



部署 Firepower 威胁防御与 FMC

本章对您适用吗？

本章介绍如何部署使用 FMC 管理的独立式 FTD 逻辑设备。要部署高可用性对或群集，请参阅 [FMC 配置指南](#)。

在大型网络的典型部署中，多个受管设备安装在网段上，监控流量以进行分析，并向负责管理的 FMC 报告，后者有一个使用 Web 界面的集中式管理控制台，您可以用其来执行管控、管理、分析和报告任务。

对于仅包含单个设备或少数设备、无需使用高性能多设备管理器（如 FMC）的网络，您可以使用集成的 Firepower 设备管理器 (FDM)。使用 FDM 基于 Web 的设备设置向导可配置小型网络部署常用的基本软件功能。



注释

隐私收集声明 - Firepower 9300 不要求或主动收集个人身份信息。不过，您可以在配置中使用个人身份信息，例如用于用户名。在这种情况下，管理员在执行配置或使用 SNMP 时可能会看到此信息。

- [关于 Firepower 威胁防御与 FMC](#)，第 2 页
- [在开始之前](#)，第 2 页
- [端到端程序](#)，第 2 页
- [Firepower 机箱管理器：添加 Firepower 威胁防御逻辑设备](#)，第 4 页
- [登录到 Firepower 管理中心](#)，第 8 页
- [获取 Firepower 管理中心的许可证](#)，第 9 页
- [向 Firepower 管理中心注册 Firepower 威胁防御](#)，第 11 页
- [配置基本安全策略](#)，第 13 页
- [访问 Firepower 威胁防御 CLI](#)，第 24 页
- [后续步骤](#)，第 26 页
- [FTD 与 FMC 搭配使用的历史记录](#)，第 26 页

关于 Firepower 威胁防御与 FMC

FTD 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 FTD，这是一个功能齐全的多设备管理器，位于单独的服务器上。

FTD 向您分配给 FTD 逻辑设备的管理接口上的 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 FXOS CLI 连接到 FTD。

在开始之前

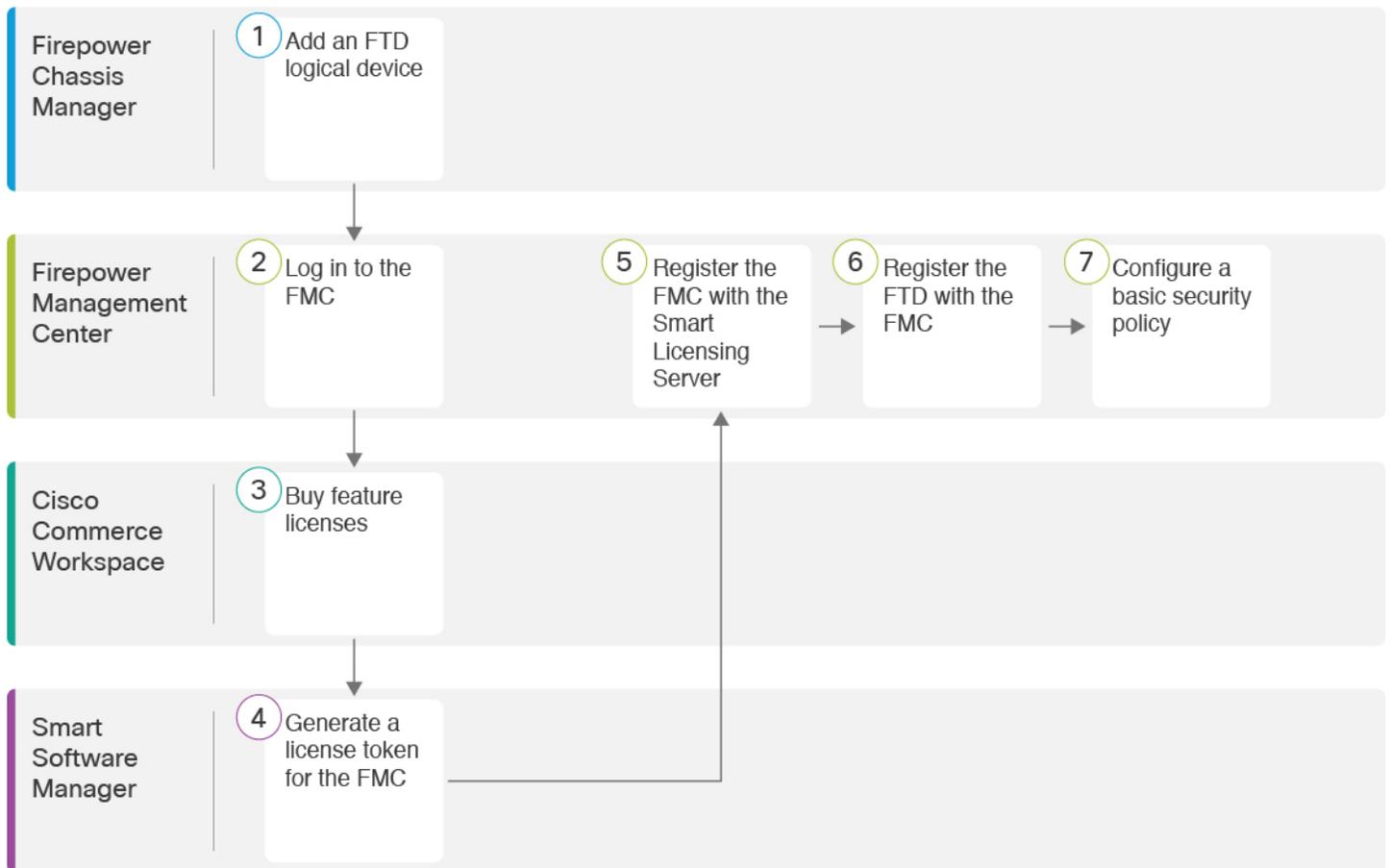
部署并执行 FMC 的初始配置。请参阅 [FMC 入门指南](#)。



注释 Firepower 设备和 FMC 具有相同的默认管理 IP 地址：192.168.45.45。本指南假设您在初始设置期间将为设备设置不同的 IP 地址。

端到端程序

请参阅以下任务以在机箱上部署和配置 FTD。



	工作空间	步骤
①	Firepower 机箱管理器	Firepower 机箱管理器: 添加 Firepower 威胁防御逻辑设备, 第 4 页。
②	FMC	登录到 Firepower 管理中心, 第 8 页。
③	思科商务工作空间	获取 Firepower 管理中心的许可证, 第 9 页: 购买功能许可证。
④	智能软件管理器	获取 Firepower 管理中心的许可证, 第 9 页: 为 FMC 生成许可证令牌。
⑤	FMC	获取 Firepower 管理中心的许可证, 第 9 页: 向智能许可证服务器注册 FMC。
⑥	FMC	向 Firepower 管理中心注册 Firepower 威胁防御, 第 11 页。
⑦	FMC	配置基本安全策略, 第 13 页。

