



## 《适用于 **AWS** 云的 **Cisco Firepower Threat Defense Virtual** 入门指南》

首次发布日期: 2018 年 7 月 31 日

上次修改日期: 2020 年 5 月 29 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 AWS 入门

Amazon 虚拟私有云 (Amazon VPC) 使您可以在自定义的虚拟网络中启动 Amazon Web 服务 (AWS) 资源。此虚拟网络非常类似于您可能在自有数据中心内运行的传统网络，并且具有使用 AWS 可扩展基础设施所带来的优势。

本文档说明如何在 AWS 上部署 Firepower Threat Defense Virtual。

- [关于 FTDv 和 AWS 云，第 1 页](#)
- [如何管理您的 Firepower 设备，第 2 页](#)
- [AWS 解决方案概述, on page 3](#)
- [Firepower Threat Defense Virtual 前提条件, on page 3](#)
- [支持的功能和限制, on page 4](#)
- [配置 AWS 环境, on page 5](#)

## 关于 FTDv 和 AWS 云

AWS 是一种公共云环境。Firepower Threat Defense Virtual 在以下实例类型的 AWS 环境中作为访客运行。



**注释** Firepower 版本 6.6 加入了对下表中所示 C5 实例类型的支持。较大的实例类型可为 AWS 虚拟机提供更多 CPU 资源，从而提高性能，有些则提供更多网络接口。

表 1: AWS 支持的 FTDv 实例

实例类型	vCPU	内存 (RAM)	vNic
C5.xlarge	4	8 GB	4
C5.2xlarge	8	16 GB	4
C5.4xlarge	16	32 GB	8
C4.xlarge	4	7.5 GB	4

实例类型	vCPU	内存 (RAM)	vNic
C3.xlarge	4	7.5 GB	4

## 如何管理您的 Firepower 设备

您可以通过两种方法来管理您的 Firepower 威胁防御设备。

### 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 威胁防御设备上可用。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 威胁防御设备的大型网络。



**注释** 有关支持 FDM 的 Firepower 威胁防御设备的列表，请参阅《[适用于 Firepower 设备管理器的 Cisco 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 威胁防御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。

## AWS 解决方案概述

AWS 是由 Amazon.com 提供并构成云计算平台的一系列远程计算服务（也称为 Web 服务）。这些服务遍布全球 11 个地区。通常，在部署 Firepower Management Center Virtual 和 Firepower Threat Defense Virtual 时，您应该会熟悉以下 AWS 服务：

- Amazon 弹性计算云 (EC2) - 使您能够通过租用虚拟计算机，在 Amazon 数据中心启动和管理自己的应用和服务（例如防火墙）的 Web 服务。
- Amazon 虚拟私有云 (VPC) - 使您能够配置 Amazon 公共云中的隔离专用网络的 Web 服务。您可以在 VPC 内运行自己的 EC2 实例。
- Amazon 简单存储服务 (S3) - 提供数据存储基础设施的 Web 服务。

您可以在 AWS 上创建账户，设置 VPC 和 EC2 组件（使用 AWS 向导或手动配置），并选择 Amazon 系统映像 (AMI) 实例。AMI 是一种模板，其中包含启动您的实例所需的软件配置。



**Note** AMI 映像可在 AWS 环境之外不可下载。

## Firepower Threat Defense Virtual 前提条件

- 拥有 Amazon 账户。您可以在 <http://aws.amazon.com/> 创建一个。
- 思科智能账户。您可以在 Cisco 软件中心创建一个 <https://software.cisco.com/>
- 许可 Firepower Threat Defense Virtual。
  - 从 Firepower Management Center 配置安全服务的所有许可证授权。
  - 有关如何管理许可证的更多信息，请参阅《Firepower 管理中心配置指南》中的“Firepower 系统许可”。
- Firepower Threat Defense Virtual 接口要求：
  - 管理接口 (2) - 一个用于将 Firepower Threat Defense Virtual 连接到 Firepower Management Center，另一个用于诊断；无法用于直通流量。
  - 流量接口 (2) - 用于将 Firepower Threat Defense Virtual 连接到内部主机和公共网络。
- 通信路径：
  - 用于接入 Firepower Threat Defense Virtual 的公共/弹性 IP。

## 支持的功能和限制

### 支持的功能

- 虚拟私有云 (VPC) 中的部署
- 增强型联网 (SR-IOV) - 在可用的情况下
- 从 Amazon Marketplace 部署
- 每个实例最多四个 vCPU
- 第 3 层网络的用户部署
- 路由模式（默认）
- ERSPAN 被动模式

### Firepower Threat Defense Virtual 限制

- c4.xlarge 是推荐实例；c3.xlarge 实例在不同 AWS 区域的可用性受限。
- 您必须在启动期间配置两个管理接口。
- 必须有两个流量接口和两个管理接口才能启动，总计四个接口。



#### Note

没有四个接口，Firepower Threat Defense Virtual 将不会启动。

- 在 AWS 中配置流量接口时，必须禁用“更改源/目标检查”选项。
- 通过 CLI 或 Firepower 管理中心完成的任何 IP 地址配置必须与 AWS 控制台中创建的内容一致；在部署期间应注意配置。
- 在注册 Firepower Threat Defense Virtual 后，必须在 Firepower Management Center 编辑并启用这些接口；请注意，IP 地址必须与 AWS 配置的接口匹配。
- 目前不支持 IPv6。
- 目前不支持透明/内联/被动模式。
- 修改接口时需要从 AWS 控制台进行更改：
  - 从 Firepower Management Center 取消注册。
  - 通过 AWS AMI 用户界面停止实例。
  - 通过 AWS AMI 用户界面分离要更改的接口。
  - 连接新接口（请记住，必须有两个流量接口和两个管理接口才能启动）。
  - 通过 AWS AMI 用户界面启动实例。
  - 重新注册到 Firepower Management Center。

- 从 Firepower Management Center 编辑设备接口，然后修改 IP 地址和其他参数，以便与通过 AWS 控制台所做的更改匹配。
- 在启动后无法添加接口。
- 目前不支持克隆/快照。

## 配置 AWS 环境

要在 AWS 上部署 Firepower Threat Defense Virtual，您需要使用部署特定的要求和设置配置 Amazon VPC。在大多数情况下，设置向导将引导您完成设置过程。AWS 提供在线文档，其中您可以找到与服务（从简介到高级功能）相关的有用信息。有关详细信息，请参阅<https://aws.amazon.com/documentation/gettingstarted/>。

为更好地控制 AWS 设置，以下各节为启动 Firepower Threat Defense Virtual 之前的 VPC 和 EC2 提供了指导：

- [创建 VPC, on page 5](#)
- [添加互联网网关, on page 6](#)
- [添加子网, on page 7](#)
- [添加路由表, on page 7](#)
- [创建安全组, on page 8](#)
- [创建网络接口, on page 9](#)
- [创建弹性 IP, on page 9](#)

### 准备工作

- 创建 AWS 账户。
- 确认 AMI 可用于您的 Firepower Threat Defense Virtual 实例。

## 创建 VPC

虚拟私有云 (VPC) 是 AWS 账户专用的虚拟网络。该网络逻辑上与 AWS 云中的其他虚拟网络相隔离。您可以将 Firepower Management Center Virtual 和 Firepower Threat Defense Virtual 实例等 AWS 资源启动到 VPC 中。您可以配置 VPC，选择其 IP 地址范围，创建子网，并配置路由表、网络网关和安全设置。

### Procedure

**步骤 1** 登录 <http://aws.amazon.com/> 并选择您所在的区域。

AWS 划分为彼此隔离的多个区域。区域显示在屏幕的右上角。一个区域中的资源不会出现在另一个区域中。请定期检查以确保您在预期的区域内。

**步骤 2** 单击 **服务 > VPC**。

**步骤 3** 单击 **VPC 控制面板 > 我的 VPC**。

**步骤 4** 单击 **创建 VPC**。

**步骤 5** 在 **创建 VPC** 对话框中输入以下信息：

- a) 用于标识 VPC 的用户自定义名称标签。
- b) IP 地址 **CIDR** 块。CIDR（无类别域间路由）是 IP 地址及其关联路由前缀的紧凑表示。例如，10.0.0.0/24。
- c) 默认的**租户**设置，以确保在此 VPC 中启动的实例启动时使用指定的租户属性。

**步骤 6** 单击 **是，创建** 以创建 VPC。

---

### What to do next

添加互联网网关到 VPC 中，详见下一部分。

## 添加互联网网关

您可以添加互联网网关以控制 VPC 与互联网的连接。您可以将 VPC 之外的 IP 地址流量路由至互联网网关。

### 准备工作

- 为 Firepower Threat Defense Virtual 实例创建 VPC。

### Procedure

---

**步骤 1** 单击 **服务 > VPC**。

**步骤 2** 单击 **VPC 控制面板 > 互联网网关**，然后单击 **创建互联网网关**。

**步骤 3** 输入用户自定义的**名称标签**以标识网关，然后单击 **是，创建** 以创建网关。

**步骤 4** 选择上一步中创建的网关。

**步骤 5** 单击 **连接到 VPC** 并选择之前创建的 VPC。

**步骤 6** 单击 **是，连接**，以将网关连接到 VPC。

默认情况下，在创建网关并将其连接到 VPC 之前，在 VPC 上启动的实例无法与互联网通信。

---

### What to do next

添加子网到 VPC 中，详见下一部分。



## 添加子网

您可以对 Firepower Threat Defense Virtual 实例可连接的 VPC IP 地址范围进行分段。您可以根据安全和运营需要创建子网，以实现实例的分组。对于虚拟 Firepower 协议防御，您需要创建一个管理子网和一个流量子网。

### 准备工作

- 为 Firepower Threat Defense Virtual 实例创建 VPC。

### Procedure

---

**步骤 1** 单击 **服务 > VPC**。

**步骤 2** 单击 **VPC 控制面板 > 子网**，然后单击 **创建子网**。

**步骤 3** 在 **创建子网** 对话框中输入以下信息：

- a) 用于标识子网的用户自定义名称标签。
- b) 子网所在的 **VPC**。
- c) 此子网将驻留的可用区域。选择 **无首选项**，由 Amazon 来选择区域。
- d) IP 地址 **CIDR 块**。子网 IP 地址范围必须为 VPC 的 IP 地址范围的子集。地址块大小必须介于网络掩码 /16 和 /28 之间。子网大小可以与 VPC 相等。

