管理 1/1 通过 第 2 层交换机连接到内部接口。
- 管理中心 和管理计算机连接到交换机。

因为管理接口独立于 威胁防御上的其他接口路由，因此这种直接连接是允许的。

图 3: 边缘网络部署



连接防火墙的电缆

要在 Cisco Secure Firewall 4200 中按建议方案之一进行布线，请参阅以下步骤。

注释 也可以使用其他拓扑，而部署情况会因基本逻辑网络连接、端口、地址和配置要求有所不同。

开始之前

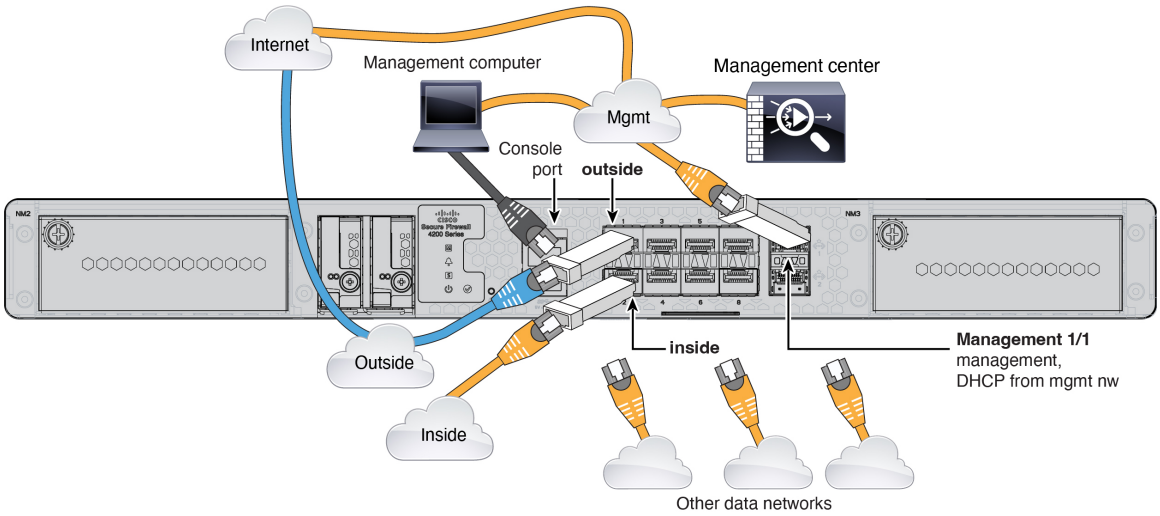
- 将 SFP 安装到管理和数据接口端口 - 内置端口是需要 SFP 模块的 1/10/25-Gb SFP 端口。
- 获取控制台电缆 - 默认情况下，防火墙不随附控制台电缆，因此您需要购买第三方 USB 转 RJ-45 串行电缆。

过程

步骤 1 安装机箱。请参阅硬件安装指南。

步骤 2 连接单独管理网络的电缆：

图 *4:* 连接单独管理网络的电缆



a) 使用电缆将以下内容连接到您的管理网络：

- 管理 1/1 接口

  如果 管理中心 具有专用的事件接口，则管理 1/2 接口可用作单独的事件接口。有关详细信息，请参阅 管理中心 管理员和设备配置指南 。

- Cisco Secure Firewall Management Center
- 管理计算机

b) 将管理计算机连接到控制台端口。如果不使用 SSH 访问管理接口，则需要使用控制台端口访问 CLI 进行初始设置。

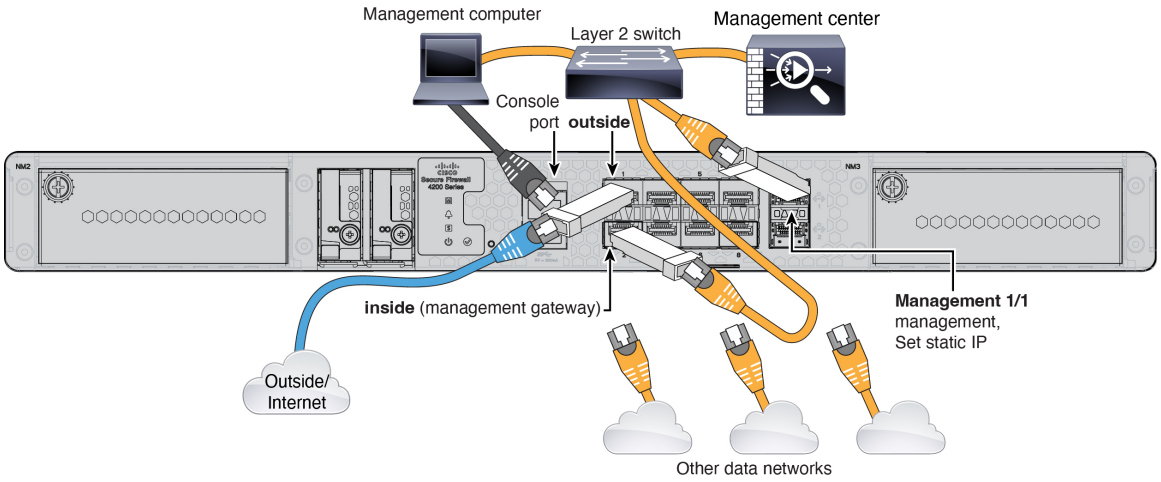
c) 将内部接口（例如，以太网 1/2）连接到内部路由器。

d) 将外部接口（例如，以太网 1/1）连接到外部路由器。

e) 将其他网络连接到其余接口。

步骤 3 为实施边缘部署进行布线：

图 *5:* 进行边缘部署布线



a) 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

  如果 管理中心 具有专用的事件接口，则管理 1/2 接口可用作单独的事件接口。有关详细信息，请参阅 管理中心 管理员和设备配置指南 。
- Cisco Secure Firewall Management Center
- 管理计算机

b) 将管理计算机连接到控制台端口。如果不使用 SSH 访问管理接口，则需要使用控制台端口访问 CLI 进行初始设置。

c) 将外部接口（例如，以太网 1/1）连接到外部路由器。

d) 将其他网络连接到其余接口。

打开防火墙电源

系统电源由位于防火墙后部的摇杆电源开关控制。电源开关以软通知开关形式实施，支持平稳地关闭系统以降低系统软件及数据损坏的风险。

注释 首次启动 威胁防御时，初始化大约需要 15 到 30 分钟。

开始之前

为防火墙提供可靠的电源（例如，使用不间断电源 (UPS)）非常重要。未事先关闭就断电可能会导致严重的文件系统损坏。后台始终有许多进程在运行，因此断电会使得系统无法正常关闭。

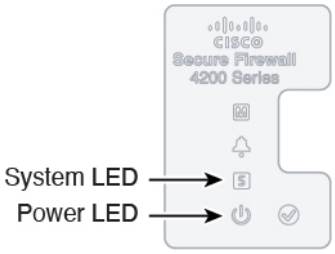
过程

步骤 1 将电源线一端连接到防火墙，另一端连接到电源插座。

步骤 2 使用位于机箱背面电源线旁边的标准摇杆型电源开关打开电源。

步骤 3 检查防火墙背面的电源 LED；如果该 LED 呈绿色稳定亮起，表示防火墙已接通电源。

图 *6:* 系统和电源 *LED*



步骤 4 检查防火墙背面的系统 LED；其呈绿色稳定亮起之后，系统已通过通电诊断。

注释 将开关从开切换到关时，系统可能需要几秒钟才会最终关闭。在此期间，机箱前面的电源 LED 将闪烁绿色。在电源 LED 完全关闭之前，请勿拔出电源。

（可选）检查软件并安装新版本

要检查软件版本并在必要时安装不同的版本，请执行以下步骤。我们建议您在配置防火墙之前安装目标版本。或者，您也可以在启动并运行后执行升级，但升级（保留配置）可能需要比按照此程序花费更长的时间。

