



## 《适用于 KVM 的 Cisco Firepower Threat Defense Virtual 入门指南》

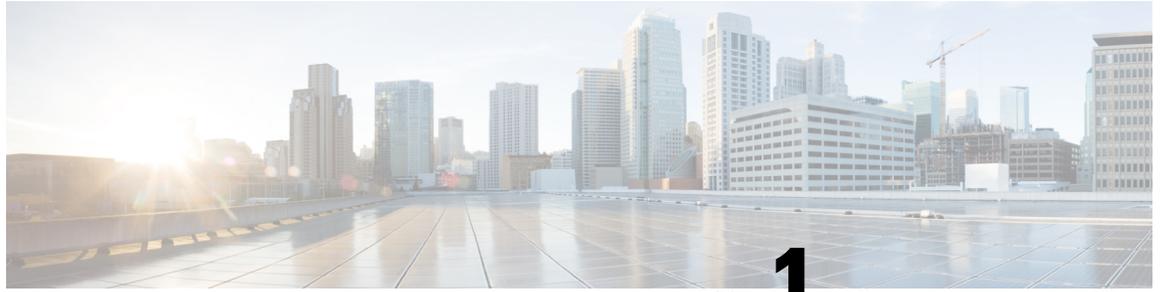
首次发布日期: 2019 年 4 月 24 日

上次修改日期: 2021 年 6 月 28 日

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883





# 第 1 章

## Firepower Threat Defense Virtual 和 KVM 入门

思科 Firepower Threat Defense Virtual (FTDv) 将 Cisco Firepower 新一代防火墙功能带到虚拟环境，支持采用一致的安全策略来跟踪物理、虚拟和云环境以及云之间的工作负载。

本章介绍这些 FTDv 功能如何使用基于内核的虚拟机 (KVM) 虚拟机监控程序环境，包括功能支持、系统要求、指导原则和限制。本章还介绍了管理 FTDv 的选项。

在开始部署之前，了解您的管理选项非常重要。您可以使用 Firepower 管理中心 或 Firepower 设备管理器 管理和监控 FTDv。其他管理选项也可能可用

- [关于使用 KVM 的 FTDv 部署，第 1 页](#)
- [如何管理您的 Firepower 设备，第 1 页](#)
- [系统要求，第 2 页](#)
- [网络准则和最佳实践，第 3 页](#)

### 关于使用 KVM 的 FTDv 部署

KVM 是适用于基于 x86 硬件的 Linux 且包含虚拟化扩展（例如英特尔 VT）的完全虚拟化解决方案。其中包含可加载的内核模块 `kvm.ko`（用于提供核心虚拟化基础设施）和一个处理器特定模块（例如 `kvm-intel.ko`）。

您可以使用 KVM 来运行多个运行未修改的操作系统映像的虚拟机。每个虚拟机都有专用的虚拟化硬件：网卡、磁盘、图形适配器等等。

### 如何管理您的 Firepower 设备

您可以通过两种方法来管理您的 Firepower Threat Defense 设备。

#### Firepower 设备管理器

Firepower 设备管理器 (FDM) 板载集成的管理器。

FDM 是一个基于 Web 的配置界面，在部分 Firepower Threat Defense 设备上可用。您可以通过 FDM 配置最常用于小型网络的软件的基本功能。此产品专为包括一台或几台设备的网络而设计，在这种网络中，无需使用高功率多设备管理器来控制包含许多 Firepower Threat Defense 设备的大型网络。



**注释** 有关支持 FDM 的 Firepower Threat Defense 设备的列表，请参阅 [《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》](#)。

## Firepower 管理中心

思科 Firepower 管理中心 (FMC)。

如果要管理大量设备或要使用 Firepower Threat Defense 支持的更复杂的功能和配置，请使用 FMC（而不是集成的 FDM）来配置您的设备。



**重要事项** 您不能同时使用 FDM 和 FMC 管理 Firepower 设备。FDM 集成管理功能启用后，将无法使用 FMC 来管理 Firepower 设备，除非您禁用本地管理功能并重新配置管理功能以使用 FMC。另一方面，当您向 FMC 注册 Firepower 设备时，FDM 板载管理服务会被禁用。



**注意** 目前，Cisco 不提供将 FDM Firepower 配置迁移到 FMC 的选项，反之亦然。选择为 Firepower 设备配置的管理类型时，请考虑这一点。

## 系统要求

有关 Firepower Threat Defense Virtual 支持的虚拟机管理程序的最新信息，请参阅 [思科 Firepower 兼容性指南](#)。

根据所需部署的实例数量和使用要求，Firepower Threat Defense Virtual 部署所使用的具体硬件可能会有所不同。每个 FTDv 实例都需要服务器保证最小的资源配置，这包括内存数量、CPU 数和磁盘空间。

表 1: FTDv 设备资源要求

| 设置     | 值  |
|--------|--|
| 核心和内存数 | <p><b>6.4 及更高版本</b></p> <p>FTDv 具有可调的 vCPU 和内存资源。支持的 vCPU/内存对值有三种：</p> <ul style="list-style-type: none"> <li>• 4vCPU/8GB（默认）</li> <li>• 8vCPU/16GB</li> <li>• 12vCPU/24GB</li> </ul> <p>注释 要更改 vCPU/内存值，必须先断开 FTDv 设备的电源。仅支持上述三种组合。</p>   |
|        | <p><b>6.3 及更低版本</b></p> <p>FTDv 具有固定的 vCPU 和内存资源。支持的 vCPU/内存对值只有一个：</p> <ul style="list-style-type: none"> <li>• 4vCPU/8GB</li> </ul> <p>注释 不允许调整 vCPU 和内存。</p>  |
| 硬盘调配容量 | <ul style="list-style-type: none"> <li>• 50 GB</li> <li>• 可调节设置。支持 virtio 块设备</li> </ul>   |
| vNIC   | <p>KVM 上的 FTDv 支持以下虚拟网络适配器：</p> <ul style="list-style-type: none"> <li>• <b>VIRTIO</b> - Virtio 是 KVM 中 IO 虚拟化的主要平台，为 IO 虚拟化的虚拟机监控程序提供通用框架。主机实施是在用户空间 qemu 中，因此主机中不需要驱动程序。</li> <li>• <b>IXGBE-VF</b> - ixgbe-vf (10 Gbit/s) 驱动程序支持只能在支持 SR-IOV 的内核上激活的虚拟功能设备。SR-IOV 需要正确的平台和操作系统支持；有关详细信息，请参阅“对 SR-IOV 的支持”。</li> </ul> |

## 网络准则和最佳实践

- 需要两个管理接口和两个数据接口来启动。



**注 释** FTDv 默认配置将管理接口、诊断接口和内部接口置于同一子网上。

- 支持 virtio 驱动程序。
  - 支持 SR-IOV 的 ixgbe-vf 驱动程序。
  - 支持共计 10 个接口
- FTDv 的默认配置假设您将管理接口（管理和诊断）和内部接口置于同一子网，并且管理地址使用内部地址作为访问互联网的网关（经过外部接口）。
  - FTDv 首次启动时，必须启用至少四个接口。如果没有四个接口，您的系统将无法部署
  - FTDv 支持共计 10 个接口 - 1 个管理接口、1 个诊断接口，以及最多 8 个用于数据流量的网络接口。接口到网络分配必须遵循以下顺序：
    - 1. 管理接口（必需）
    - 2. 诊断接口（必需）
    - 3. 外部接口（必需）
    - 4. 内部接口（必需）
    - 5-10 数据接口（可选）

请查看 FTDv 接口的以下网络适配器、源网络和目标网络的对应关系：

表 2: 源网络与目标网络的映射

| 网络适配器          | 源网络                | 目标网络               | 功能         |
|----------------|--------------------|--------------------|------------|
| vnic0*         | Management0-0      | Management0/0      | 管理         |
| vnic1          | Diagnostic0-0      | Diagnostic0/0      | Diagnostic |
| vnic2*         | GigabitEthernet0-0 | GigabitEthernet0/0 | 外部         |
| vnic3*         | GigabitEthernet0-1 | GigabitEthernet0/1 | 内部         |
| *重要信息。连接到同一子网。 |                    |                    |            |

- 不支持克隆虚拟机。
- 对于控制台访问，通过 telnet 支持终端服务器。

## CPU 模式

KVM 可以模拟许多不同的 CPU 类型。对于 VM，通常应选择与主机系统的 CPU 密切匹配的处理器类型，因为这意味着主机 CPU 功能（也称为 CPU 标志）将在 VM 中可用。您应将 CPU 类型设置为**主机**，在这种情况下，虚拟机将具有与主机系统完全相同的 CPU 标志。

