使用管理中心部署威胁防御

本章对您适用吗？

本章介绍如何部署使用管理中心管理的独立式威胁防御逻辑设备。要部署高可用性对或集群，请参阅《Firepower 管理中心配置指南》。

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。

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 管理中心）的网络，您可以使用集成的 设备管理器。使用 设备管理器 基于 Web 的设备安装向导可配置小型网络部署常用的基本软件功能。

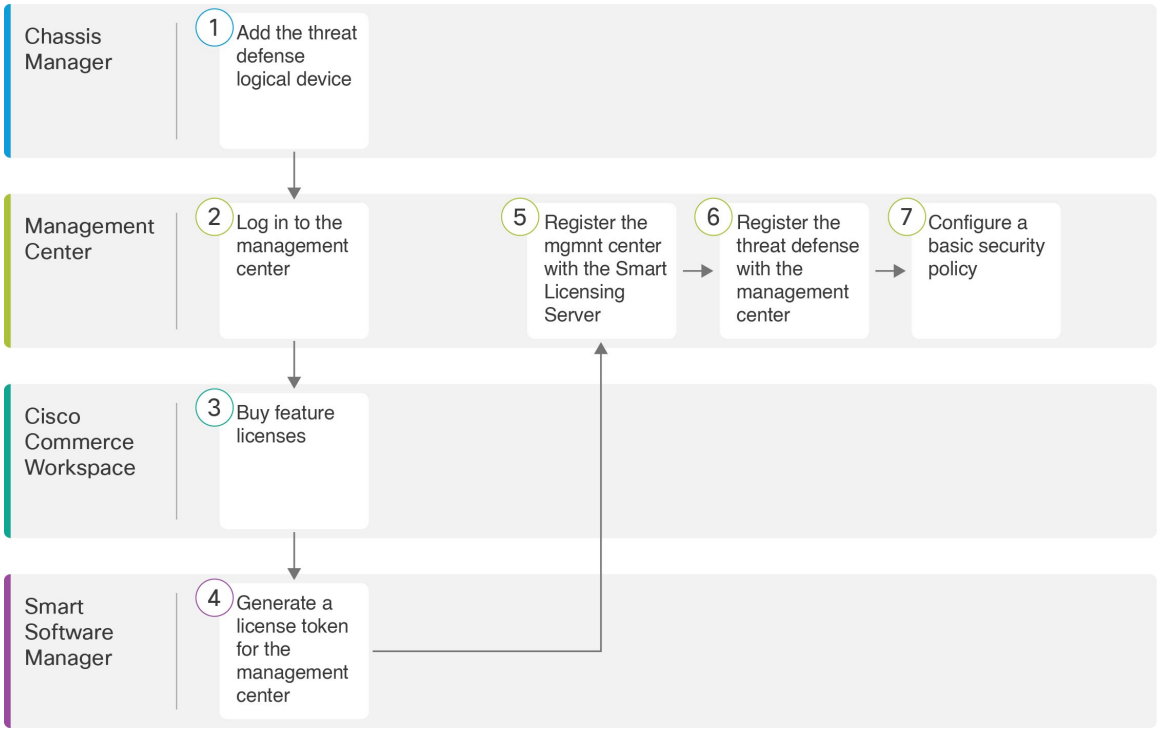
隐私收集声明 - Firepower 4100 不要求或主动收集个人身份信息。不过，您可以在配置中使用个人身份信息，例如用于用户名。在这种情况下，管理员在执行配置或使用 SNMP 时可能会看到此信息。

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和配置 威胁防御。



	工作空间	步骤
1	机箱管理器	机箱管理器：添加威胁防御逻辑设备， 第 3 页。
2	管理中心	登录管理中心， 第 7 页。
3	Cisco Commerce Workspace	获取管理中心的许可证， 第 8 页：购买功能许可证。
4	智能软件管理器	获取管理中心的许可证， 第 8 页：为 管理中心 生成许可证令牌。
5	管理中心	获取管理中心的许可证， 第 8 页：向智能许可证服务器注册管理中心。
6	管理中心	向管理中心注册威胁防御， 第 10 页。
7	管理中心	配置基本安全策略， 第 13 页。

机箱管理器：添加威胁防御逻辑设备

您可以从 Firepower 4100将 威胁防御 部署为本地实例或容器实例。您可以为每个安全引擎安全引擎部署多个容器实例，但只能部署一个本机实例。有关每个型号的最大容器实例数，请参阅逻辑设备应用程序实例：容器或本地。

要添加高可用性对或集群，请参阅《Firepower 管理中心配置指南》。

您可以通过此程序配置逻辑设备特性，包括应用程序使用的引导程序配置。

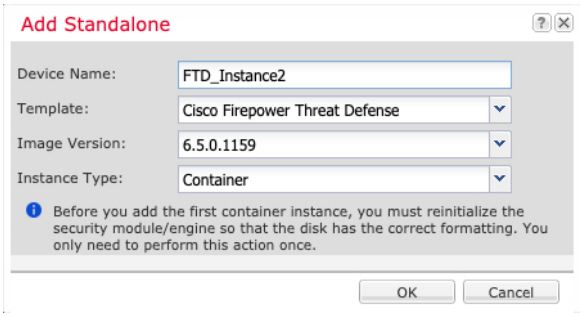
开始之前

- 配置与 威胁防御一起使用的管理接口；请参阅配置接口。管理接口是必需的。在 6.7 和更高版本中，您可以稍后从数据接口启用管理；但必须将管理接口分配给逻辑设备，即使您不打算在启用数据管理后使用该接口。请注意，此管理接口与仅用于机箱管理的机箱管理端口（并且该端口在**接口**选项卡的顶部显示为 **MGMT**）不同。
- 您还必须至少配置一个数据接口。
- 对于容器实例，如果您不想采用使用最少资源的默认配置文件，请在**平台设置** > **资源配置文件**上添加资源配置文件。
- 对于容器实例，在您第一次安装容器实例之前，可能需要重新初始化安全引擎，以保证磁盘具有正确的格式。如果必须完成此操作，您将无法保存逻辑设备。点击**安全引擎**，然后点击重新初始化图标（）。
- 收集以下信息：
  - 此设备的接口 ID
  - 管理接口 IP 地址和网络掩码
  - 网关 IP 地址
  - 您选择的管理中心 IP 地址和/或 NAT ID
  - DNS 服务器 IP 地址

