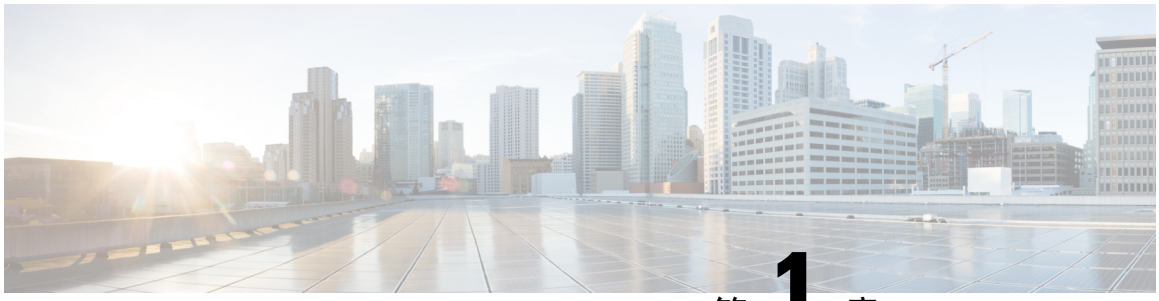


Cisco Firepower 4100 入门指南

首次发布日期: 2019 年 3 月 5 日

上次修改日期: 2023 年 1 月 23 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

哪种应用和管理器适合您？

您的硬件平台可以运行两种应用之一。对于每种应用，您都可以选择管理器。本章介绍应用和管理器选项。

- 应用，第 1 页
- 管理器，第 1 页

应用

您可以在硬件平台上使用 Cisco Secure Firewall ASA 或 Cisco Secure Firewall Threat Defense（之前的 Firepower Threat Defense） 应用。

- ASA - ASA 是传统的高级状态防火墙和 VPN 集中器。

  如果您不需要 威胁防御 的高级功能，或者您需要 威胁防御 尚未提供的纯 ASA 功能，则可能需要使用 ASA。Cisco 提供 ASA-to-威胁防御 的迁移工具，如果您最初为 ASA，后期要重新映像到 威胁防御，可使用这些工具将 ASA 转换为 威胁防御。

- 威胁防御—威胁防御是下一代防火墙，它将高级状态防火墙、VPN 集中器和新一代 IPS 结合在一起。也就是说，威胁防御 拥有最佳的 ASA 功能，并将其与最佳的新一代防火墙和 IPS 功能结合起来。

  我们建议使用 威胁防御 而非 ASA，因为它包含 ASA 的大多数主要功能，以及额外的新一代防火墙和 IPS 功能。

管理器

威胁防御和 ASA 支持多个管理器。

威胁防御管理器

表 *1:* 威胁防御管理器

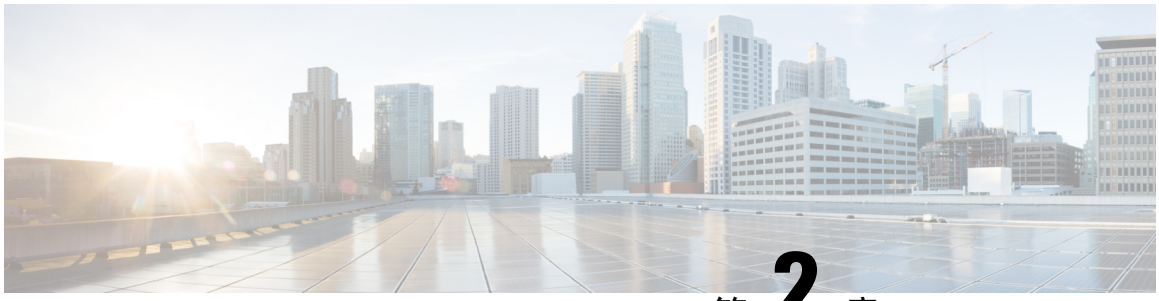
理器	说明
Cisco Secure Firewall Management Center（之前的 Firepower 管理中心）	管理中心 是一个功能强大的、基于 Web 的多设备管理器，它在自己的服务器硬件上运行，或者在虚拟机监控程序上作为虚拟设备运行。如果您需要多设备管理器，并且您需要 威胁防御上的所有功能，则应使用 管理中心 。管理中心 还提供强大的流量和事件的分析与监控功能。 **注释** 管理中心与其他管理器不兼容，因为管理中心拥有威胁防御配置，不允许绕过管理中心直接配置威胁防御。 要开始使用 管理中心，请首先按照 Firepower 4100 机箱初始配置， 第 5 页 设置机箱，然后参阅使用管理中心部署威胁防御， 第 29 页。
Secure Firewall 设备管理器（之前的 Firepower 设备管理器）	设备管理器 是一个基于 Web 的、简化的设备上管理器。由于它是简化的，因此使用 设备管理器 时不支持某些 威胁防御 功能。如果您只管理少量设备，而不需要多设备管理器，应使用 设备管理器。 **注释** 设备管理器 和 CDO 在 FDM 模式下都能发现防火墙上的配置，因此您可以使用 设备管理器 和 CDO 来管理相同的防火墙。管理中心与其他管理器不兼容。 要开始使用 设备管理器，请首先按照 Firepower 4100 机箱初始配置， 第 5 页 设置机箱，然后参阅使用设备管理器部署威胁防御， 第 57 页。
思科防御协调器 (CDO)	CDO 提供两种管理模式： • （7.2 及更高版本）云交付的管理中心模式，拥有本地管理中心的所有配置功能。对于分析功能，您可以使用云中的 Cisco Secure Cloud Analytics 或本地管理中心。 • （仅限现有 CDO 用户）可带来简化用户体验的设备管理器模式。此模式仅适用于已在设备管理器模式下使用 CDO 管理 威胁防御 的用户。本指南不介绍该模式。 由于 CDO 是基于云的，因此在自己的服务器上运行 CDO 不会产生任何开销。CDO 还管理其他安全设备（例如 ASA），因此您可以对所有安全设备使用单一的管理器。 要开始 CDO 调配，请参阅使用 CDO 部署威胁防御， 第 85 页。
Cisco Secure Firewall Threat Defense REST API	威胁防御 REST API 支持自动化直接配置 威胁防御。此 API 可与 设备管理器 和 CDO 同时使用，因为二者都可以发现防火墙上的配置。如果您使用 管理中心 管理 威胁防御，则无法使用此 API。 本指南未涵盖威胁防御 REST API。有关详细信息，请参阅Cisco Secure Firewall Threat Defense REST API 指南。

理器	说明
Cisco Secure Firewall Management Center REST API	管理中心 REST API 允许自动配置 管理中心 策略，随后可将其应用于托管的 威胁防御。该 API 不直接管理 威胁防御。 本指南未涵盖管理中心 REST API。有关详细信息，请参阅Secure Firewall Management Center REST API 快速入门指南。

ASA 管理器

表 *2: ASA* 管理器

理器	说明
自适应安全设备管理器 (ASDM)	ASDM 是基于 Java 的设备上管理器，提供完整的 ASA 功能。如果您喜欢使用 GUI 胜于 CLI，并且只需管理少量 ASA，应使用 ASDM。ASDM 可以发现防火墙上的配置，因此您还可以将 CLI、CDO 或 CSM 与 ASDM 配合使用。 要开始使用 ASDM，请首先按照Firepower 4100 机箱初始配置， 第 5 页设置机箱，然后参阅使用 ASDM 部署 ASA， 第 113 页。
CLI	如果您喜欢 CLI 胜过 GUI，应使用 ASA CLI。 本指南不涵盖 CLI。有关详细信息，请参阅 ASA 配置指南。
CDO	CDO 是一个简化的、基于云的多设备管理器。由于它是简化的，因此使用 CDO 时不支持某些 ASA 功能。如果您需要一个多设备管理器来提供简化的管理体验，应使用 CDO。由于 CDO 是基于云的，因此在自己的服务器上运行 CDO 不会产生任何开销。CDO 还管理其他安全设备（例如 威胁防御），因此您可以对所有安全设备使用单一的管理器。CDO 可以发现防火墙上的配置，因此您也可以使用 CLI 或 ASDM。 本指南中不涵盖 CDO。要开始使用 CDO，请参阅 CDO 主页。
Cisco Security Manager (CSM)	CSM 是在自己的服务器硬件上运行的功能强大的多设备管理器。如果您需要管理大量的 ASA，应使用 CSM。CSM 可以发现防火墙上的配置，因此您也可以使用 CLI 或 ASDM。CSM 不支持管理 威胁防御。 本指南中不涵盖 CSM。有关详细信息，请参阅 CSM 用户指南。
ASA REST API	使用 ASA REST API 可自动化 ASA 配置。但是，API 不包括所有 ASA 功能，也不再增强。 本指南不涵盖 ASA REST API。有关详细信息，请参阅思科 ASA REST API 快速入门指南。



第 2 章

Firepower 4100 机箱初始配置

本章对您适用吗？

本章介绍如何执行 Cisco Firepower 4100 机箱的初始设置，包括配置与 ASA 和 威胁防御 逻辑设备配合使用的接口。

- 本指南适用对象， 第 5 页
- 关于 Firepower 4100 机箱， 第 6 页
- 端到端程序， 第 8 页
- 连接机箱电缆， 第 9 页
- 执行初始机箱设置， 第 12 页
- 登录机箱管理器， 第 16 页
- 配置 NTP， 第 17 页
- 添加 FXOS 用户， 第 19 页
- 配置接口， 第 20 页
- 将软件映像上传到机箱， 第 25 页
- FXOS 的历史记录， 第 27 页

本指南适用对象

本指南介绍了如何设置 Firepower 4100 机箱，使其与 ASA 和/或 威胁防御 应用程序配合使用。本指南介绍以下部署：

- 使用管理中心的独立威胁防御，用作本地或容器实例（多实例功能）
- 使用设备管理器的独立威胁防御

注释 设备管理器 不支持多实例。

- 使用CDO的独立威胁防御

注释 CDO 不支持多实例。

- 使用 ASDM 的独立式 ASA

本指南不包含以下部署，请参考 FXOS、ASA、FDM、CDO 和 FMC 配置指南了解相关内容：

- 高可用性/故障转移
- 集群（ASA，或仅使用 管理中心 的 威胁防御）
- 多实例（仅使用 管理中心 的 威胁防御）
- Radware DefensePro 修饰器应用程序
- CLI 配置（仅限 ASA 或 FXOS）

本指南还将指导您完成基本安全策略的配置；如果您有更高级的要求，请参阅配置指南。

关于 Firepower 4100 机箱

Firepower 4100 机箱是面向网络和内容安全解决方案的下一代平台。Firepower 4100 包括一个管理引擎和一个安全引擎，您可以在其中安装逻辑设备。还能安装多个高性能网络模块。

逻辑设备如何与以下产品一起使用： Firepower 4100/9300

Firepower 4100/9300 在名为 Firepower 可扩展操作系统 (FXOS) 的管理引擎上运行其操作系统。即用型 机箱管理器 提供简单的基于 GUI 的管理功能。您可以使用 机箱管理器在管理引擎上配置硬件接口设置、智能许可（适用于 ASA）和其他基本运行参数。要使用 FXOS CLI，请参阅 FXOS CLI 配置指南。

逻辑设备允许您运行一个应用实例和一个可选的修饰器应用以形成服务链。部署逻辑设备时，管理引擎将下载您选择的应用映像，并创建默认配置。然后，您可以在应用操作系统中配置安全策略。

逻辑设备不能彼此形成服务链，也不能通过背板彼此通信。所有流量必须在一个接口上退出机箱，并在另一个接口上返回以到达另一个逻辑设备。对于容器实例，可以共享数据接口；只有在这种情况下，多个逻辑设备才能通过背板进行通信。

支持的应用

您可以使用以下应用类型在机箱上部署逻辑设备。

威胁防御

威胁防御 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，以及恶意软件防护。

您可以使用以下管理器之一

- 管理中心- 位于单独服务器上的功能齐全的多设备管理器。
- 设备管理器 - 设备上的单设备管理器。
- CDO - 基于云的多设备管理器。

ASA

ASA 在一台设备中提供高级状态防火墙和 VPN 集中器功能。您可以使用以下任一管理器管理 ASA：

- ASDM - 设备上的单设备管理器。本指南介绍使用 *ASDM* 管理 *ASA* 的方法。
- CLI
- CDO - 基于云的多设备管理器。
- CSM - 位于单独服务器上的多设备管理器。

Radware DefensePro （修饰器）

您可以安装 Radware DefensePro (vDP) 以在 ASA 前面运行，或者安装 威胁防御 作为修饰器应用程序。vDP 是基于 KVM 的虚拟平台，可在 Firepower 4100/9300 上提供分布式拒绝服务 (DDoS) 检测和缓解功能。来自网络的流量必须先经过 vDP，然后才能到达 ASA 或 威胁防御。

要部署 vDP，请参阅 FXOS 配置指南。

逻辑设备应用程序实例：容器或本地

逻辑设备应用程序实例在以下部署类型中运行：

- 本地实例 - 本地实例使用安全引擎的所有资源（CPU、RAM 和磁盘空间），因此仅可安装一个本地实例。
- 容器实例 - 容器实例使用安全引擎的部分资源，因此可以安装多个容器实例。**注意**：仅 威胁防御支持多实例功能；ASA 不支持，且其不能与vDP搭配使用。

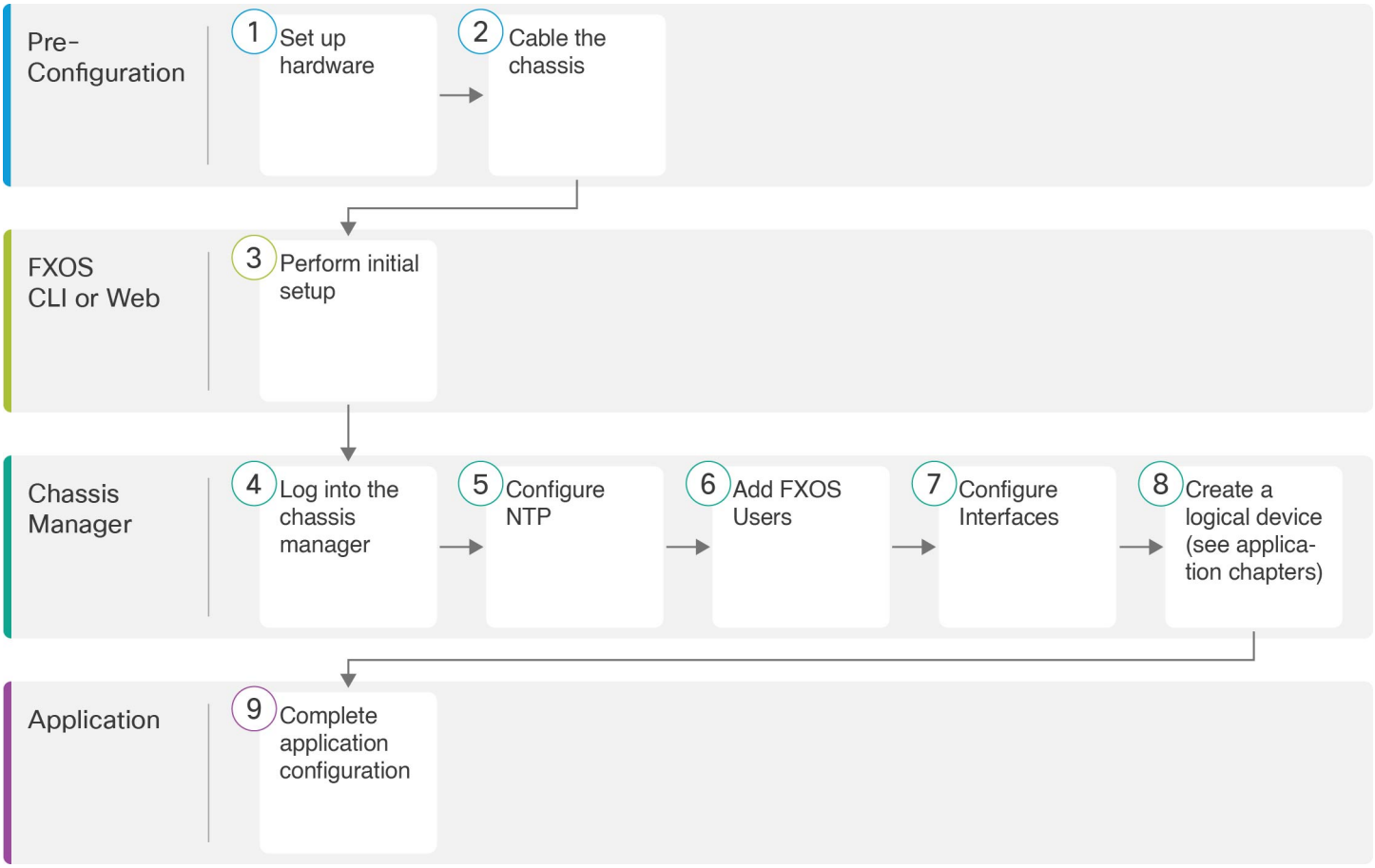
每个型号的最大容器实例数

- Firepower 4110-3
- Firepower 4112-3
- Firepower 4115-7
- Firepower 4120-3
- Firepower 4125-10
- Firepower 4140-7
- Firepower 4145—14

- Firepower 4150-7

端到端程序

请参阅以下任务以设置 Firepower 4100 机箱并在您的机箱上部署逻辑设备。



1	配置前准备工作	设置 Firepower 4100 硬件。请参阅 Firepower 4100 硬件指南。
2	配置前准备工作	连接机箱电缆， 第 9 页。
3	FXOS CLI 或 Web	执行初始机箱设置， 第 12 页。
4	机箱管理器	登录机箱管理器， 第 16 页。
5	机箱管理器	配置 NTP， 第 17 页。

6	机箱管理器	添加 FXOS 用户，第 19 页。
7	机箱管理器	配置接口，第 20 页。
8	机箱管理器	创建逻辑设备： • 具有 管理中心 的 威胁防御 — 请参阅使用管理中心部署威胁防御，第 29 页。 • 具有 设备管理器 的 威胁防御 — 请参阅使用设备管理器部署威胁防御，第 57 页。 • 具有 CDO 的 威胁防御 — 请参阅 使用 CDO 部署威胁防御，第 85 页。 • ASA - 请参阅使用 ASDM 部署 ASA，第 113 页。 注释 FXOS 2.7.1/威胁防御6.5 中，添加了对搭配使用 威胁防御 与设备管理器 的支持
9	应用	完成应用配置： • 具有 管理中心 的 威胁防御 — 请参阅使用管理中心部署威胁防御，第 29 页。 • 具有 设备管理器 的 威胁防御 — 请参阅使用设备管理器部署威胁防御，第 57 页。 • 具有 CDO 的 威胁防御 — 请参阅 使用 CDO 部署威胁防御，第 85 页。 • ASA - 请参阅使用 ASDM 部署 ASA，第 113 页。

连接机箱电缆

连接以下接口以执行机箱初始设置、持续监控以及使用逻辑设备。

- 控制台端口 -（可选）如果不在机箱管理端口上执行初始设置，请将管理计算机连接到控制台端口以执行机箱的初始设置。Firepower 4100 随附 RS-232 转 RJ-45 串行控制台电缆。可能需要使用第三方串口转 USB 电缆建立连接。
- 机箱管理端口 - 将机箱管理端口连接至您的管理网络，以进行配置和持续的机箱管理。如果从 DHCP 服务器收到 IP 地址，可以在此端口上执行初始设置。
- 逻辑设备管理接口 - 使用一个或多个接口管理逻辑设备。本指南假设您有单独的管理网络，并且有自己的互联网接入。您可以选择机箱上除预留给 FXOS 管理的机箱管理端口以外的任何接口用于此目的。可以在逻辑设备之间共享管理接口，也可以按照逻辑设备使用单独的接口，以

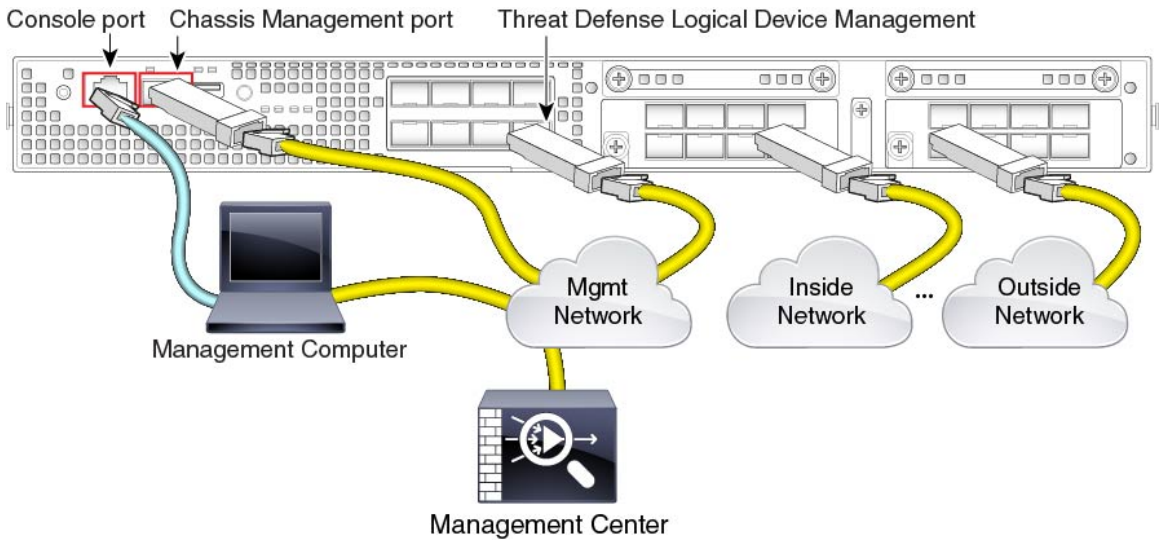
获取多实例支持。通常，您与所有逻辑设备共享一个管理接口，或者如果您使用单独的接口，请将其置于单一管理网络中。但是确切的网络要求可能有所不同。对于 威胁防御，管理接口是不同于数据接口的独立接口，具有自己的网络设置。在 6.7 和更高版本中，您可以选择为管理访问配置数据接口，而不使用管理接口。在这种情况下，您仍必须出于内部架构原因为逻辑设备分配管理接口，但无需用电缆连接它。请注意，对于 管理中心，在高可用性或集群部署中，不支持从数据接口进行管理器访问。有关详细信息，请参阅FTD 命令参考中的**configure network management-data-interface** 命令。

- 数据接口 - 将数据接口连接至您的逻辑设备数据网络。可以配置物理接口、Etherchannel、VLAN 子接口（仅适用于容器实例）和分支端口，以划分高容量接口。可以根据网络要求将多个设备连接至相同网络或不同网络，以获取多实例支持。对于容器实例，可以共享数据接口；只有在这种情况下，多个逻辑设备才能通过背板进行通信。否则，所有流量必须在一个接口上退出机箱，并在另一个接口上返回以到达另一个逻辑设备。有关共享接口限制和指导原则的详细信息，请参阅 FXOS 配置指南。

注释 除控制台端口之外的所有接口均需要 SFP/SFP+/QSFP 收发器。请参阅受支持收发器的硬件安装指南。

注释 虽然本指南中没有涉及到，但对于高可用性，请将数据接口用于故障转移/状态链路。对于机箱间集群，请将机箱上定义的 EtherChannel 用作集群类型接口。

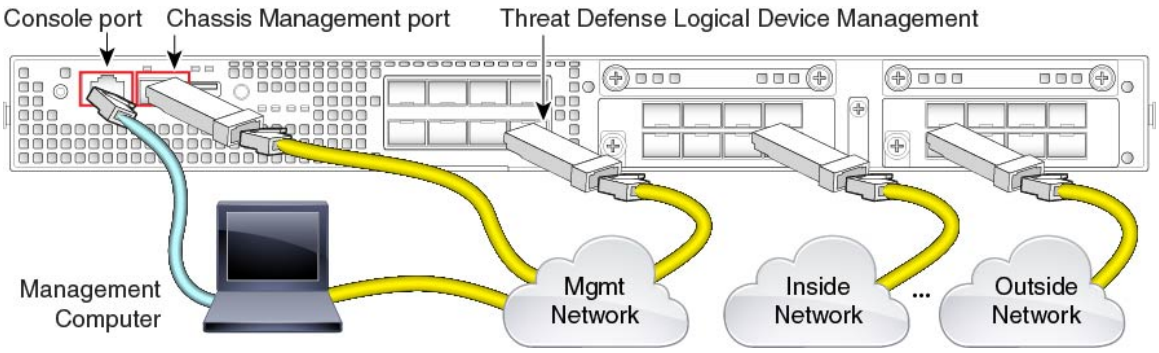
带有 管理中心 的 威胁防御 布线



本指南假设您有单独的管理网络，并且有自己的互联网接入。默认情况下，管理接口在部署时已预配置，但稍后还必须配置数据接口。

将 管理中心 置于逻辑设备管理网络，或者从逻辑设备管理网络进行访问。威胁防御 和 管理中心 必须通过管理网络访问互联网，才能进行更新和许可。在 6.7 和更高版本中，可以选择为 管理中心 管理配置数据接口，而非管理接口。请注意，在高可用性或集群部署中，不支持从数据接口进行 管理中心 访问。有关为 管理中心 访问配置数据接口的详细信息，请参阅 FTD 命令参考中的 **configure network management-data-interface** 命令。

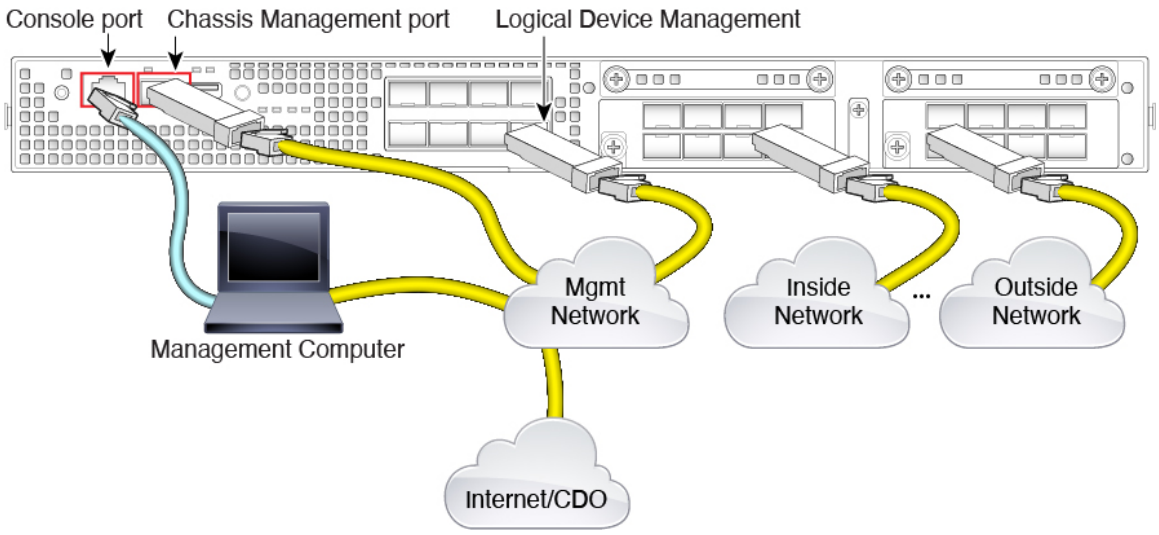
带有 设备管理器 的 威胁防御 布线



本指南假设您有单独的管理网络，并且有自己的互联网接入。默认情况下，管理接口在部署时已预配置，但稍后还必须配置数据接口。

在逻辑设备管理接口上执行初始威胁防御配置。威胁防御需连接互联网才可访问许可、更新和CDO管理，且默认行为是将管理流量路由至部署 威胁防御 时指定的网关 IP 地址。您可以稍后从任何数据接口启用 设备管理器 管理。

带有 CDO 的 威胁防御 布线

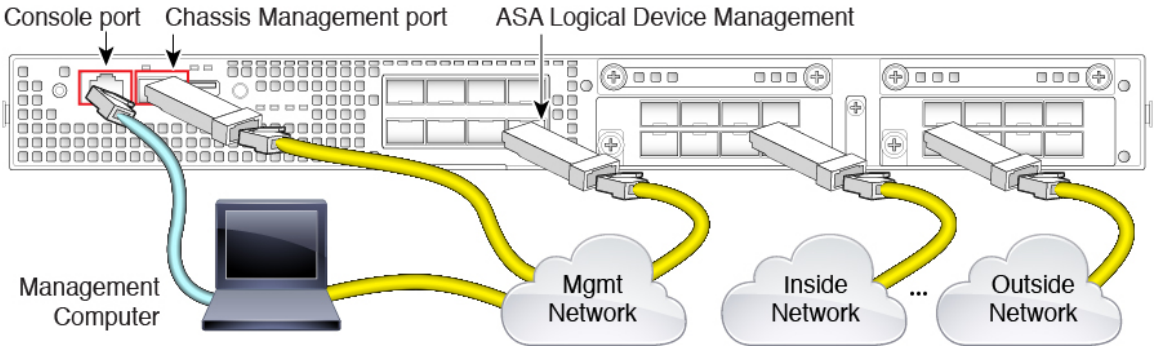


本指南假设您有单独的管理网络，并且有自己的互联网接入。默认情况下，管理接口在部署时已预配置，但稍后还必须配置数据接口。

确保可以从逻辑设备管理网络访问互联网。威胁防御 需要通过管理网络访问互联网，以进行 CDO 管理、更新和许可。您可以选择为CDO管理配置数据接口，而非管理接口。有关为管理器访问配置

数据接口的详细信息，请参阅 FTD 命令参考中的 **configure network management-data-interface** 命令。

ASA 连接



本指南假设您有一个单独的管理网络，并且有自己的互联网接入。默认情况下，管理接口在部署时已预配置，但稍后还必须配置数据接口。

在逻辑设备管理接口上执行初始 ASA 配置。可以稍后从任何数据接口启用管理。

执行初始机箱设置

在可以使用机箱管理器配置和管理系统之前，必须执行一些初始配置任务。您可以使用控制台端口上的 FXOS CLI 或与机箱管理端口的 SSH 会话，或者使用机箱管理端口上的 HTTPS，执行初始配置。

使用浏览器执行初始机箱设置

机箱管理端口使用 DHCP 获取 IP 地址。对于初始配置，您可以使用网络浏览器配置机箱的基本设置。如果没有 DHCP 服务器，则需要使用控制台端口进行初始设置。

注释 要重复初始设置，您需要在 CLI 中使用以下命令清除任何现有配置：

```
Firepower-chassis# connect local-mgmt
firepower-chassis(local-mgmt)# erase configuration
```

开始之前

收集以下信息以与设置脚本一起使用：

- 新管理员密码
- 管理 IP 地址和子网掩码

- 网关 IP 地址
- 要允许 HTTPS 和 SSH 访问的子网
- 主机名和域名
- DNS 服务器 IP 地址

过程

步骤 1 配置您的 DHCP 服务器以将 IP 地址分配到机箱管理端口。

来自机箱的 DHCP 客户端请求包含以下信息：

- 管理接口的 MAC 地址。
- DHCP 选项 60 (vendor-class-identifier) - 设置为“FPR4100”。
- DHCP 选项 61 (dhcp-client-identifier) - 设置为机箱序列号。此序列号可在机箱的拉出卡舌上找到。

步骤 2 接通机箱电源。

步骤 3 在浏览器中输入以下 URL：

https://*ip_address***/api**

指定由 DHCP 服务器分配给机箱管理端口的 IP 地址。

步骤 4 系统提示时，使用用户名 **install** 和密码 *chassis_serial_number* 登录。

chassis_serial_number 可在机箱的拉出卡舌上找到。

步骤 5 根据提示完成系统配置。

- 强密码实施策略。
- 管理员帐户的密码。
- 系统名称
- 监控程序管理端口 IPv4 地址和子网掩码，或者 IPv6 地址和前缀。
- 默认网关 IPv4 或 IPv6 地址。
- 允许使用 SSH 访问的主机/网络地址和网络掩码/前缀。
- 允许使用 HTTPS 访问的主机/网络地址和网络掩码/前缀。
- DNS 服务器 IPv4 或 IPv6 地址。
- 默认域名。

步骤 6 点击**提交**。

在 CLI 中执行初始机箱设置

当您第一次在控制台上或使用与机箱管理端口的 SSH 会话访问 FXOS CLI 时，安装向导将提示您输入基本网络配置，以便您可以从机箱管理端口访问 机箱管理器（使用 HTTPS）或 FXOS CLI（使用 SSH）。

机箱管理端口使用 DHCP 获取 IP 地址。如果没有 DHCP 服务器，则需要使用控制台端口进行初始设置。

注释 要重复初始设置，您需要使用以下命令清除任何现有配置：

```
Firepower-chassis# connect local-mgmt
firepower-chassis(local-mgmt)# erase configuration
```

开始之前

收集以下信息以与设置脚本一起使用：

- 新管理员密码
- 管理 IP 地址和子网掩码
- 网关 IP 地址
- 要从中允许 HTTPS 和 SSH 访问的子网
- 主机名和域名
- DNS 服务器 IP 地址

过程

步骤 1 接通机箱电源。

步骤 2 使用终端仿真器连接至串行控制台端口或使用 SSH 连接机箱管理端口。

Firepower 4100 随附 RS-232 转 RJ-45 串行控制台电缆。可能需要使用第三方串口转 USB 电缆建立连接。使用以下串行参数：

- 9600 波特率
- 8 个数据位
- 无奇偶校验

- 1 个停止位

步骤 3 系统提示时，使用用户名 **admin** 和密码 **cisco123** 登录。

步骤 4 根据提示完成系统配置。

示例：

```
          ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Only minimal configuration including IP connectivity to
the FXOS Supervisor is performed through these steps.

Type Ctrl-C at any time for more options or to abort configuration
and reboot system.
To back track or make modifications to already entered values,
complete input till end of section and answer no when prompted
to apply configuration.


You have chosen to setup a new Security Appliance.
      Continue? (yes/no): y

Enforce strong password? (yes/no) [y]: n

Enter the password for "admin": Farscape&32
Confirm the password for "admin": Farscape&32
Enter the system name:  firepower-4125

Supervisor Mgmt IP address : 10.80.6.12

Supervisor Mgmt IPv4 netmask : 255.255.255.0

IPv4 address of the default gateway : 10.80.6.1

The system cannot be accessed via SSH if SSH Mgmt Access is not configured.

Do you want to configure SSH Mgmt Access? (yes/no) [y]: y

SSH Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0

SSH Mgmt Access IPv4 netmask: 255.0.0.0

Firepower Chassis Manager cannot be accessed if HTTPS Mgmt Access is not configured.

Do you want to configure HTTPS Mgmt Access? (yes/no) [y]: y

HTTPS Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0

HTTPS Mgmt Access IPv4 netmask: 255.0.0.0

Configure the DNS Server IP address? (yes/no) [n]: y

  DNS IP address : 10.164.47.13

Configure the default domain name? (yes/no) [n]: y

  Default domain name : cisco.com

Following configurations will be applied:
```

```
    Switch Fabric=A
    System Name=firepower-4125
    Enforced Strong Password=no
    Supervisor Mgmt IP Address=10.89.5.14
    Supervisor Mgmt IP Netmask=255.255.255.192
    Default Gateway=10.89.5.1
    SSH Access Configured=yes
        SSH IP Address=10.0.0.0
        SSH IP Netmask=255.0.0.0
    HTTPS Access Configured=yes
        HTTPS IP Address=10.0.0.0
        HTTPS IP Netmask=255.0.0.0
    DNS Server=72.163.47.11
    Domain Name=cisco.com

  Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): y
  Applying configuration. Please wait...  Configuration file - Ok
.....

Cisco FPR Series Security Appliance
firepower-9300 login:  admin
Password: Farscape&32
Successful login attempts for user 'admin' : 1
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2019, Cisco Systems, Inc. All rights reserved.

[...]

firepower-chassis#
```

步骤 5 您可以从控制台端口断开连接（如果已使用）或结束 SSH 会话。

登录机箱管理器

使用 机箱管理器 配置机箱设置，包括启用接口和部署逻辑设备。

开始之前

- 有关受支持的浏览器的信息，请参阅您使用的版本的发行说明（请参阅 http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.html）。
- 您只能从 IP 地址在初始机箱设置期间指定的范围内的管理计算机访问机箱管理器。

