使用管理中心部署威胁防御

本章对您适用吗？

要查看所有可用的操作系统和管理器，请参阅哪种操作系统和管理器适合您？。本章适用于威胁防御和管理中心。

本章介绍如何完成威胁防御的初始配置以及如何将防火墙注册到位于管理网络中的管理中心。 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。

在大型网络的典型部署中，要在网段上安装多个托管设备。每个设备控制、检查、监控和分析流量，然后向管理 管理中心 报告。管理中心 通过一个 Web 界面提供集中式管理控制台，可在运行中用来执行管理、分析和报告任务，以保护您的本地网络。

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。请参阅重新映像思科 ASA 或 Firepower 威胁防御设备。

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 的思科 FXOS 故障排除指南。

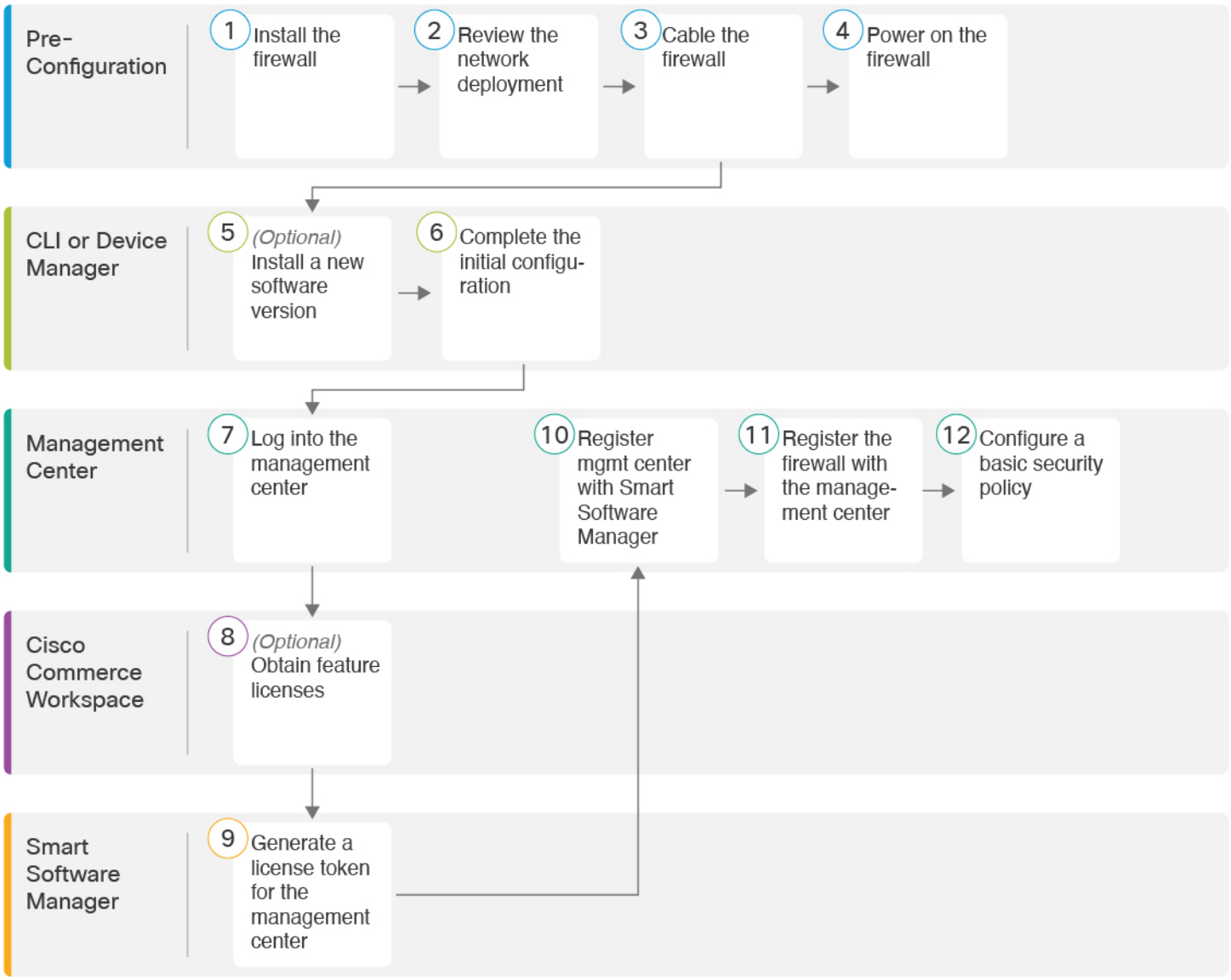
隐私收集声明-防火墙不要求或主动收集个人身份信息。但是，您可以在配置中使用个人身份信息，例如用户名。在这种情况下，管理员在执行配置或使用 SNMP 时可能会看到此信息。

在开始之前

部署并执行管理中心的初始配置。请参阅《思科 Firepower 管理中心 1600、2600 和 4600 硬件安装指南》或Cisco Secure Firewall Management Center Virtual 快速入门指南。

端到端程序

请参阅以下任务以在机箱上部署 威胁防御 和 管理中心。



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 4 页。
3	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 8 页。
4	配置前准备工作	打开防火墙电源， 第 9 页。
5	CLI	（可选）检查软件并安装新版本， 第 10 页

6	CLI 或 设备管理器	完成威胁防御初始配置，第 11 页。
7	管理中心	登录管理中心，第 19 页。
8	思科商务工作空间	获取管理中心的许可证，第 20 页：购买功能许可证。
9	智能软件管理器	获取管理中心的许可证，第 20 页：为 管理中心 生成许可证令牌。
10	管理中心	获取管理中心的许可证，第 20 页：向智能许可证服务器注册管理中心。
11	管理中心	向管理中心注册威胁防御，第 21 页
12	管理中心	配置基本安全策略，第 24 页

查看网络部署

6.5 和更高版本部署

专用管理 1/1 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。您可以在将 威胁防御 连接到 管理中心 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。

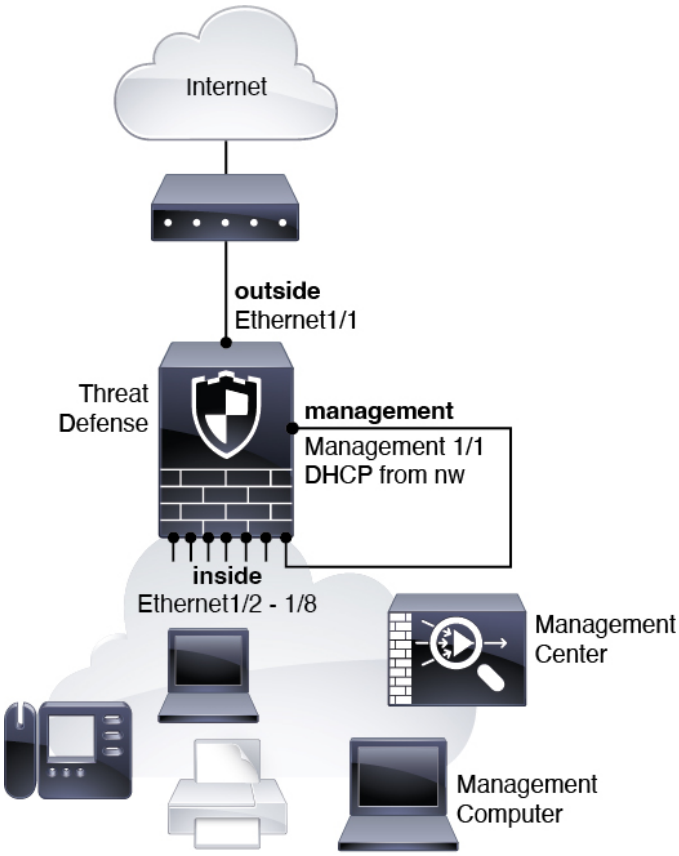
注释 在 6.5 和更早版本中，管理接口配置了 IP 地址 (192.168.45.45）。

下图显示了推荐用于 Firepower 1010 的网络部署。

管理中心只能在管理接口上与威胁防御通信。此外，管理中心和威胁防御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，Firepower 1010 充当管理接口和管理中心的互联网网关，它将管理 1/1 直接连接到内部交换机端口，并将管理中心和管理计算机连接到其他内部交换机端口。（因为管理接口独立于威胁防御上的其他接口，因此这种直接连接是允许的。）