过程

步骤 1 在 机箱管理器中，选择**逻辑设备**。

步骤 2 点击**添加** > **独立设备**，并设置以下参数：



a) 提供**设备名称**。

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

b) 对于**模板**，请选择 **Cisco Firepower 威胁防御**。

c) 选择**映像版本**。

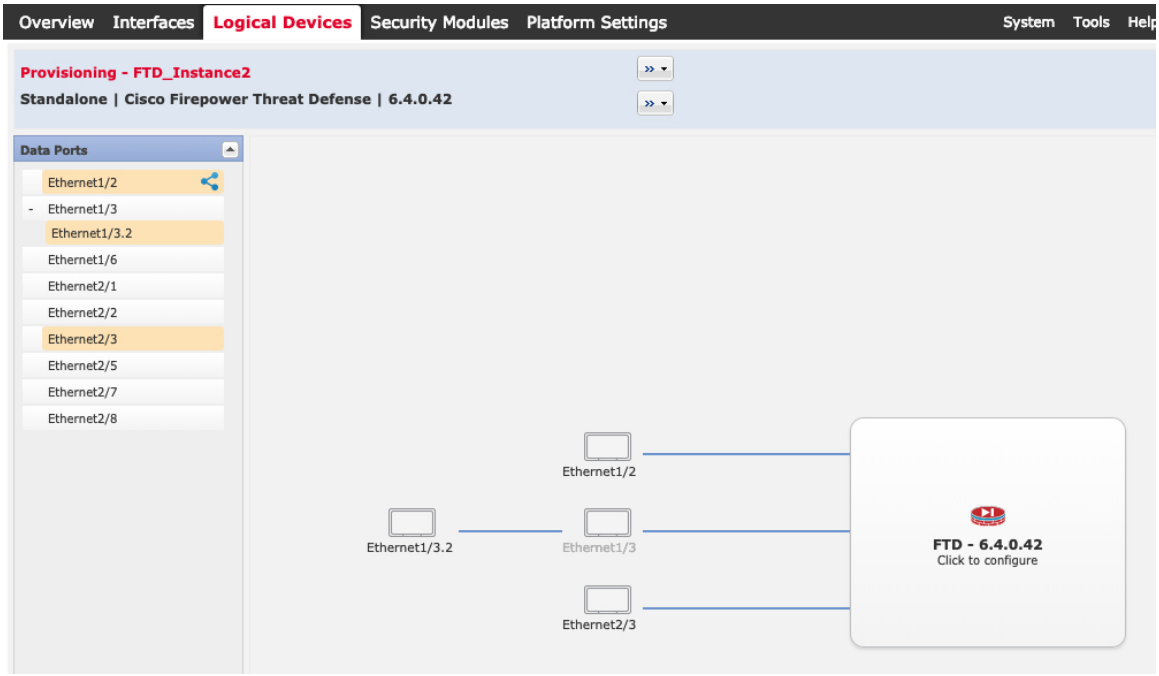
d) 选择**实例类型：容器**或**本地**。

本地实例使用安全模块/引擎的所有资源（CPU、RAM和磁盘空间），因此仅可安装一个本地实例。容器实例使用部分安全模块/引擎资源，因此可以安装多个容器实例。

e) 点击**确定 (OK)**。

屏幕会显示调配 - 设备名称窗口。

步骤 3 展开**数据端口 (Data Ports)** 区域，然后点击要分配给设备的每个接口。



您仅可分配先前在**接口**页面上启用的数据和数据共享接口。稍后您需要在管理中心中启用和配置这些接口，包括设置 IP 地址。

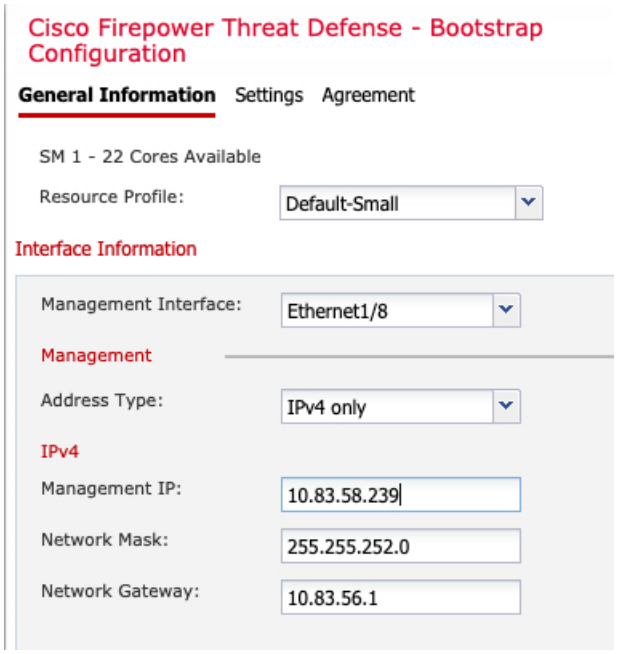
仅可向一个容器实例分配最多 10 个数据共享接口。此外，可以将每个数据共享接口分配至最多 14 个容器实例。数据共享接口以共享图标（）表示。

具有硬件旁路功能的端口使用以下图标显示：。对于某些接口模块，仅可启用用于内联集接口的硬件旁路功能（有关内联集的信息，请参阅《Firepower 管理中心配置指南》）。硬件绕行确保流量在断电期间继续在接口对之间流动。在软件或硬件发生故障时，此功能可用于维持网络连接性。如果您未同时分配一个硬件旁路对中的两个接口，则会收到一条警告消息，确认您是故意这样分配。您不需要使用硬件旁路功能，因此如果您愿意，可以分配单个接口。

步骤 4 点击屏幕中心的设备图标。

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

步骤 5 在**一般信息 (General Information)** 页面上，完成下列操作：



a) 对于容器实例，指定**资源配置文件**。

如果您稍后分配一个不同的资源配置文件，则实例将重新加载，这可能需要大约 5 分钟的时间。请注意，对于已建立的高可用性对或集群，如果分配不同大小的资源配置文件，请务必尽快确保所有成员大小一致。