过程

步骤 1 使用支持的浏览器输入以下 URL。

https://*chassis_mgmt_ip_address*

- *chassis_mgmt_ip_address* - 标识在初始配置期间输入的机箱管理端口的 IP 地址或主机名。

步骤 2 输入用户名 **admin** 和新密码。

您可以在以后根据添加 FXOS 用户，第 19 页添加更多用户。

步骤 3 点击 **Login**。
您将登录，机箱管理器将打开以显示**概述**页面。

配置 NTP

尽管可以手动设置时间，但我们建议使用 NTP 服务器。对于 ASA 以及采用 设备管理器 的 威胁防御来说，需要正确的智能软件许可时间。对于采用 管理中心 的 威胁防御，机箱与 管理中心 之间的时间必须匹配。这种情况下，我们建议您在机箱上使用与 管理中心 相同的 NTP 服务器。请勿将 管理中心 自身用作 NTP 服务器；此方法不受支持。

开始之前

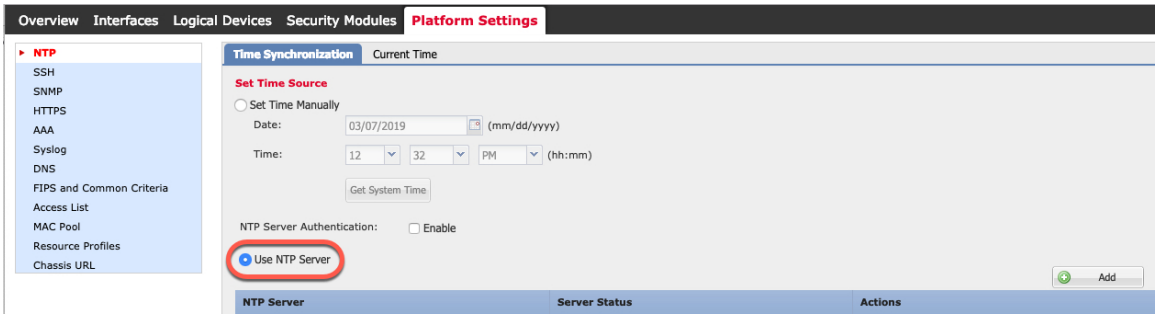
如果您要将主机名用于 NTP 服务器，则必须配置 DNS 服务器（如果尚未在初始设置中执行此操作）。请参阅**平台设置** > **DNS**。

过程

步骤 1 选择**平台设置 (Platform Settings)** > **NTP**。

默认情况下，系统会选择**时间同步**选项卡。

步骤 2 点击**使用 NTP 服务器 (Use NTP Server)** 单选按钮。

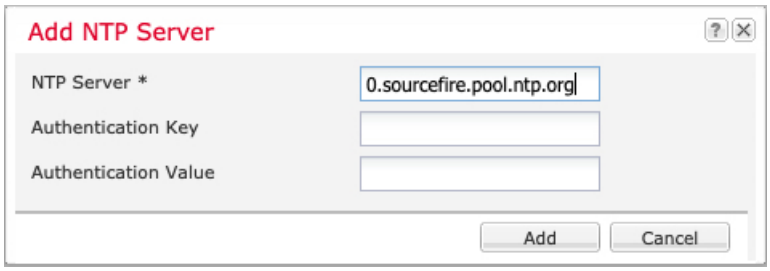


步骤 3 （可选） 如果需要对 NTP 服务器进行身份验证，请选中 **NTP 服务器身份验证: 启用**复选框。

系统将提示您启用 NTP 验证。点击**是**将要求所有 NTP 服务器条目的验证密钥 ID 和值。

仅支持使用 SHA1 进行 NTP 服务器身份验证。

步骤 4 点击**添加**，然后设置以下参数：



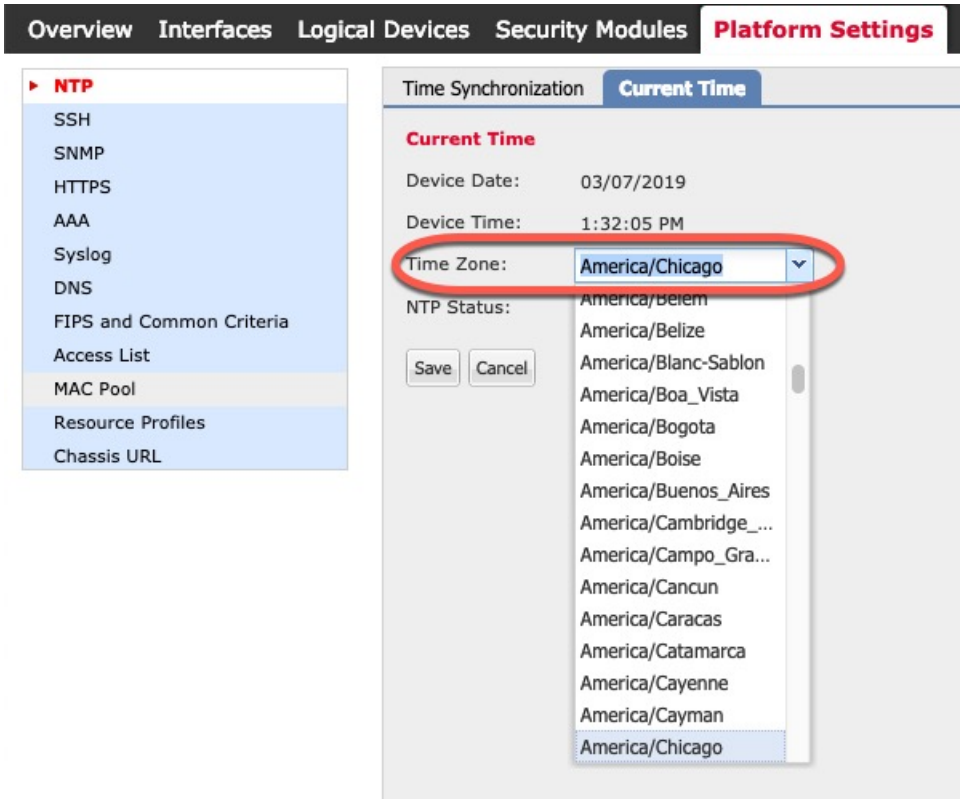
- **NTP 服务器** - NTP 服务的 IP 地址或主机名。
- **验证密钥**和**验证值** - 从 NTP 服务器获取密钥 ID 和值。例如，要在安装了 OpenSSL 的 NTP 服务器 4.2.8p8 版或更高版本上生成 SHA1 密钥，请输入 **ntp-keygen -M** 命令，然后在 ntp.keys 文件中查看密钥 ID 和值。密钥用于告知客户端和服务器在计算消息摘要时要使用哪个值。

步骤 5 点击**添加**以添加服务器。

最多可以添加 4 个 NTP 服务器。

步骤 6 点击**保存**以保存服务器。

步骤 7 从**时区**下拉列表中选择**当前时间**，然后为机箱选择适当的时区。



步骤 8 点击**保存 (Save)**。

注释　　如果系统时间修改超过10分钟，系统会将您注销，稍后，您需要再次登录机箱管理器。

添加 FXOS 用户

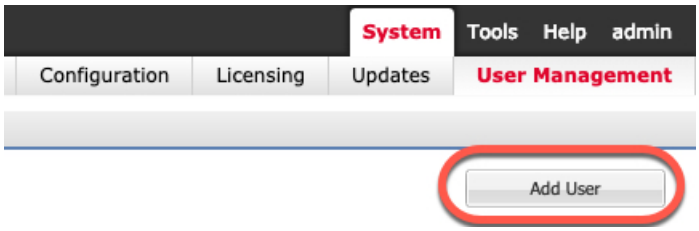
为机箱管理器和 FXOS CLI 登录添加本地用户。

过程

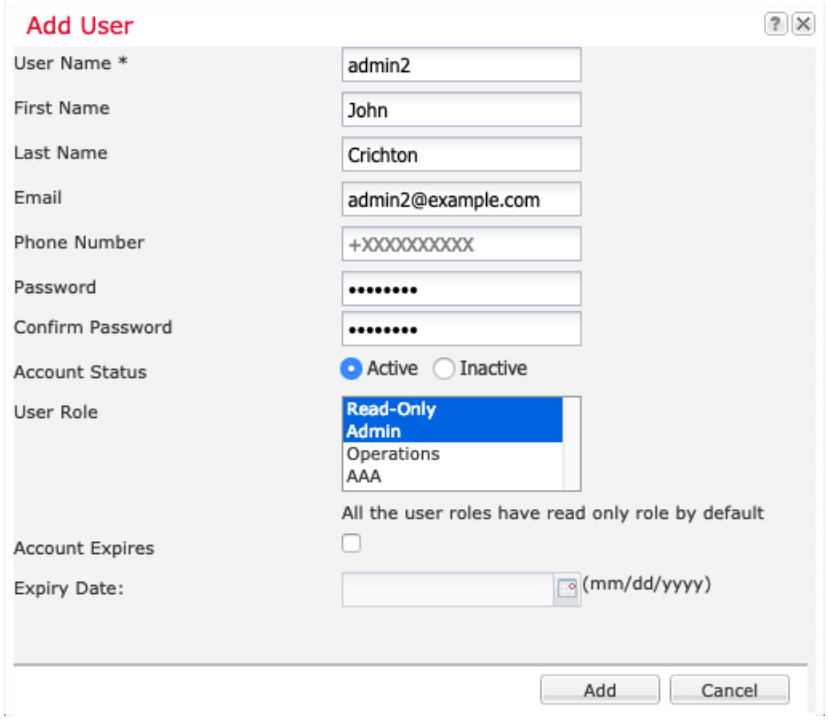
步骤 1 依次选择 **System** > **User Management**。

步骤 2 点击**本地用户**。

步骤 3 点击**添加用户 (Add User)**，可打开**添加用户 (Add User)** 对话框。



步骤 4 使用关于用户的必填信息，填写下列字段：



- **用户名** - 设置用户名，最多 32 个字符。保存用户后，不能更改登录 ID。必须删除该用户帐户，创建新的用户帐户。
- （可选）**名字** - 设置用户的名字，最多 32 个字符。
- （可选）**姓氏** - 设置用户的姓氏，最多 32 个字符。
- （可选）**电子邮箱** - 设置用户的电子邮件地址。
- （可选）**电话号码** - 设置用户的电话号码。
- **密码**和**确认密码** - 设置与此帐户关联的密码。如果启用了密码强度检查，则密码必须为强密码，FXOS 会拒绝任何不满足强度检查要求的密码。有关强密码指导原则，请参阅 FXOS 配置指南。
- **帐户状态** - 将状态设置为**活动**或**非活动**。
- **用户角色** - 设置表示要分配给用户帐户的权限的角色。系统会默认为所有用户分配**只读**角色，并且此角色无法取消选择。要分配不同的角色，请在窗口中点击角色名称以使其突出显示。您可以使用以下用户角色之一：
  - **管理员** - 完成对整个系统的读写访问。
  - **只读** - 对系统配置进行只读访问，但无权修改系统状态。
  - **操作** - 对 NTP 配置、用于智能许可的 Smart Call Home 配置和系统日志（包括系统日志服务器和故障）进行读写访问。对系统其余部分的读取访问。
  - **AAA 管理员** - 对用户、角色和 AAA 配置的读写访问。对系统其余部分的读取访问。
- （可选）**帐户到期** - 设置帐户到期。在**到期日期**字段中指定的日期过后，无法使用帐户。在为用户帐户配置过期日期后，无法将帐户重新配置为不过期。然而，您可以为帐户配置可用的最新过期日期。默认情况下，用户帐户不会到期。
- （可选）**到期日期** - 帐户到期的日期。日期格式应为 *yyyy-mm-dd*。点击此字段末尾的日历图标，查看您可以用来选择到期日期的日历。

步骤 5 点击**添加**。

配置接口

默认情况下，物理接口处于禁用状态。在 FXOS 中，您可以启用接口、添加以太网通道、添加 VLAN 子接口和编辑接口属性。要使用某一接口，必须在 FXOS 中以物理方式启用它，并在应用中以逻辑方式启用它。

要配置分支端口，请参阅 FXOS 配置指南。

接口类型

每个接口为以下类型之一：

- 数据 - 用于常规数据。不能在逻辑设备之间共享数据接口，且逻辑设备无法通过背板与其他逻辑设备通信。对于数据接口上的流量，所有流量必须在一个接口上退出机箱，并在另一个接口上返回以到达另一个逻辑设备。
- 数据共享 - 用于常规数据。仅容器实例支持这些数据接口，可由一个或多个逻辑设备/容器实例（仅限威胁防御-使用-管理中心 ）共享。 每个容器实例都可通过背板与共享此接口的所有其他实例通信。共享的接口可能会影响您可以部署容器实例的数量。共享接口不支持用于网桥组成员接口（在透明模式或路由模式下）、内联集、被动接口、集群或故障切换链路。
- 管理 - 用于管理应用程序实例。这些接口可以由一个或多个逻辑设备共享，以访问外部主机；逻辑设备无法通过此接口与共享接口的其他逻辑设备通信。只能为每个逻辑设备分配一个管理接口。根据您的应用和管理器，您可以稍后从数据接口启用管理；但必须将管理接口分配给逻辑设备，即使您不打算在启用数据管理后使用该接口。

注释 管理接口更改会导致逻辑设备重新启动，例如将管理接口从 e1/1 更改为 e1/2 会导致逻辑设备重新启动以应用新的管理接口。

- 事件 - 用作 威胁防御-using-管理中心 设备的辅助管理接口。 要使用此接口，您必须在 威胁防御 CLI 上配置其 IP 地址和其他参数。例如，您可以将管理流量从活动（例如网络活动）中分隔出来。有关详细信息，请参阅《管理中心配置指南》。事件接口可以由一个或多个逻辑设备共享，以访问外部主机；逻辑设备无法通过此接口与共享接口的其他逻辑设备通信。 如果稍后为管理配置数据接口，则无法使用单独的事件接口。

注释 安装每个应用实例时，会分配一个虚拟以太网接口。如果应用不使用事件接口，则虚拟接口将处于管理员关闭状态。

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- 集群 - 用作集群逻辑设备的集群控制链路。默认情况下，系统会在端口通道 48 上自动创建集群控制链路。“集群”类型仅在 EtherChannel 接口上受支持。 对于多实例集群，无法在设备之间共享集群类型接口。您可以将 VLAN 子接口添加到集群 EtherChannel，以便为每个集群提供单独的集群控制链路。如果向某个集群接口添加子接口，则不能将该接口用于本地集群。设备管理器 和 CDO 不支持集群。

在部署逻辑设备之前，必须配置管理接口和至少一个数据（或数据共享）接口。

配置物理接口

您可以通过物理方式启用和禁用接口，并设置接口速度和双工。要使用某一接口，必须在 FXOS 中以物理方式启用它，并在应用中以逻辑方式启用它。

开始之前

不能单独修改已经是 EtherChannel 成员的接口。务必在将接口添加到 EtherChannel 之前为其配置设置。

过程

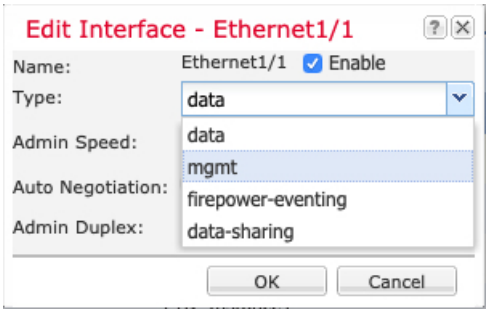
步骤 1 点击 **Interfaces**。

所有接口页面顶部显示当前已安装的接口的直观展示图，在下表中提供已安装接口列表。

步骤 2 点击要编辑的接口的 **编辑**（ ） 以打开**编辑接口**对话框。

步骤 3 选中**启用**复选框。

步骤 4 选择接口**类型**：**数据**、**数据共享**、**管理**或 **Firepower 事件**



注释 使用数据共享型接口时有一些限制；有关详细信息，请参阅 FXOS 配置指南。

对于 Firepower 事件，请参阅《Firepower 管理中心配置指南》。

步骤 5 （可选） 选择接口的**速度**。

步骤 6 （可选） 如果您的接口支持**自动协商**，请点击**是**或**否**单选按钮。

步骤 7 （可选） 选择接口的**双工**。

步骤 8 点击**确定**。

添加 EtherChannel（端口通道）

EtherChannel（也称为端口通道）最多可以包含 16 个同一介质类型和容量的成员接口，并且必须设置为相同的速度和双工模式。介质类型可以是 RJ-45 或 SFP；可以混合使用不同类型（铜缆和光纤）的 SFP。不能通过在大容量接口上将速度设置为较低值来混合接口容量（例如 1GB 和 10GB 接口）。

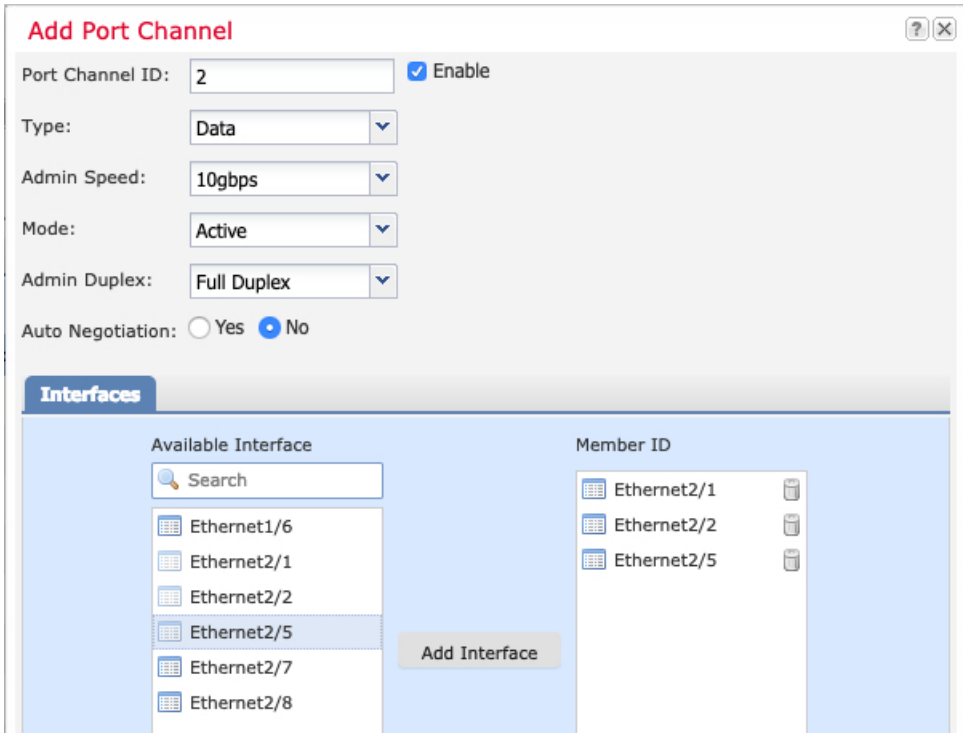
注释 机箱创建 EtherChannel 时，EtherChannel 将处于**挂起**状态（对于主动 LACP 模式）或**关闭**状态（对于打开 LACP 模式），直到将其分配给逻辑设备，即使物理链路是连通的。

过程

步骤 1 点击 **Interfaces**。

所有接口页面顶部显示当前已安装的接口的直观展示图，在下表中提供已安装接口列表。

步骤 2 点击**新增** > **端口通道**。



步骤 3 输入一个介于 1 和 47 之间的**端口通道 ID**。

步骤 4 选中**启用**复选框。

步骤 5 选择**接口类型**：

- **数据**
- **数据共享** - 仅用于容器实例。
- **管理**
- **Firepower 事件** - 仅用于 威胁防御 。
- **Cluster** - 仅用于集群。

注释　使用数据共享型接口时有一些限制；有关详细信息，请参阅 FXOS 配置指南。

对于 Firepower 事件，请参阅《Firepower 管理中心配置指南》。

步骤 6　从下拉列表设置成员接口的**管理速度**。

步骤 7　对于数据或数据共享接口，选择 LACP 端口通道**模式**：**主用**或**保持**。

对于非数据或数据共享接口，模式始终是主用模式。除非您需要最大限度地减少 LACP 流量，否则应使用主用模式。

步骤 8　从下拉列表中选择**管理双工**。

步骤 9　要将某个接口添加到端口通道，请在**可用接口**列表中选择接口，然后点击**添加接口**以将其移至**成员 ID** 列表。

最多可以添加 16 个接口。

提示　一次可添加多个接口。在按住 **Ctrl** 键的同时点击所需接口。要选择一个接口范围，请选择范围中的第一个接口，然后，在按住 **Shift** 键的同时，点击选择范围中的最后一个接口。

步骤 10　要从端口通道删除接口，请点击**成员 ID** 列表中接口右侧的 **删除**（ ）。

步骤 11　点击**确定**。

为容器实例添加 VLAN 子接口

您最多可以将 500 个子接口连接到您的机箱。仅容器实例支持子接口；有关详细信息，请参阅逻辑设备应用程序实例：容器或本地，第 7 页。

对于多实例集群，只能将子接口添加到集群类型接口；不支持数据接口上的子接口。

每个接口的 VLAN ID 都必须具有唯一性，并且在容器实例内，VLAN ID 在所有已分配接口上也必须具有唯一性。只要系统将 VLAN ID 分配至不同的容器实例，您就可以在单独接口上重新使用它们。然而，即使每个子接口使用相同的 ID，这些子接口仍将计入限值。

您还可以在应用内添加子接口。有关何时使用 FXOS 子接口与应用子接口的详细信息，请参阅 FXOS 配置指南。

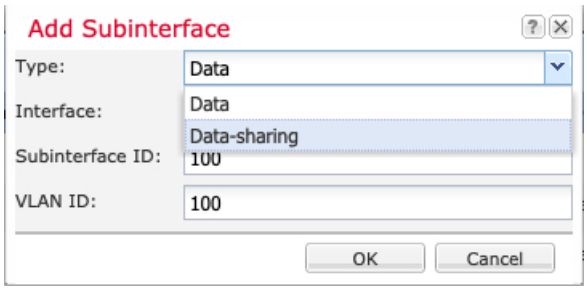
过程

步骤 1　点击 **Interfaces**。

所有接口页面顶部显示当前已安装的接口的直观展示图，在下表中提供已安装接口列表。

步骤 2　点击**添加新** > **子接口**打开**添加子接口**对话框。

步骤 3　选择接口**类型**：



- **数据**
- **数据共享**
- **集群** - 如果向某个集群接口添加子接口，则不能将此接口用于本地集群。

对于数据和数据共享接口：此类型独立于父接口类型；例如，您可以设数据共享父接口和数据子接口。

使用数据共享型接口时有一些限制；有关详细信息，请参阅 FXOS 配置指南。

步骤 4 从下拉列表选择父**接口**。

不得将子接口添加到当前已分配至逻辑设备的物理接口。如果系统已分配父接口的其他子接口，只要未分配此父接口，您就可以添加新的子接口。

步骤 5 输入一个介于 1 和 4294967295 之间的**子接口 ID**。

此 ID 将附加到父接口 ID，作为 *interface_id.subinterface_id*。例如，如果您将子接口添加到 ID 为 100 的以太网接口 1/1，则子接口 ID 将为：以太网接口 1/1.100。尽管可以出于方便目的将此 ID 和 VLAN ID 设置为相互匹配，但两者始终不同。

步骤 6 设置介于 1 和 4095 之间的 **VLAN ID** 。

步骤 7 点击**确定 (OK)**。

展开父接口查看其项下所有子接口。

将软件映像上传到机箱

此程序介绍如何上传新的 FXOS 和应用程序映像，以及如何升级 FXOS 映像。如果预先安装的映像不是所需的版本，可能需要上传新的映像。

开始之前

- 查看 FXOS 兼容性指南，了解 FXOS、ASA 和 威胁防御 版本之间的兼容性。
- 确保您要上传的映像在本地计算机上可用。要获取 Firepower 4100 的 FXOS 和应用程序软件，请参阅：

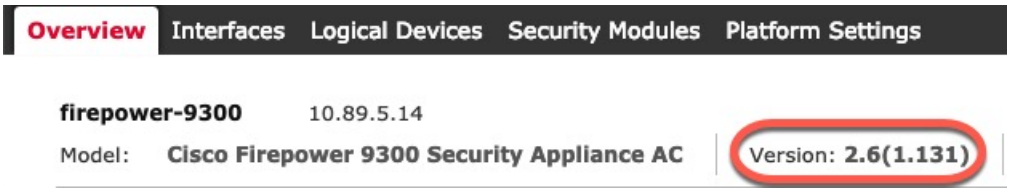
http://www.cisco.com/go/firepower4100-software