我应该运行什么版本？

思科建议运行软件下载页面上的版本号旁边标有金色星号的 Gold Star 版本。您还可以参考 https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html 中所述的发布策略；例如，此公告描述短期版本编号（包含最新功能）、长期版本编号（较长时间的维护版本和补丁）或额外长期版本编号（最长期限的维护版本和补丁，用于政府认证）。

过程

步骤 1 连接到控制台端口。有关详细信息，请参阅访问威胁防御和FXOS CLI，第 33 页。

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

您连接到 FXOS CLI。第一次输入登录时，系统会提示您更改密码。此密码也用于 SSH 的威胁防御登录。

注释 如果密码已更改，但您不知道，则必须执行出厂重置以将密码重置为默认值。有关出厂重置程序的信息，请参阅 FXOS 故障排除指南 。

示例：

```
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 2 在 FXOS CLI 中，显示正在运行的版本。

scope ssa

show app-instance

示例：

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name     Slot ID    Admin State     Operational State    Running Version Startup
 Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- ------------------
ftd                  1          Enabled         Online               7.6.0.65        7.6.0.65
        Not Applicable
```

步骤 3 如果要安装新版本，请执行这些步骤。

a) 如果要为管理接口设置静态 IP 地址，请参阅使用 CLI 完成威胁防御初始配置 ， 第 10 页。默认情况下，管理接口将使用 DHCP。

您需要从可通过管理接口访问的服务器下载新的映像。

b) 执行《FXOS 故障排除指南》中的重新映像程序。

防火墙重新启动后，您可以再次连接到 FXOS CLI。

使用 CLI 完成威胁防御初始配置

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。

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。

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。

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。有关重新映像程序的信息，请参阅 FXOS 故障排除指南。

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 如果在控制台端口上连接到 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 Cisco Secure Firewall Threat Defense 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。

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 网关** - 为管理网络上的管理 1/1 设置网关 IP 地址。在网络部署部分中显示的边缘部署示例中，内部接口用作管理网关。在这种情况下，应将网关 IP 地址设置为意向内部接口 IP 地址；后期必须使用 管理中心 设置内部 IP 地址。**data-interfaces** 设置仅适用于 远程 管理中心 管理。
- **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。
- **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。

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 change the password for 'admin' to continue.
Enter new password: ********
Confirm new password: ********
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 [192.168.45.45]: 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]: ftd-1.cisco.com
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 ftd-1.cisco.com
Setting static IPv4: 10.10.10.15 netmask: 255.255.255.192 gateway: 10.10.10.1 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'
```

```
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**} *regkey* [*nat_id*]

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} - 指定 管理中心 的 FQDN 或 IP 地址。如果 管理中心 不能直接寻址，请使用 **DONTRESOLVE** 并指定 *nat_id*。必须至少有一个设备（管理中心 或 威胁防御）具有可访问的 IP 地址，才能在两个设备之间建立双向 SSL 加密的通信通道。如果在此命令中指定 **DONTRESOLVE**，则 威胁防御 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。如果将 管理中心 设置为 **DONTRESOLVE**，则需要指定它。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。

Example:

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

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：

Example:

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

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：

Example:

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

What to do next

将防火墙注册到 管理中心。

登录管理中心

使用管理中心配置并监控威胁防御。

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 点击登录。

获取管理中心的许可证

所有许可证都由管理中心提供给威胁防御。您可以购买下列许可证：

- **基础版**-（必需） 基础版 许可证。
- **IPS** - 安全情报和下一代 IPS
- **恶意软件 防御**-恶意软件 防御
- **URL 过滤**—URL 过滤
- **Cisco Secure 客户端**-Secure Client Advantage、Secure Client Premier 或 Secure Client VPN Only
- **运营商** - Diameter、GTP/GPRS、M3UA、SCTP

有关思科许可的更详细概述，请访问 cisco.com/go/licensingguide

开始之前

- 拥有一个智能软件管理器帐户。

  如果您还没有账户，请点击此链接以设置新账户。通过思科智能软件管理器，您可以为组织创建一个账户。

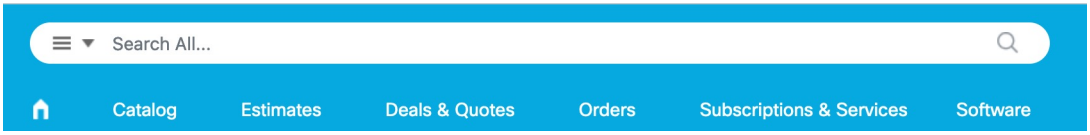
- 您的智能软件许可帐户必须符合强加密 (3DES/AES) 许可证的要求，才能使用某些功能（已使用导出合规性标志启用）。

过程

步骤 1 请确保智能许可帐户包含所需的可用许可证。

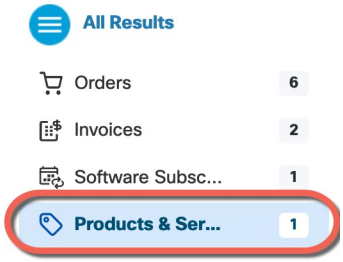
当您从思科或经销商那里购买设备时，您的许可证应该已链接到您的智能软件许可证帐户。但是，如果您需要自己添加许可证，则请使用思科商务工作空间上的**搜索全部 (Search All)** 字段。

图 7: 许可证搜索



从结果中选择**产品和服务 (Products & Services)**。

图 8: 成果



搜索以下许可证 PID：

注释 如果未找到 PID，您可以手动将 PID 添加到订单中。

- 基础版 许可证：
  - L-FPR4215-BSE=
  - L-FPR4225-BSE=
  - L-FPR4245-BSE=
- IPS、恶意软件 防御和 URL 许可证组合：
  - L-FPR4215T-TMC=

- L-FPR4225T-TMC=
- L-FPR4245T-TMC=

当您将上述 PID 之一添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：

- L-FPR4215T-TMC-1Y
- L-FPR4215T-TMC-3Y
- L-FPR4215T-TMC-5Y
- L-FPR4225T-TMC-1Y
- L-FPR4225T-TMC-3Y
- L-FPR4225T-TMC-5Y
- L-FPR4245T-TMC-1Y
- L-FPR4245T-TMC-3Y
- L-FPR4245T-TMC-5Y