b) 选择**管理接口**。

此接口用于管理逻辑设备。此接口独立于机箱管理端口。

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

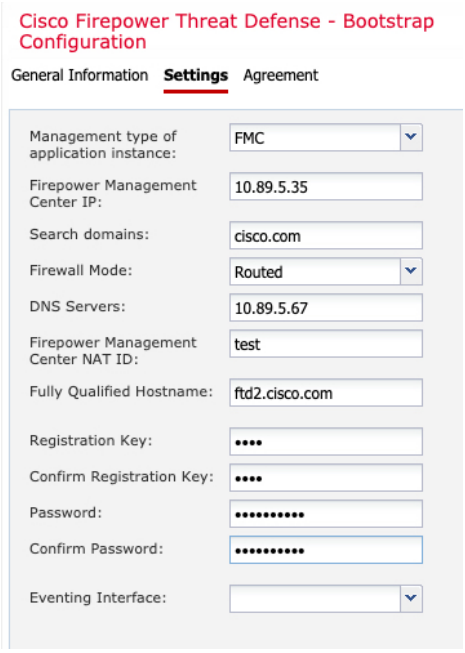
d) 配置**管理 IP** 地址。

设置用于此接口的唯一 IP 地址。

e) 输入**网络掩码**或**前缀长度**。

f) 输入**网络网关**地址。

步骤 6 在**设置**选项卡上，完成下列操作：



a) 对于本地实例，在**应用实例的管理类型**下拉列表中，选择 **FMC**。

本地实例还支持 设备管理器 作为管理器。部署逻辑设备后，无法更改管理器类型。

b) 输入管理 管理中心 的 **Firepower 管理中心 IP** 或主机名。如果不知道 管理中心 IP 地址，请将此字段留空，并在 **Firepower 管理中心 NAT ID** 字段中输入口令。

c) 对于容器实例，选择**是否允许 FTD SSH 会话专家模式 (Permit Expert mode from FTD SSH sessions)**：**是 (Yes)** 或**否 (No)**。专家模式提供 威胁防御 外壳访问以确保实现高级故障排除。

对于此选项，如果您选择**是 (Yes)**，拥有直接从 SSH 会话访问容器实例的权限的用户可以输入专家模式。如果您选择**否 (No)**，只有拥有从 FXOS CLI 访问容器实例的权限的用户可以输入专家模式。我们建议选择**否 (No)** 以加强实例之间的隔离。

仅当书面程序指出必须使用或思科技术支持中心要求使用专家模式时，才使用专家模式。要进入此模式下，请在 威胁防御 CLI 中使用 **expert** 命令。

d) 输入逗号分隔列表形式的**搜索域**。

e) 选择**防火墙模式：透明**或**路由式**。

在路由模式中，威胁防御被视为网络中的路由器跃点。要在其间路由的每个接口都位于不同的子网上。另一方面，透明防火墙是一个第 2 层防火墙，充当“电缆中的块”或“隐蔽的防火墙”，不被视为是到所连接设备的路由器跃点。

系统仅在初始部署时设置防火墙模式。如果您重新应用引导程序设置，则不会使用此设置。

f) 输入逗号分隔列表形式的 **DNS 服务器**。

例如，如果指定 管理中心 主机名，则 威胁防御 使用 DNS。

g) 输入 威胁防御 的**完全限定主机名**。

h) 输入注册期间要在管理中心和设备之间共享的**注册密钥**。

可以为此密钥选择介于 1 至 37 个字符之间的任何文本字符串；添加威胁防御时，需要在管理中心上输入相同的密钥。

i) 输入供威胁防御管理员用户用于 CLI 访问的**密码**。

j) 选择应该发送事件的**事件接口**。如果未指定，系统将使用管理接口。

此接口必须定义为 Firepower 事件接口。

k) 对于容器实例，请将**硬件加密**设置为**已启用**或**已禁用**。

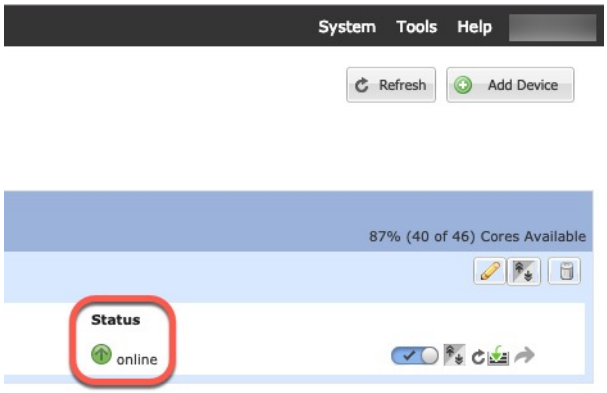
此设置在硬件中启用 TLS 加密加速，并提高某些类型流量的性能。有关详细信息，请参阅《Firepower 管理中心配置指南》。本地实例不支持此功能。要查看分配给该实例的硬件加密资源百分比，请输入 **show hw-crypto** 命令。

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

步骤 8 点击**确定 (OK)** 关闭配置对话框。

步骤 9 点击**保存 (Save)**。

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



登录管理中心

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**胁-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。

  如果您还没有帐户，请点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。

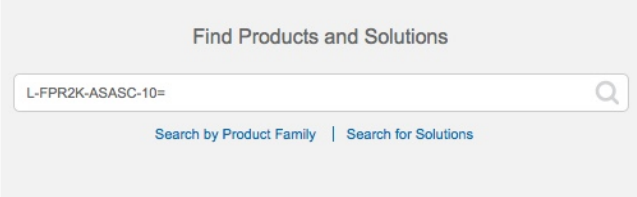
- 您的智能软件许可帐户必须符合强加密 (3DES/AES) 许可证的要求，才能使用某些功能（已使用导出合规性标志启用）。

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Cisco Commerce Workspace上的 **Find Products and Solutions** 搜索字段。搜索以下许可证 PID：

图 *1:* 许可证搜索



注释　　如果未找到 PID，您可以手动将 PID 添加到订单中。

- IPS、恶意软件 防御和 URL 许可证组合：
  - L-FPR4112T-TMC=
  - L-FPR4115T-TMC=
  - L-FPR4125T-TMC=
  - L-FPR4145T-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-FPR4112T-TMC-1Y
  - L-FPR4112T-TMC-3Y
  - L-FPR4112T-TMC-5Y
  - L-FPR4115T-TMC-1Y
  - L-FPR4115T-TMC-3Y
  - L-FPR4115T-TMC-5Y
  - L-FPR4125T-TMC-1Y
  - L-FPR4125T-TMC-3Y
  - L-FPR4125T-TMC-5Y
  - L-FPR4145T-TMC-1Y
  - L-FPR4145T-TMC-3Y
  - L-FPR4145T-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：
  - L-FPR4K-FTD-CAR=

