



使用 Firepower 管理中心管理 Firepower Threat Defense Virtual

本章介绍如何部署使用 FMC 管理的独立式 FTDv 设备。



注释 本文档涵盖最新的 FTDv 版本功能；有关功能更改的详细信息，请参阅[使用 Firepower Management 管理 Firepower Threat Defense Virtual 的历史](#)，第 15 页。如果您使用的是旧版本的软件，请参考您的版本的《FMC 配置指南》中的步骤。

- 关于使用 Firepower 管理中心管理的 Firepower Threat Defense Virtual，第 1 页
- 登录到 Firepower 管理中心，第 2 页
- 向 Firepower 管理中心注册设备，第 2 页
- 配置基本安全策略，第 4 页
- 访问 Firepower 威胁防御 CLI，第 14 页
- 使用 Firepower Management 管理 Firepower Threat Defense Virtual 的历史，第 15 页

关于使用 Firepower 管理中心管理的 Firepower Threat Defense Virtual

Firepower Threat Defense Virtual (FTDv) 是思科 NGFW 解决方案的虚拟化组件。FTDv 提供各种下一代防火墙服务，包括状态防火墙、路由、下一代入侵防御系统(NGIPS)、应用可视性与可控性(AVC)、URL 过滤，以及高级恶意软件防护 (AMP)。

您可以使用 Firepower 管理中心(FMC)管理 FTDv，这是一个功能齐全的多设备管理器，位于单独的服务器上。有关安装 FMC 的详细信息，请参阅[FMC 入门指南](#)。

FTDv 向您分配给 FTDv 虚拟机的管理接口上的 FMC 注册并与之通信。

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

■ 登录到 Firepower 管理中心

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>）。

步骤 1 使用支持的浏览器输入以下 URL。

https://fmc_ip_address

- *fmc_ip_address* - 标识 FMC 的 IP 地址或主机名。

步骤 2 输入您的用户名和密码。

步骤 3 单击“**Log In**”。

向 Firepower 管理中心注册设备

开始之前

确保 FTDv 虚拟机已部署成功、已接通电源并且已首次完成其启动程序。

步骤 1 选择设备 > 设备管理。

步骤 2 从添加下拉列表选择添加设备，然后输入以下参数。

Add Device

Host: [†]	192.168.101.10
Display Name:	192.168.101.10
Registration Key: [*]	1a2b3c4d5e
Group:	None
Access Control Policy: [*]	initial ac
Smart Licensing	
Malware:	<input checked="" type="checkbox"/>
Threat:	<input checked="" type="checkbox"/>
URL Filtering:	<input checked="" type="checkbox"/>
Advanced	
Unique NAT ID: [†]	
Transfer Packets:	<input checked="" type="checkbox"/>

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

Register **Cancel**

- **主机** - 输入要添加的逻辑设备的 IP 地址。如果您在 FTD 引导程序配置中指定了 FMC IP 地址和 NAT ID，则可以将此字段留空。
- **显示名称** - 输入要在 FMC 中显示的逻辑设备的名称。
- **注册密钥** - 输入您在 FTDv 引导程序配置中指定的注册密钥。
- **域** - 如果有多域环境，请将设备分配给分叶域。
- **组** - 如果在使用组，则将其分配给设备组。
- **访问控制策略** - 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，否则选择创建新策略，然后选择封锁所有流量。之后您可以更改此设置以允许流量通过；请参阅[配置访问控制，第 12 页](#)。

New Policy

Name:	ftd_ac_policy
Description:	
Select Base Policy:	None
Default Action:	<input checked="" type="radio"/> Block all traffic <input type="radio"/> Intrusion Prevention <input type="radio"/> Network Discovery

Save **Cancel**

- **智能许可** - 为要部署的功能分配所需的智能许可证：恶意软件（如果您打算使用 AMP 恶意软件检查）、威胁（如果您打算使用入侵防御）或 URL（如果您打算实施基于类别的 URL 过滤）。
- **唯一 NAT ID** - 指定您在 FTDv 启动程序配置中指定的 NAT ID。

配置基本安全策略

- **传输数据包** - 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 单击注册，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 FTDv 注册失败，请检查以下项：