- 运营商许可证：
  - L-FPR4200K-FTD-CAR=
- Cisco Secure 客户端-请参阅 思科安全客户端订购指南。

步骤 2 如果尚未执行此操作，请向智能许可服务器注册管理中心。

注册需要您在智能软件管理器中生成注册令牌。有关详细说明，请参阅 《Cisco Secure Firewall Management Center 管理指南》 。

向管理中心注册威胁防御

使用设备 IP 地址或主机名将威胁防御手动注册到管理中心。

开始之前

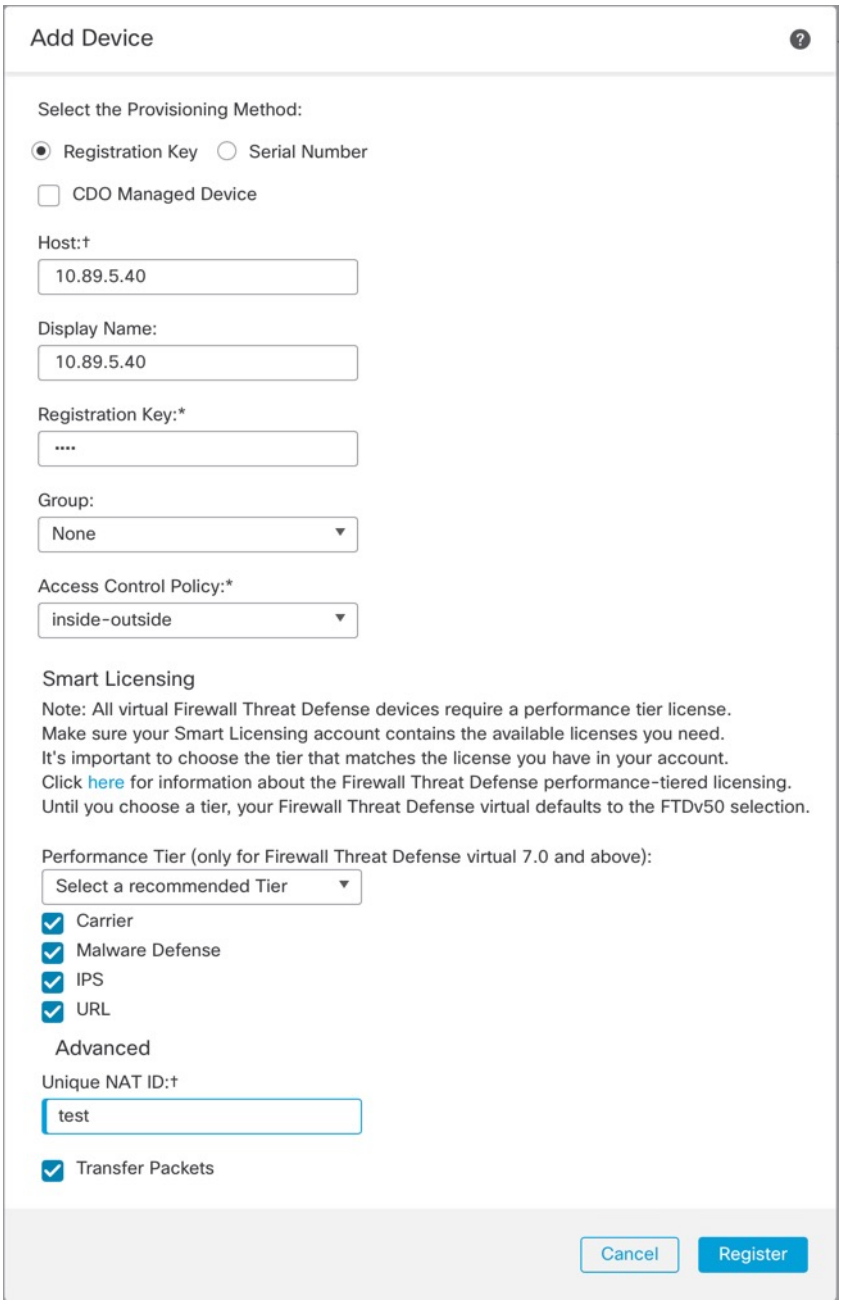
过程

步骤 1 在 管理中心 上，选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 从**添加**下拉列表中，选择**添加设备**。

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



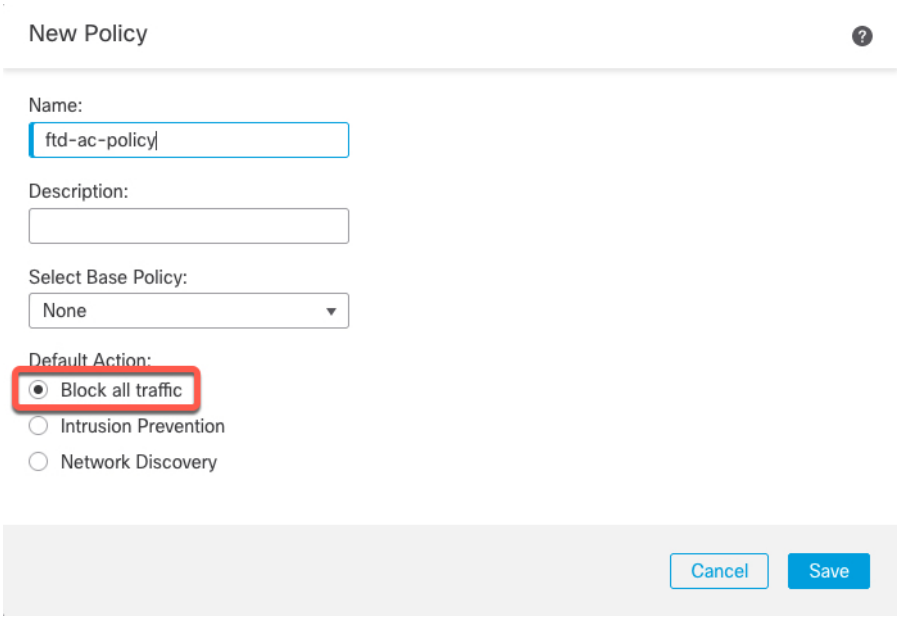
设置以下参数：

- **主机 (Host)** - 输入要添加的 威胁防御 的 IP 地址或主机名。如果在 威胁防御 初始配置中同时指定了 管理中心 IP 地址和 NAT ID，可以将此字段留空。

  注释 在 HA 环境中，当两个管理中心都位于 NAT 之后时，则可以在主管理中心中注册威胁防御而无需主机 IP 或名称。但是，要在辅助 管理中心 中注册 威胁防御，则必须提供 威胁防御 的 IP 地址或主机名。

- **显示名称 (Display Name)** - 输入要在管理中心中显示的威胁防御的名称。
- **注册密钥 (Registration Key)** - 输入您在威胁防御初始配置中指定的注册密钥。
- **域 (Domain)** - 如果有多域环境，请将设备分配给分叶域。
- **组 (Group)** - 如果在使用组，则将其分配给设备组。
- **访问控制策略 (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**新建策略 (Create new policy)**，然后选择**阻止所有流量 (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 30 页。

图 *10:* 新建策略



- **智能许可**—为要部署的功能分配所需的智能许可证。**注意：** 在添加设备后，您可以从 **系统 > 许可证 > 智能许可证** 页面应用 Secure Client 远程访问 VPN 许可证。
- **唯一 NAT ID (Unique NAT ID)** - 指定您在 威胁防御 初始配置中指定的 NAT ID。
- **转移数据包 (Transfer Packets)** - 可让设备将数据包传输至 管理中心。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，只有事件信息会发送到 管理中心，数据包数据不发送。

步骤 3 单击**注册 (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 威胁防御注册失败，请检查以下项：

- Ping - 访问威胁防御 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 威胁防御 管理 IP 地址，请使用 **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）。可以在管理中心使用 **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。

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，第 18 页。
2	配置 DHCP 服务器，第 23 页。
3	添加默认路由，第 25 页。
4	配置 NAT，第 27 页。
5	允许流量从内部传到外部，第 30 页。
6	部署配置，第 31 页。

配置接口

启用 威胁防御接口，为其分配安全区域并设置 IP 地址。还要配置分支接口。。

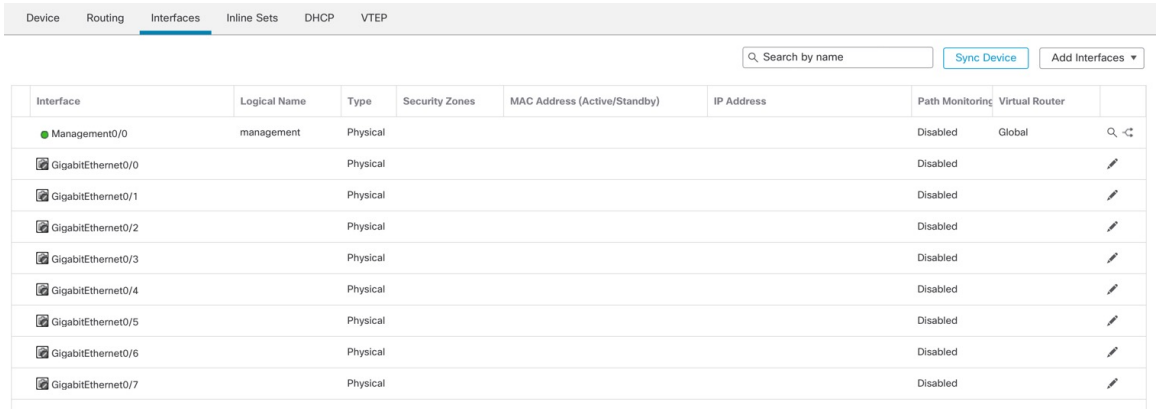
以下示例使用 DHCP 在接口内部配置了一个路由模式（含静态地址），并在接口外部配置了一个路由模式。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**，然后点击防火墙的**编辑**（）。

