



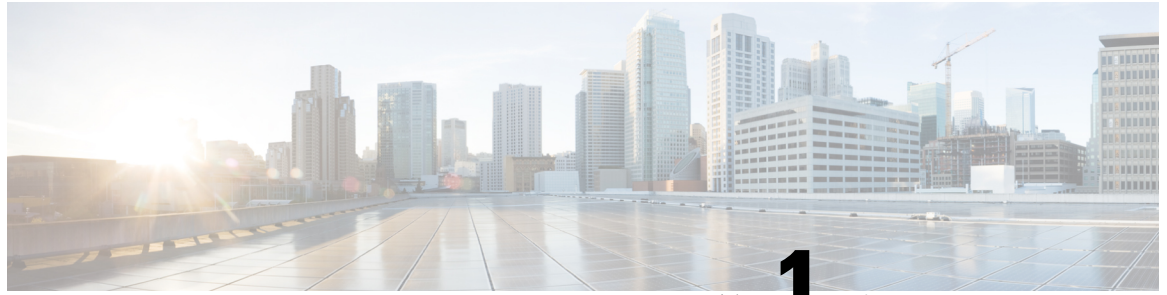
Cisco Secure Firewall 3100 入门指南

首次发布日期: 2022 年 2 月 24 日

上次修改日期: 2023 年 7 月 27 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

哪种操作系统和管理器适合您？

您的硬件平台可以运行两种操作系统之一。对于每种操作系统，您都可以选择管理器。本章介绍操作系统和管理器选项。

- [操作系统，第 1 页](#)
- [管理器，第 1 页](#)

操作系统

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）操作系统。

- 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。

要在 ASA 和威胁防御之间重新映像，请参阅 [Cisco Secure Firewall ASA 和 Secure Firewall Threat Defense 重新映像指南](#)。

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

管理器	说明
Cisco Secure Firewall Management Center (之前的 Firepower 管理中心)	<p>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。</p> <p>管理中心可以从外部（或其他数据）接口而不是标准管理接口来管理威胁防御。此功能用于远程分支机构部署。</p> <p>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。</p> <p>要开始使用管理网络上的管理中心，请参阅使用管理中心部署威胁防御，第 5 页。</p> <p>要开始使用远程网络上的管理中心，请参阅使用远程管理中心部署威胁防御，第 43 页。</p>
Secure Firewall 设备管理器（之前的 Firepower 设备管理器）	<p>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。</p> <p>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。</p> <p>要开始使用设备管理器，请参阅使用设备管理器部署威胁防御，第 87 页。</p>
思科防御协调器 (CDO)	<p>CDO 提供两种管理模式：</p> <ul style="list-style-type: none"> • (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。 <p>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。</p> <p>要开始 CDO 调配，请参阅使用 CDO 部署威胁防御，第 113 页。</p>

管理器	说明
Cisco Secure Firewall Threat Defense REST API	<p>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。</p> <p>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。</p>
Cisco Secure Firewall Management Center REST API	<p>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。</p> <p>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。</p>

ASA 管理器

表 2: ASA 管理器

管理器	说明
自适应安全设备管理器 (ASDM)	<p>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。</p> <p>要开始使用 ASDM，请参阅使用 ASDM 部署 ASA，第 163 页。</p>
CLI	<p>如果您喜欢 CLI 胜过 GUI，应使用 ASA CLI。</p> <p>本指南不涵盖 CLI。有关详细信息，请参阅ASA 配置指南。</p>
CDO	<p>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。</p> <p>本指南中不涵盖 CDO。要开始使用 CDO，请参阅CDO 主页。</p>
Cisco Security Manager (CSM)	<p>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。</p> <p>本指南中不涵盖 CSM。有关详细信息，请参阅CSM 用户指南。</p>

理器	说明
ASA REST API	<p>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。</p> <p>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。</p>



第 2 章

使用管理中心部署威胁防御

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[哪种操作系统和管理器适合您？](#)，第 1 页。本章适用于威胁防御和管理中心。

本章介绍如何完成威胁防御的初始配置以及如何将防火墙注册到位于管理网络中的管理中心。对于管理中心位于中央总部的远程分支机构部署，请参阅[使用远程管理中心部署威胁防御](#)，第 43 页。

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。

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。

- [开始之前](#)，第 6 页
- [端到端程序](#)，第 6 页
- [查看网络部署](#)，第 8 页
- [连接防火墙的电缆](#)，第 10 页
- [打开防火墙电源](#)，第 12 页
- (可选) [检查软件并安装新版本](#)，第 13 页
- [完成威胁防御初始配置](#)，第 15 页
- [登录管理中心](#)，第 23 页
- [获取管理中心的许可证](#)，第 23 页
- [向管理中心注册威胁防御](#)，第 25 页

- [配置基本安全策略，第 28 页](#)
- [访问威胁防御和FXOS CLI，第 40 页](#)
- [关闭防火墙电源，第 41 页](#)
- [后续步骤, on page 42](#)

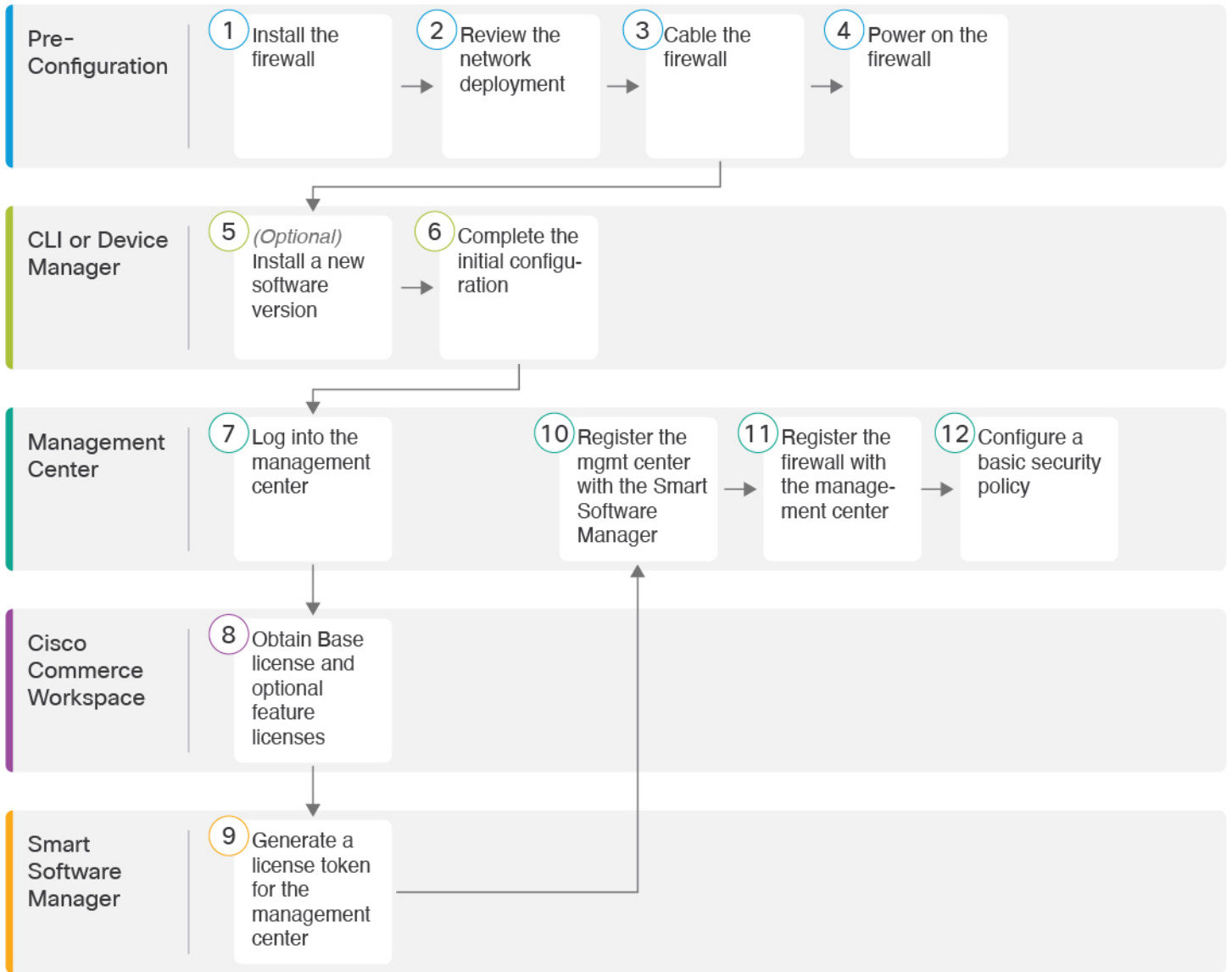
开始之前

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 威胁防御 和 管理中心。

图 1: 端到端程序



①	配置前准备工作	安装防火墙。请参阅 硬件安装指南 。
②	配置前准备工作	查看网络部署 ，第 8 页。
③	配置前准备工作	连接防火墙的电缆 ，第 10 页。
④	配置前准备工作	打开防火墙电源 ，第 12 页。
⑤	CLI	(可选) 检查软件并安装新版本 ，第 13 页。