- 要确保在 HTTPS 会话期间上传成功，您可能需要在 FXOS CLI 上更改绝对超时。绝对超时为 60 分钟（最大值）；如果上传的内容较大，可能需要超过 60 分钟的时间。要禁用绝对超时，请输入：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope default-auth
Firepower-chassis /security/default-auth # set absolute-session-timeout 0
Firepower-chassis /security/default-auth* # commit-buffer
```

过程

步骤 1 查看**概述**页面，检查您当前的 FXOS 版本。



您可以在下一步中查看机箱上当前可用的应用程序映像。

步骤 2 依次选择**系统 (System)** > **更新 (Updates)**。

可用更新页面显示 FXOS 平台捆绑包映像和应用映像列表。

步骤 3 点击**上传映像**以打开**上传映像**对话框。

步骤 4 点击**浏览 (Browse)**，可导航到并选择想要上传的映像。

步骤 5 点击**上传**。所选映像将上传到机箱。

上传映像对话框会显示一个进度条，映像上传完成时会显示**成功**对话框。

步骤 6 要升级 FXOS 映像：

a) 点击想要升级到的 FXOS 平台捆绑包所对应的 升级图标（）。

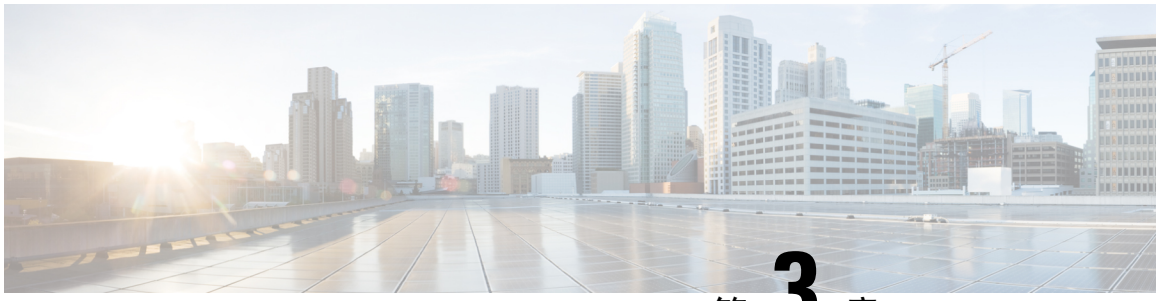
b) 点击**是**以确认要继续安装。

机箱会重新加载。升级过程通常需要 20 到 30 分钟。

FXOS 的历史记录

功能名称	版本	功能信息
用于容器实例的VLAN子接口	2.4.1	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。 注释 要求使用 6.3 或更高版本的 威胁防御。 新增/修改的菜单项： **接口 (Interfaces)** > **所有接口 (All Interfaces)** > **新增 (Add New)**下拉菜单 > **子接口 (Subinterface)** 新增/修改的 管理中心菜单项： **设备** > **设备管理** > **编辑** 图标> **接口**
用于容器实例的数据共享接口	2.4.1	要确保灵活使用物理接口，可以在多个实例之间共享接口。 注释 要求使用 6.3 或更高版本的 威胁防御。 新增/修改的菜单项： **接口** > **所有接口** > **类型**
支持保存模式下的数据Etherchannel	2.4.1	现在可以将数据和数据共享 Etherchannel 设置为“主用”LACP 模式或“保持”模式。其他类型 Etherchannel 仅支持“主用”模式。 新增/修改的菜单项： **接口** > **所有接口** > **编辑端口通道** > **模式**
支持 威胁防御 内联集中的 Etherchannel	2.1.1	现在可以使用 威胁防御 内联集中的 EtherChannel。
威胁防御 支持的内联集链路状态传播	2.0.1	当您在 威胁防御 应用中配置内联集并启用链路状态传播时，威胁防御 会向 FXOS 机箱发送内联集成员身份。链路状态传播意味着，当内联集的一个接口断开时，机箱将自动关闭内联接口对的第二个接口。 新增/修改的命令：**show fault |grep link-down**, **show interface detail**
威胁防御 支持的硬件绕行网络模块	2.0.1	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。 新增/修改的 管理中心菜单项： **设备** > **设备管理** > **接口** > **编辑物理接口**

功能名称	版本	功能信息
用于 威胁防御 的 Firepower事件类型接口	1.1.4	可以将接口指定为用于 威胁防御 的 Firepower 事件接口。此接口是 威胁防御 设备的辅助管理接口。要使用此接口，您必须在 威胁防御 CLI 上配置其 IP 地址和其他参数。例如，您可以将管理流量从活动（例如网络活动）中分隔出来。请参阅《管理中心配置指南》“系统配置”一章中的“管理接口”部分。 新增/修改的 机箱管理器菜单项： **接口 > 所有接口 > 类型**



第 3 章

使用管理中心部署威胁防御

本章对您适用吗？

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

在大型网络的典型部署中，要在网段上安装多个托管设备。每个设备控制、检查、监控和分析流量，然后向管理 管理中心 报告。管理中心 通过一个 Web 界面提供集中管理控制台，可在运行中用来执行管理、分析和报告任务，以保护您的本地网络。

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

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

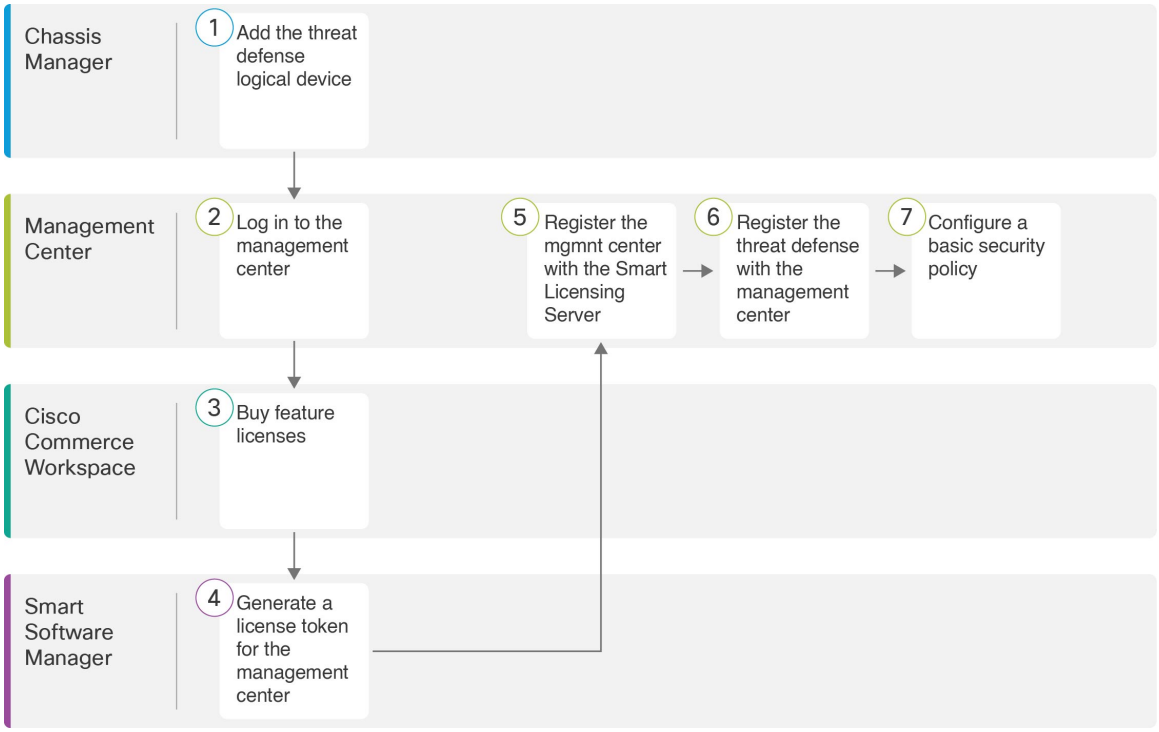
- 开始之前， 第 29 页
- 端到端程序， 第 30 页
- 机箱管理器：添加威胁防御逻辑设备， 第 31 页
- 登录管理中心， 第 35 页
- 获取管理中心的许可证， 第 36 页
- 向管理中心注册威胁防御， 第 38 页
- 配置基本安全策略， 第 41 页
- 访问威胁防御 CLI， 第 53 页
- 后续步骤, on page 55
- 使用管理中心的威胁防御历史记录， 第 55 页

开始之前

部署并执行 管理中心的初始配置。请参阅《思科 Firepower 管理中心 1600、2600 和 4600 硬件安装指南》或Cisco Secure Firewall Management Center Virtual 快速入门指南。

端到端程序

请参阅以下任务以在机箱上部署和配置 威胁防御。



	工作空间	步骤
1	机箱管理器	机箱管理器：添加威胁防御逻辑设备， 第 31 页。
2	管理中心	登录管理中心， 第 35 页。
3	Cisco Commerce Workspace	获取管理中心的许可证， 第 36 页：购买功能许可证。
4	智能软件管理器	获取管理中心的许可证， 第 36 页：为 管理中心 生成许可证令牌。
5	管理中心	获取管理中心的许可证， 第 36 页：向智能许可证服务器注册管理中心。
6	管理中心	向管理中心注册威胁防御， 第 38 页。
7	管理中心	配置基本安全策略， 第 41 页。

机箱管理器：添加威胁防御逻辑设备

您可以从 Firepower 4100将 威胁防御 部署为本地实例或容器实例。您可以为每个安全引擎安全引擎部署多个容器实例，但只能部署一个本机实例。有关每个型号的最大容器实例数，请参阅逻辑设备应用程序实例：容器或本地，第 7 页。

要添加高可用性对或集群，请参阅《Firepower 管理中心配置指南》。

您可以通过此程序配置逻辑设备特性，包括应用程序使用的引导程序配置。

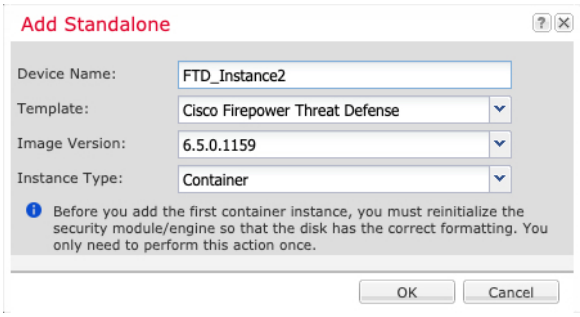
开始之前

- 配置与 威胁防御一起使用的管理接口；请参阅配置接口，第 20 页。管理接口是必需的。在 6.7 和更高版本中，您可以稍后从数据接口启用管理；但必须将管理接口分配给逻辑设备，即使您不打算在启用数据管理后使用该接口。请注意，此管理接口与仅用于机箱管理的机箱管理端口（并且该端口在**接口**选项卡的顶部显示为 **MGMT**）不同。
- 您还必须至少配置一个数据接口。
- 对于容器实例，如果您不想采用使用最少资源的默认配置文件，请在**平台设置** > **资源配置文件**上添加资源配置文件。
- 对于容器实例，在您第一次安装容器实例之前，可能需要重新初始化安全引擎，以保证磁盘具有正确的格式。如果必须完成此操作，您将无法保存逻辑设备。点击**安全引擎**，然后点击重新初始化图标（）。
- 收集以下信息：
  - 此设备的接口 ID
  - 管理接口 IP 地址和网络掩码
  - 网关 IP 地址
  - 您选择的管理中心 IP 地址和/或 NAT ID
  - DNS 服务器 IP 地址

过程

步骤 1 在 机箱管理器中，选择**逻辑设备**。

步骤 2 点击**添加** > **独立设备**，并设置以下参数：



a) 提供**设备名称**。

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

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

c) 选择**映像版本**。

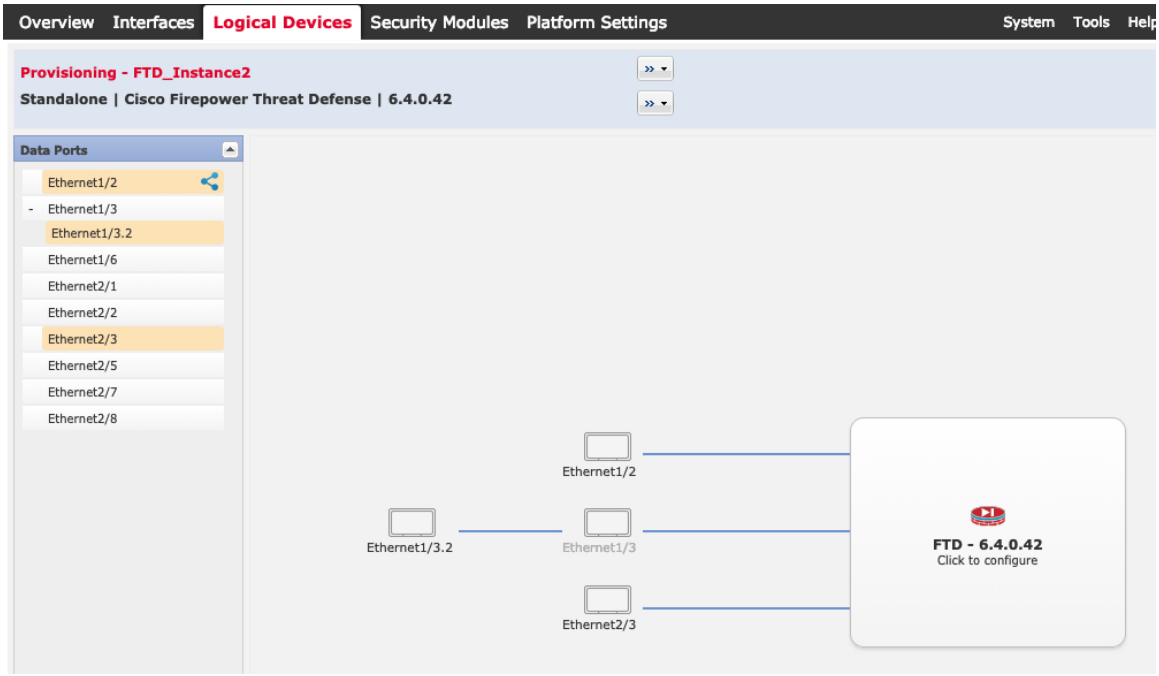
d) 选择**实例类型：容器**或**本地**。

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

e) 点击**确定 (OK)**。

屏幕会显示调配 - 设备名称窗口。

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



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

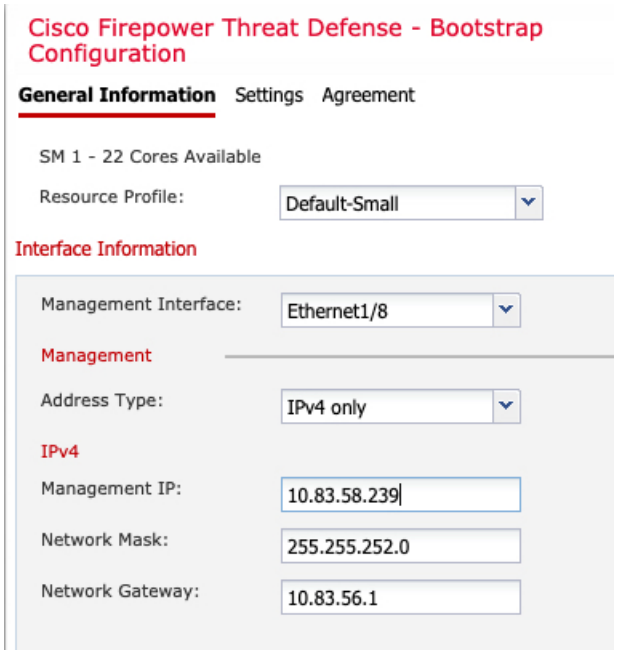
仅可向一个容器实例分配最多 10 个数据共享接口。此外，可以将每个数据共享接口分配至最多 14 个容器实例。数据共享接口以共享图标（）表示。

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

步骤 4 点击屏幕中心的设备图标。

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

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



a) 对于容器实例，指定**资源配置文件**。

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

b) 选择**管理接口**。

此接口用于管理逻辑设备。此接口独立于机箱管理端口。

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

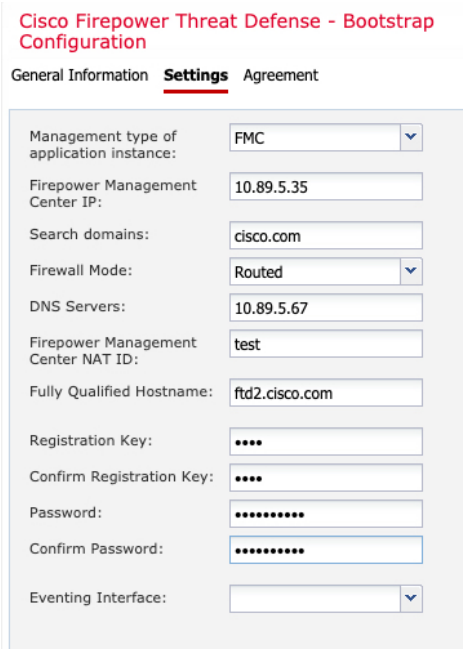
d) 配置**管理 IP** 地址。

设置用于此接口的唯一 IP 地址。

e) 输入**网络掩码**或**前缀长度**。

f) 输入**网络网关**地址。

步骤 6 在**设置**选项卡上，完成下列操作：



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

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

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

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

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

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

d) 输入逗号分隔列表形式的**搜索域**。

e) 选择**防火墙模式：透明**或**路由式**。

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

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

f) 输入逗号分隔列表形式的 **DNS 服务器**。

例如，如果指定 管理中心 主机名，则 威胁防御 使用 DNS。

g) 输入 威胁防御 的**完全限定主机名**。

h) 输入注册期间要在管理中心和设备之间共享的**注册密钥**。

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

i) 输入供威胁防御管理员用户用于 CLI 访问的**密码**。

j) 选择应该发送事件的**事件接口**。如果未指定，系统将使用管理接口。

此接口必须定义为 Firepower 事件接口。

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

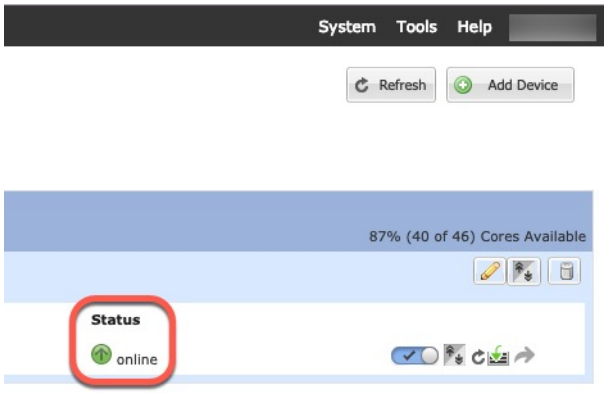
此设置在硬件中启用 TLS 加密加速，并提高某些类型流量的性能。有关详细信息，请参阅《Firepower 管理中心配置指南》。本地实例不支持此功能。要查看分配给该实例的硬件加密资源百分比，请输入 **show hw-crypto** 命令。

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

步骤 8 点击**确定 (OK)** 关闭配置对话框。

步骤 9 点击**保存 (Save)**。

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



登录管理中心

使用 管理中心配置并监控 威胁防御。

开始之前

有关受支持浏览器的信息，请参阅您所用版本的发行说明（参阅https://www.cisco.com/go/firepower-notes）。

过程

步骤 1 使用支持的浏览器输入以下 URL。

https://*fmc_ip_address*

步骤 2 输入您的用户名和密码。

步骤 3 点击**登录**。

获取管理中心的许可证

所有许可证都由 管理中心提供给 威胁防御。您可以购买下列许可证：

- **IPS**胁-安全情报和下一代 IPS
- **恶意软件 防御**-恶意软件 防御
- **URL** - URL 过滤
- **Cisco Secure 客户端**-Secure Client Advantage、Secure Client Premier 或 Secure Client VPN Only
- **运营商** - Diameter、GTP/GPRS、M3UA、SCTP

有关思科许可的更详细概述，请访问 cisco.com/go/licensingguide

开始之前

- 拥有 智能软件管理器主帐户。

  如果您还没有帐户，请点击此链接以设置新帐户。通过智能软件管理器，您可以为组织创建一个主帐户。

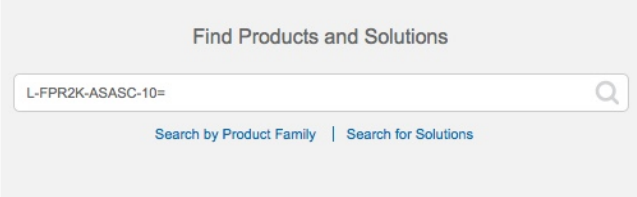
- 您的智能软件许可帐户必须符合强加密 (3DES/AES) 许可证的要求，才能使用某些功能（已使用导出合规性标志启用）。

过程

步骤 1 请确保智能许可帐户包含所需的可用许可证。

当您从思科或经销商那里购买设备时，您的许可证应该已链接到您的智能软件许可证帐户。但是，如果您需要自己添加许可证，则请使用Cisco Commerce Workspace上的 **Find Products and Solutions** 搜索字段。搜索以下许可证 PID：

图 *1:* 许可证搜索



注释　　如果未找到 PID，您可以手动将 PID 添加到订单中。

- IPS、恶意软件 防御和 URL 许可证组合：
  - L-FPR4112T-TMC=
  - L-FPR4115T-TMC=
  - L-FPR4125T-TMC=
  - L-FPR4145T-TMC=

  当您将上述 PID 之一添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：
  - L-FPR4112T-TMC-1Y
  - L-FPR4112T-TMC-3Y
  - L-FPR4112T-TMC-5Y
  - L-FPR4115T-TMC-1Y
  - L-FPR4115T-TMC-3Y
  - L-FPR4115T-TMC-5Y
  - L-FPR4125T-TMC-1Y
  - L-FPR4125T-TMC-3Y
  - L-FPR4125T-TMC-5Y
  - L-FPR4145T-TMC-1Y
  - L-FPR4145T-TMC-3Y
  - L-FPR4145T-TMC-5Y
- Cisco Secure 客户端-请参阅 思科安全客户端订购指南。
- 运营商许可证：
  - L-FPR4K-FTD-CAR=

步骤 2　如果尚未执行此操作，请向智能许可服务器注册管理中心。

注册需要您在智能软件管理器中生成注册令牌。有关详细说明，请参阅 《Cisco Secure Firewall Management Center 管理指南》 。

向管理中心注册威胁防御

将每个逻辑设备分别注册到同一个 管理中心。

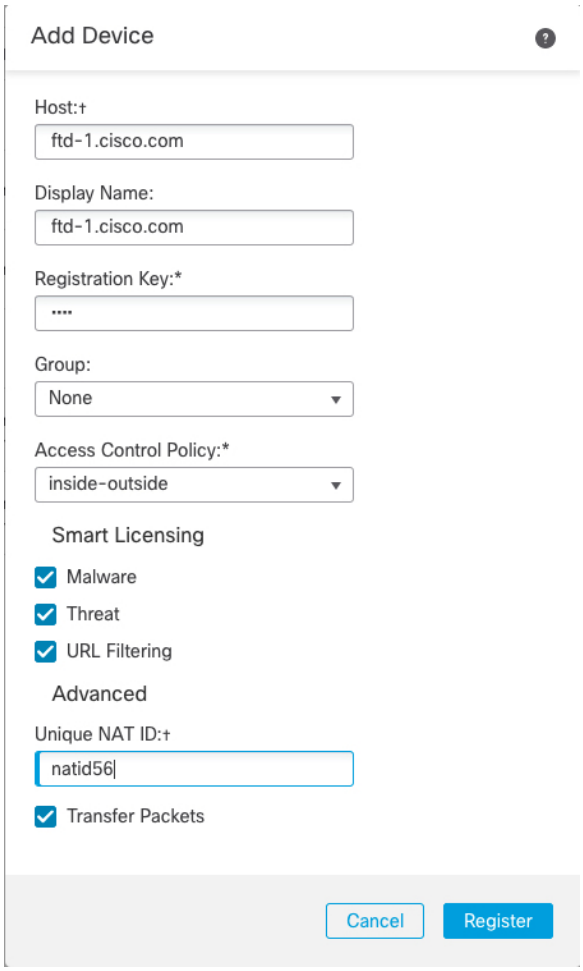
开始之前

- 确保 机箱管理器 **逻辑设备 (Logical Devices)**页面上 威胁防御 逻辑设备的**状态 (Status)** 为**在线 (online)**。
- 收集您在 威胁防御 初始引导程序配置中设置的以下信息（请参阅机箱管理器：添加威胁防御逻辑设备，第 31 页）；
  - 威胁防御管理 IP 地址或主机名，以及 NAT ID
  - 管理中心注册密钥
- 在 6.7 和更高版本中，如果要使用数据接口进行管理，请在 威胁防御 CLI 上使用 **configure network management-data-interface** 命令。有关详细信息，请参阅 Cisco Secure Firewall Threat Defense 命令参考。

过程

步骤 1 在 管理中心 上，选择**设备 (Devices)** > **设备管理 (Device Management)**。

步骤 2 从**添加**下拉列表中，选择**添加设备**。



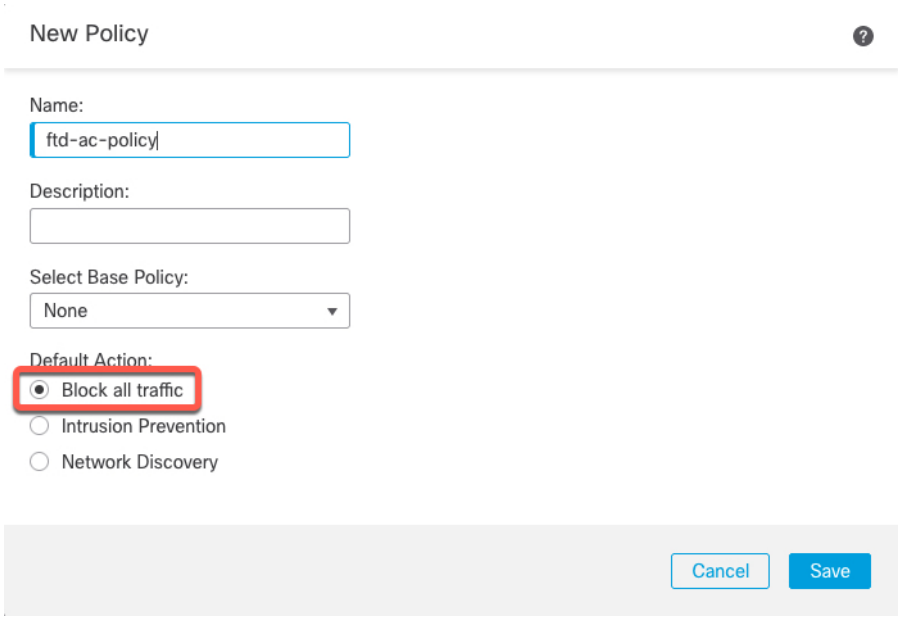
设置以下参数：

- **主机 (Host)** - 输入要添加的 威胁防御 的 IP 地址或主机名。如果在 威胁防御 初始引导程序配置中同时指定了 管理中心 IP 地址和 NAT ID，可以将此字段留空。

  注释 在 HA 环境中，当两个管理中心都位于 NAT 之后时，则可以在主管理中心中注册威胁防御而无需主机 IP 或名称。但是，要在辅助 管理中心 中注册 威胁防御，则必须提供 威胁防御 的 IP 地址或主机名。

- **显示名称 (Display Name)** - 输入要在管理中心中显示的威胁防御的名称。
- **注册密钥 (Registration Key)** - 输入您在威胁防御初始引导程序配置中指定的注册密钥。
- **域 (Domain)** - 如果有多域环境，请将设备分配给分叶域。
- **组 (Group)** - 如果在使用组，则将其分配给设备组。
- **访问控制策略 (Access Control Policy)** - 选择初始策略。除非已经拥有您知道自己需要使用的自定义策略，否则选择**新建策略 (Create new policy)**，然后选择**阻止所有流量 (Block all traffic)**。之后您可以更改此设置以允许流量通过；请参阅允许流量从内部传到外部，第 50 页。

图 *2: New Policy*



- **智能许可 (Smart Licensing)** - 为要部署的功能分配所需的智能许可证：**Malware**（如果您打算使用恶意软件检查）、**Threat**（如果您打算使用入侵防御）、**URL**（如果您打算实施基于类别的 URL 过滤）。**注意**：在添加设备后，您可以从**系统 > 许可证 > 智能许可证**页面应用 Secure Client 远程访问 VPN 许可证。
- **唯一 NAT ID (Unique NAT ID)** - 指定您在 威胁防御 初始引导程序配置中指定的 NAT ID。
- **转移数据包 (Transfer Packets)** - 可让设备将数据包传输至 管理中心。如果在启用此选项时触发了 IPS 或 Snort 等事件，设备会将事件元数据信息和数据包数据发送到 管理中心进行检测。如果禁用此选项，只有事件信息会发送到 管理中心，数据包数据不发送。

步骤 3 点击**注册 (Register)**，或者如果要添加另一台设备，请点击**注册并添加其他 (Register and Add Another)**，并确认注册成功。

如果注册成功，设备将添加到列表中。如果注册失败，您会看到一则错误消息。如果 威胁防御注册失败，请检查以下项：

- Ping - 访问 威胁防御CLI (访问威胁防御 CLI，第 53 页)，然后使用以下命令 ping 管理中心 IP 地址：

  ping system *ip_address*

  如果 ping 不成功，使用 **show network** 命令检查网络设置。如果需要更改 威胁防御 管理 IP 地址，请使用 **configure network** {**ipv4** | **ipv6**} **manual** 命令。如果为 管理中心 访问配置了数据接口，请使用 **configure network management-data-interface** 命令。

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

- 注册密钥、NAT ID 和管理中心 IP 地址 - 确保在两个设备上使用相同的注册密钥和 NAT ID（如有使用）。可以在管理中心使用 **configure manager add** 命令设定注册密钥和 NAT ID。

有关更多故障排除信息，请参阅 https://cisco.com/go/fmc-reg-error。

配置基本安全策略

本部分介绍如何使用以下设置配置基本安全策略：

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

要配置基本安全策略，需完成以下任务。

1	配置接口，第 41 页。
2	配置 DHCP 服务器，第 45 页。
3	添加默认路由，第 46 页。
4	配置 NAT，第 47 页。
5	允许流量从内部传到外部，第 50 页。
6	部署配置，第 51 页。

配置接口

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

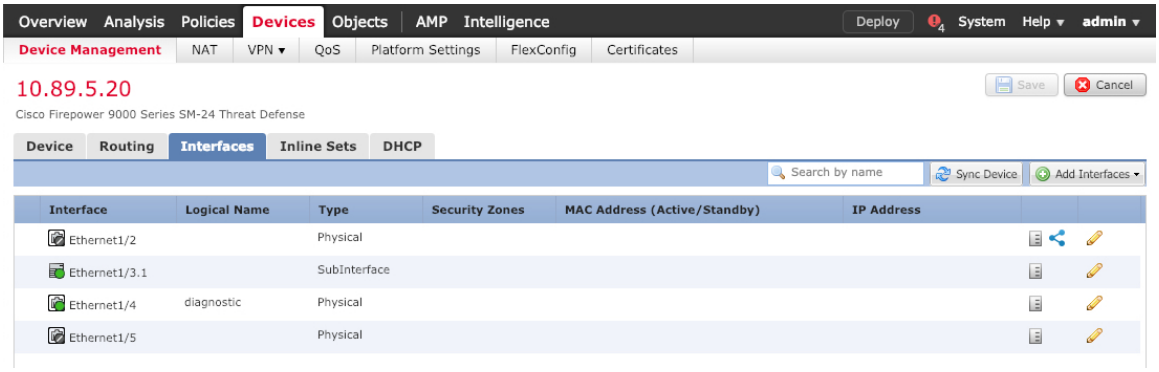
典型的边缘路由情况是通过 DHCP 从 ISP 获取外部接口地址，同时在内部接口上定义静态地址。

以下示例使用 DHCP 在接口内部配置了一个路由模式（含静态地址），并在接口外部配置了一个路由模式。

过程

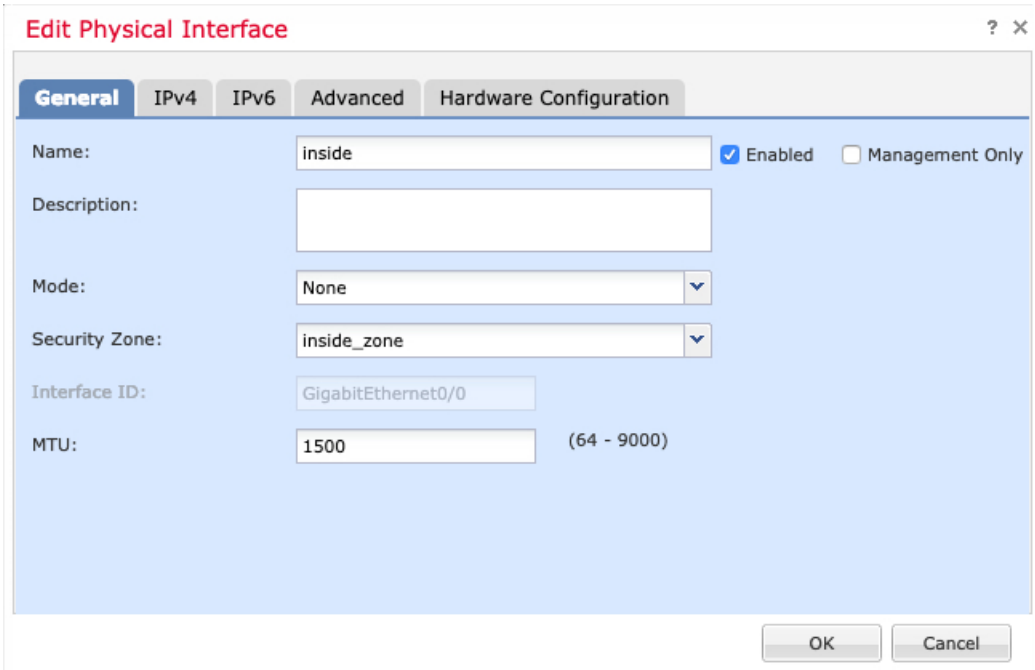
步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**，然后点击防火墙的**编辑**（ ）。

步骤 2 点击**接口 (Interfaces)**。



步骤 3 点击要用于内部的接口的**编辑**（ ）。

此时将显示**一般 (General)** 选项卡。



a) 输入长度最大为 48 个字符的 **Name**。

例如，将接口命名为 **inside**。

b) 选中 **Enabled** 复选框。

c) 将 **Mode** 保留为 **None**。

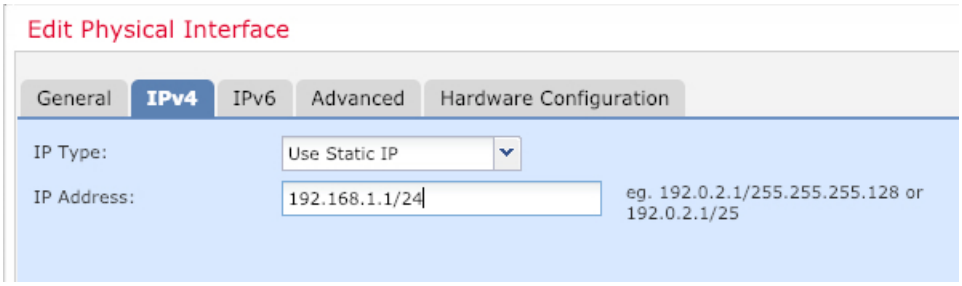
d) 从**安全区域 (Security Zone)** 下拉列表中选择一个现有的内部安全区域，或者点击**新建 (New)** 添加一个新的安全区域。

例如，添加一个名为 **inside_zone** 的区域。必须将每个接口分配给安全区域和/或接口组。每个接口只能属于一个安全区域，但可以同时属于多个接口组。您可以根据区域或组应用安全策略。例如，您可以将内部接口分配到内部区域，而将外部接口分配到外部区域。然后可以配置访问控制策略，允许流量从内部传到外部，但不允许从外部传入内部。大多数策略仅支持安全区域；您可以在 NAT 策略、预过滤器策略和 QoS 策略中使用区域或接口组。

e) 点击 **IPv4** 和/或 **IPv6** 选项卡。

- **IPv4** - 从下拉列表中选择**使用静态 IP (Use Static IP)**，然后以斜杠表示法输入 IP 地址和子网掩码。

  例如，输入 **192.168.1.1/24**

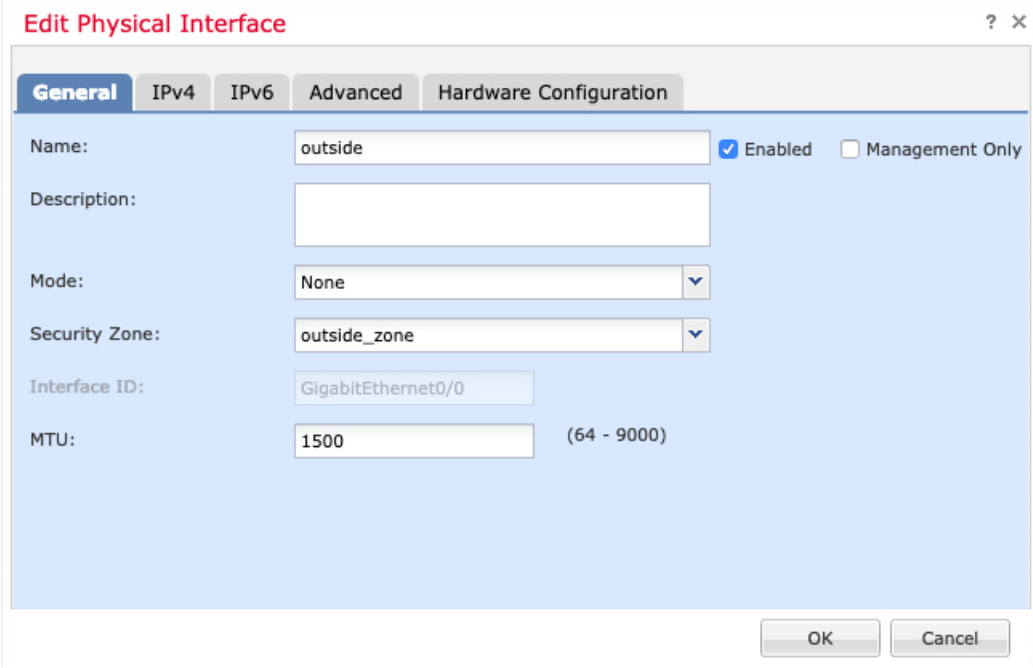


- **IPv6** - 为无状态自动配置选中**自动配置 (Autoconfiguration)** 复选框。

f) 点击**确定 (OK)**。

步骤 4 点击要用于外部的接口的 **编辑**（ ）。

此时将显示**一般 (General)** 选项卡。



注释　如果您为此接口预配置了管理器访问，则该接口就已经命名、启用和寻址。您不应更改任何这些基本设置，因为这样做会中断管理中心管理连接。您仍然可以在此屏幕上为直通流量策略配置安全区域。

a) 输入长度最大为 48 个字符的 **Name**。

例如，将接口命名为 **outside**。

b) 选中 **Enabled** 复选框。

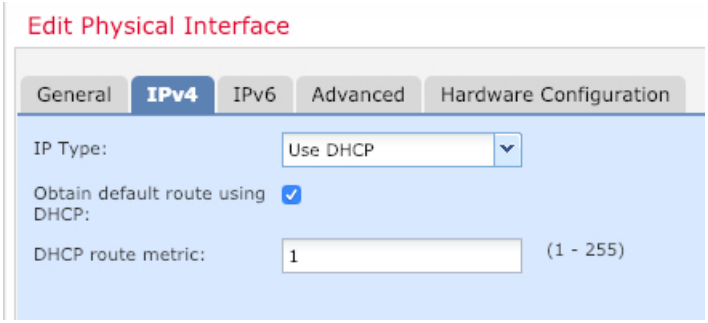
c) 将 **Mode** 保留为 **None**。

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

例如，添加一个名为 **outside_zone** 的区域。

e) 点击 **IPv4** 和/或 **IPv6** 选项卡。

- **IPv4** - 选择**使用 DHCP (Use DHCP)**，然后配置以下选填参数：
  - **使用 DHCP 获取默认路由 (Obtain default route using DHCP)** - 从 DHCP 服务器获取默认路由。
  - **DHCP 路由指标 (DHCP route metric)** - 分配到所获悉路由的管理距离，介于 1 和 255 之间。获悉的路由的默认管理距离为 1。



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

f) 点击**确定 (OK)**。

步骤 5 点击**保存**。

配置 DHCP 服务器

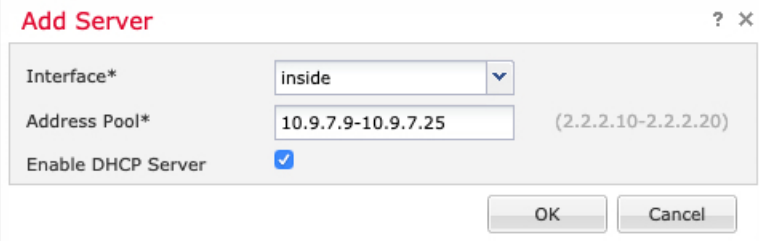
如果希望客户端使用 DHCP 从 威胁防御处获取 IP 地址，请启用 DHCP 服务器。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**，然后点击设备的**编辑**（ ）。

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

步骤 3 在**服务器 (Server**） 页面上点击**添加 (Add)**，然后配置以下选项：



- **接口 (Interface)** - 从下拉列表中选择接口。
- **地址池 (Address Pool)** - DHCP 服务器使用的 IP 地址的范围（从最低到最高）。IP 地址范围必须与选定接口位于相同的子网上，且不能包括接口自身的 IP 地址。
- **启用 DHCP 服务器 (Enable DHCP Server)** - 在所选接口上启用 DHCP 服务器。

步骤 4 点击**确定 (OK)**。

步骤 5 点击**保存**。

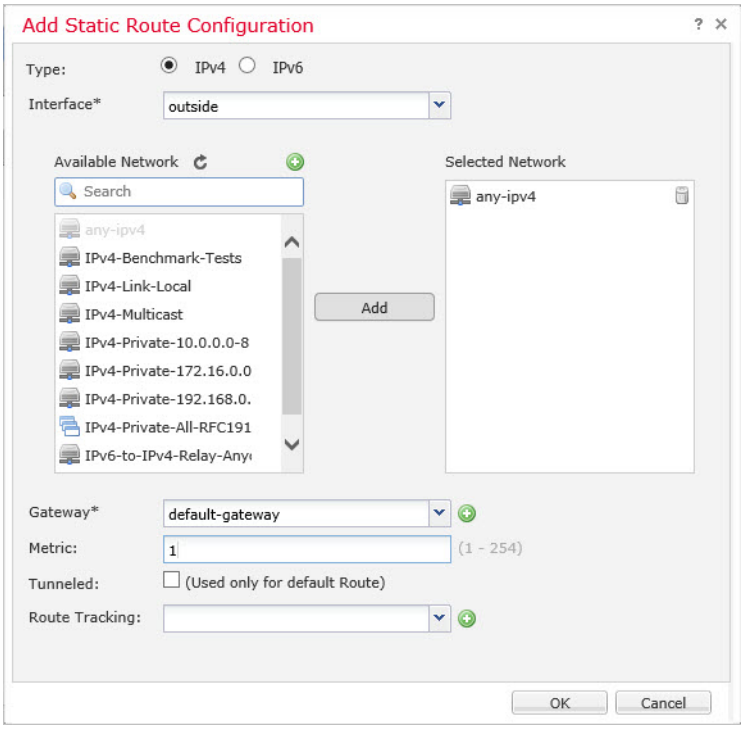
添加默认路由

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

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**，然后点击设备的**编辑**（ ）。

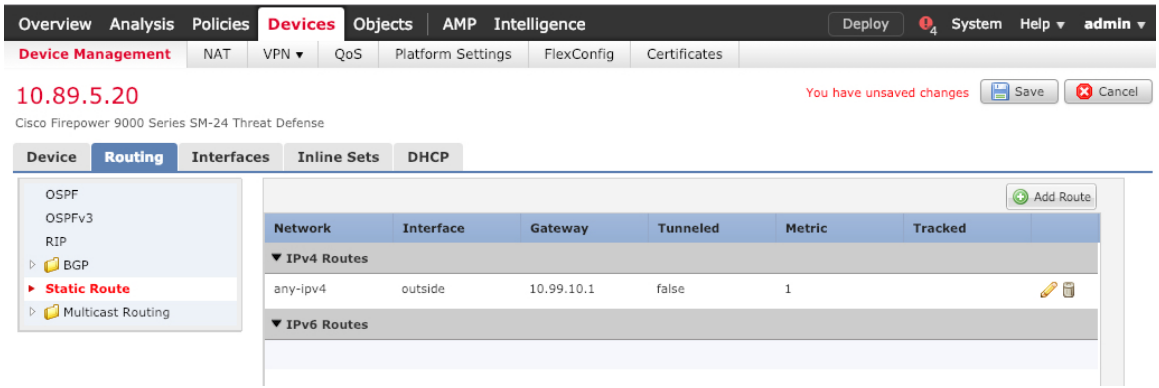
步骤 2 选择**路由 (Route)** > **静态路由 (Static Route)**，点击**添加路由 (Add Route)**，然后设置以下项：



- **类型 (Intrusion)** - 根据要添加静态路由的类型，点击 **IPv4** 或 **IPv6** 单选按钮。
- **接口 (Interface)** - 选择出口接口；通常是外部接口。
- **Available Network** - 为 IPv4 默认路由选择 **any-ipv4**，为 IPv6 默认路由选择 **any-ipv6**，然后点击 **Add** 将其移至 **Selected Network** 列表。
- **网关 (Gateway)** 或 **IPv6 网关 (IPv6 Gateway)** - 输入或选择作为此路由的下一个跃点的网关路由器。您可以提供 IP 地址或网络/主机对象。
- **指标 (Metric)** - 输入到目标网络的跃点数。有效值范围为 1 到 255；默认值为 1。

步骤 3 点击**确定 (OK)**。

路由即已添加至静态路由表。



步骤 4 点击保存。

配置 NAT

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

过程

步骤 1 选择**设备 (Devices)** > **NAT**，然后点击**新策略 (New Policy)** > **威胁防御 NAT (Threat Defense NAT)**。

步骤 2 为策略命名，选择要使用策略的设备，然后点击**Save**。



策略即已添加 管理中心。您仍然需要为策略添加规则。

步骤 3 点击**添加规则 (Add Rule)**。

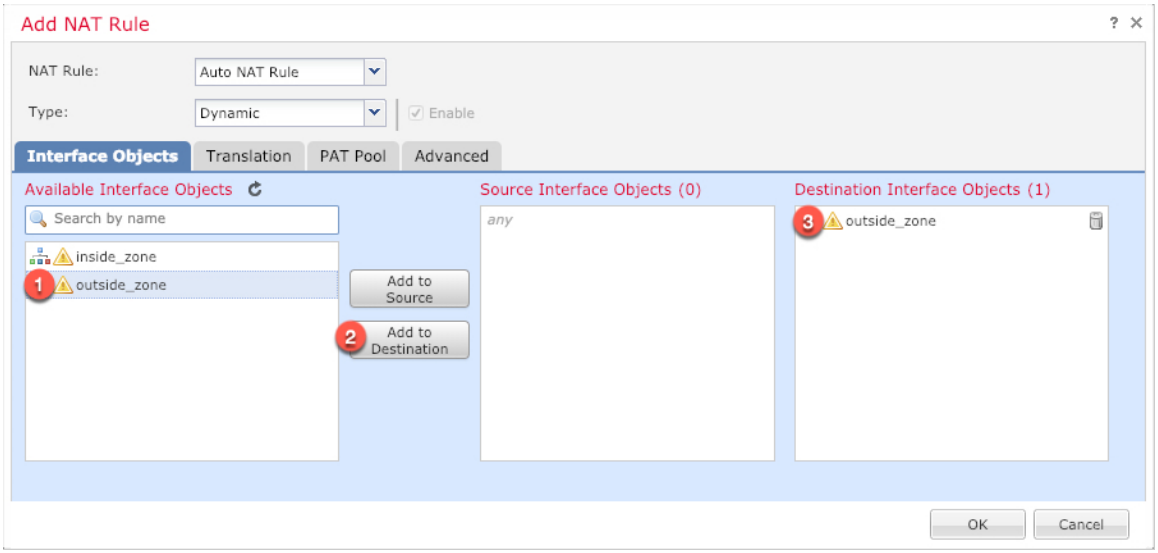
Add NAT Rule 对话框将显示。

步骤 4 配置基本规则选项：

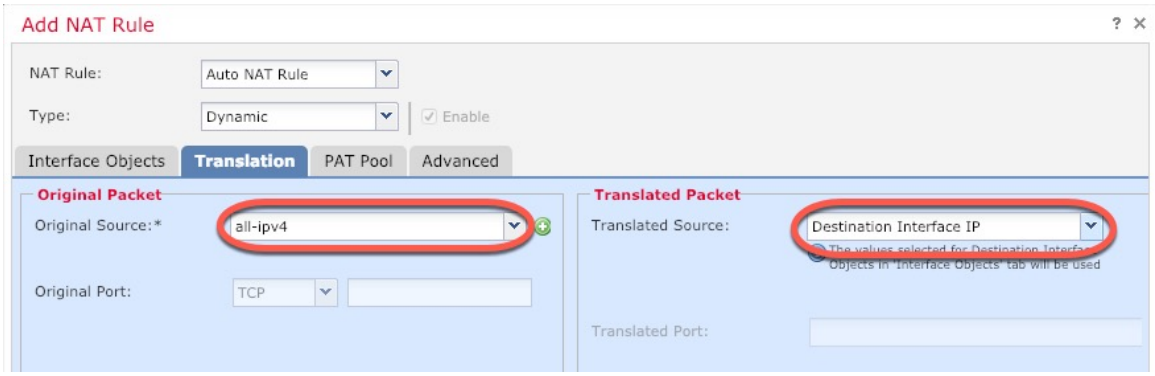


- **NAT 规则 (NAT Rule)** - 选择**自动 NAT 规则 (Auto NAT Rule)**。
- **类型 (Type)** - 选择**动态 (Dynamic)**。

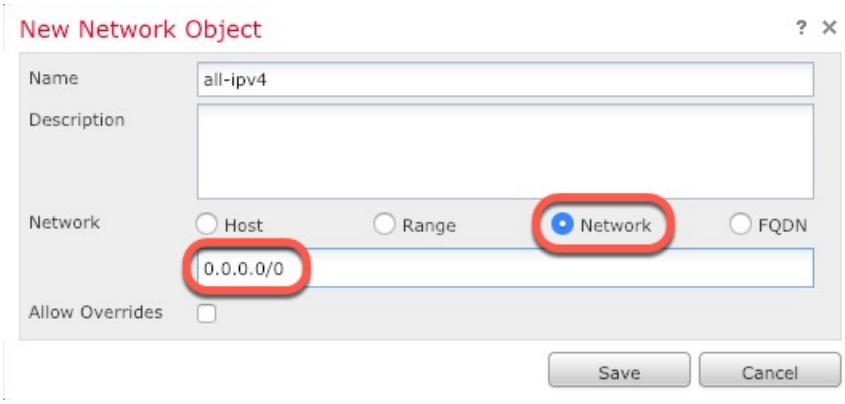
步骤 5 在 **Interface Objects** 页面，将 **Available Interface Objects** 区域中的外部区域添加到 **Destination Interface Objects** 区域。



步骤 6 在**转换 (Translation)** 页面上配置以下选项：



- **原始源** - 点击**添加**（+）为所有 IPv4 流量添加网络对象 (0.0.0.0/0)。

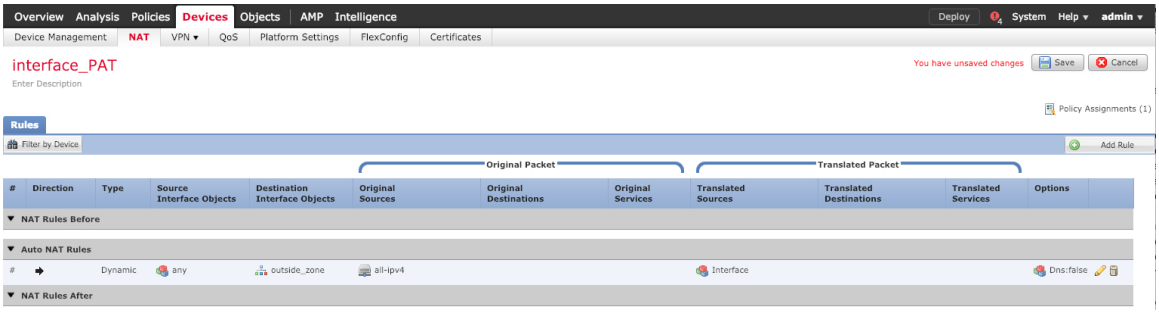


注释 您不能使用系统定义的 **any-ipv4** 对象，因为自动 NAT 规则在对象定义过程中添加 NAT，并且您无法编辑系统定义的对象。

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

步骤 7 点击**保存 (Save)** 以添加规则。

规则即已保存至 **Rules** 表。



步骤 8 点击 **NAT** 页面上的**保存 (Save)** 以保存更改。

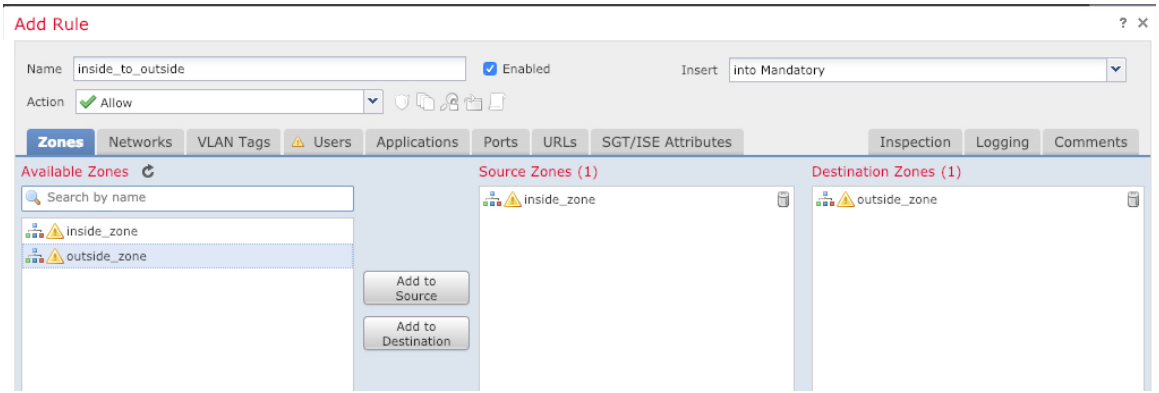
允许流量从内部传到外部

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

过程

步骤 1 选择**策略 (Policy)** > **访问策略 (Access Policy)** > **访问策略 (Access Policy)**，然后点击分配给 威胁防御 的访问控制策略的 **编辑**（ ）。

步骤 2 点击**添加规则 (Add Rule)** 并设置以下参数：



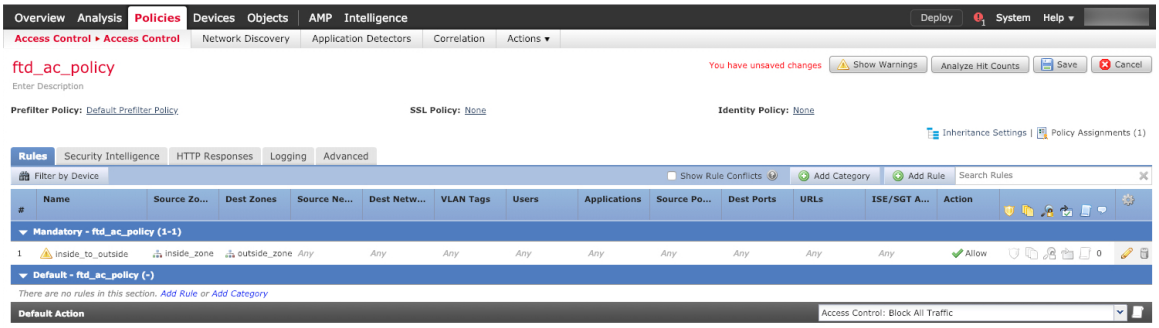
- **名称 (Name)** - 为此规则命名，例如 **inside_to_outside**。
- **源区域 (Source Zones)** - 从**可用区域 (Available Zones)** 中选择内部区域，然后点击**添加到源 (Add to Source)**。

- 目标区域 **(Destination Zones)** - 从可用区域 **(Available Zones**） 中选择外部区域，然后点击添加到目标 **(Add to Destination)**。

其他设置保留原样。

步骤 3 点击添加 **(Add)**。

规则即已添加至 **Rules** 表。



步骤 4 点击保存。

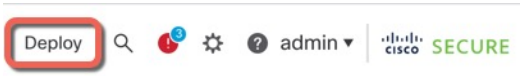
部署配置

将配置更改部署到 威胁防御；在部署之前，您的所有更改都不会在设备上生效。

过程

步骤 1 点击右上方的部署 **(Deploy)**。

图 *3:* 部署



步骤 2 点击全部部署 **(Deploy All)** 以部署到所有设备，或点击高级部署 **(Advanced Deploy)** 以部署到选择的设备。

图 *4:* 全部部署

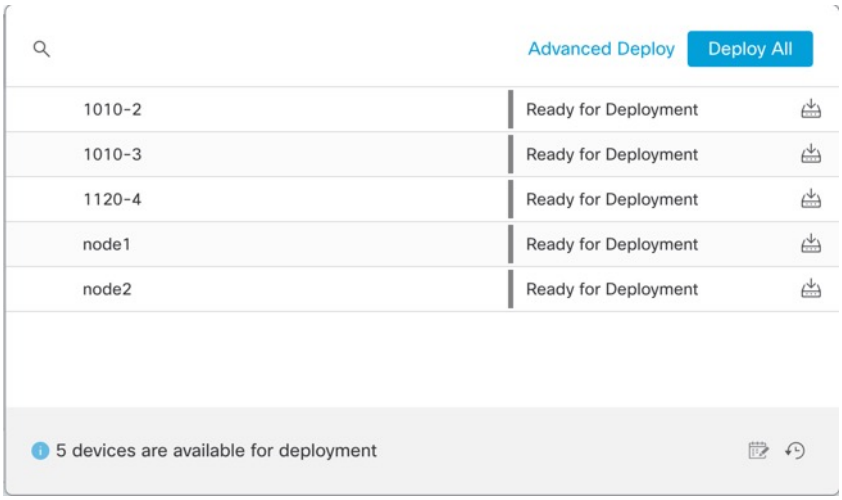
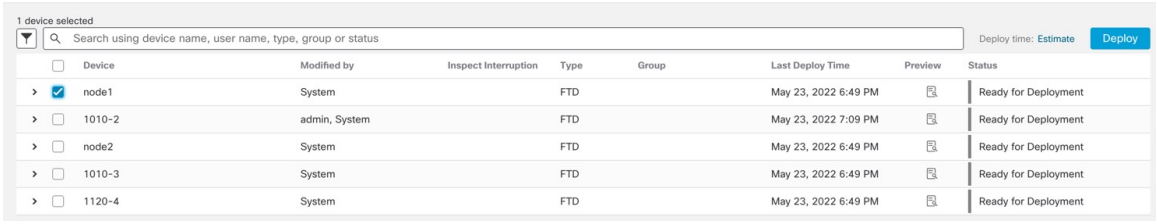
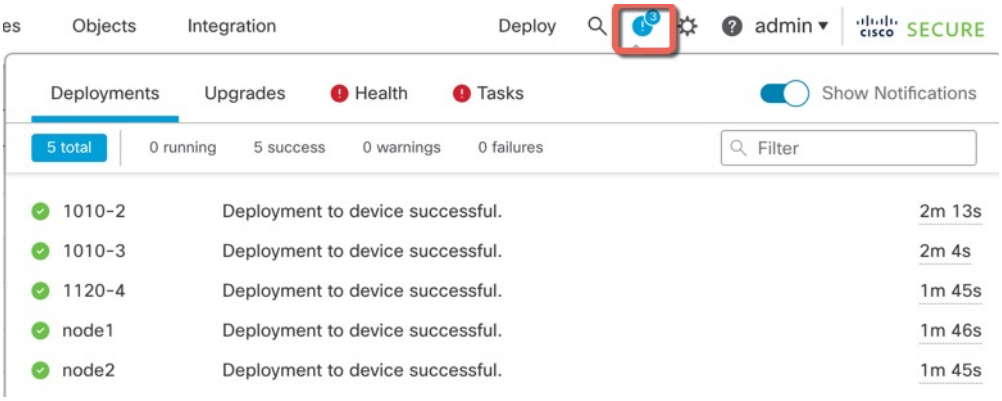


图 *5:* 高级部署



步骤 3 确保部署成功。点击菜单栏中**部署 (Deploy)** 按钮右侧的图标可以查看部署状态。

图 *6:* 部署状态



访问威胁防御 CLI

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

过程

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

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

如果忘记密码，可以通过编辑 机箱管理器 中的逻辑设备来更改密码。

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

a) 连接到 安全引擎。

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

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

示例：

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

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) 连接到 威胁防御控制台。

connect ftd *name*

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

示例：