Firepower 机箱管理器：添加 Firepower 威胁防御逻辑设备

您可以从 Firepower 9300 将 FTD 部署为本地实例或容器实例。您可以为每个安全模块安全引擎部署多个容器实例，但只能部署一个本机实例。有关每个型号的最大容器实例数，请参阅[逻辑设备应用程序实例：容器或本地](#)。可以在某些模块上使用本地实例，在其他模块上使用容器实例。

要添加高可用性对或群集，请参阅[FMC配置指南](#)。

您可以通过此程序配置逻辑设备特性，包括应用程序使用的引导程序配置。

开始之前

- 配置与 FTD 一起使用的管理接口；请参阅[配置接口](#)。管理接口是必需的。请注意，此管理接口与仅用于机箱管理的机箱管理端口（并且该端口在接口选项卡的顶部显示为 **MGMT**）不同。
- 您还必须至少配置一个数据接口。
- 对于容器实例，如果您不想采用使用最少资源的默认配置文件，请在平台设置 > 资源配置文件上添加资源配置文件。
- 对于容器实例，在您第一次安装容器实例之前，可能需要重新初始化安全模块，以保证磁盘具有正确的格式。如果必须完成此操作，您将无法保存逻辑设备。单击安全模块，然后单击重新初始化图标 (🔄)。
- 收集以下信息：
 - 此设备的接口 ID
 - 管理接口 IP 地址和网络掩码
 - 网关 IP 地址
 - FMC 您选择的 IP 地址和/或 NAT ID
 - DNS 服务器 IP 地址