- Ping - 访问 FTD CLI ([访问 Firepower 威胁防御 CLI，第 14 页](#))，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 FTD IP 地址，使用 **configure network {ipv4 | ipv6} manual** 命令。

- NTP - 确保 NTP 服务器与系统 > 配置 > 时间同步页面上的 FMC 服务器设定一致。
- 注册密钥、NAT ID 和 FMC 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 FTDv 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 FMC IP 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。

步骤 1 配置接口，第 5 页

步骤 2 配置 DHCP 服务器，第 8 页

步骤 3 添加默认路由，第 9 页

步骤 4 配置 NAT，第 10 页

步骤 5 配置访问控制，第 12 页

步骤 6 部署配置，第 13 页

配置接口

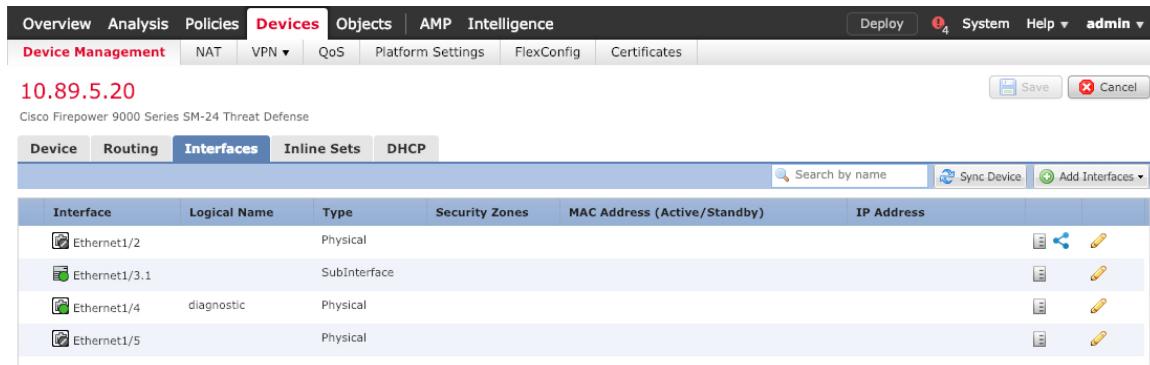
启用 FTDv 接口，为其分配安全区域并设置 IP 地址。通常，您必须至少配置两个接口才能让系统传递有意义的流量。通常，您将拥有面向上游路由器或互联网的外部接口，以及组织网络的一个或多个内部接口。其中一些接口可能是“隔离区”(DMZ)，您可以在其中放置可公开访问的资产，例如 Web 服务器。