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

将每个逻辑设备分别注册到同一个 管理中心。

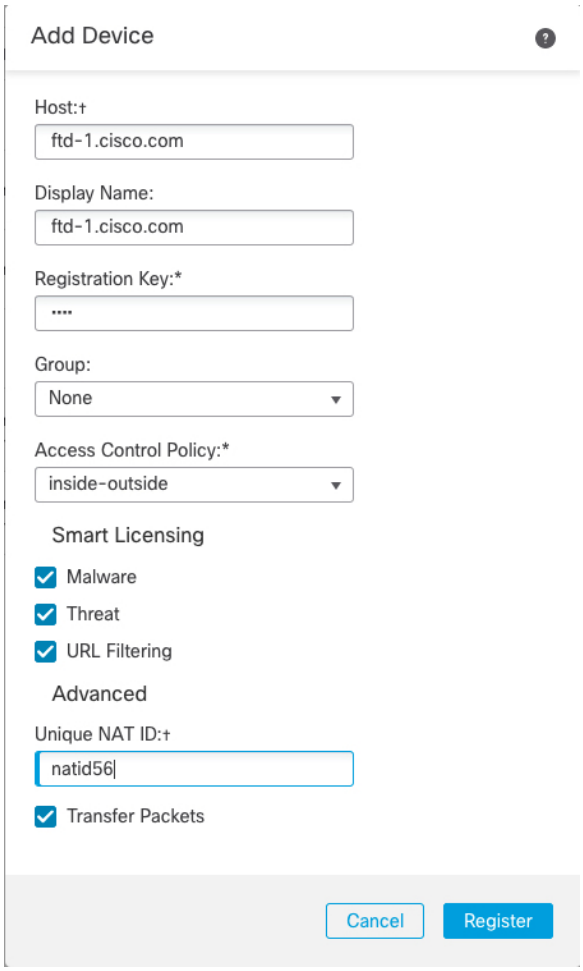
开始之前

- 确保 机箱管理器 **逻辑设备 (Logical Devices)**页面上 威胁防御 逻辑设备的**状态 (Status)** 为**在线 (online)**。
- 收集您在 威胁防御 初始引导程序配置中设置的以下信息（请参阅机箱管理器：添加威胁防御逻辑设备，第 3 页）；
  - 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
- 在 6.7 和更高版本中，如果要使用数据接口进行管理，请在 威胁防御 CLI 上使用 **configure network management-data-interface** 命令。有关详细信息，请参阅 Cisco Secure Firewall Threat Defense 命令参考。

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**。



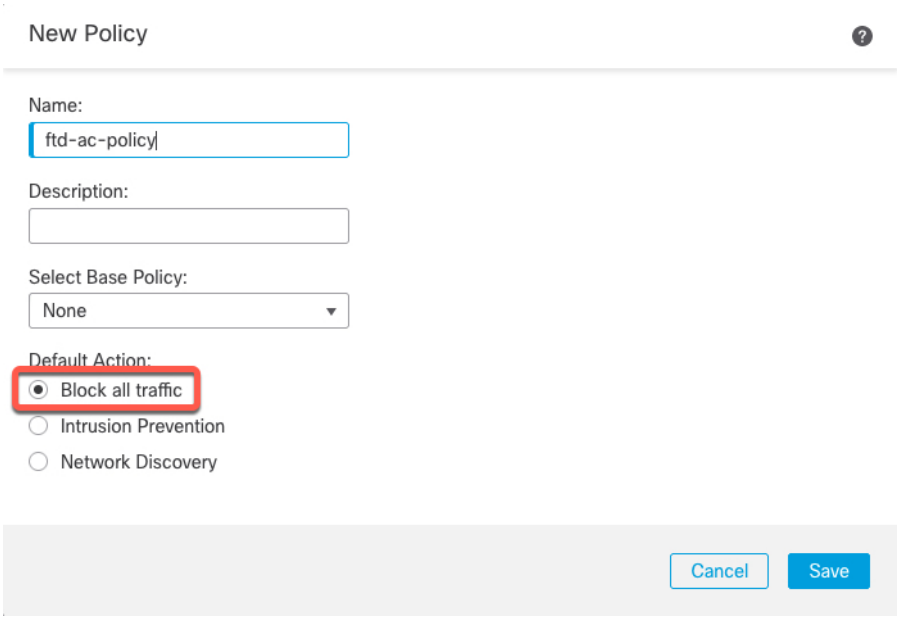
设置以下参数：

- **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 初始引导程序配置中同时指定了 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引导程序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 22 页。

图 *2: New Policy*



- **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 初始引导程序配置中指定的 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 (访问威胁防御 CLI，第 25 页)，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。如果为 管理中心 访问配置了数据接口，请使用 **configure network management-data-interface** 命令。

- NTP - 确保 Firepower 4100 NTP 服务器与**系统 > 配置 > 时间同步**页面上的 管理中心 服务器设定一致。

- 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 13 页。
2	配置 DHCP 服务器，第 17 页。
3	添加默认路由，第 18 页。
4	配置 NAT，第 19 页。
5	允许流量从内部传到外部，第 22 页。
6	部署配置，第 23 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。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。

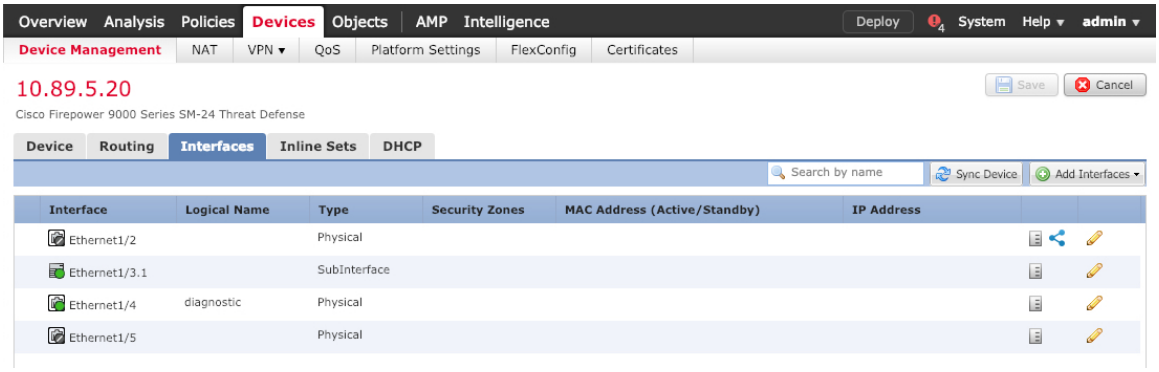
典型的边缘路由情况是通过 DHCP 从 ISP 获取外部接口地址，同时在内部接口上定义静态地址。