```
Firepower-module1> connect ftd FTD_Instance1

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

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

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

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

注释　　对于 6.3 之前的版本，输入 **Ctrl-a, d**。

d) 返回 FXOS CLI的管理引擎层。

要退出控制台：

1. 输入 **~**

   您将退出至 Telnet 应用。

2. 要退出 Telnet 应用，请输入：

   telnet>**quit**

要退出 Telnet 会话：

输入 **Ctrl-],**。

示例

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

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

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect ftd FTD_Instance1

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

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

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

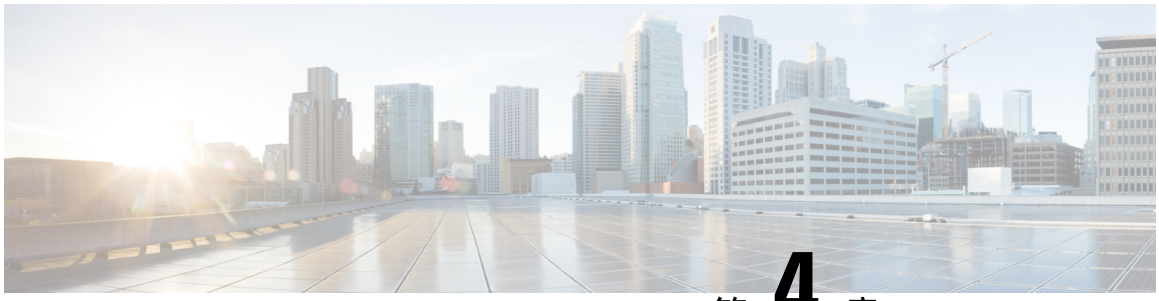
后续步骤

要继续配置 威胁防御，请参阅适用于您的软件版本的文档：导航思科 Firepower 文档。

有关使用 管理中心的信息，请参阅《Firepower 管理中心配置指南》。

使用管理中心的威胁防御历史记录

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



第 4 章

使用设备管理器部署威胁防御

本章对您适用吗？

本章介绍如何部署使用设备管理器管理的独立式威胁防御逻辑设备。要部署高可用性对，请参阅《Cisco Secure Firewall 设备管理器配置指南》。

设备管理器可以配置小型网络最常用软件的基本功能。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 设备管理器 设备的大型网络。

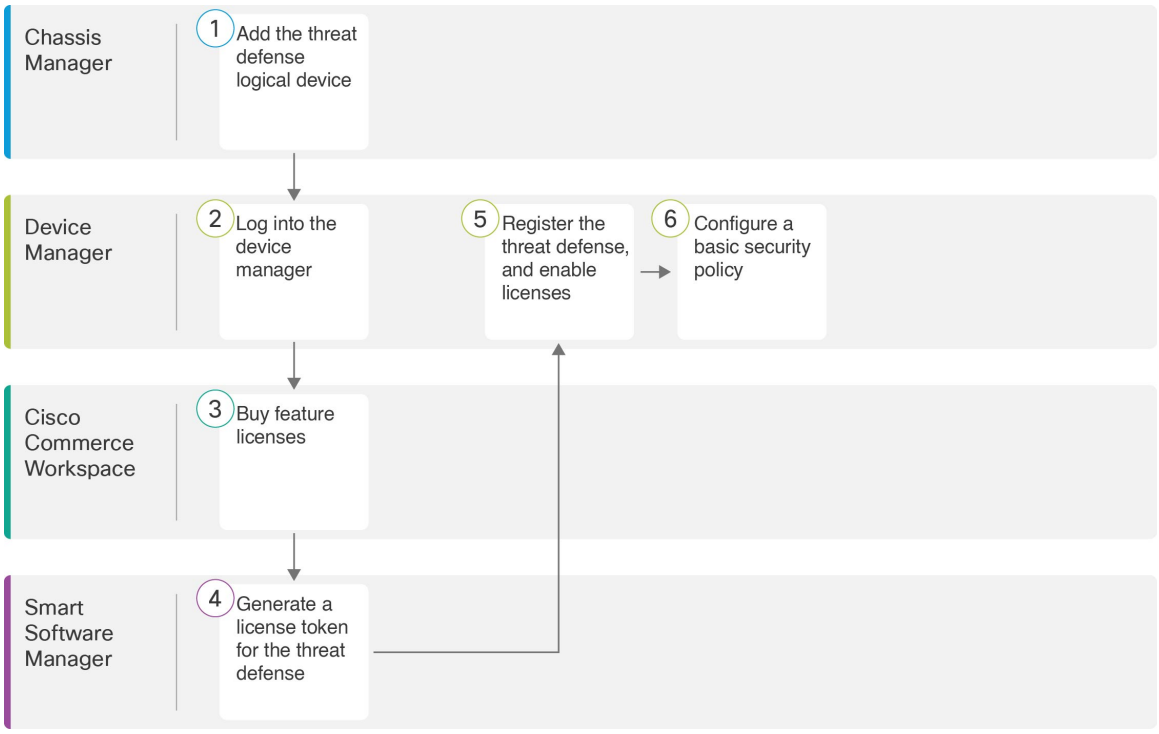
如果要管理大量设备或要使用 威胁防御 支持的更复杂的功能和配置，则改为使用 管理中心。

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

- 端到端程序， 第 57 页
- 机箱管理器：添加威胁防御逻辑设备， 第 58 页
- 登录设备管理器， 第 62 页
- 配置许可， 第 62 页
- 配置基本安全策略， 第 69 页
- 访问威胁防御 CLI， 第 81 页
- 后续步骤， 第 83 页
- 使用设备管理器的威胁防御历史记录， 第 84 页

端到端程序

请参阅以下任务以在机箱上部署和配置 威胁防御。



	工作空间	步骤
1	机箱管理器	机箱管理器：添加威胁防御逻辑设备， 第 58 页。
2	设备管理器	登录设备管理器， 第 62 页。
3	Cisco Commerce Workspace	配置许可， 第 62 页：购买功能许可证。
4	智能软件管理器	配置许可， 第 62 页：为 设备管理器 生成许可证令牌。
5	设备管理器	配置许可， 第 62 页：向智能许可服务器注册设备管理器，并启用功能许可证。
6	设备管理器	配置基本安全策略， 第 69 页。

机箱管理器：添加威胁防御逻辑设备

可以从 Firepower 4100 将 威胁防御 部署为本地实例。不支持容器实例。

要添加高可用性对，请参阅《Cisco Secure Firewall 设备管理器配置指南》。

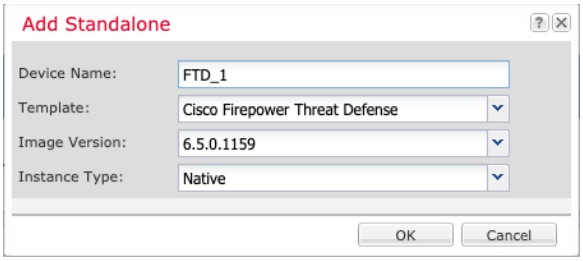
开始之前

- 配置与 威胁防御一起使用的管理接口；请参阅配置接口，第 20 页。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。
- 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
  - DNS 服务器 IP 地址
  - 威胁防御 主机名和域名

过程

步骤 1 在 机箱管理器中，选择**逻辑设备**。

步骤 2 点击**添加** > **独立设备**，并设置以下参数：



a) 提供**设备名称**。

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

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

c) 选择**映像版本**。

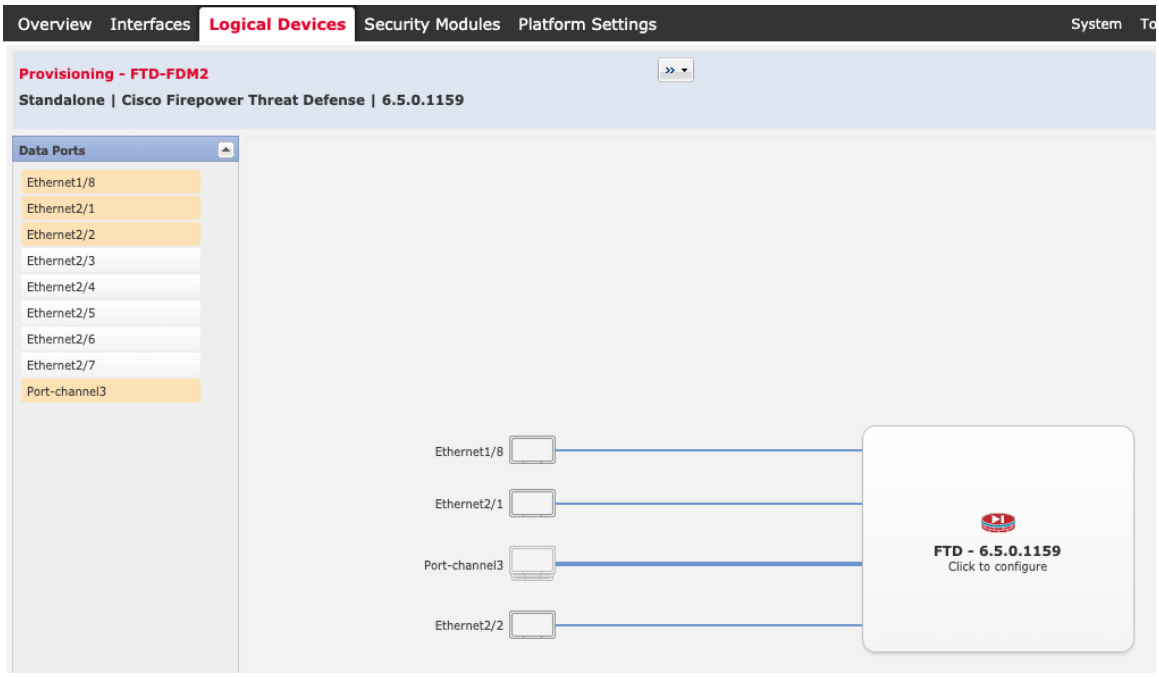
d) 选择**实例类型**：**本地**。

设备管理器不支持容器实例。

e) 点击**确定 (OK)**。

屏幕会显示调配 - 设备名称窗口。

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

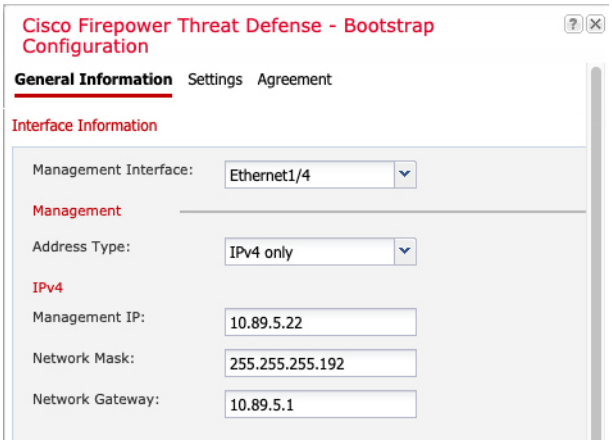


仅可分配先前在**接口 (Interfaces)** 页面上启用的数据接口。稍后您需要在 设备管理器 中启用和配置这些接口，包括设置 IP 地址。

步骤 4 点击屏幕中心的设备图标。

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

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



a) 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。

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

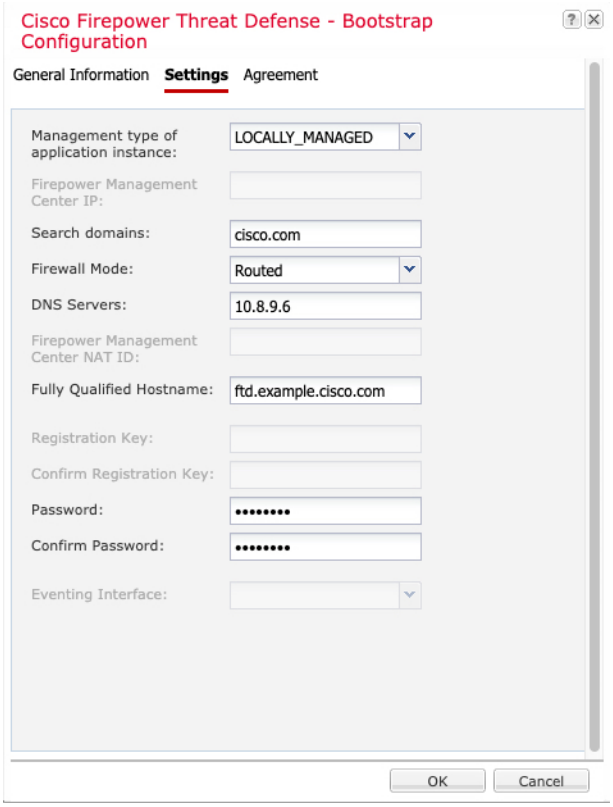
c) 配置**管理 IP** 地址。

设置用于此接口的唯一 IP 地址。

d) 输入**网络掩码**或**前缀长度**。

e) 输入**网络网关**地址。

步骤 6 在**设置**选项卡上，完成下列操作：



a) 在**应用实例的管理类型**下拉列表中，选择 **LOCALLY_MANAGED**。

本地实例还支持 管理中心 作为管理器。如果在部署逻辑设备后更改管理器，则系统会清除您的配置，并重新初始化设备。

b) 输入逗号分隔列表形式的**搜索域**。

c) **防火墙模式**仅支持**路由式**。

d) 输入逗号分隔列表形式的 **DNS 服务器**。

e) 输入威胁防御的**完全限定主机名**。

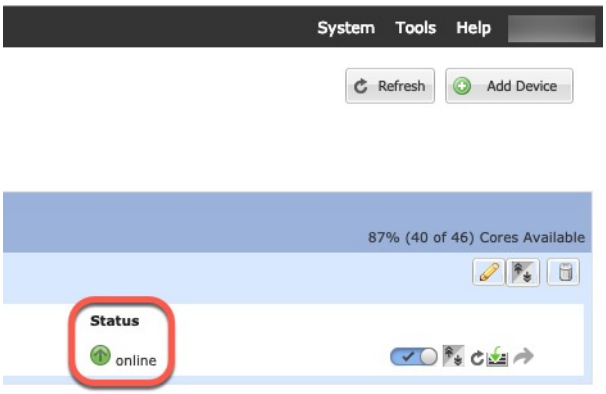
f) 输入供威胁防御管理员用户用于 CLI 访问的**密码**。

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

步骤 8 点击**确定 (OK)** 关闭配置对话框。

步骤 9 点击**保存 (Save)**。

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



登录设备管理器

登录设备管理器以配置威胁防御。

开始之前

- 使用 Firefox、Chrome、Safari、Edge 或 Internet Explorer 的当前版本。
- 确保 机箱管理器 **逻辑设备 (Logical Devices)**页面上 威胁防御 逻辑设备的**状态 (Status)** 为**在线 (online)**。

过程

步骤 1 在浏览器中输入以下 URL。

- 管理 - **https://***management_ip*。输入您在引导程序配置中输入的接口 IP 地址。

步骤 2 使用用户名 **admin** 和部署威胁防御时设置的密码 登录。

步骤 3 系统会提示您接受 90 天评估许可证。

配置许可

威胁防御 使用智能软件许可，这使得您可以集中购买和管理许可证池。

注册机箱时，智能软件管理器会为机箱和智能软件管理器之间的通信颁发ID证书。它还会将机箱分配到相应的虚拟帐户。

有关思科许可的更详细概述，请访问 cisco.com/go/licensingguide

基础版 许可证会自动包含在内。智能许可不会阻止您使用尚未购买的产品功能。只要您向智能软件管理器进行了注册，即可立即开始使用许可证，并在以后购买该许可证。这使您能够部署和使用功能，并避免由于采购订单审批造成延迟。请参阅以下许可证：

- **IPS**胁-安全情报和下一代 IPS
- **恶意软件 防御**-恶意软件 防御
- **URL** - URL 过滤
- **Cisco Secure 客户端**-Secure Client Advantage、Secure Client Premier 或 Secure Client VPN Only

开始之前

- 拥有 智能软件管理器主帐户。

  如果您还没有帐户，请点击此链接以设置新帐户。通过智能软件管理器，您可以为组织创建一个主帐户。

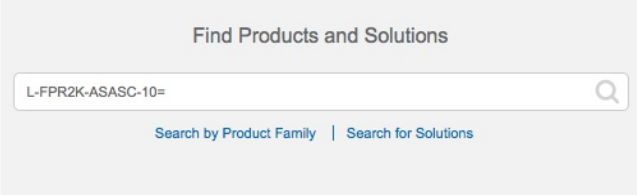
- 您的智能软件许可帐户必须符合强加密 (3DES/AES) 许可证的要求，才能使用某些功能（已使用导出合规性标志启用）。

过程

步骤 1 请确保智能许可帐户包含所需的可用许可证。

当您从思科或经销商那里购买设备时，您的许可证应该已链接到您的智能软件许可证帐户。但是，如果您需要自己添加许可证，则请使用Cisco Commerce Workspace上的 **Find Products and Solutions** 搜索字段。搜索以下许可证 PID：

图 7: 许可证搜索



注释 如果未找到 PID，您可以手动将 PID 添加到订单中。

- IPS、恶意软件 防御和 URL 许可证组合：
  - L-FPR4112T-TMC=
  - L-FPR4115T-TMC=
  - L-FPR4125T-TMC=
  - L-FPR4145T-TMC=

当您将上述 PID 之一添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：

- L-FPR4112T-TMC-1Y
- L-FPR4112T-TMC-3Y
- L-FPR4112T-TMC-5Y
- L-FPR4115T-TMC-1Y
- L-FPR4115T-TMC-3Y
- L-FPR4115T-TMC-5Y
- L-FPR4125T-TMC-1Y
- L-FPR4125T-TMC-3Y
- L-FPR4125T-TMC-5Y
- L-FPR4145T-TMC-1Y
- L-FPR4145T-TMC-3Y
- L-FPR4145T-TMC-5Y

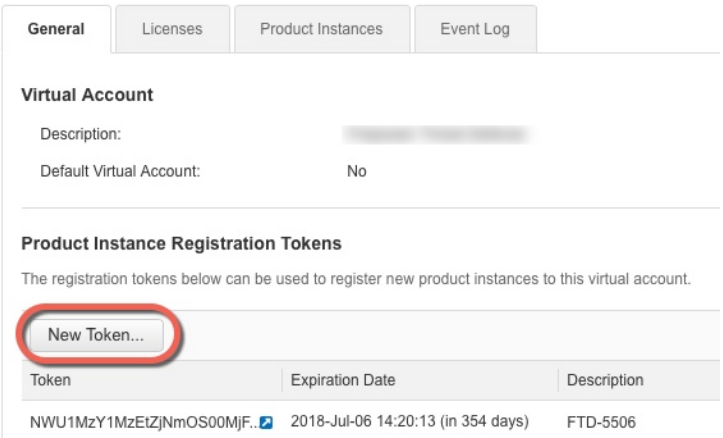
- Cisco Secure 客户端-请参阅 思科安全客户端订购指南。

步骤 2 在 智能软件管理器 中，为要将此设备添加到的虚拟帐户请求并复制注册令牌。

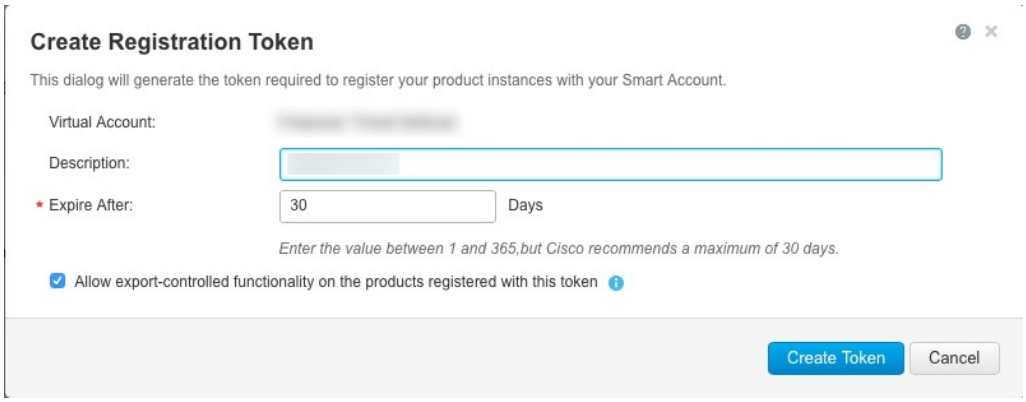
a) 点击 **Inventory**。



b) 在 **General** 选项卡上，点击 **New Token**。



c) 在 **Create Registration Token** 对话框中，输入以下设置，然后点击 **Create Token**：



- **Description**
- **Expire After** - 思科建议该时间为 30 天。
- **在使用此令牌注册的产品上允许导出控制的功能 (Allow export-controlled functionaility on the products registered with this token** — 在您所在的国家/地区允许进行强加密的情况下启用导出合规性标志。如果打算使用此功能，则须立即选择该选项。如果稍后启用此功能，则需要使用新产品密钥重新注册设备并重新加载设备。如果您没有看到此选项，则您的帐户不支持出口控制功能。

系统将令牌添加到您的资产中。

d) 点击令牌右侧的箭头图标可以打开 **Token** 对话框，可以从中将令牌 ID 复制到剪贴板。当需要注册威胁防御时，请准备好此令牌，以在该程序后面的部分使用。

图 *8:* 查看令牌

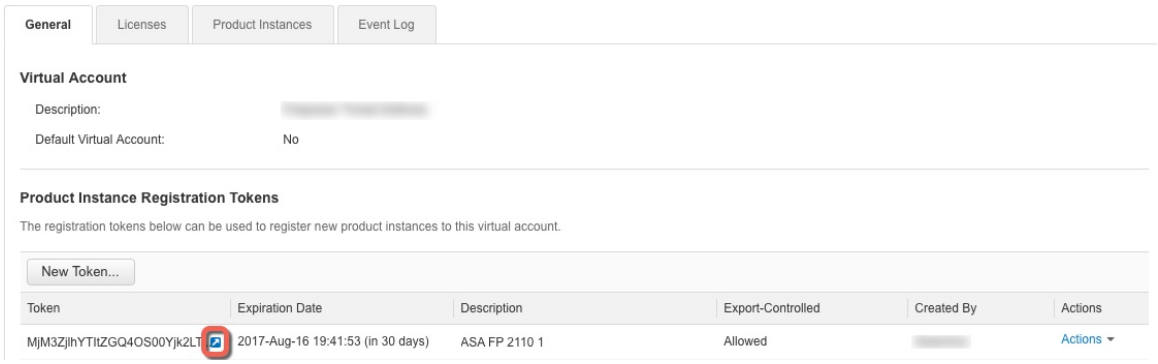
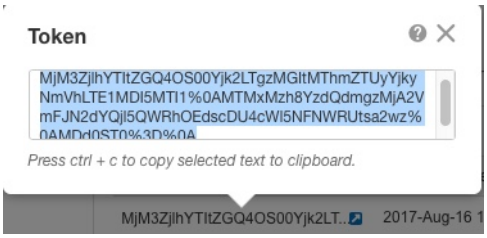