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。

步骤 1 选择设备 > 设备管理，然后单击设备的 编辑图标 ()。

步骤 2 单击 Interfaces。

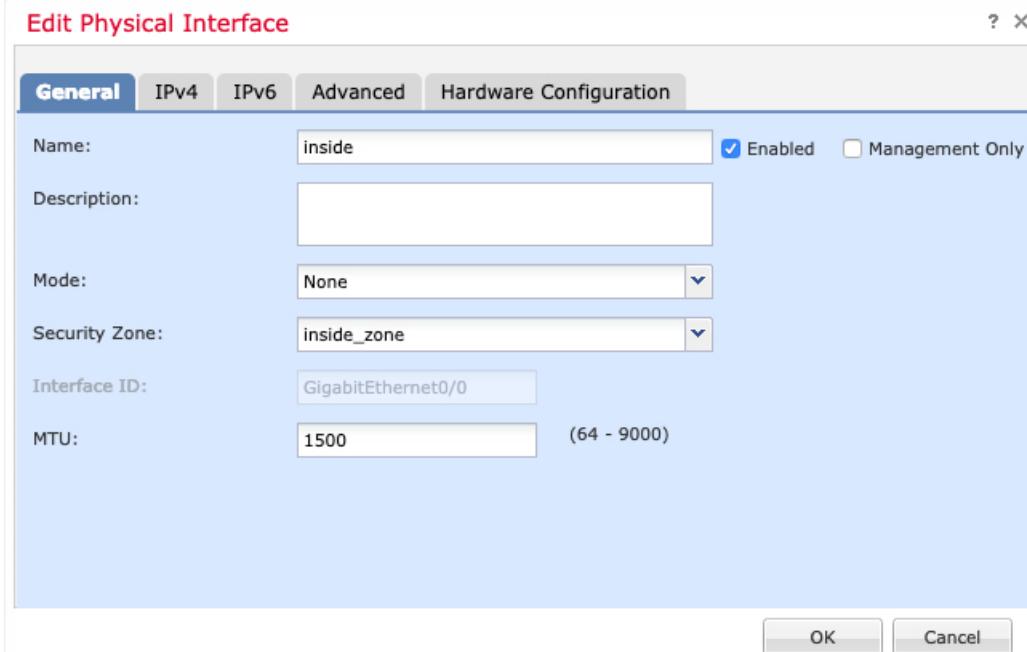


Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Ethernet1/2		Physical			 
Ethernet1/3.1		SubInterface			 
Ethernet1/4	diagnostic	Physical			 
Ethernet1/5		Physical			 

步骤 3 单击要用于内部的接口的 编辑图标 ()。

常规选项卡将显示。

配置接口



- a) 输入长度最大为 48 个字符的名称。

例如，将接口命名为内部。

- b) 选中已启用 (Enabled) 复选框。

- c) 将模式保留为无。

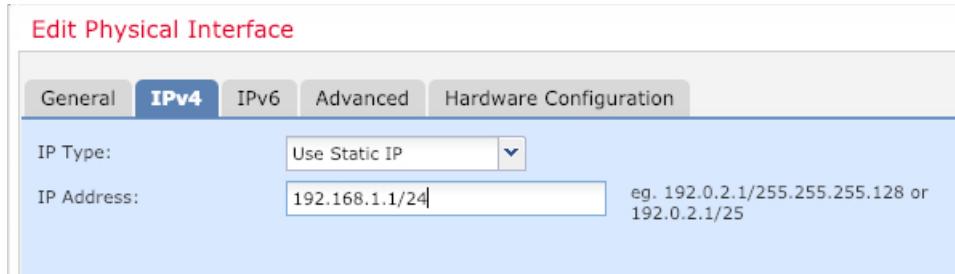
- d) 从安全区域下拉列表中选择一个现有的内部安全区域，或者单击新建添加一个新的安全区域。

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** - 从下拉列表中选择使用静态 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**