## 对 SR-IOV 的支持

SR-IOV 虚拟功能需要特定的系统资源。除支持 SR-IOV 功能的 PCIe 适配器之外，还需要支持 SR-IOV 的服务器。您必须了解以下硬件注意事项：

- 不同供应商和设备的 SR-IOV NIC 功能有所不同，包括可用的 VF 数量。支持以下 NIC：
  - [英特尔以太网服务器适配器 X710](#)
  - [Intel 以太网服务器适配器 X520 - DA2](#)
- 并非所有 PCIe 插槽都支持 SR-IOV。
- 支持 SR-IOV 的 PCIe 插槽可能具有不同的功能。
- x86\_64 多核 CPU - Intel 沙桥或更高版本（推荐）。



---

**注** 我们在 Intel 的 Broadwell CPU (E5-2699-v4) 上以 2.3Ghz 的频率对 FTDv 进行了测试。

---

- 核心
  - 每个 CPU 插槽至少 8 个物理核心
  - 8 个核心必须位于一个插槽中。



---

**注** 建议通过 CPU 固定来实现完整的吞吐量。

---

- 请查阅制造商的文档，以了解系统对 SR-IOV 的支持情况。对于 KVM，您可以验证 SR-IOV 支持方面的 [CPU 兼容性](#)。请注意，对于 KVM 上的 FTDv，我们仅支持 x86 硬件。





## 第 2 章

# 部署 Firepower Threat Defense Virtual

本章介绍将 Firepower Threat Defense Virtual 部署到 KVM 环境的程序。

- 使用 KVM 进行部署的前提条件，第 7 页
- 准备 Day 0 配置文件，第 8 页
- 启动 Firepower Threat Defense Virtual，第 10 页

## 使用 KVM 进行部署的前提条件

- 从 Cisco.com 下载 Firepower Threat Defense Virtual qcow2 文件并将其放在 Linux 主机上：

<https://software.cisco.com/download/navigator.html>



**注** 需要 Cisco.com 登录信息和思科服务合同。

- 本文档出于示例部署目的，假设您使用 Ubuntu 14.04 LTS。在 Ubuntu 18.04 LTS 主机之上安装以下软件包：
  - qemu-kvm
  - libvirt-bin
  - bridge-utils
  - virt-manager
  - virtinst
  - virsh tools
  - genisoimage
- 性能受主机及其配置的影响。通过调整主机，您可以最大化 KVM 上的 Firepower Threat Defense Virtual 吞吐量。有关通用的主机调整概念，请参阅[网络功能虚拟化：具备 Linux 和 Intel 架构的宽带远程访问服务器的服务质量](#)。

- Ubuntu 18.04 LTS 的有用优化包括以下各项：
  - `macvtap` - 高性能 Linux 网桥；您可以使用 `macvtap`，而不是 Linux 网桥。您必须配置特定设置才能使用 `macvtap`，而不是 Linux 网桥。
  - 透明大页 - 增加内存页面大小，在 Ubuntu 18.04 中默认开启。
  - 禁用超线程 - 用于将两个 vCPU 减少到一个单核。
  - `txqueuelength` - 用于将默认 `txqueuelength` 增加到 4000 个数据包并减少丢包率。
  - 固定 - 用于将 `qemu` 和 `vhost` 进程固定到特定 CPU 内核；在某些情况下，固定可显著提高性能。
- 有关优化基于 RHEL 的分布的信息，请参阅《[Red Hat Enterprise Linux6 虚拟化调整和优化指南](#)》。
- 有关 KVM 与 Firepower 系统的兼容性，请参阅《[Cisco Firepower Threat Defense Virtual 的兼容性](#)》。

## 准备 Day 0 配置文件

在启动 FTDv 之前，您可以准备一个 Day 0 配置文件。此文件是一个文本文件，其中包含了在部署虚拟机时需要应用的初始配置数据。此初始配置将放入您选择的工作目录中名为“`day0-config`”的文本文件，并写入首次启动时装载和读取的 `day0.iso` 文件。



### 重要事项

该 `day0.iso` 文件必须在首次启动期间可用。

如果使用 Day 0 配置文件进行部署，该过程将允许您执行 FTDv 设备的整个初始设置。可以指定：

- 接受《最终用户许可协议》(EULA)。
- 系统的主机名。
- 管理员账户的新管理员密码。
- 管理模式；请参阅[如何管理您的 Firepower 设备，第 1 页](#)。

您可以将本地管理设置为是，或者输入 Firepower 管理中心 字段（`FmcIp`、`FmcRegKey` 和 `FmcNatId`）的信息。对于您未使用的管理模式，保留字段为空。

- 初始防火墙模式；设置初始防火墙模式：**已路由**或**透明**。

如果您打算使用本地 Firepower 设备管理器 (FDM) 管理部署，可以仅为防火墙模式输入**已路由**。不能使用 FDM 配置透明防火墙模式接口。

- 使设备可以在管理网络上进行通信的网络设置。

如果您在没有 Day 0 配置文件的情况下进行部署，则必须在启动后配置 Firepower 系统所需的设置；有关更多信息，请参阅[在没有 Day 0 配置文件的情况下启动](#)，第 14 页。



注释 我们在本示例中使用的是 Linux，但对于 Windows 也有类似的实用程序。

## SUMMARY STEPS

1. 在名为“day0-config”的文本文件中输入 Firepower Threat Defense Virtual 的 CLI 配置。添加网络设置和关于管理 Firepower 管理中心的信息。
2. 通过将文本文件转换成 ISO 文件生成虚拟 CD-ROM:
3. 为每个要部署的 FTDv 重复创建唯一的默认配置文件。

## DETAILED STEPS

**步骤 1** 在名为“day0-config”的文本文件中输入 Firepower Threat Defense Virtual 的 CLI 配置。添加网络设置和关于管理 Firepower 管理中心的信息。

示例:

```
#Firepower Threat Defense
{
  "EULA": "accept",
  "Hostname": "ftdv-production",
  "AdminPassword": "Admin123",
  "FirewallMode": "routed",
  "DNS1": "1.1.1.1",
  "DNS2": "1.1.1.2",
  "DNS3": "",
  "IPv4Mode": "manual",
  "IPv4Addr": "10.12.129.44",
  "IPv4Mask": "255.255.0.0",
  "IPv4Gw": "10.12.0.1",
  "IPv6Mode": "disabled",
  "IPv6Addr": "",
  "IPv6Mask": "",
  "IPv6Gw": "",
  "FmcIp": "",
  "FmcRegKey": "",
  "FmcNatId": "",
  "ManageLocally": "Yes"
}
```

在 Day 0 配置文件的本地管理中输入是以使用本地 Firepower 设备管理器 (FDM)；输入 Firepower 管理中心 字段 (**FmcIp**、**FmcRegKey** 和 **FmcNatId**) 的值。对于您未使用的管理选项，将这些字段留空。

**步骤 2** 通过将文本文件转换成 ISO 文件生成虚拟 CD-ROM:

示例:

```
/usr/bin/genisoimage -r -o day0.iso day0-config
```

或

示例:

```
/usr/bin/mkisofs -r -o day0.iso day0-config
```

**步骤 3** 为每个要部署的 FTDv 重复创建唯一的默认配置文件。

#### 下一步做什么

- 如果使用 `virt-install`，请在 `virt-install` 命令中添加以下行：

```
--disk path=/home/user/day0.iso,format=iso,device=cdrom \
```

- 如果使用 `virt-manager`，则可以使用 `virt-manager` GUI 创建虚拟 CD-ROM；请参阅[使用图形用户界面 \(GUI\) 进行启动](#)，第 12 页。

## 启动 Firepower Threat Defense Virtual

### 使用部署脚本启动

使用基于 `virt-install` 的部署脚本启动 FTDv。

请注意，您可以通过选择适合您环境的最佳访客缓存模式来优化性能。正在使用的缓存模式不仅会影响是否发生数据丢失，还会影响到磁盘性能。

每个 KVM 访客磁盘接口都可以指定以下缓存模式之一：`writethrough`、`writeback`、`none`、`directsync` 或 `unsafe`。`writethrough` 提供读取缓存。`writeback` 提供读取和写入缓存。`directsync` 会绕过主机页面缓存。`unsafe` 可能会缓存所有内容，并忽略来自访客的刷新请求。