过程

步骤 1 在 Firepower 机箱管理器中，选择逻辑设备。

步骤 2 点击添加 > 独立设备，并设置以下参数：



a) 提供设备名称。

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

b) 对于模板 (Template)，请选择思科 Firepower 威胁防御 (Cisco Firepower Threat Defense)。

c) 选择映像版本。

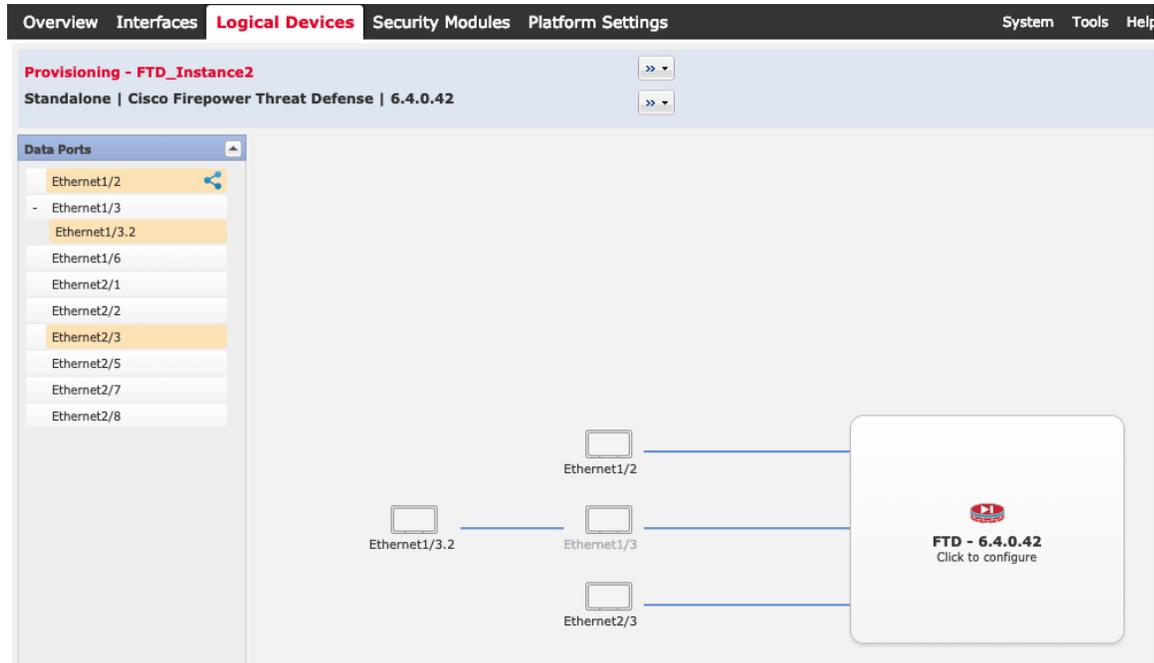
d) 选择实例类型：容器或本地。

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

e) 点击确定。

屏幕会显示调配 - 设备名称 (*Provisioning - device name*) 窗口。

步骤 3 展开数据端口区域，然后点击要分配给设备的每个接口。



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

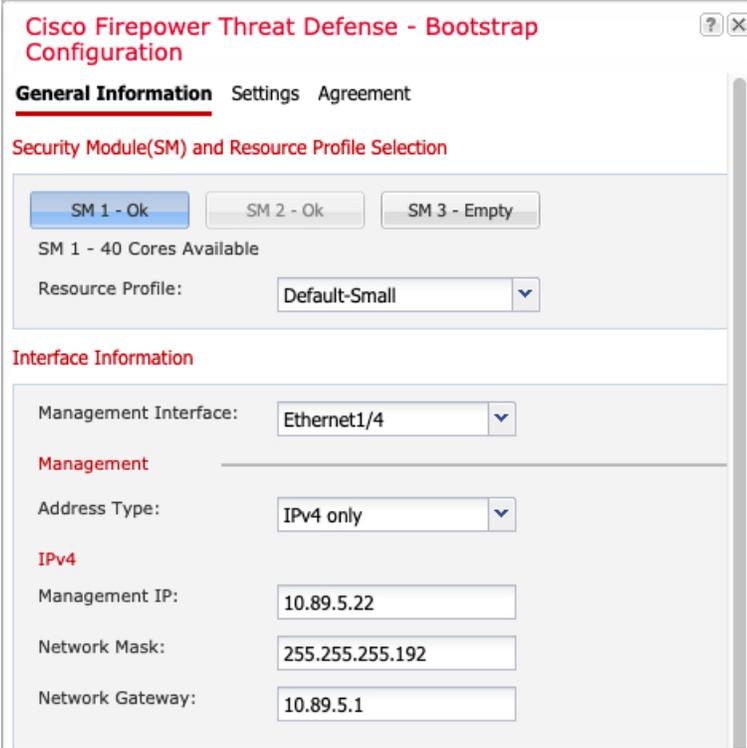
仅可向一个容器实例分配最多 10 个数据共享接口。此外，可以将每个数据共享接口分配至最多 14 个容器实例。数据共享接口以共享图标（）表示。

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

步骤 4 点击屏幕中心的设备图标。

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

步骤 5 在一般信息页面上，完成下列操作：



The screenshot shows the 'Cisco Firepower Threat Defense - Bootstrap Configuration' window. It has three tabs: 'General Information', 'Settings', and 'Agreement'. The 'General Information' tab is active. Under the heading 'Security Module(SM) and Resource Profile Selection', there are three buttons: 'SM 1 - Ok' (highlighted in blue), 'SM 2 - Ok', and 'SM 3 - Empty'. Below these, it says 'SM 1 - 40 Cores Available' and 'Resource Profile: Default-Small' with a dropdown arrow. Under the heading 'Interface Information', 'Management Interface: Ethernet1/4' is selected. Below that, under 'Management', 'Address Type: IPv4 only' is selected. Under 'IPv4', there are three input fields: 'Management IP: 10.89.5.22', 'Network Mask: 255.255.255.192', and 'Network Gateway: 10.89.5.1'.

- 在安全模块选择下，单击您想用于此逻辑设备的安全模块。
- 对于容器实例，指定资源配置文件。

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

- 选择管理接口。
此接口用于管理逻辑设备。此接口独立于机箱管理端口。
- 选择管理接口地址类型：仅 IPv4、仅 IPv6 或 IPv4 和 IPv6。

- e) 配置管理 IP 地址。
设置用于此接口的唯一 IP 地址。
- f) 输入网络掩码 (Network Mask) 或前缀长度 (Prefix Length)。
- g) 输入网络网关 (Network Gateway) 地址。

步骤 6 在设置 (Settings) 选项卡上，完成下列操作：

Cisco Firepower Threat Defense - Bootstrap Configuration

General Information **Settings** Agreement

Management type of application instance: FMC

Firepower Management Center IP: 10.89.5.35

Search domains: cisco.com

Firewall Mode: Routed

DNS Servers: 10.89.5.67

Firepower Management Center NAT ID: test

Fully Qualified Hostname: ftd2.cisco.com

Registration Key:

Confirm Registration Key:

Password:

Confirm Password:

Eventing Interface: [dropdown]

- a) 对于本地实例，在应用实例的管理类型下拉列表中，选择 **FMC**。
本地实例还支持 FDM 作为管理器。部署逻辑设备后，无法更改管理器类型。
- b) 输入管理 FMC 的 **Firepower 管理中心 IP**。如果不知道 FMC IP 地址，请将此字段留空，并在 **Firepower 管理中心 NAT ID** 字段中输入口令。
- c) 对于容器实例，选择是否允许 **FTD SSH 会话专家模式**：是或否。专家模式提供 FTDshell 访问权限以确保实现高级故障排除。

对于此选项，如果您选择是，拥有直接从 SSH 会话访问容器实例的权限的用户可以输入专家模式。如果您选择否，只有拥有从 FXOS CLI 访问容器实例的权限的用户可以输入专家模式。我们建议选择否以加强实例之间的隔离。

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

- d) 输入逗号分隔列表形式的搜索域。
- e) 选择防火墙模式：透明或路由式。

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

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

- f) 输入逗号分隔列表形式的 **DNS 服务器**。
- 例如，如果指定 FMC 主机名，则 FTD 使用 DNS。
- g) 输入 FTD 的完全限定主机名。
- h) 输入注册期间要在 FMC 和设备之间共享的 **注册密钥**。

可以为该密钥选择介于 1 至 37 个字符之间的任何文本字符串；添加 FTD 时，需要在 FMC 上输入相同的密钥。

- i) 输入供 FTD 管理员用户用于 CLI 访问的 **密码**。
 - j) 选择应该发送 Firepower 事件的 **事件接口**。如果未指定，系统将使用管理接口。
- 此接口必须定义为 Firepower 事件接口。

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

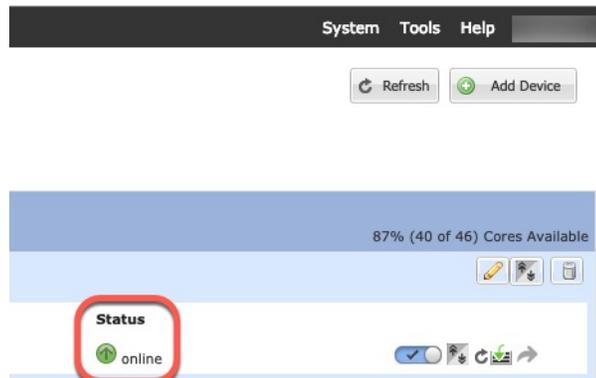
此设置在硬件中启用 TLS 加密加速，并提高某些类型流量的性能。有关详细信息，请参阅《FMC 配置指南》。本地实例不支持此功能。要查看分配给该实例的硬件加密资源百分比，请输入 **show hw-crypto** 命令。