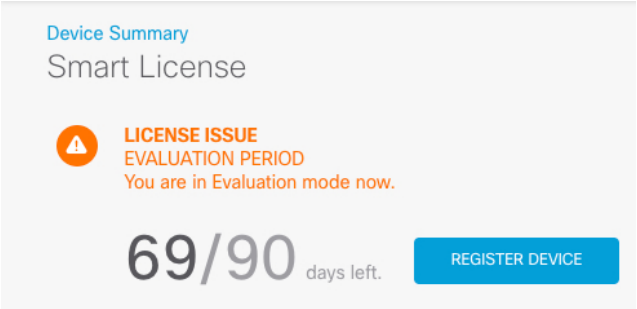
图 *9:* 复制令牌



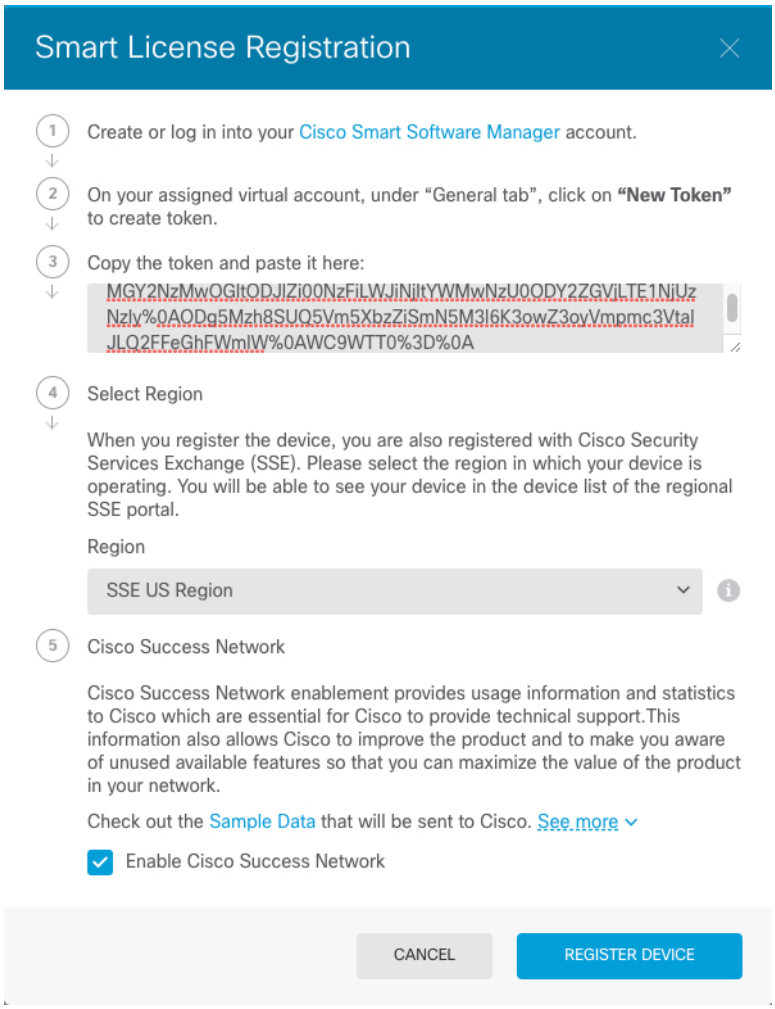
步骤 3 在 设备管理器中，点击 **设备**，然后在 **智能许可证** 摘要中，点击 **查看配置**。

您会看到**智能许可证**页面。

步骤 4 点击 **Register Device**。

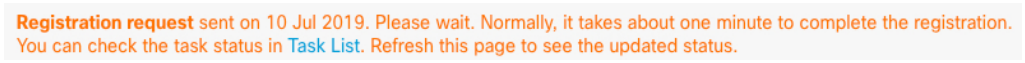


然后，按照**智能许可证注册**对话框中的说明粘贴令牌：

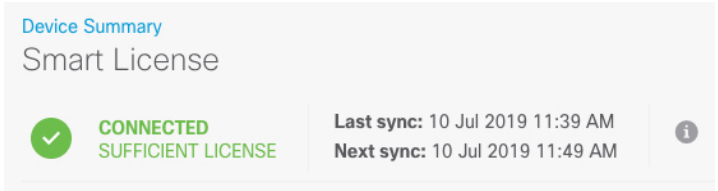


步骤 5 点击 **Register Device**。

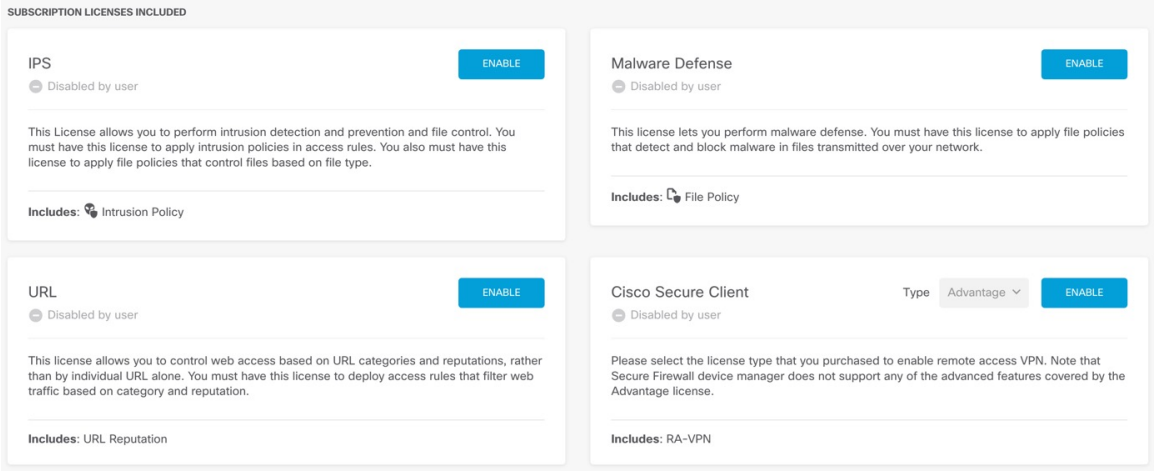
您会返回到**智能许可证**页面。在设备注册时，您会看到以下消息：



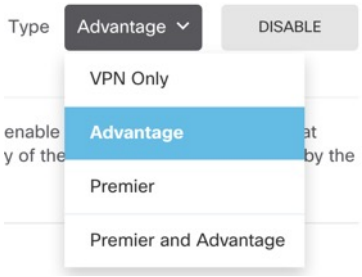
在设备成功注册并刷新页面后，您会看到以下内容：



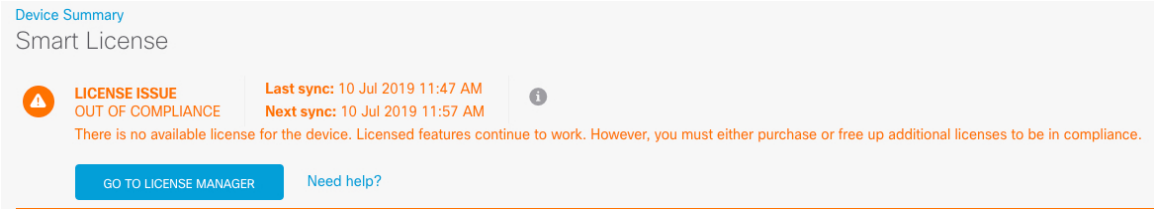
步骤 6 根据需要，点击每个可选许可证的**启用/禁用**控件。



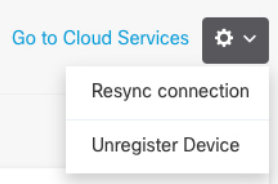
- **启用** - 将许可证注册到您的思科智能软件管理器帐户，并启用控制的功能。现在，您可以配置和部署该许可证控制的策略了。
- **禁用** - 取消许可证向思科智能软件管理器帐户的注册，并禁用控制的功能。新策略中无法配置这些功能，也不能再部署使用该功能的策略。
- 如果启用了 **Cisco Secure 客户端** 许可证，请选择要使用的许可证类型： **Advantage**、 **Premier**、 **VPN Only**或 **Premier** 和**Advantage**。



启用功能后，如果帐户中没有许可证，则在刷新页面后，您会看到以下不合规消息：



步骤 7 从齿轮下拉列表中选择 **Resync Connection**（再同步连接），将许可证信息与思科智能软件管理器同步。



配置基本安全策略

要配置基本安全策略，需完成以下任务。

1	配置接口， 第 69 页。 为内部接口分配静态 IP 地址，并将 DHCP 用于外部接口。
2	将接口添加到安全区域， 第 72 页。 将内部和外部接口添加到访问控制所需的内部和外部安全区域。
3	添加默认路由， 第 73 页。 如果没有收到来自外部 DHCP 服务器的默认路由，则需要手动添加它。
4	配置 NAT， 第 75 页。 在外部接口上使用接口 PAT。
5	允许流量从内部传到外部， 第 77 页。 允许流量从内部传到外部。
6	（可选）配置 DHCP 服务器， 第 78 页。 在内部接口上为客户端使用 DHCP 服务器。
7	（可选）配置管理网关并允许在数据接口上进行管理， 第 79 页。 更改管理网关和/或允许从数据接口进行管理。
8	部署配置， 第 81 页。

配置接口

启用 威胁防御 接口并设置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。

以下示例配置了一个具有静态地址的内部接口，以及一个使用 DHCP 的外部接口。

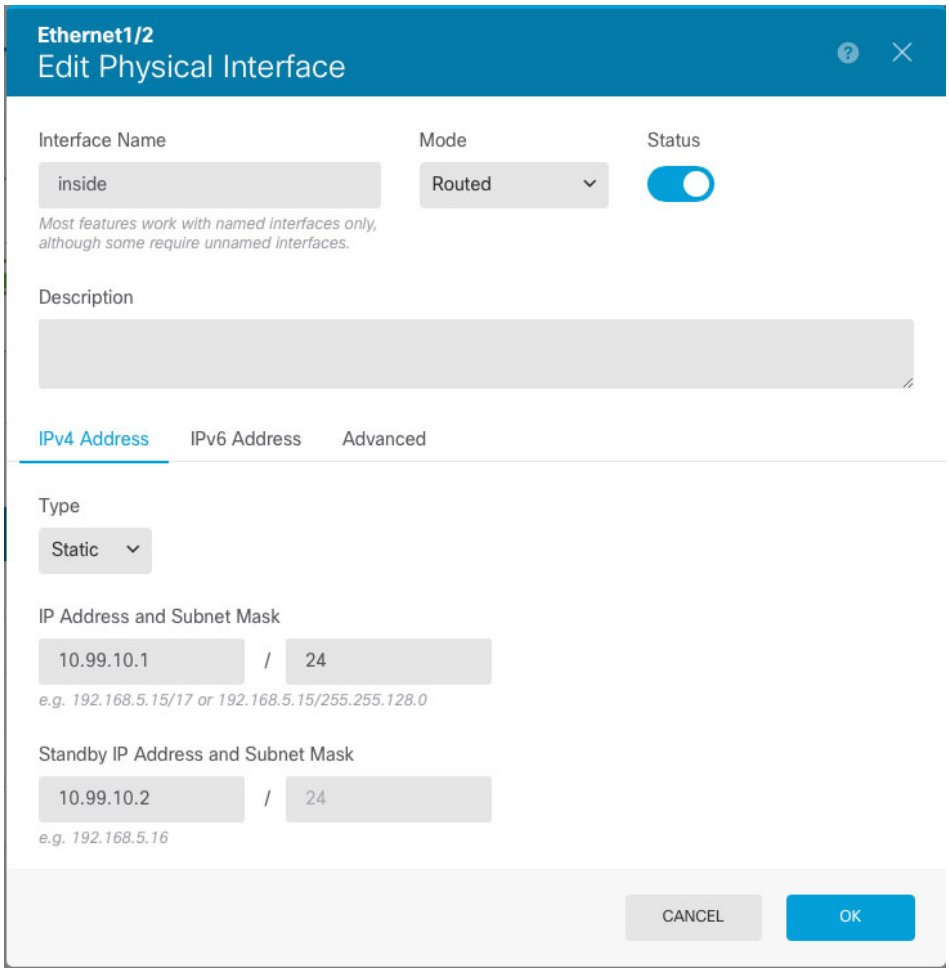
过程

步骤 1 点击**设备**，然后点击**接口**摘要中的链接。

系统默认选择**接口 (Interfaces)** 页面。接口列表显示可用物理接口、物理接口名称、地址和状态。

步骤 2 点击要用于内部的接口的编辑图标 ( )。

步骤 3 进行以下设置：



a) 设置**接口名称**。

设置接口名称，最多 48 个字符。字母字符必须为小写。例如 **inside** 或 **outside**。如果没有名称，将忽略其余的接口配置。除非配置子接口，否则接口应有名称。

b) 将**模式**设置为**路由**。

如果要使用被动接口，请参阅《Cisco Secure Firewall 设备管理器配置指南》。

c) 将**状态**滑块设置为已启用设置 ( )。

重要事项 还必须在 FXOS 中启用该接口。

d) （可选） 设置**说明**。

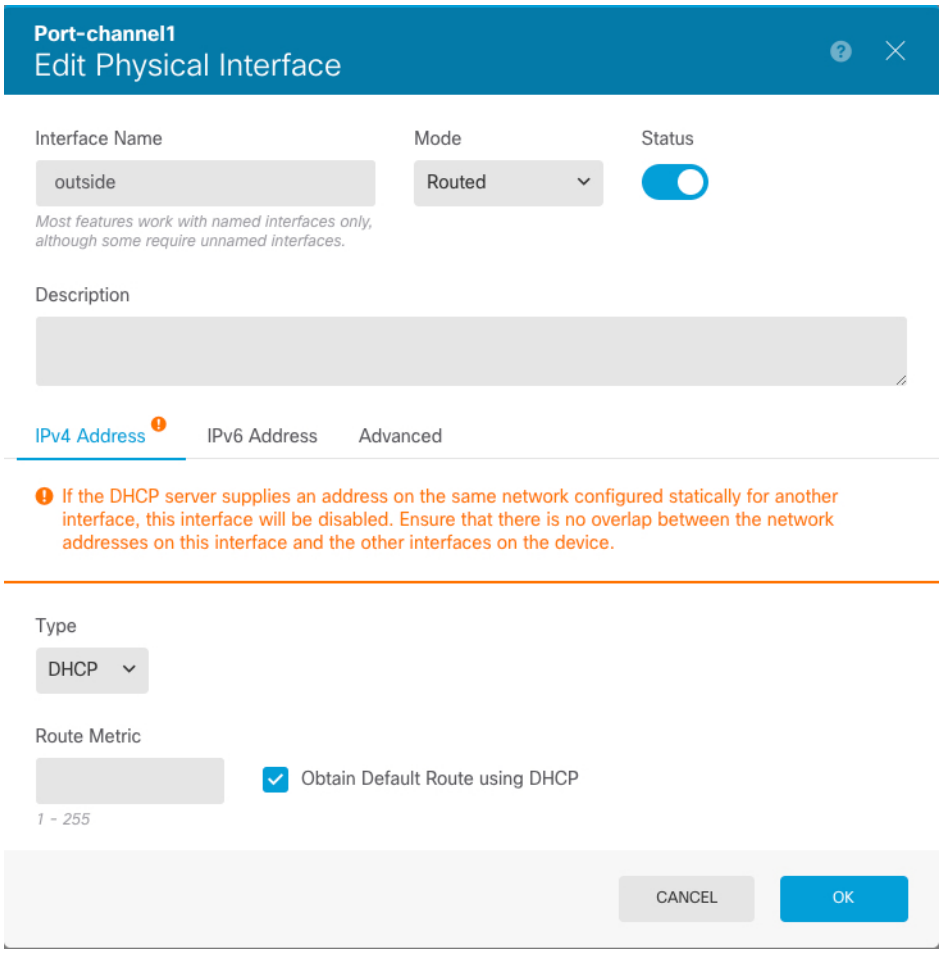
一行说明最多可包含 200 个字符（不包括回车符）。

e) 在 **IPv4 地址**页面上，配置静态 IP 地址。

f) （可选） 点击 **IPv6 地址**，并配置 IPv6。

步骤 4 点击**点击**。

步骤 5 点击要用于外部的接口的编辑图标 ( )，并设置适用于内部的相同字段；对于此接口，请为 IPv4 地址选择**DHCP** 。



注释 如果使用静态 IP 地址或不接收来自 DHCP 的默认路由，则需要手动设置默认路由；请参阅《Cisco Secure Firewall 设备管理器配置指南》。

将接口添加到安全区域

安全区是一组接口。区域将网络划分成网段，帮助您管理流量以及对流量进行分类。您可以定义多个区域，但一个给定接口只能位于一个区域中。

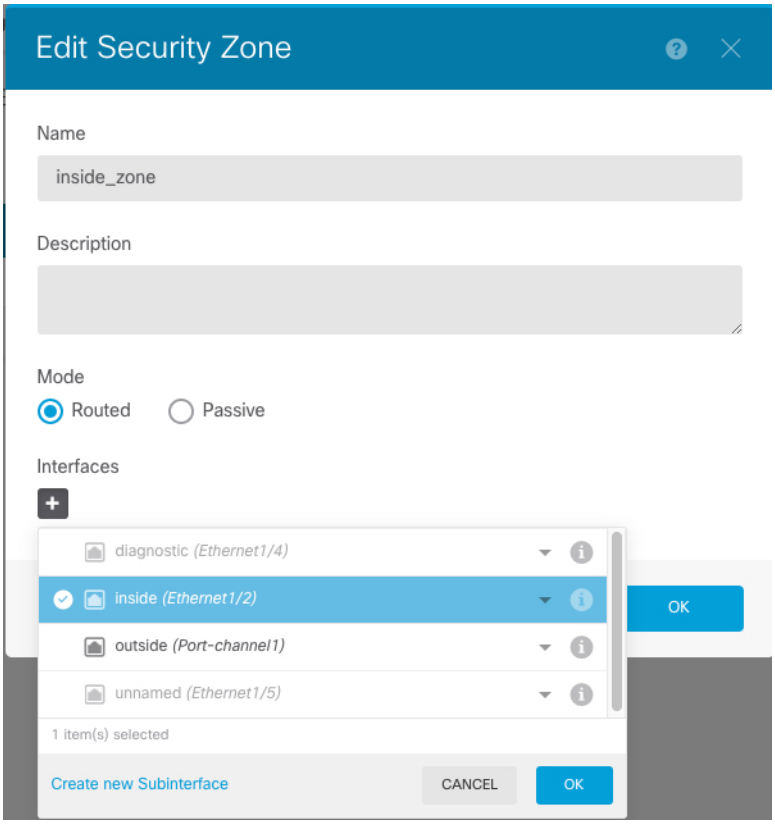
此程序介绍如何将接口添加到以下预配置的区域：

- **inside_zone** - 此区域用于表示内部网络。
- **outside_zone** - 此区域用于表示在您控制之外的网络，例如互联网。

过程

步骤 1 选择**对象**，然后从目录中选择**安全区**。

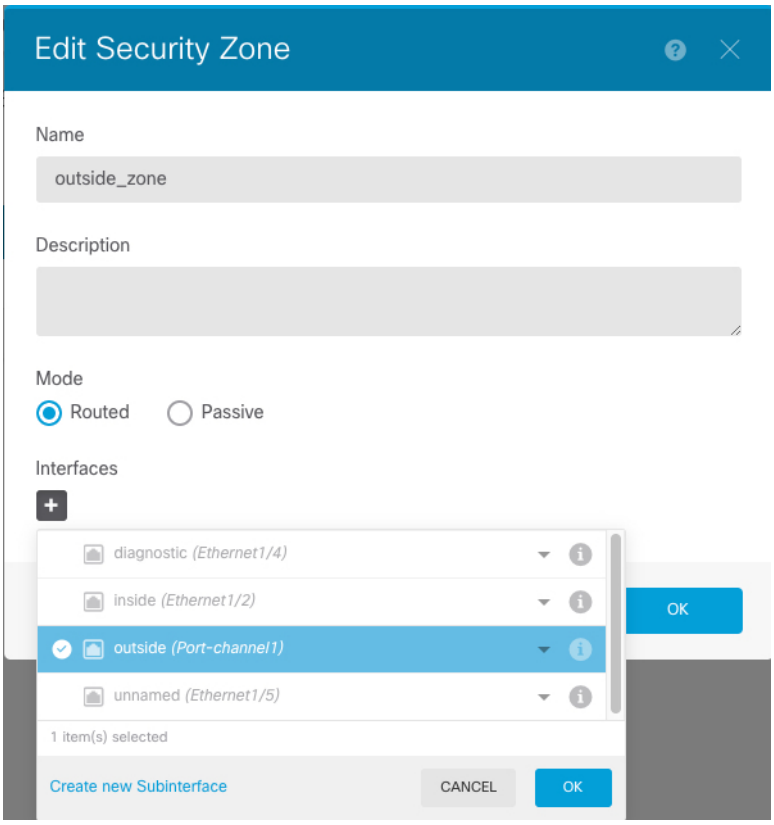
步骤 2 点击 **inside_zone** 的编辑图标 ( )。



步骤 3 在**接口**列表中，点击 + 并选择要添加到该区域的内部接口。

步骤 4 点击 **确定**，保存更改。

步骤 5 重复这些步骤以将外部接口添加到 **outside_zone** 中。



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，那么它将显示在**设备摘要** > **静态路由**页面上。

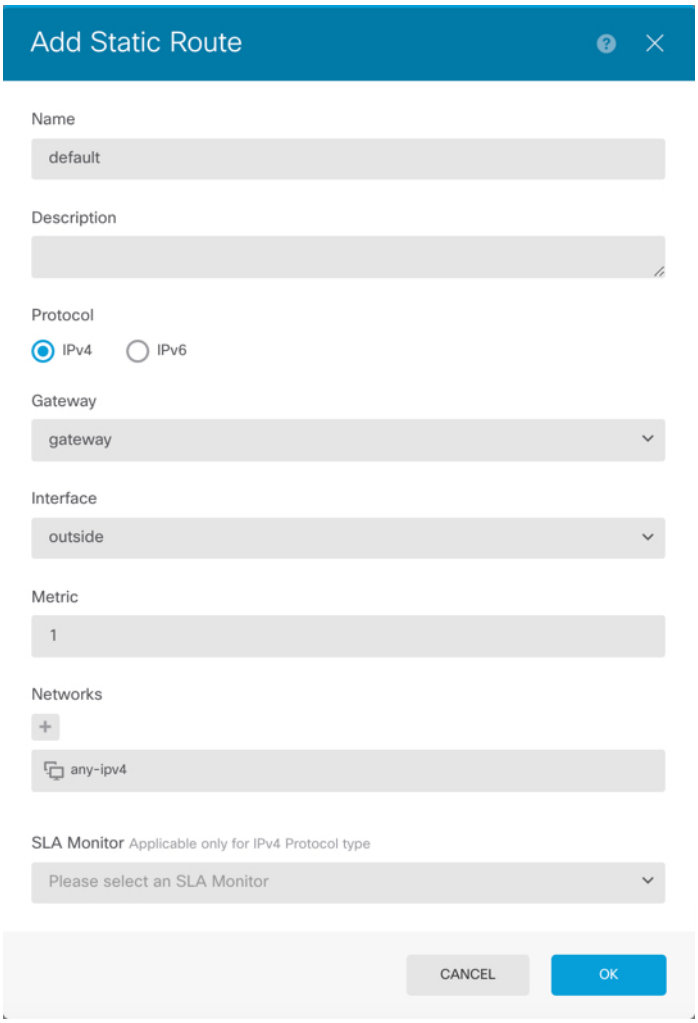
过程

步骤 1 点击**设备**，然后点击**路由**摘要中的链接。

系统将显示**静态路由**页面。

步骤 2 点击 + 或**添加静态路由**。

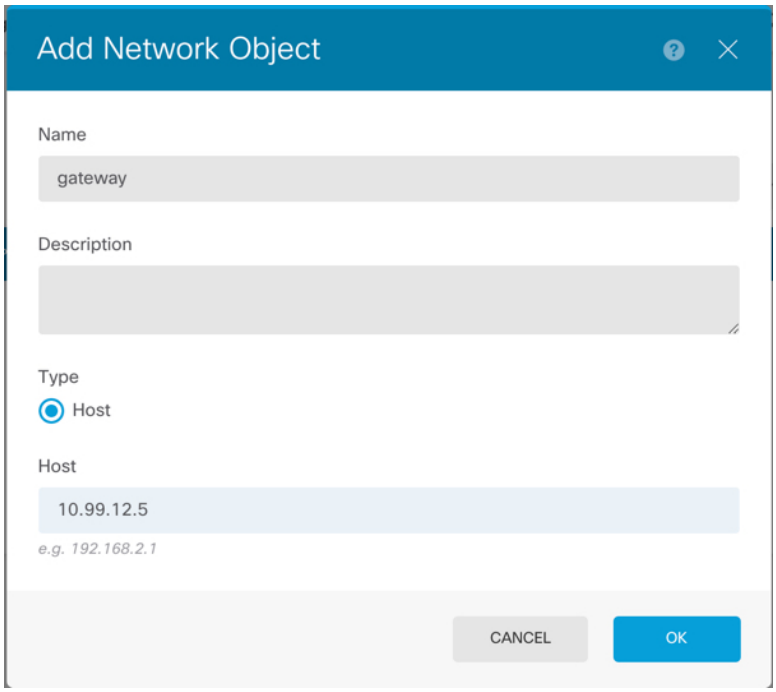
步骤 3 配置默认路由属性。



a) 输入**名称**，例如，**默认值**。
b) 点击 **IPv4** 或 **IPv6** 单选按钮。

需要为 IPv4 和 IPv6 创建单独的默认路由。

c) 点击**网关**，然后点击**创建新网络**以将网关 IP 地址添加为主机对象。



d) 选择网关**接口**，例如**外部**。

e) 点击**网络** + 图标，为 IPv4 默认路由选择 **any-ipv4**，为 IPv6 默认路由选择 **any-ipv6**。

步骤 4 点击**确定**。

配置 NAT

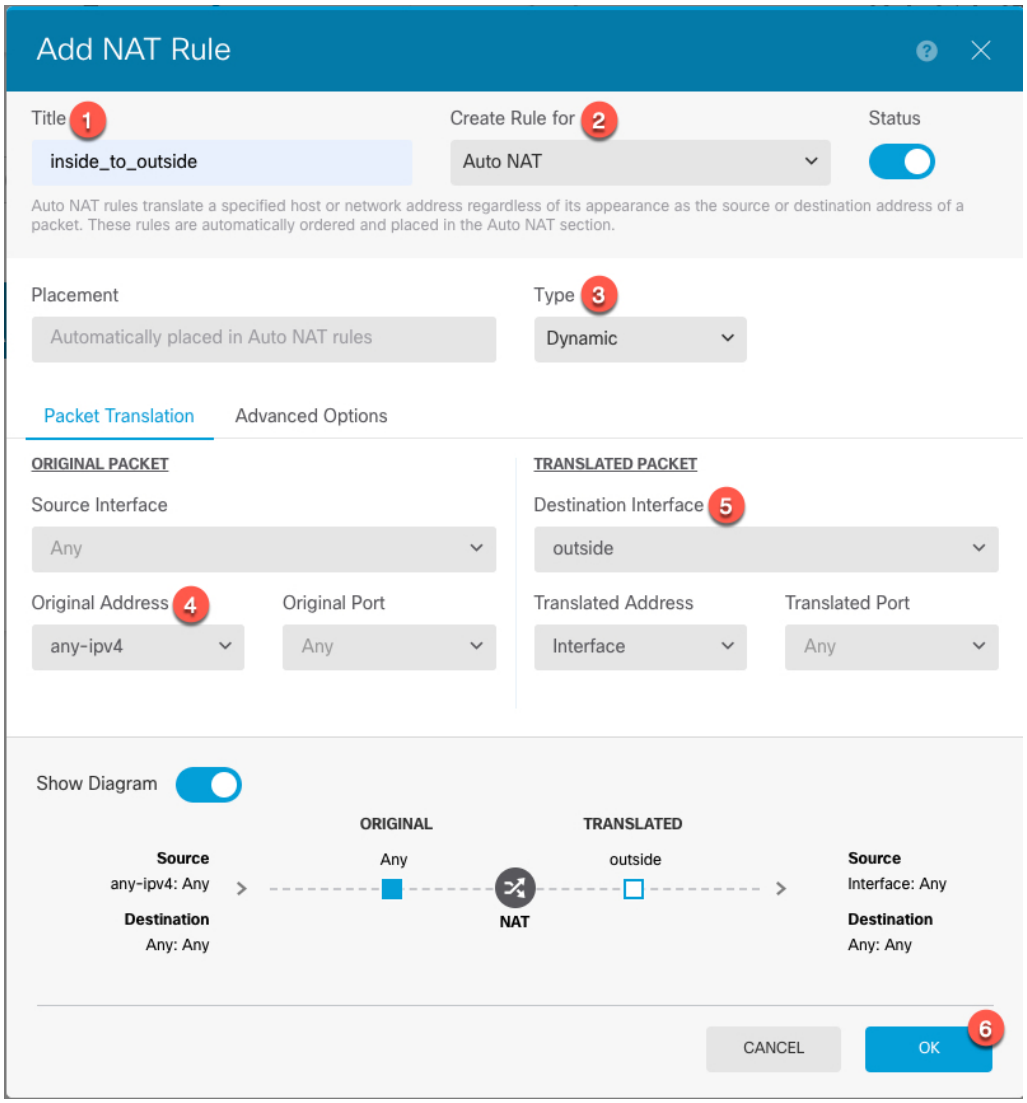
典型的 NAT 规则会将内部地址转换为外部接口 IP 地址上的端口。这类 NAT 规则称为接口端口地址转换 *(PAT)*。您不能将接口 PAT 用于 IPv6。

过程

步骤 1 点击**策略**，然后点击 **NAT**。

步骤 2 点击 + 或**创建 NAT 规则**。

步骤 3 配置基本规则选项：



a) 设置**标题**。
b) 选择**创建规则用于** > **自动 NAT**。
c) 选择**类型** > **动态**。

步骤 4 配置以下数据包转换选项：

a) 对于**原始数据包**，请将**原始地址**设置为**任意 ipv4**。

此规则将转换源自任何接口的所有 IPv4 流量。如果要限制接口或地址，可以选择特定的**源接口**，并为**原始地址**指定 IP 地址。

b) 对于**转换后的数据包**，请将**目标接口**设置为外部接口。

默认情况下，接口 IP 地址用于转换后的地址。

步骤 5 （可选） 点击**显示图表**以查看规则的直观示意图。

步骤 6 点击**确定**。

允许流量从内部传到外部

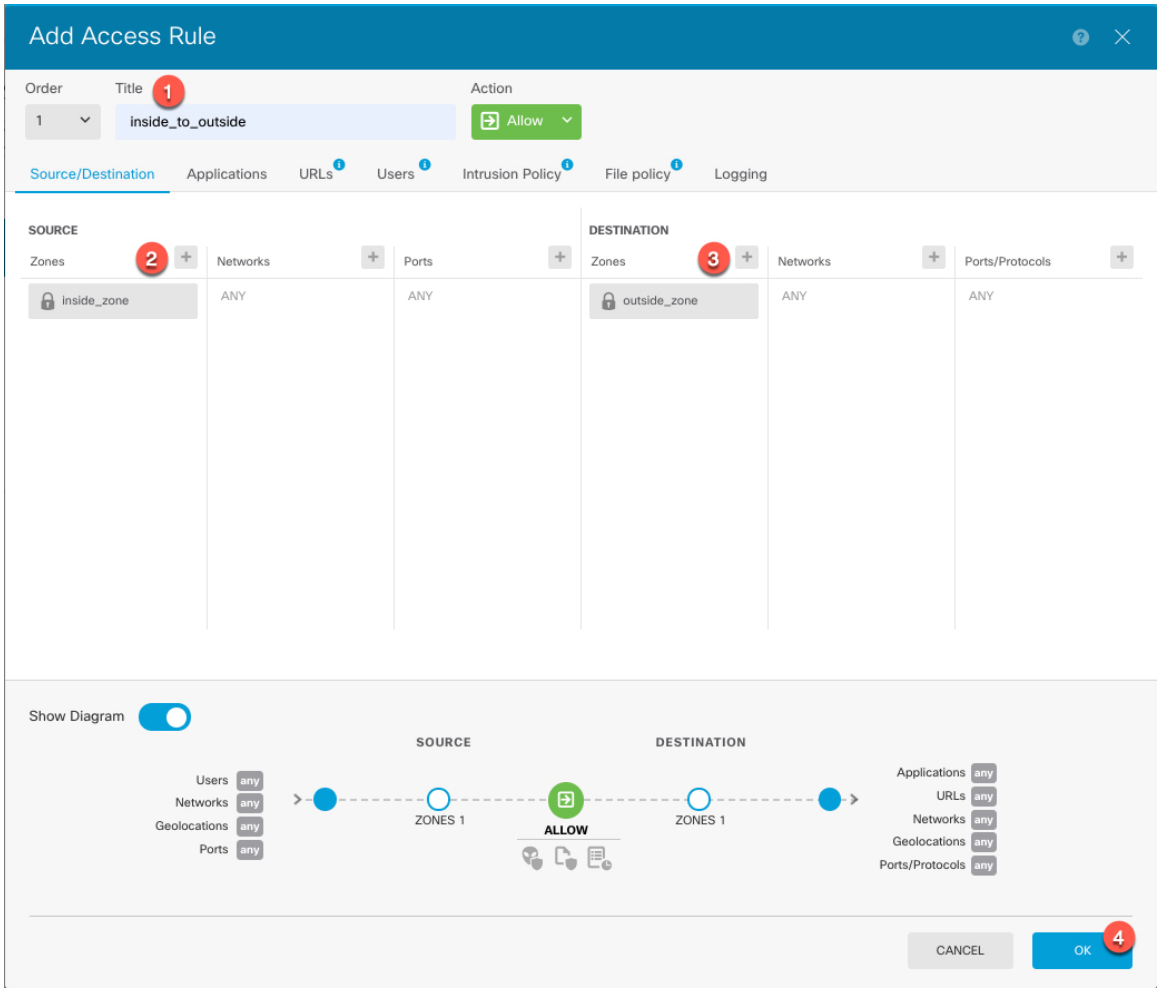
默认情况下，会在安全区域之间阻止流量。此程序介绍如何允许流量从内部传到外部。

过程

步骤 1 选择**策略** > **访问控制**。

步骤 2 点击 **+** 或**创建访问规则**。

步骤 3 配置基本规则选项：



a) 设置**标题**。

b) 对于**源**，请点击**区域** **+** 图标，然后选择内部区域。

c) 对于**目标**，请点击**区域** + 图标，然后选择外部区域。
d) （可选） 点击**显示图表**以查看规则的直观示意图。
e) 点击**确定**。

（可选）配置 DHCP 服务器

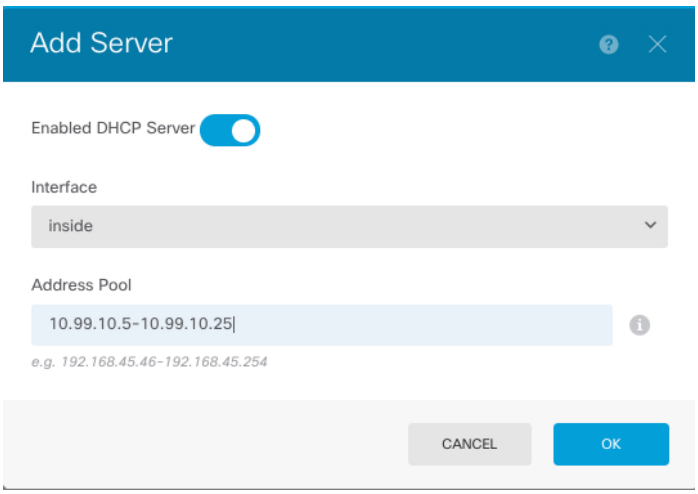
如果希望客户端使用 DHCP 从 威胁防御处获取 IP 地址，请启用 DHCP 服务器。