**步骤 4** 单击 **是，创建** 以创建子网。

**步骤 5** 如需多个子网，重复以上步骤。为管理流量创建单独的子网，根据需要为数据流量创建多个子网。

---

### What to do next

添加路由表到 VPC 中，详见下一部分。

## 添加路由表

您可以将路由表连接到为 VPC 配置的网关。您还可以关联多个子网与单个路由表，但子网一次只能关联一个路由表。

### Procedure

---

**步骤 1** 单击 **服务 > VPC**。

**步骤 2** 单击 **VPC 控制面板 > 路由表**，然后单击 **创建路由表**。

**步骤 3** 输入用于标识路由表的用户自定义名称标签。

**步骤 4** 从下拉列表中选择将使用此路由表的 **VPC**。

**步骤 5** 单击 **是，创建** 以创建路由表。

**步骤 6** 选择刚创建的路由表。

**步骤 7** 单击 **路由** 选项卡，以在详细信息窗格中显示路由信息。

**步骤 8** 单击编辑，然后单击添加其他路由。

- a) 在目的地址列中，输入**0.0.0.0/0**。
- b) 在目标列中，选择您的网关。

**步骤 9** 单击保存。

---

### What to do next

创建安全组，详见下一部分。

## 创建安全组

您可以创建安全组，并在安全组中通过规则指定允许的协议、端口和源 IP 地址范围。可以创建具有不同规则的多个安全组；可以将这些规则分配给每个实例。

---

### Procedure

**步骤 1** 单击服务 > **EC2**。

**步骤 2** 单击 **EC2 控制面板 > 安全组**。

**步骤 3** 单击创建安全组。

**步骤 4** 在创建安全组对话框中输入以下信息：

- a) 用于标识安全组的用户自定义**安全组名称**。
- b) 此安全组的**说明**。
- c) 与此安全组关联的 **VPC**。

**步骤 5** 配置安全组规则：

- a) 单击**进站**选项卡，然后单击**添加规则**。

**Note** 要从 AWS 外部管理 Firepower Management Center Virtual，需要 HTTPS 和 SSH 访问。您应指定相应的源 IP 地址。此外，如果在 AWS VPC 内同时配置 Firepower Management Center Virtual 和 Firepower Threat Defense Virtual，则应允许专用 IP 管理子网访问。

- b) 单击**出站**选项卡，然后单击**添加规则**以添加出站流量规则，或保留**所有流量**（作为类型）和任意**位置**（作为目标）的默认设置。

**步骤 6** 单击**创建**以创建安全组。

---

### What to do next

创建网络接口，详见下一部分。

## 创建网络接口

您可以使用静态 IP 地址为 Firepower Threat Defense Virtual 创建网络接口。根据具体部署需要，创建网络接口（外部和内部）。

### Procedure

---

- 步骤 1 单击 **服务 > EC2**。
- 步骤 2 单击 **EC2 控制面板 > 网络接口**。
- 步骤 3 单击 **创建网络接口**。
- 步骤 4 在 **创建网络接口** 对话框中输入以下信息：
  - a) 网络接口的 **用户自定义说明**（可选）。
  - b) 从下拉列表中选择 **子网**。确保选择要创建 Firepower Threat Defense Virtual 实例的 VPC 子网。
  - c) 输入 **专用 IP** 地址。建议使用静态 IP 地址，而不是选择 **自动分配**。
  - d) 选择一个或多个 **安全组**。确保安全组已打开所有必需的端口。
- 步骤 5 单击 **是，创建** 以创建网络接口。
- 步骤 6 选择刚创建的网络接口。
- 步骤 7 右键单击并选择 **更改源/目的地址检查**。
- 步骤 8 单击 **编辑**，然后单击 **添加其他路由**。
- 步骤 9 选择 **禁用**。对于创建的任何网络接口，都要重复此操作。

### What to do next

创建弹性 IP 地址，详见下一部分。

## 创建弹性 IP

创建实例时，实例会关联一个公共 IP 地址。停止和启动实例时，该公共 IP 地址会自动更改。要解决此问题，可使用弹性 IP 地址为实例分配一个永久性的公共 IP 地址。弹性 IP 是预留公共 IP，用于远程访问 Firepower Threat Defense Virtual 以及其他实例。



**Note** 至少，您要为 Firepower Threat Defense Virtual 管理和诊断接口创建两个弹性 IP 地址。

---

### Procedure

---

- 步骤 1 单击 **服务 > EC2**。
- 步骤 2 单击 **EC2 控制面板 > 弹性 IP**。

**步骤 3** 单击分配新地址。

**步骤 4** 根据弹性/公共 IP 地址分配需要，重复此步骤。

**步骤 5** 单击是，分配以创建弹性 IP 地址。

**步骤 6** 根据部署需要，重复上述步骤以创建其他弹性 IP 地址。

---

### What to do next

按照下一节中所述，部署 Firepower Threat Defense Virtual。



## 第 2 章

# 部署 Firepower Threat Defense Virtual

本章介绍如何从 AWS 门户部署 Firepower Threat Defense Virtual。

- 部署 Firepower Threat Defense Virtual 实例, on page 11

## 部署 Firepower Threat Defense Virtual 实例

### Before you begin

Cisco 建议以下操作：

- 如配置 AWS 环境, on page 5 中所述，配置 AW VPC 和 EC2 元素。
- 确认 AMI 可用于 Firepower Threat Defense Virtual 实例。

### Procedure

**步骤 1** 前往 <https://aws.amazon.com/marketplace>(Amazon Marketplace) 并登录。

**步骤 2** 登录 Amazon Marketplace 后，单击所提供的 Firepower Threat Defense Virtual 链接 (Cisco Firepower NGFW Virtual (NGFWv) - BYOL)。

**Note** 如果之前已登录 AWS，您可能需要注销并重新登录，以确保链接有效。

**步骤 3** 单击继续，然后单击手动启动选项卡。

**步骤 4** 单击接受条款。

**步骤 5** 在期望的区域单击使用 EC2 控制台启动。

**步骤 6** 选择 Firepower Threat Defense Virtual 支持的实例类型，建议 c4.xlarge。

**步骤 7** 单击屏幕底部的下一步：配置实例详细信息按钮：

- 更改网络，以匹配先前创建的 VPC。
- 更改子网，以匹配先前创建的管理子网。您可以指定 IP 地址或使用自动生成。
- 在网络接口下单击添加设备按钮以添加 eth1 网络接口。

- 更改子网，使其与之前创建的用于 eth0 的管理子网匹配。

**Note** Firepower Threat Defense Virtual 需要两个管理接口。

- 在高级详细信息下方，添加默认登录信息。修改以下示例，以满足设备名称和密码要求。

**小心：**在高级详细信息字段中输入数据时，请仅使用纯文本。如果从文本编辑器复制此信息，请确保仅以纯文本形式复制。如果将任何 Unicode 数据（包括空格）复制到高级详细信息字段，可能会造成实例损坏，然后您必须终止此实例并重新创建实例。

使用 Firepower Management Center 管理 FTDv 的登录配置示例：

```
#Sensor { "AdminPassword": "<your_password>", "主机名": "<Your_hostname>", "ManageLocally":
  "No", "FmcIp": "<FMC 的 IP 地址>", "FmcRegKey": "<registration_passkey>",
  "FmcNatId": "<NAT_ID_if_required>", }
```

使用 Firepower Device Manager 管理 FTDv 的登录配置示例：

```
#Sensor { "AdminPassword": "<your_password>", "主机名": "<Your_hostname>", "ManageLocally":
  "Yes", }
```

**步骤 8** 单击下一步：添加存储。

您可以接受默认值或更改卷。

**步骤 9** 单击下一步：标记实例。

标签由区分大小写的键值对组成。例如，您可以按照“**Key = 名称**”和“**Value = 防火墙**”的格式定义标签。

**步骤 10** 选择下一步：配置安全组。

**步骤 11** 单击选择现有安全组并选择先前配置的安全组，或创建新的安全组；有关创建安全组的详细信息，请参阅 AWS 文档。

**步骤 12** 单击检查和启动。

**步骤 13** 单击启动。

**步骤 14** 选择现有的密钥对或创建新的密钥对。

**Note** 您可以选择现有的密钥对或者创建新的密钥对。密钥对由 AWS 存储的一个公共密钥和用户存储的一个专用密钥文件组成。两者共同确保安全连接到实例。请务必将密钥对保存到已知位置，以备连接到实例之需。

**步骤 15** 单击启动实例。

**步骤 16** 单击查看启动，然后按照提示进行操作。

**步骤 17** 单击 **EC2 控制面板 > 网络接口**。

**步骤 18** 查找之前在配置 AWS 环境, on page 5 中创建的流量接口，然后单击连接。这将成为 Firepower Threat Defense Virtual 实例上的 eth2 接口。

**步骤 19** 查找之前在配置 AWS 环境, on page 5 中创建的流量接口，然后单击连接。这将成为 Firepower Threat Defense Virtual 实例上的 eth3 接口。

**Note** 您必须配置四个接口，否则 Firepower Threat Defense Virtual 将不会完成启动过程。

**步骤 20** 单击 **EC2 控制面板 > 实例**。

**步骤 21** 右键单击实例，然后选择**实例设置 > 获取系统日志**以查看状态。

**Note** 系统可能会显示连接问题的警告。这在预料之内，因为 eth0 接口在 EULA 完成之前不会激活。

**步骤 22** 20 分钟后，您应该能够将 Firepower Threat Defense Virtual 注册到 Firepower Management Center。

---

### What to do next

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选择否，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, on page 35](#)。
- 如果为启用本地管理器选择是，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, on page 51](#)。

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, on page 2](#)。







## 第 3 章

# 部署适用于 AWS 的 Firepower Threat Defense Virtual Auto Scale

本文档说明如何为 AWS 中的 FTDv Auto Scale Manager 部署无服务器组件。



### 重要事项

在开始部署之前，请阅读整个文档。在开始部署之前，请确保满足前提条件。

- [适用于 AWS 上 FTDv 的 Auto Scale 解决方案](#)，第 15 页
- [Auto Scale 解决方案前提条件](#)，第 19 页
- [Auto Scale 部署](#)，第 22 页
- [Auto Scale 维护任务](#)，第 29 页
- [Auto Scale 故障排除](#)，第 32 页
- [附录 - 用于访问 VPC 专用 IP 的 Lambda 函数](#)，第 33 页

## 适用于 AWS 上 FTDv 的 Auto Scale 解决方案

以下各节介绍 Auto Scale 解决方案的组件如何对 AWS 上的 FTDv 发挥作用。

### 关于 Auto Scale 解决方案

Cisco 提供 CloudFormation 模板和脚本，用于使用多个 AWS 服务部署 FTDv 防火墙的自动扩展组，包括 Lambda、自动扩展组、弹性负载均衡 (ELB)、Amazon S3 存储桶、SNS 和 CloudWatch。

AWS 中的 FTDv Auto Scale 是完整的无服务器实现（即此功能的自动化不涉及辅助虚拟机），它可以将水平自动扩展功能加入到 AWS 环境中的 FTDv 实例。

FTDv Auto Scale 解决方案是基于 CloudFormation 模板的部署，可提供：

- FMC 中完全自动化的 FTDv 实例注册和取消注册。
- 自动应用到外向扩展 FTDv 实例的 NAT 策略、访问策略和路由。
- 对负载均衡器和多可用性区域的支持。

- 对启用和禁用自动扩展功能的支持。
- 仅适用于 FMC；不支持 Firepower Device Manager。
- **(FP 6.7 新增)** AWS Auto Scale 增强功能：
  - 自定义指标发布方 — 新的 Lambda 函数每 2 分钟轮询一次 FMC 以获取 Auto Scale 组中所有 FTDv 实例的内存消耗情况，然后将值发布到 CloudWatch 指标；有关说明，请参阅[输入参数](#)，第 22 页。
  - 用于连接 FMC 的 FTDv 专用 SSH 和安全隧道 IP 连接。
  - FMC 配置验证。
  - 支持在 ELB 上打开更多侦听端口。
  - 修改为单堆栈部署。所有 Lambda 函数和 AWS 资源都从单堆栈进行部署，以便简化部署。
  - 使用发布的指标，可以实现基于内存的新扩展策略。