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

步骤 8 点击 **确定 (确定)** 关闭配置对话框。

步骤 9 点击 **保存**。

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



登录到 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

步骤 2 输入您的用户名和密码。

步骤 3 单击 **Log In**。

获取 Firepower 管理中心的许可证

所有许可证都由 FMC 提供给 FTD。您可以选择购买以下功能许可证：

- 威胁 - 安全情报和思科 Firepower 下一代 IPS
- 恶意软件 - 适用于网络的高级恶意软件防护 (AMP)
- URL - URL 过滤
- RA VPN - AnyConnect Plus、AnyConnect Apex 或仅 AnyConnect VPN。

除上述许可证外，您还需要订阅相关内容以获取 1 年、3 年或 5 年的更新。

开始之前

- 拥有 [思科智能软件管理器](#) 主帐户。

如果您还没有帐户，请单击此链接以 [设置新帐户](#)。通过智能软件管理器，您可以为组织创建一个主帐户。

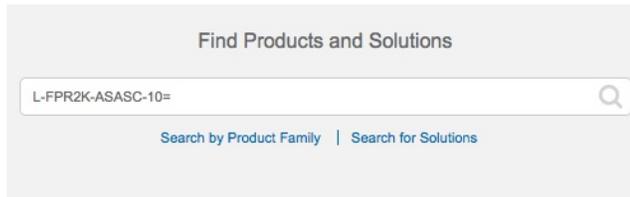
- 您的思科智能软件许可帐户必须符合强加密 (3DES/AES) 许可证的要求，才能使用某些功能（已使用导出合规性标志启用）。

过程

步骤 1 请确保智能许可帐户包含所需的可用许可证。

当您从思科或经销商那里购买设备时，您的许可证应该已链接到您的智能软件许可帐户。但是，如果您需要自己添加许可证，则请使用 [思科商务工作空间](#) 上的 **Find Products and Solutions** 搜索字段。搜索以下许可证 PID：

图 1: 许可证搜索



注释 如果未找到 PID，您可以手动将 PID 添加到订单中。

- 威胁、恶意软件和 URL 许可证组合：

- L-FPR9K-24T-TMC=
- L-FPR9K-36T-TMC=
- L-FPR9K-40T-TMC=
- L-FPR9K-44T-TMC=
- L-FPR9K-48T-TMC=
- L-FPR9K-56T-TMC=

- 威胁、恶意软件和 URL 订阅组合：

- L-FPR9K-24T-TMC-1Y
- L-FPR9K-24T-TMC-3Y
- L-FPR9K-24T-TMC-5Y
- L-FPR9K-36T-TMC-1Y
- L-FPR9K-36T-TMC-3Y
- L-FPR9K-36T-TMC-5Y
- L-FPR9K-40T-TMC-1Y
- L-FPR9K-40T-TMC-3Y
- L-FPR9K-40T-TMC-5Y
- L-FPR9K-44T-TMC-1Y
- L-FPR9K-44T-TMC-3Y
- L-FPR9K-44T-TMC-5Y
- L-FPR9K-48T-TMC-1Y
- L-FPR9K-48T-TMC-3Y
- L-FPR9K-48T-TMC-5Y

- L-FPR9K-56T-TMC-1Y
 - L-FPR9K-56T-TMC-3Y
 - L-FPR9K-56T-TMC-5Y
- RA VPN - 请参阅[思科 AnyConnect 订购指南](#)。

步骤 2 如果尚未执行此操作，请向智能许可服务器注册 FMC。

注册需要您在智能软件管理器中生成注册令牌。有关详细指示，请参阅[FMC配置指南](#)。

向 Firepower 管理中心注册 Firepower 威胁防御

将每个逻辑设备分别注册到同一个 FMC。

开始之前

- 确保 Firepower 机箱管理器 **logical device** 页面上 FTD 逻辑设备 **Status** 为 **online**。
- 收集您在 FTD 初始引导程序配置中设置的以下信息（请参阅[Firepower 机箱管理器：添加 Firepower 威胁防御逻辑设备，第 4 页](#)）；
 - FTD管理 IP 地址和/或 NAT ID
 - FMC 注册密钥

过程

步骤 1 在 FMC 中，选择 **Devices > Device Management**。

步骤 2 从 **Add** 下拉列表选择 **Add Device**，然后输入以下参数。

Add Device ? X

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

- **Host** - 输入要添加 FTD 的 IP 地址。如果在 FTD 初始引导程序配置中同时指定了 FMC IP 地址和 NAT ID，可以将此字段留空。
- **Display Name** - 输入要在 FMC 中显示的 FTD 的名称。
- **Registration Key** - 输入您在 FTD 初始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 [允许流量从内部传到外部](#)，第 22 页。

New Policy ? X

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

- **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）。
- **Unique NAT ID** - 指定您在 FTD 初始引导程序配置中指定的 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 FTD 注册失败，请检查以下项：

- **Ping** - 访问 FTD CLI (访问 [Firepower 威胁防御 CLI](#)，第 24 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 Firepower 9300 NTP 服务器与 **System > Configuration > Time Synchronization** 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 FTD 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。

要配置基本安全策略，需完成以下任务。

- 1 配置接口，第 14 页。

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

配置接口

启用 FTD 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。

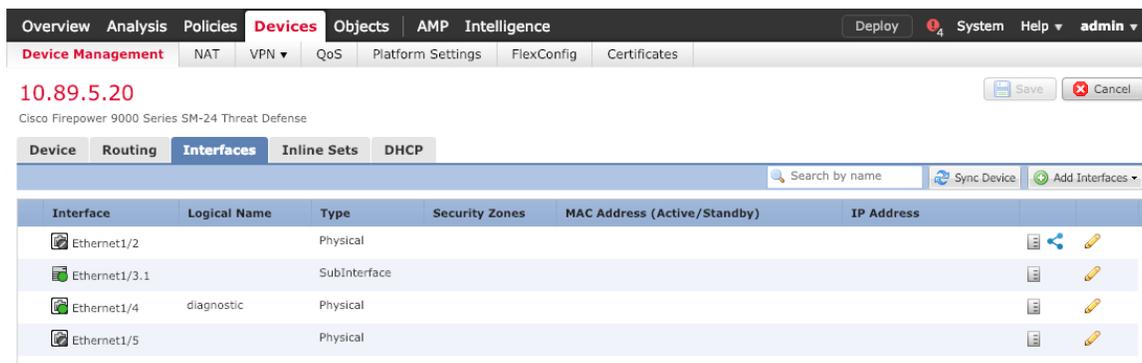
典型的边缘路由情况是通过 DHCP 从 ISP 获取外部接口地址，同时在内部接口上定义静态地址。