过程

步骤 1 点击**设备**，然后点击**系统设置** > **DHCP 服务器**链接。

步骤 2 点击 + 或**创建 DHCP 服务器**。

步骤 3 配置服务器属性。



a) 点击**启用 DHCP 服务器**滑块，使其显示为已启用状态 ( )。
b) 选择要在其上启用 DHCP 服务器的**接口**。

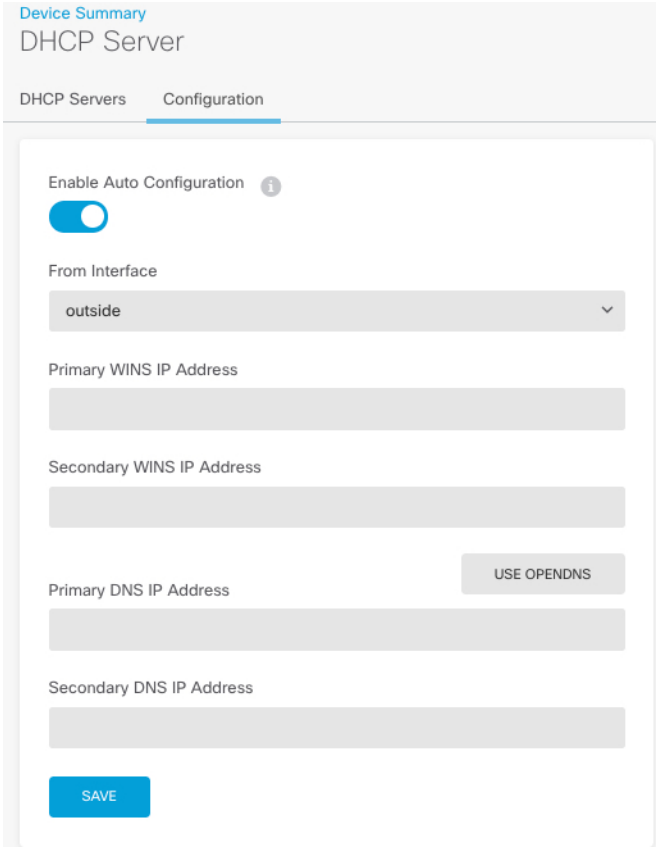
接口必须拥有静态 IP 地址；如果要在接口上运行 DHCP 服务器，则不能使用 DHCP 获取接口。

c) 输入**地址池**

该 IP 地址范围必须与所选接口位于同一子网上，并且不能包括接口本身的 IP 地址、广播地址或子网地址。

d) 点击**点击**。

步骤 4 （可选） 点击**配置**以配置自动配置和全局设置。



DHCP 自动配置使 DHCP 服务器能为 DHCP 客户端提供从运行于指定接口上的 DHCP 客户端获得的 DNS 服务器、域名和 WINS 服务器信息。通常，如果您是在使用 DHCP 获取地址，则会使用自动配置，但您可以选择通过 DHCP 获取其地址的任何接口。如果无法使用自动配置，可以手动定义所需的选项。

a) 点击**启用自动配置**滑块，使其显示为已启用状态 ( )。
b) 在 **From Interface**（从接口）下拉菜单中，选择希望客户端继承其服务器设置的接口。
c) 如果未启用自动配置，或者如果要覆盖任何一个自动配置的设置，请配置一个或多个全局选项。这些设置将发送到运行 DHCP 服务器的所有接口上的 DHCP 客户端。
d) 点击**保存**。

（可选）配置管理网关并允许在数据接口上进行管理

部署 威胁防御 时，配置了管理地址和外部网关。通过以下程序，可以将 威胁防御 配置为通过数据接口（而不是管理接口）在背板上发送管理流量。在这种情况下，如果位于直接连接的管理网络上，则仍可以管理 威胁防御，但发往任何其他网络的管理流量将在数据接口之外路由，而不是通过管理接口进行路由。

此外，默认情况下，只能通过管理接口（设备管理器 或 CLI 访问）来管理 威胁防御。通过以下程序，还可以在一个或多个数据接口上启用管理。请注意，管理接口网关不会影响数据接口上的 设备管理器 管理流量；在这种情况下，威胁防御 会使用常规路由表。

开始之前

根据配置接口，第 69 页配置数据接口。

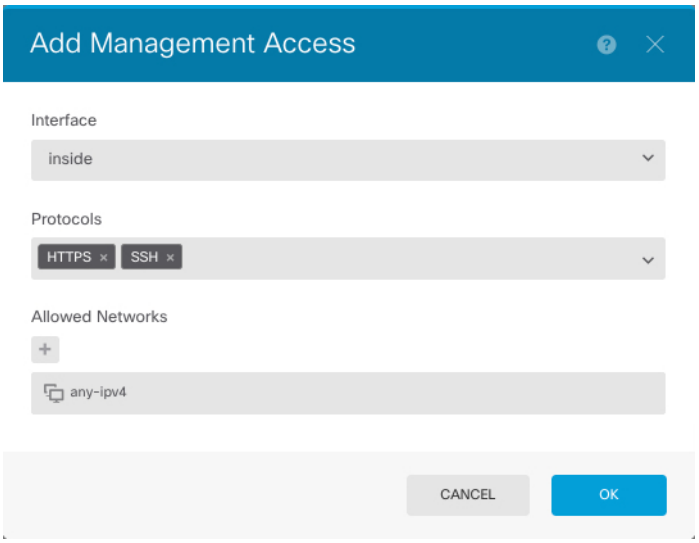
过程

步骤 1 允许从数据接口进行管理。

a) 点击**设备**，然后依次点击**系统设置** > **管理访问**链接。

b) 点击**数据接口**。

c) 点击 + 或**创建数据接口**，并为每个接口创建一个规则：



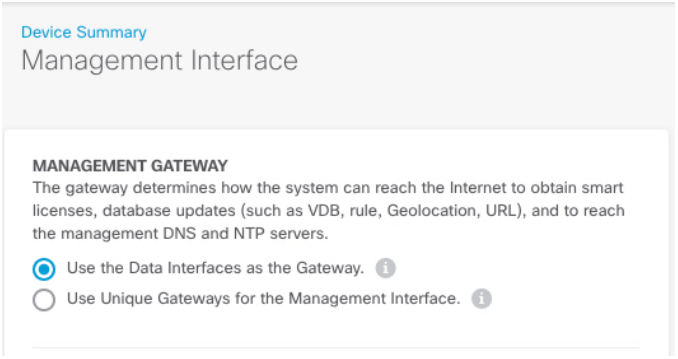
- **接口** - 选择要在其上允许管理访问的接口。
- **协议** - 选择规则是用于 HTTPS（端口 443）、SSH（端口 22）还是二者。
- **允许的网络** - 选择定义应该能够访问系统的 IPv4 或 IPv6 网络或主机的网络对象。要指定“任何”地址，请选择 **any-ipv4** (0.0.0.0/0) 和 **any-ipv6** (::/0)。

d) 点击**确定**。

步骤 2 将管理网关设置为使用数据接口。

a) 点击**设备**，然后依次点击**系统设置** > **管理接口**链接。

b) 选择**使用数据接口作为网关**。



c) 点击**保存**，阅读警告，然后点击**确定**。

部署配置

将配置更改部署到 威胁防御；在部署之前，您的所有更改都不会在设备上生效。

过程

步骤 1 点击网页右上角的**部署更改 (Deploy Changes)** 图标。

若有未部署的更改，系统会用圆点高亮显示。



“待处理更改”窗口显示配置的部署版本与待处理更改之间的对比信息。这些更改进行了颜色编码，表示出删除、添加或编辑的元素。有关每种颜色的解释，请参阅窗口中的说明。

步骤 2 如果您对所做的更改比较满意，可以点击**立即部署 (Deploy Now)** 立即启动作业。

窗口将显示部署正在进行。您可以关闭窗口，或等待部署完成。如果您在部署过程中关闭窗口，作业不会停止。您可以在任务列表或审核日志中查看结果。如果将窗口保持打开状态，请点击**部署历史记录 (Deployment History)** 链接查看结果。

访问威胁防御 CLI

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

过程

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

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

如果忘记密码，可以通过编辑 机箱管理器 中的逻辑设备来更改密码。

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

a) 连接到 安全引擎。

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

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

示例：

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

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) 连接到 威胁防御控制台。

connect ftd *name*

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

示例：

```
Firepower-module1> connect ftd FTD_Instance1

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

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

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

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

注释　　对于 6.3 之前的版本，输入 **Ctrl-a, d**。

d) 返回 FXOS CLI的管理引擎层。

要退出控制台：

1. 输入 **~**

   您将退出至 Telnet 应用。

2. 要退出 Telnet 应用，请输入：

   telnet>**quit**

要退出 Telnet 会话：

输入 **Ctrl-],**。

示例

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

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

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect ftd FTD_Instance1

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

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

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

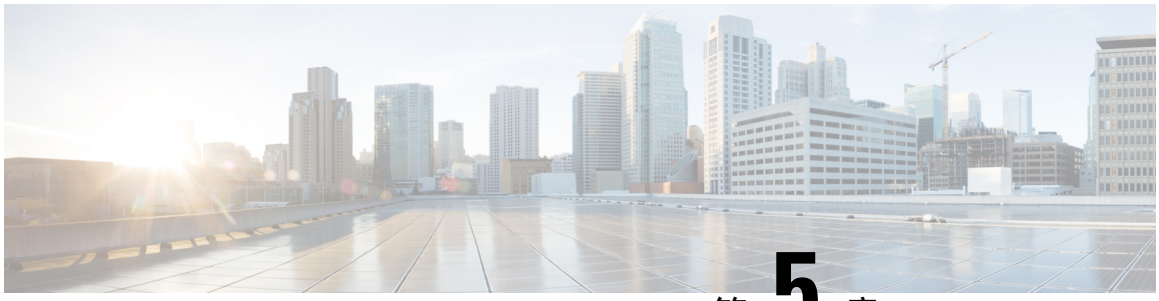
后续步骤

要继续配置 威胁防御，请参阅适用于您的软件版本的文档：导航思科 Firepower 文档。

有关使用设备管理器的信息，请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》。

使用设备管理器的威胁防御历史记录

功能名称	版本	功能信息
支持具有本地实例的设备管理器	6.5.0	现在，可以使用 设备管理器 部署本地实例。 新增/修改的屏幕： **逻辑设备** > **添加设备** **注释** 需要 FXOS 2.7.1。



第 5 章

使用 CDO 部署威胁防御

本章对您适用吗？

要查看所有可用的操作系统和管理器，请参阅哪种应用和管理器适合您？ ，第 1 页。本章适用于使用 思科防御协调器 (CDO) 的云交付 Cisco Secure Firewall Management Center 的 威胁防御。要通过设备管理器 功能使用 CDO，请参阅 CDO 文档。

注释 云交付 管理中心 支持 威胁防御 7.2 及更高版本。对于早期版本，您可以使用 CDO 的 设备管理器 功能。然而，设备管理器模式仅适用于已经使用该模式管理 威胁防御 的现有 CDO 用户。

每个 威胁防御 会控制、检查、监控和分析流量。CDO 通过一个 Web 界面提供集中管理控制台，可在运行中用来执行运营和管理任务，以保护您的本地网络。

关于防火墙

硬件可以运行 威胁防御 软件或 ASA 软件。在 威胁防御 和 ASA 之间切换需要您对设备进行重新映像。如果您需要不同于当前安装的软件版本，则还应重新映像。请参阅重新映像思科 ASA 或 Firepower 威胁防御设备。

防火墙会运行被称为 Secure Firewall eXtensible 操作系统 (FXOS) 的底层操作系统。防火墙不支持 FXOS Cisco Secure Firewall 机箱管理器；出于故障排除目的，仅支持受限的 CLI。有关详细信息，请参阅 适用于具备 Firepower 威胁防御 的 Firepower 1000/2100 和 Cisco Secure Firewall 3100 的思科 FXOS 故障排除指南。

隐私收集声明-防火墙不要求或主动收集个人身份信息。但是，您可以在配置中使用个人身份信息，例如用户名。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。

- 关于通过 CDO 管理威胁防御 ，第 86 页
- 端到端程序 ，第 86 页
- 获取许可证 ，第 87 页
- 登录 CDO ，第 89 页
- 使用激活向导激活设备 ，第 93 页
- 机箱管理器：添加威胁防御逻辑设备 ，第 94 页
- 配置基本安全策略 ，第 98 页
- 访问威胁防御和 FXOS CLI ，第 110 页

- 后续操作，第 112 页

关于通过 CDO 管理威胁防御

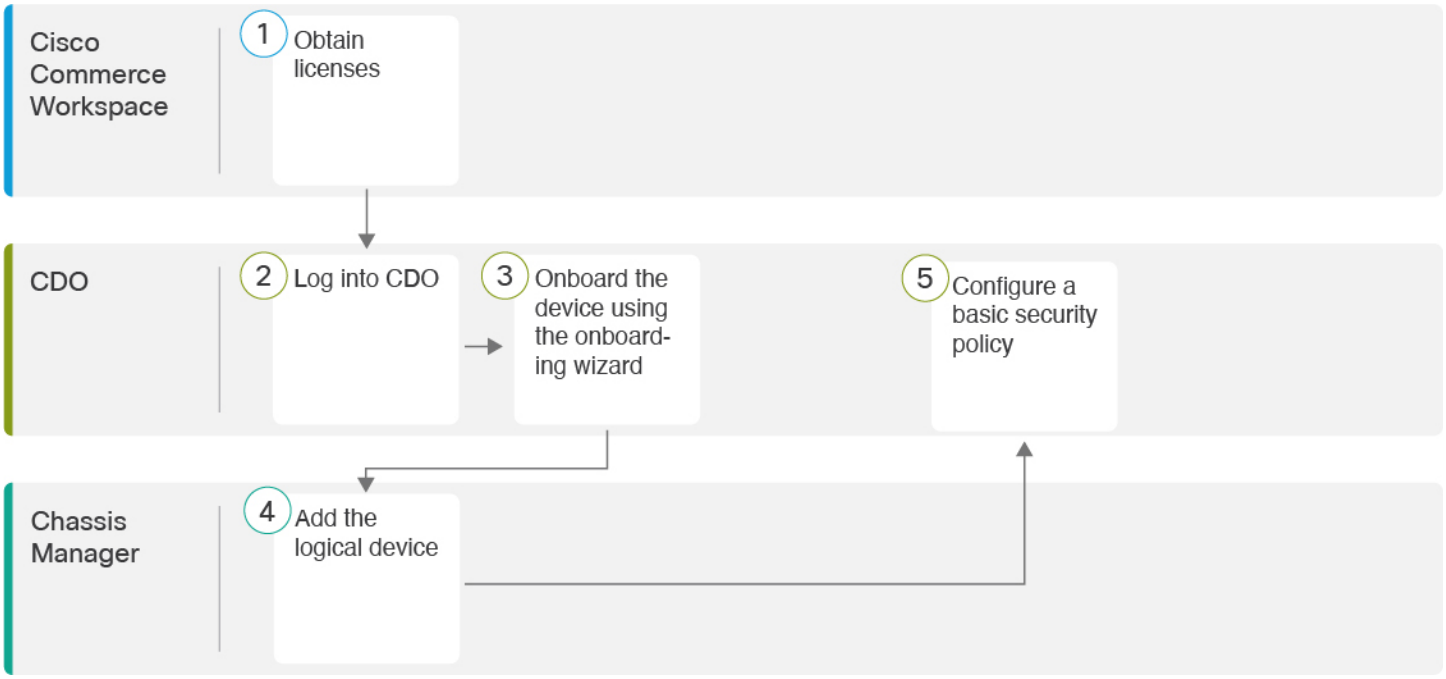
云交付的 管理中心 管理中心 提供许多与本地部署 管理中心 相同的功能，并且具有相同的外观。在将 CDO 用作主管理器时，您只能使用本地部署 管理中心 进行分析。本地部署 管理中心 不支持策略配置或升级。

注释 CDO 不支持容器实例或集群。

端到端程序

请参阅以下任务，使用激活向导在 CDO 中激活 威胁防御。

图 *10:* 端到端程序



1	Cisco Commerce Workspace	获取许可证，第 87 页。
2	CDO	登录 CDO，第 89 页。
3	CDO	使用激活向导激活设备，第 93 页。

4	机箱 管理器	机箱管理器：添加威胁防御逻辑设备，第 94 页。
5	CDO	配置基本安全策略，第 41 页。

获取许可证

所有许可证都由 CDO 提供给 威胁防御。您可以选择购买以下功能许可证：

- **IPS**胁-安全情报和下一代 IPS
- **恶意软件 防御**-恶意软件 防御
- **URL** - URL 过滤
- **Cisco Secure 客户端**-Secure Client Advantage、Secure Client Premier 或 Secure Client VPN Only
- **运营商** - Diameter、GTP/GPRS、M3UA、SCTP

有关思科许可的更详细概述，请访问 cisco.com/go/licensingguide

开始之前

- 拥有 智能软件管理器主帐户。

  如果您还没有帐户，请点击此链接以设置新帐户。通过智能软件管理器，您可以为组织创建一个主帐户。

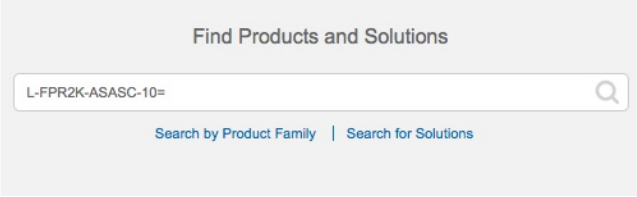
- 您的智能软件许可帐户必须符合强加密 (3DES/AES) 许可证的要求，才能使用某些功能（已使用导出合规性标志启用）。

过程

步骤 1 请确保智能许可帐户包含所需的可用许可证。

当您从思科或经销商那里购买设备时，您的许可证应该已链接到您的智能软件许可证帐户。但是，如果您需要自己添加许可证，则请使用Cisco Commerce Workspace上的 **Find Products and Solutions** 搜索字段。搜索以下许可证 PID：

图 *11:* 许可证搜索



注释　　如果未找到 PID，您可以手动将 PID 添加到订单中。

- IPS、恶意软件 防御和 URL 许可证组合：
  - L-FPR4112T-TMC=
  - L-FPR4115T-TMC=
  - L-FPR4125T-TMC=
  - L-FPR4145T-TMC=

  当您将上述 PID 之一添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：
  - L-FPR4112T-TMC-1Y
  - L-FPR4112T-TMC-3Y
  - L-FPR4112T-TMC-5Y
  - L-FPR4115T-TMC-1Y
  - L-FPR4115T-TMC-3Y
  - L-FPR4115T-TMC-5Y
  - L-FPR4125T-TMC-1Y
  - L-FPR4125T-TMC-3Y
  - L-FPR4125T-TMC-5Y
  - L-FPR4145T-TMC-1Y
  - L-FPR4145T-TMC-3Y
  - L-FPR4145T-TMC-5Y
- Cisco Secure 客户端-请参阅 思科安全客户端订购指南。
- 运营商许可证：
  - L-FPR4K-FTD-CAR=

步骤 2 如果尚未注册，请向智能软件管理器注册 CDO。

注册需要您在智能软件管理器中生成注册令牌。有关详细说明，请参阅 CDO 文档。

登录 CDO

CDO 使用 Cisco Secure Sign-On 作为身份提供商，并使用 Duo Security 进行多因素身份验证 (MFA)。CDO 需要 MFA，它为保护您的用户身份提供额外的一重保障。双因素身份验证（一种 MFA）需要两个部分或因素来确保登录 CDO 的用户身份真实。

第一个因素是用户名和密码，第二个是 Duo Security 按需生成的一次性密码 (OTP)。

建立 Cisco Secure Sign-On 凭证后，您可以从 Cisco Secure Sign-On 控制板登录 CDO。在 Cisco Secure Sign-On 控制板上，还可以登录任何其他支持的 Cisco 产品。

- 如果您有 Cisco Secure Sign-On 帐户，请提前跳转至 使用 Cisco Secure Sign-On 登录 CDO，第 91 页。
- 如果您没有 Cisco Secure Sign-On 帐户，请继续创建新的 Cisco Secure Sign-On 帐户，第 89 页。

创建新的 Cisco Secure Sign-On 帐户

初始登录工作流程分为四步。您需要完成所有四个步骤。

开始之前

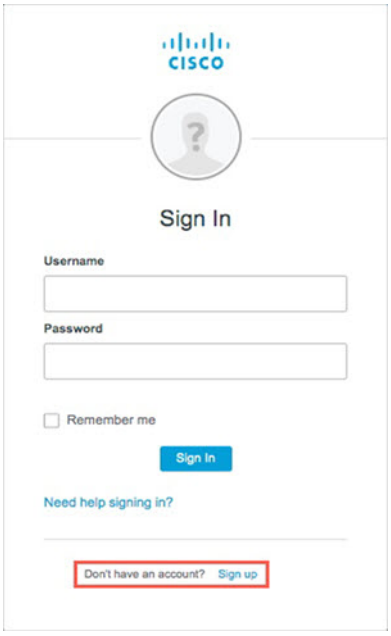
- **安装 DUO Security** - 我们建议您在手机上安装 Duo Security 应用。如果您对于如何安装 Duo 有疑问，请查看 Duo 双因素身份验证指南：注册指南。
- **时间同步** — 您要使用移动设备生成一次性密码。由于 OTP 是基于时间的，所以您的设备时钟与实时同步是非常重要的。请确保您的设备时钟设置为正确的时间。
- 使用当前版本的 Firefox 或 Chrome。

过程

步骤 1 注册新的 **Cisco Secure Sign-On** 帐户。

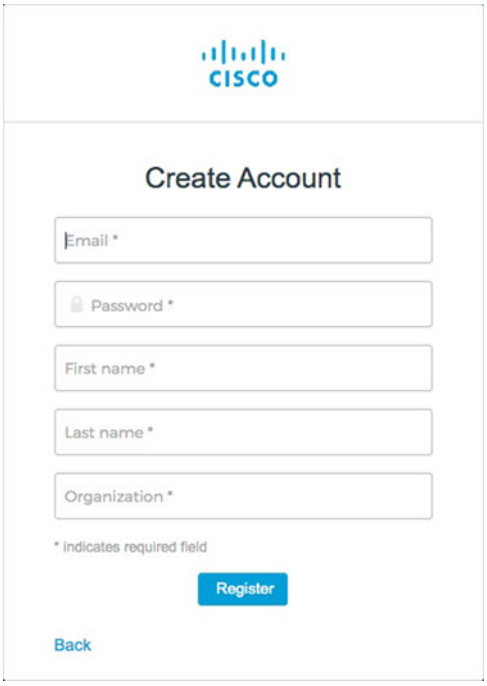
a) 浏览到 https://sign-on.security.cisco.com。
b) 在“登录”屏幕的底部，点击**注册**。

图 *12: Cisco SSO* 注册



c) 填写**创建帐户**对话框中的字段，然后点击**注册**。

图 *13:* 创建帐户



提示 输入您计划用于登录 CDO 的电子邮件地址，并添加组织名称以代表您的公司。

d) 点击**注册**后，Cisco会将验证电子邮件发送到您注册的地址。打开电子邮件，然后点击**激活帐户**。

步骤 2 使用 **Duo** 设置多因素身份验证。

a) 在**设置多因素身份验证**屏幕中，点击**配置**。

b) 点击**开始设置**，按照提示选择设备，然后验证该设备与您的帐户是否配对。

有关详细信息，请参阅 Duo 双因素身份验证指南：注册指南。如果您的设备上已经有 Duo 应用，您将收到此帐户的激活代码。Duo 支持一个设备上的多个帐户。

c) 在向导结束时，点击**继续登录**。

d) 通过双因素身份验证登录 Cisco Secure Sign-On。

步骤 3 （可选） **将 Google Authenticator 设置为附加身份验证器**。

a) 选择要与 Google Authenticator 配对的移动设备，然后点击**下一步**。

b) 按照安装向导中的提示设置 Google Authenticator。

步骤 4 配置 **Cisco Secure Sign-On** 帐户的帐户恢复选项。

a) 选择一个“忘记密码”问答。

b) 选择恢复电话号码以使用 SMS 重置帐户。

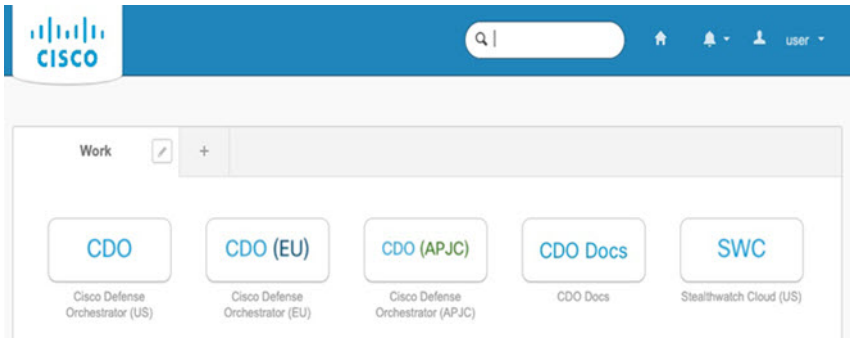
c) 选择安全图像。

d) 点击**创建帐户**。

现在，您会看到包含 CDO 应用图块的 Cisco Security Sign-On 控制板。您还可以看到其他应用图块。

提示 您可以在控制板上拖动图块以按您喜欢的顺序进行排序，创建选项卡对图块分组并重命名选项卡。

图 *14: Cisco SSO* 控制板



使用 Cisco Secure Sign-On 登录 CDO

登录 CDO 以激活和管理您的设备。

开始之前

Cisco Defense Orchestrator (CDO) 使用 Cisco Secure Sign-On 作为身份提供商，并使用 Duo Security 进行多因素身份验证 (MFA)。

- 要登录 CDO，必须先在 Cisco Secure Sign-On 中创建帐户，然后再使用 Duo 配置 MFA；请参阅创建新的 Cisco Secure Sign-On 帐户，第 89 页。
- 使用当前版本的 Firefox 或 Chrome。

过程

步骤 1 在网络浏览器中，导航到https://sign-on.security.cisco.com/。

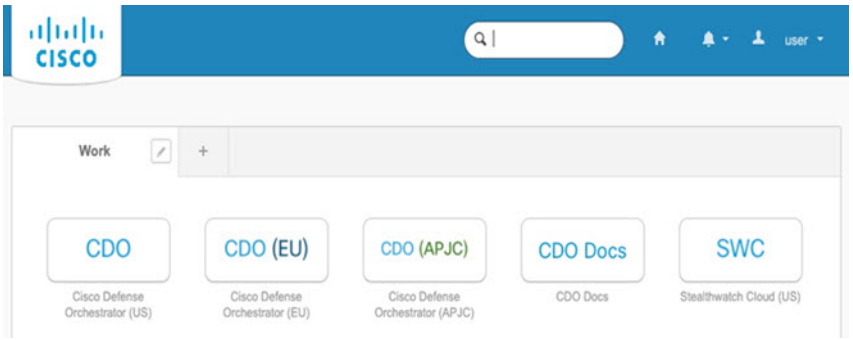
步骤 2 输入您的**用户名**和**密码**。

步骤 3 点击 **Log in**（登录）。

步骤 4 使用 Duo Security 接收另一个身份验证因素，然后确认登录。系统将确认您登录并显示 Cisco Secure Sign-On 控制板。

步骤 5 在 Cisco Secure Sign-On 控制板上点击适当的 CDO 图块。**CDO** 磁贴会带您转至 https://defenseorchestrator.com，**CDO (EU)** 磁贴会带您转至 https://defenseorchestrator.eu，而 **CDO (APJC)** 磁贴会带您转至 https://www.apj.cdo.cisco.com。

图 *15: Cisco SSO* 控制板



步骤 6 请点击身份验证器徽标以选择 **Duo Security** 或 **Google Authenticator**， 如果您已设置这两个身份验证器。

- 如果您在现有租户上已有用户记录，则将登录该租户。
- 如果您在若干租户上已有用户记录，则将能够选择要连接的 CDO 租户。
- 如果您在现有租户上尚无用户记录，将能够了解有关 CDO 的详细信息或申请试用帐户。

使用激活向导激活设备

通过 CDO 的激活向导使用 CLI 注册键激活威胁防御。

过程

步骤 1 在 CDO 导航窗格中，点击 **资产 (Inventory)**，然后点击蓝色加号按钮（ ）以便**激活**设备。

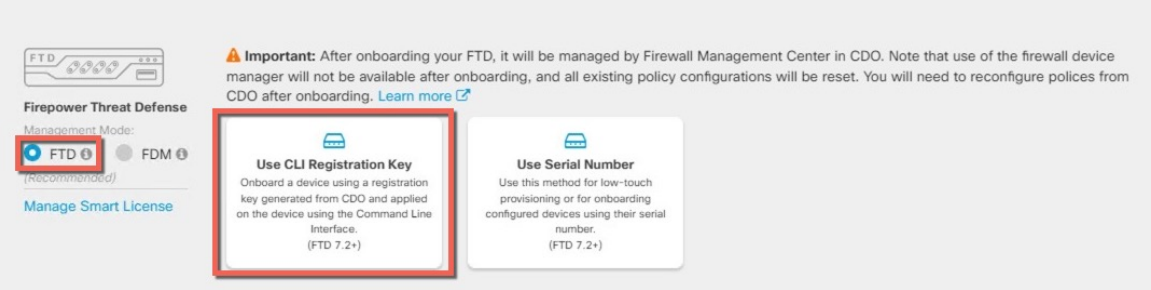
步骤 2 选择 **FTD** 磁贴。

步骤 3 在 **管理模式**下，确保选择 **FTD** 。

选择 **FTD** 作为管理模式后，您可以随时点击 **管理智能许可证** 注册或修改设备可用的现有智能许可证。请参阅获取许可证，第 87 页以查看可用的许可证。

步骤 4 选择**使用 CLI 注册密钥 (Use CLI Registration Key)** 作为载入方法。

图 *16:* 使用 *CLI* 注册密钥



步骤 5 输入**设备名称 (Device Name)**，然后点击**下一步 (Next)**。

步骤 6 对于**策略分配 (Policy Assignment)**，请使用下拉菜单为设备选择访问控制策略。如果未配置策略，请选择**默认访问控制策略 (Default Access Control Policy)**。

步骤 7 对于**订用许可证 (Subscription License)**，请点击**物理 FTD 设备 (Physical FTD Device)** 单选按钮，然后选中要启用的每个功能许可证。点击**下一步**。

步骤 8 对于 **CLI 注册密钥**，CDO 会使用注册密钥和其他参数来生成命令。您必须复制此命令并在 威胁防御 的初始配置中使用它。

configure manager add *cdo_hostname registration_key nat_id display_name*

在 机箱管理器 中，在部署逻辑设备时（请参阅机箱管理器：添加威胁防御逻辑设备，第 94 页），将命令的这一复制到**CDO 激活 (CDO Onboard)** 和**确认 CDO 激活 (Confirm CDO Onboard)** 字段中。

示例：

命令示例：