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

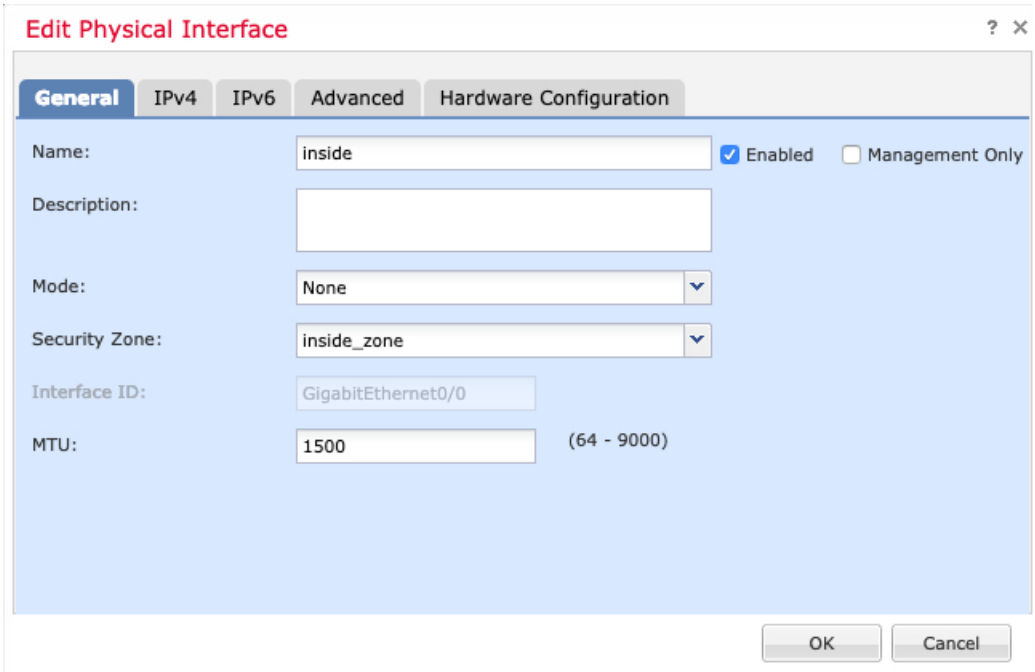
步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**，然后点击防火墙的**编辑**（ ）。

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**。

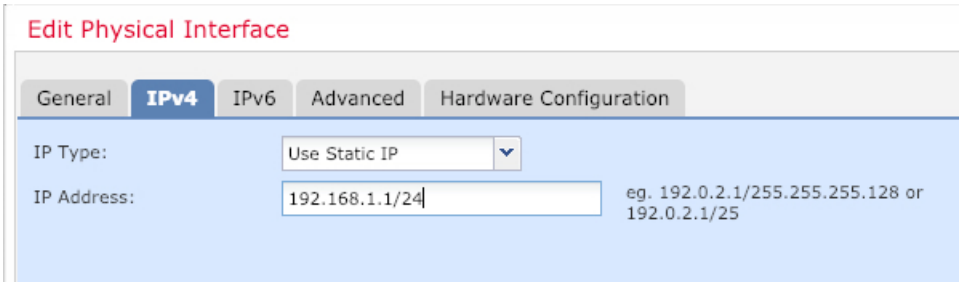
d) 从**安全区域 (Security Zone)** 下拉列表中选择一个现有的内部安全区域，或者点击**新建 (New)** 添加一个新的安全区域。

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**

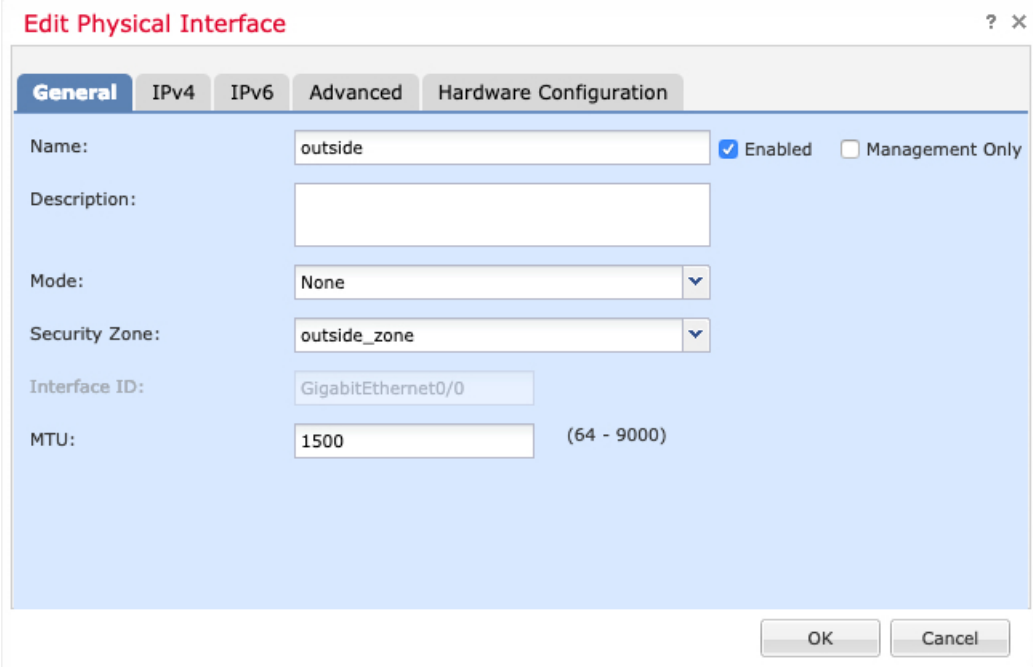


- **IPv6** - 为无状态自动配置选中**自动配置 (Autoconfiguration)** 复选框。

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。

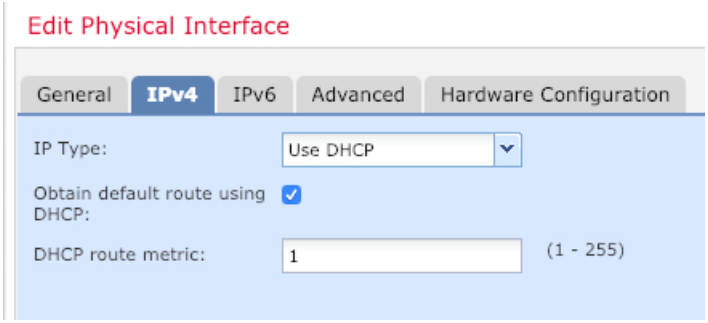
c) 将 **Mode** 保留为 **None**。

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**。

配置 DHCP 服务器

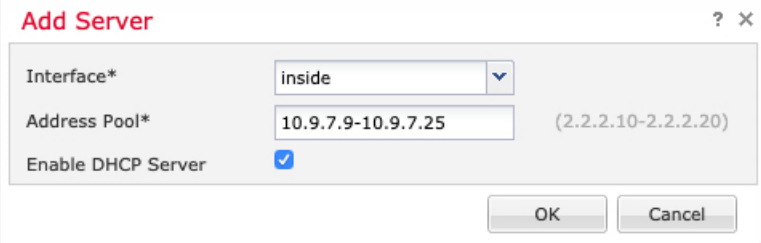
如果希望客户端使用 DHCP 从 威胁防御处获取 IP 地址，请启用 DHCP 服务器。