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

步骤 2 单击 **Interfaces**。



步骤 3 单击要用于内部的接口的编辑图标（）。

General 选项卡将显示。

Edit Physical Interface

General | IPv4 | IPv6 | Advanced | Hardware Configuration

Name: Enabled Management Only

Description:

Mode: ▼

Security Zone: ▼

Interface ID:

MTU: (64 - 9000)

OK Cancel

- 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** 下拉列表中选择一个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。

- 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**

Edit Physical Interface

General | **IPv4** | IPv6 | Advanced | Hardware Configuration

IP Type: ▼

IP Address: eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

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

f) 单击 **OK**。

步骤 4 单击要用于外部的接口的 编辑图标 (✎)。

General 选项卡将显示。

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

- Name:** outside
- Description:** (empty)
- Mode:** None
- Security Zone:** outside_zone
- Interface ID:** GigabitEthernet0/0
- MTU:** 1500 (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 **outside**。
- 选中 **Enabled** 复选框。
- 将 **Mode** 保留为 **None**。
- 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。
- 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。

Edit Physical Interface

General **IPv4** IPv6 Advanced Hardware Configuration

IP Type: Use DHCP

Obtain default route using DHCP:

DHCP route metric: 1 (1 - 255)

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

f) 点击确定。

步骤 5 点击保存。

配置 DHCP 服务器

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

过程

步骤 1 选择 **Devices > Device Management**，然后单击设备的编辑图标（）。

步骤 2 选择 **DHCP > DHCP Server**。

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

Add Server ? x

Interface* inside

Address Pool* 10.9.7.9-10.9.7.25 (2.2.2.10-2.2.2.20)

Enable DHCP Server

OK Cancel

- **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 点击确定。

步骤 5 点击保存。

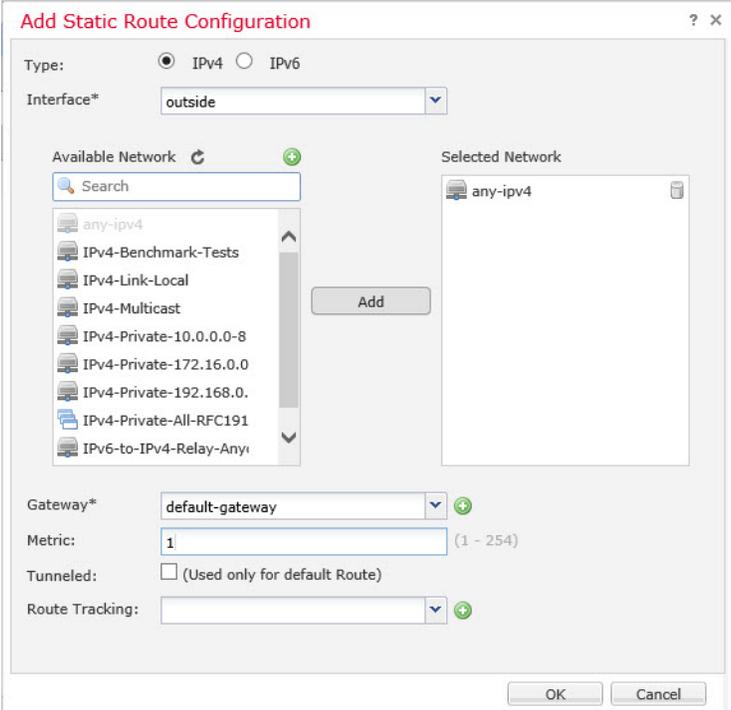
添加默认路由

默认路由通常指向可从外部接口访问的上游路由器。如果您将 DHCP 用作外部接口，则您的设备可能已经收到了默认路由。如果需要手动添加路由，则遵照此程序执行。如果收到来自 DHCP 服务器的默认路由，其将显示在 **Devices > Device Management > Routing > Static Route** 页面上的 **IPv4 Routes** 或 **IPv6 Routes** 表中。

过程

步骤 1 选择 **Devices > Device Management**，然后单击设备的编辑图标（）。

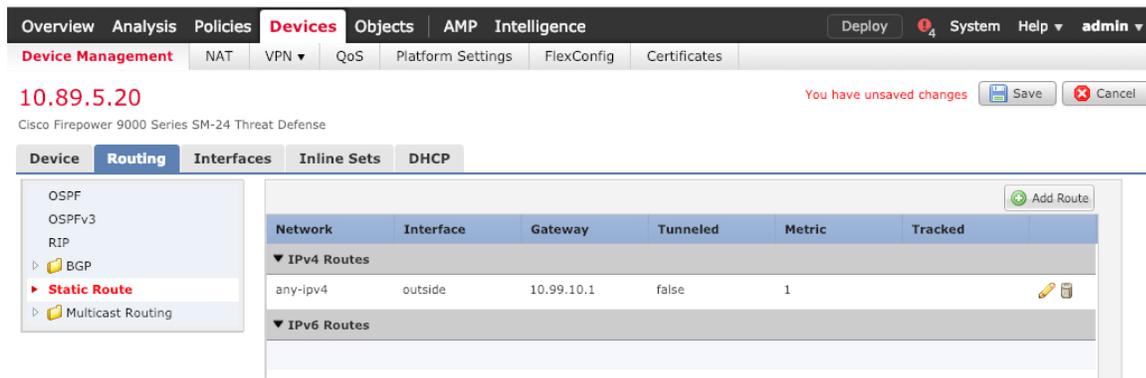
步骤 2 选择 **Route > Static Route**，单击 **Add Route**，然后设置以下项：