### 支持的软件平台

FTDv Auto Scale 解决方案适用于 FMC 管理的 FTDv，与软件版本无关。《[Cisco Firepower 兼容性指南](#)》提供 Cisco Firepower 软件和硬件兼容性，包括操作系统和托管环境要求。

- [Firepower Management Center](#)：虚拟表列出 AWS 上 FMCv 的 Firepower 兼容性和虚拟托管环境要求。
- [Firepower Threat Defense Virtual 兼容性](#)表列出了 AWS 上 FTDv 的 Firepower 兼容性和虚拟托管环境要求。



**注释** 为了部署 AWS Auto Scale 解决方案，AWS 上 FTDv 的最低支持 Firepower 版本是版本 6.4。FMC 必须至少运行版本 6.6+，才能使用基于内存的扩展。

## Auto Scale 使用案例

[图 1: FTDv Auto Scale 用例图](#)，第 17 页显示了此 FTDv AWS Auto Scale 解决方案的使用案例。由于 AWS 负载均衡器只允许入站发起的连接，因此只允许外部生成的流量通过 Cisco FTDv 防火墙传入内部。面向互联网的负载均衡器将有一个 DNS 名称，还可能保持开启 0 到 4 个端口。在这些端口中，0 到 2 个可以是不安全的端口，如 HTTP/80，0 到 2 个可以是安全端口，如 HTTPS/443。



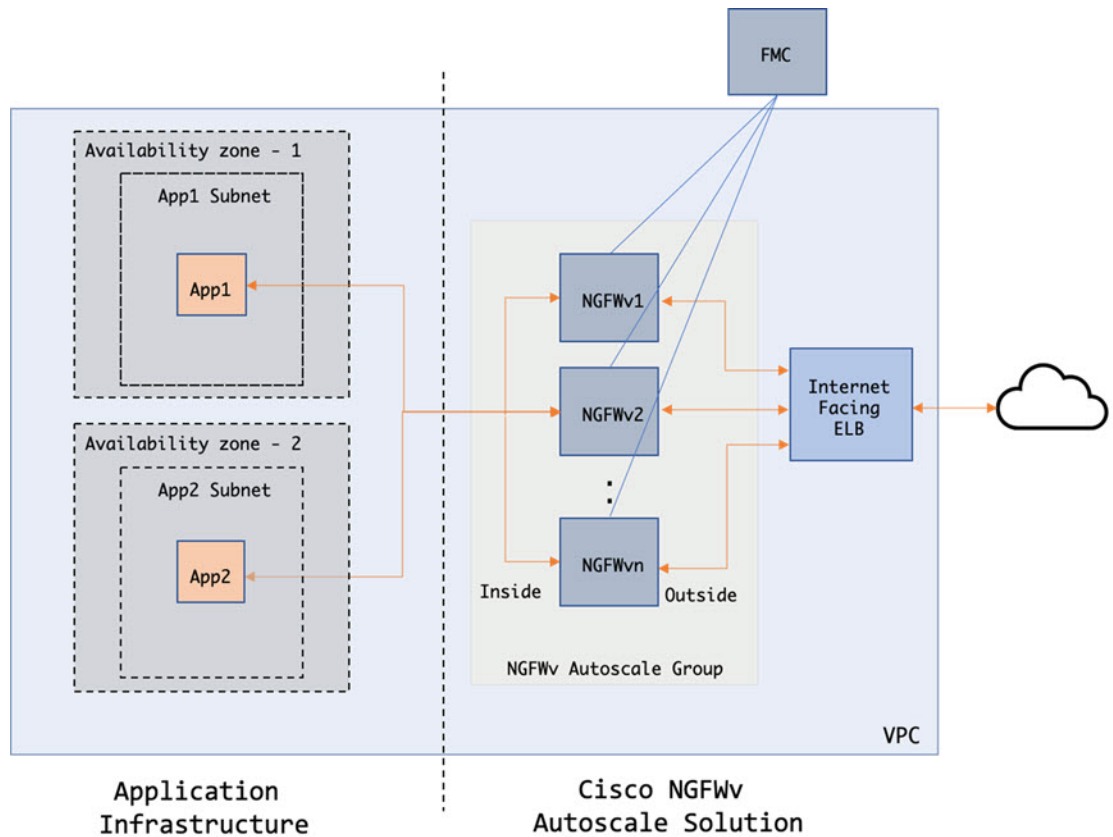
**注释** 如前提条件 [SSL 服务器证书](#)，第 21 页中所述，安全端口需要 SSL/TLS 证书。

面向互联网的负载均衡器可以是网络负载均衡器或应用程序负载均衡器。在两种情况下，所有 AWS 要求和条件均适用。如用例图中所示，虚线右侧是通过 FTDv 模板部署的。左侧完全由用户定义。



注释 应用程序发起的出站流量将不会经过 FTDv。

图 1: FTDv Auto Scale 用例图



基于端口的流量分叉是可能的。这可通过 NAT 规则实现；请参阅[在 FMC 中配置对象、设备组、NAT 规则和访问策略](#)，第 27 页。例如，面向互联网的 LB DNS、端口：80 上的流量可以路由到应用程序 1；端口：88 流量可路由到应用程序 2。

## Auto Scale 解决方案的工作机制

为了内向扩展和向外扩展 FTDv 实例，一个称为 Auto Scale Manager 的外部实体会监控指标、命令自动扩展组添加或删除 FTDv 实例、向管理 FMC 注册和取消注册 FTDv 设备，并配置 FTDv 实例。

Auto Scale Manager 使用 AWS 无服务器架构进行实施，并且与 AWS 资源、FTDv 和 FMC 通信。我们提供 CloudFormation 模板来自动执行 Auto Scale Manager 组件的部署。此模板还用于部署完整解决方案发挥作用所需的其他资源。



注释 无服务器 Auto Scale 脚本只由 CloudWatch 事件调用，因此它们仅在启动实例时才会运行。

## Auto Scale 解决方案组件

以下组件构成了 Auto Scale 解决方案。

### CloudFormation 模板

CloudFormation 模板用于部署 AWS 中 Auto Scale 解决方案所需的资源。该模板包括以下各项：

- Auto Scale 组、负载均衡器、安全组和其他各种组件。
- 模板需要用户输入来自定义部署。



**注 释** 模板在验证用户输入方面有限制，因此，用户应负责在部署期间验证输入。

### Lambda 函数

Auto Scale 解决方案是在 Python 中开发的一组 Lambda 函数，可以通过生命周期钩子、SNS、CloudWatch 事件/警报事件触发。基本功能包括：

- 触发内向扩展/外向扩展操作。
- 向 FMC 注册新的 FTDv。
- 通过 FMC 配置新的 FTDv。
- 从 FMC 取消注册（删除）内向扩展的 FTDv。

Lambda 函数以 Python 包的形式交付给客户。

### 内向扩展/外向扩展插件

- 内向扩展/外向扩展插件可确保有正确数量的 Amazon EC2 实例可用，以便处理应用程序的负载。
- 扩展插件可通过用于自动扩展的内置 AWS 框架进行配置，或使用自定义 Lambda 函数进行配置。

### 生命周期 Hook

- 生命周期钩子用于获取关于实例的生命周期更改通知。
- 在启动实例时，生命周期钩子用于触发 Lambda 函数，可将接口添加到 FTDv 实例，并将外部接口 IP 注册到目标组。
- 在终止实例时，生命周期钩子用于触发 Lambda 函数，以便从目标组取消注册 FTDv 实例。

### Simple Notification Service (SNS)

- 来自 AWS 的 Simple Notification Service (SNS) 用于生成事件。

- 受限于 AWS 中的无服务器 Lambda 函数没有适合的编排器，因此该解决方案使用 SNS 作为一种函数链，以便基于事件来编排 Lambda 函数。

## Auto Scale 解决方案前提条件

### 下载部署文件

#### 下载 Beta 版部署

下载启动 FTDv AWS Auto Scale 解决方案所需的文件。部署脚本和模板可从您的 Beta 版经理获得：代码在 Zip 存档的 Box 文件夹中：**ftdv\_aws\_autoscale\_v2.zip**。



**注意** 请注意，Cisco 提供的自动扩展部署脚本和模板作为开源示例提供，不在常规 Cisco TAC 支持范围内。

### VPC

您应根据应用程序要求创建 VPC。预计 VPC 具有一个互联网网关，而且至少有一个通过到互联网的路由连接的子网。有关安全组、子网等的要求，请参阅相应的部分。

### 子网

可以根据需要创建符合应用程序要求的子网。如用例中所示，FTDv VM 需要 3 个子网才能运行。请注意，如果需要多个可用性区域支持，则每个区域都需要子网，因为子网是 AWS 云中的区域属性。



**注释** 如果需要多个可用性区域支持，则每个区域都需要子网，因为子网是 AWS 云中的区域属性

#### 外部子网

外部子网应该具有能够通过“0.0.0.0/0”连接互联网网关的路由。这将包含 FTDv 的外部接口，而面向互联网的 NLB 将位于此子网中。

#### 内部子网

这可能与具有或没有 NAT/互联网网关的应用程序子网类似。请注意，对于 FTDv 运行状况探测，应该可以通过端口 80 到达 AWS 元数据服务器 (169.254.169.254)。

### 管理子网

此子网是 FTDv 管理接口，会被分配一个弹性 IP 地址 (EIP)，并且需要它才能具有到互联网的默认路由。



**注释** 要在管理接口上避免 EIP，请参阅[附录 - 用于访问 VPC 专用 IP 的 Lambda 函数](#)，第 33 页。

### 应用程序子网

Auto Scale 解决方案对此子网不施加限制，但如果应用程序需要 VPC 外部的出站连接，则应在子网上配置各自的路由。这是因为出站发起的流量不会穿过负载均衡器。请参阅《[AWS 弹性负载均衡用户指南](#)》。

## 安全组

在提供的 Auto Scale 组模板中允许所有连接。只需以下连接即可使 Auto Scale 解决方案发挥作用。

表 2: 所需端口

端口	使用方式	子网 (Subnet)
8305	FMC 到 FTDv 安全隧道的连接	管理子网
运行状况探测端口 (默认: 8080)	面向互联网的负载均衡器运行状况探测 器	外部、内部子网
应用程序端口	应用程序数据流量	外部、内部子网

### FMC 实例的安全组或 ACL

要允许 Lambda 函数与 FMC 之间的 HTTPS 连接，应该将一组 IP 地址范围列入白名单。如果不可能允许一组 IP 地址范围，则应手动将 Lambda 函数放在 VPC 中。请参阅[附录 - 用于访问 VPC 专用 IP 的 Lambda 函数](#)，第 33 页。

之后，FTDv 和 FMC 安全组或 ACL 只能通过 NAT 网关 IP 地址进行更新。

## Amazon S3 存储桶

Amazon Simple Storage Service (Amazon S3) 是一项可提供行业领先可扩展性、数据可用性、安全性和性能的对象存储服务。您可以将防火墙模板和应用程序模板的所有必需文件都放在 S3 存储桶中。