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**。

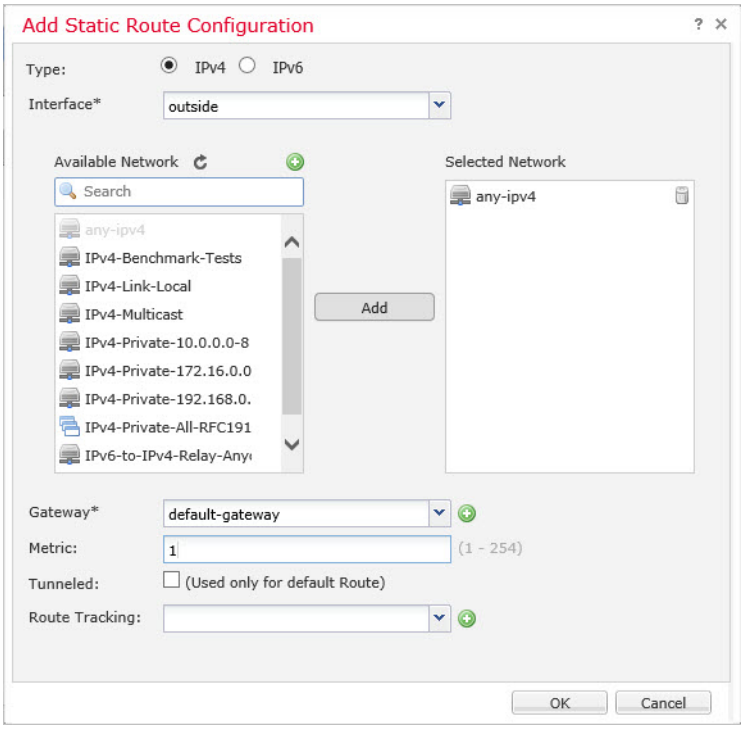
添加默认路由

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**（ ）。

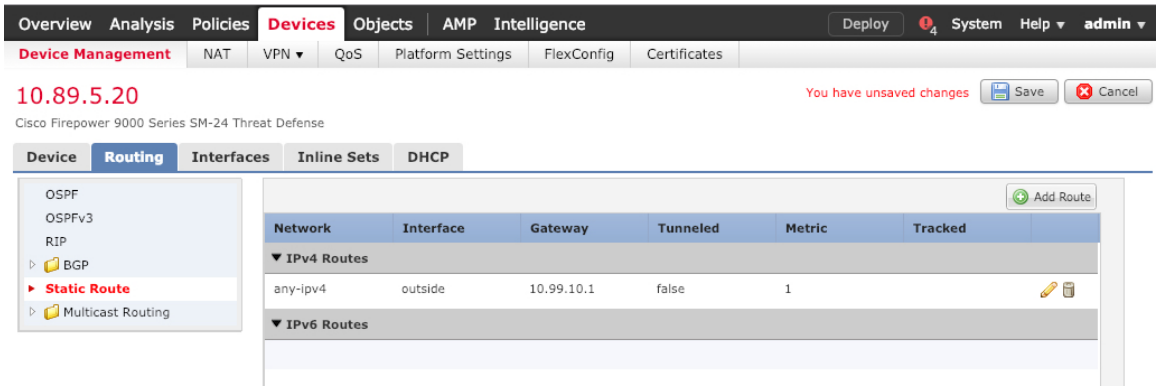
步骤 2 选择**路由 (Route)** > **静态路由 (Static Route)**，点击**添加路由 (Add Route)**，然后设置以下项：



- **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。
- **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 **Add** 将其移至 **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。