- 当主机遇到突然断电时，`cache=writethrough` 有助于降低 KVM 访客计算机上的文件损坏。我们建议使用 `writethrough` 模式。
- 但是，由于 `cache=writethrough` 的磁盘 I/O 写入次数高于 `cache=none`，所以该模式也会影响磁盘性能。
- 如果删除了 `--disk` 选项上的 `cache` 参数，则默认值为 `writethrough`。
- 未指定缓存选项还有可能大幅减少创建虚拟机所需的时间。这是因为，一些较旧的 RAID 控制器的磁盘缓存能力较差。因此，禁用磁盘缓存 (`cache=none`)，从而使用默认值 `writethrough`，有助于确保数据完整性。
- 从版本 6.4 开始，FTDv 随可调的 vCPU 和内存资源一起部署。在 6.4 版之前，FTDv 部署为固定配置 4vCPU/8GB 设备。请参阅下表，了解每个 FTDv 平台大小的 `--vcpus` 和 `--ram` 参数所支持的值。

表 3: virt-install 支持的 vCPU 和内存参数

| --vcpus | --ram | FTDv 平台规模      |
|---------|-------|----------------|
| 4       | 8192  | 4vCPU/8GB (默认) |
| 8       | 16384 | 8vCPU/16GB     |
| 12      | 24576 | 12vCPU/24GB    |

**步骤 1** 创建名为 “virt\_install\_ftdv.sh” 的 virt-install 脚本。

FTDv 虚拟机 (VM) 的名称在此 KVM 主机上的所有其他虚拟机中必须是唯一的。FTDv 可支持多达 10 个网络接口。此示例使用了四个接口。虚拟 NIC 必须是 Virtio。

**注释** FTDv 的默认配置假定您将管理接口、诊断接口和内部接口置于同一子网上。系统至少需要 4 个接口才能成功启动。虚拟 NIC 必须是 Virtio。接口到网络分配必须遵循以下顺序：

- 1. 管理接口 (必需)
- 2. 诊断接口 (必需)
- 3. 外部接口 (必需)
- 4. 内部接口 (必需)
- 5. (可选) 数据接口 - 最多 6 个

**示例:**

```
virt-install \
  --connect=qemu:///system \
  --network network=default,model=virtio \
  --network network=default,model=virtio \
  --network network=default,model=virtio \
  --network network=default,model=virtio \
  --name=ftdv \
  --arch=x86_64 \
  --cpu host \
  --vcpus=8 \
  --ram=16384 \
  --os-type=linux \
  --os-variant=generic26 \
  --virt-type=kvm \
  --import \
  --watchdog i6300esb,action=reset \
  --disk path=<ftd_filename>.qcow2,format=qcow2,device=disk,bus=virtio,cache=none \
  --disk path=<day0_filename>.iso,format=iso,device=cdrom \
  --console pty,target_type=serial \
  --serial tcp,host=127.0.0.1:<port>,mode=bind,protocol=telnet \
  --force
```

**步骤 2** 运行 virt\_install 脚本:

**示例:**

```
/usr/bin/virt_install_ftdv.sh
```

```
Starting install...
Creating domain...
```

此时将出现一个窗口，其中显示虚拟机的控制台。您可以看到虚拟机正在启动。启动虚拟机需要几分钟时间。一旦虚拟机停止启动，您便可以从控制台屏幕发出 CLI 命令。

### 下一步做什么

接下来的步骤取决于您选择的管理模式。

- 如果为本地管理 (**ManageLocally**) 选择否 (**No**)，您将使用 Firepower 管理中心 管理 FTDv；请参阅 [使用 Firepower 管理中心管理 Firepower Threat Defense Virtual](#)，第 25 页。
- 如果为本地管理 (**ManageLocally**) 选择是 (**Yes**)，您将使用集成的 Firepower 设备管理器 管理 FTDv；请参阅 [使用 Firepower 设备管理器管理 Firepower Threat Defense Virtual](#)，第 17 页。

有关如何选择管理选项的概述，请参阅 [如何管理您的 Firepower 设备](#)，第 1 页。

## 使用图形用户界面 (GUI) 进行启动

有多个开源选项可用于通过 GUI 来管理 KVM 虚拟机。以下程序使用 virt-manager（也称为虚拟机管理器）启动 FTDv。Virt-manager 是用于创建和管理访客虚拟机的图形化工具。



**注释** KVM 可以模拟许多不同的 CPU 类型。对于 VM，通常应选择与主机系统的 CPU 密切匹配的处理器类型，因为这意味着主机 CPU 功能（也称为 CPU 标志）将在 VM 中可用。您应将 CPU 类型设置为 **主机**，在这种情况下，虚拟机将具有与主机系统完全相同的 CPU 标志。

**步骤 1** 启动 virt-manager（应用 > 系统工具 > 虚拟机管理器）。

系统可能要求您选择虚拟机监控程序和/或输入您的 root 口令。

**步骤 2** 单击左上角的按钮，打开新建虚拟机 (**New VM**) 向导。

**步骤 3** 输入虚拟机的详细信息：

- 对于操作系统，选择导入现有的磁盘映像 (**Import existing disk image**)。

此方法允许您向其导入磁盘映像（包含预安装的可启动操作系统）。

- 单击 **继续 (Forward)** 继续操作。

**步骤 4** 加载磁盘映像：

- 单击 **浏览...(Browse...)**，选择映像文件。
- 选择通用 (*Generic*) 作为 **操作系统类型 (OS type)**。
- 单击 **继续 (Forward)** 继续操作。

**步骤 5** 配置内存和 CPU 选项:

从版本 6.4 开始, FTDv 随可调的 vCPU 和内存资源一起部署。在 6.4 版之前, FTDv 部署为固定配置 4vCPU/8GB 设备。请参阅下表, 了解每个 FTDv 平台大小的 --vcpus 和 --ram 参数所支持的值。

表 4: 虚拟机管理器支持的 vCPU 和内存参数

| CPU | 内存    | FTDv 平台规模      |
|-----|-------|----------------|
| 4   | 8192  | 4vCPU/8GB (默认) |
| 8   | 16384 | 8vCPU/16GB     |
| 12  | 24576 | 12vCPU/24GB    |

- 针对 FTDv 平台大小设置内存 (RAM) 参数。
- 针对 FTDv 平台大小设置对应的 CPU 参数。
- 单击继续 (Forward) 继续操作。

**步骤 6** 选中安装前自定义配置 (Customize configuration before install) 框, 指定一个名称 (Name), 然后单击完成 (Finish)。

执行此操作将会打开另一个向导, 您可以在其中添加、删除和配置虚拟机的硬件设置。

**步骤 7** 修改 CPU 配置:

从左侧面板中, 选择处理器 (Processor), 然后选择配置 (Configuration) > 复制主机 CPU 配置 (Copy host CPU configuration)。

这会将物理主机的 CPU 型号和配置应用于您的 VM。

**步骤 8** 配置虚拟磁盘:

- 从左侧面板中, 选择磁盘 1 (Disk 1)。
- 选择高级选项 (Advanced options)。
- 将磁盘总线设为 Virtio。
- 将存储格式设为 qcow2。

**步骤 9** 配置串行控制台:

- 从左侧面板中, 选择控制台 (Console)。
- 选择删除 (Remove), 删除默认的控制台。
- 单击添加硬件 (Add Hardware), 添加一台串行设备。
- 对于设备类型 (Device Type), 选择 TCP net 控制台 (tcp) (TCP net console [tcp])。
- 对于模式 (Mode), 选择服务器模式 (绑定) (Server mode [bind])。
- 对于主机 (Host), 输入 0.0.0.0 作为 IP 地址, 然后输入唯一的端口 (Port) 号。
- 选中使用 Telnet 框。
- 配置设备参数。