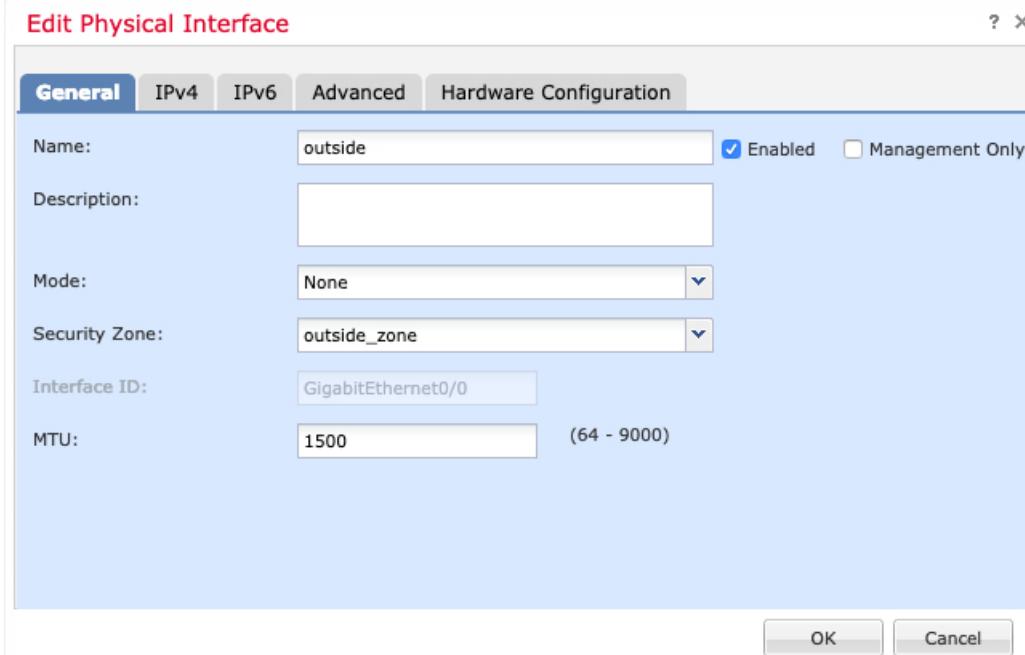


- **IPv6** - 为无状态自动配置选中自动配置复选框。

f) 单击确定。

步骤 4 单击要用于外部的接口的 编辑图标 (-pencil)。

常规选项卡将显示。



a) 输入长度最大为 48 个字符的名称。

例如，将接口命名为外部。

b) 选中已启用 (Enabled) 复选框。

c) 将模式保留为无。

d) 从安全区域下拉列表中选择一个现有的外部安全区域，或者单击新建添加一个新的安全区域。

例如，添加一个名为 outside_zone 的区域。

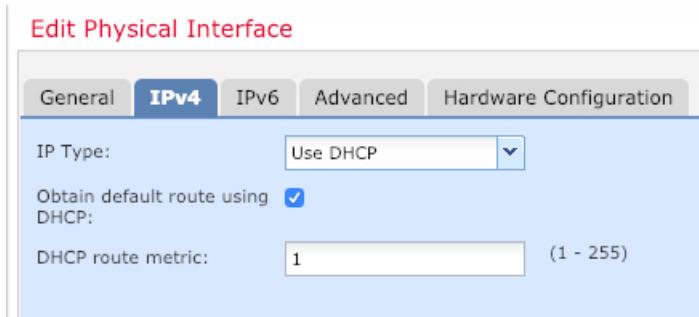
e) 单击 IPv4 和/或 IPv6 选项卡。

- **IPv4** - 选择使用 DHCP，然后配置以下选填参数：

- 使用 DHCP 获取默认路由 - 从 DHCP 服务器获取默认路由。

- **DHCP 路由指标** - 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。

配置 DHCP 服务器



- **IPv6** - 为无状态自动配置选中自动配置复选框。

f) 单击确定。

步骤 5 单击保存。

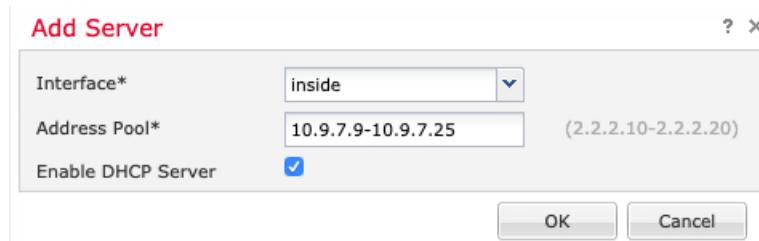
配置 DHCP 服务器

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

步骤 1 选择设备 > 设备管理，然后单击设备的 编辑图标 ()。

步骤 2 选择 DHCP > DHCP 服务器。

步骤 3 在服务器页面上单击添加，然后配置以下选项：



- **接口** -- 从下拉列表中选择接口。
- **地址池** - 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** - 在所选接口上启用 DHCP 服务器。