步骤 2 点击**接口 (Interfaces)**。

图 *11:* 接口



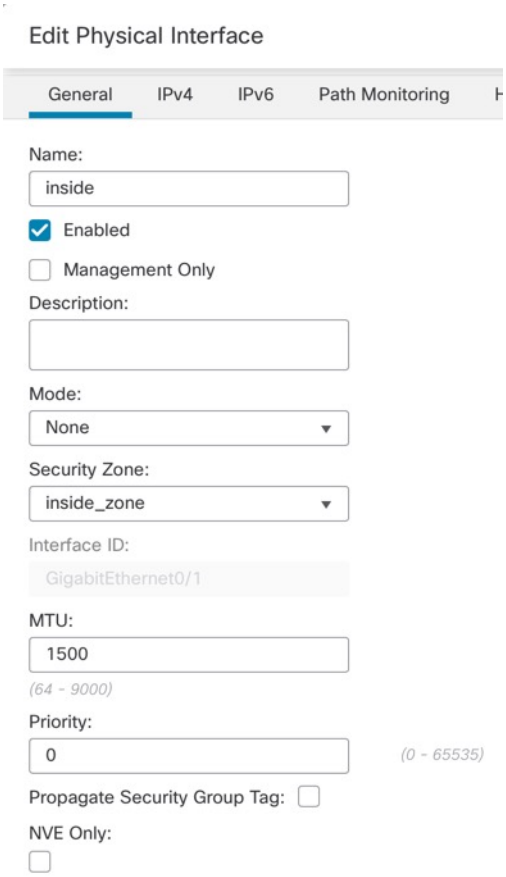
步骤 3 要从 40-Gb 或更大的接口创建分支端口，请点击该接口的 **中断** 图标。

如果您已经在配置中使用了全接口，则必须在继续创建分支之前删除该配置。

步骤 4 点击要用于内部的接口的**编辑**（）。

此时将显示**一般 (General)** 选项卡。

图 *12:*“常规”选项卡



a) 输入长度最大为 48 个字符的**名称 (Name)**。

例如，将接口命名为 **inside**。

b) 选中**启用 (Enabled)** 复选框。

c) 将**模式 (Mode)** 保留为**无 (None)**。

d) 从**安全区域 (Security Zone)** 下拉列表中选择一个现有的内部安全区域，或者点击**新建 (New)** 添加一个新的安全区域。

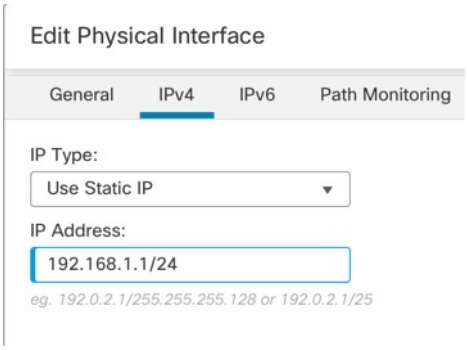
例如，添加一个名为 **inside_zone** 的区域。必须将每个接口分配给安全区域和/或接口组。每个接口只能属于一个安全区域，但可以同时属于多个接口组。您可以根据区域或组应用安全策略。例如，您可以将内部接口分配到内部区域，而将外部接口分配到外部区域。然后可以配置访问控制策略，允许流量从内部传到外部，但不允许从外部传入内部。大多数策略仅支持安全区域；您可以在 NAT 策略、预过滤器策略和 QoS 策略中使用区域或接口组。

e) 点击 **IPv4** 和/或 **IPv6** 选项卡。

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

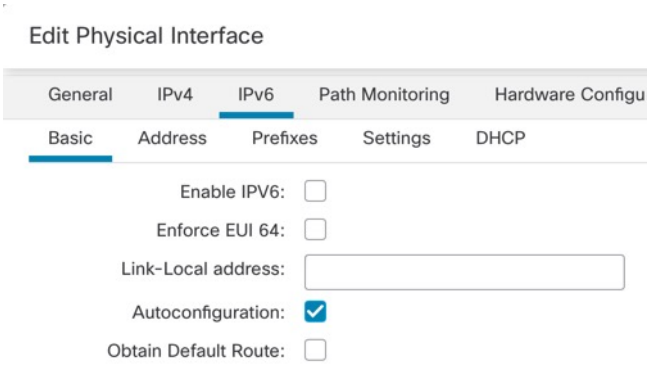
  例如，输入 **192.168.1.1/24**

图 *13: IPv4* 选项卡



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

图 *14: IPv6* 选项卡

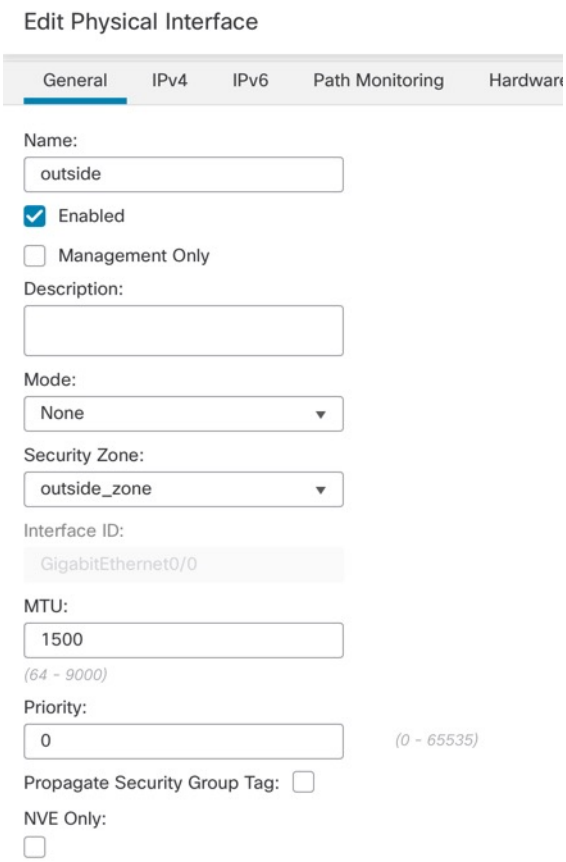


f) 点击**确定 (OK)**。

步骤 5 点击要用于外部的接口的 **编辑**（✎）。

此时将显示**一般 (General)** 选项卡。

图 *15:*“常规”选项卡



a) 输入长度最大为 48 个字符的**名称 (Name)**。

例如，将接口命名为 **outside**。

b) 选中**启用 (Enabled)** 复选框。

c) 将**模式 (Mode)** 保留为**无 (None)**。

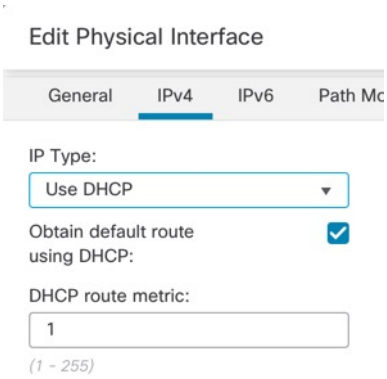
d) 从**安全区域 (Security Zone)** 下拉列表中选择一个现有的外部安全区域，或者点击**新建 (New)** 添加一个新的安全区域。