**步骤 10** 配置看门狗设备, 在 KVM 访客挂起或崩溃时自动触发某项操作:

- 单击添加硬件 (Add Hardware), 添加一台看门狗设备。
- 对于型号 (Model), 选择默认值 (default)。

在没有 Day 0 配置文件的情况下启动

c) 对于操作 (**Action**)，选择强制重置访客 (*Forcefully reset the guest*)。

**步骤 11** 配置至少 4 个虚拟网络接口。

单击**添加硬件 (Add Hardware)** 以添加接口，然后选择 **macvtap** 或指定共享设备名称（使用网桥名称）。

**注释** KVM 上的 FTDv 支持共计 10 个接口 - 1 个管理接口、1 个诊断接口，以及最多 8 个用于数据流量的网络接口。接口到网络分配必须遵循以下顺序：

vnic0 - 管理接口（必需）

vnic1—诊断接口（必需）

vnic2 - 外部接口（必需）

vnic3 - 内部接口（必需）

vnic4-9 - 数据接口（可选）

**重要事项** 请确保将 vnic0、vnic1 和 vnic3 映射到同一子网。

**步骤 12** 如果使用 Day 0 配置文件进行部署，则为 ISO 创建虚拟 CD-ROM：

a) 单击**添加硬件(Add Hardware)**。

b) 选择**存储 (Storage)**。

c) 单击**选择托管或其他现有存储 (Select managed or other existing storage)**，然后浏览至 ISO 文件的位置。

d) 对于**设备类型 (Device type)**，选择 *IDE CDROM*。

**步骤 13** 配置虚拟机的硬件后，单击**应用 (Apply)**。

**步骤 14** 单击**开始安装 (Begin installation)**，以便 virt-manager 使用您指定的硬件设置创建虚拟机。

### 下一步做什么

接下来的步骤取决于您选择的管理模式。

- 如果为**本地管理 (Manage Locally)**选择否 (**No**)，您将使用 Firepower 管理中心管理 FTDv；请参阅[使用 Firepower 管理中心管理 Firepower Threat Defense Virtual](#)，第 25 页。
- 如果为**本地管理 (Manage Locally)**选择是 (**Yes**)，您将使用集成的 Firepower 设备管理器管理 FTDv；请参阅[使用 Firepower 设备管理器管理 Firepower Threat Defense Virtual](#)，第 17 页。

有关如何选择管理选项的概述，请参阅[如何管理您的 Firepower 设备](#)，第 1 页。

## 在没有 Day 0 配置文件的情况下启动

由于 FTDv 设备没有 Web 界面，如果您在没有 Day 0 配置文件的情况下进行部署，必须使用 CLI 来设置虚拟设备。

首次登录新部署的设备时，必须阅读并接受 EULA。然后，请按照设置提示更改管理员密码，并配置设备的网络设置和防火墙模式。

按照设置提示操作时，如遇单选问题，选项会列在括号内，例如 (y/n)。默认值会列在方括号内，例如 [y]。按 Enter 键确认选择。



**注释** 要在完成初始设置后更改虚拟设备的任何设置，必须使用 CLI。

**步骤 1** 打开 FTDv 的控制台。

**步骤 2** 在 **firepower login** 提示符下，使用默认凭据（**username admin**，**password Admin123**）登录。

**步骤 3** 当 Firepower Threat Defense 系统启动时，安装向导会提示您执行以下操作，并输入配置系统所需的下列信息：

- 接受 EULA
- 新管理员密码
- IPv4 或 IPv6 配置
- IPv4 或 IPv6 DHCP 设置
- 管理端口 IPv4 地址和子网掩码，或者 IPv6 地址和前缀
- 系统名称
- 默认网关
- DNS 设置
- HTTP 代理
- 管理模式（需要进行本地管理）

**步骤 4** 检查设置向导的设置。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。

**步骤 5** 根据提示完成系统配置。

**步骤 6** 当控制台返回到 **firepower #** 提示符时，确认设置是否成功。

**步骤 7** 关闭 CLI：

### 下一步做什么

接下来的步骤取决于您选择的管理模式。

- 如果为启用本地管理器 (**Enable Local Manager**) 选择否 (**No**)，您将使用 Firepower 管理中心管理 FTDv；请参阅[使用 Firepower 管理中心管理 Firepower Threat Defense Virtual](#)，第 25 页。
- 如果为启用本地管理器 (**Enable Local Manager**) 选择是 (**Yes**)，您将使用集成的 Firepower 设备管理器管理 FTDv；请参阅[使用 Firepower 设备管理器管理 Firepower Threat Defense Virtual](#)，第 17 页。

有关如何选择管理选项的概述，请参阅[如何管理您的 Firepower 设备](#)，第 1 页。

在没有 Day 0 配置文件的情况下启动



## 第 3 章

# 使用 Firepower 设备管理器管理 Firepower Threat Defense Virtual

本章介绍如何部署使用 FDM 管理的独立式 FTDv 设备。要部署高可用性对，请参阅 FDM 配置指南。

- [关于使用 Firepower 设备管理器管理的 Firepower Threat Defense Virtual](#)，第 17 页
- [初始配置](#)，第 18 页
- [如何在 Firepower 设备管理器中配置设备](#)，第 20 页

## 关于使用 Firepower 设备管理器管理的 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 设备管理器 (FDM) 管理 FTDv，这是部分 Firepower Threat Defense 型号中包含的基于 Web 的设备设置向导。您可以通过 FDM 配置最常用于小型网络的软件的基本功能。此产品专为包括一台或几台设备的网络而设计，在这种网络中，无需使用高功率多设备管理器来控制包含许多 Firepower Threat Defense 设备的大型网络。

如果要管理大量设备或要使用 Firepower Threat Defense 支持的更复杂的功能和配置，请使用 Firepower 管理中心（而不是集成的 Firepower 设备管理器）来配置您的设备。有关详细信息，请参阅[使用 Firepower 管理中心管理 Firepower Threat Defense Virtual](#)，第 25 页。

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。

### 默认配置

FTDv 默认配置将管理接口和内部接口置于同一子网上。您的管理接口必须具有互联网连接，才能使用智能许可并获取系统数据库的更新。

因此，默认配置的设计使您可以将 Management0-0 和 GigabitEthernet0-1（内部）两个接口都连接到虚拟交换机上的同一网络。默认管理地址使用内部 IP 地址作为网关。因此，管理接口路由通过内部接口，然后通过外部接口连通互联网。

您还可以选择将 Management0-0 连接到与用于内部接口的子网不同的子网，只要使用具有互联网接入的网络即可。确保为网络正确配置管理接口 IP 地址和网关。

FTDv 首次启动时，必须启用至少四个接口：

- 虚拟机的第一个接口 (Management0-0) 是管理接口。
- 虚拟机上的第二个接口是诊断接口 (Diagnostic0-0)。
- 虚拟机的第三个接口 (GigabitEthernet0-0) 是外部接口。
- 虚拟机的第四个接口 (GigabitEthernet0-1) 是内部接口。

您还可以添加最多六个额外的数据流量接口，使数据接口的总数达到八个。如果添加额外的数据接口，请确保源网络映射到正确的目标网络，而且每个数据接口都映射到一个唯一的子网或 VLAN。请参阅“配置 VMware 接口”。

## 初始配置

您必须完成初始配置，才能使 FTDv 在网络中正常运行，其中包括配置将安全设备插入网络以及将其连接到互联网或其他上游路由器所需的地址。您可以通过以下两种方式进行系统初始配置：

- 使用 FDM Web 界面（推荐）。FDM 在您的网络浏览器中运行。使用该界面可配置、管理和监控系统。
- 使用命令行界面 (CLI) 设置向导（可选）。可以使用 CLI 设置向导（而不是 FDM）进行初始配置，并可以使用 CLI 执行故障排除。您仍然可以使用 FDM 来配置、管理和监控系统；请参阅（可选）“启动 Firepower 威胁防护 CLI 向导”。

以下主题介绍如何使用这些界面来执行系统初始配置。

## 启动 Firepower 设备管理器

在首次登录 Firepower 设备管理器 (FDM) 时，系统会通过设备设置向导指导您完成初始系统配置。

**步骤 1** 打开浏览器并登录 FDM。如果您未在 CLI 中进行初始配置，请通过 <https://192.168.45.45> 打开 Firepower 设备管理器。

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

**步骤 3** 如果是首次登录系统，而且您未使用过 CLI 安装向导，系统将提示您阅读并接受“最终用户许可协议”以及更改管理员密码。只有完成这些步骤，才能继续。

**步骤 4** 为外部接口和管理接口配置以下选项，然后单击下一步 (Next)。

**注释** 单击下一步 (**Next**) 后，您的设置将部署到设备中。该接口将命名为 “outside”，并添加到 “outside\_zone” 安全区。确保您的设置正确。

- a) **外部接口 (Outside Interface)** - 即连接到网关调制解调器或路由器的数据端口。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。

**配置 IPv4 (Configure 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 (**Off**)，不配置 IPv4 地址。

**配置 Ipv6 (Configure 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 (**Off**)，不配置 IPv6 地址。

- b) **管理接口**

**DNS 服务器 (DNS Servers)** - 系统管理地址的 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，请单击使用 **OpenDNS (Use OpenDNS)** 以重新将合适的 IP 地址载入字段。