6	CLI 或 设备管理器	完成威胁防御初始配置，第 15 页。
7	管理中心	登录管理中心，第 23 页。
8	Cisco Commerce Workspace	购买基本许可证和可选功能许可证 (获取管理中心的许可证，第 23 页)。
9	智能软件管理器	为 管理中心 (获取管理中心的许可证，第 23 页) 生成许可证令牌。
10	管理中心	向智能许可证服务器 (获取管理中心的许可证，第 23 页) 注册管理中心。
11	管理中心	向管理中心注册威胁防御，第 25 页。
12	管理中心	配置基本安全策略，第 28 页。

查看网络部署

专用管理 1/1 接口是一种具有自己的网络设置的特殊接口。默认情况下，管理 1/1 接口已启用并配置为 DHCP 客户端。如果您的网络不包括 DHCP 服务器，您可以在控制台端口的初始设置期间，将管理接口设置为使用静态 IP 地址。您可以在将威胁防御 连接到 管理中心 后配置其他接口。

有关如何在网络中放置 威胁防御 的想法，请参阅以下示例网络部署。

单独的管理网络

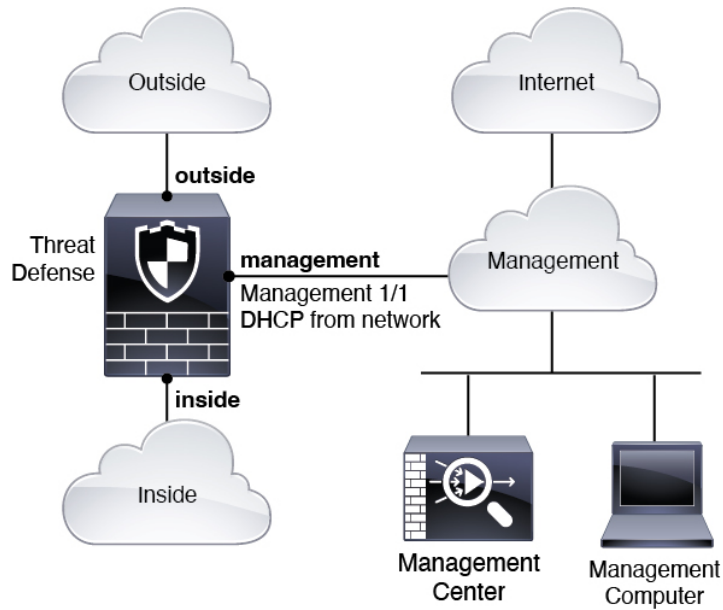
管理中心和威胁防御都需要从管理接口接入互联网以用于许可和更新。



注释 管理连接是信道自身与设备之间的 SSL 加密的安全通信信道。出于安全考虑，您无需通过额外的加密隧道（例如站点到站点 VPN）来运行此流量。例如，如果 VPN 发生故障，您将失去管理连接，因此建议使用简单的管理路径。

下图显示 Secure Firewall 3100 的一种可能网络部署，其中管理中心和管理计算机连接到管理网络。管理网络具有互联网接入路径以用于许可和更新。

图 2: 单独的管理网络



边缘网络部署

管理中心和威胁防御都需要从管理接口接入互联网以用于许可和更新。

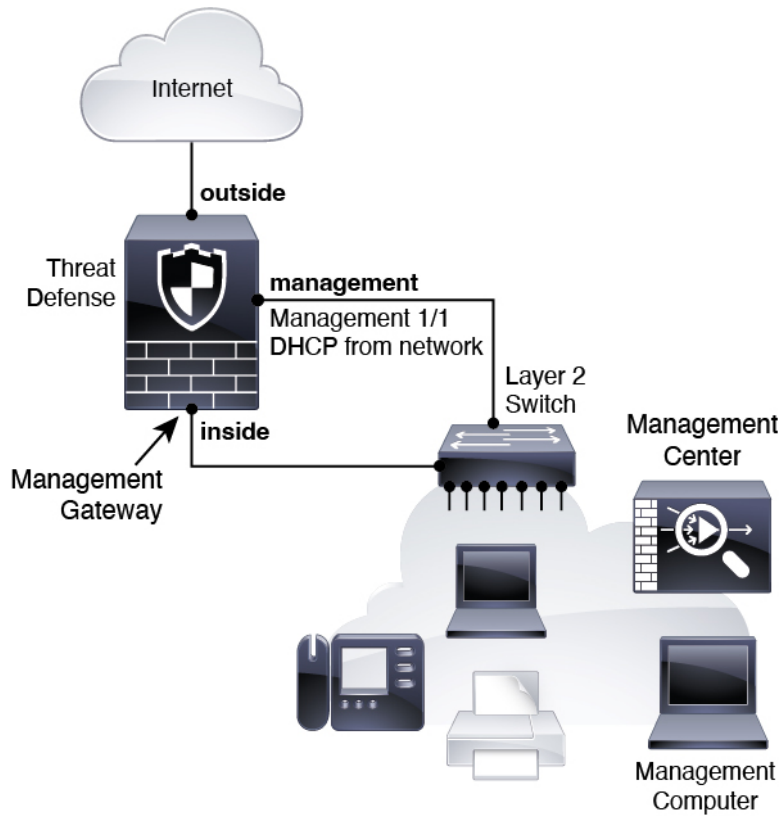


注释 管理连接是信道自身与设备之间的 SSL 加密的安全通信信道。出于安全考虑，您无需通过额外的加密隧道（例如站点到站点 VPN）来运行此流量。例如，如果 VPN 发生故障，您将失去管理连接，因此建议使用简单的管理路径。

下图显示 Secure Firewall 3100 的一种可能网络部署，其中 Secure Firewall 3100 充当管理中心和威胁防御管理的互联网网关。

在下图中，通过经第 2 层交换机将管理 1/1 连接到内部接口，并将管理中心和管理计算机连接到交换机，Secure Firewall 3100 充当管理接口和管理中心的互联网网关。（因为管理接口独立于威胁防御上的其他接口，因此这种直接连接是允许的。）

图 3: 边缘网络部署



连接防火墙的电缆

要在 Secure Firewall 3100 中按建议方案之一进行布线，请参阅以下步骤。



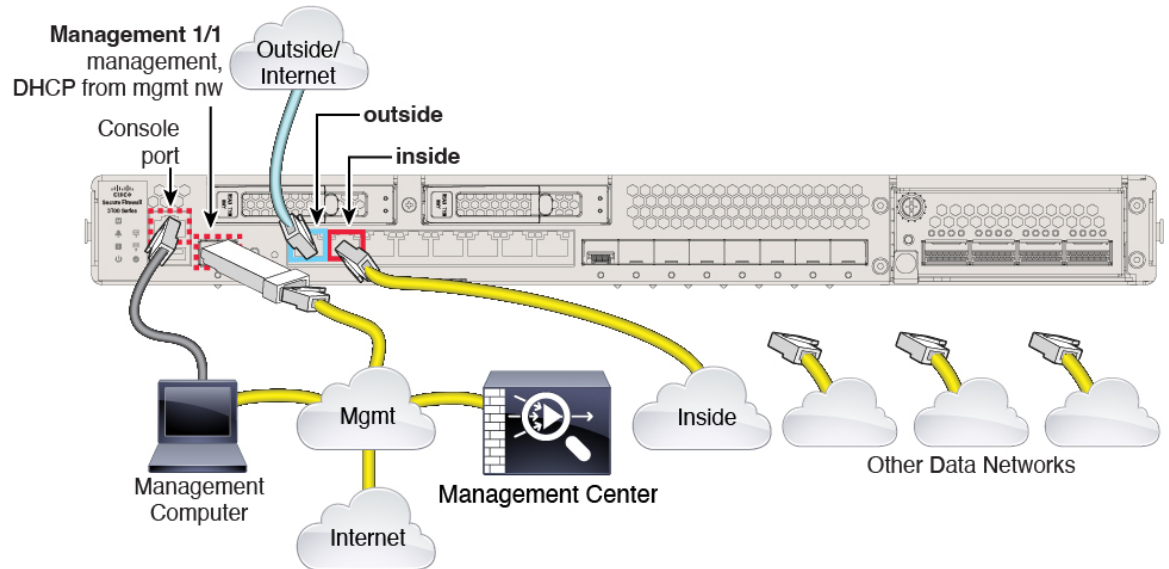
注释 也可以使用其他拓扑，而部署情况会因基本逻辑网络连接、端口、地址和配置要求有所不同。