例如，添加一个名为 **outside_zone** 的区域。

e) 点击 **IPv4** 和/或 **IPv6** 选项卡。

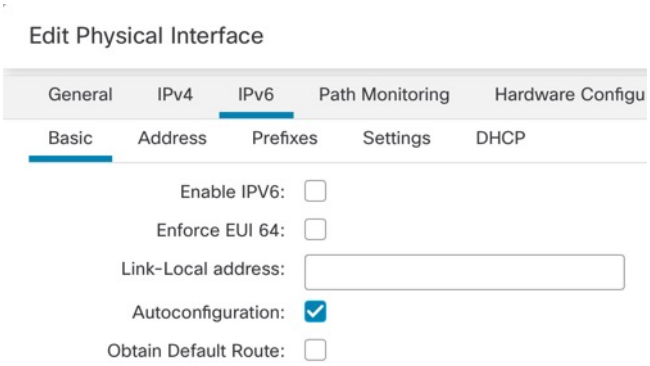
- **IPv4** - 选择**使用 DHCP (Use DHCP)**，然后配置以下选填参数：
  - **使用 DHCP 获取默认路由 (Obtain default route using DHCP)** - 从 DHCP 服务器获取默认路由。
  - **DHCP 路由指标 (DHCP route metric)** - 分配到所获悉路由的管理距离，介于 1 和 255 之间。获悉的路由的默认管理距离为 1。

图 *16: IPv4* 选项卡



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

图 *17: IPv6* 选项卡



f) 点击**确定 (OK)**。

步骤 6 点击**保存 (Save)**。

配置 DHCP 服务器

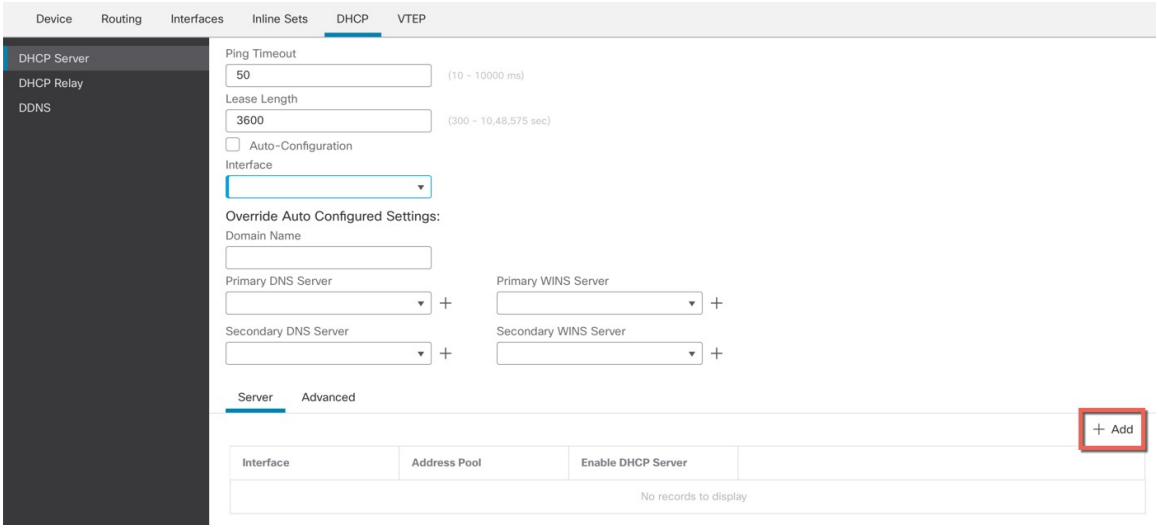
如果希望客户端使用 DHCP 从 威胁防御处获取 IP 地址，请启用 DHCP 服务器。

过程

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

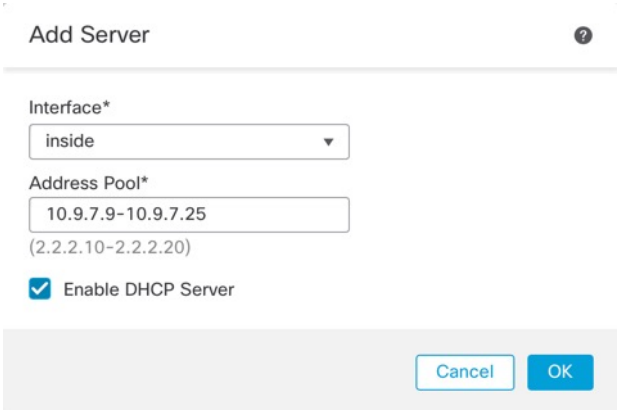
步骤 2 选择 **DHCP** > **DHCP 服务器 (DHCP Server)**。

图 *18: DHCP* 服务器



步骤 3 在服务器 (Server） 页面上点击添加 (Add)，然后配置以下选项：

图 *19:* 添加服务器



- 接口 (Interface) - 从下拉列表中选择接口。
- 地址池 (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。
- 启用 DHCP 服务器 (Enable DHCP Server) - 在所选接口上启用 DHCP 服务器。

步骤 4 点击确定 (OK)。

步骤 5 点击保存 (Save)。

添加默认路由

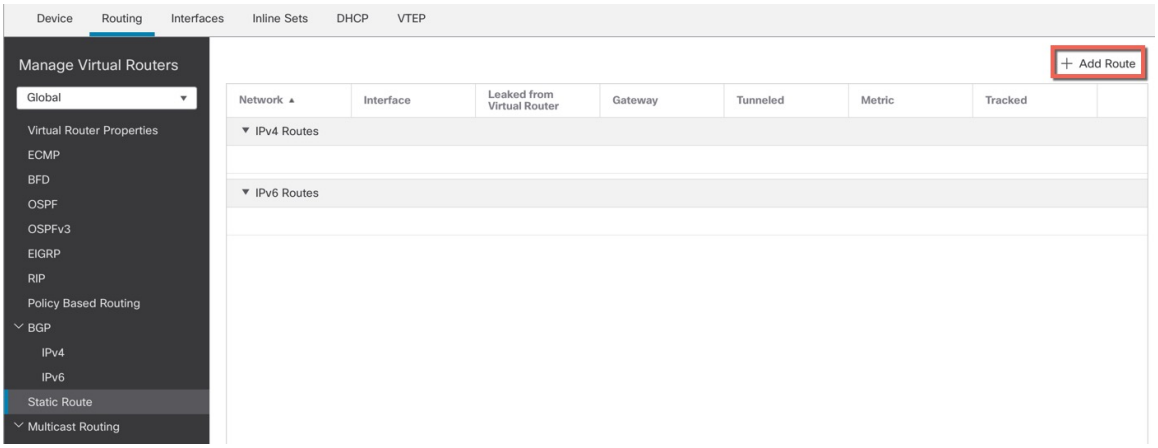
默认路由通常指向可从外部接口访问的上游路由器。如果您将 DHCP 用作外部接口，则您的设备可能已经收到了默认路由。如果需要手动添加路由，则遵照此程序执行。如果收到来自 DHCP 服务器的默认路由，其将显示在**设备 (Devices)** > **设备管理 (Device Management)** > **路由 (Routing)** > **静态路由 (Static Route)** 页面上的 **IPv4 路由 (IPv4 Routes)** 或 **IPv6 路由 (IPv6 Routes)** 表中。