**防火墙主机名 (Firewall Hostname)** - 系统管理地址的主机名。

**注释** 在使用设备设置向导配置 Firepower Threat Defense 设备时，系统会为出站和入站流量提供两个默认访问规则。您可以在完成初始配置后更改这些访问规则。

**步骤 5** 配置系统时间设置，然后单击下一步 (**Next**)。

- a) **时区 (Time Zone)** - 选择系统时区。
- b) **NTP 时间服务器 (NTP Time Server)** - 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。

**步骤 6** 为系统配置智能许可证。

只有具有智能许可证账户，才能获取和应用系统需要的许可证。最初，可以使用为期 90 天的评估许可证，以后再设置智能许可。

要立即注册设备，请单击链接登录您的智能软件管理器账户，生成新的令牌，并将该令牌复制到编辑框。

要使用评估许可证，请选择启动 **90 日评估期而不注册 (Start 90 day evaluation period without registration)**。如需稍后注册设备并获取智能许可证，请单击菜单中的设备名称打开设备控制面板 (**Device Dashboard**)，然后单击智能许可证 (**Smart Licenses**) 组中的链接。

**步骤 7** 单击完成 (**Finish**)。

---

### 下一步做什么

- 使用 Firepower 设备管理器配置设备；请参阅[如何在 Firepower 设备管理器中配置设备](#)，第 20 页。

## 如何在 Firepower 设备管理器中配置设备

完成设置向导后，您的设备应该会正常工作并应部署了下列基本策略：

- 内部和外部接口的安全区域。
- 信任所有内部到外部流量的访问规则。
- 接口 NAT 规则，用于将所有内部到外部流量转换到外部接口 IP 地址上的唯一端口。
- 在内部接口或网桥组上运行的 DHCP 服务器。

以下步骤概述了可能需要配置的其他功能。请单击页面上的帮助按钮(?)，获取有关每个步骤的详细信息。

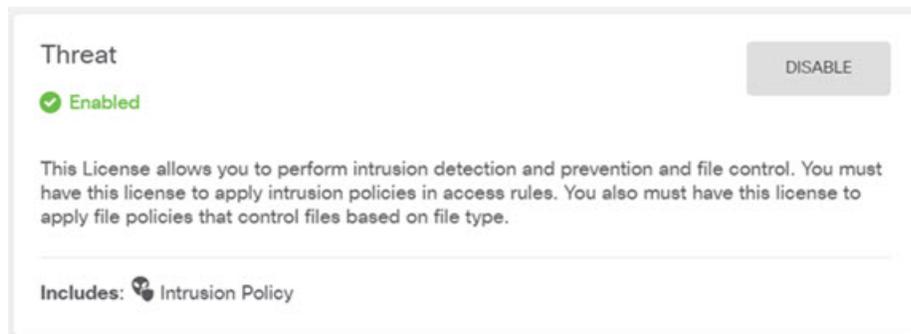
**步骤 1** 选择设备 (Device)，然后单击智能许可证 (Smart License) 组中的查看配置 (View Configuration)。

对于您想要使用的可选许可证 (威胁、恶意软件、URL)，单击启用 (Enable)。如果在安装过程中注册设备，还可启用所需的 RA VPN 许可证。如果不确定是否需要使用某个许可证，请参阅该许可证的说明。

如果尚未注册，可以从该页面执行该操作。单击申请注册 (Request Register)，并按照说明执行操作。请在评估版许可证到期前进行注册。

例如，以下是启用的威胁许可证：

图 1: 已启用的威胁许可证



**步骤 2** 如果配置了其他接口，请选择设备 (Device)，然后单击接口 (Interfaces) 组中的查看配置 (View Configuration) 并配置每个接口。

可以为其他接口创建网桥组或配置单独的网络，或同时采用这两种方法。单击每个接口的编辑图标 (🔗)，定义 IP 地址和其他设置。

以下示例将一个接口配置为“隔离区”(DMZ)，可以将可公开访问的资产 (例如 Web 服务器) 放在该区域中。完成后单击保存 (Save)。

图 2: 编辑接口

**Edit Physical Interface**

Interface Name: dmz      Status:

Description:

**IPv4 Address**    IPv6 Address    Advanced Options

Type: Static

IP Address and Subnet Mask: 192.168.6.1 / 24  
e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

**步骤 3** 如果已配置新接口，请选择对象 (Objects)，然后从目录中选择安全区域 (Security Zones)。

根据需要编辑或创建新区域。每个接口都必须属于一个区域，因为需要根据安全区域而不是接口来配置策略。配置接口时不能将其放在区域中，因此每当创建新接口或更改现有接口的用途之后，都必须编辑区域对象。

以下示例显示如何为 DMZ 接口创建一个新的 DMZ 区域。

图 3: 安全区域对象

**Add Security Zone**

Name: dmz-zone

Description:

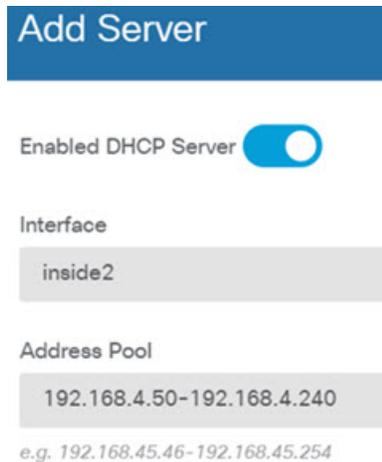
Interfaces: +  
dmz

**步骤 4** 如果要让内部客户端使用 DHCP 从设备获取 IP 地址，请选择**设备 (Device) > 系统设置 (System Settings) > DHCP 服务器 (DHCP Server)**，然后选择**DHCP 服务器 (DHCP Server)** 选项卡。

内部接口已配置了 DHCP 服务器，但可以编辑地址池或甚至将其删除。如果配置了其他内部接口，则在这些接口上设置 DHCP 服务器是非常典型的做法。单击 +，为每个内部接口配置服务器和地址池。

此外，您还可以在**配置 (Configuration)** 选项卡中对为客户端提供的 WINS 和 DNS 列表进行精细调整。以下示例显示如何在 inside2 接口（地址池为 192.168.4.50-192.168.4.240）上设置 DHCP 服务器。

图 4: DHCP 服务器



**步骤 5** 选择**设备 (Device)**，然后单击路由 (**Routing**) 组中的**查看配置 (View Configuration)**（或创建第一个静态路由 (**Create First Static Route**)），配置默认路由。

默认路由通常指向位于外部接口之外的上游或 ISP 路由器。默认的 IPv4 路由适用于 any-ipv4 (0.0.0.0/0)，而默认的 IPv6 路由适用于 any-ipv6 (:::0/0)。为所使用的每个 IP 版本创建路由。如果使用 DHCP 获取外部接口的地址，则可能已经拥有所需的默认路由。

**注释** 此页面上定义的路由仅适用于数据接口，而不会影响管理接口。在**设备 > 系统设置 > 管理接口**上设置管理网关。

以下示例显示 IPv4 的默认路由。在此示例中，isp-gateway 是用于标识 ISP 网关 IP 地址的网络对象（必须从 ISP 中获取地址）。可以通过单击**网关 (Gateway)** 下拉菜单底部的**创建新网络 (Create New Network)**，来创建该对象。

图 5: 默认路由

The screenshot shows the 'Add Static Route' configuration interface. It includes the following fields and options:

- Protocol:** Radio buttons for IPv4 (selected) and IPv6.
- Gateway:** A text input field containing 'isp-gateway'.
- Interface:** A text input field containing 'outside'.
- Metric:** A text input field containing '1'.
- Networks:** A dropdown menu with a '+' icon and a selected option 'any-ipv4'.