图 *1:* 建议的网络部署



6.4 部署

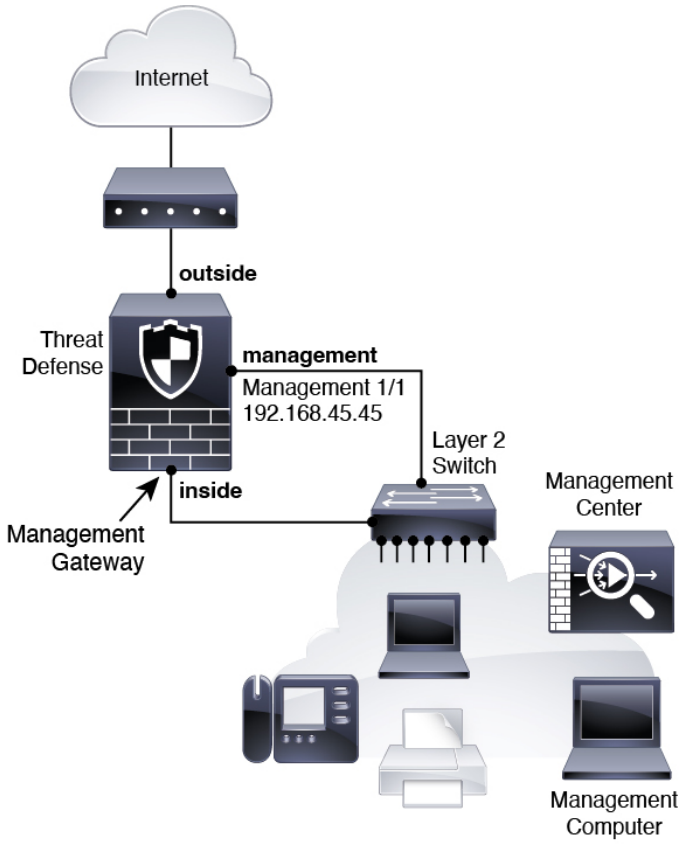
专用管理 1/1 接口是一种具有自己的网络设置的特殊接口。默认情况下，仅启用管理1/1 接口并为其配置 IP 地址 (192.168.45.45)。此接口最初也会运行 DHCP 服务器；在初始设置过程中选择 管理中心 作为管理器时，会禁用 DHCP 服务器。您可以在将 威胁防御 连接到 管理中心 后配置其他接口。

下图显示了推荐用于 Firepower 1010 的网络部署。

管理中心 只能在管理接口上与 威胁防御 通信。此外，管理中心和威胁防御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，并将管理中心和管理计算机连接到交换机，Firepower 1010 充当管理接口和管理中心的互联网网关。（因为管理接口独立于 威胁防御 上的其他接口，因此这种直接连接是允许的。）

图 *2:* 建议的网络部署

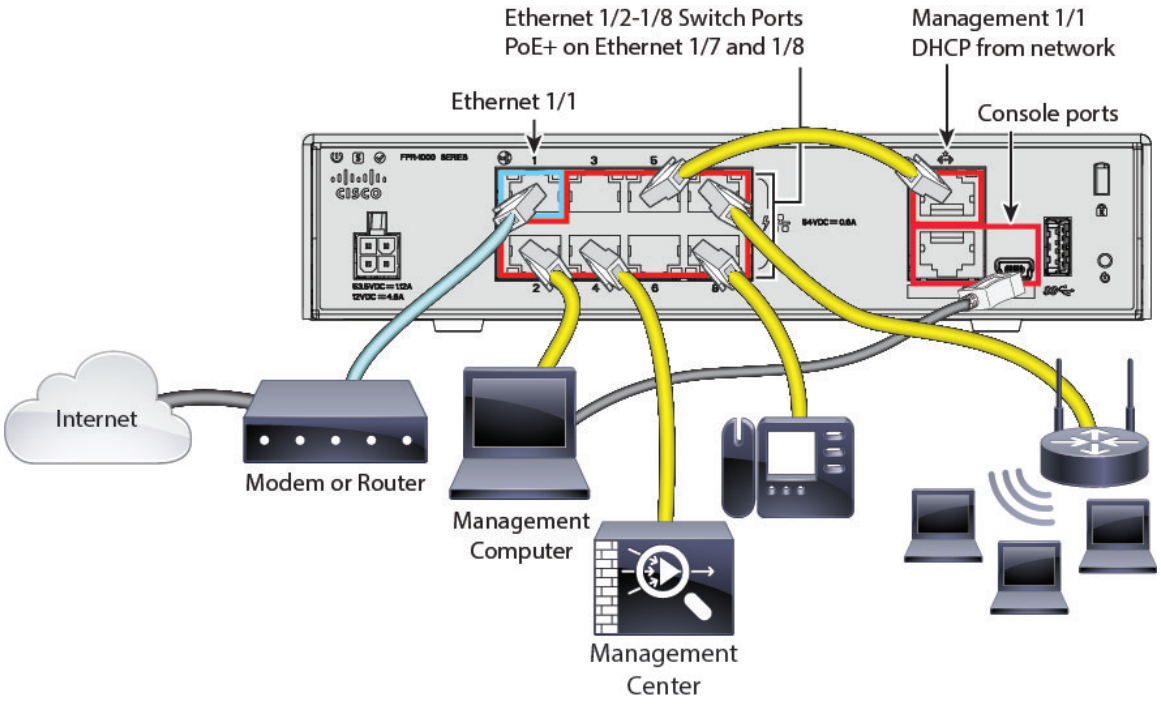


连接设备电缆（6.5 及更高版本）

要按照建议方案为 Firepower 1010 布线，请参阅下图，其中显示了使用 Ethernet1/1 作为外部接口、其余接口作为内部网络的交换机端口的拓扑示例。

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



注释 对于 6.5 及更早版本，管理 1/1 默认 IP 地址为 192.168.45.45。

注释 Firepower 1010E 上不支持 PoE。

过程

步骤 1 安装机箱。请参阅硬件安装指南。

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

步骤 3 使用电缆将以下各项连接到交换机端口 Ethernet1/2 至 1/8：

- 管理中心
- 管理计算机
- 其他端点

步骤 4 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 进行初始设置或使用设备管理器进行初始设置。

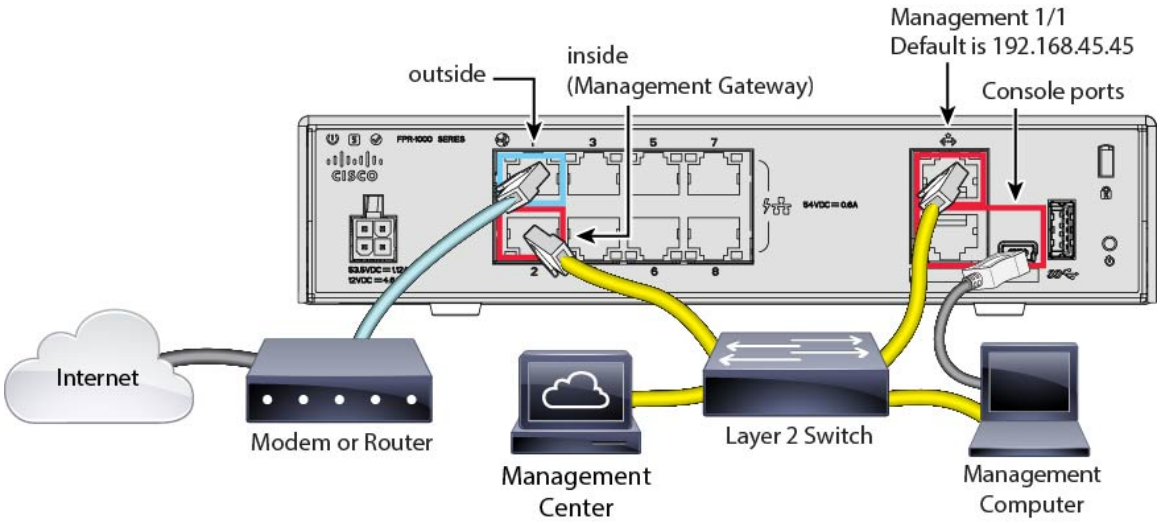
步骤 5 将以太网1/1 连接到外部路由器。

连接设备电缆 (6.4)

要按照建议方案为 Firepower 1010 布线，请参阅下图，其中显示了使用第 2 层交换机的拓扑示例。

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 使用硬件安装指南进行安装并熟悉您的硬件。

步骤 2 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
- 管理中心
- 管理计算机

注释 Firepower 1010 和 管理中心 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。请注意，6.5 和更高版本的 管理中心 管理接口默认为 DHCP 客户端；但是，如果没有 DHCP 服务器，默认为 192.168.45.45。

步骤 3 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。

步骤 4 将外部接口（例如，以太网 1/1）连接到外部路由器。

步骤 5 将其他网络连接到其余接口。

打开防火墙电源

系统电源由电源线控制；没有电源按钮。

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

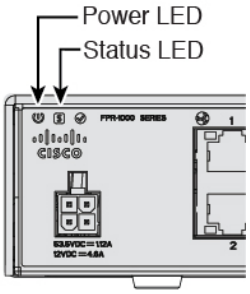
为设备提供可靠的电源（例如，使用不间断电源 (UPS)）非常重要。未事先关闭就断电可能会导致严重的文件系统损坏。后台始终有许多进程在运行，因此断电会使得系统无法正常关闭。

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。

（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 CLI。有关详细信息，请参阅访问威胁防御和 FXOS CLI，第 39 页。此程序显示使用控制台端口，但您也可以使用 SSH。

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               7.2.0.65        7.2.0.65
        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 16 页。默认情况下，管理接口将使用 DHCP。