过程

步骤 1 安装机箱。请参阅[硬件安装指南](#)。

步骤 2 连接单独管理网络的电缆：

图 4: 连接单独管理网络的电缆



a) 使用电缆将以下内容连接到您的管理网络：

- 管理 1/1 接口

注释 管理 1/1 是需要 SFP 模块的 10 Gb 光纤接口。

- Cisco Secure Firewall Management Center
- 管理计算机

b) 将管理计算机连接到控制台端口。如果不使用 SSH 访问管理接口，则需要使用控制台端口访问 CLI 进行初始设置。

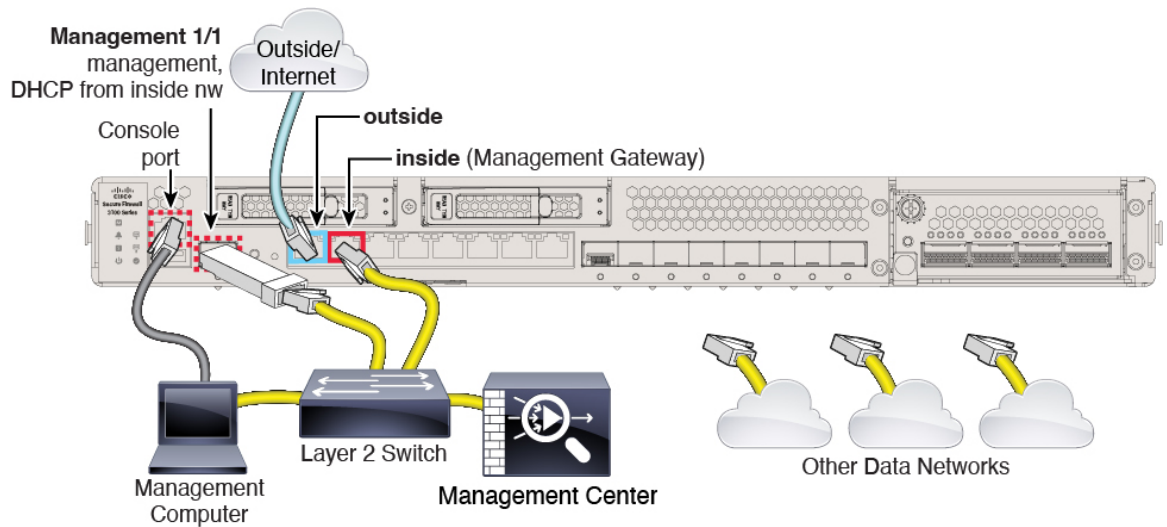
c) 将内部接口（例如，以太网 1/2）连接到内部路由器。

d) 将外部接口（例如，以太网 1/1）连接到外部路由器。

e) 将其他网络连接到其余接口。

步骤 3 为实施边缘部署进行布线：

图 5: 进行边缘部署布线



- a) 将以下各项布线到第 2 层以太网交换机：
 - 内部接口（例如，以太网 1/2）
 - 管理 1/1 接口

注释 管理 1/1 是需要 SFP 模块的 10 Gb 光纤接口。
 - Cisco Secure Firewall Management Center
 - 管理计算机
- b) 将管理计算机连接到控制台端口。如果不使用 SSH 访问管理接口，则需要使用控制台端口访问 CLI 进行初始设置。
- c) 将外部接口（例如，以太网 1/1）连接到外部路由器。
- d) 将其他网络连接到其余接口。

打开防火墙电源

系统电源由位于防火墙后部的摇杆电源开关控制。电源开关以软通知开关形式实施，支持平稳地关闭系统以降低系统软件及数据损坏的风险。



注释 首次启动 威胁防御时，初始化大约需要 15 到 30 分钟。

开始之前

为防火墙提供可靠的电源（例如，使用不间断电源 (UPS)）非常重要。未事先关闭就断电可能会导致严重的文件系统损坏。后台始终有许多进程在运行，因此断电会使得系统无法正常关闭。

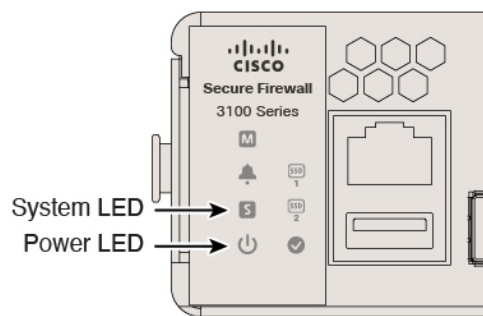
过程

步骤 1 将电源线一端连接到防火墙，另一端连接到电源插座。

步骤 2 使用位于机箱背面电源线旁边的标准摇杆型电源开关打开电源。

步骤 3 检查防火墙背面的电源 LED；如果该 LED 呈绿色稳定亮起，表示防火墙已接通电源。

图 6: 系统和电源 LED



步骤 4 检查防火墙背面的系统 LED；其呈绿色稳定亮起之后，系统已通过通电诊断。

注释 将开关从开切换到关时，系统可能需要几秒钟才会最终关闭。在此期间，机箱前面的电源 LED 将闪烁绿色。在电源 LED 完全关闭之前，请勿拔出电源。

(可选) 检查软件并安装新版本

要检查软件版本并在必要时安装不同的版本，请执行以下步骤。我们建议您在配置防火墙之前安装目标版本。或者，您也可以在启动并运行后执行升级，但升级（保留配置）可能需要比按照此程序花费更长的时间。

我应该运行什么版本？

思科建议运行软件下载页面上的版本号旁边标有金色星号的 Gold Star 版本。您还可以参考 <https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html> 中所述的发布策略；例如，此公告描述短期版本编号（包含最新功能）、长期版本编号（较长时间的维护版本和补丁）或额外长期版本编号（最长期限的维护版本和补丁，用于政府认证）。

过程

步骤 1 连接到控制台端口。有关详细信息，请参阅[访问威胁防御和FXOS CLI](#)，第 40 页。

使用用户名 **admin** 和默认密码 **Admin123** 登录。

您连接到 FXOS CLI。第一次输入登录时，系统会提示您更改密码。此密码也用于 SSH 的威胁防御登录。

注释 如果密码已更改，但您不知道，则必须执行出厂重置以将密码重置为默认值。有关 [出厂重置程序](#) 的信息，请参阅 [FXOS 故障排除指南](#)。

示例:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: *****
Confirm new password: *****
Your password was updated successfully.

[...]

firepower#
```

步骤 2 在 FXOS CLI 中，显示正在运行的版本。

scope ssa

show app-instance

示例:

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name      Slot ID      Admin State      Operational State      Running Version Startup
Version Cluster Oper State
-----
ftd                   1            Enabled          Online                  7.2.0.65             7.2.0.65
                        Not Applicable
```

步骤 3 如果要安装新版本，请执行这些步骤。

- a) 如果要为管理接口设置静态 IP 地址，请参阅[使用 CLI 完成威胁防御初始配置](#)，第 15 页。默认情况下，管理接口将使用 DHCP。

您需要从可通过管理接口访问的服务器下载新的映像。

- b) 执行《[FXOS 故障排除指南](#)》中的[重新映像程序](#)。

完成威胁防御初始配置

您可以使用 CLI 或设备管理器来完成威胁防御初始配置。

使用 CLI 完成威胁防御初始配置

连接到威胁防御 CLI 以执行初始设置，包括使用设置向导设置管理 IP 地址、网关和其他基本网络设置。专用管理接口是一种具有自己的网络设置的特殊接口。如果不想使用管理接口访问管理器，可以使用 CLI 配置数据接口。您还将配置管理中心通信设置。当您使用设备管理器执行初始设置时，如果您切换到管理中心进行管理，除管理接口和管理器访问接口设置外，在设备管理器中完成的所有接口配置都将保留。请注意，不会保留其他默认配置设置，例如访问控制策略。

Procedure

- 步骤 1** 从控制台端口连接到威胁防御 CLI，或使用管理接口连接至 SSH，默认情况下其从 DHCP 获取 IP 地址。如果您打算更改网络设置，我们建议使用控制台端口，以免断开连接。

控制台端口连接到 FXOS CLI。SSH 会话直接连接到威胁防御 CLI。

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

在控制台端口，您可以连接到 FXOS CLI。第一次登录 FXOS 时，系统会提示您更改密码。此密码也用于 SSH 的威胁防御登录。

Note 如果密码已更改，但您不知道，则必须重新映像设备以将密码重置为默认值。有关[重新映像程序](#)的信息，请参阅 [FXOS 故障排除指南](#)。

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: *****
Confirm new password: *****
Your password was updated successfully.