部署模板时，将引用 S3 存储桶中的 Zip 文件创建 Lambda 函数。因此，S3 存储桶应该能够供用户帐户访问。

## SSL 服务器证书

如果面向互联网的负载均衡器必须支持 TLS/SSL，则需要证书 ARN。有关详细信息，请参阅以下链接：

- [使用服务器证书](#)
- [创建私钥和自签名证书进行测试](#)
- [使用自签名 SSL 证书创建 AWS ELB](#)（第三方链接）

ARN 示例：`arn:aws:iam::[AWS 帐户]:server-certificate/[证书名称]`

## Lambda 层

必须创建一个 Lambda 层，以便为 Lambda 函数提供少数 Python 库。

需要在此目录中创建名为 *autoscale\_layer.zip* 的文件，以便为 Lambda 函数提供一些基本的 Python 库。以下库需要供 lambda 函数使用：

```
pycrypto==2.6.1 paramiko==2.7.1 requests==2.23.0 scp==0.13.2 jsonschema==3.2.0
```

可在 Linux 环境中创建 *autoscale\_layer.zip* 文件，如安装了 Python 3.6 的 Ubuntu 18.04。

```
#!/bin/bash mkdir -p layer virtualenv -p /usr/bin/python3.6 ./layer/ source
./layer/bin/activate pip3 install pycrypto==2.6.1 pip3 install paramiko==2.7.1 pip3 install
requests==2.23.0 pip3 install scp==0.13.2 pip3 install jsonschema==3.2.0 echo "Copy from
./layer directory to ./python\n" mkdir -p ./python/.libs_cffi_backend/ cp -r
./layer/lib/python3.6/site-packages/* ./python/ cp -r
./layer/lib/python3.6/site-packages/.libs_cffi_backend/* ./python/.libs_cffi_backend/ zip
-r autoscale_layer.zip ./python
```

使用 S3 存储桶中的 *autoscale\_layer.zip* 文件创建 Lambda 层。记录 ARN 供进一步使用。

ARN 的示例：

```
arn:aws:lambda:us-east-1:[AWS 帐户]:layer:[层名称]:[版本]
```

有关详细信息，请参阅 [AWS Lambda 层](#)。

## KMS 主密钥

如果 FMC 和 FTDv 密码为加密格式，则需要此项。否则，不需要此组件。密码应只使用此处提供的 KMS 加密。如果在 CFT 上输入 KMS ARN，则必须对密码加密。否则，密码应为纯文本。

有关主密钥和加密的详细信息，请参阅 AWS 文档 [《创建密钥》](#) 和关于密码加密和 KMS 的 [AWS CLI 命令参考](#)。

示例：

```
$ aws kms encrypt --key-id <KMS-ARN> --plaintext 'MyC0mplIc@tedProtectIoN' { "KeyId":
"KMS-ARN", "CiphertextBlob":
"AQICAHgcQFAGtz/hvaxMtJvY/x/rfHnKI3clFPpSXUU7HQrnCAFwfXhXHJAHL8tcVmDqurALAAAAajBoBqkqkhi
G9w0BBwagWzBZAgEAMFQGCSqGSib3DQEhATAeBglghkgBZQMEAS4wEQQM45AIkTqjSekX2mniAgEQgCcOav6Hhol
+wxpWkTXY4y1Z1d0z1P4fx0jTdosfCbPnUExmNJ4zdx8=" } $
```

`CiphertextBlob` 密钥的值应用作密码。

## 使用 AWS CLI 的 Python 3 环境

可以在克隆存储库顶级目录中找到 `utility.py` 文件。它应在修改 `Configuration.json` 后用来压缩文件并上传至所需的 S3 存储桶。为了运行 `utility.py` 文件，应该具有已设置 AWS CLI 的 Python 3 环境。

<https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-configure.html>

## Auto Scale 部署

### 准备

应用程序可能已部署或其部署计划可用。

### 输入参数

在部署之前，应收集以下输入参数。

表 3: *Auto Scale* 输入参数

参数	允许的值/类型	说明
PodNumber	整数	这是 pod 号。更改此值可让您部署具有不同 pod 号的相同堆栈。
AutoscaleGrpNamePrefix	字符串	这是 Auto Scale 组名称前缀。pod 号将作为后缀添加。 示例: Cisco-FTDv-1
NotifyEmailID	字符串	Auto Scale 事件将被发送到此电子邮件地址。您需要接受订用电子邮件请求。 示例: admin@company.com
VpcId	字符串	需要部署设备的 VPC ID。它应根据 AWS 要求配置。 如果使用 “ <i>infrastructure.yaml</i> ” 文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。 示例: vpc-81f042fb
LambdaSubnets	字符串	将部署 Lambda 函数的子网。 如果使用 “ <i>infrastructure.yaml</i> ” 文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。 示例: subnet-0d71f40e3d86f99cc,subnet-012c9bea5f85bdab4



参数	允许的值/类型	说明
LambdaSG	字符串	<p>Lambda 函数的安全组。</p> <p>如果使用 “<i>infrastructure.yaml</i>” 文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。</p> <p>示例：sg-0581f3c10bf5918c6</p>
S3BktName	字符串	<p>文件的 S3 存储桶名称。应根据 AWS 要求在您的帐户中配置此项。</p> <p>如果使用 “<i>infrastructure.yaml</i>” 文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。</p> <p>示例：infra-stack-s3bucketautoscale-s4u8twavojm4</p>
LoadBalancerType	字符串	<p>面向互联网的负载均衡器类型，可以是 “application” 或 “network”。</p> <p>示例：application</p>
LoadBalancerSG	字符串	<p>负载均衡器的安全组。如果是网络负载均衡器，则不会使用它。但您应提供一个安全组 ID。</p> <p>如果使用 “<i>infrastructure.yaml</i>” 文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。</p> <p>示例：sg-0144c997033024167</p>
LoadBalancerPort	整数	<p>负载均衡器端口。</p> <p>示例：80</p>
SSL证书	字符串	<p>用于安全端口连接的 SSL 证书 ARN。如果未指定，则在负载均衡器上开启的端口将为 TCP/HTTP。如果已指定，则在负载均衡器上开启的端口将为 TLS/HTTPS。</p> <p>如果必须打开任何安全端口，则必须输入证书 ARN。否则，可自主选择。</p> <p>示例：arn:aws:iam::[AWS 帐户]:server-certificate/[证书名称]</p>
TgHealthPort	整数	<p>此端口供目标组用于运行状况探测。默认值为 8080。</p> <p>在 FTDv 上到达此端口的运行状况探测将被路由到 AWS 元数据服务器。它应该是有效的 TCP 端口。</p> <p>示例：8080</p>

参数	允许的值/类型	说明
AssignPublicIP	布尔值	如果选择“true”，则将分配公共 IP。如果是 BYOL 类型 FTDv，则需要它才能连接到 <a href="https://tools.cisco.com">https://tools.cisco.com</a> 。 示例：TRUE
InstanceType	字符串	虚拟机实例类型，来自受支持的选项。应仅使用支持 FTDv 的实例。请参阅 Firepower 发行说明。 示例：c4.xlarge
LicenseType	字符串	FYDv 许可证类型，可以是 BYOL 或 PAYG。 示例：BYOL
AmiId	字符串	FTDv AMI ID（有效的 Cisco FTDv AMI ID）。 示例：ami-0de5d3956a718f517 注：请根据地区和所需的映像版本选择正确的 AMI ID。Auto Scale 功能支持 Firepower 版本 6.4+、BYOL/PAYG 映像。在两种情况下，您都应在 AWS Marketplace 中接受许可证。 如果是 BYOL，请使用诸如“BASE”、“MALWARE”、“THREAT”、“URLFilter”等功能更新 Configuration JSON 中的“licenseCaps”键值。
NoOfAZs	整数	FTDv 应跨越的可用性区域数，介于 1 到 3 之间。如果是 ALB 部署，根据 AWS 的要求，最小值为 2。 示例：2
ListOfAZs	逗号分隔的字符串	按顺序列出的逗号分隔区域列表。 注释 它们的列出顺序十分重要。应按相同的顺序给出子网列表。 如果使用“ <i>infrastructure.yaml</i> ”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。 示例：us-east-1a, us-east-1b, us-east-1c
MgmtInterfaceSG	字符串	FTDv 管理接口的安全组。 如果使用“ <i>infrastructure.yaml</i> ”文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。 示例：sg-038bb9e22742102d0

参数	允许的值/类型	说明
InsideInterfaceSG	字符串	FTDv 内部接口的安全组。 如果使用 “ <i>infrastructure.yaml</i> ” 文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。 示例：sg-05311dbe5f5676ad5
OutsideInterfaceSG	字符串	FTDv 外部接口的安全组。 如果使用 “ <i>infrastructure.yaml</i> ” 文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。 示例：sg-0c190a824b22d52bb
MgmtSubnetId	逗号分隔列表	逗号分隔的管理子网 ID 列表。此列表应与相应的可用性区域顺序相同。 如果使用 “ <i>infrastructure.yaml</i> ” 文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。 示例：subnet-0778e74f6e603b13b、 subnet-02d1d7842f5f11c8、subnet-01c1d55b157335002
InsideSubnetId	逗号分隔列表	逗号分隔的内部 /Gig0/0 子网 ID 列表。此列表应与相应的可用性区域顺序相同。 如果使用 “ <i>infrastructure.yaml</i> ” 文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。 示例：subnet-0379e9e745772e8f3、 subnet-0a199b943939b9b6f、subnet-0ac38cf812f69d23c
OutsideSubnetId	逗号分隔列表	逗号分隔的外部 /Gig0/1 子网 ID 列表。此列表应与相应的可用性区域顺序相同。 如果使用 “ <i>infrastructure.yaml</i> ” 文件来部署基础架构，堆栈的输出部分将具有此值。请使用该值。 示例：subnet-086096d4a09745b70、 subnet-08566e6c2f99a4e6a、subnet-0bd03219da105a27c
KmsArn	字符串	现有 KMS（用于静态加密的 AWS KMS 密钥）的 ARN。如果已指定，FMC 和 FTDv 密码应该会被加密。密码加密应仅使用指定的 ARN 进行。 生成加密密码示例：“aws kms encrypt --key-id <KMS ARN> --纯文本 <密码>” 请按照所示使用生成的密码。 示例：arn:aws:kms:us-east-1:[AWS Account]:key/7d586a25-5875-43b1-bb68-a452e2f6468e

参数	允许的值/类型	说明
ngfwPassword	字符串	如果未使用 KMS ARN，请使用纯文本密码。如果使用 KMS ARN，则应使用加密的密码。 示例：Cisco123789! 或 AQIAgcQFAGtz/hvaxMtJvY/x/rfHnI3lPpSXU
fmcServer	数字字符串	用于管理 FMC 的 IP 地址，Lambda 函数和 FTDv 均可访问该地址。 示例：10.10.17.21
fmcOperationsUsername	字符串	在管理 FMC 时创建的网络管理员或更高权限用户。 示例：apiuser-1
fmcOperationsPassword	字符串	如果未提及 KMS ARN，请使用纯文本密码。如果已提及，则应使用加密的密码。 示例：Cisco123@ 或 AQICAHgcQAtz/hvaxMtJvY/x/mKI3clFPpSXUHQRnCAajB
fmcDeviceGrpName	字符串	FMC 设备组名称。 示例：AWS-Cisco-NGFW-VMs-1
fmcPublishMetrics	布尔值	如果设置为“TRUE”，则将创建一个 Lambda 函数，该函数每 2 分钟运行一次，将获取所提供的设备组中已注册 FTDv 传感器的内存消耗情况。 示例：TRUE
fmcMetricsUsername	字符串	用于向 AWS CloudWatch 进行指标发布的 FMC 用户名。如果将“fmcPublishMetrics”设置为“FALSE”，则无需提供此输入。 示例：publisher-1
fmcMetricsPassword	字符串	用于向 AWS CloudWatch 进行指标发布的 FMC 密码。如果将“fmcPublishMetrics”设置为“FALSE”，则无需提供此输入。 示例：Cisco123789!
CpuThresholds	逗号分隔的整数	下限 CPU 阈值和上限 CPU 阈值。最小值为 0，最大值为 99。 请注意，下限阈值应小于上限阈值。 示例：30、70