步骤 4 单击确定。

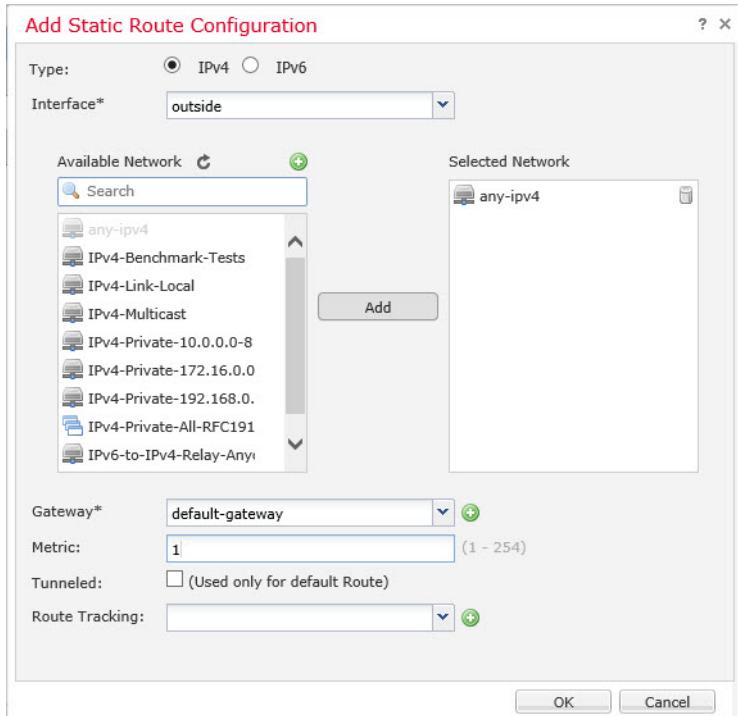
步骤 5 单击保存。

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 > 设备管理 > 路由 > 静态路由页面上的 **IPv4 路由** 或 **IPv6 路由表** 中。

步骤 1 选择设备 > 设备管理，然后单击设备的 编辑图标 ()。

步骤 2 选择路由 > 静态路由，单击添加路由，然后设置以下项：



- **类型** - 根据要添加静态路由的类型，单击 **IPv4** 或 **IPv6** 单选按钮。
- **接口** - 选择出口接口；通常是外部接口。
- **可用网络** - 为 IPv4 默认路由选择 **any-ipv4**，为 IPv6 默认路由选择 **any-ipv6**。
- **网关或 IPv6 网关** - 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** - 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 单击确定。

路由即已添加至静态路由表。

配置 NAT

The screenshot shows the Firepower Threat Defense Virtual device management interface. The top navigation bar includes Overview, Analysis, Policies, Devices (selected), Objects, AMP, and Intelligence. Sub-tabs under Devices include Device Management, NAT, VPN, QoS, Platform Settings, FlexConfig, and Certificates. The main content area has tabs for Device, Routing (selected), Interfaces, Inline Sets, and DHCP. On the left, a sidebar lists OSPF, OSPFv3, RIP, BGP (with Static Route selected), and Multicast Routing. The main panel displays network routes. Under IPv4 Routes, there is one entry: 'any-ipv4' to 'outside' gateway '10.99.10.1' with metric 1. There is also a section for IPv6 Routes which is currently empty.

步骤 4 单击保存。

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)。

步骤 1 选择设备 > NAT，然后单击新策略 > 威胁防御 NAT。

步骤 2 为策略命名，选择要使用策略的设备，然后单击保存。

The screenshot shows the 'New Policy' dialog box. It has fields for Name (set to 'interface_PAT') and Description. Below these, the 'Targeted Devices' section shows 'Available Devices' on the left and 'Selected Devices' on the right. The 'Selected Devices' list contains '192.168.0.16', which is highlighted with a red circle. At the bottom are 'Save' and 'Cancel' buttons.