[...]

firepower#
```

- 步骤 3** 如果在控制台端口上连接到 FXOS，请连接到威胁防御 CLI。

connect ftd**Example:**

```
firepower# connect ftd
>
```

步骤 4 第一次登录威胁防御时，系统会提示您接受《最终用户许可协议》(EULA)和，如果使用 SSH 连接，则会提示您更改 admin 密码。然后，系统将显示 CLI 设置脚本。

Note 除非清除配置，否则无法重复 CLI 安装向导（例如，通过重新建立映像）。但是，可以稍后在 CLI 中使用 **configure network** 命令更改所有这些设置。请参阅 [Cisco Secure Firewall Threat Defense 命令参考](#)。

默认值或以前输入的值会显示在括号中。要接受之前输入的值，请按 **Enter** 键。

请参阅以下准则：

- **输入管理接口的 IPv4 默认网关 - 数据接口** 设置仅适用于远程管理中心或设备管理器管理；在管理网络上使用管理中心时，应为管理 1/1 设置网关 IP 地址。在网络部署部分中显示的边缘部署示例中，内部接口用作管理网关。在这种情况下，应将网关 IP 地址设置为意向内部接口 IP 地址；后期必须使用管理中心设置内部 IP 地址。
- **如果您的网络信息已更改，需要重新连接** - 如果您已建立 SSH 连接，但在初始设置时更改了 IP 地址，连接将断开。使用新 IP 地址和密码重新进行连接。控制台连接不会受影响。
- **本地管理设备？** - 输入 **否** 以使用管理中心。回答 **yes** 意味着您将改为使用设备管理器。
- **配置防火墙模式？** - 建议您在初始配置时设置防火墙模式。在初始设置后更改防火墙模式将会清除正在运行的配置。

Example:

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress. Please stand by.
You must change the password for 'admin' to continue.
Enter new password: *****
Confirm new password: *****
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
```

```

For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...

Update policy deployment information
  - add device configuration
  - add network discovery
  - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required. In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>

```

步骤 5 确定将管理此威胁防御的管理中心。

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} regkey [nat_id]
```

- {hostname | IPv4_address | IPv6_address | **DONTRESOLVE**} - 指定管理中心的 FQDN 或 IP 地址。如果管理中心不能直接寻址，请使用 **DONTRESOLVE** 并指定 *nat_id*。必须至少有一个设备（管理中心或威胁防御）具有可访问的 IP 地址，才能在两个设备之间建立双向 SSL 加密的通信通道。如果在此命令中指定 **DONTRESOLVE**，则威胁防御必须有可访问的 IP 地址或主机名。
- *reg_key* - 指定您选择的一次性注册密钥，注册威胁防御时也要在管理中心上指定它。注册密钥不得超过 37 个字符。有效字符包括字母数字（A - Z、a - z、0 - 9）和连字符（-）。
- *nat_id* - 指定您选择的唯一的一次性字符串，注册威胁防御时若一方没有指定可访问的 IP 地址或主机名，则也要在管理中心上指定它。如果将管理中心设置为 **DONTRESOLVE**，则需要指定它。NAT ID 不得超过 37 个字符。有效字符包括字母数字（A - Z、a - z、0 - 9）和连字符（-）。此 ID 不能用于将任何其他设备注册到管理中心。

Example:

```
> configure manager add MC.example.com 123456
Manager successfully configured.
```

如果管理中心位于 NAT 设备之后，请输入唯一的 NAT ID 以及注册密钥，并指定 **DONTRESOLVE** 而非主机名，例如：

Example:

```
> configure manager add DONTRESOLVE regk3y78 natid90
Manager successfully configured.
```

如果威胁防御位于 NAT 设备之后，请输入唯一的 NAT ID 以及管理中心 IP 地址或主机名，例如：

Example:

```
> configure manager add 10.70.45.5 regk3y78 natid56
Manager successfully configured.
```

What to do next

将防火墙注册到管理中心。

使用设备管理器完成威胁防御初始配置

连接到设备管理器以执行威胁防御的初始设置。当您使用设备管理器执行初始设置时，如果您切换到管理中心进行管理，除管理接口和管理器访问设置外，在设备管理器中完成的所有接口配置都将保留。请注意，不会保留其他默认配置设置，例如访问控制策略或安全区。使用 CLI 时，只有管理接口和管理器访问设置会被保留（例如，不保留默认的内部接口配置）。

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》。在设置威胁防御之前，您需要知道管理中心 IP 地址或主机名。
- 使用 Firefox、Chrome、Safari、Edge 或 Internet Explorer 的当前版本。

过程

步骤 1 登录设备管理器。

- a) 在浏览器中输入以下 URL 之一。
 - 内部（以太网 1/2） - <https://192.168.95.1>。
 - 管理 - https://management_ip。管理接口是 DHCP 客户端，因此 IP 地址取决于您的 DHCP 服务器。在此过程中，您可能必须将管理 IP 地址设置为静态地址，因此我们建议您使用内部接口，以免连接被断开。
- b) 使用用户名 **admin** 和默认密码 **Admin123** 登录。
- c) 系统会提示您阅读和接受“最终用户许可协议”并更改管理员密码。

步骤 2 首次登录设备管理器以完成初始配置时，请使用设置向导。您可以选择通过点击页面底部的跳过设备设置 (Skip device setup) 来跳过安装向导。

完成安装向导后，除了内部接口 (Ethernet1/2) 的默认配置外，您还将拥有外部（以太网 1/1）接口的配置，该接口会在您切换到管理中心管理接口时进行维护。

a) 为外部接口和管理接口配置以下选项，然后点击下一步 (Next)。

1. **外部接口地址 (Outside Interface Address)** - 此接口通常是互联网网关，并且可用作管理器访问接口。在初始设备设置期间，您不能选择其他外部接口。第一个数据接口是默认的外部接口。

如果要使用与外部（或内部）不同的接口来进行管理器访问，则必须在完成安装向导后手动配置该接口。

配置 IPv4 - 外部接口的 IPv4 地址。可以使用 DHCP，也可以手动输入静态 IP 地址、子网掩码和网关。另外，也可以选择关，不配置 IPv4 地址。您无法使用安装向导配置 PPPoE。如果接口连接到 DSL、电缆调制解调器或 ISP 的其他连接，并且 ISP 使用 PPPoE 来提供 IP 地址，则可能需要使用 PPPoE。您可以在完成向导后配置 PPPoE。

配置 Ipv6 - 外部接口的 Ipv6 地址可以使用 DHCP，也可以手动输入静态 IP 地址、前缀和网关。另外，也可以选择关，不配置 IPv6 地址。

2. **管理接口**

如果在 CLI 中执行了初始设置，您将不会看到管理接口设置。请注意，设置管理接口 IP 地址不是安装向导的一部分。请参阅步骤 3，第 19 页以设置管理 IP 地址。

DNS 服务器 - 防火墙的管理接口的 DNS 服务器。输入 DNS 服务器的一个或多个地址以解析名称。默认值为 OpenDNS 公共 DNS 服务器。如果您编辑字段并想要恢复默认值，请点击使用 **OpenDNS (Use OpenDNS)** 以重新将合适的 IP 地址载入字段。

防火墙主机名 - 防火墙的管理接口的主机名。

b) 配置时间设置 (NTP) (Time Setting [NTP]) 并点击下一步 (Next)。

1. **时区** - 选择系统时区。
2. **NTP 时间服务器** - 选择使用默认 NTP 服务器，还是手动输入 NTP 服务器的地址。可以添加多个服务器来提供备份。

c) 选择启动 90 日评估期而不注册。

不要向智能软件管理器注册威胁防御；所有许可均在管理中心上执行。

d) 点击完成。

e) 系统将提示您选择云管理 (Cloud Management) 或独立 (Standalone)。对于管理中心管理，请选择独立 (Standalone)，然后选择知道了 (Got It)。

步骤 3 (可能需要) 为管理接口配置一个静态 IP 地址。选择设备 (Device)，然后依次点击系统设置 (System Settings) > 管理接口 (Management Interface) 链接。

如果您要配置静态 IP 地址，请确保另将默认网关设置为唯一网关，而不是数据接口。如果您使用 DHCP，则无需进行任何配置。

步骤 4 如果要配置其他接口，包括外部或内部之外的接口，请选择设备 (Device)，然后点击接口 (Interfaces) 摘要中的链接。

有关在设备管理器中配置接口的更多信息，请参阅[在设备管理器中配置防火墙](#)，第 105 页。在向管理中心注册设备时，不会保留其他设备管理器配置。

步骤 5 选择 **设备 > 系统设置 > 集中管理**，然后点击 **继续** 设置管理中心管理。

步骤 6 配置管理中心/CDO 详细信息。

图 7:管理中心/CDO 详细信息

Configure Connection to Management Center or CDO


Provide details to register to the management center/CDO.

Management Center/CDO Details

Do you know the Management Center/CDO hostname or IP address?

Yes No


Threat Defense



10.89.5.16
fe80::6a87:c6ff:fea6:4c00/64

→

Management Center/CDO



10.89.5.35

Management Center/CDO Hostname or IP Address

10.89.5.35

Management Center/CDO Registration Key

●●●● 👁

NAT ID

Required when the management center/CDO hostname or IP address is not provided. We recommend always setting the NAT ID even when you specify the management center/CDO hostname or IP address.

11203

Connectivity Configuration

Threat Defense Hostname

1120-3

DNS Server Group

CustomDNSServerGroup ▼

Management Center/CDO Access Interface

Data Interface

Please select an interface ▼

Management Interface [View details](#)

CANCEL
CONNECT

- a) 对于 是否知道管理中心/CDO 主机名或 IP 地址，如果您可以使用 IP 地址或主机名访问 管理中心，请点击 是，如果管理中心 位于 NAT 之后或没有公共 IP 地址或主机名，请点击 否。

必须至少有一个设备（管理中心或威胁防御设备）具有可访问的 IP 地址，才能在两个设备之间建立双向 SSL 加密的通信通道。

- b) 如果您选择 **是**，则输入 **管理中心/CDO 主机名/IP 地址**。
- c) 指定 **管理中心/CDO 注册密钥**。

此密钥是您选择的一次性注册密钥，注册威胁防御设备时也要在管理中心上指定它。注册密钥不得超过 37 个字符。有效字符包括字母数字（A - Z、a - z、0 - 9）和连字符 (-)。此 ID 可用于将多台设备注册到管理中心。

- d) 指定 **NAT ID**。

此 ID 是您选择的唯一一次性字符串，您还需要在管理中心上指定它。如果仅在其中一台设备上指定 IP 地址，则此字段必填；但建议您即使在知道两台设备的 IP 地址时，仍指定 NAT ID。NAT ID 不得超过 37 个字符。有效字符包括字母数字（A - Z、a - z、0 - 9）和连字符 (-)。此 ID 不能用于将任何其他设备注册到管理中心。NAT ID 与 IP 地址结合使用，用于验证连接是否来自正确的设备；只有在对 IP 地址/NAT ID 进行身份验证后，才会检查注册密钥。

步骤 7 配置连接配置。

- a) 指定 **FTD 主机名**。
- b) 指定 **DNS 服务器组**。

选择现有组或创建一个新组。默认 DNS 组名为 **CiscoUmbrellaDNSServerGroup**，其中包括 OpenDNS 服务器。

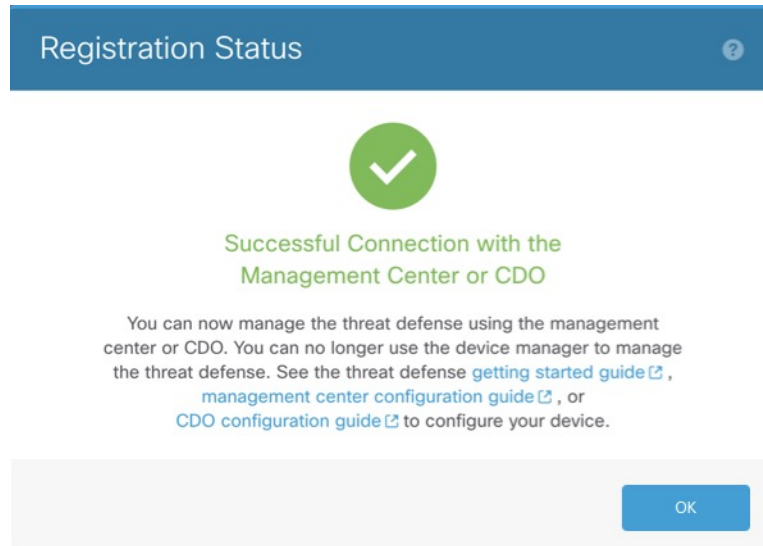
- c) 对于 **管理中心/CDO 访问接口 (Management Center/CDO Access Interface)**，请选择 **管理 (management)**。