- **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。
- **Available Network** - 为 IPv4 默认路由选择 **any-ipv4**，为 IPv6 默认路由选择 **any-ipv6**，然后单击 **Add** 将其移至 **Selected Network** 列表。
- **Gateway** 或 **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。
- **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。



10.89.5.20 You have unsaved changes Save Cancel

Cisco Firepower 9000 Series SM-24 Threat Defense

Device Routing Interfaces Inline Sets DHCP

OSPF
OSPFv3
RIP
BGP
Static Route
Multicast Routing

Network	Interface	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes					
any-ipv4	outside	10.99.10.1	false	1	
▼ IPv6 Routes					

步骤 4 点击保存。

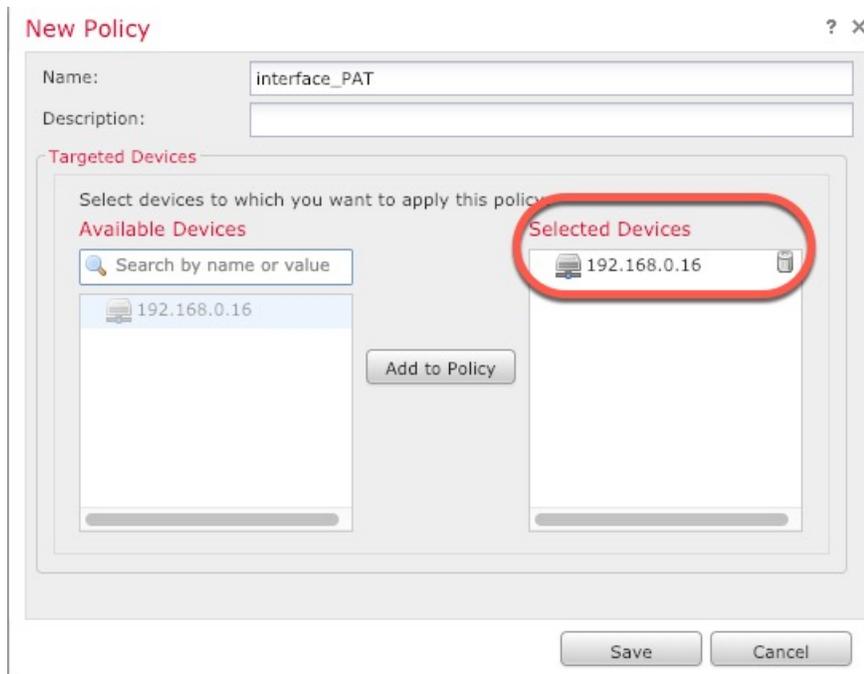
配置 NAT

典型的 NAT 规则会将内部地址转换为外部接口 IP 地址上的端口。这类 NAT 规则称为接口端口地址转换 (PAT)。

过程

步骤 1 选择 **Devices > NAT**，然后单击 **New Policy > 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**。