您需要从可通过管理界面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。

完成威胁防御初始配置

您可以使用 CLI 或设备管理器来完成威胁防御初始配置。

使用设备管理器完成威胁防御初始配置

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

开始之前

- 部署并执行管理中心的初始配置。请参阅《思科 Firepower 管理中心 1600、2600 和 4600 硬件安装指南》。在设置 威胁防御 之前，您需要知道 管理中心 IP 地址或主机名。
- 使用 Firefox、Chrome、Safari、Edge 或 Internet Explorer 的当前版本。

过程

步骤 1 登录设备管理器。

a) 在浏览器中输入以下 URL。

- 内部（Ethernet1/2 到 1/8）- **https://192.168.95.1**。可以连接到任何内部交换机端口（Ethernet1/2 到 1/8）上的内部地址。

- 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，您可能必须将管理 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)** 来跳过设置向导。

完成设置向导后，除了内部接口（Ethernet1/2 至 1/8，它们是 VLAN1 上的交换机端口）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**。

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，则必须在完成设置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。您无法使用设置向导配置 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。请注意，设置管理接口 IP 地址不是设置向导的一部分。请参阅步骤 步骤 3，第 13 页 以设置管理 IP 地址。

   DNS 服务器 - 防火墙的管理接口的 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 - 防火墙的管理接口的主机名。

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）为管理界面配置一个静态 IP 地址。选择**设备 (Device)**，然后依次点击**系统设置 (System Settings)** > **管理接口 (Management Interface)** 链接。

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。

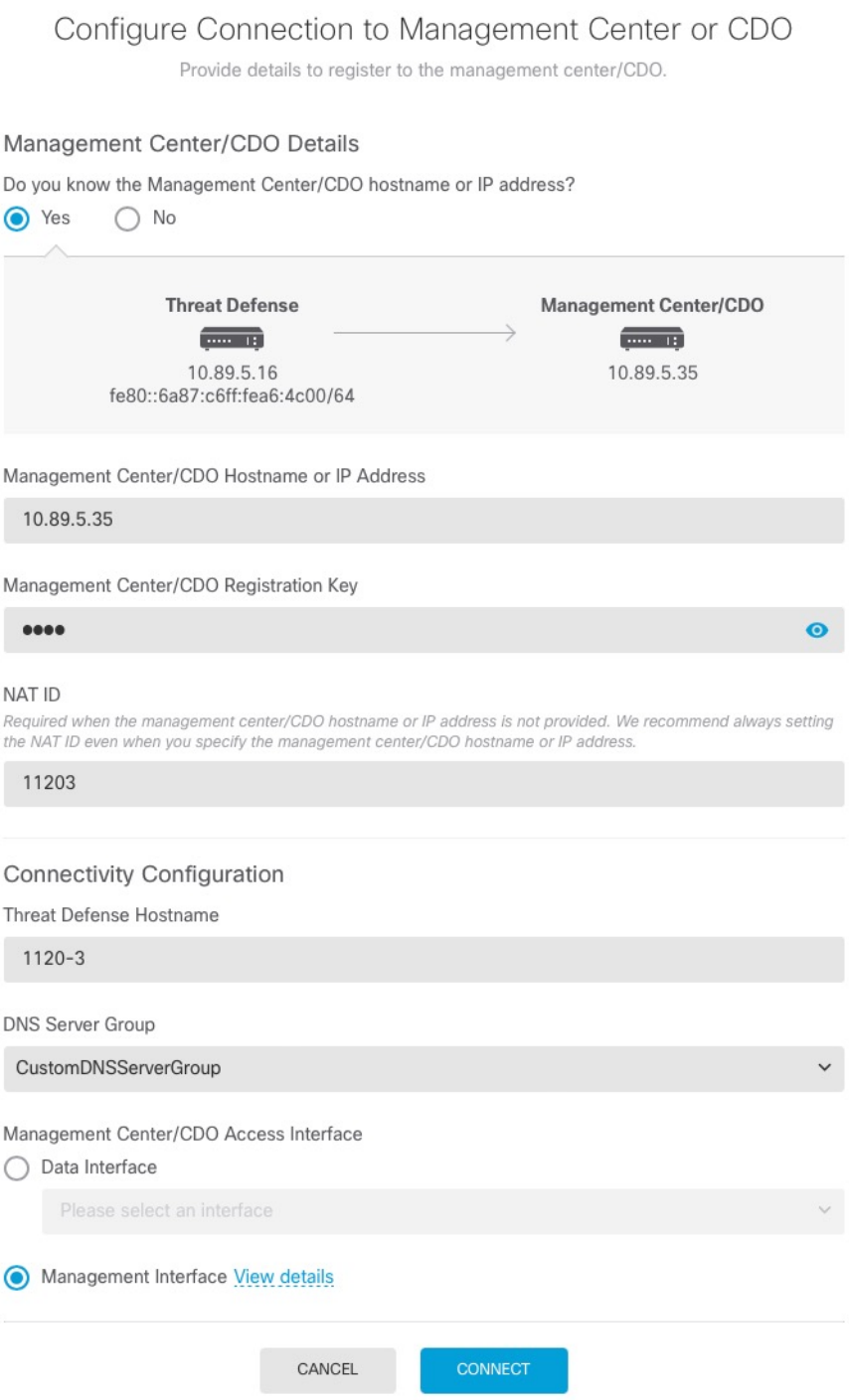
步骤 4 如果要配置其他接口，包括外部或内部之外的接口，请选择**设备 (Device)**，然后点击**接口 (Interfaces)** 摘要中的链接。

有关在 设备管理器 中配置接口的更多信息，请参阅在 设备管理器中配置防火墙。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 *5:* 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 SSL 加密的通信通道。

b) 如果您选择 **是**，则输入 **管理中心/CDO 主机名/IP 地址**。

c) 指定 **管理中心/CDO 注册密钥**。

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

d) 指定 **NAT ID**。

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

步骤 7 配置**连接配置**。

a) 指定 **FTD 主机名**。

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。

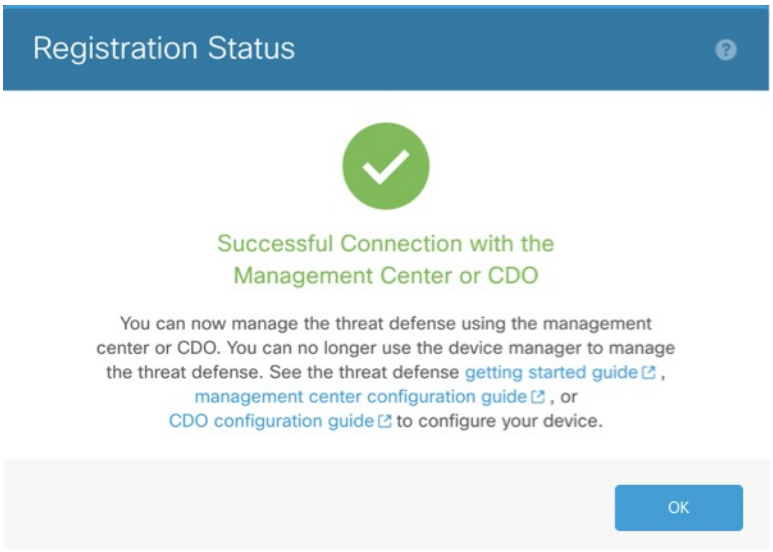
c) 对于**管理中心/CDO 访问接口 (Management Center/CDO Access Interface)**，请选择**管理 (management)**。

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 *6:* 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。在 6.7 和更高版本中：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。当您使用 设备管理器（7.1 和更高版本）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。

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 设置向导（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：

- **输入管理接口的 IPv4 默认网关 - 数据接口**设置仅适用于远程 管理中心 或 设备管理器 管理；在管理网络上使用 管理中心 时，应为管理 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。
- **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 **yes** 意味着您将改为使用 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。

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.
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]: ftd-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.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
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 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。

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 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：

- **IPS** - 安全情报和下一代 IPS
- **恶意软件 防御**-恶意软件 防御
- **URL** - 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

- 拥有智能软件管理器主帐户。

  如果您还没有账户，请点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。

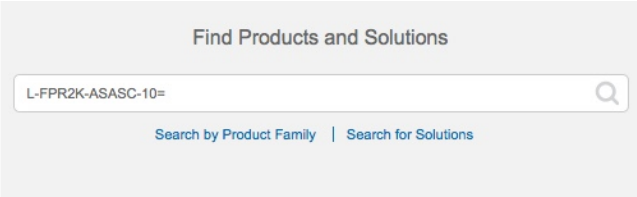
- 您的智能软件许可帐户必须符合强加密 (3DES/AES) 许可证的要求，才能使用某些功能（已使用导出合规性标志启用）。

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 7: 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。

- IPS、恶意软件 防御和 URL 许可证组合：
  - L-FPR1010T-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-FPR1010T-TMC-1Y
- L-FPR1010T-TMC-3Y
- L-FPR1010T-TMC-5Y