```
configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
```

步骤 9 在激活向导中点击**下一步 (Next)**，以便开始注册设备。

步骤 10 （可选）向设备添加标签，以帮助对**资产 (Inventory)** 页面进行排序和过滤。输入标签，然后选择蓝色加号按钮（）。标签会在设备于 CDO 中激活后应用到设备。

下一步做什么

在**资产 (Inventory)** 页面中，选择您刚刚载入的设备，然后选择位于右侧的**管理 (Management)** 窗格下列出的任何选项。

机箱管理器：添加威胁防御逻辑设备

您可以从Firepower 4100将威胁防御部署为独立的本地实例。CDO 不支持容器实例或集群。

您可以通过此程序配置逻辑设备特性，包括应用程序使用的引导程序配置。

开始之前

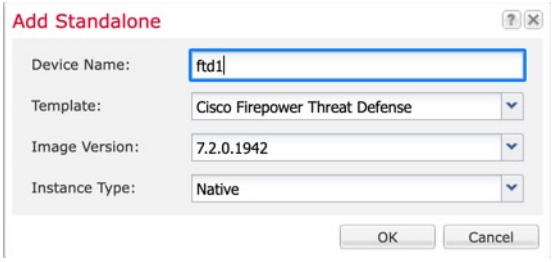
- 配置与 威胁防御一起使用的管理接口；请参阅配置接口，第 20 页。管理接口是必需的。您可以稍后从数据接口启用管理；但必须将管理接口分配给逻辑设备，即使您不打算在启用数据管理后使用该接口。请注意，此管理接口与仅用于机箱管理的机箱管理端口（并且该端口在**接口**选项卡的顶部显示为 **MGMT**）不同。
- 您还必须至少配置一个数据接口。
- 收集以下信息：
  - 此设备的接口 ID
  - 管理接口 IP 地址和网络掩码
  - 网关 IP 地址
  - CDO 生成的 CDO 主机名、注册密钥和 NAT ID。请参阅使用激活向导激活设备，第 93 页。
  - DNS 服务器 IP 地址

过程

步骤 1 在 机箱管理器中，选择**逻辑设备**。

步骤 2 点击**添加** > **独立设备**，并设置以下参数：

图 *17:* 添加独立设备



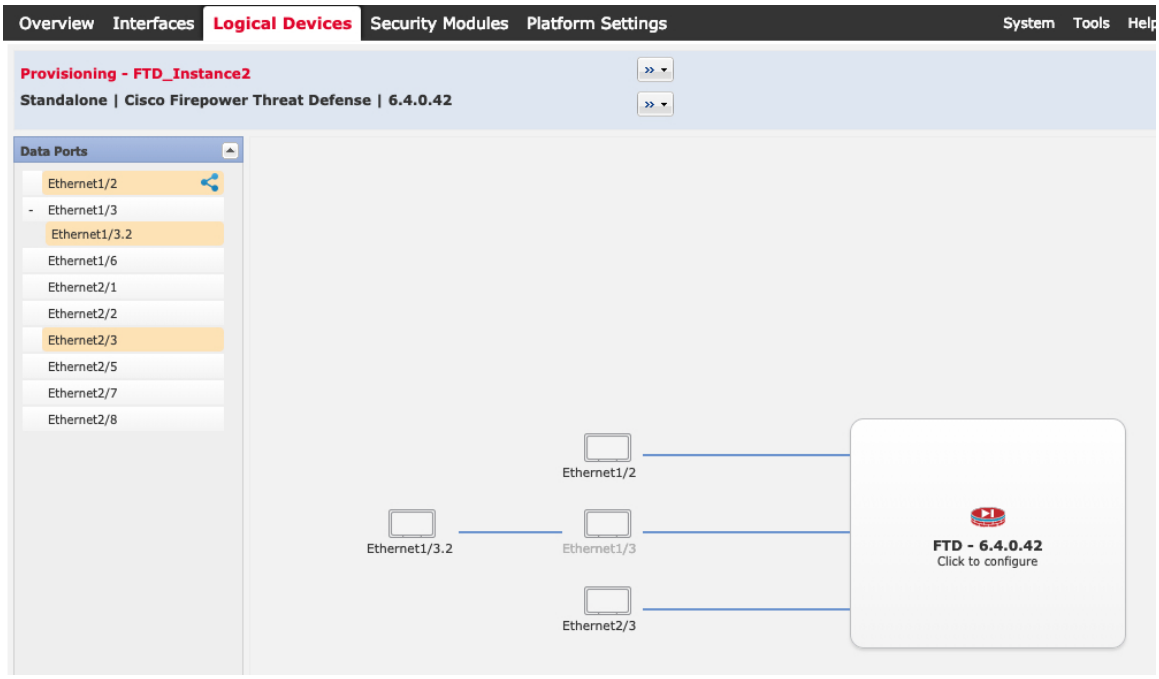
a) 提供**设备名称**。

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

b) 对于**模板**，请选择 **Cisco Firepower 威胁防御**。
c) 选择**映像版本**。
d) 选择**实例类型：本地**。
e) 点击**确定 (OK)**。

屏幕会显示调配 - 设备名称窗口。

步骤 3 展开**数据端口**区域，然后点击要分配给设备的每个接口。



仅可分配先前在**接口**页面上启用的数据接口。稍后您需要在CDO中启用和配置这些接口，包括设置IP 地址。

具有硬件旁路功能的端口使用以下图标显示：。对于某些接口模块，仅可启用用于内联集接口的硬件旁路功能。硬件绕行确保流量在断电期间继续在接口对之间流动。在软件或硬件发生故障时，此功能可用于维持网络连接性。如果您未同时分配一个硬件旁路对中的两个接口，则会收到一条警

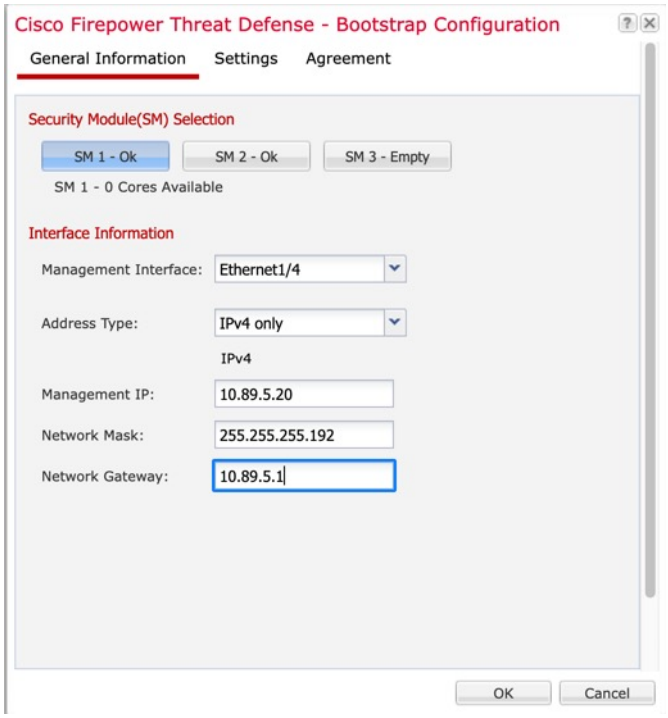
告消息，确认您是故意这样分配。您不需要使用硬件旁路功能，因此如果您愿意，可以分配单个接口。

步骤 4 点击屏幕中心的设备图标。

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

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

图 *18:* 常规信息



a) 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。

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

c) 配置**管理 IP** 地址。

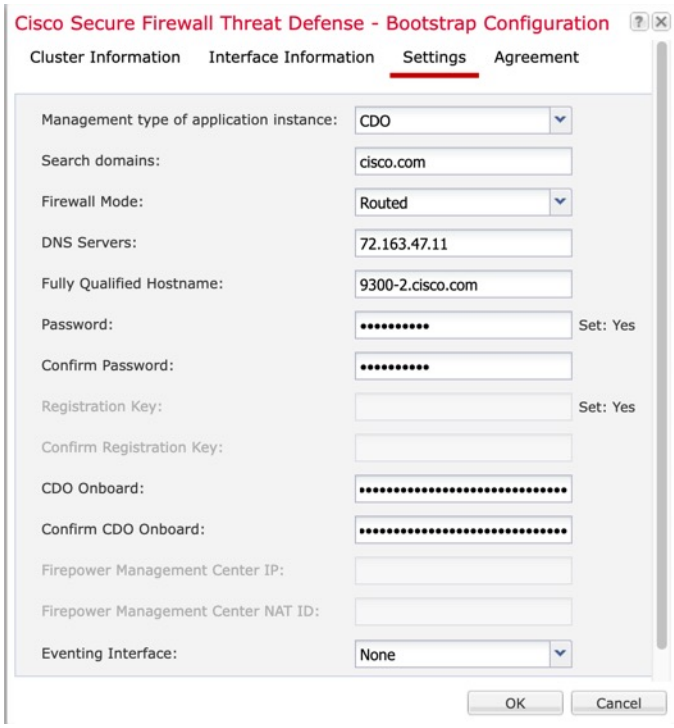
设置用于此接口的唯一 IP 地址。

d) 输入**网络掩码**或**前缀长度**。

e) 输入**网络网关**地址。

步骤 6 在**设置**选项卡上，完成下列操作：

图 *19:* 设置



a) 在**应用实例的管理类型 (Management type of application instance)** 下拉列表中，选择 **CDO**。
b) 输入逗号分隔列表形式的**搜索域**。
c) 选择**防火墙模式：透明**或**路由式**。

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

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

d) 输入逗号分隔列表形式的 **DNS 服务器**。

例如，如果指定 管理中心 主机名，则 威胁防御 使用 DNS。

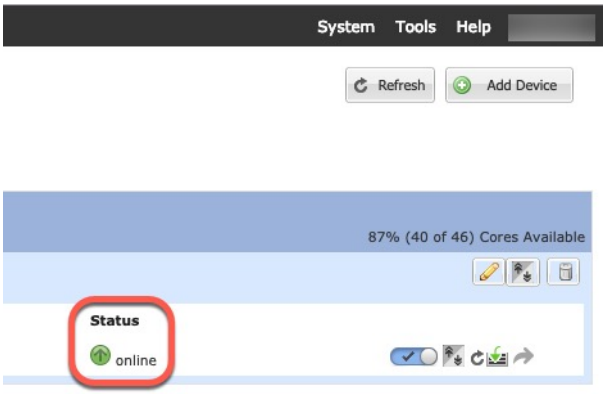
e) 输入 威胁防御 的**完全限定主机名**。
f) 输入供威胁防御管理员用户用于 CLI 访问的**密码**。
g) 将 CDO 生成的命令复制到**CDO 激活 (CDO Onboard)** 和**确认 CDO 激活 (Confirm CDO Onboard)** 字段中。
h) CDO 不支持单独的**事件接口**，因此将忽略此设置。

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

步骤 8 点击**确定 (OK)** 关闭配置对话框。

步骤 9 点击**保存 (Save)**。

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



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 41 页。
2	配置 DHCP 服务器， 第 45 页。
3	添加默认路由， 第 46 页。
4	配置 NAT， 第 47 页。
5	允许流量从内部传到外部， 第 50 页。
6	部署配置， 第 51 页。

配置接口

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

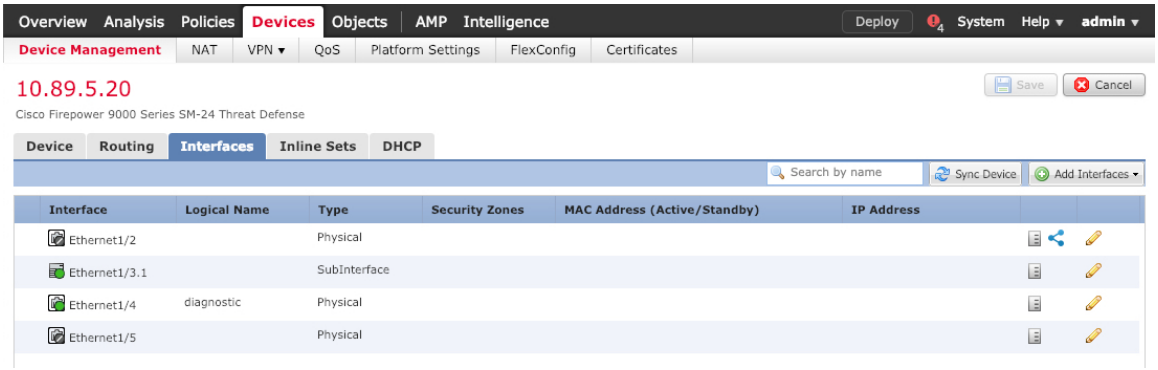
典型的边缘路由情况是通过 DHCP 从 ISP 获取外部接口地址，同时在内部接口上定义静态地址。

以下示例使用 DHCP 在接口内部配置了一个路由模式（含静态地址），并在接口外部配置了一个路由模式。

过程

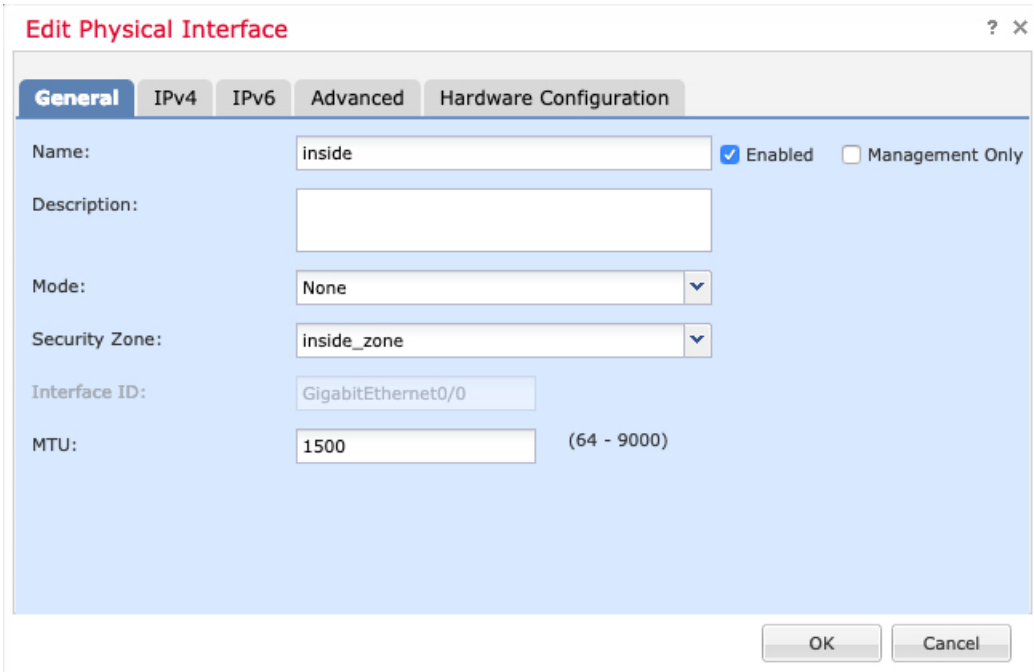
步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**，然后点击防火墙的**编辑**（ ）。

步骤 2 点击**接口 (Interfaces)**。



步骤 3 点击要用于内部的接口的**编辑**（ ）。

此时将显示**一般 (General)** 选项卡。



a) 输入长度最大为 48 个字符的 **Name**。

例如，将接口命名为 **inside**。

b) 选中 **Enabled** 复选框。

c) 将 **Mode** 保留为 **None**。

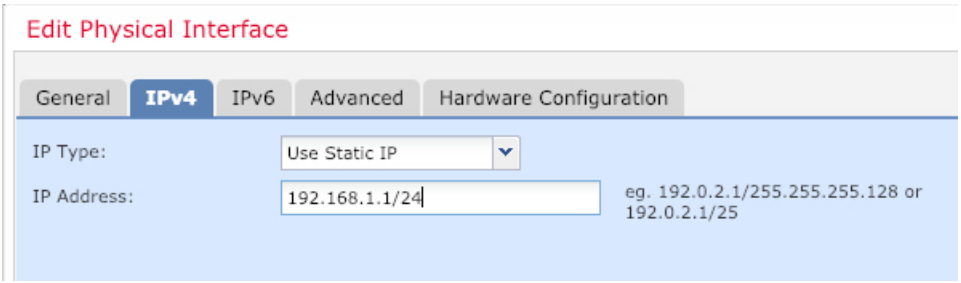
d) 从**安全区域 (Security Zone)** 下拉列表中选择一个现有的内部安全区域，或者点击**新建 (New)** 添加一个新的安全区域。

例如，添加一个名为 **inside_zone** 的区域。必须将每个接口分配给安全区域和/或接口组。每个接口只能属于一个安全区域，但可以同时属于多个接口组。您可以根据区域或组应用安全策略。例如，您可以将内部接口分配到内部区域，而将外部接口分配到外部区域。然后可以配置访问控制策略，允许流量从内部传到外部，但不允许从外部传入内部。大多数策略仅支持安全区域；您可以在 NAT 策略、预过滤器策略和 QoS 策略中使用区域或接口组。

e) 点击 **IPv4** 和/或 **IPv6** 选项卡。

- **IPv4** - 从下拉列表中选择**使用静态 IP (Use Static IP)**，然后以斜杠表示法输入 IP 地址和子网掩码。

  例如，输入 **192.168.1.1/24**

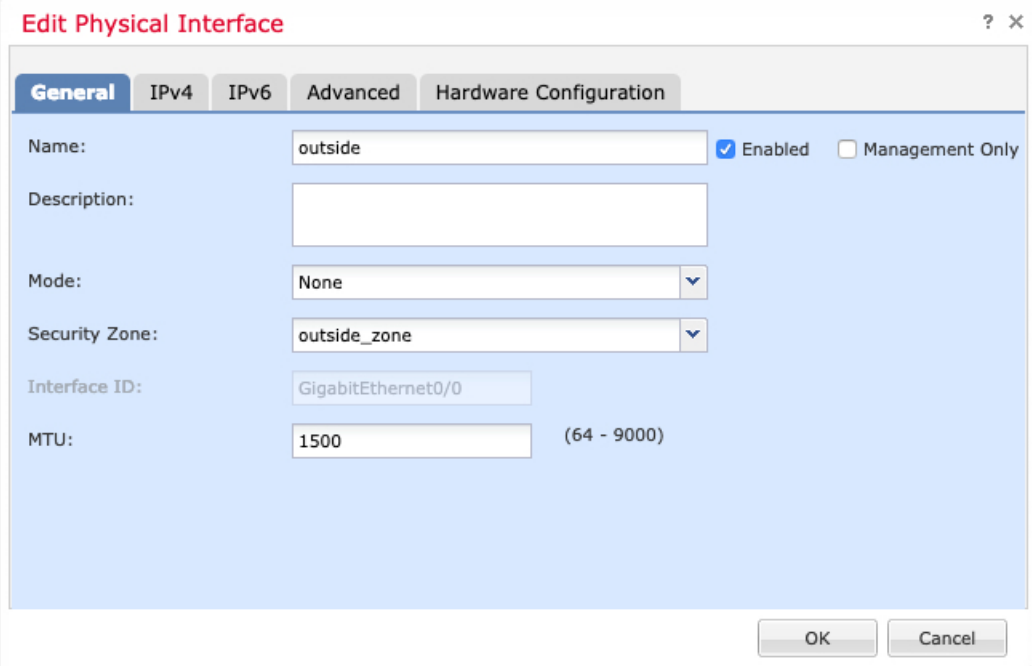


- **IPv6** - 为无状态自动配置选中**自动配置 (Autoconfiguration)** 复选框。

f) 点击**确定 (OK)**。

步骤 4 点击要用于外部的接口的 **编辑**（ ）。

此时将显示**一般 (General)** 选项卡。



注释 如果您为此接口预配置了管理器访问，则该接口就已经命名、启用和寻址。您不应更改任何这些基本设置，因为这样做会中断管理中心管理连接。您仍然可以在此屏幕上为直通流量策略配置安全区域。

a) 输入长度最大为 48 个字符的 **Name**。

例如，将接口命名为 **outside**。

b) 选中 **Enabled** 复选框。

c) 将 **Mode** 保留为 **None**。

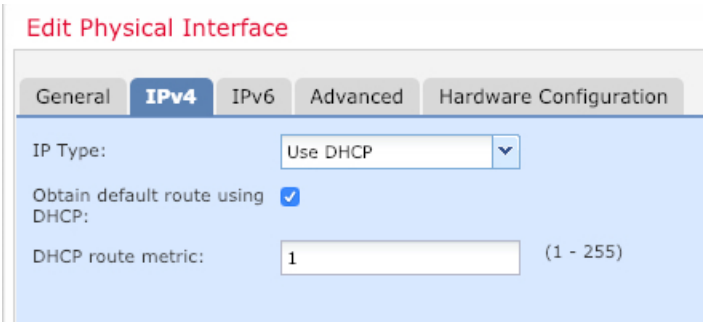
d) 从**安全区域 (Security Zone)** 下拉列表中选择一个现有的外部安全区域，或者点击**新建 (New)** 添加一个新的安全区域。

例如，添加一个名为 **outside_zone** 的区域。

e) 点击 **IPv4** 和/或 **IPv6** 选项卡。

- **IPv4** - 选择**使用 DHCP (Use DHCP)**，然后配置以下选填参数：
  - **使用 DHCP 获取默认路由 (Obtain default route using DHCP)** - 从 DHCP 服务器获取默认路由。

- **DHCP 路由指标 (DHCP route metric)** - 分配到所获悉路由的管理距离，介于 1 和 255 之间。获悉的路由的默认管理距离为 1。



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

f) 点击**确定 (OK)**。

步骤 5 点击**保存**。

配置 DHCP 服务器

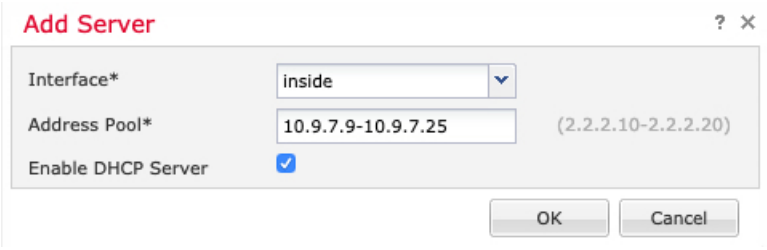
如果希望客户端使用 DHCP 从 威胁防御处获取 IP 地址，请启用 DHCP 服务器。

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**，然后点击设备的**编辑**（ ）。

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

步骤 3 在**服务器 (Server)** 页面上点击**添加 (Add)**，然后配置以下选项：



- **接口 (Interface)** - 从下拉列表中选择接口。
- **地址池 (Address Pool)** - DHCP 服务器使用的 IP 地址的范围（从最低到最高）。IP 地址范围必须与选定接口位于相同的子网上，且不能包括接口自身的 IP 地址。
- **启用 DHCP 服务器 (Enable DHCP Server)** - 在所选接口上启用 DHCP 服务器。

步骤 4 点击**确定 (OK)**。

步骤 5 点击保存。

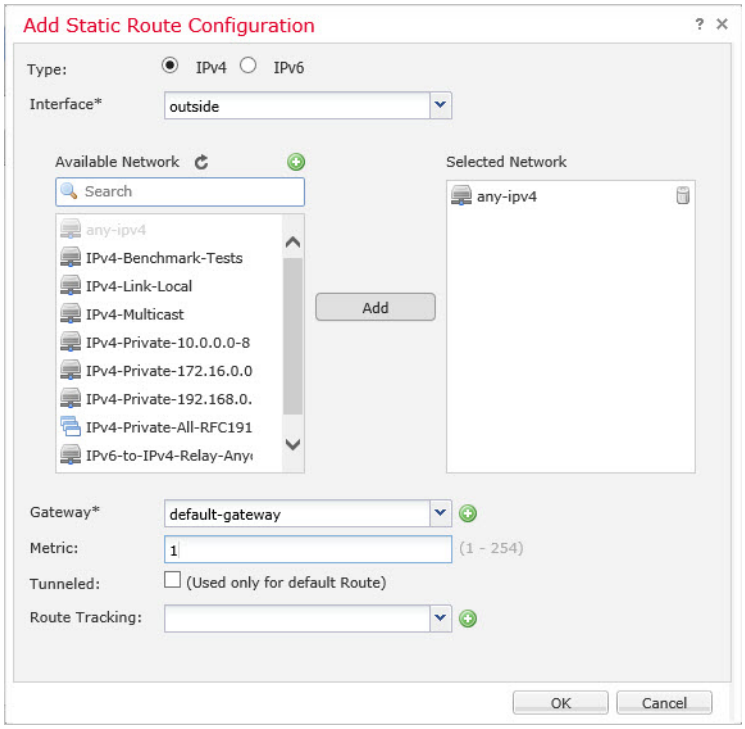
添加默认路由

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

过程

步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**，然后点击设备的**编辑**（ ）。

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

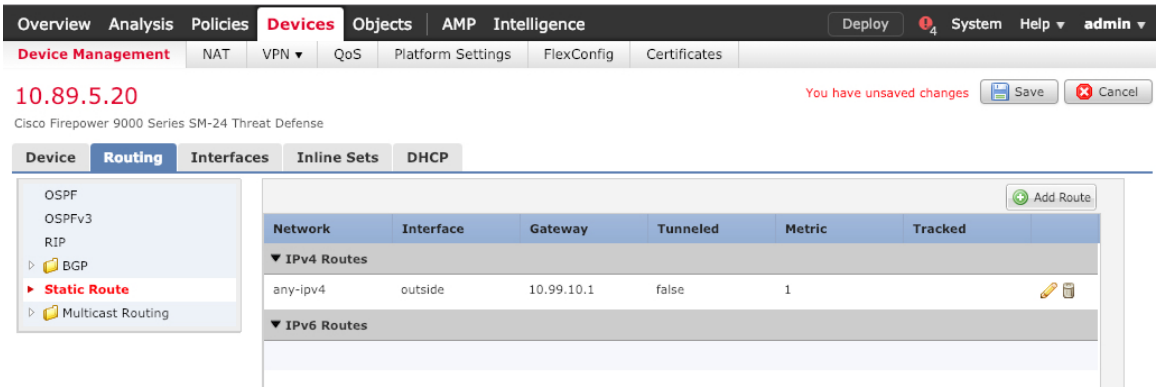


- **类型 (Intrusion)** - 根据要添加静态路由的类型，点击 **IPv4** 或 **IPv6** 单选按钮。
- **接口 (Interface)** - 选择出口接口；通常是外部接口。
- **Available Network** - 为 IPv4 默认路由选择 **any-ipv4**，为 IPv6 默认路由选择 **any-ipv6**，然后点击 **Add** 将其移至 **Selected Network** 列表。
- **网关 (Gateway)** 或 **IPv6 网关 (IPv6 Gateway)** - 输入或选择作为此路由的下一个跃点的网关路由器。您可以提供 IP 地址或网络/主机对象。

- **指标 (Metric)** - 输入到目标网络的跃点数。有效值范围为 1 到 255；默认值为 1。

步骤 3 点击**确定 (OK)**。

路由即已添加至静态路由表。



步骤 4 点击**保存**。

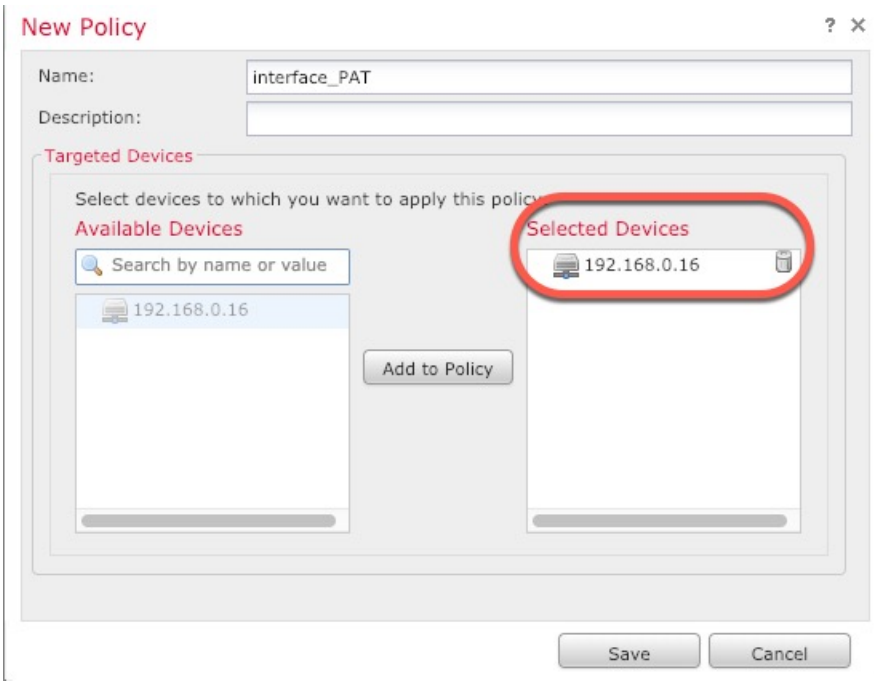
配置 NAT

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

过程

步骤 1 选择**设备 (Devices)** > **NAT**，然后点击**新策略 (New Policy)** > **威胁防御 NAT (Threat Defense NAT)**。

步骤 2 为策略命名，选择要使用策略的设备，然后点击**Save**。



策略即已添加 管理中心。您仍然需要为策略添加规则。

步骤 3 点击**添加规则 (Add Rule)**。

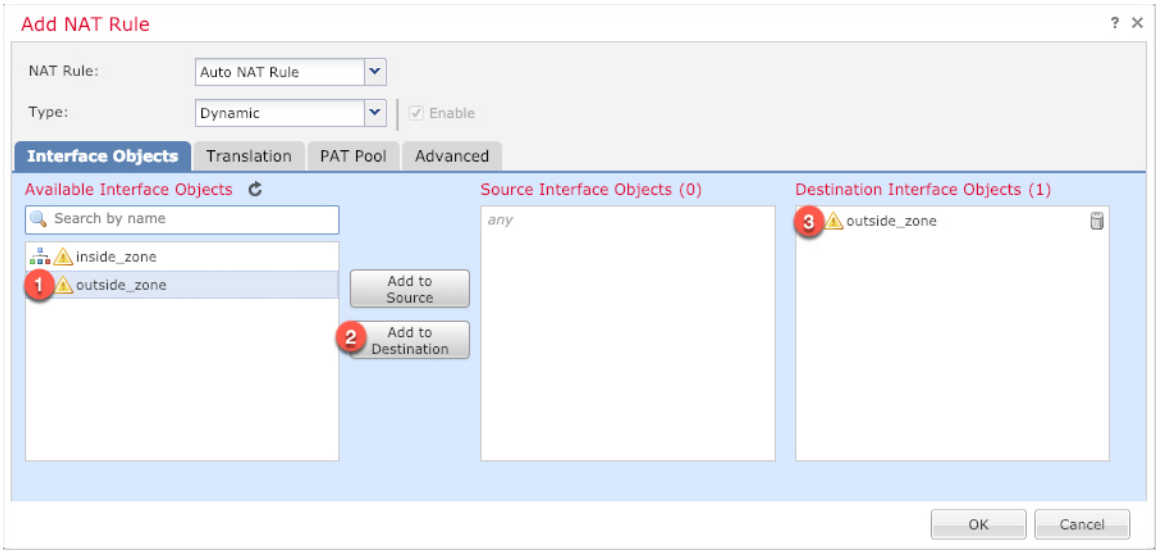
Add NAT Rule 对话框将显示。

步骤 4 配置基本规则选项：

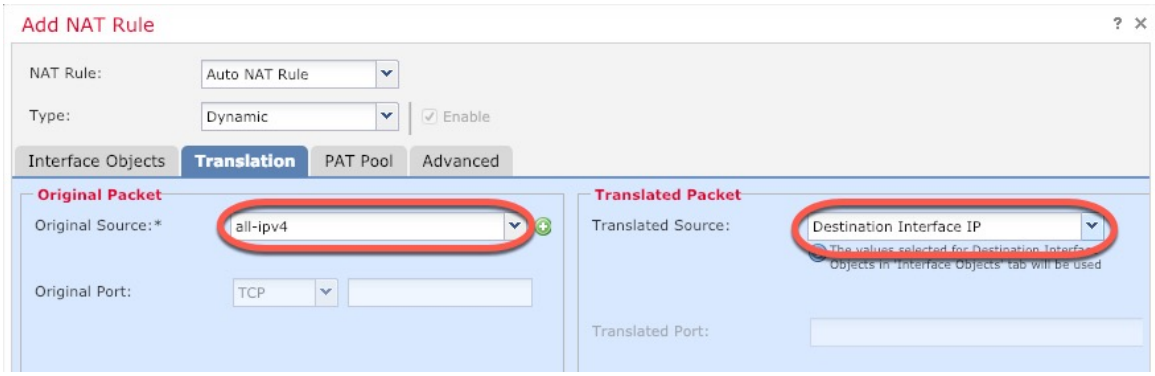


- **NAT 规则 (NAT Rule)** - 选择**自动 NAT 规则 (Auto NAT Rule)**。
- **类型 (Type)** - 选择**动态 (Dynamic)**。

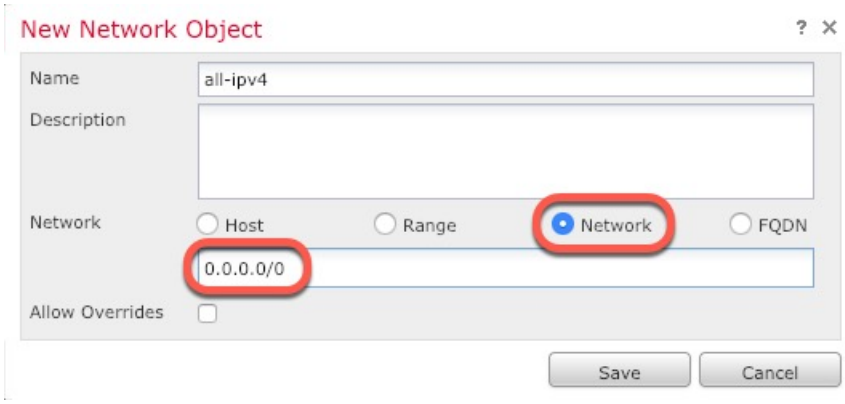
步骤 5 在 **Interface Objects** 页面，将 **Available Interface Objects** 区域中的外部区域添加到 **Destination Interface Objects** 区域。



步骤 6 在**转换 (Translation)** 页面上配置以下选项：



- **原始源** - 点击**添加**（+）为所有 IPv4 流量添加网络对象 (0.0.0.0/0)。

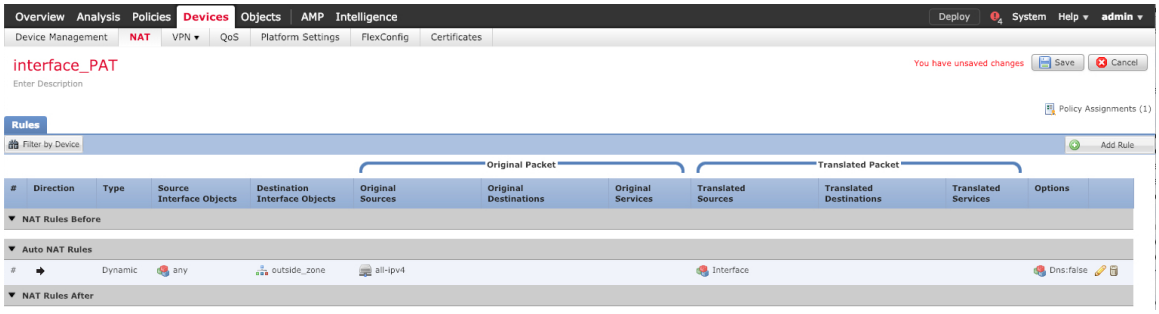


注释　您不能使用系统定义的 **any-ipv4** 对象，因为自动 NAT 规则在对象定义过程中添加 NAT，并且您无法编辑系统定义的对象。

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

步骤 7 点击**保存 (Save)** 以添加规则。

规则即已保存至 **Rules** 表。



步骤 8 点击 **NAT** 页面上的**保存 (Save)** 以保存更改。

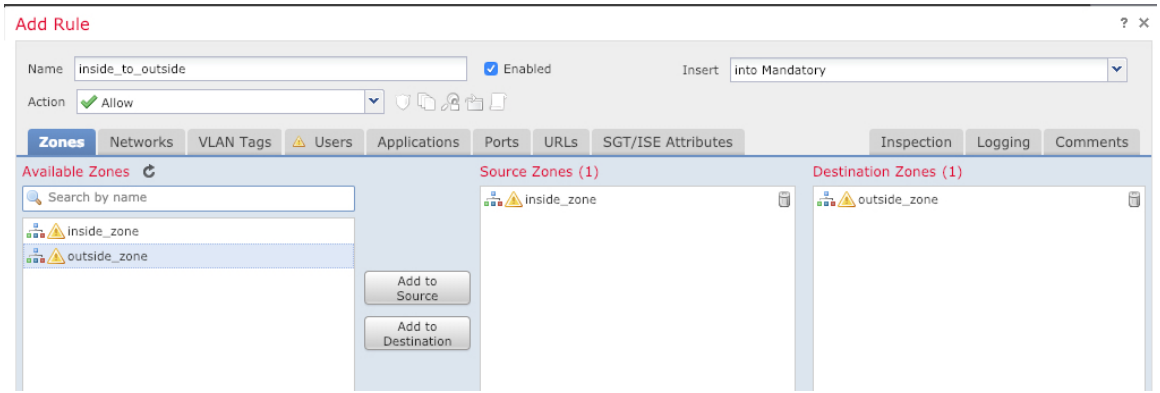
允许流量从内部传到外部

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

过程

步骤 1 选择**策略 (Policy)** > **访问策略 (Access Policy)** > **访问策略 (Access Policy)**，然后点击分配给 威胁防御 的访问控制策略的 **编辑**（ ）。

步骤 2 点击**添加规则 (Add Rule)** 并设置以下参数：



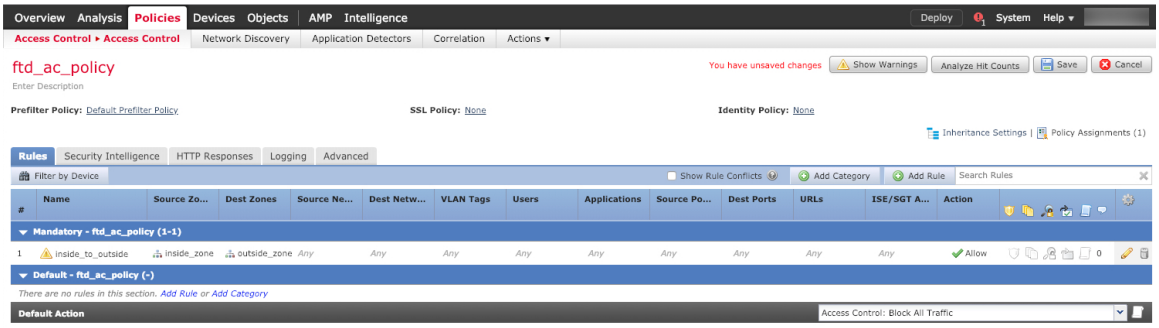
- **名称 (Name)** - 为此规则命名，例如 **inside_to_outside**。
- **源区域 (Source Zones)** - 从**可用区域 (Available Zones)** 中选择内部区域，然后点击**添加到源 (Add to Source)**。

- 目标区域 **(Destination Zones)** - 从可用区域 **(Available Zones**） 中选择外部区域，然后点击添加到目标 **(Add to Destination)**。

其他设置保留原样。

步骤 3 点击添加 **(Add)**。

规则即已添加至 **Rules** 表。



步骤 4 点击保存。

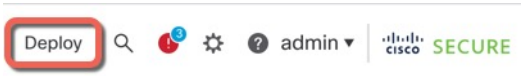
部署配置

将配置更改部署到 威胁防御；在部署之前，您的所有更改都不会在设备上生效。

过程

步骤 1 点击右上方的部署 **(Deploy)**。

图 *20:* 部署



步骤 2 点击全部部署 **(Deploy All)** 以部署到所有设备，或点击高级部署 **(Advanced Deploy)** 以部署到选择的设备。

图 *21:* 全部部署

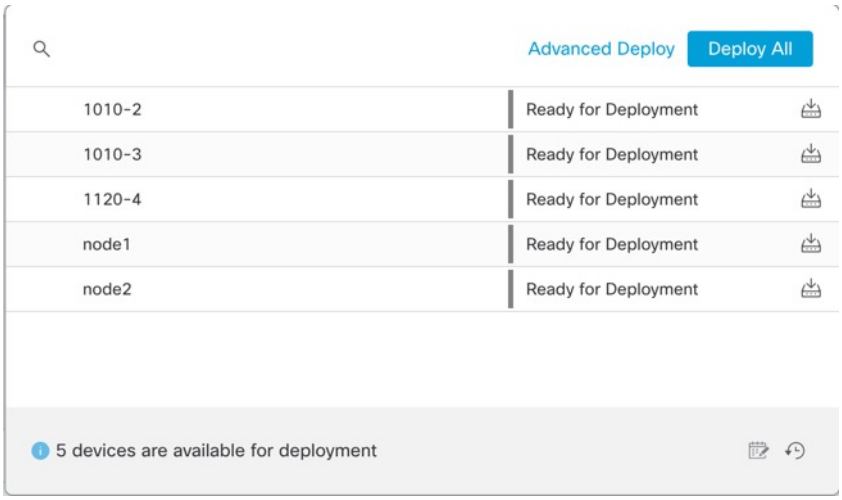
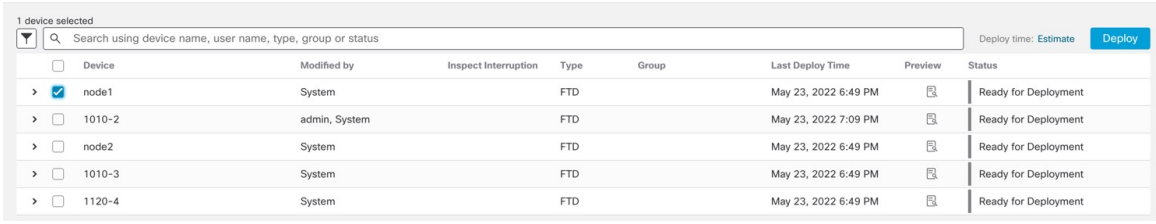
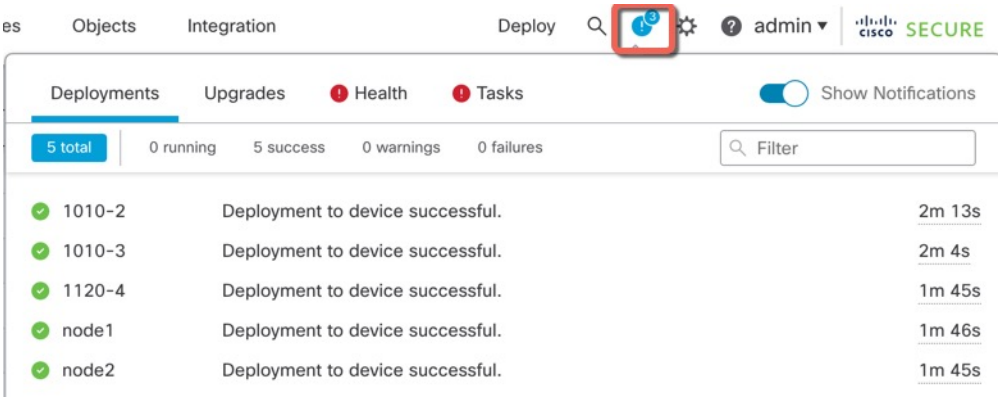


图 *22:* 高级部署



步骤 3 确保部署成功。点击菜单栏中**部署 (Deploy)** 按钮右侧的图标可以查看部署状态。

图 *23:* 部署状态



访问威胁防御和 FXOS CLI

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

过程

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

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

如果忘记密码，可以通过编辑 机箱管理器 中的逻辑设备来更改密码。

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

a) 连接到 安全引擎。

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

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

示例：

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

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) 连接到 威胁防御控制台。

connect ftd *name*

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

示例：