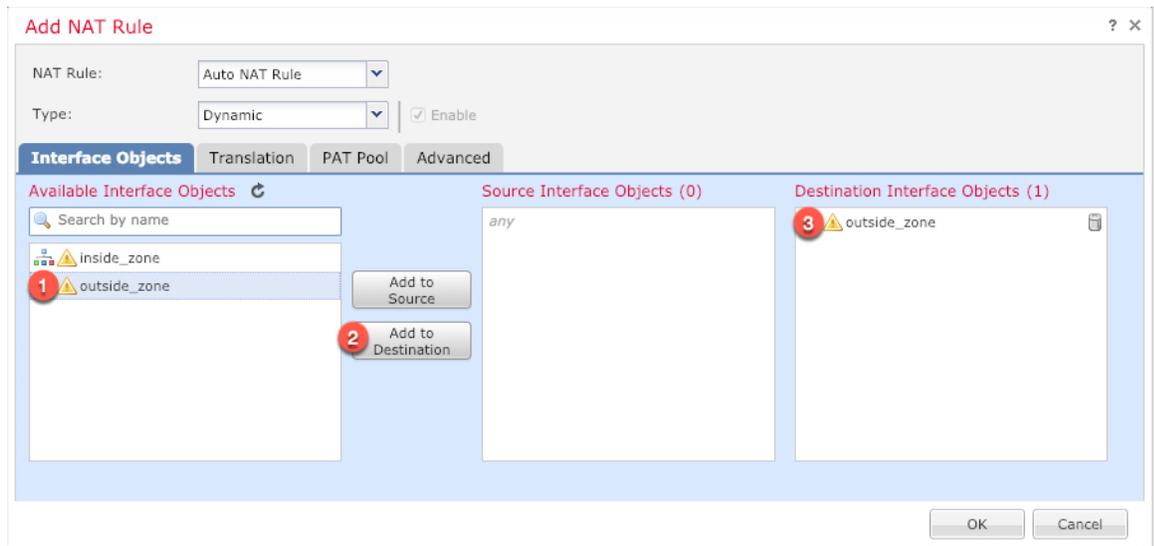
Add NAT Rule 对话框将显示。

步骤 4 配置基本规则选项：

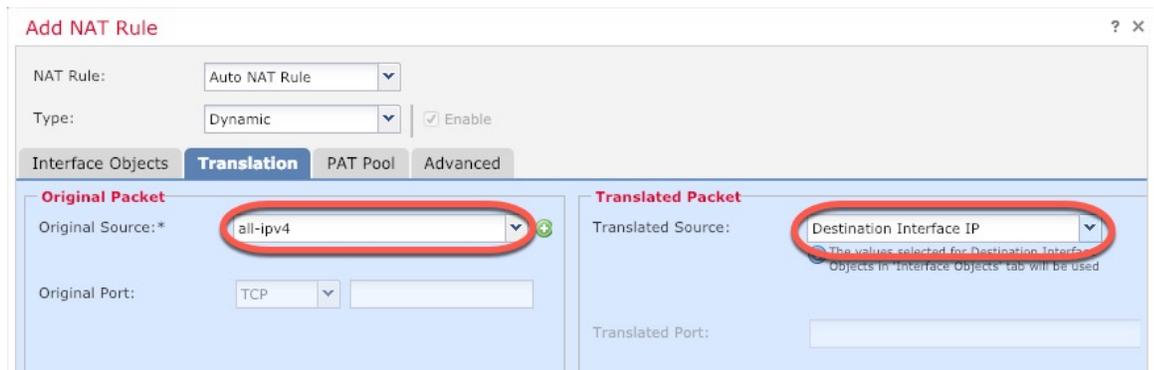


- **NAT Rule** - 选择 **Auto NAT Rule**。
- **Type** - 选择 **Dynamic**。

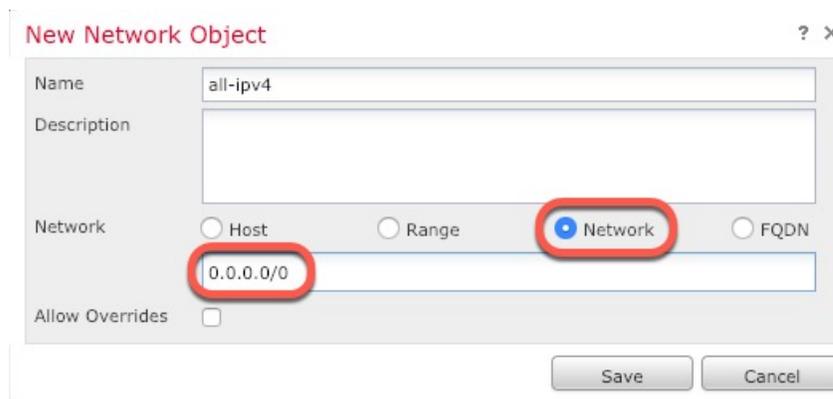
步骤 5 在 **Interface Objects** 页面，将 **Available Interface Objects** 区域中的外部区域添加到 **Destination Interface Objects** 区域。



步骤 6 在 **Translation** 页面上配置以下选项：



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

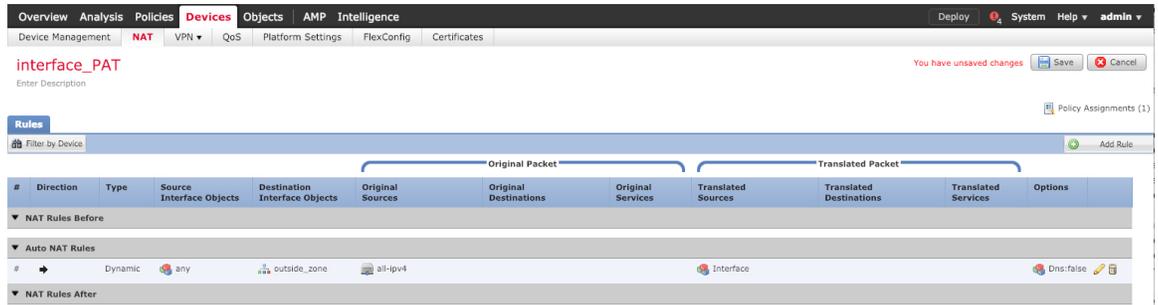


注释 您不能使用系统定义的 **any-ipv4** 对象，因为自动 NAT 规则将 NAT 添加为对象定义的一部分，您无法编辑系统定义的对象。

- **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。



步骤 8 单击 **NAT** 页面上的 **Save** 以保存更改。

允许流量从内部传到外部

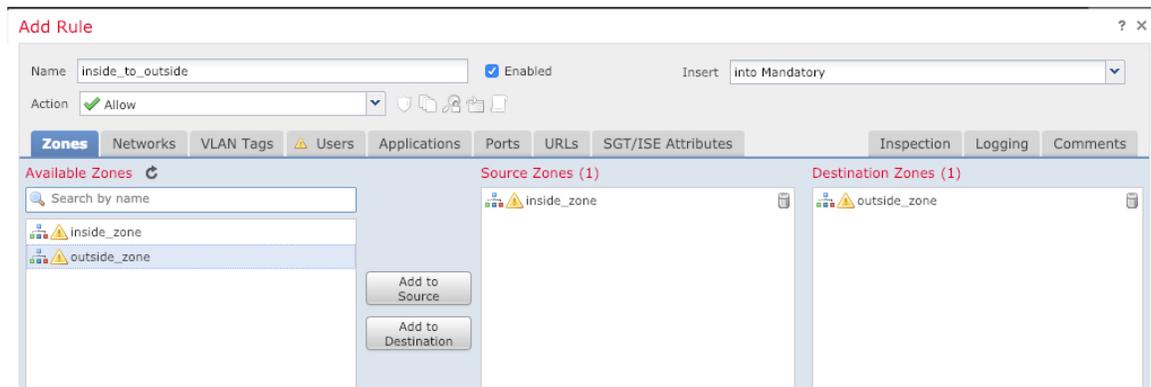
如果您在使用 FMC 注册 FTD 时创建了基本的封锁所有流量访问控制策略，则需要向策略添加规则以允许流量通过设备。以下程序可添加规则以允许从内部区域到外部区域的流量。如有其他区域，请务必添加允许流量到适当网络的规则。

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 **Policy > Access Policy > Access Policy**，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 **Add Rule** 并设置以下参数：