过程

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

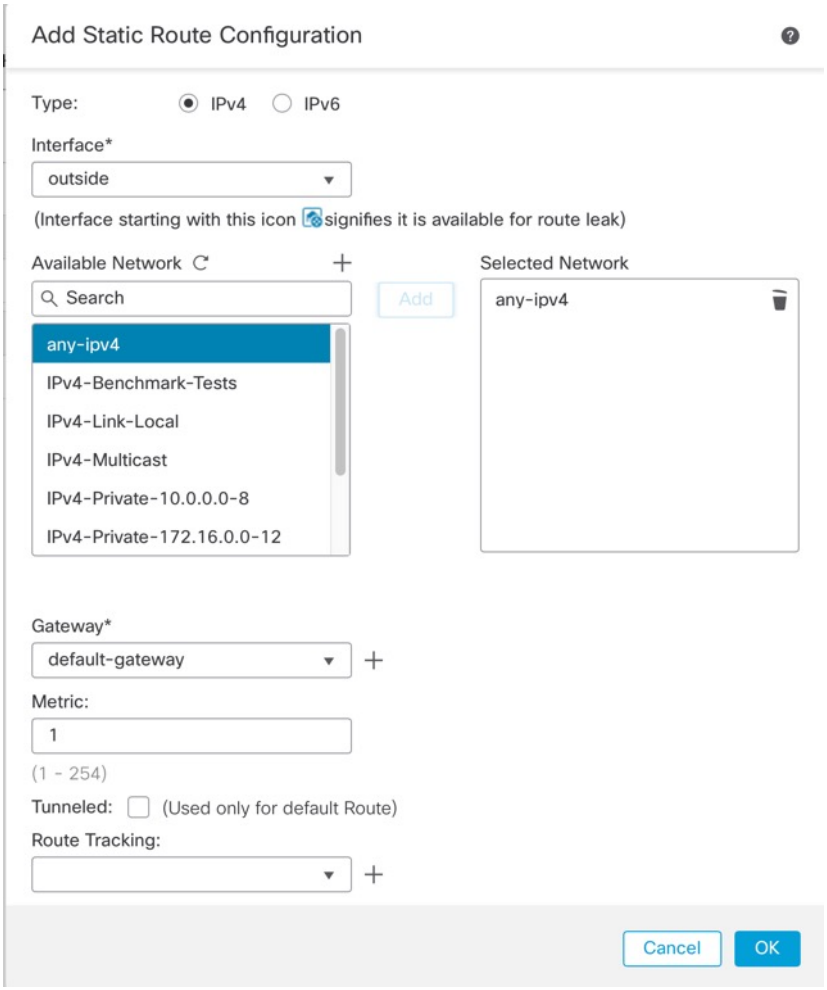
步骤 2 选择 **路由** > **静态路由**。

图 *20:* 静态路由



步骤 3 点击 **添加路由**，然后设置以下参数：

图 *21:* 添加静态路由配置



- **类型 (Intrusion)** - 根据要添加静态路由的类型，点击 **IPv4** 或 **IPv6** 单选按钮。
- **接口 (Interface)** - 选择出口接口；通常是外部接口。
- **可用网络 (Available Network)** - 为 IPv4 默认路由选择 **any-ipv4**，为 IPv6 默认路由选择 **any-ipv6**，然后点击**添加 (Add)** 将其移至**选定网络 (Selected Network)** 列表。
- **网关 (Gateway)** 或 **IPv6 网关 (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。
- **指标 (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 4 点击**确定 (OK)**。

路由即已添加至静态路由表。

步骤 5 点击**保存 (Save)**。

配置 NAT

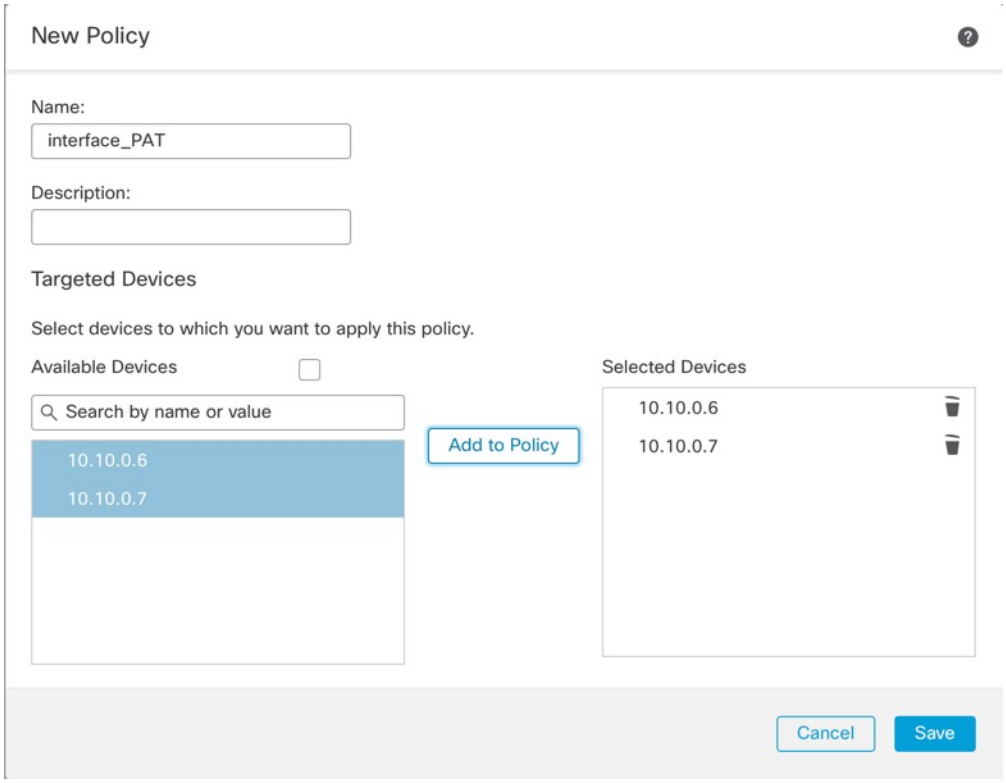
典型的 NAT 规则会将内部地址转换为外部接口 IP 地址上的端口。这类 NAT 规则称为接口端口地址转换 *(PAT)*。

过程

步骤 1 选择**设备 (Devices)** > **NAT**，然后点击**新建策略 (New Policy)** > **威胁防御 NAT (Threat Defense NAT)**。