#### 步骤 6 选择策略 (Policies)，并为网络配置安全策略。

设备安装向导设置允许内部区域与外部区域之间存在流量流动，并对所有接口上流向外部接口的流量启用网络地址转换 (NAT)。即使配置了新接口，如果将其添加到内部区域对象中，访问控制规则也将自动应用于这些接口。

但是，如果有多个内部接口，则需要一条访问控制规则来允许内部区域之间的流量。如要添加其他安全区域，则需要规则来允许这些区域之间的流量。这是您需要进行的最低限度的更改。

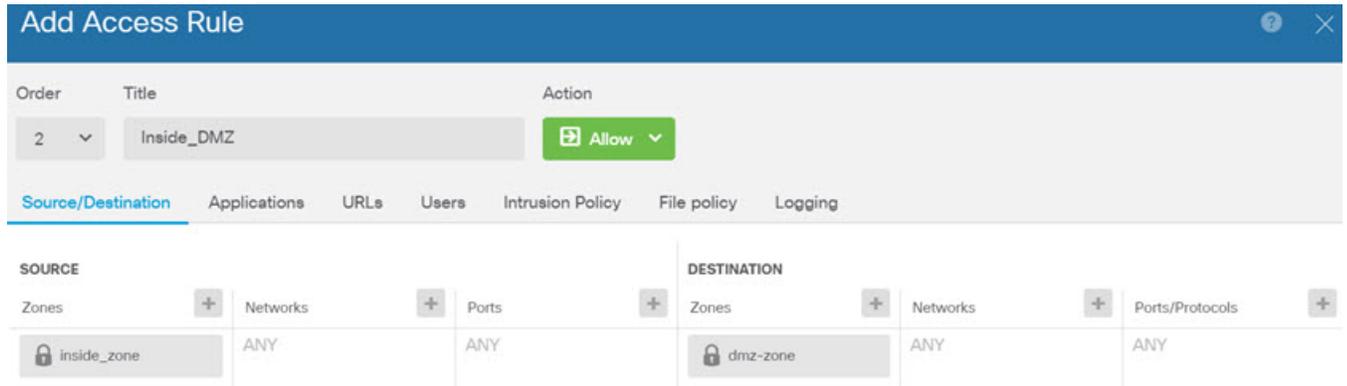
此外，您还可配置其他策略以提供附加服务，并对 NAT 和访问规则进行精细调整，以实现组织需要的结果。您可以配置以下策略：

- **SSL 解密 (SSL Decryption)** - 如果要检查加密连接（例如 HTTPS）是否存在入侵、恶意软件等，则必须解密连接。使用 SSL 解密策略确定需要解密的连接。系统检查连接后，会将其重新加密。
- **身份 (Identity)** - 如果要将网络活动与各个用户相关联，或根据用户或用户组成员身份控制网络访问，请使用身份策略确定与给定源 IP 地址关联的用户。
- **安全情报 (Security Intelligence)** - 使用安全情报策略快速丢弃进出列入黑名单的 IP 地址或 URL 的连接。将已知恶意站点列入黑名单后，在访问控制策略中即可无需考虑这些站点。思科提供定期更新的已知恶意地址和 URL 源，可使安全情报黑名单实现动态更新。使用情报源，无需通过编辑策略来添加或删除黑名单中的项目。
- **NAT (Network Address Translation)** - 使用 NAT 策略将内部 IP 地址转换为外部可路由地址。
- **访问控制 (Access Control)** - 使用访问控制策略确定网络上允许的连接。您可以按安全区域、IP 地址、协议、端口、应用、URL、用户或用户组进行过滤。您还可以使用访问控制规则来应用入侵策略和文件（恶意软件）策略。使用此策略实施 URL 过滤。

- **入侵 (Intrusion)** - 使用入侵策略检测已知威胁。即使使用访问控制规则应用入侵策略，也仍可以编辑入侵策略，以选择性地启用或禁用特定的入侵规则。

以下示例显示如何在访问控制策略中允许内部区域与 DMZ 区域之间的流量。在此示例中，任何其他选项卡上均未设置任何选项，日志记录 (**Logging**) 除外，其中在连接结束时 (**At End of Connection**) 选项已被选中。

图 6: 访问控制策略



**步骤 7** 选择设备 (**Device**)，然后单击更新 (**Updates**) 组中的查看配置 (**View Configuration**)，为系统数据库配置更新计划。

如果使用入侵策略，请为“规则”和“VDB”数据库设置定期更新。如果使用安全情报源，请为“规则”和“VDB”数据库设置更新计划。如果在任何安全策略中使用地理位置作为匹配条件，请为“规则”和“VDB”数据库设置更新计划。

**步骤 8** 单击菜单中的部署 (**Deploy**) 按钮，然后单击立即部署按钮 (  )，以部署对设备的更改。

只有将更改部署至设备，更改才会生效。

## 下一步做什么

有关使用 Firepower 设备管理器管理 Firepower Threat Defense Virtual 的详细信息，请参阅 [《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》](#) 或 Firepower 设备管理器联机帮助。



## 第 4 章

# 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 版本功能的详细信息，请参阅 [使用 Firepower Management 管理 Firepower Threat Defense Virtual 的历史](#)。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 25 页
- [登录到 Firepower 管理中心](#)，第 26 页
- [向 Firepower 管理中心注册设备](#)，第 26 页
- [配置基本安全策略](#)，第 28 页
- [访问 Firepower 威胁防御 CLI](#)，第 39 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

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`

其中 `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** 单击登录 (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。



#### 注释

此过程假定您通过 `day0/bootstrap` 脚本为 FMC 提供了的注册信息。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 [FTD 命令参考](#)。

**步骤 1** 选择设备 (Devices) > 设备管理 (Device Management)。

**步骤 2** 从添加 (Add) 下拉列表选择添加设备 (Add Device)，然后输入以下参数。

**Add Device** ? X

Host: ftd-1.cisco.com

Display Name: ftd-1.cisco.com

Registration Key: \*\*\*\*\*

Group: None

Access Control Policy: Initial Policy

**Smart Licensing**

Malware

Threat

URL Filtering

**Advanced**

Unique NAT ID: cisco123nat

Transfer Packets

Register Cancel

- **主机 (Host)** - 输入要添加的设备的 IP 地址。
- **显示名称 (Display Name)** - 输入要在 FMC 中显示的设备名称。
- **注册密钥 (Registration Key)** - 输入您在 FTDv 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 **Create new policy**，然后选择 **Block all traffic**。之后您可以更改此设置以允许流量通过；请参阅[配置访问控制](#)，第 37 页。

**New Policy** ? X

Name: ftd\_ac\_policy

Description:

Select Base Policy: None

Default Action:  Block all traffic  Intrusion Prevention  Network Discovery

Save Cancel

- **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 AMP 恶意软件检查）、**Threat**（如果您打算使用入侵防御）、**URL**（如果您打算实施基于类别的 URL 过滤）。
- **唯一 NAT ID (Unique NAT ID)** - 指定您在 FTDv 启动程序配置中指定的 NAT ID。

- **转移数据包 (Transfer Packets)** - 可让设备将数据包传输至 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 (**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 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 39 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 FTDIP 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 FMCIP 地址 - 确保在两个设备上使用相同的注册密钥和 NAT ID（如有使用）。可以在 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 FMCIP 地址。

## 配置基本安全策略

本部分介绍如何使用以下设置配置基本安全策略：

- 内部和外部接口 - 为内部接口分配静态 IP 地址，并将 DHCP 用作外部接口。
- DHCP 服务器 - 在内部接口上为客户端使用 DHCP 服务器。
- 默认路由 - 通过外部接口添加默认路由。
- NAT - 在外部接口上使用接口 PAT。
- 访问控制 - 允许流量从内部传到外部。

**步骤 1** [配置接口，第 29 页](#)

**步骤 2** [配置 DHCP 服务器，第 32 页](#)

**步骤 3** [添加默认路由，第 33 页](#)

**步骤 4** [配置 NAT，第 34 页](#)

**步骤 5** [配置访问控制，第 37 页](#)

**步骤 6** [部署配置，第 38 页](#)

## 配置接口

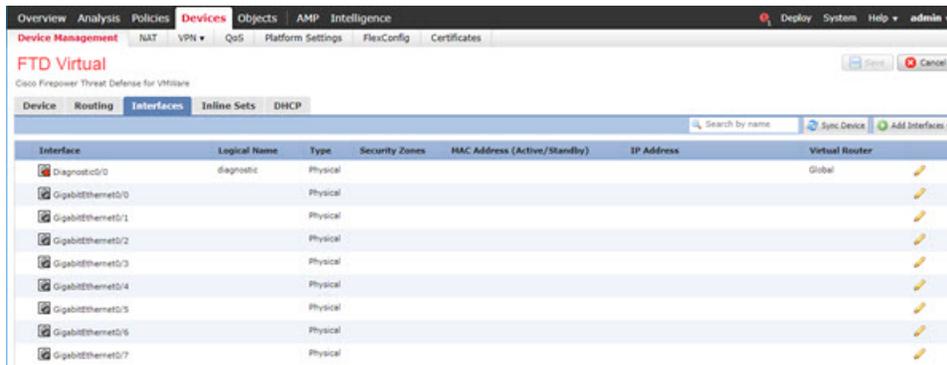
启用 FTDv 接口，为其分配安全区域并设置 IP 地址。通常，您必须至少配置两个接口才能让系统传递有意义的流量。通常，您将拥有面向上游路由器或互联网的外部接口，以及组织网络的一个或多个内部接口。其中一些接口可能是“隔离区”（DMZ），您可以在其中放置可公开访问的资产，例如 Web 服务器。