参数	允许的值/类型	说明
MemoryThresholds	逗号分隔的整数	<p>下限 MEM 阈值和上限 MEM 阈值。最小值为 0，最大值为 99。</p> <p>请注意，下限阈值应小于上限阈值。如果“fmcPublishMetrics”参数为“FALSE”，则它不起作用。</p> <p>示例：40、50</p>

## 在 FMC 中配置对象、设备组、NAT 规则和访问策略

您可以使用 Firepower Management Center (FMC) 管理 FTDv，前者是位于单独服务器上功能齐全的多设备管理器。FTDv 在您分配给 FTDv 虚拟机的管理接口上向 FMC 注册并与之通信。有关详细信息，请参阅[关于使用 Firepower 管理中心管理的 Firepower Threat Defense Virtual](#)，第 35 页。

用于 FTDv 配置的所有对象都应由用户创建。



### 重要事项

应创建一个设备组，然后应对其应用规则。设备组上应用的所有配置都将被推送到 FTDv 实例。

### 对象

创建以下对象：

表 4: 用于 FTDv 管理的 FMC 配置对象

对象类型	名称	值
主机	aws-metadata-server	169.254.169.254
端口	health-check-port	8080/所要求的任何其他端口
区	内部/任何其他名称	-
区	外部/任何其他名称	-

### NAT 策略

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)。有关 NAT 策略的信息，请参阅[使用 Firepower 管理中心管理 Firepower Threat Defense Virtual](#)，第 35 页中的[配置 NAT](#)，第 45 页。

您的 NAT 策略中必须有一个强制规则：

- 原始源：任意 ipv4
- 原始目标端口：8080/或用户配置的任何运行状况端口

- 转换后的目标: aws-metadata-server
- 转换后目标端口: 80

同样, 可以添加任何数据流量 NAT 规则, 以便将此配置推送到 FTDv 设备。

### 访问策略

配置访问控制以允许从内部到外部的流量。可以创建具有所有必需策略的访问策略, 应允许运行状况端口对象, 以便允许此端口上的流量到达。有关访问策略的信息, 请参阅[使用 Firepower 管理中心管理 Firepower Threat Defense Virtual](#), 第 35 页中的[配置访问控制](#), 第 47 页。

## 更新配置 JSON 文件

*Configuration.json* 文件可在 *autoscale\_manager* 文件夹中找到, 它包含在从 [GitHub](#) 存储库获取的存档 ZIP 中。请注意, 不应更改 JSON 键值。应在 JSON 文件中配置 FTDv VM 的任何静态路由。

请参阅下面的静态路由配置示例。

```
{ "interface": "inside", "network": "any-ipv4", "gateway": "", "metric": "1" }
```

除默认 FTDv 密码外, JSON 文件中的所有值都可根据您的要求修改。

## 将文件上传到 Amazon Simple Storage Service (S3)

当修改 *Configuration.json* 文件并且收集所有必需的参数后, 应将文件上传到 Amazon S3 存储桶。请注意, 应压缩并上传 *autoscale\_manager*、*autoscale\_grp* 和 *scale\_functions*。

[GitHub](#) 克隆根目录中的 *utility.py* 文件将为您执行此操作。当修改 *Configuration.json* 文件后, 请运行以下命令 (已配置 AWS CLI 的 Python 3.6 环境):

```
$ python utility.py --create-zip-file true --upload-file true --s3-bucket
mygroup-autoscale-lambda
```

这将压缩所需的文件并上传到 S3 存储桶。



**注释** 您可以手动压缩文件, 但这将对 Lambda 函数的目录结构造成一些问题。因此, 我们建议您通过 *utility.py* 函数创建 Zip 文件。

如果只需创建 Zip 文件, 不需要上传到 S3 存储桶, 请运行以下命令并手动上传到 S3 存储桶 (这在未设置 AWS CLI 的情况下非常有用)。

```
$ python utility.py --create-zip-file true
```

在手动上传的情况下, 请上传 Zip 文件、YAML 文件。

## 部署嵌套堆栈

完成部署的所有前提条件后, 您可以创建 AWS CloudFormation 堆栈。

使用克隆存储库顶层目录中的 *deploy.yaml* 文件。

提供输入参数，第 22 页中收集的参数。

## 验证部署

当成功部署模板后，应验证是否根据 *asm.yaml* 和 *asg.yaml* CloudFormation 模板创建 Lambda 函数和 CloudWatch 事件。系统会发送订用确认电子邮件，提供电子邮件通知。

# Auto Scale 维护任务

## 扩展过程

本主题说明如何挂起、然后恢复 Auto Scale 组的一个或多个扩展过程。

### 开始和停止外向扩展操作

要开始和停止外向扩展操作，请执行以下步骤。

- 对于 AWS 动态扩展 - 参阅以下链接，了解关于启用或禁用外向扩展操作的信息：

[挂起和恢复扩展过程](#)

- 对于 AWS 自定义 Lambda - 导航到 CloudWatch CPU 上限阈值警报，然后编辑警报以添加或删除“外向扩展 SNS”主题。

### 开始和停止内向扩展操作

要开始和停止内向扩展操作，请执行以下步骤。

- 对于 AWS 动态扩展 - 参阅以下链接以启用或禁用内向扩展操作：

[挂起和恢复扩展过程](#)

- 对于 AWS 自定义 Lambda - 导航到 CloudWatch CPU 上限阈值警报，然后编辑警报以添加或删除“内向扩展 SNS”主题。

## 运行状况监控

运行状况监控器配置如下：如果不正常的 IP 目标增加大于或等于 1，则保持 60 分钟，然后发布 SNS 事件。

- 如果有属于有效 FTDv VM 的不正常 IP，该实例将被删除。
- 如果这些 IP 不是来自有效的 FTDv VM，则仅从目标组中删除 IP。

### 禁用运行状况监控器

要禁用运行状况监控器，请导航到 SNS 订用。在 ASG 组主题的 AWS Lambda 订用中，删除该订用。或者，您也可以删除电子邮件预订。

### 启用运行状况监控器

要启用运行状况监控器，请导航到 SNS 订用。创建订用并选择正确的主题 ARN（Auto Scale 组主题 ARN）、AWS Lambda 作为协议。此外，选择 Auto Scale 生命周期钩子 lambda 作为 Lambda ARN。

## 禁用生命周期钩子

在极少数需要禁用生命周期钩子的情况下，如果禁用，将不会向实例添加额外的接口。它还可能导致一系列 FTDv 实例部署失败。

## 禁用 Auto Scale 管理器

要禁用 Auto Scale Manager，应禁用相应的 CloudWatch 事件“notify-instance-launch”和“notify-instance-terminate”。禁用这些不会对任何新事件触发 Lambda。但是，已在执行的 Lambda 操作将会继续。Auto Scale Manager 不会突然停止。通过删除堆栈或删除资源尝试突然停止可能会导致状态不确定。

## 负载均衡器目标

由于 AWS 负载均衡器不允许对具有多个网络接口的实例使用实例类型目标，因此将 Gigabit0/1 接口 IP 配置为目标组上的目标。但是，截至目前，AWS Auto Scale 运行状况检查仅对实例类型目标（而不是 IP）有效。此外，这些 IP 不会自动添加到目标组或从目标组中删除。因此，我们的 Auto Scale 解决方案会以编程方式处理这两个任务。但在进行维护或故障排除时，可能会有需要手动完成此操作的情况。

### 将目标注册到目标组

要将 FTDv 实例注册到负载均衡器，其 Gigabit0/1 实例 IP（外部子网）应添加为目标组中的目标。请参阅[按 IP 地址注册或取消注册目标](#)。

### 从目标组取消注册目标

要从负载均衡器取消注册 FTDv 实例，其 Gigabit0/1 实例 IP（外部子网）应作为目标组中的目标删除。请参阅[按 IP 地址注册或取消注册目标](#)。

## 实例备用

AWS 不允许在 Auto Scale 组中重新启动实例，但允许用户将实例置于备用状态并执行这类操作。但是，当负载均衡器目标为实例类型时，这将发挥最佳效果。但是，由于多个网络接口，FTDv VM 无法配置为实例类型目标。



### 将实例置于备用状态

如果实例被置于备用状态，则其目标组中的 IP 在运行状况探测失败之前仍将继续处于相同状态。因此，建议在将实例置于备用状态之前，从目标组取消注册各自的 IP；有关详细信息，请参阅[从目标组取消注册目标](#)，第 30 页。

删除 IP 后，请参阅[暂时从 Auto Scaling 组中删除实例](#)。

### 从备用状态删除实例

同样，您也可以将实例从备用状态移至运行状态。从备用状态删除后，实例的 IP 应注册到目标组目标。请参阅[将目标注册到目标组](#)，第 30 页。

有关如何将实例置于备用状态以进行故障排除或维护的详细信息，请参阅 [AWS 新闻博客](#)。

### 从 Auto Scale 组删除/分离实例

要从 Auto Scale 组中删除实例，应首先将其移到备用状态。请参阅“将实例置于备用状态”。当实例处于备用状态后，可以将其删除或分离。请参阅[从 Auto Scaling 组分离 EC2 实例](#)。

FMC 端不会有任何更改。需要手动执行任何必要的更改。

## 终止 FTDv 实例

要终止实例，应将其置于备用状态；请参阅[实例备用](#)，第 30 页。当实例处于备用状态后，即可继续终止。

## 实例内向扩展保护

为避免从 Auto Scale 组中意外删除任何特定实例，可以对其进行内向扩展保护。如果实例受到内向扩展保护，则不会因内向扩展事件而终止。

请参阅以下链接，以便将实例置于内向扩展保护状态。

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-termination.html>



#### 重要事项

建议将状况良好的最小数量的实例（目标 IP 应正常运行，而不仅是 EC2 实例）设为内向扩展保护。

## 更改凭证和 FTDv 注册 ID

配置中的任何更改都不会自动反映在运行中的实例上。更改将仅反映在未来的设备上。应手动将此类更改推送到现有设备。

### 更改 FMC 用户名和密码

在更改 FMC IP、用户名或密码的情况下，应对 Auto Scale Manager Lambda 函数环境变量执行相应的更改。请参阅[使用 AWS Lambda 环境变量](#)。

当 Lambda 下次运行时，将引用更改后的环境变量。



**注释** 环境变量直接送入 Lambda 函数。此处不检查密码复杂性。

### 更改 FTDv Admin 密码

对于运行中的实例，更改 FTDv 密码时要求用户在每个设备上手动更改。对于要载入的新 FTDv 设备，将从 Lambda 环境变量提取 FTDv 密码。请参阅[使用 AWS Lambda 环境变量](#)。