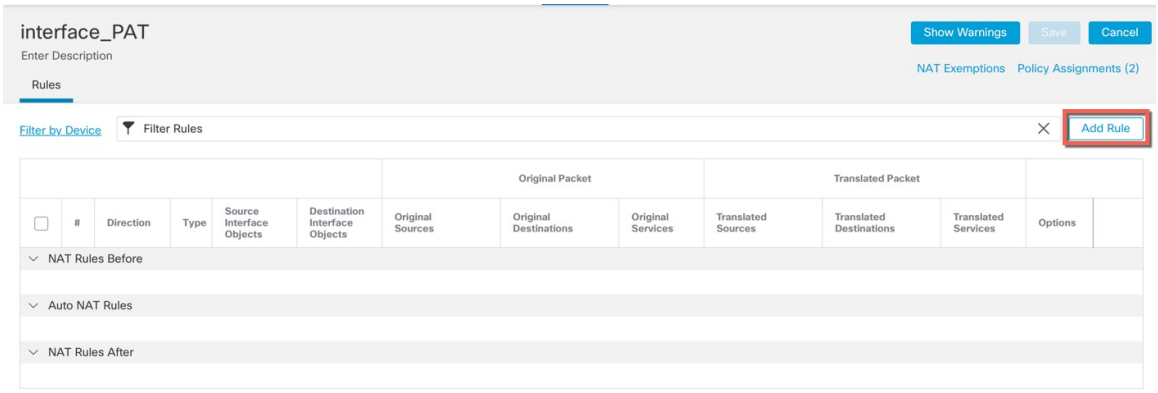
步骤 2 为策略命名，选择要使用策略的设备，然后点击**Save**。

图 *22:* 新建策略



策略即已添加 管理中心。您仍然需要为策略添加规则。

图 *23: NAT* 策略

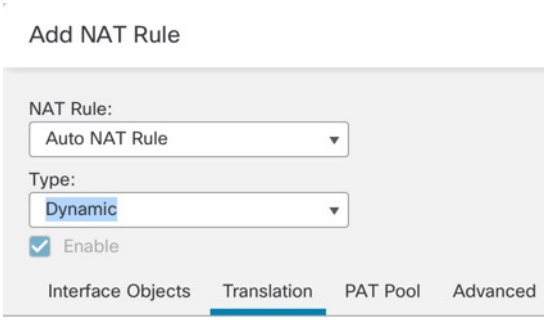


步骤 3 点击添加规则 **(Add Rule)**。

Add NAT Rule 对话框将显示。

步骤 4 配置基本规则选项：

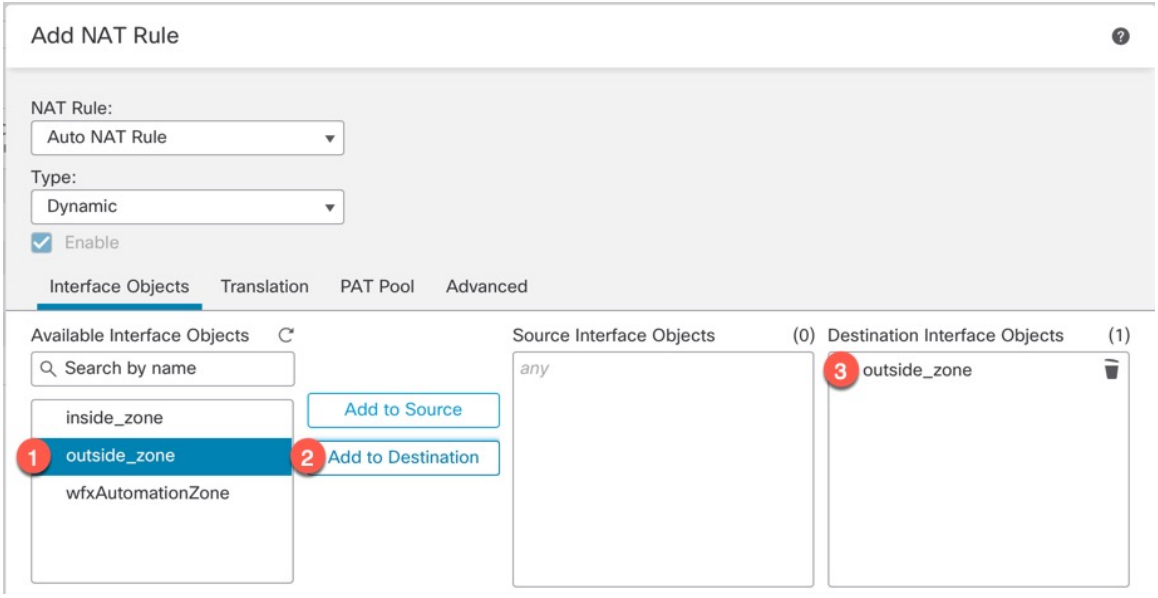
图 *24:* 基本规则选项



- **NAT 规则 (NAT Rule)** - 选择**自动 NAT 规则 (Auto NAT Rule)**。
- **类型 (Type)** - 选择**动态 (Dynamic)**。

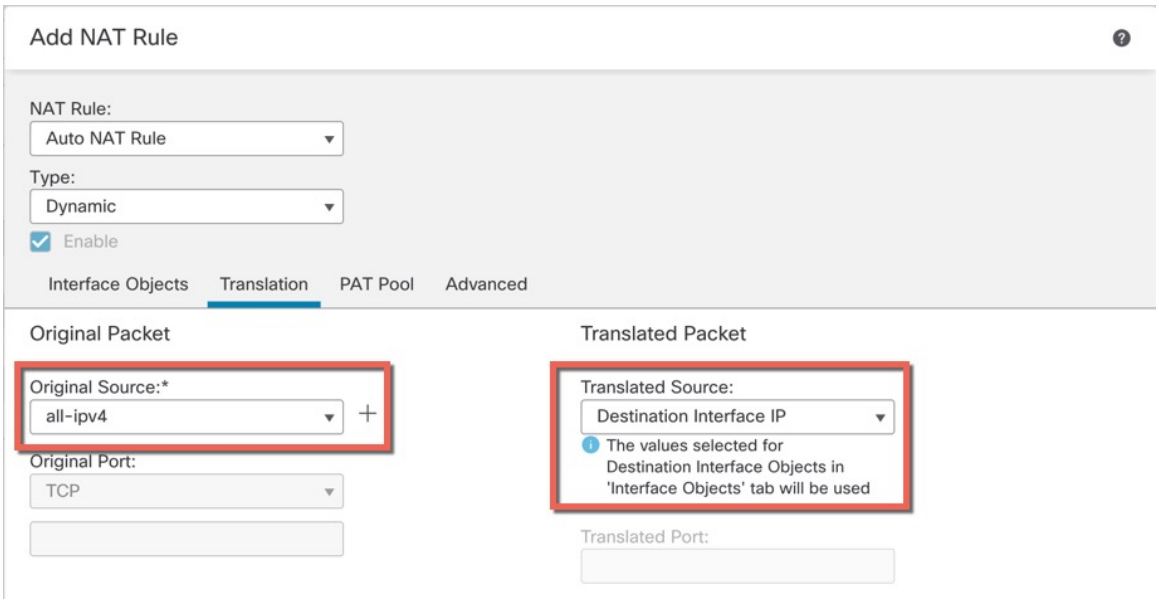
步骤 5 在 **Interface Objects** 页面，将 **Available Interface Objects** 区域中的外部区域添加到 **Destination Interface Objects** 区域。

图 *25:* 接口对象



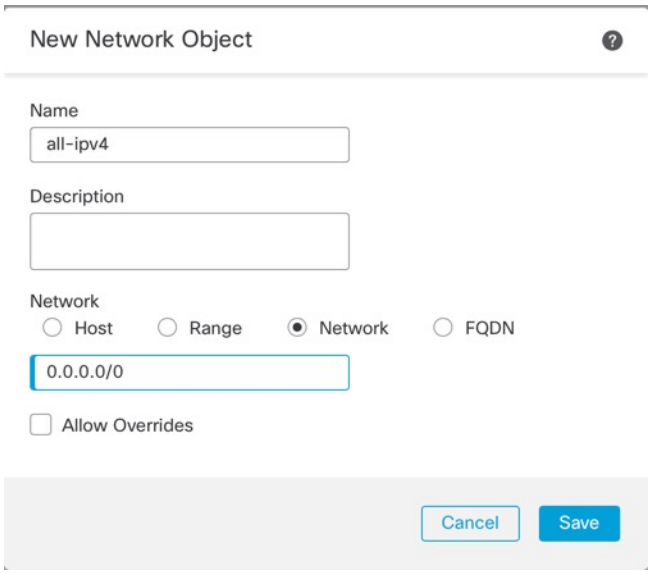
步骤 6 在转换 **(Translation)** 页面上配置以下选项：

图 *26:* 转换



- 原始源-点击 添加（+） 为所有 IPv4 流量添加网络对象 (**0.0.0.0/0**)。

图 *27:* 新的网络对象



注释 您不能使用系统定义的**any-ipv4**对象，因为自动NAT规则在对象定义过程中添加NAT，并且您无法编辑系统定义的对象。

- **转换的源 (Translated Source)** - 选择**目标接口 IP (Destination Interface IP)**。

步骤 7 点击**保存 (Save)** 以添加规则。

规则即已保存至 **Rules** 表。

步骤 8 点击 **NAT** 页面上的**保存 (Save)** 以保存更改。

允许流量从内部传到外部

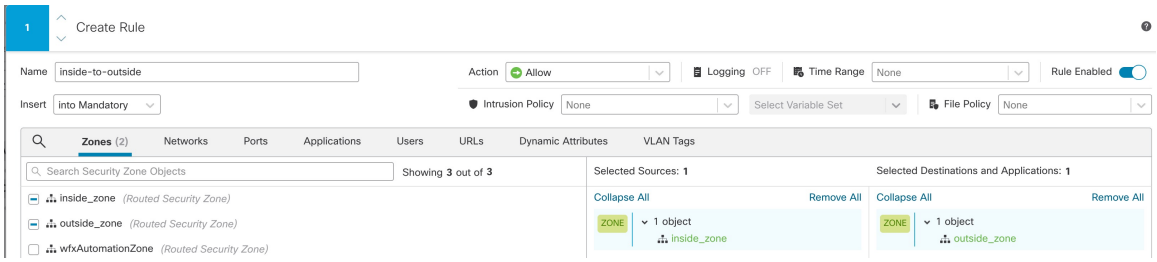
如果您在注册 威胁防御时创建了基本的**封锁所有流量**访问控制策略，则需要向策略添加规则以允许流量通过设备。以下程序可添加规则以允许从内部区域到外部区域的流量。如有其他区域，请务必添加允许流量到适当网络的规则。