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

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。

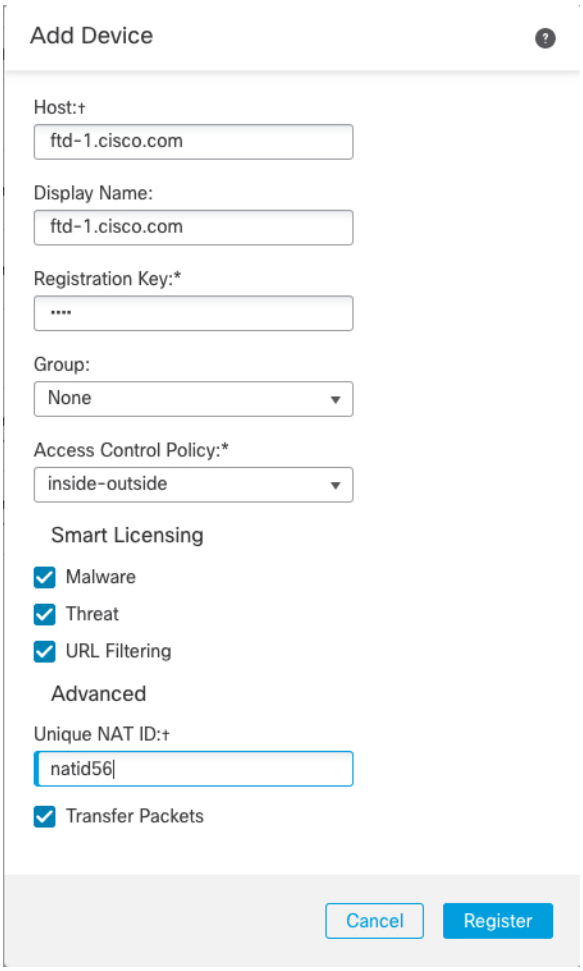
开始之前

- 收集您在 威胁防御 初始配置中设置的以下信息：
  - 威胁防御管理 IP 地址或主机名，以及 NAT ID
  - 管理中心注册密钥

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**。



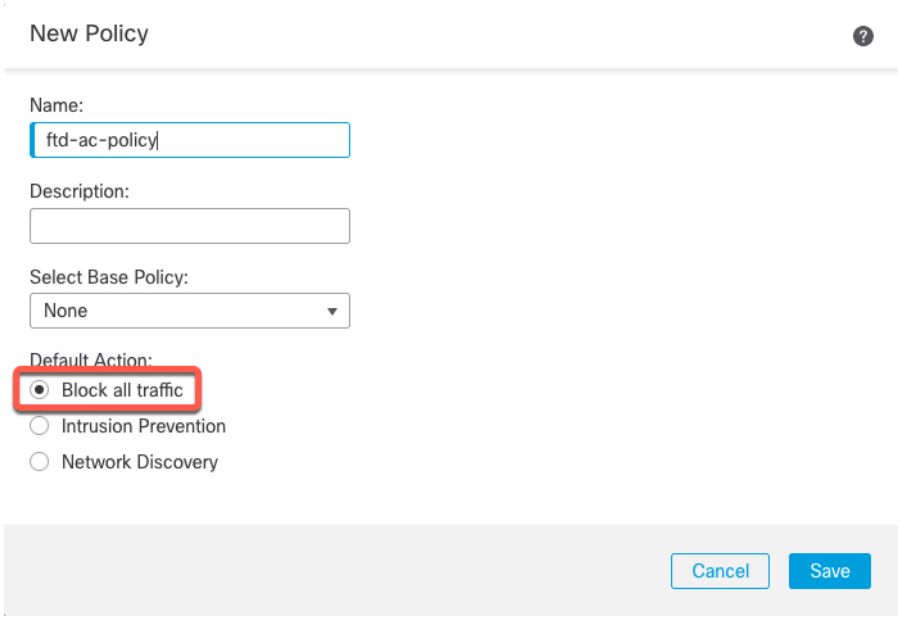
设置以下参数：

- **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 36 页。

图 *8:* 新建策略



- **智能许可 (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）。**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 点击**注册 (Register)**，或者如果要添加另一台设备，请点击**注册并添加其他 (Register and Add Another)**，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（6.5 及更高版本），第 24 页 配置接口 (6.4)，第 28 页。
2	配置 DHCP 服务器，第 31 页。
3	添加默认路由，第 32 页。
4	配置 NAT，第 34 页。
5	允许流量从内部传到外部，第 36 页。
6	部署配置，第 37 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。

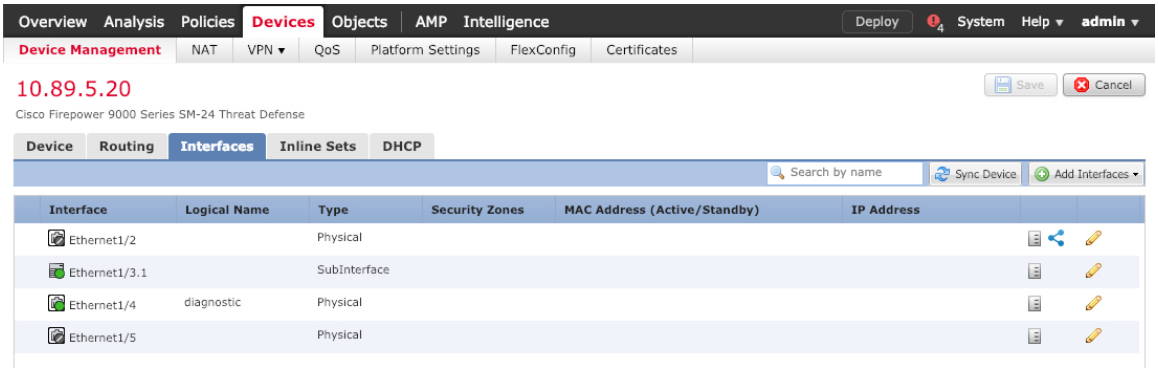
典型的边缘路由情况是通过 DHCP 从 ISP 获取外部接口地址，同时在内部接口上定义静态地址。

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

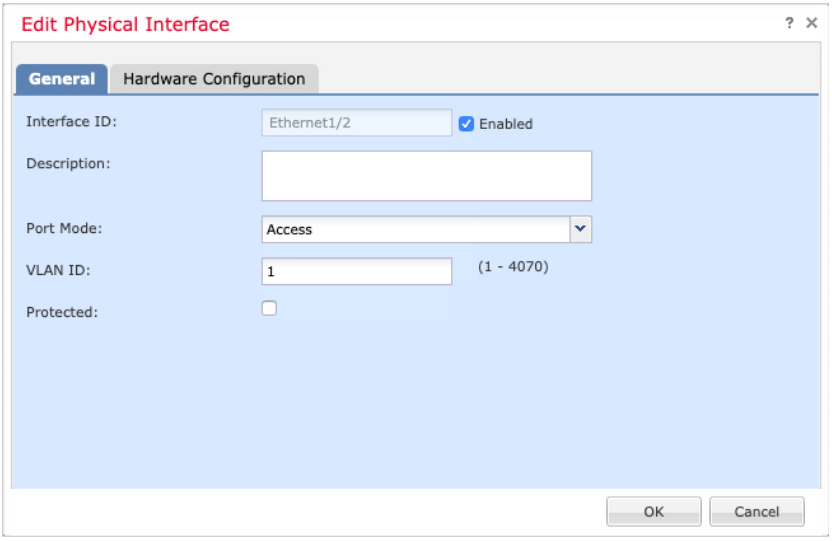
步骤 2 点击**接口 (Interfaces)**。



步骤 3 （可选） 点击**交换机端口 (SwitchPort)** 列中的滑块，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，使其显示为已禁用（ ）。

步骤 4 启用交换机端口。

a) 点击与交换机端口相对应的**编辑**（ ）。



b) 选中**启用**复选框以启用此接口。

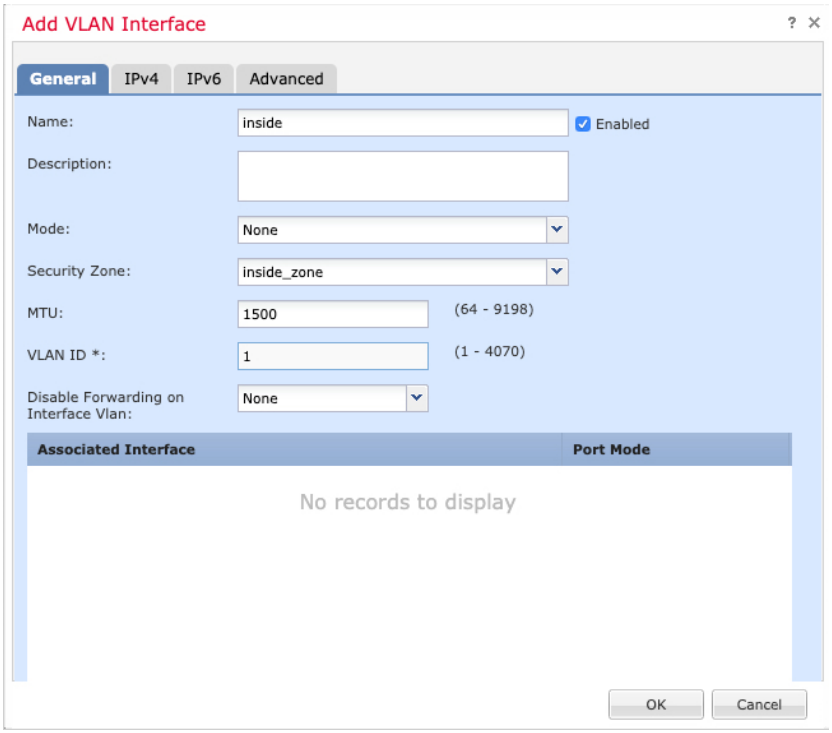
c) （可选） 更改 VLAN ID；默认值为 1。接下来，您将添加一个 VLAN 接口来匹配此 ID。