策略即已添加 FMC。您仍然需要为策略添加规则。

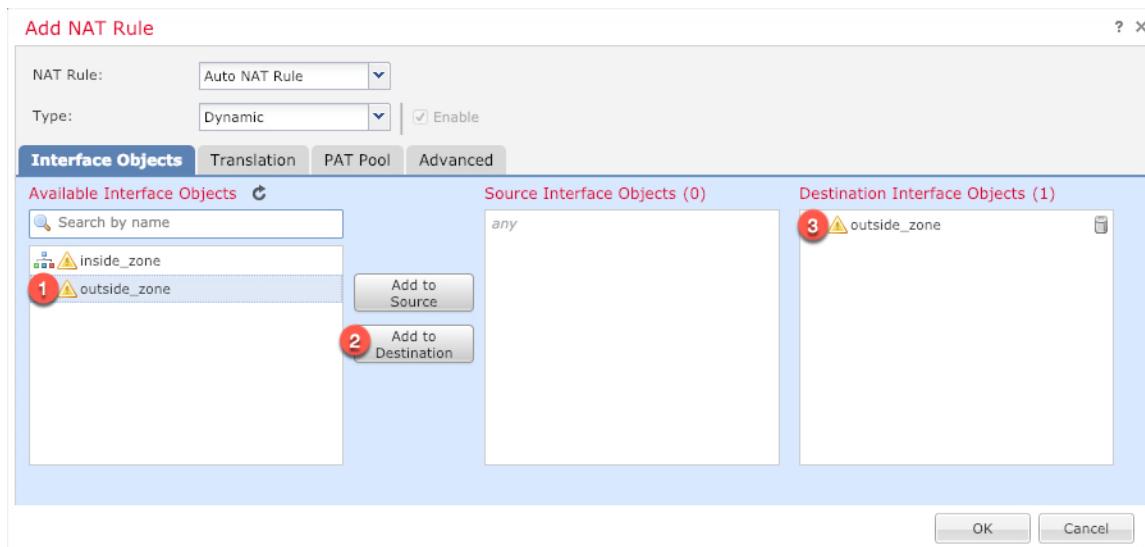
步骤 3 单击添加规则。

添加 NAT 规则对话框将显示。

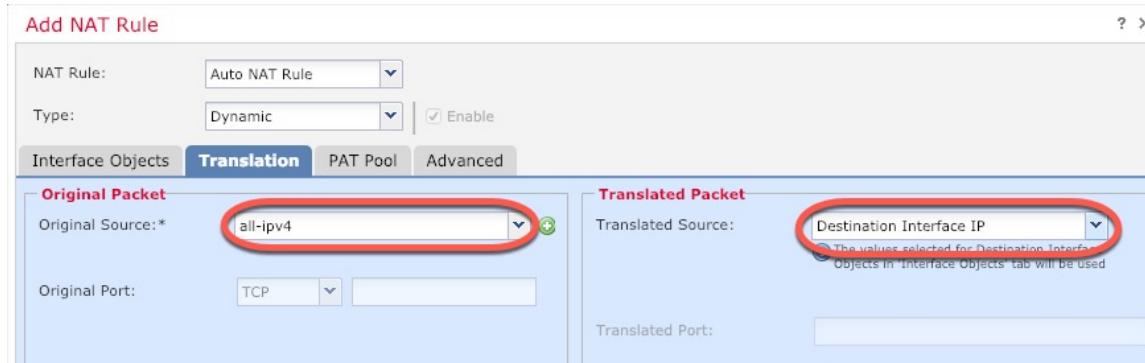
步骤 4 配置基本规则选项：



步骤 5 在接口对象页面，将可用接口对象区域中的外部区域添加到目标接口对象 区域。

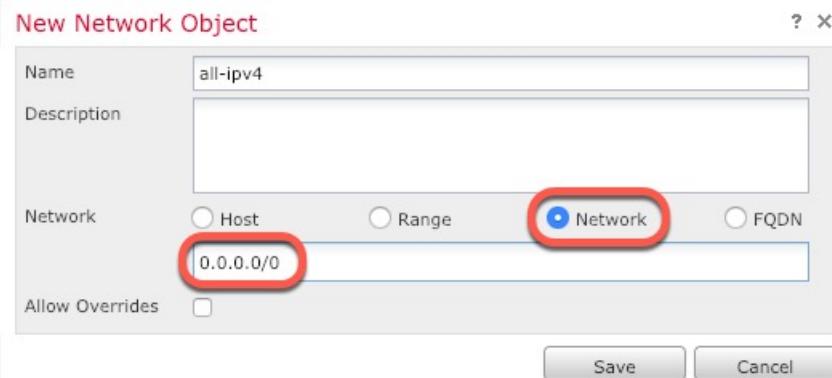


步骤 6 在转换页面上配置以下选项：



- 原始源 - 单击 添加图标 (⊕) 为所有 IPv4 流量添加网络对象 (0.0.0.0/0)。

配置访问控制



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。

- 转换后的源 - 选择目标接口 **IP**。

步骤 7 单击保存以添加规则。

规则即已保存至规则表。

步骤 8 单击 NAT 页面上的保存以保存更改。

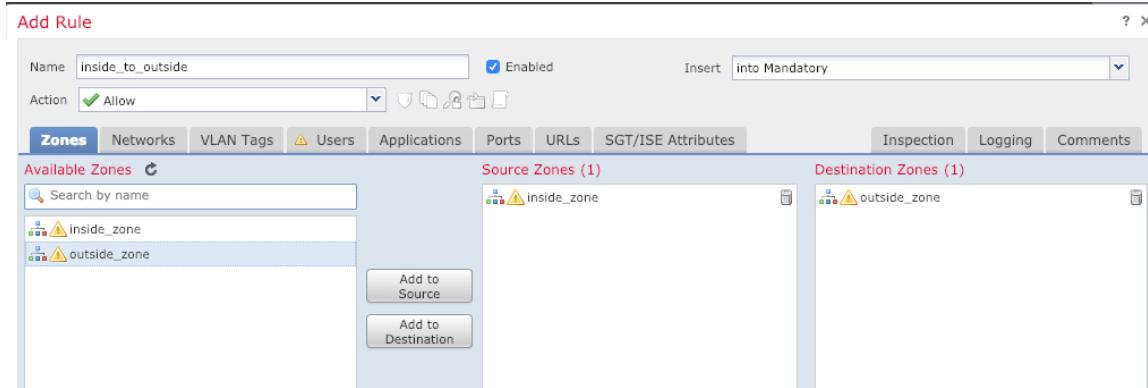
配置访问控制

如果您在使用 FMC 注册 FTDv 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。

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

步骤 2 单击添加策略并设置以下参数：



- 名称 - 为此规则命名，例如 **inside_to_outside**。
- 源区域 - 从可用区域中选择内部区域，然后单击添加到源。
- 目标区域 - 从可用区域中选择外部区域，然后单击添加到目标。

其他设置保留原样。

步骤 3 单击添加。

规则即已添加至规则表。