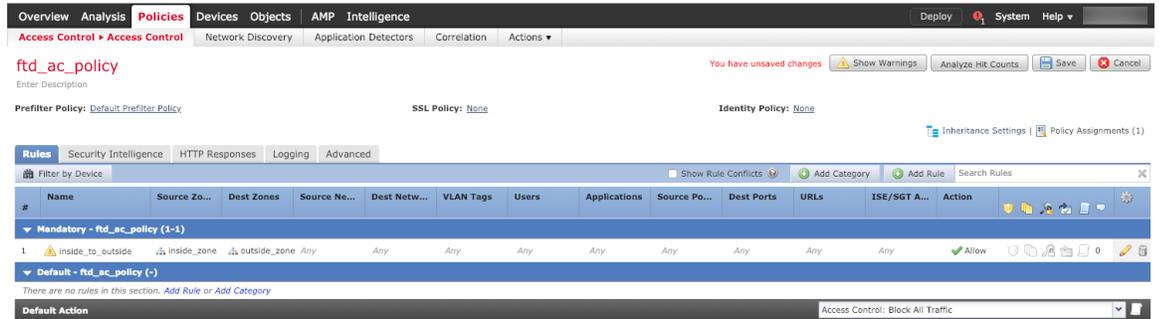


- **Name** - 为此规则命名，例如 **inside_to_outside**。
- **Source Zones** - 从 **Available Zones** 中选择内部区域，然后单击 **Add to Source**。
- **Destination Zones** - 从 **Available Zones** 中选择外部区域，然后单击 **Add to Destination**。

其他设置保留原样。

步骤 3 单击 **Add**。

规则即已添加至 **Rules** 表。



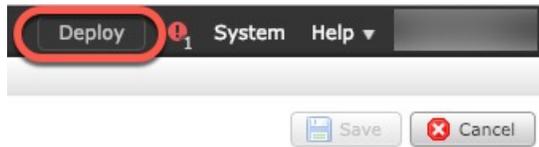
步骤 4 点击保存。

部署配置

将配置更改部署到 FTD；在部署之前，您的所有更改都不会在设备上生效。

过程

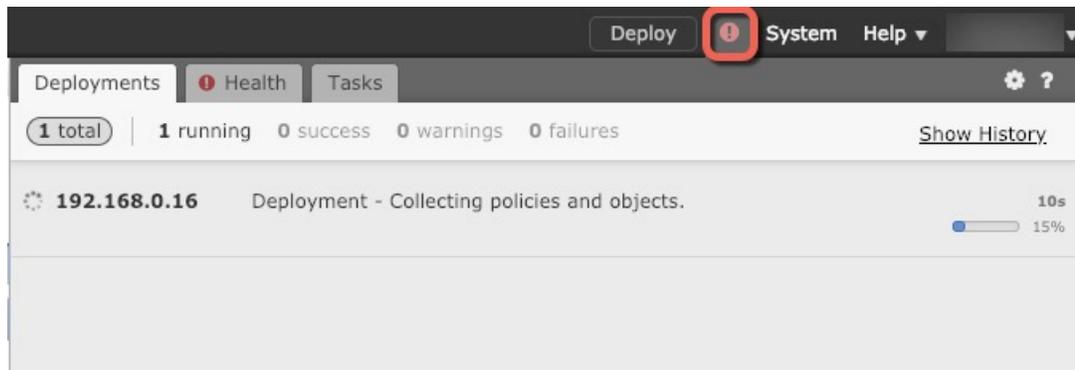
步骤 1 单击右上方的 **Deploy**。



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

过程

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

在部署逻辑设备时，您需要设置管理 IP 地址。使用 `admin` 帐户和初始部署期间设定的密码登录 FTD。如果忘记密码，可以编辑 Firepower 机箱管理器中的逻辑设备以更改密码。

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

a) 连接到安全模块。

```
connect module slot_number { console | telnet }
```

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

示例：

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

```
CISCO Serial Over LAN:
Close Network Connection to Exit
```

```
Firepower-module1>
```

b) 连接到 FTD 控制台。

```
connect ftd name
```

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

示例:

```
Firepower-module1> connect ftd FTD_Instance1

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

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

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

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

注释 对于 6.3 之前的版本，输入 **Ctrl-a, d**。

- d) 返回 FXOS CLI 的管理引擎层。

要退出控制台:

1. 输入 ~

您将退出至 Telnet 应用。

2. 要退出 Telnet 应用，请输入:

```
telnet>quit
```

要退出 Telnet 会话:

输入 **Ctrl-], .**

示例

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

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

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect ftd FTD_Instance1
```

```
===== ATTENTION =====
You are connecting to ftd from a serial console. Please avoid
executing any commands which may produce large amount of output.
```

Otherwise, data cached along the pipe may take up to 12 minutes to be drained by a serial console at 9600 baud rate after pressing Ctrl-C.

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

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

后续步骤

要继续配置 FTD，请参阅适用于您的软件版本的文档：[导航思科 Firepower 文档](#)。

有关使用 FMC 的信息，请参阅 [《Firepower 管理中心配置指南》](#)。

FTD 与 FMC 搭配使用的历史记录

功能名称	版本	功能信息
支持在同一个 Firepower 9300 上使用独立的 ASA 和 FTD 模块	6.4	您现在可以在同一个 Firepower 9300 上同时部署 ASA 和 FTD 逻辑设备。 注释 需要 FXOS 2.6.1。

功能名称	版本	功能信息
Firepower 4100/9300 上 Firepower 威胁防御的多实例功能	6.3.0	<p>您现在可以在单个安全引擎/模块上部署多个逻辑设备，每台逻辑设备都设 Firepower 威胁防御容器实例。以前，您仅可部署单个本地应用实例。</p> <p>要确保灵活使用物理接口，可以在 FXOS 中创建 VLAN 子接口，还可以在多个实例之间共享接口。资源管理允许您自定义每个实例的性能。</p> <p>您可以使用在 2 个独立机箱上使用一个容器实例的高可用性。不支持群集。</p> <p>注释 尽管实现方式不同，但多实例功能与 ASA 多情景模式类似。Firepower 威胁防御不支持多情景模式。</p> <p>新增/修改的 Firepower 管理中心菜单项：</p> <ul style="list-style-type: none"> • 设备 > 设备管理 > 编辑图标 > 接口选项卡 <p>新增/修改的 Firepower 机箱管理器菜单项：</p> <ul style="list-style-type: none"> • 概述 > 设备 • 接口 > 所有接口 > 添加新下拉菜单 > 子接口 • 接口 > 所有接口 > 类型 • 逻辑设备 > 添加设备 • 平台设置 > Mac 池 • 平台设置 > 资源配置文件