d) 点击**确定 (OK)**。

步骤 5 添加内部 VLAN 接口。

a) 点击**添加接口 (Add Interfaces)** > **VLAN 接口 (VLAN Interface)**。

此时将显示**一般 (General)** 选项卡。



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**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。

f) 将 **VLAN ID** 设置为 **1**。

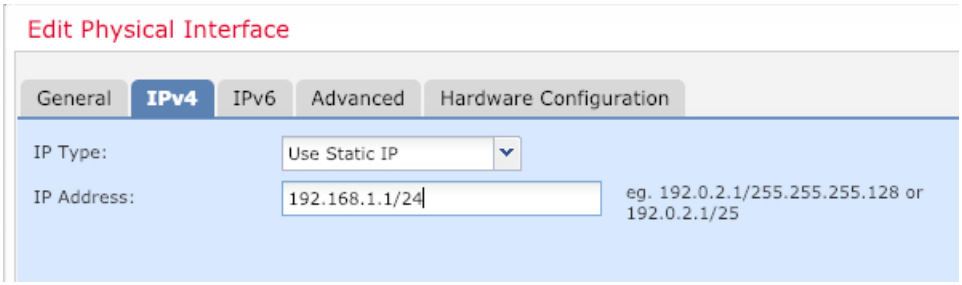
默认情况下，所有交换机端口都设置为 VLAN 1；如果在此处选择不同的 VLAN ID，还需要编辑每个交换机端口，使其位于新 VLAN ID 所对应的 VLAN 上。

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) 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**

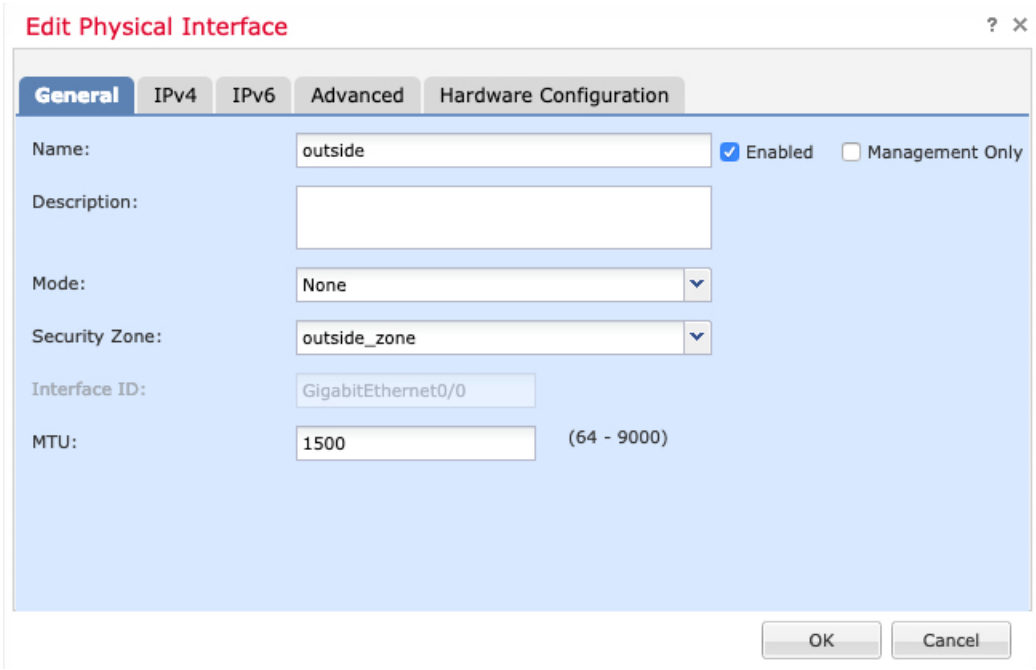


- **IPv6** - 为无状态自动配置选中**自动配置 (Autoconfiguration)** 复选框。

h) 点击**确定 (OK)**。

步骤 6 点击要用于外部的以太网 1/1 的 **编辑**（ ）。

General 选项卡将显示。



注释 如果您为此接口预配置了管理器访问，则该接口就已经命名、启用和寻址。您不应更改任何这些基本设置，因为这样做会中断管理中心管理连接。您仍然可以在此屏幕上为直通流量策略配置安全区域。

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。

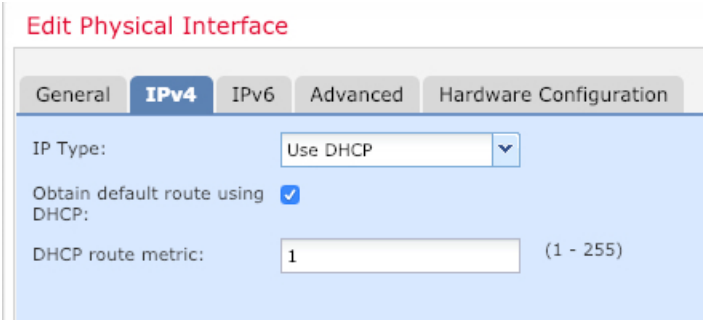
c) 将 **Mode** 保留为 **None**。

d) 从**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。



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

f) 点击**确定 (OK)**。

步骤 7 点击**保存 (Save)**。

配置接口 (6.4)

启用威胁防御接口，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。

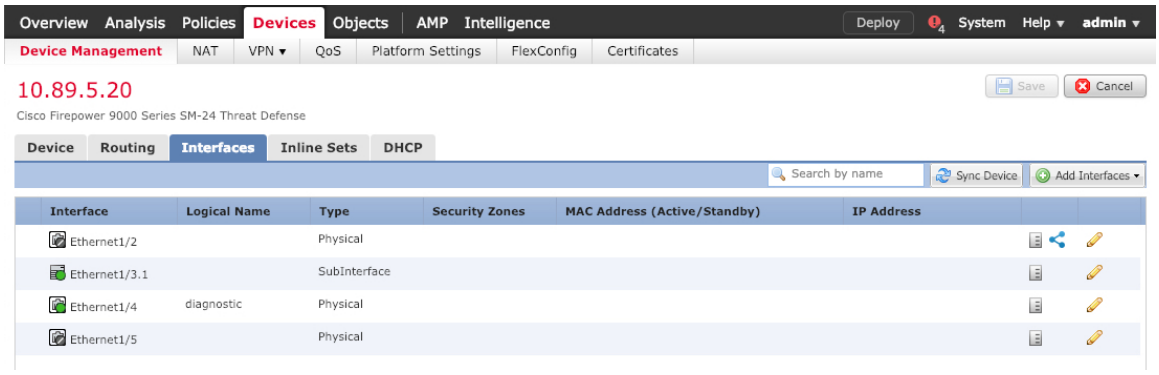
典型的边缘路由情况是通过 DHCP 从 ISP 获取外部接口地址，同时在内部接口上定义静态地址。

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

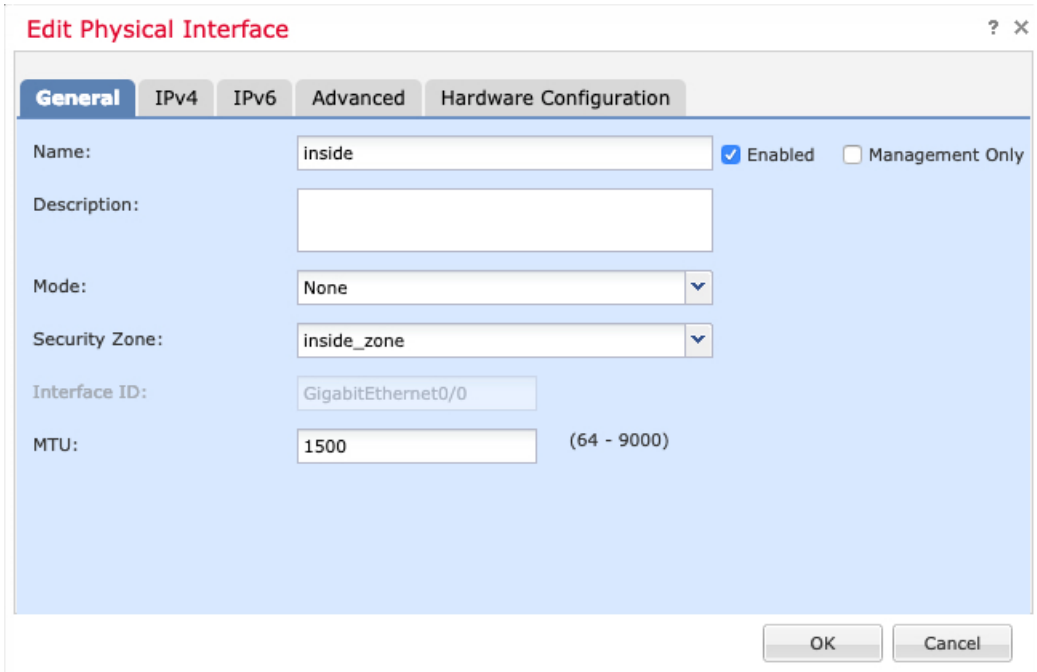
步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**，然后点击防火墙的**编辑**（ ）。