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 (Devices) > 设备管理 (Device Management)，然后单击设备的编辑 (✎)。

**步骤 2** 单击接口 (Interfaces)。



**步骤 3** 单击要用于内部的接口的编辑 (✎)。

此时将显示一般 (General) 选项卡。

The screenshot shows the 'Edit Physical Interface' dialog box with the following configuration:

- Name:** inside
- Description:** (empty)
- Mode:** None
- Security Zone:** inside\_zone
- Interface ID:** GigabitEthernet0/0
- MTU:** 1500 (range: 64 - 9000)
- Enabled:**  Enabled
- Management Only:**  Management Only

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

- 单击 **IPv4** 和/或 **IPv6** 选项卡。

注释 Google 云平台上的 VPC 网络不支持 IPv6。

- **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 **Autoconfiguration** 复选框。

f) 单击确定 (OK)。

**步骤 4** 单击要用于外部的接口的 **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 **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，或者单击**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) 单击 **IPv4** 和/或 **IPv6** 选项卡。

注释 Google 云平台上的 VPC 网络不支持 IPv6。

- **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。

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

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

f) 单击确定 (**OK**)。

步骤 5 单击保存 (**Save**)。

## 配置 DHCP 服务器



注释 如果要部署到公共云环境（例如 AWS、Azure、GCP、OCI），请跳过此程序。

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 (**Devices**) > 设备管理 (**Device Management**)，然后单击设备的编辑 (  )。

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

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

The screenshot shows the 'Add Server' configuration window. The 'Interface\*' dropdown is set to 'inside'. The 'Address Pool\*' is set to '10.9.7.9-10.9.7.25' with '(2.2.2.10-2.2.2.20)' shown in smaller text. The 'Enable DHCP Server' checkbox is checked. 'OK' and 'Cancel' buttons are at the bottom.

- 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 单击确定 (OK)。

步骤 5 单击保存 (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 **Devices > Device Management > Routing > Static Route** 页面上的 **IPv4 Routes** 或 **IPv6 Routes** 表中。

步骤 1 选择设备 (Devices) > 设备管理 (Device Management)，然后单击设备的编辑 (✎)。

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

The screenshot shows the 'Add Static Route Configuration' dialog box. It has a title bar with a question mark and a close button. The 'Type' section has radio buttons for 'IPv4' (selected) and 'IPv6'. The 'Interface\*' dropdown is set to 'outside'. Below this are two panes: 'Available Network' and 'Selected Network'. The 'Available Network' pane has a search bar and a list of network options, with 'any-ipv4' selected. An 'Add' button is between the panes. The 'Selected Network' pane shows 'any-ipv4'. Below the panes are fields for 'Gateway\*' (set to 'default-gateway'), 'Metric' (set to '1'), 'Tunneled' (checkbox), and 'Route Tracking' (dropdown). At the bottom are 'OK' and 'Cancel' buttons.

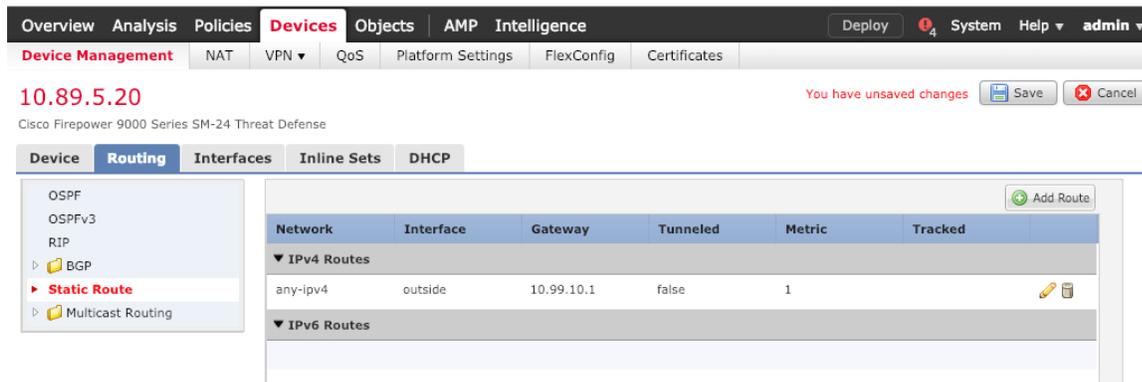
- 类型 (Intrusion) - 根据要添加静态路由的类型，单击 **IPv4** 或 **IPv6** 单选按钮。
- 接口 (Interface) - 选择出口接口；通常是外部接口。

## 配置 NAT

- 可用网络 (Available Network) - 为 IPv4 默认路由选择任意 **ipv4 (any-ipv4)**，为 IPv6 默认路由选择任意 **ipv6 (any-ipv6)**。
- 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 单击确定 (OK)。

路由即已添加至静态路由表。



步骤 4 单击保存 (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)。

步骤 1 选择设备 (Devices) > NAT，然后单击新策略 (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，然后单击 Save。



策略即已添加 FMC。您仍然需要为策略添加规则。

**步骤 3** 单击添加规则 (Add Rule)。

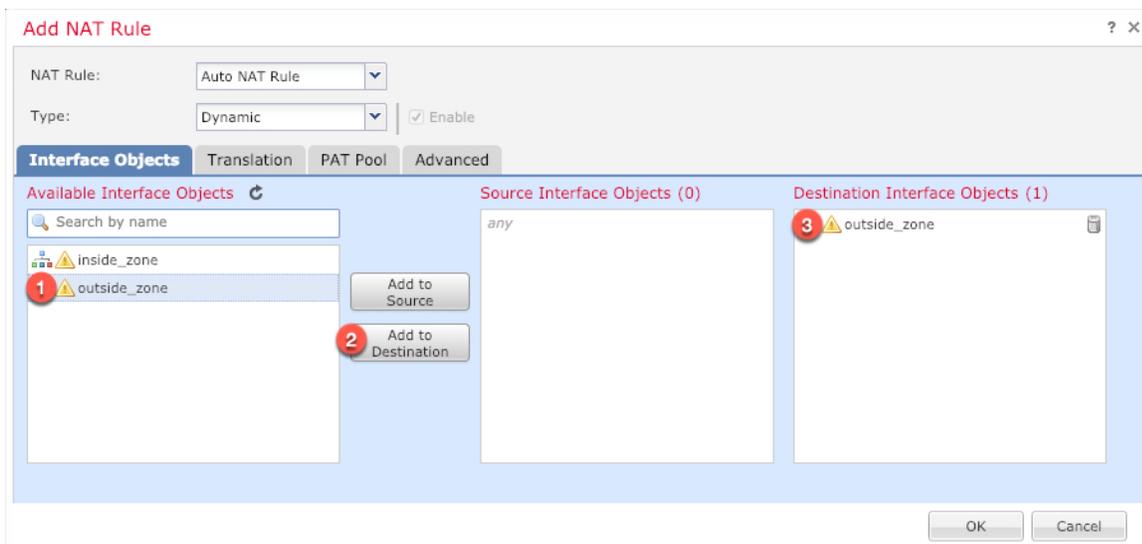
**Add NAT Rule** 对话框将显示。

**步骤 4** 配置基本规则选项：

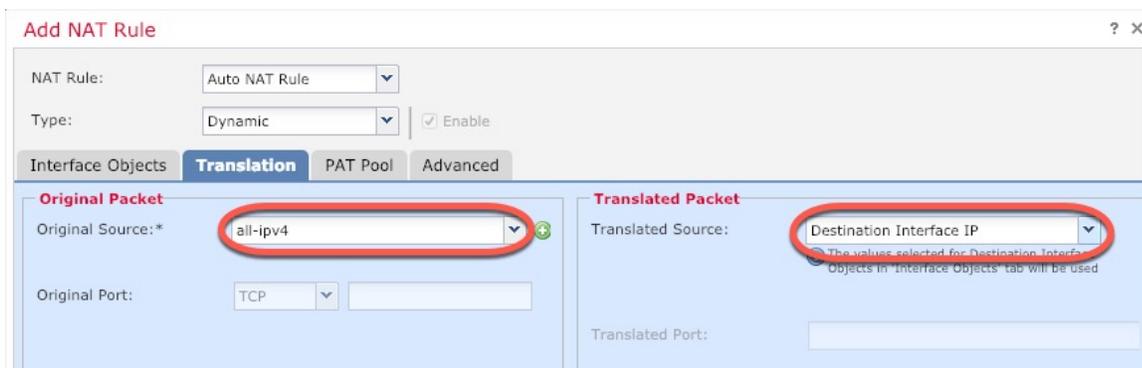


- **NAT 规则 (NAT Rule)** - 选择自动 NAT 规则 (Auto NAT Rule)。
- **类型 (Type)** - 选择动态 (Dynamic)。