步骤 8 点击 **连接 (Connect)**。注册状态对话框显示切换到管理中心的当前状态。在 **保存管理中心/CDO 注册设置** 步骤后，转到管理中心，并添加防火墙。

如果要取消切换到管理中心，请点击 **取消注册**。否则，请在 **保存管理中心/CDO 注册设置** 步骤之后关闭设备管理器浏览器窗口。如果这样做，该过程将暂停，并且只有在您重新连接到设备管理器时才会恢复。

如果您在 **保存管理中心/CDO 注册设置** 步骤后保持连接到设备管理器，您最终将看到 **与管理中心的成功连接或 CDO 对话框**。您将断开与设备管理器的连接。

图 8: 成功连接



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：

- 基础版-（必需）基础版 许可证。

- **IPS** - 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

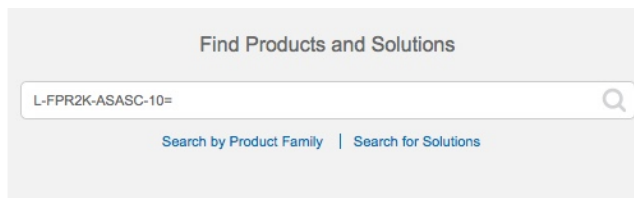
- 拥有 [智能软件管理器](#) 主帐户。
如果您还没有帐户，请点击此链接以 [设置新帐户](#)。通过智能软件管理器，您可以为组织创建一个主帐户。
- 您的智能软件许可帐户必须符合强加密 (3DES/AES) 许可证的要求，才能使用某些功能（已使用导出合规性标志启用）。

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 9: 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。

- 基础版 许可证：
 - L-FPR3110-BSE=
 - L-FPR3120-BSE=
 - L-FPR3130-BSE=
 - L-FPR3140-BSE=

- IPS、恶意软件防御和 URL 许可证组合：

- L-FPR3110T-TMC =
- L-FPR3120T-TMC =
- L-FPR3130T-TMC =
- L-FPR3140T-TMC =

当您将在上述 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-FPR3110T-TMC-1Y
- L-FPR3110T-TMC-3Y
- L-FPR3110T-TMC-5Y
- L-FPR3120T-TMC-1Y
- L-FPR3120T-TMC-3Y
- L-FPR3120T-TMC-5Y
- L-FPR3130T-TMC-1Y
- L-FPR3130T-TMC-3Y
- L-FPR3130T-TMC-5Y
- L-FPR3140T-TMC-1Y
- L-FPR3140T-TMC-3Y
- L-FPR3140T-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-FPR3K-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

使用设备 IP 地址或主机名将威胁防御手动注册到管理中心。

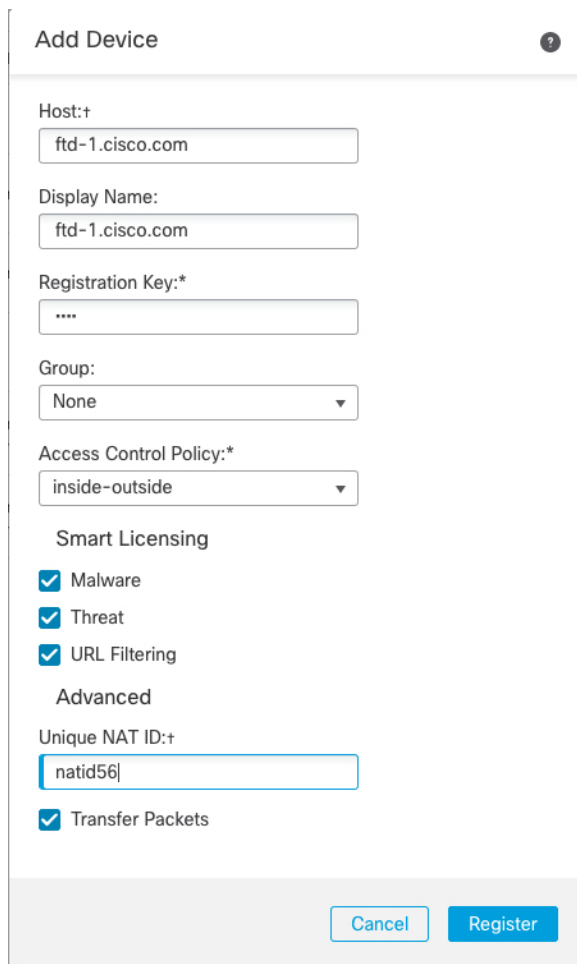
开始之前

- 收集您在 威胁防御 初始配置中设置的以下信息：
 - 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

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。



The screenshot shows the 'Add Device' configuration page. It contains the following fields and options:

- Host:** ftd-1.cisco.com
- Display Name:** ftd-1.cisco.com
- Registration Key:** ****
- Group:** None
- Access Control Policy:** inside-outside
- Smart Licensing:**
 - Malware
 - Threat
 - URL Filtering
- Advanced:**
 - Unique NAT ID:** natid56
 - Transfer Packets

At the bottom, there are two buttons: 'Cancel' and 'Register'.

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 37 页。

图 10: 新建策略

The screenshot shows a 'New Policy' configuration window. It has a title bar with a question mark icon. The form contains the following elements:

- Name:** A text input field containing 'ftd-ac-policy'.
- Description:** An empty text input field.
- Select Base Policy:** A dropdown menu currently set to 'None'.
- Default Action:** Three radio button options:
 - Block all traffic (This option is highlighted with a red rectangular box in the image)
 - Intrusion Prevention
 - Network Discovery
- Buttons:** 'Cancel' and 'Save' buttons are located at the bottom right of the form area.

- **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，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。

- 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 29 页。
②	配置 DHCP 服务器，第 32 页。
③	添加默认路由，第 33 页。
④	配置 NAT，第 34 页。
⑤	允许流量从内部传到外部，第 37 页。
⑥	部署配置，第 38 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。

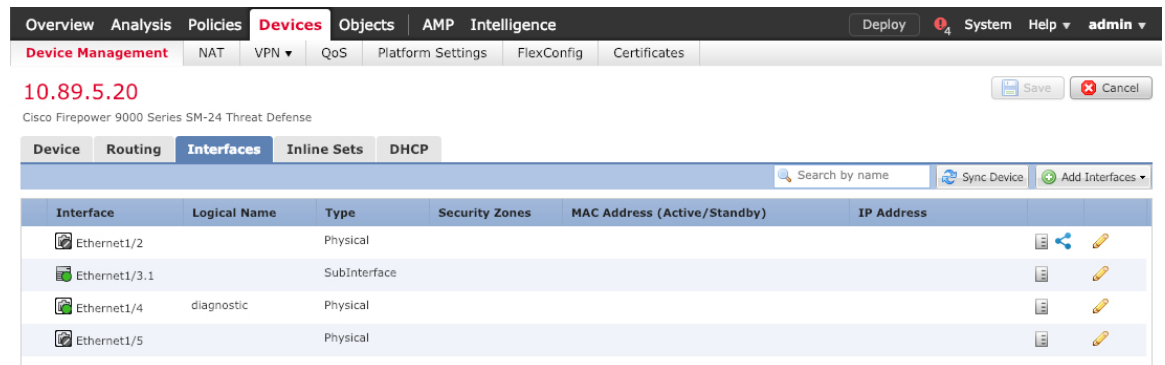
典型的边缘路由情况是通过 DHCP 从 ISP 获取外部接口地址，同时在内部接口上定义静态地址。

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 要从 40-Gb 接口（部分型号上可用）创建 4 x 10-Gb 分支接口，请点击接口的分支图标。

如果您已经在配置中使用了 40-Gb 接口，则必须在继续创建分支之前删除该配置。

步骤 4 点击要用于内部的接口的编辑 (✎)。

此时将显示一般 (**General**) 选项卡。

Edit Physical Interface ? X

General IPv4 IPv6 Advanced Hardware Configuration

Name: Enabled Management Only

Description:

Mode: ▼

Security Zone: ▼

Interface ID:

MTU: (64 - 9000)

OK Cancel

- 输入长度最大为 48 个字符的名称 (**Name**)。
例如，将接口命名为 **inside**。
- 选中启用 (**Enabled**) 复选框。
- 将模式 (**Mode**) 保留为无 (**None**)。
- 从安全区域 (**Security Zone**) 下拉列表选择一个现有的内部安全区域，或者点击新建 (**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。

- 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**

Edit Physical Interface

General **IPv4** IPv6 Advanced Hardware Configuration

IP Type: ▼

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

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

f) 点击**确定 (OK)**。

步骤 5 点击要用于外部的接口的 **编辑** (✎)。

此时将显示**一般 (General)** 选项卡。

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

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