步骤 2 点击**接口 (Interfaces)**。



步骤 3 点击要用于内部的接口的**编辑**（ ）。

此时将显示**一般 (General)** 选项卡。



a) 输入长度最大为 48 个字符的 **Name**。

例如，将接口命名为 **inside**。

b) 选中 **Enabled** 复选框。

c) 将 **Mode** 保留为 **None**。

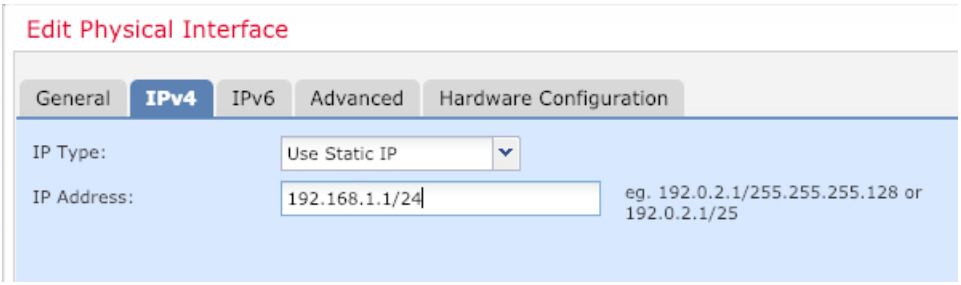
d) 从**安全区域 (Security Zone)** 下拉列表中选择一个现有的内部安全区域，或者点击**新建 (New)** 添加一个新的安全区域。

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**

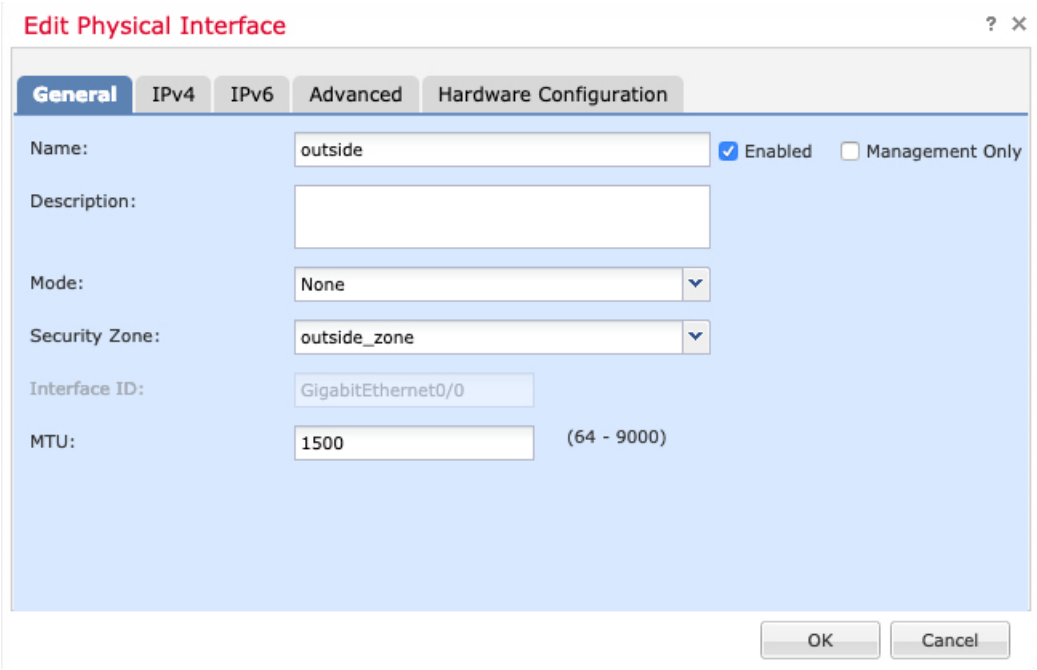


- **IPv6** - 为无状态自动配置选中**自动配置 (Autoconfiguration)** 复选框。

f) 点击**确定 (OK)**。

步骤 4 点击要用于外部的接口的 **编辑**（ ）。

此时将显示**一般 (General)** 选项卡。



注释 如果您为此接口预配置了管理器访问，则该接口就已经命名、启用和寻址。您不应更改任何这些基本设置，因为这样做会中断管理中心管理连接。您仍然可以在此屏幕上为直通流量策略配置安全区域。

a) 输入长度最大为 48 个字符的 **Name**。

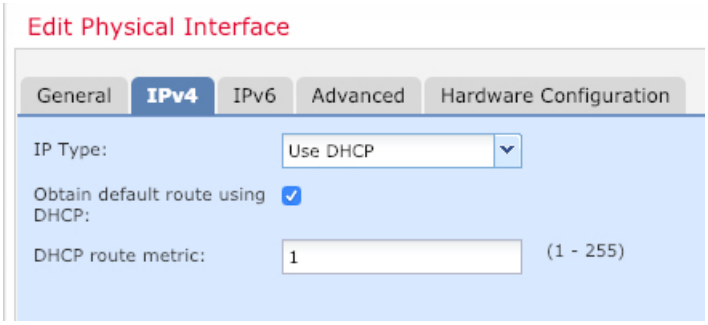
例如，将接口命名为 **outside**。

b) 选中 **Enabled** 复选框。
c) 将 **Mode** 保留为 **None**。
d) 从**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。