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。

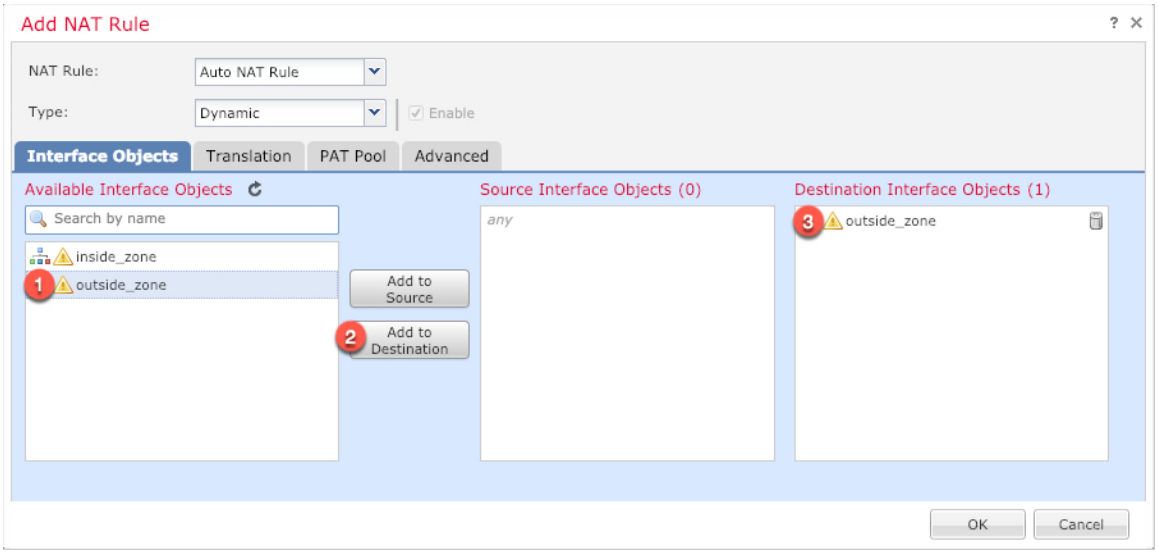
步骤 3 点击**添加规则 (Add Rule)**。

Add NAT Rule 对话框将显示。

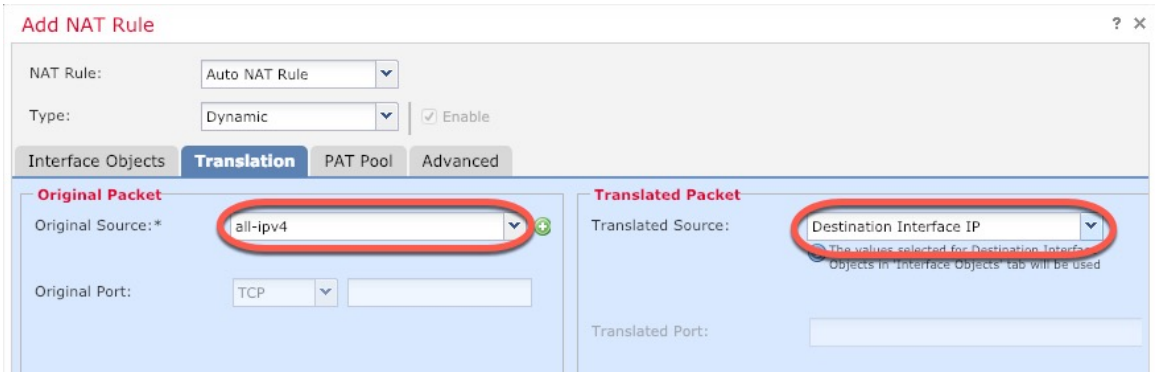
步骤 4 配置基本规则选项：

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

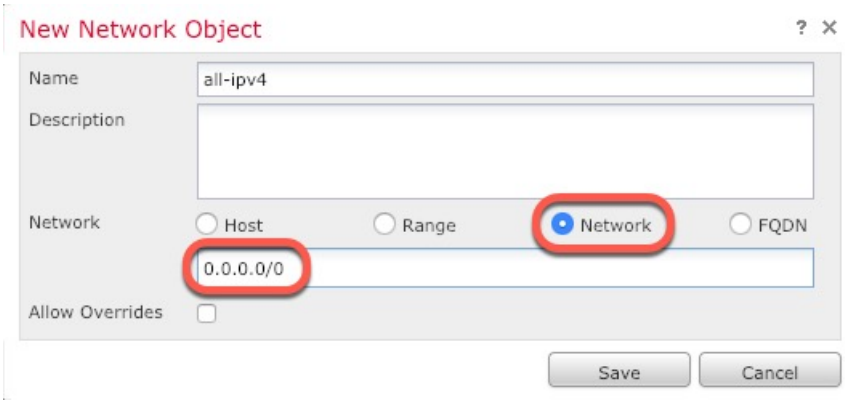
步骤 5 在 **Interface Objects** 页面，将 **Available Interface Objects** 区域中的外部区域添加到 **Destination Interface Objects** 区域。



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)。

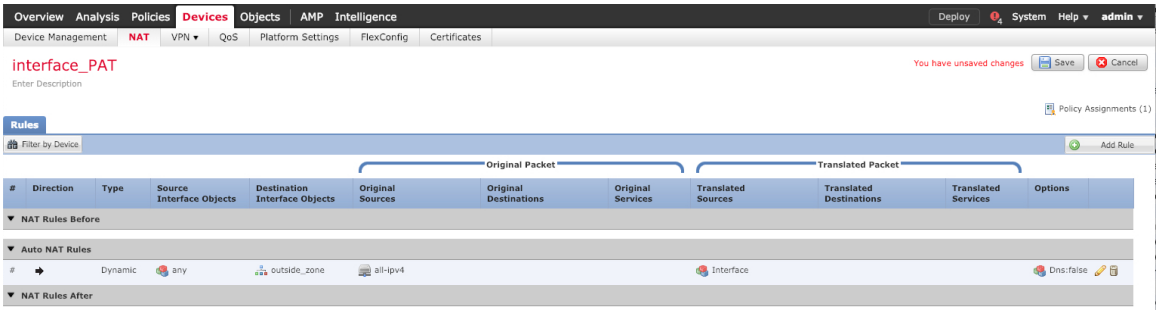


注释　　您不能使用系统定义的 **any-ipv4** 对象，因为自动 NAT 规则在对象定义过程中添加 NAT，并且您无法编辑系统定义的对象。

- **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。

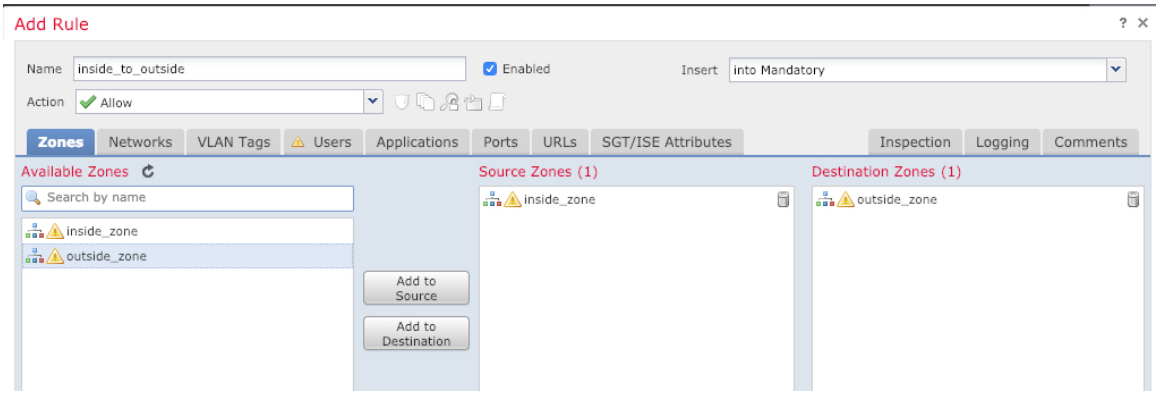
允许流量从内部传到外部

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：



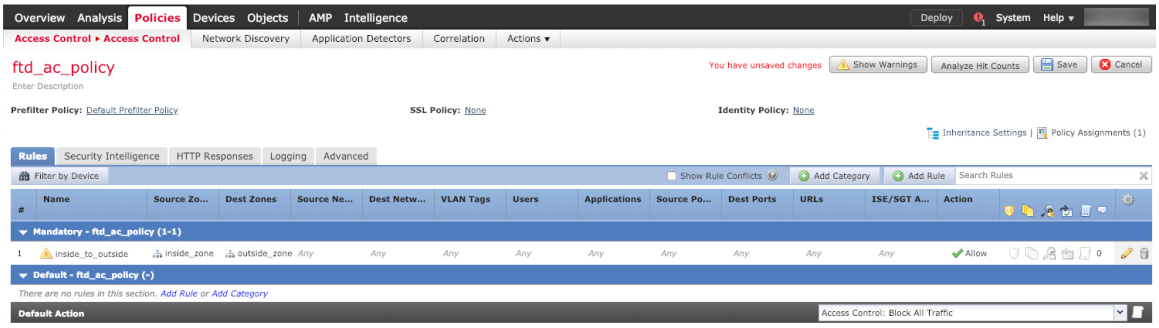
- **名称 (Name)** - 为此规则命名，例如 **inside_to_outside**。
- **源区域 (Source Zones)** - 从**可用区域 (Available Zones)** 中选择内部区域，然后点击**添加到源 (Add to Source)**。