### 更改注册和 NAT ID

对于要使用不同的注册和 NAT ID 载入的新 FTDv 设备，在进行 FMC 注册时，应在 Configuration.json 文件中更改这些信息。可以在 Lambda 资源页中找到 Configuration.json 文件。

## 访问策略和 NAT 策略更改

通过设备组分配的帮助，访问策略或 NAT 策略的任何更改都将自动应用到未来的实例。不过，要更新现有的 FTDv 实例，您需要手动推送配置更改，然后从 FMC 部署这些更改。

## AWS 资源更改

部署后可以在 AWS 中更改许多内容，如 Auto Scale 组、启动配置、CloudWatch 事件、扩展策略等。您可以将资源导入 CloudFormation 堆栈，或通过现有资源创建新的堆栈。

有关如何管理对 AWS 资源执行的更改的详细信息，请参阅[将现有资源引入 CloudFormation 管理](#)。

## 收集和分析 CloudWatch 日志

为了导出 CloudWatch 日志，请参阅[使用 AWS CLI 将日志数据导出到 Amazon S3](#)。

## Auto Scale 故障排除

### 启用/禁用调试日志

部署堆栈时，有一个选项用于将调试日志设置为 True 或 False。请注意，调试日志非常有描述性，它将包括来自 AWS 端的许多不必要的日志详细信息。您可以在部署后通过 Lambda 环境变量更改日志记录。

- Auto Scale Manager 调试日志 - 要禁用来自 Auto Scale Manager Lambda 函数的日志记录，请导航到 Lambda 函数管理器，然后将 DEBUG\_DISABLED 变量更改为“false”。
- Auto Scale 组调试日志 - 要禁用来自 Auto Scale Manager Lambda 函数的日志记录，请导航到 Lambda 生命周期函数，然后将 DEBUG\_DISABLED 变量更改为“false”。



注释 启用调试后，作为调试日志记录的错误消息将不会有问题，因此将得到错误的处理。

#### 检查部署后的输入参数

您可以在 AWS CloudFormation 控制台中验证 CloudFormation 堆栈的输入参数。导航到所需的堆栈，然后选中“参数”选项卡。您还可以在 Lambda 函数环境变量选项卡中检查 Lambda 函数的输入。此外，还可以在 Auto Scale Manager Lambda 函数本身上查看 `configuration.json` 文件。

## 附录 - 用于访问 VPC 专用 IP 的 Lambda 函数

要强制 Lambda 函数访问 VPC 专用 IP 地址（默认情况下，Lambda 函数使用 AWS 从其 EIP 池提供的 IP 地址），您需要从 AWS 控制台进行以下更改。

AWS Lambda 函数具有全局性，具有 AWS 提供的公共 IP 以用于各种 AWS 服务连接、FTDv SSH 连接和 FMC HTTPS 连接。通过将 Lambda 函数置于相同的 VPC 中，借助具有 NAT 作为默认路由的子网，可以使 Lambda 函数使用专用 IP 地址本身访问 VPC 元素（即 FTDv 实例）。

此配置可在部署 Auto Scale 解决方案后完成。有关详细信息，请参阅此链接：

<https://aws.amazon.com/premiumsupport/knowledge-center/internet-access-lambda-function/>

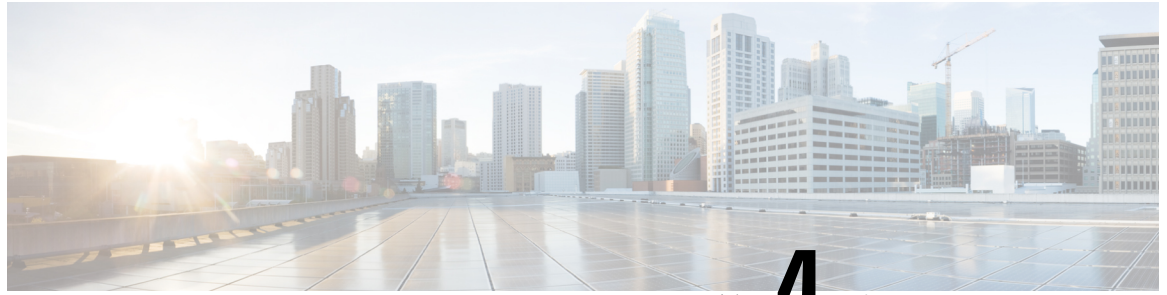
做出这些更改后，将可以使用 AWS NAT 网关 IP 地址限制 FMC 和 FTDv 安全组（入站规则）。此外，如果要在 FTDv 管理接口上避免 EIP（假设 FMC 与 FTDv VPC 连接），您需要使 Lambda 函数为专用于 VPC，以便 Lambda 函数能够访问 VPC 元素（FTDv 实例管理专用 IP 地址）。

应相应修改 `autoscale_manager` 文件夹中的 `asg.yaml` 模板和 `aws.py` python 文件，以使用专用 IP 本身连接 FTDv 实例。

- 对于 `asg.yaml` - 在资源 `AWS::AutoScaling::LaunchConfiguration` 中，参数 `AssociatePublicIpAddress` 设置为“true”。它需要设置为“false”，否则应删除此参数。执行此操作后，FTDv 实例将仅以专用 IP 地址出现。
- 对于 `aws.py` - 线路号码 62 可以复制到线路号码 55，通过这样做，公共 IP 也会更新为管理接口的专用 IP。

截至目前，Python 模块的编写方式使得仅使用公共 IP 地址。这一修改可以使其使用专用 IP 地址。





## 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；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 50 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 35 页
- [登录到 Firepower 管理中心](#)，第 36 页
- [向 Firepower 管理中心注册设备](#)，第 36 页
- [配置基本安全策略](#)，第 38 页
- [访问 Firepower 威胁防御 CLI](#)，第 49 页
- [使用 Firepower Management 管理 Firepower Threat Defense Virtual 的历史](#)，第 50 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>）。

### 过程

---

**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。

### 过程

---

**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:†

Display Name:

Registration Key:\*

Group:

Access Control Policy:\*

#### Smart Licensing

Malware  
 Threat  
 URL Filtering

#### Advanced

Unique NAT ID:†

Transfer Packets

- **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。
- **Domain** - 如果有多域环境，请将设备分配给分叶域。
- **Group** - 如果在使用组，则将其分配给设备组。

- **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 47 页。

- **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** - 指定您在 FTDv 启动程序配置中指定的 NAT ID。
- **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 **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 49 页)，然后使用以下命令 ping FMC IP 地址：  
`ping system ip_address`  
如果 ping 不成功，请使用 **show network** 命令检查您的网络设置。如果需要更改 FTD IP 地址，请使用 **configure network {ipv4 | ipv6} manual** 命令。
- **NTP** - 确保 NTP 服务器与以下页面上设置的 FMC 服务器相符：[系统 > 配置 > 时间同步](#) 页面。
- **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）。您可以在 FTDv 上使用 **configure manager add** 命令设置注册密钥和 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。

## 过程

---

- 步骤 1 [配置接口，第 39 页](#)
  - 步骤 2 [配置 DHCP 服务器，第 42 页](#)
  - 步骤 3 [添加默认路由，第 43 页](#)
  - 步骤 4 [配置 NAT，第 45 页](#)
  - 步骤 5 [配置访问控制，第 47 页](#)
  - 步骤 6 [部署配置，第 48 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。

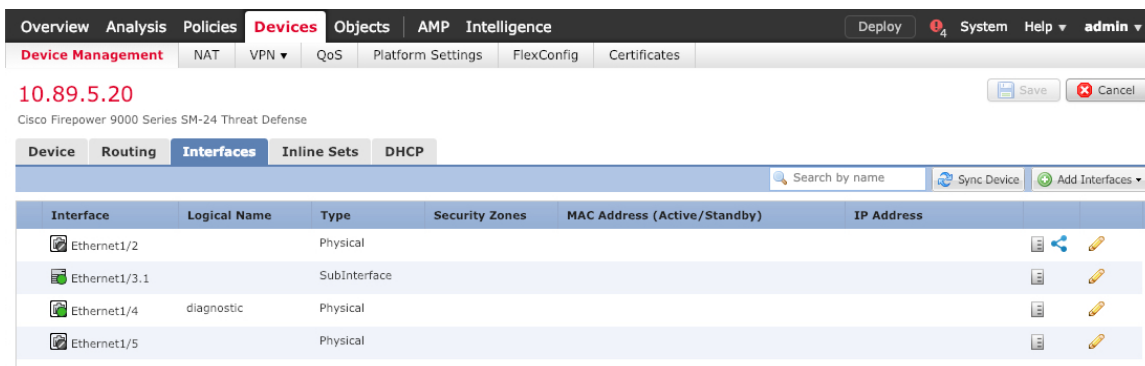
典型的边缘路由情况是通过 DHCP 从 ISP 获取外部接口地址，同时在内部接口上定义静态地址。


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。

## 过程

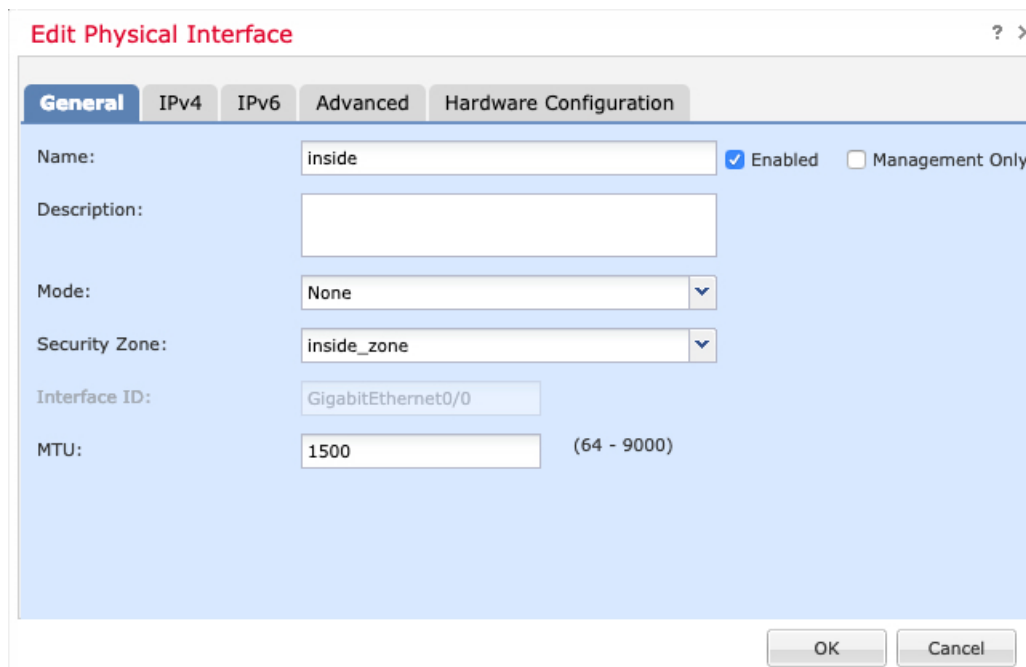
---

- 步骤 1 选择 **设备 > 设备管理**，然后单击该设备的 **编辑**（）。
- 步骤 2 单击 **Interfaces**。



步骤 3 单击要用于内部的接口的编辑（）。

**General** 选项卡将显示。



- 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 **Security Zone** 下拉列表中选择现有的内部安全区域，或者单击 **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) 单击 **IPv4** 和/或 **IPv6** 选项卡。