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

f) 点击**确定 (OK)**。

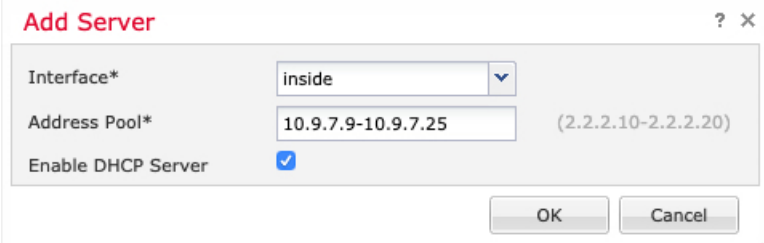
步骤 5 点击**保存 (Save)**。

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



- **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)**。

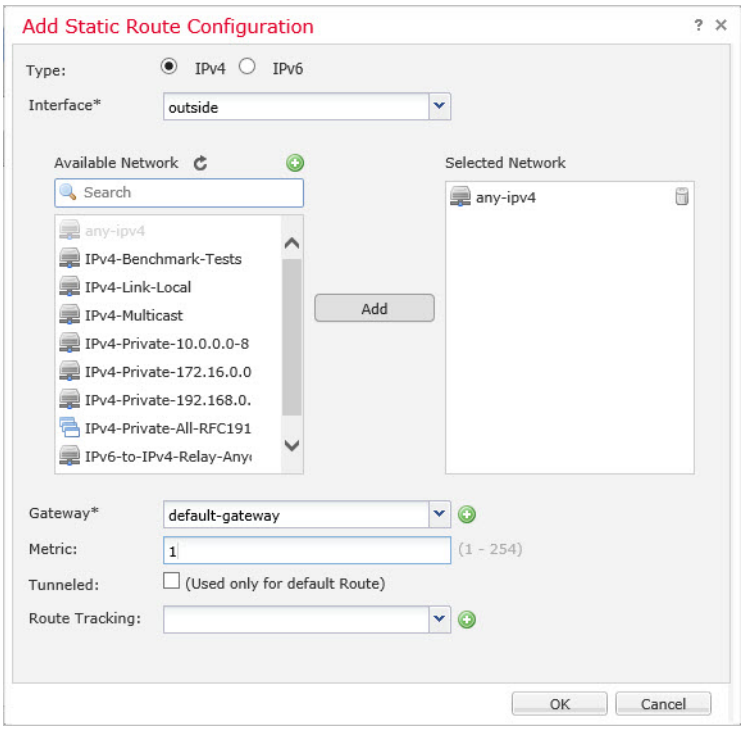
添加默认路由

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**（ ）。

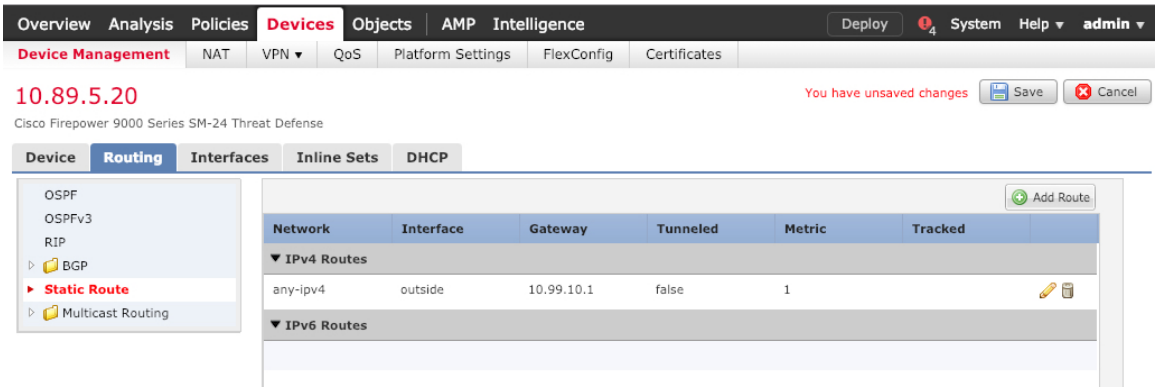
步骤 2 选择**路由 (Route)** > **静态路由 (Static Route)**，点击**添加路由 (Add Route)**，然后设置以下项：



- **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 3 点击**确定 (OK)**。

路由即已添加至静态路由表。



步骤 4 点击保存 (Save)。

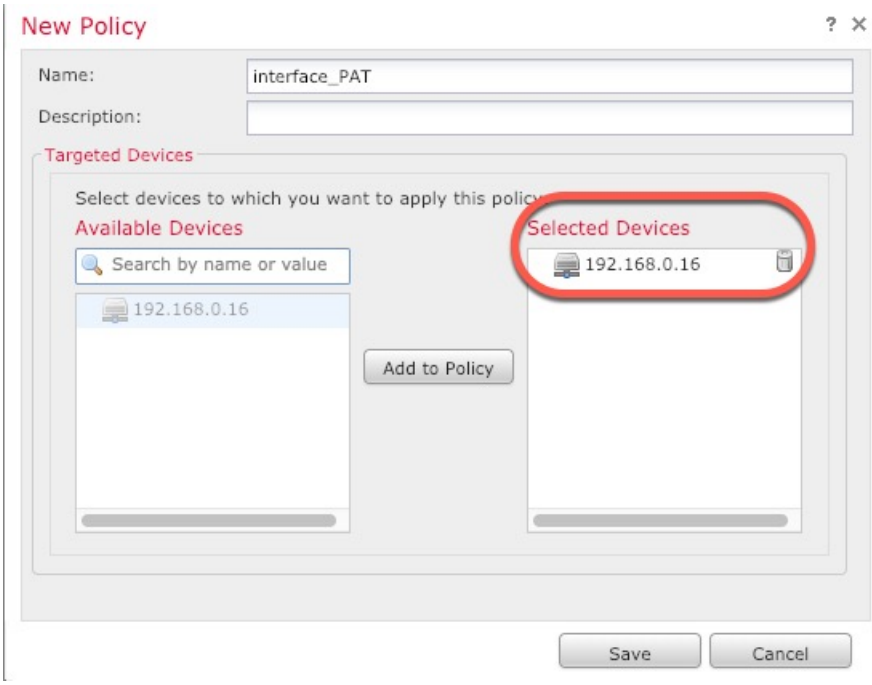
配置 NAT

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。



策略即已添加 管理中心。您仍然需要为策略添加规则。

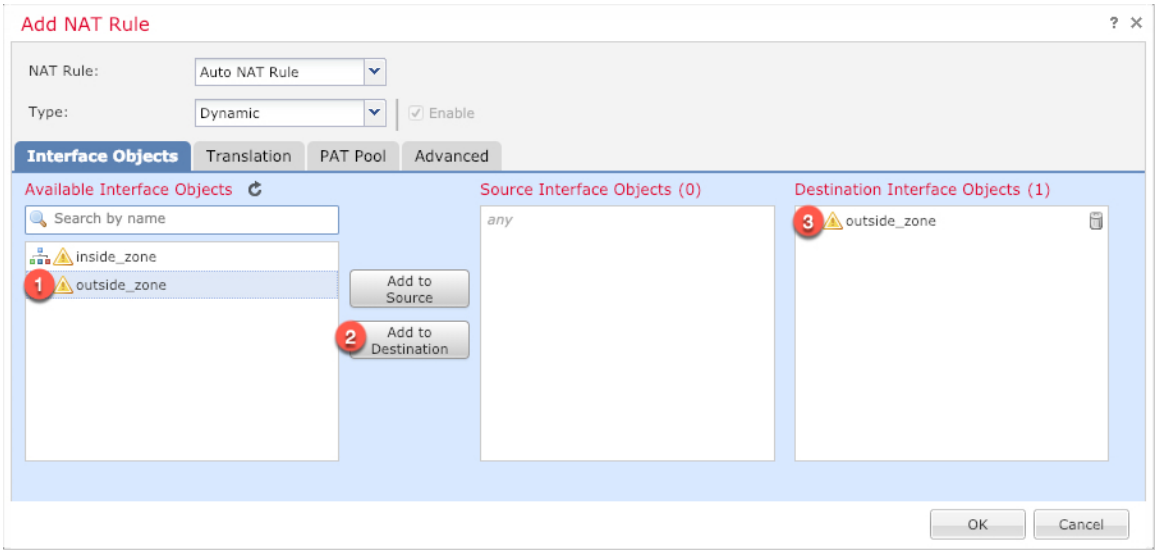
步骤 3 点击添加规则 (Add Rule)。

Add NAT Rule 对话框将显示。

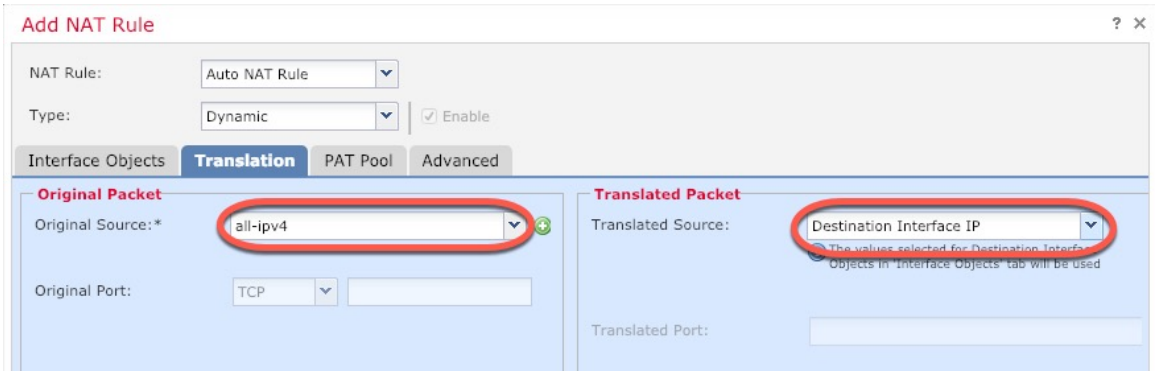
步骤 4 配置基本规则选项：

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

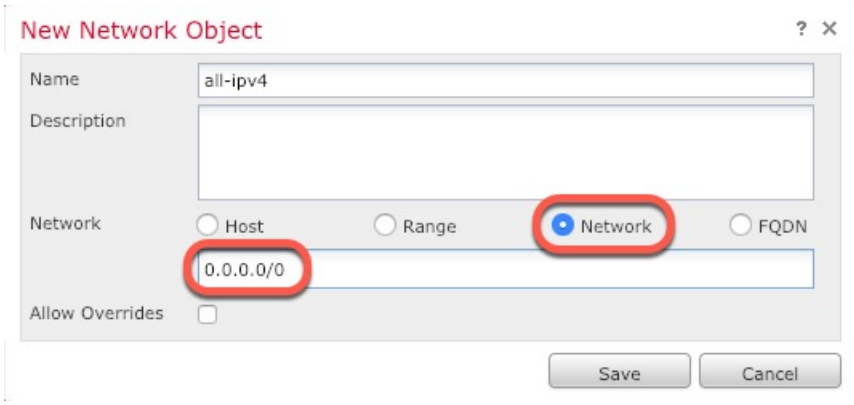
步骤 5 在 **Interface Objects** 页面，将 **Available Interface Objects** 区域中的外部区域添加到 **Destination Interface Objects** 区域。