- 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。

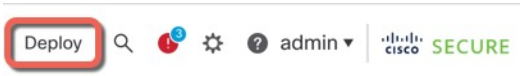
部署配置

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 *3:* 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 *4:* 全部部署

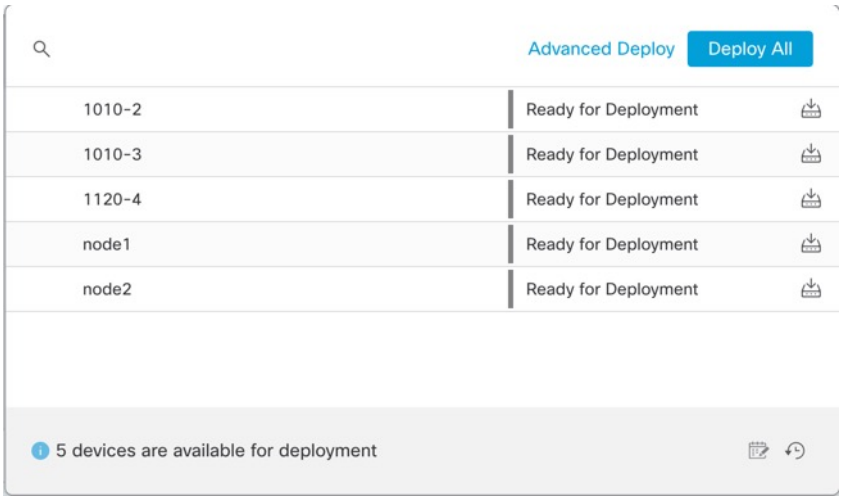
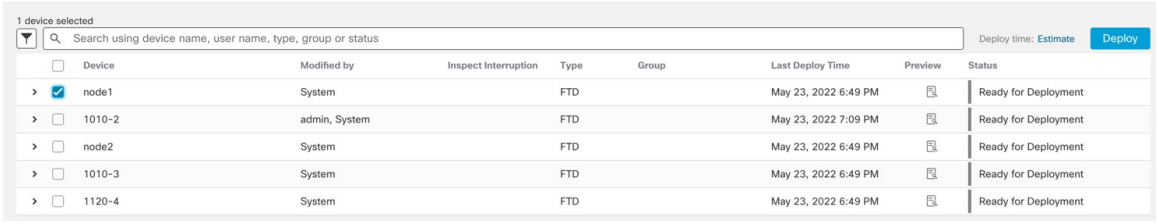
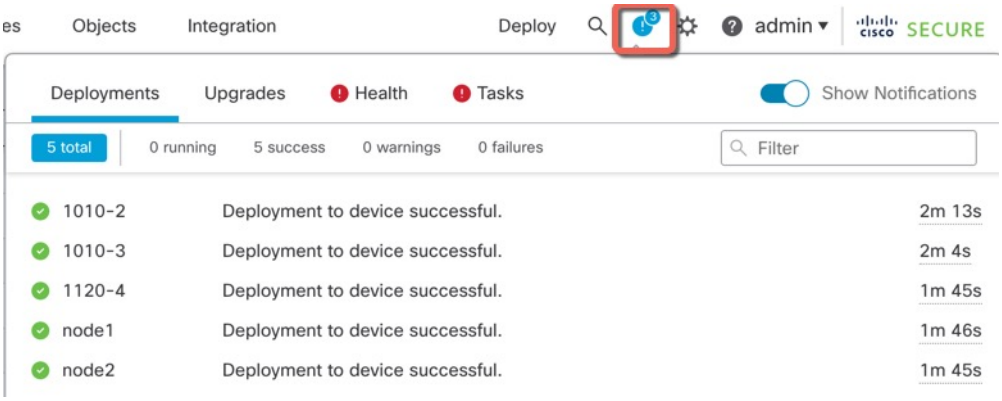


图 *5:* 高级部署



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 *6:* 部署状态



访问威胁防御 CLI

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

过程

步骤 1 （选项 1）通过 SSH 直接连接到 威胁防御管理接口的 IP 地址。

在部署逻辑设备时，您需要设置管理 IP 地址。使用 admin 帐户和初始部署期间设定的密码登录威胁防御。

如果忘记密码，可以通过编辑 机箱管理器 中的逻辑设备来更改密码。

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

a) 连接到 安全引擎。

connect module 1 {**console** | **telnet**}

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

示例：

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

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) 连接到 威胁防御控制台。

connect ftd *name*

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

示例：

```
Firepower-module1> connect ftd FTD_Instance1

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

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

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

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

注释　　对于 6.3 之前的版本，输入 **Ctrl-a, d**。

d) 返回 FXOS CLI的管理引擎层。

要退出控制台：

1. 输入 **~**

   您将退出至 Telnet 应用。

2. 要退出 Telnet 应用，请输入：

   telnet>**quit**

要退出 Telnet 会话：

输入 **Ctrl-],**。

示例

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

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

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect ftd FTD_Instance1

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

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

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

后续步骤

要继续配置 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》。

使用管理中心的威胁防御历史记录

功能名称	版本	功能信息
支持在同一个Firepower 9300 上使用独立的 ASA 和 威胁防御 模块	6.4	您现在可以在同一个 Firepower 9300 上同时部署 ASA 和 威胁防御 逻辑设备。 **注释** 需要 FXOS 2.6.1。
威胁防御 适用于 Firepower 4115、4125 和 4145	6.4	我们推出了 Firepower 4115、4125 和 4145。 **注释** 需要 FXOS 2.6.1。
Firepower 4100/9300 上威胁防御的多实例功能	6.3.0	您现在可以在单个安全引擎/模块上部署多个逻辑设备，每台逻辑设备都设 威胁防御 容器实例。以前，您仅可部署单个本地应用实例。 要确保灵活使用物理接口，可以在FXOS中创建VLAN子接口，还可以在多个实例之间共享接口。资源管理允许您自定义每个实例的性能。 您可以使用在 2 个独立机箱上使用一个容器实例的高可用性。不支持集群。 **注释** 尽管实现方式不同，但多实例功能与 ASA 多情景模式类似。威胁防御 的多情景模式不可用。 新增/修改的 管理中心菜单项： • **设备** > **设备管理** > **编辑**图标> **接口**选项卡 新增/修改的 机箱管理器屏幕： • **概述** > **设备** • **接口 (Interfaces)** > **所有接口 (All Interfaces)** > **新增 (Add New)**下拉菜单 > **子接口 (Subinterface)** • **接口** > **所有接口** > **类型** • **逻辑设备** > **添加设备** • **平台设置** > **Mac 池** • **平台设置** > **资源配置文件**

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。