过程

步骤 1 选择**策略 (Policy)** > **访问策略 (Access Policy)** > **访问策略 (Access Policy)**，然后点击分配给 威胁防御的访问控制策略的 **编辑**（ ）。

步骤 2 点击**添加规则 (Add Rule)** 并设置以下参数：

图 *28:* 添加规则



- **名称 (Name)** - 为此规则命名，例如 **inside-to-outside**。
- **所选择的源 (Selected Sources)** - 从 **区域 (Zones)**中选择内部区域，然后点击 **添加到源 (Add to Source)**。
- **所选择目标区域 (Selected Destination Zones)** - 从 **区域 (Zones)**中选择外部区域，然后点击 **添加到目标 (Add to Destination)**。

其他设置保留原样。

步骤 3 点击**应用 (Apply)**。

规则即已添加至 **Rules** 表。

步骤 4 点击**保存 (Save)**。

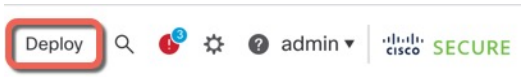
部署配置

将配置更改部署到 威胁防御；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 点击右上方的**部署 (Deploy)**。

图 *29:* 部署



步骤 2 要快速部署，请选中特定设备，然后点击**部署 (Deploy)**，或者点击**全部部署 (Deploy All)** 以部署到所有设备。否则，对于其他部署选项，请点击**高级部署 (Advanced Deploy)**。

图 *30:* 全部部署

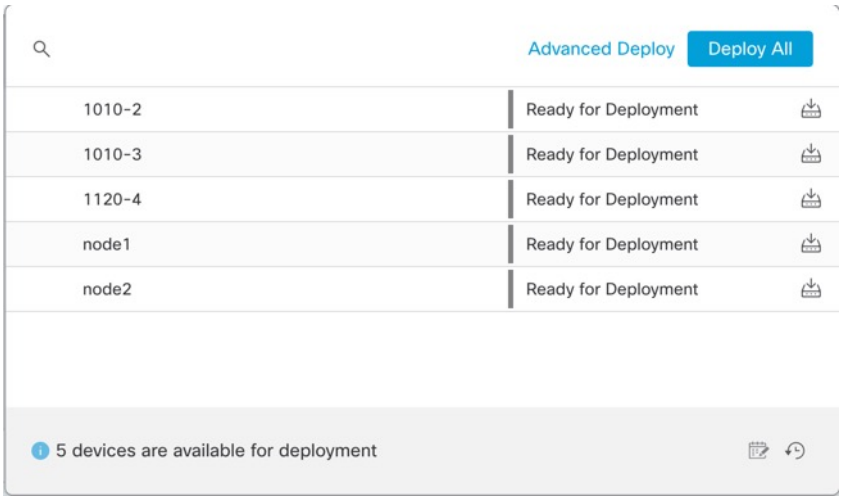
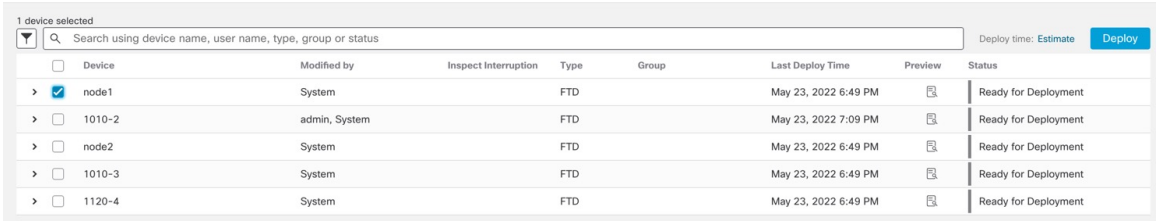
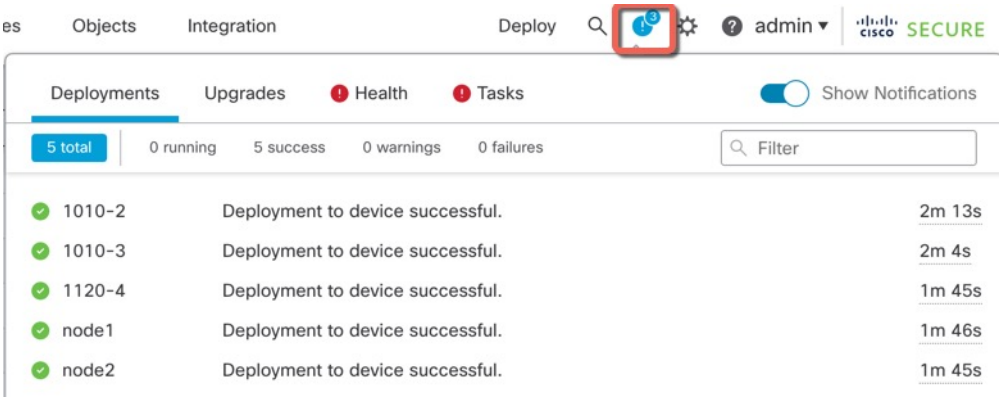


图 *31:* 高级部署



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

图 *32:* 部署状态



访问威胁防御和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。

也可以访问FXOS CLI以进行故障排除。

注释 您也可以通过 SSH 连接到 威胁防御 设备的管理接口。与控制台会话不同，SSH 会话默认使用 威胁防御 CLI，由此可使用 **connect fxos** 命令连接到 FXOS CLI。如果您为 SSH 连接打开某个数据接口，稍后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。此程序介绍控制台端口的访问（默认使用 FXOS CLI）。

过程

步骤 1 要登录 CLI，请将管理计算机连接到控制台端口。 默认情况下，安全防火墙 4200 不随附控制台电缆，因此您需要购买第三方 USB 转 RJ-45 串行电缆。确保为操作系统安装任何必要的 USB 串行驱动程序。控制台端口默认为 FXOS CLI。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

您连接到FXOS CLI。使用 **admin** 用户名和初始设置时设置的密码（默认值为 **Admin123**）登录 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 2 访问威胁防御 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Cisco Secure Firewall Threat Defense 命令参考。

步骤 3 要退出 威胁防御FTD CLI，请输入 **exit** 或 **logout** 命令。

此命令会将您重新导向至 FXOS CLI 提示。有关 FXOS CLI 中可用命令的相关信息，请输入 **?**。

示例：

```
> exit
firepower#
```

关闭防火墙电源

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系统。

您可以使用管理中心设备管理页面来关闭设备电源，也可以使用FXOS CLI。

使用管理中心关闭防火墙电源

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。

您可以使用 管理中心 正确关闭系统。

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)** 选项卡。

步骤 4 在**系统 (System)** 部分中点击 **关闭设备** （ ）。

步骤 5 出现提示时，确认是否要关闭设备。

步骤 6 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。

步骤 7 您现在可以关闭电源开关并在必要时拔下电源插头以物理方式断开机箱的电源。

在 CLI 关闭防火墙电源

您可以使用 FXOS CLI 安全地关闭系统并关闭设备。您可以通过连接到控制台端口来访问 CLI；请参阅访问威胁防御和FXOS CLI，第 33 页。

过程

步骤 1 在 FXOS CLI 中，连接到 local-mgmt：

firepower # **connect local-mgmt**

步骤 2 发出 **shutdown** 命令：

firepower(local-mgmt) # **shutdown**

示例：

```
firepower(local-mgmt)# shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
```

步骤 3 留意防火墙关闭时的系统提示。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]
```

步骤 4 您现在可以关闭电源开关并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 威胁防御，请参阅适用于您的软件版本的文档：浏览 Cisco Secure Firewall Threat Defense 文档。

有关使用 管理中心的信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。