- **IPv4** - 从下拉列表中选择 **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**。

**步骤 4** 单击要用于外部的接口的 **编辑** (✎)。

**General** 选项卡将显示。

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 **Security Zone** 下拉列表中选择一个现有的外部安全区域，或者单击 **New** 添加一个新的安全区域。

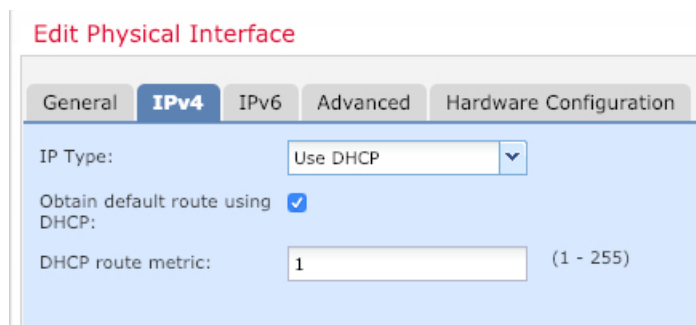
例如，添加一个名为 **outside\_zone** 的区域。

- e) 单击 **IPv4** 和/或 **IPv6** 选项卡。

- **IPv4** - 选择 **Use DHCP**，然后配置以下选填参数：

- **Obtain default route using DHCP** - 从 DHCP 服务器获取默认路由。

- **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 **Autoconfiguration** 复选框。

- f) 单击 **确定**。

**步骤 5** 单击 **保存**。

## 配置 DHCP 服务器

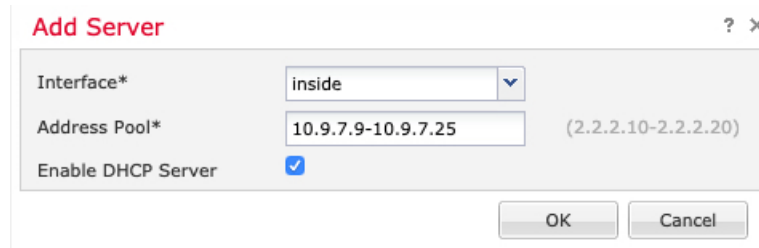
如果希望客户端使用 DHCP 从 FTDv 处获取 IP 地址，请启用 DHCP 服务器。

过程

**步骤 1** 选择 **设备 > 设备管理**，然后单击该设备的 **编辑** (✎)。

**步骤 2** 选择 **DHCP > DHCP 服务器**。

**步骤 3** 在 **Server** 页面上单击 **Add**，然后配置以下选项：



- **Interface** -- 从下拉列表中选择接口。
- **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。
- **Enable DHCP Server** - 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。如果从 DHCP 服务器收到默认路由，它将显示在 **IPv4 路由** 或 **IPv6 路由** 表中，该表位于 **设备 > 设备管理 > 路由 > 静态路由** 页面。

### 过程

步骤 1 选择 **设备 > 设备管理**，然后单击该设备的 **编辑** (✎)。

步骤 2 选择 **路由 > 静态路由**，单击**添加路由**，然后设置以下参数：

The screenshot shows the 'Add Static Route Configuration' dialog box with the following settings:

- Type:  IPv4  IPv6
- Interface\*: outside
- Available Network: any-ipv4 (selected from a list including any-ipv4, IPv4-Benchmark-Tests, IPv4-Link-Local, IPv4-Multicast, IPv4-Private-10.0.0.0-8, IPv4-Private-172.16.0.0, IPv4-Private-192.168.0.0, IPv4-Private-All-RFC191, and IPv6-to-IPv4-Relay-Any)
- Selected Network: any-ipv4
- Gateway\*: default-gateway
- Metric: 1 (range 1 - 254)
- Tunneled:  (Used only for default Route)
- Route Tracking: (empty)

- **Type** - 根据要添加静态路由的类型，单击 **IPv4** 或 **IPv6** 单选按钮。
- **Interface** - 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**。
- **Gateway** 或 **IPv6 Gateway** - 输入或选择作为此路由的下一个跃点的网关节路由器。您可以提供 IP 地址或网络/主机对象。
- **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 **OK**。

路由即已添加至静态路由表。

The screenshot shows the Cisco Firepower 9000 Series SM-24 Threat Defense web interface. The 'Routing' tab is active, and the 'Static Route' configuration is visible. The table below shows the configured static route:

Network	Interface	Gateway	Tunneled	Metric	Tracked
<b>IPv4 Routes</b>					
any-ipv4	outside	10.99.10.1	false	1	
<b>IPv6 Routes</b>					

步骤 4 单击保存。

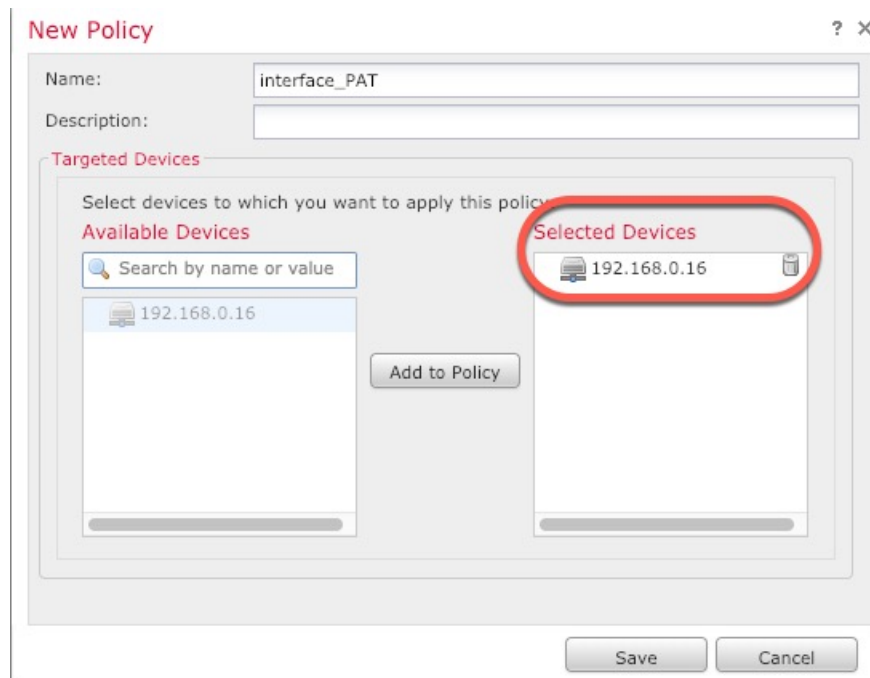
## 配置 NAT

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)。

### 过程

步骤 1 选择 设备 > NAT，然后单击 新策略 > 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。

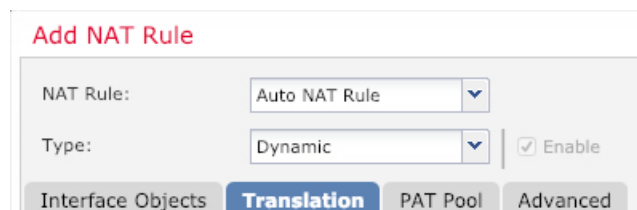


策略即已添加 FMC。您仍然需要为策略添加规则。

步骤 3 单击 **Add Rule**。

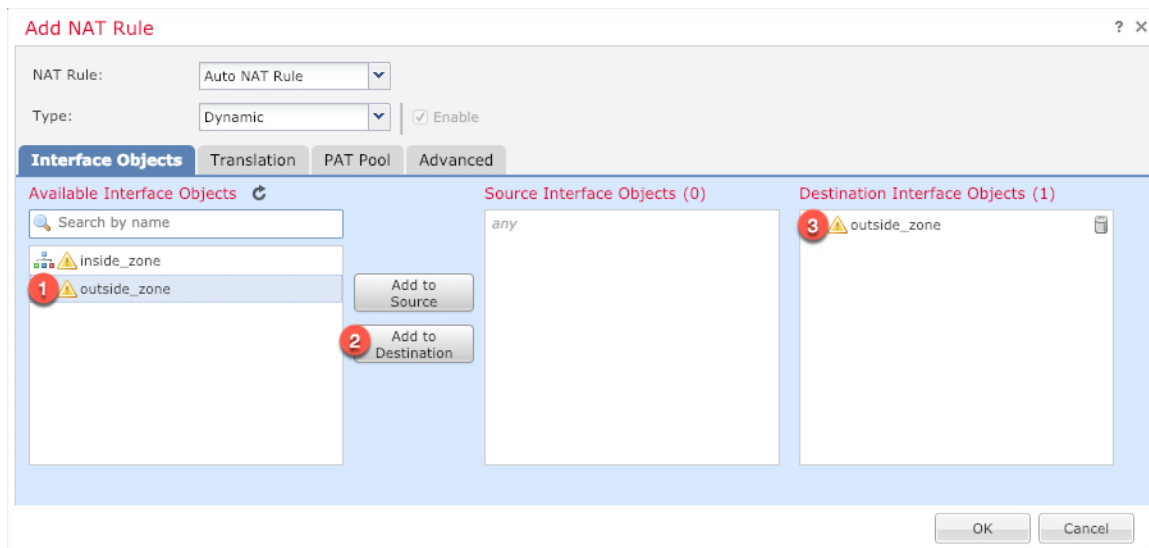
**Add NAT Rule** 对话框将显示。

步骤 4 配置基本规则选项：

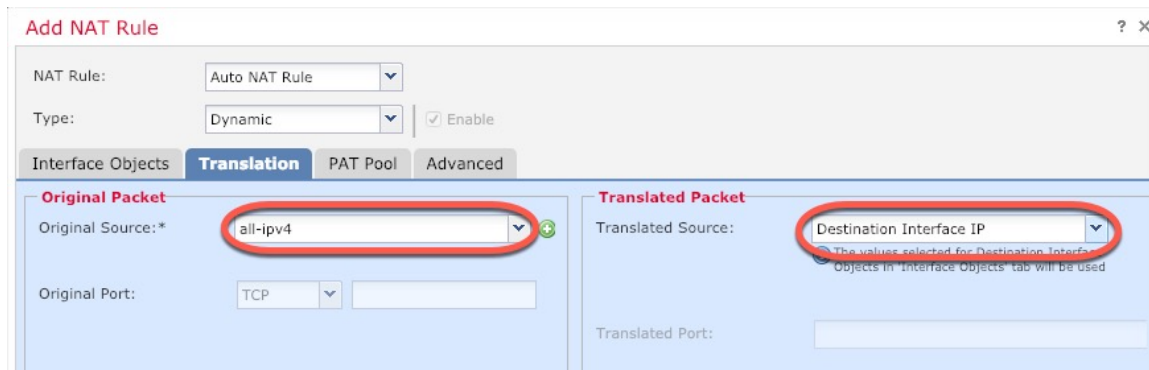


- NAT Rule - 选择 Auto NAT Rule。
- Type - 选择 Dynamic。

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 **Translation** 页面上配置以下选项：



- 原始源 - 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。

- **Translated Source** - 选择 **Destination Interface IP**。

**步骤 7** 单击 **Save** 以添加规则。

规则即已保存至 **Rules** 表。

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
▼ NAT Rules Before											
▼ Auto NAT Rules											
1	+	Dynamic	any	outside_zone	all-ipv4			Interface			Dns:false
▼ NAT Rules After											