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) 选中启用 (**Enabled**) 复选框。

c) 将模式 (**Mode**) 保留为无 (**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。

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

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

f) 点击确定 (OK)。

步骤 6 点击保存 (Save)。

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：

The screenshot shows the 'Add Server' dialog box. The 'Interface*' dropdown is set to 'inside'. The 'Address Pool*' text box contains '10.9.7.9-10.9.7.25', with '(2.2.2.10-2.2.2.20)' displayed to its right. The 'Enable DHCP Server' checkbox is checked. At the bottom, there are 'OK' and 'Cancel' buttons.

- **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 (Save)。

添加默认路由

默认路由通常指向可从外部接口访问的上游路由器。如果您将 DHCP 用作外部接口，则您的设备可能已经收到了默认路由。如果需要手动添加路由，则遵照此程序执行。如果收到来自 DHCP 服务器的默认路由，其将显示在设备 (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：

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

- 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。
- 可用网络 (Available Network) - 为 IPv4 默认路由选择 any-ipv4，为 IPv6 默认路由选择 any-ipv6，然后点击添加 (Add) 将其移至选定网络 (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。

The screenshot shows the Cisco Firepower 9000 Series SM-24 Threat Defense configuration interface. The top navigation bar includes tabs for Overview, Analysis, Policies, **Devices**, Objects, AMP, and Intelligence. Below this, there are sub-tabs for Device Management, NAT, VPN, QoS, Platform Settings, FlexConfig, and Certificates. The main content area shows the configuration for a device, with the Routing tab selected. On the left, a tree view shows routing protocols: OSPF, OSPFv3, RIP, BGP, **Static Route**, and Multicast Routing. The main table displays the following routes:

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

步骤 4 点击保存 (**Save**)。

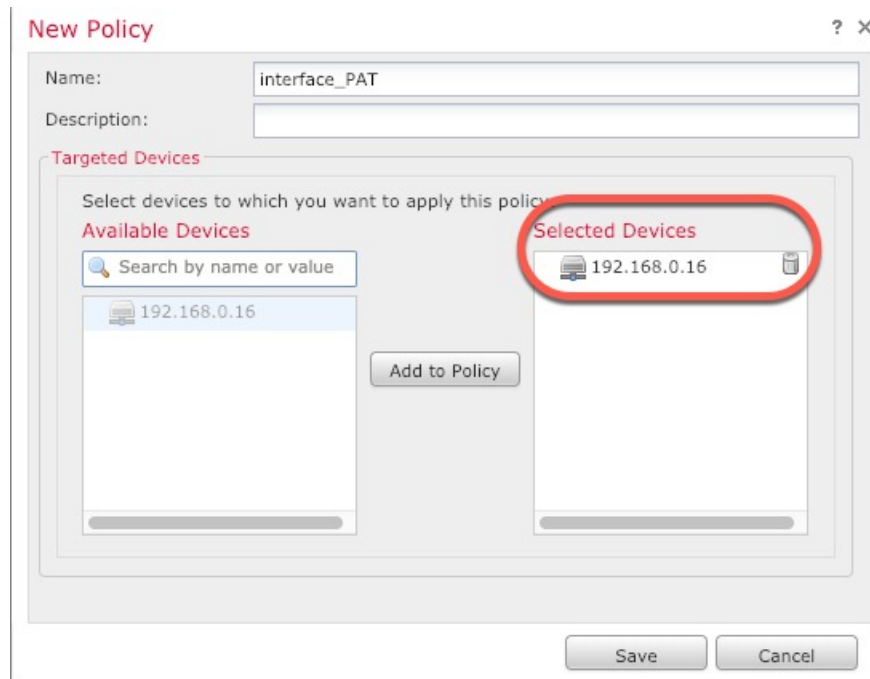
配置 NAT

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

过程

步骤 1 选择设备 (**Devices**) > **NAT**，然后点击新建策略 (**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**。

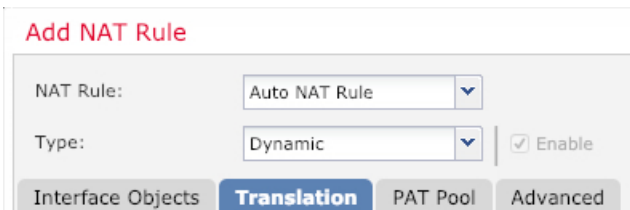


策略即已添加 管理中心。您仍然需要为策略添加规则。

步骤 3 点击添加规则 (**Add Rule**)。

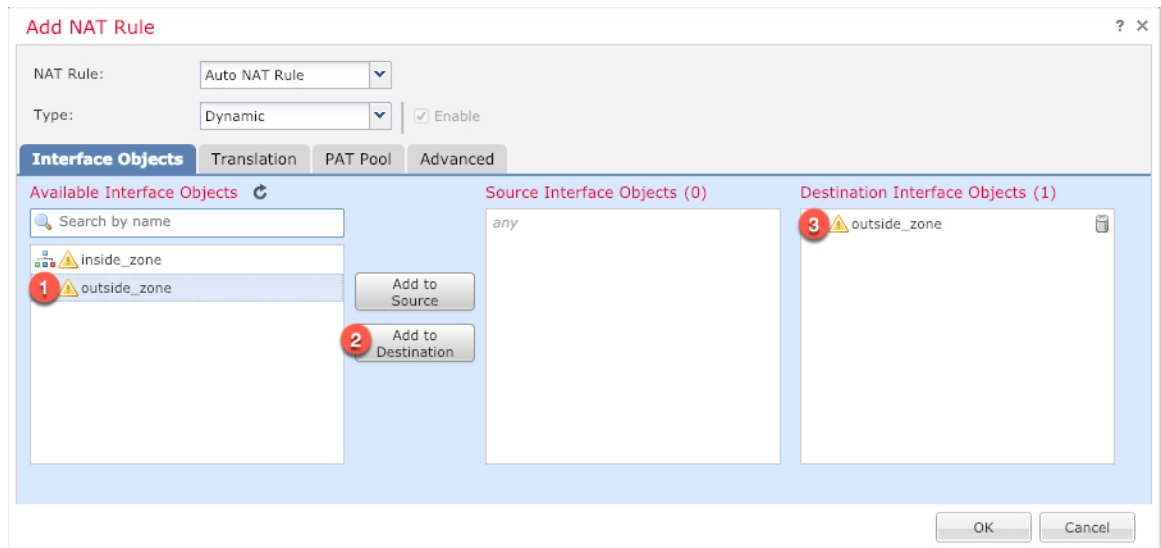
Add NAT Rule 对话框将显示。

步骤 4 配置基本规则选项：

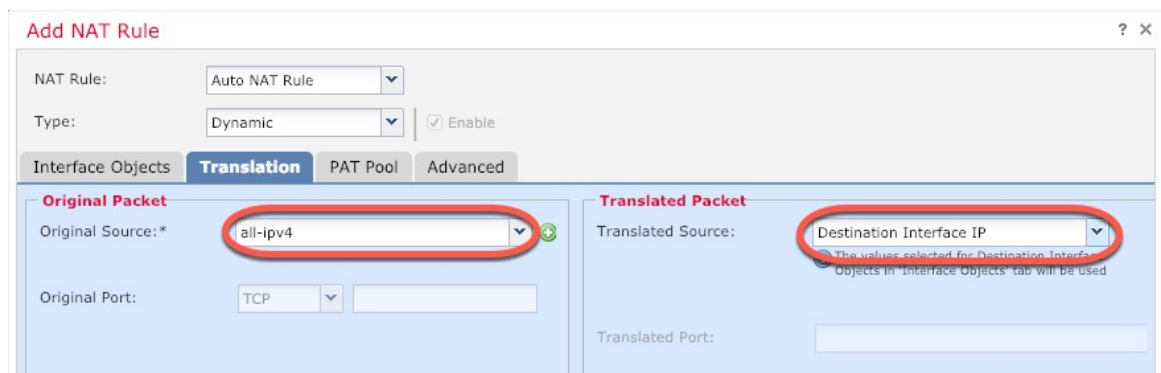


- **NAT 规则 (NAT Rule)** - 选择自动 NAT 规则 (**Auto NAT Rule**)。
- **类型 (Type)** - 选择动态 (**Dynamic**)。

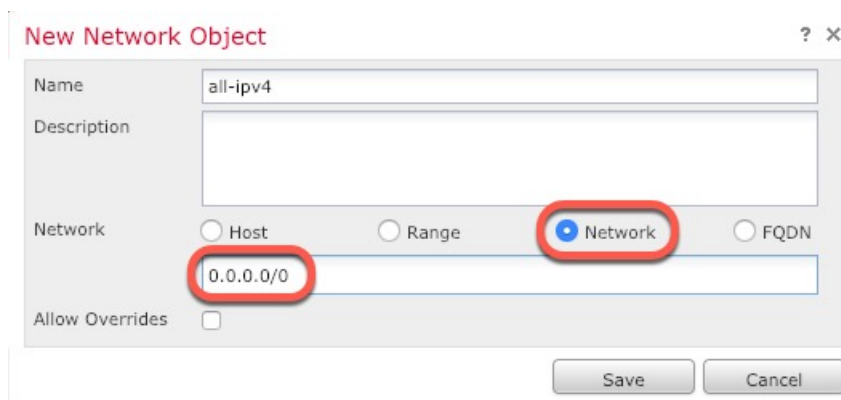
步骤 5 在 **Interface Objects** 页面，将 **Available Interface Objects** 区域中的外部区域添加到 **Destination Interface Objects** 区域。



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)。

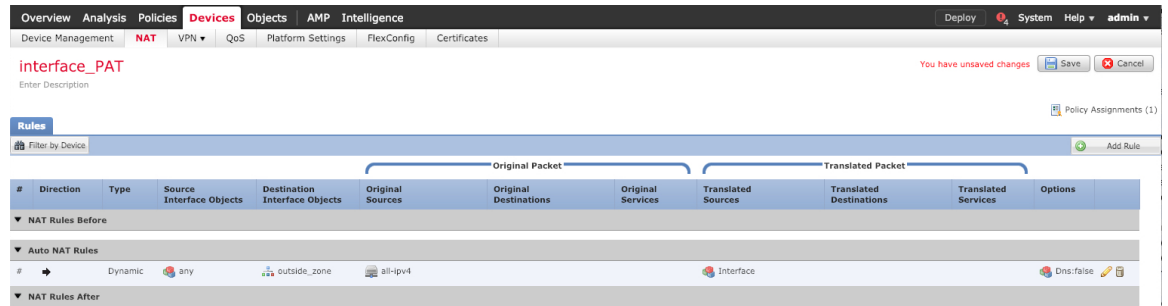


注释 您不能使用系统定义的 **any-ipv4** 对象，因为自动 NAT 规则在对象定义过程中添加 NAT，并且您无法编辑系统定义的对象。

- 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。

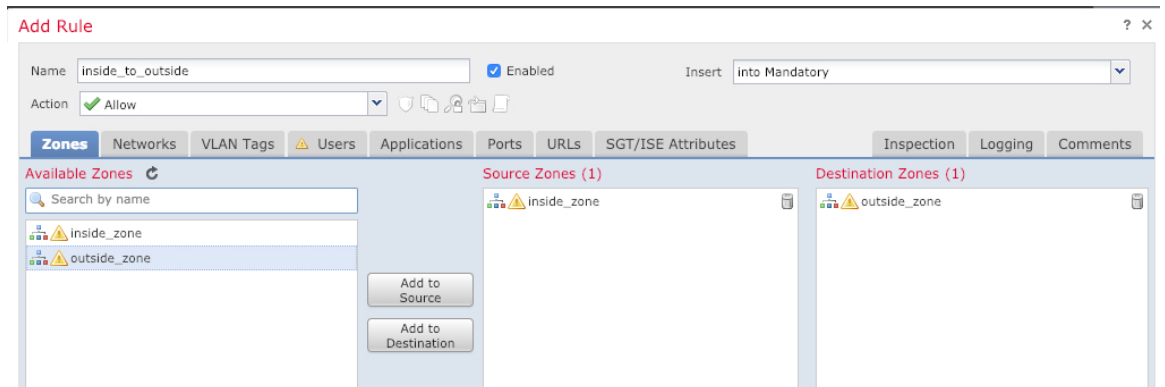
允许流量从内部传到外部

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：



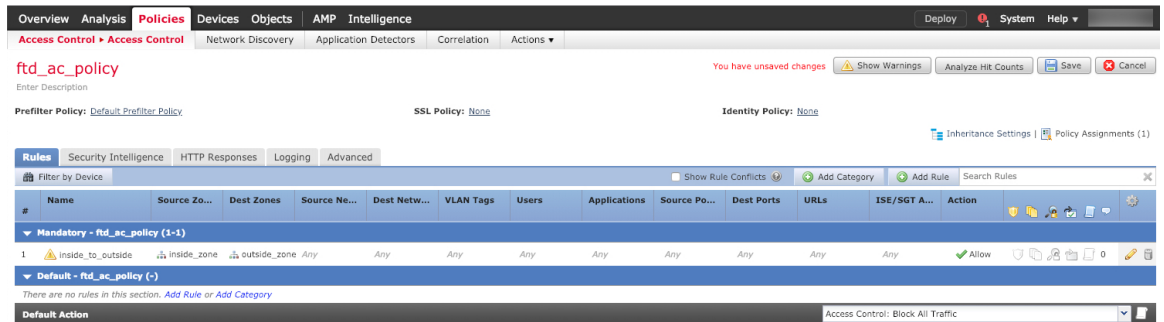
- 名称 (Name) - 为此规则命名，例如 **inside_to_outside**。
- 源区域 (Source Zones) - 从可用区域 (Available Zones) 中选择内部区域，然后点击添加到源 (Add to Source)。

- 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 (**Save**)。

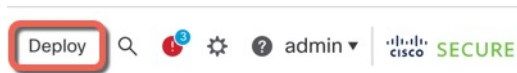
部署配置

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 11: 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 12: 全部部署

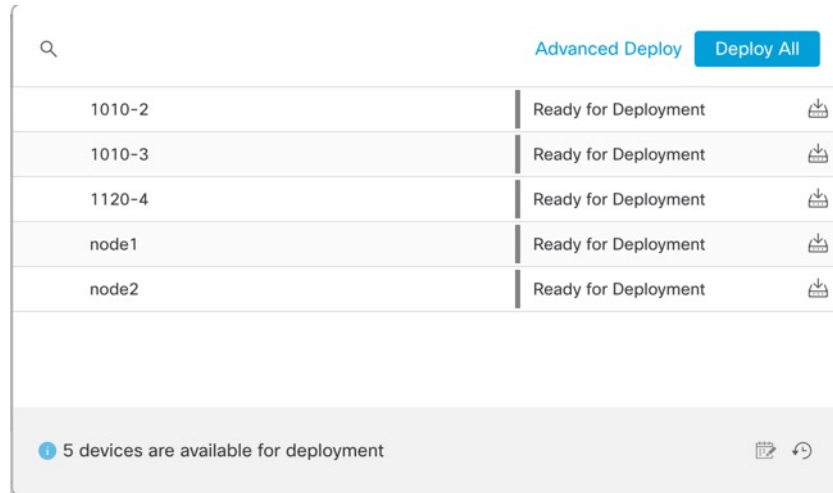
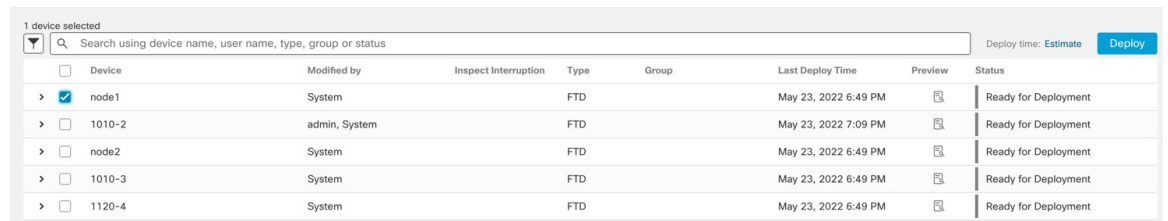
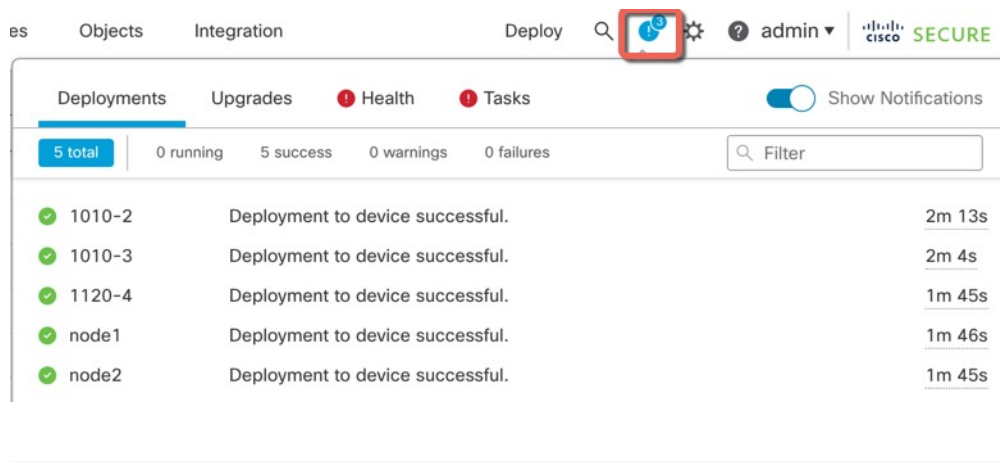


图 13: 高级部署



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 14: 部署状态



访问威胁防御和FXOS CLI

使用命令行界面 (CLI) 可设置系统以及对系统进行基本的故障排除。无法通过 CLI 会话配置策略。可以连接到控制台端口以访问 CLI。

也可以访问FXOS CLI以进行故障排除。



注释 您也可以通过 SSH 连接到 威胁防御 设备的管理接口。与控制台会话不同，SSH 会话默认使用 威胁防御 CLI，由此可使用 **connect fxos** 命令连接到 FXOS CLI。如果您为 SSH 连接打开某个数据接口，稍后可以连接到该接口上的地址。默认情况下，禁用 SSH 数据接口访问。此程序介绍控制台端口的访问（默认使用 FXOS CLI）。

过程

步骤 1 要登录 CLI，请将管理计算机连接到控制台端口。Secure Firewall 3100 配有一条 DB-9 转 RJ-45 串行电缆，所以您需要第三方串行转 USB 电缆进行连接。确保为您的操作系统安装必要的 USB 串行驱动程序（请参阅 Secure Firewall 3100 [硬件指南](#)）。控制台端口默认为 FXOS CLI。使用以下串行设置：

- 9600 波特率
- 8 个数据位
- 无奇偶校验
- 1 个停止位

您连接到 FXOS CLI。使用 **admin** 用户名和初始设置时设置的密码（默认值为 **Admin123**）登录 CLI。

示例：

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

步骤 2 访问威胁防御 CLI。

connect ftd

示例：