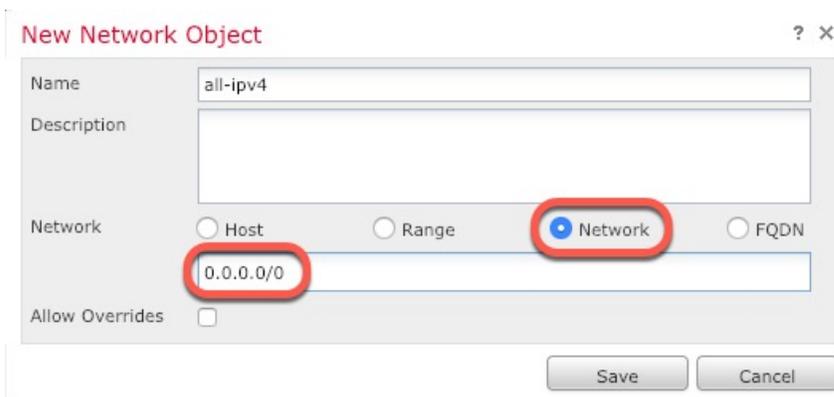
**步骤 5** 在 **Interface Objects** 页面，将 **Available Interface Objects** 区域中的外部区域添加到 **Destination Interface Objects** 区域。



步骤 6 在转换 (Translation) 页面上配置以下选项:



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

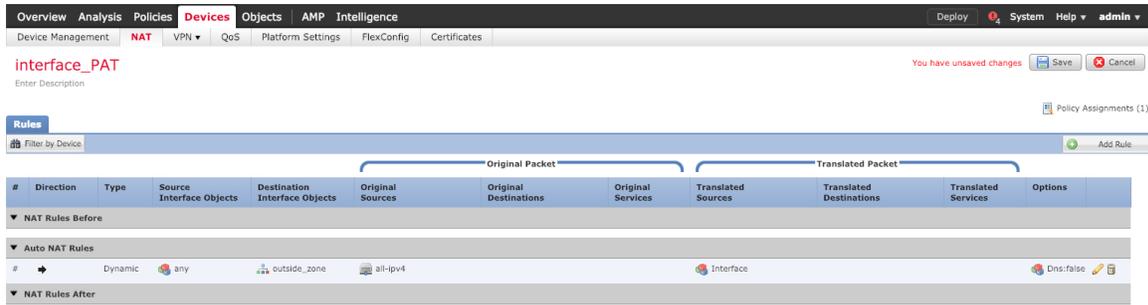


注释 您不能使用系统定义的 **any-ipv4** 对象，因为自动 NAT 规则在对象定义过程中添加 NAT，并且您无法编辑系统定义的对象。

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

步骤 7 单击保存 (Save) 以添加规则。

规则即已保存至 **Rules** 表。



步骤 8 单击 **NAT** 页面上的保存 (Save) 以保存更改。

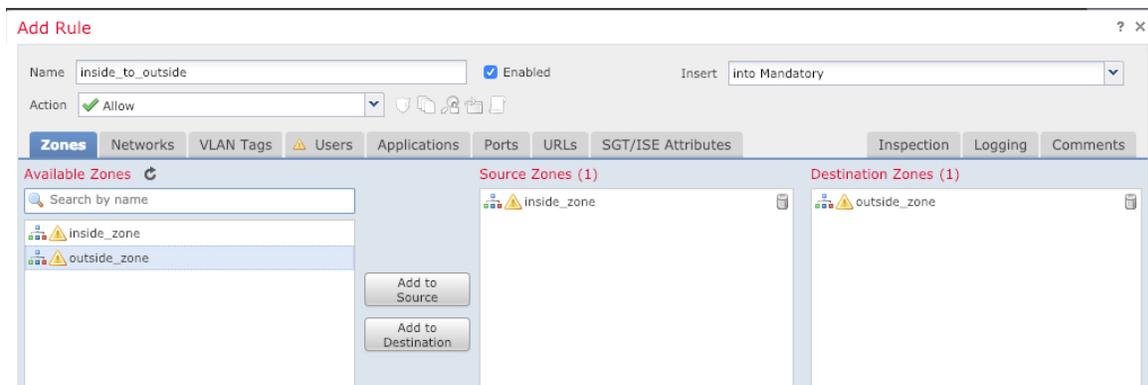
## 配置访问控制

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 (Policy) > 访问策略 (Access Policy) > 访问策略 (Access Policy)，然后单击分配给 FTD 的访问控制策略的编辑 (✎)。

步骤 2 单击添加规则 (Add Rule) 并设置以下参数：

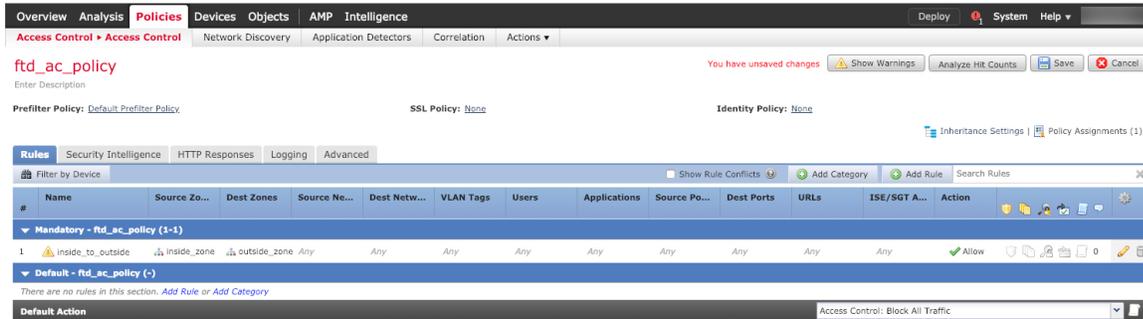


- 名称 (Name) - 为此规则命名，例如 **inside\_to\_outside**。
- 源区域 (Source Zones) - 从可用区域 (Available Zones) 中选择内部区域，然后单击添加到源 (Add to Source)。
- 目标区域 (Destination Zones) - 从可用区域 (Available Zones) 中选择外部区域，然后单击添加到目标 (Add to Destination)。

其他设置保留原样。

**步骤 3** 单击添加 (Add)。

规则即已添加至 **Rules** 表。

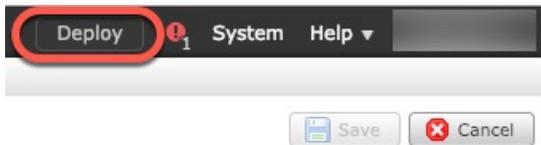


**步骤 4** 单击保存 (Save)。

## 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。

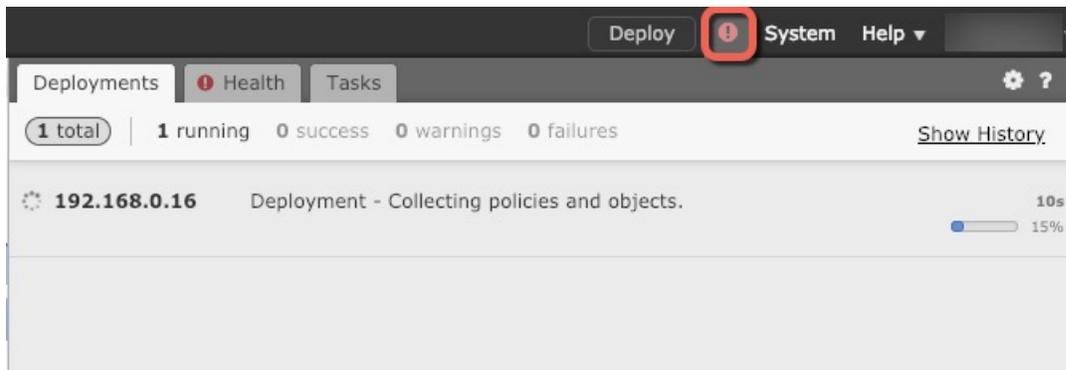
**步骤 1** 单击右上方的部署 (Deploy)。



**步骤 2** 选择部署策略 (Deploy Policies) 对话框中的设备，然后单击部署 (Deploy)。



**步骤 3** 确保部署成功。单击菜单栏中部署 (Deploy) 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。