**步骤 8** 单击 **NAT** 页面上的 **Save** 以保存更改。

## 配置访问控制

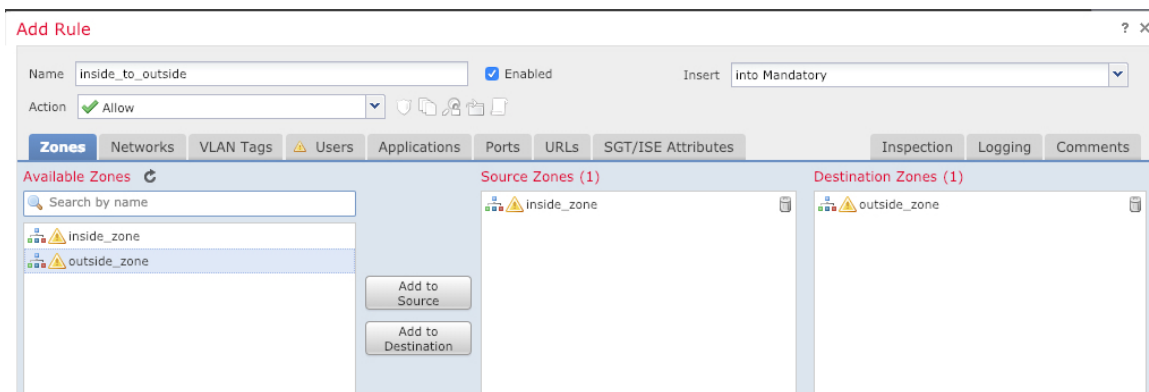
如果您在使用 FMC 注册 FTDv 时创建了基本的封锁所有流量访问控制策略，则需要向策略添加规则以允许流量通过设备。以下程序可添加规则以允许从内部区域到外部区域的流量。如有其他区域，请务必添加允许流量到适当网络的规则。

请参阅 **FMC 配置指南** 以配置更高级的安全设置和规则。

### 过程

**步骤 1** 选择 **策略 > 访问策略 > 访问策略**，然后单击分配给 FTD 的访问控制策略对应的 **编辑** (✎)。

**步骤 2** 单击 **Add Rule** 并设置以下参数：

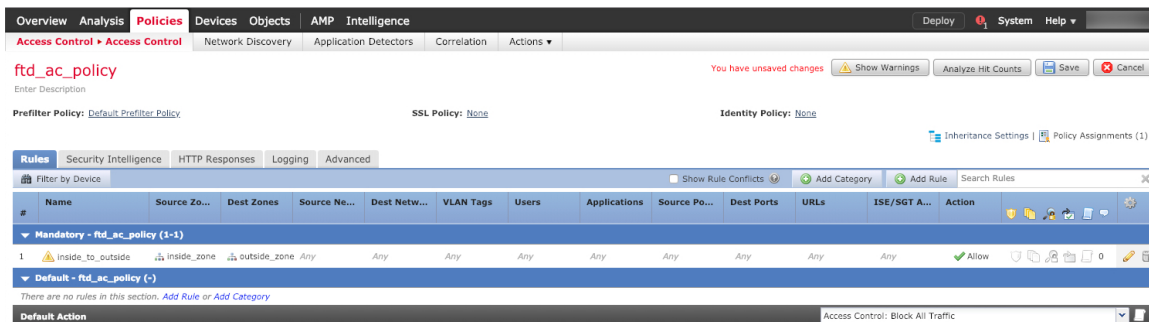


- **Name** - 为此规则命名，例如 **inside\_to\_outside**。
- **Source Zones** - 从 **Available Zones** 中选择内部区域，然后单击 **Add to Source**。
- **Destination Zones** - 从 **Available Zones** 中选择外部区域，然后单击 **Add to Destination**。

其他设置保留原样。

**步骤 3** 单击 **Add**。

规则即已添加至 **Rules** 表。



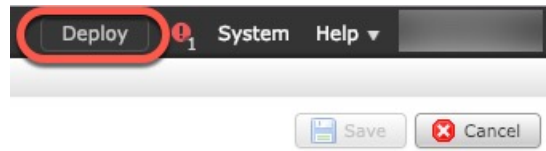
**步骤 4** 单击保存。

## 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。

### 过程

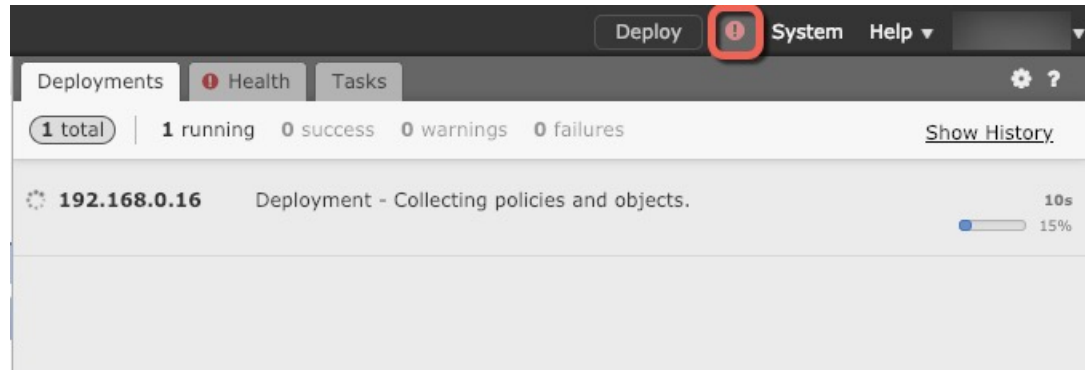
**步骤 1** 单击右上方的 **Deploy**。



步骤 2 选择 **Deploy Policies** 对话框中的设备，然后单击 **Deploy**。



步骤 3 确保部署成功。单击菜单栏中 **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 FTDvCLI 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。

### 过程

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。



## 第 5 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 51 页
- [初始配置](#)，第 52 页
- [如何在 Firepower 设备管理器中配置设备](#)，第 54 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 威胁防御 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 威胁防御 设备的大型网络。

如果要管理大量设备或要使用 Firepower 威胁防御 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 35 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。

### 过程

**步骤 1** 打开浏览器并登录 FDM。假定您未在 CLI 中进行初始配置，请在 <https://ip-address> 中打开 Firepower 设备管理器，其中地址为以下项之一：

- 如果您连接到内部桥组界面：<https://192.168.1.1>。
- 如果连接到管理物理接口，则地址为：<https://192.168.45.45>。

**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。

**注释** 单击下一步后，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) **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，不配置 IPv4 地址。

**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。

b) **管理接口**

**DNS 服务器** - 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** 以重新将合适的 IP 地址载入字段。

**防火墙主机名** - 系统管理地址的主机名。

**注释** 在使用设备设置向导配置 Firepower 威胁防御设备时，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。

a) **时区** - 选择系统时区。

b) **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。

**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 **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 **Device Dashboard**，然后单击 **Smart Licenses** 组中的链接。

**步骤 7** 单击 **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 54 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。

### 过程

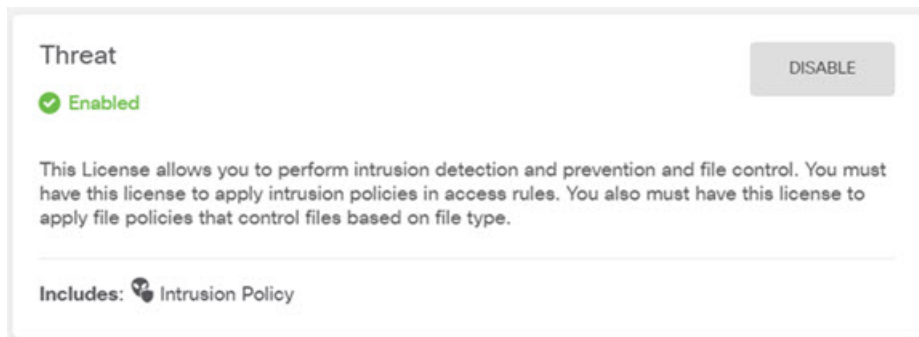
#### 步骤 1 选择 **Device**，然后单击 **Smart License** 组中的 **View Configuration**。

对于您想要使用的可选许可证（威胁、恶意软件、URL），单击**启用**。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**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 2: 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，然后单击接口组中的**查看配置**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**。

图 3: 编辑接口

**Edit Physical Interface**

Interface Name:  Status:

Description:

**IPv4 Address** | IPv6 Address | Advanced Options

Type:

IP Address and Subnet Mask:  /

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，然后从目录中选择安全区域。

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 4: 安全区域对象

**步骤 4** 如果希望内部客户端使用 DHCP 从设备获取 IP 地址，请选择 **设备 > 系统设置 > DHCP 服务器**，然后选择 **DHCP 服务器** 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 **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 5: DHCP 服务器

**步骤 5** 选择 **Device**，然后单击 **Routing** 组中的 **View Configuration**（或 **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** 下拉菜单底部的 **创建新网络**，来创建该对象。

图 6: 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 showing a plus sign and the selected network 'any-ipv4'.

#### 步骤 6 选择策略，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。

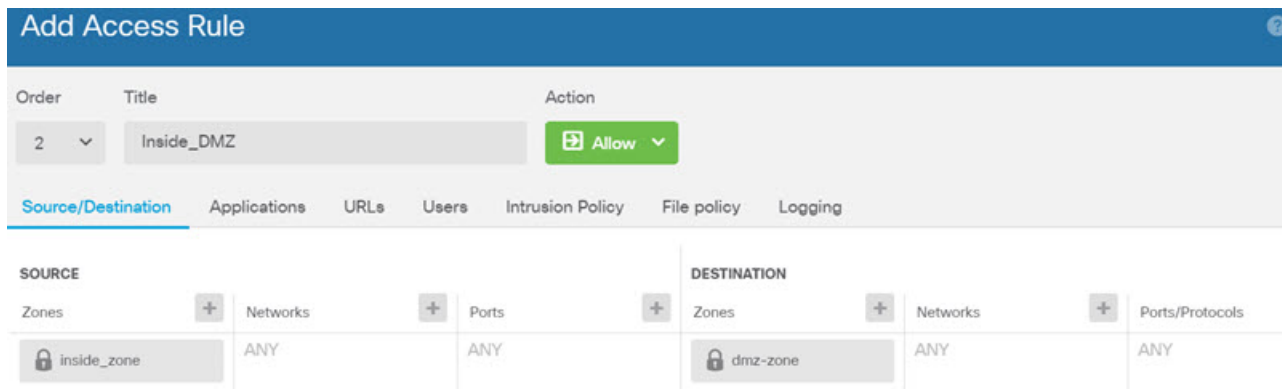
此外，您还可配置其他策略以提供附加服务，并对 NAT 和访问规则进行精细调整，以实现组织需要的结果。您可以配置以下策略：

- **SSL 解密** - 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** - 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。

- **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** - 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** - 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，日志记录除外，其中在连接结束时选项已被选中。

图 7: 访问控制策略



**步骤 7** 选择 **Device**，然后单击 **Updates** 组中的 **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 **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 Cisco Firepower 威胁防御配置指南》](#) 或 Firepower 设备管理器联机帮助。