```
Firepower-module1> connect ftd FTD_Instance1

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

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

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

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

注释　　对于 6.3 之前的版本，输入 **Ctrl-a, d**。

d) 返回 FXOS CLI的管理引擎层。

要退出控制台：

1. 输入 **~**

   您将退出至 Telnet 应用。

2. 要退出 Telnet 应用，请输入：

   telnet>**quit**

要退出 Telnet 会话：

输入 **Ctrl-],**。

示例

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

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

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect ftd FTD_Instance1

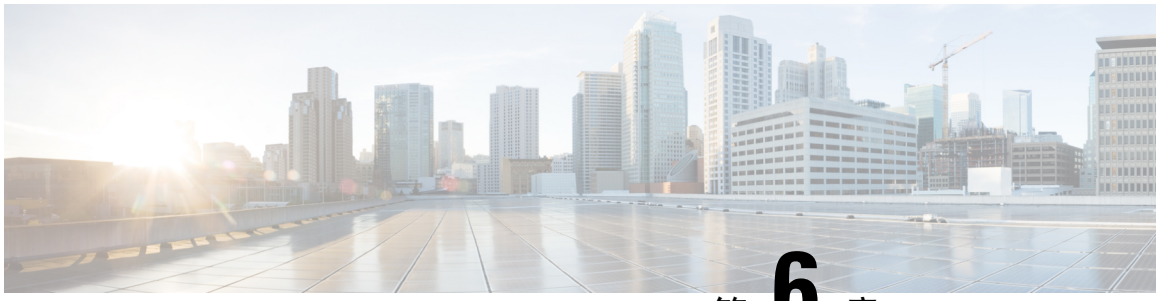
============================ ATTENTION ==============================
You are connecting to ftd from a serial console. Please avoid
executing any commands which may produce large amount of output.
Otherwise, data cached along the pipe may take up to 12 minutes to be
drained by a serial console at 9600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

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

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

后续操作

要使用 CDO 继续配置 威胁防御，请参阅 思科防御协调器 主页。



第 6 章

使用 ASDM 部署 ASA

本章对您适用吗？

本章介绍如何部署独立式 ASA 逻辑设备，包括如何配置智能许可。本章不涉及以下部署，请参考《ASA 配置指南》了解相关内容：

- 集群
- 故障切换
- CLI 配置

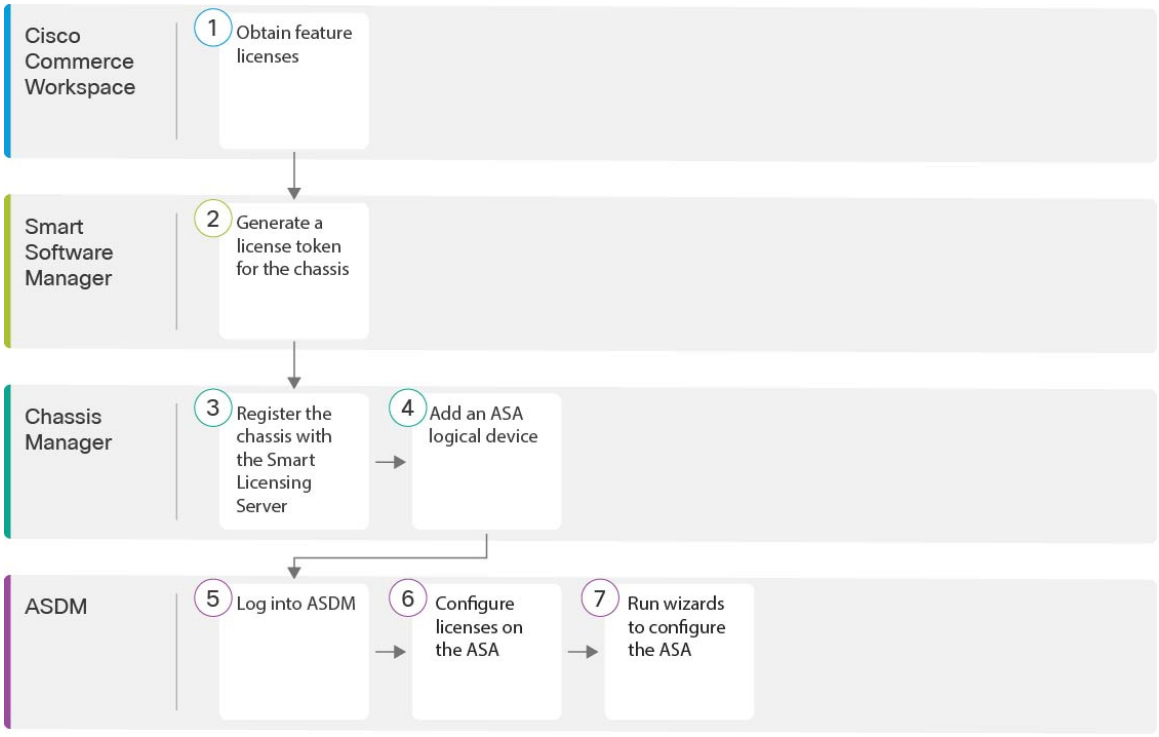
本章还演示如何配置基本安全策略；如果您有更高级的要求，请参阅配置指南。

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

- 端到端程序，第 113 页
- 机箱管理器：向许可证服务器注册机箱，第 114 页
- 机箱管理器：添加 ASA 逻辑设备，第 119 页
- 登录 ASDM，第 122 页
- 在 ASA 上配置许可证授权，第 123 页
- 配置 ASA，第 124 页
- 访问 ASA CLI，第 125 页
- 后续步骤，第 126 页
- ASA 的历史记录，第 127 页

端到端程序

请参阅以下任务以在机箱上部署和配置 ASA。



1	Cisco Commerce Workspace	机箱管理器：向许可证服务器注册机箱，第 114 页：获取功能许可证。
2	智能软件管理器	机箱管理器：向许可证服务器注册机箱，第 114 页：为机箱生成许可证令牌。
3	机箱管理器	机箱管理器：向许可证服务器注册机箱，第 114 页：向智能许可服务器注册机箱。
4	机箱管理器	机箱管理器：添加 ASA 逻辑设备，第 119 页。
5	ASDM	登录 ASDM，第 122 页。
6	ASDM	在 ASA 上配置许可证授权，第 123 页。
7	ASDM	配置 ASA，第 124 页。

机箱管理器：向许可证服务器注册机箱

ASA 使用智能许可。您可以使用常规智能许可，这需要互联网接入；或者对于离线管理，您可以配置永久许可证预留或智能软件管理器本地版（之前称为卫星服务器）。有关这些离线许可方法的更多信息，请参阅思科 ASA 系列功能许可证；本指南适用于常规智能许可。

有关思科许可的更详细概述，请访问 cisco.com/go/licensingguide

对于 Firepower 4100 上的 ASA，智能软件许可配置分为两部分，分别在机箱上的 FXOS 和 ASA 中进行。

- Firepower 4100- 所有智能软件许可基础设施均在 FXOS 中配置，包括用于与许可证颁发机构进行通信的参数。Firepower 4100本身无需任何许可证即可运行。
- ASA - 在 ASA 中配置所有许可证授权。

注册机箱时，智能软件管理器会为防火墙和智能软件管理器之间的通信颁发ID证书。它还会将防火墙分配到相应的虚拟帐户。除非您向智能软件管理器注册，否则您将无法进行配置更改，因为有些功能需要特殊许可，但其他方面的操作不受影响。许可的功能包括：

- 基础
- 安全情景
- 运营商 - Diameter、GTP/GPRS、M3UA、SCTP
- 强加密 (3DES/AES) - 如果您的智能帐户未获得强加密授权，但Cisco已确定允许您使用强加密，您可以手动将强加密许可证添加到您的帐户。
- Cisco Secure 客户端 - Secure Client Advantage、Secure Client Premier 或 Secure Client VPN Only

当您向智能软件管理器请求ASA的注册令牌时，请选中**在使用此令牌注册的产品上允许导出控制的功能 (Allow export-controlled functionaility on the products registered with this token)** 复选框，以便应用完整的强加密许可证（您的帐户必须符合其使用条件）。当您在机箱上应用注册令牌时，对于符合条件的用户，系统会自动启用强加密许可证，因此您无需进行其他操作。如果您的智能帐户未获得强加密授权，但Cisco已确定允许您使用强加密，您可以手动将强加密许可证添加到您的帐户。

进行 ASDM 访问需要强加密。

开始之前

- 拥有 智能软件管理器主帐户。

  如果您还没有帐户，请点击此链接以设置新帐户。通过智能软件管理器，您可以为组织创建一个主帐户。

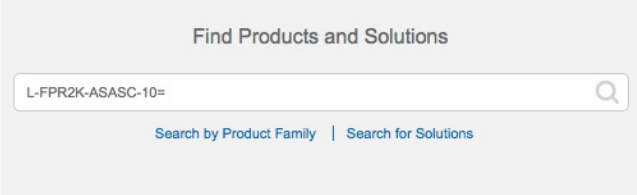
- 您的智能软件管理器帐户必须符合强加密 (3DES/AES) 许可证的要求，才能使用某些功能（已使用导出合规性标志启用）。
- 如果尚未执行此操作，请配置 NTP，第 17 页。
- 如果在初始设置期间没有配置 DNS，请在**平台设置** > **DNS**页面添加 DNS 服务器。

过程

步骤 1 请确保您的智能许可帐户包含您所需的可用许可证，包括最低限度的基础许可证。

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管理器帐户。但是，如果您需要自己添加许可证，则请使用Cisco Commerce Workspace上的 **Find Products and Solutions** 搜索字段。搜索以下许可证 PID：

图 *24:* 许可证搜索



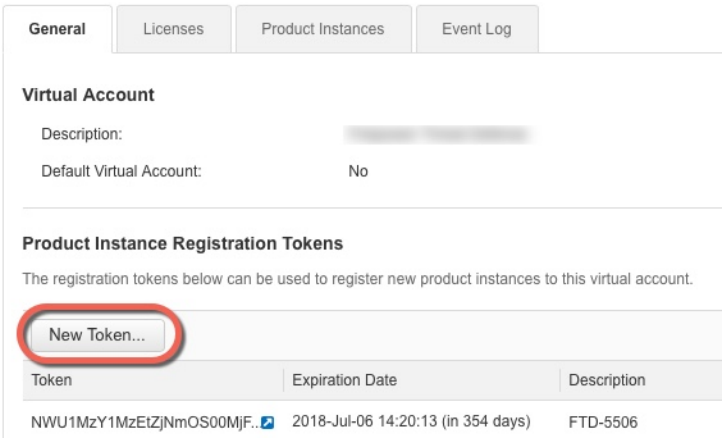
- 基础许可证 — L-FPR4100-ASA=。基础许可证是免费的，但您仍然需要将其添加到您的智能软件许可帐户中。
- 10 情景许可证 - L-FPR4K-ASASC-10=。情景许可证是附加的；请购买多份许可证以满足您的需要。
- 230 情景许可证 - L-FPR4K-ASASC-230=。情景许可证是附加的；请购买多份许可证以满足您的需要。
- 250 情景许可证 - L-FPR4K-ASASC-250=。情景许可证是附加的；请购买多份许可证以满足您的需要。
- 运营商 (Diameter, GTP/GPRS, M3UA, SCTP) — L-FPR4K-ASA-CAR=
- 强加密 (3DES/AES) 许可证 - FPR4K-ENC-K9 =。仅当帐户未获授权使用强加密时需要。
- Cisco Secure 客户端 - 请参阅思科安全客户端订购指南。您不能直接在 ASA 中启用此许可证。

步骤 2 在 Cisco Smart Software Manager 中，为要将此设备添加到的虚拟帐户请求并复制注册令牌。

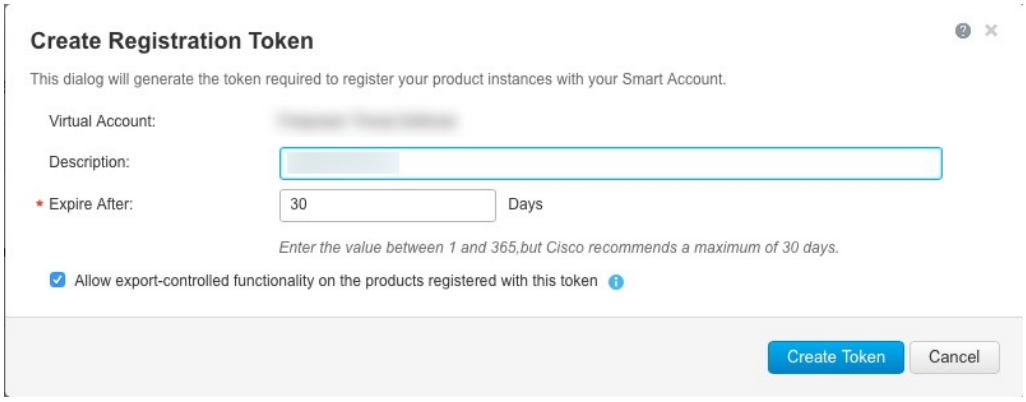
a) 点击 **Inventory**。



b) 在 **General** 选项卡上，点击 **New Token**。



c) 在 **Create Registration Token** 对话框中，输入以下设置，然后点击 **Create Token**：



- **Description**
- **Expire After** - 思科建议该时间为 30 天。
- **Allow export-controlled functionaility on the products registered with this token** - 启用导出合规性标志。

系统将令牌添加到您的资产中。

d) 点击令牌右侧的箭头图标可以打开 **Token** 对话框，可以从中将令牌 ID 复制到剪贴板。当需要注册ASA时，请准备好此令牌，以在该程序后面的部分使用。

图 *25:* 查看令牌

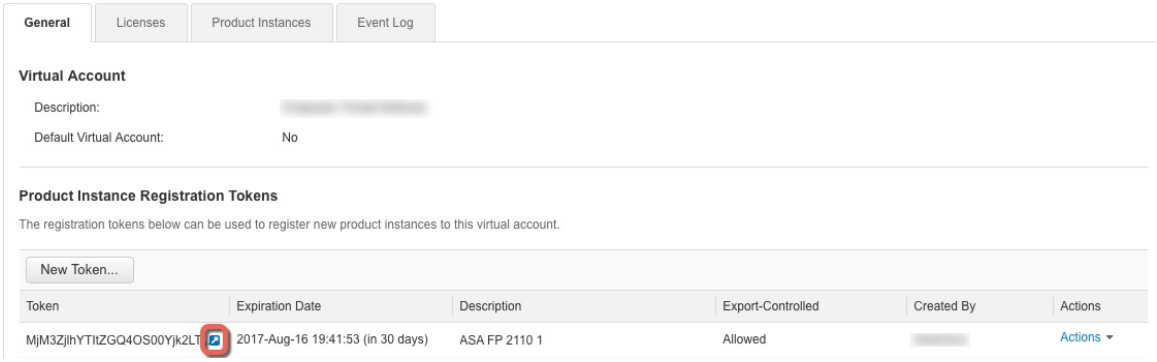
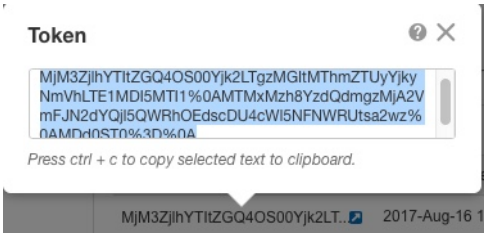
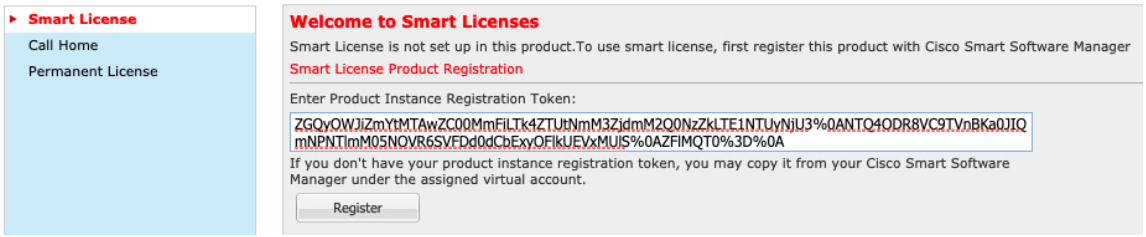


图 *26:* 复制令牌



步骤 3 在 机箱管理器 中，选择**系统 (System)** > **许可 (Licensing)** > **智能许可证 (Smart License)**。

步骤 4 在**输入产品实例注册令牌 (Enter Product Instance Registration Token)** 字段中输入注册令牌。



步骤 5 点击 **Register**。

Firepower 4100 向许可证颁发机构注册。成功注册可能需要几分钟时间。刷新此页面可查看状态。

图 *27:* 正在注册

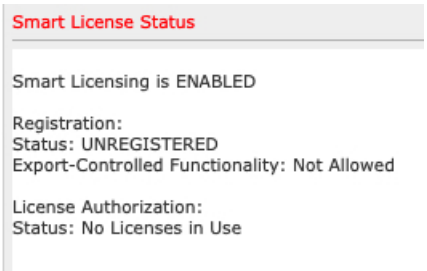
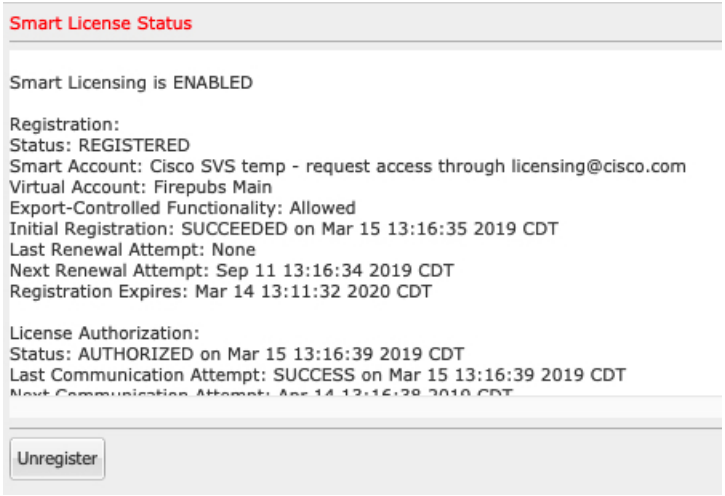


图 *28:* 注册成功



机箱管理器：添加 ASA 逻辑设备

您可以从 Firepower 4100 将 ASA 部署为本地实例。

要添加故障转移对或集群，请参阅 ASA 通用操作配置指南。

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。

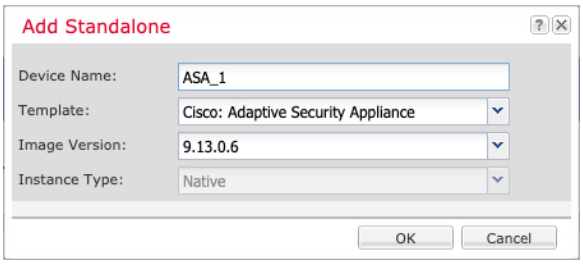
开始之前

- 配置与 ASA 一起使用的管理接口；请参阅配置接口，第 20 页。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。
- 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
  - 新管理员密码/启用密码

过程

步骤 1 在 机箱管理器中，选择**逻辑设备**。

步骤 2 点击**添加** > **独立设备**，并设置以下参数：



a) 提供**设备名称**。

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

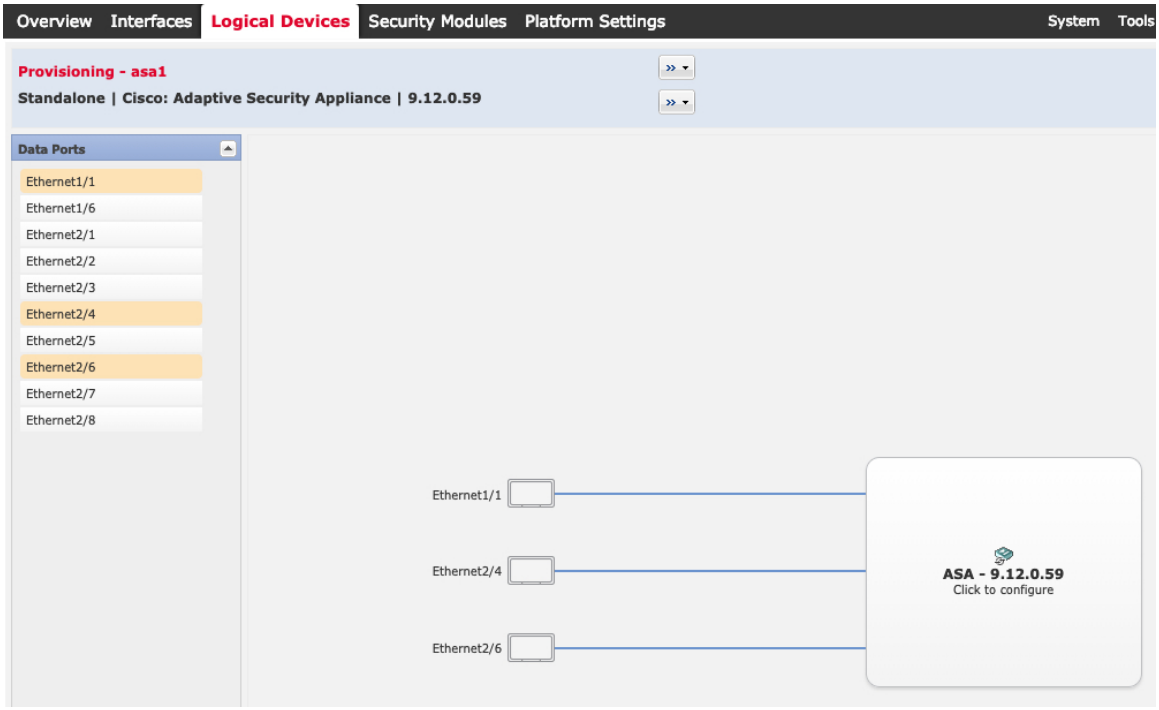
b) 对于**模板**，请选择**思科：自适应安全设备**。

c) 选择**映像版本**。

d) 点击**确定 (OK)**。

屏幕会显示调配 - 设备名称窗口。

步骤 3 展开**数据端口**区域，然后点击要分配给设备的每个接口。

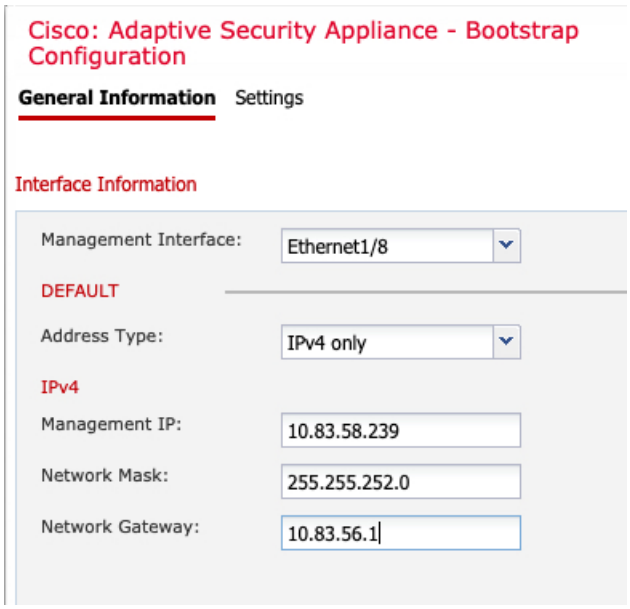


仅可分配先前在**接口**页面上启用的数据接口。稍后需要在 ASDM 中启用和配置这些接口，包括设置 IP 地址。

步骤 4 点击屏幕中心的设备图标。

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

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



a) 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。

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

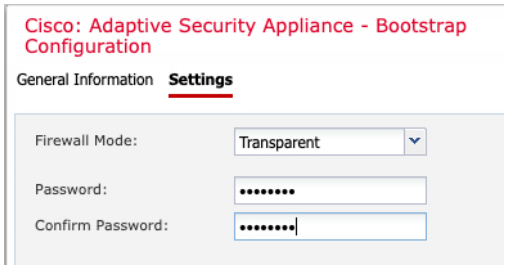
c) 配置**管理 IP** 地址。

设置用于此接口的唯一 IP 地址。

d) 输入**网络掩码**或**前缀长度**。

e) 输入**网络网关**地址。

步骤 6 点击**设置**。



a) 选择**防火墙模式**：**路由式**或**透明**。

在路由模式下，ASA 被视为网络中的一个路由器跃点。要在其间路由的每个接口都位于不同的子网上。另一方面，透明防火墙是一个第2层防火墙，充当“电缆中的块”或“隐蔽的防火墙”，不被视为是到所连接设备的路由器跃点。

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

b) 输入并确认管理员用户和启用密码的**密码**。

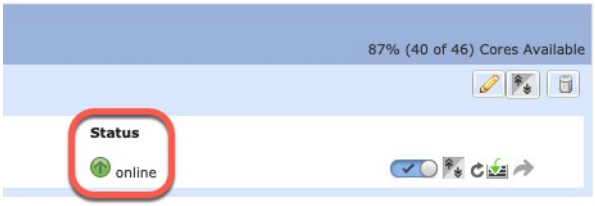
预配置的 ASA 管理员用户/密码和启用密码在进行密码恢复时非常有用；如果有 FXOS 访问权限，在忘记管理员用户密码/启用密码时，可以将其重置。

步骤 7 点击**确定 (OK)** 关闭配置对话框。

步骤 8 点击**保存 (Save)**。

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





登录 ASDM

启动 ASDM 以便配置 ASA。

开始之前

- 请参阅 Cisco.com 上的 ASDM 发行说明了解运行 ASDM 的要求。
- 确保 机箱管理器 **逻辑设备 (Logical Devices)**页面上 ASA 逻辑设备的**状态 (Status)** 为**在线 (online)**。

过程

步骤 1 在浏览器中输入以下 URL。

- **https://***management_ip* - 在引导程序配置中输入的管理接口 IP 地址。

注释 确保指定 **https://**，而非指定 **http://** 或只指定 IP 地址（默认为 HTTP）；ASA 不会自动将 HTTP 请求转发到 HTTPS。

此时将显示 **Cisco ASDM** 网页。您可能会看到浏览器安全警告，因为 ASA 没有安装证书；您可以安全地忽略这些警告并访问网页。

步骤 2 点击以下可用选项之一：**Install ASDM Launcher** 或 **Run ASDM**。

步骤 3 根据您选择的选项，按照屏幕上的说明启动 ASDM。

系统将显示 **Cisco ASDM-IDM Launcher**。

步骤 4 将用户名留空，输入在部署 ASA 时设置的启用密码，然后点击**确定**。

系统将显示 ASDM 主窗口。

在 ASA 上配置许可证授权

向 ASA 分配许可证。必须至少分配标准许可证。

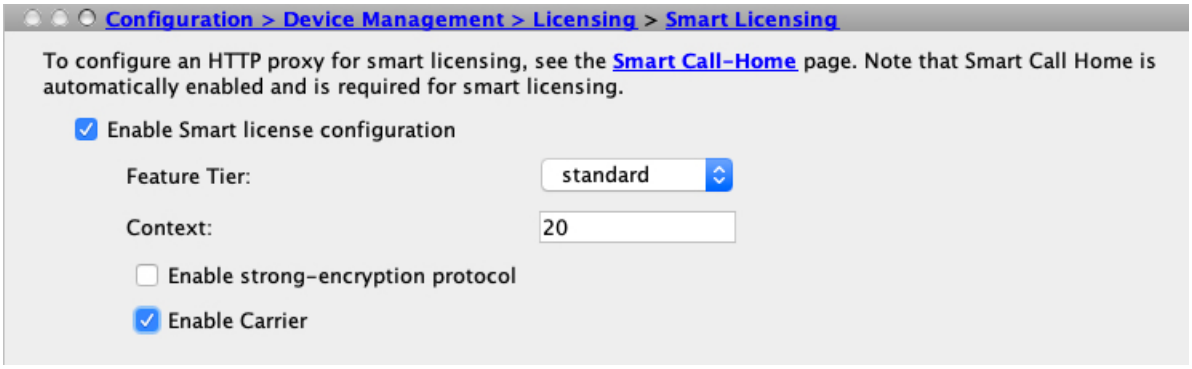
开始之前

- 机箱管理器：向许可证服务器注册机箱，第 114 页。

过程

步骤 1 在 ASDM 中，依次选择 **Configuration** > **Device Management** > **Licensing** > **Smart Licensing**。

步骤 2 设置以下参数：



a) 选中 **Enable Smart license configuration**。

b) 从**功能层 (Feature Tier)** 下拉列表中，选择**基础 (Essentials)**。

仅基础层可用。

c) （可选） 对于**情景 (Context)** 许可证，输入情景的数目。

您可以在没有许可证的情况下使用 10 种情景。最大情景数为 250。例如，要使用最大值，请为情景数输入 240；此值将与默认值 10 相加。

d) （可选） 检查**运营商**。

步骤 3 点击 **Apply**。

如果您的帐户中没有相应的许可证，则无法应用许可证更改。

步骤 4 点击工具栏中的 **Save** 图标。

步骤 5 退出并重新启动 ASDM。

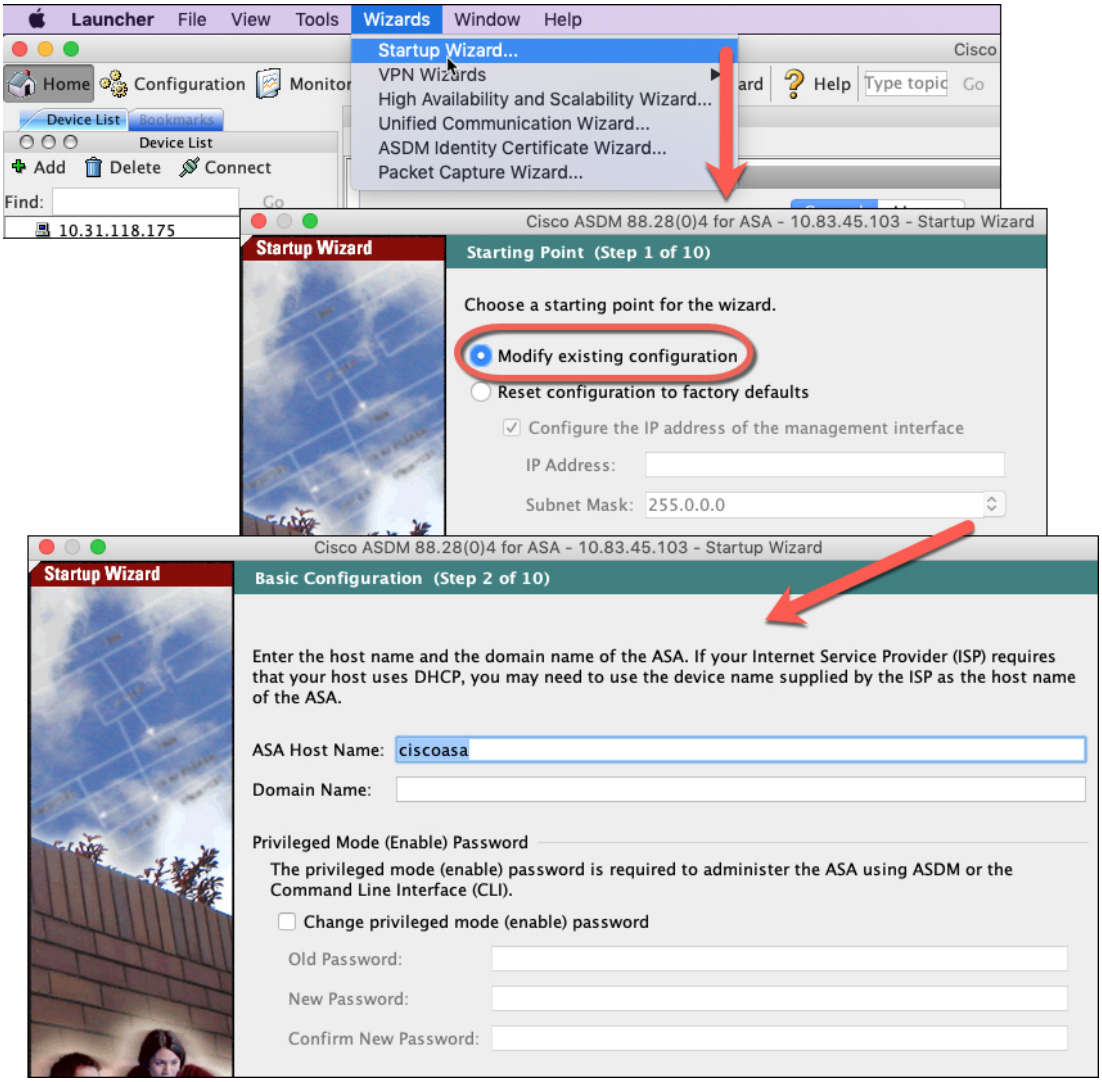
当您更改许可证时，您需要重新启动 ASDM 才能显示更新屏幕。

配置 ASA

利用 ASDM，您可以使用向导来配置基本功能和高级功能。您还可以手动配置向导中未包括的功能。

过程

步骤 1 依次选择 **Wizards > Startup Wizard**，然后点击 **Modify existing configuration** 单选按钮。



步骤 2 **Startup Wizard** 将引导您完成配置：

- 启用密码
- 接口，包括更改内部和外部接口 IP 地址以及启用接口。
- 静态路由
- DHCP 服务器
- 其他...

步骤 3 （可选） 在 **Wizards** 菜单中，运行其他向导。

步骤 4 要继续配置 ASA，请参阅浏览思科 ASA 系列文档中适合您的软件版本的文档。

访问 ASA CLI

您可以使用 ASA CLI（而非 ASDM）对 ASA 进行故障排除或配置。您可以通过 FXOS CLI 连接以访问 CLI。之后，您就可以在任何接口上配置对 ASA 的 SSH 访问。有关更多信息，请参阅 ASA 一般操作配置指南。

过程

步骤 1 从 FXOS CLI，使用控制台连接或 Telnet 连接以连接到模块 CLI。

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

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

示例：

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

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

步骤 2 连接到 ASA 控制台。

connect asa

示例：

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
```

```
[...]
asa>
```

步骤 3 输入 **Ctrl-a, d** 使应用程序控制台返回到 FXOS 模块 CLI。

步骤 4 返回 FXOS CLI 的管理引擎层。

退出控制台：

a) 输入 **~**

您将退出至 Telnet 应用。

b) 要退出 Telnet 应用，请输入：

telnet>**quit**

退出 Telnet 会话：

a) 输入 **Ctrl-],**。

示例

以下示例说明了如何连接至 上的 ASA，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 asa
asa> ~
telnet> quit
Connection closed.
Firepower#
```

后续步骤

- 要继续配置 ASA，请参阅浏览思科 ASA 系列文档中适合您的软件版本的文档。

ASA 的历史记录

特性	版本	详细信息
适用于 Firepower 4115、4125 和 4145 的 ASA	9.12(1)	我们推出了 Firepower 4115、4125 和 4145。 注释 需要 FXOS 2.6.1。
支持在同一个 Firepower 9300 上使用独立的 ASA 和 威胁防御 模块	9.12(1)	您现在可以在同一个 Firepower 9300 上同时部署 ASA 和 威胁防御 逻辑设备。 注释 需要 FXOS 2.6.1。
支持 ASA 逻辑设备的透明模式部署	9.10(1)	您现在可以在部署 ASA 时指定透明模式或路由模式。 注释 需要 FXOS 2.4.1。 新增/修改的 机箱管理器 菜单项： **逻辑设备** > **添加设备** > **设置** > **防火墙模式**下拉列表
智能代理升级至 v1.6	9.6(2)	智能代理从 1.1 版本升级到 1.6 版本。此升级支持永久许可证预留，同时也支持依据许可证账号中的权限集设置强加密 (3DES/AES) 许可证授权。
新运营商许可证	9.5(2)	用于替换现有的 GTP/GPRS 许可证的新运营商许可证提供的支持包括 SCTP 和 Diameter 检测。对于 Firepower 9300 上的 ASA，**feature mobile-sp** 命令将自动迁移到 **feature carrier** 命令。 修改了以下菜单项：**配置** > **设备管理** > **许可** > **智能许可**

© 2023 Cisco Systems, Inc. 保留所有权利。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。