步骤 6 在**转换 (Translation)** 页面上配置以下选项：



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

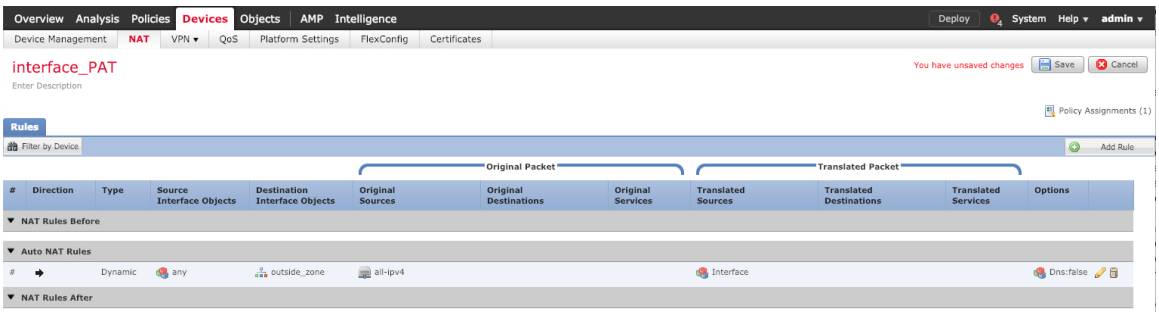


注释　　您不能使用系统定义的 **any-ipv4** 对象，因为自动 NAT 规则在对象定义过程中添加 NAT，并且您无法编辑系统定义的对象。

- **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。

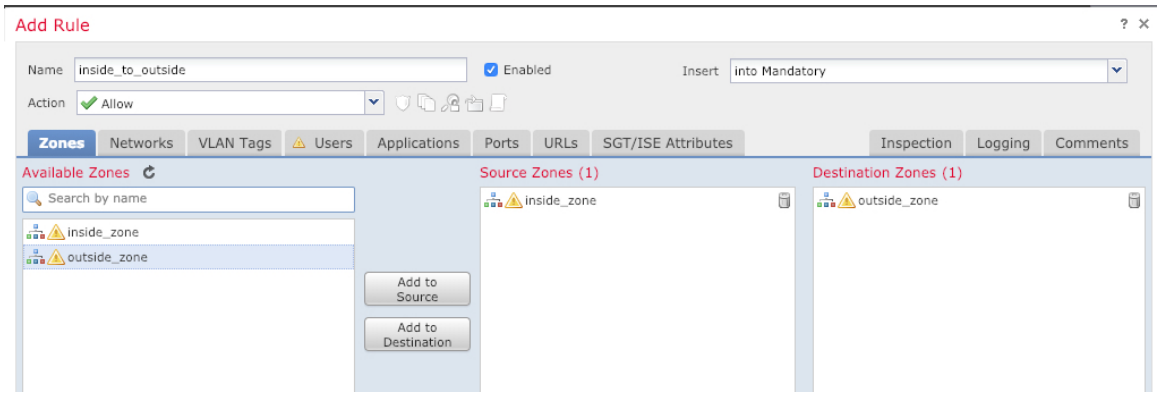
允许流量从内部传到外部

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：

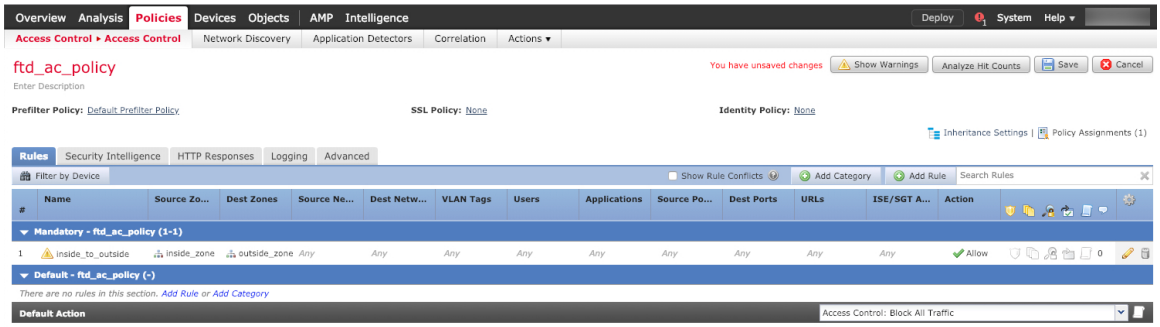


- **名称 (Name)** - 为此规则命名，例如 **inside_to_outside**。
- **源区域 (Source Zones)** - 从**可用区域 (Available Zones)** 中选择内部区域，然后点击**添加到源 (Add to Source)**。
- **目标区域 (Destination Zones)** - 从**可用区域 (Available Zones**） 中选择外部区域，然后点击**添加到目标 (Add to Destination)**。

其他设置保留原样。

步骤 3 点击**添加 (Add)**。

规则即已添加至 **Rules** 表。



步骤 4 点击**保存 (Save)**。

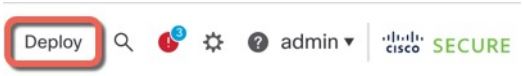
部署配置

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 *9:* 部署



步骤 2 点击**全部部署 (Deploy All)** 以部署到所有设备，或点击**高级部署 (Advanced Deploy)** 以部署到选择的设备。

图 *10:* 全部部署

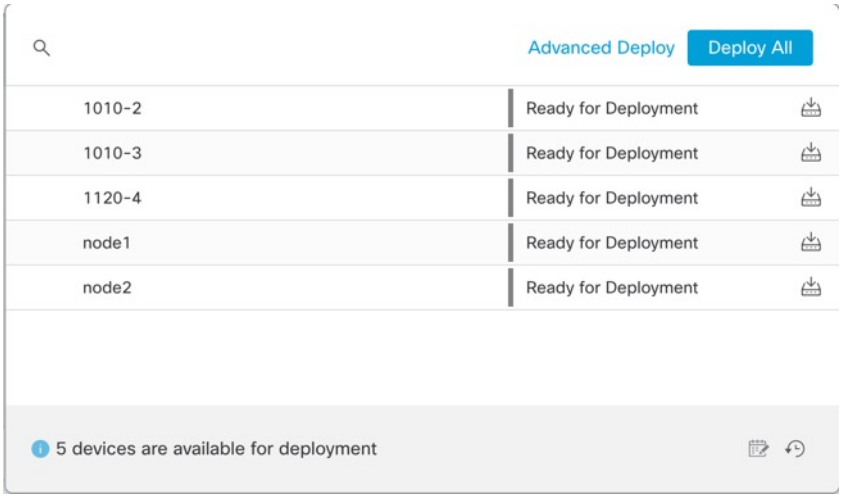
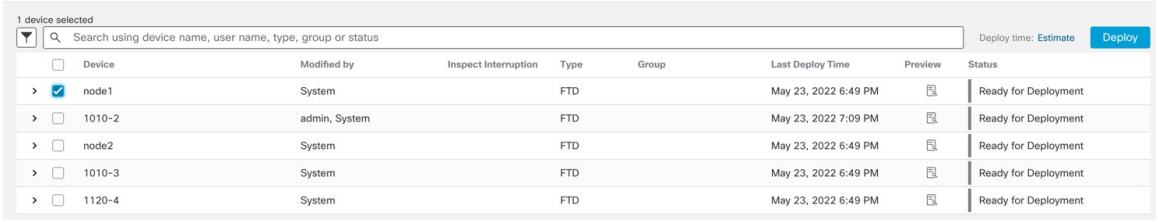
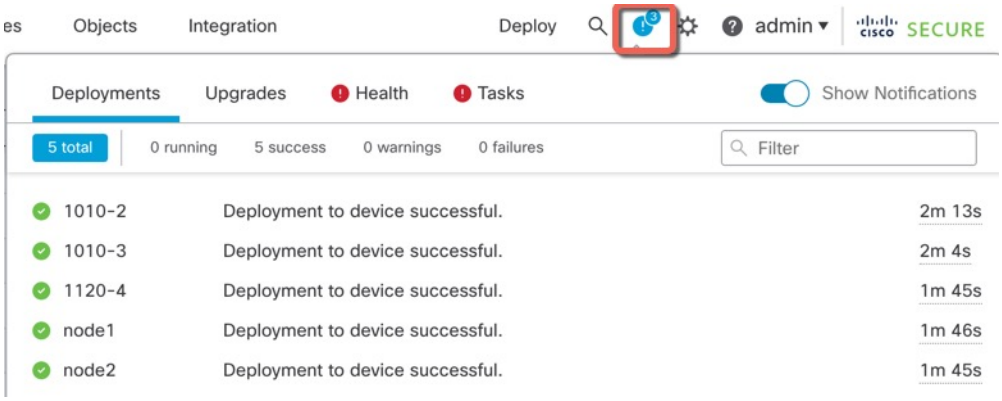


图 *11:* 高级部署



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 *12:* 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。Firepower 1000 随附了一根 USB A 转 B 串行电缆。确保为您的操作系统安装必要的 USB 串行驱动程序（请参阅 Firepower 1010 硬件指南）。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。

Firepower 1010机箱没有外部电源开关。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，点击编辑图标 ( )。

步骤 3 点击**设备 (Device)** 选项卡。

步骤 4 点击**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 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 您现在可以在必要时拔下电源插头以物理方式断开机箱的电源。

在 CLI 断开设备电源

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 39 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：导航思科 Firepower 文档。

有关使用 管理中心的信息，请参阅《Firepower 管理中心配置指南》。

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。