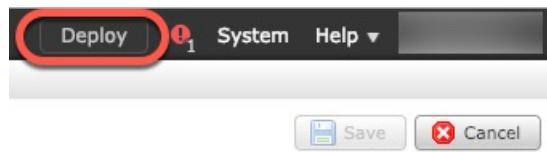
步骤 4 单击保存。

部署配置

将配置更改部署到 FTDv；在部署之前，您的所有更改都不会在设备上生效。

步骤 1 单击右上方的部署。

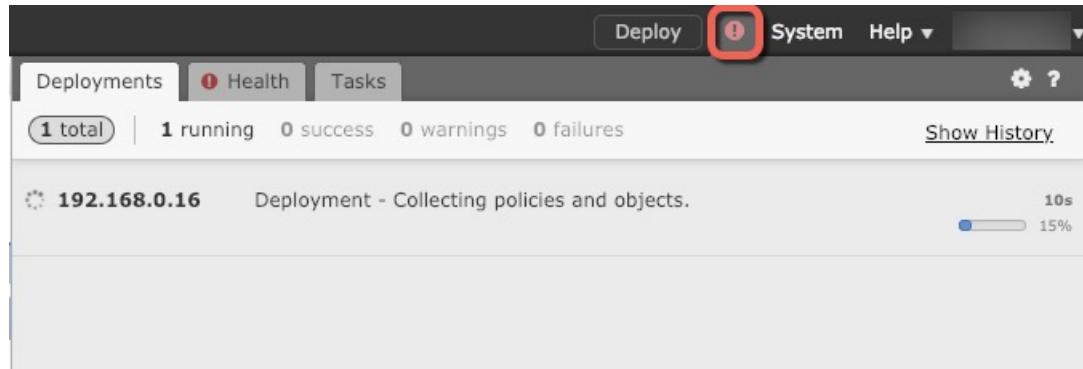
访问 Firepower 威胁防御 CLI



步骤 2 选择部署策略对话框中的设备，然后单击部署。

	Device	Inspect Interruption	Type	Group	Current Version
<input checked="" type="checkbox"/>	192.168.0.16	No	FTD		2019-02-28 07:11 AM

步骤 3 确保部署成功。单击菜单栏中部署按钮右侧的图标可以查看部署状态。



访问 Firepower 威胁防御 CLI

您可以使用 FTDv 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 VMware 控制台连接。

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

在部署虚拟机时，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 FTDv。

步骤 2（选项 2）打开 VMware 控制台并使用默认用户名 **admin** 帐户和初始部署期间设定的密码登录。

使用 Firepower Management 管理 Firepower Threat Defense Virtual 的历史

功能名称	平台版本	功能信息
FMC 管理	6.0	初始支持。

■ 使用 Firepower Management 管理 Firepower Threat Defense Virtual 的历史