```
firepower# connect ftd
>
```

登录后，如需了解 CLI 中可用命令的相关信息，请输入 **help** 或 **?**。有关使用信息，请参阅 [Cisco Secure Firewall Threat Defense 命令参考](#)。

步骤 3 要退出 威胁防御 FTD CLI，请输入 **exit** 或 **logout** 命令。

此命令会将您重新导向至 FXOS CLI 提示。有关 FXOS CLI 中可用命令的相关信息，请输入 **?**。

示例：

```
> exit
firepower#
```

关闭防火墙电源

正确关闭系统非常重要。仅拔掉电源或按下电源开关可能会导致文件系统严重损坏。请记住，有许多进程一直在后台运行，拔掉或关闭电源不能正常关闭防火墙系统。

您可以使用管理中心设备管理页面来关闭设备电源，也可以使用 FXOS CLI。

使用管理中心关闭防火墙电源

正确关闭系统非常重要。仅拔掉电源或按下电源开关可能会导致文件系统严重损坏。请记住，有许多进程一直在后台运行，拔掉或关闭电源不能正常关闭防火墙。

您可以使用 管理中心 正确关闭系统。

过程

步骤 1 选择设备 > 设备管理。

步骤 2 在要重新启动的设备旁边，点击编辑图标 (✎)。

步骤 3 点击设备 (Device) 选项卡。

步骤 4 点击系统 (System) 部分中的关闭设备图标 (🔴)。

步骤 5 出现提示时，确认是否要关闭设备。

步骤 6 如果您与防火墙建立了控制台连接，请在防火墙关闭时留意系统提示。您将看到以下提示：

```
System is stopped.
It is safe to power off now.

Do you want to reboot instead? [y/N]
```

如果没有控制台连接，请等待大约 3 分钟以确保系统已关闭。

步骤 7 您现在可以关闭电源开关并在必要时拔下电源插头以物理方式断开机箱的电源。

在 CLI 关闭防火墙电源

您可以使用 FXOS CLI 安全地关闭系统并关闭设备。您可以通过连接到控制台端口来访问 CLI；请参阅[访问威胁防御和FXOS CLI，第 40 页](#)。

过程

步骤 1 在 FXOS CLI 中，连接到 local-mgmt:

```
firepower # connect local-mgmt
```

步骤 2 发出 **shutdown** 命令:

```
firepower(local-mgmt) # shutdown
```

示例:

```
firepower(local-mgmt) # shutdown
This command will shutdown the system. Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense.....ok
```

步骤 3 留意防火墙关闭时的系统提示。您将看到以下提示:

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

步骤 4 您现在可以关闭电源开关并在必要时拔下电源插头以物理方式断开机箱的电源。

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》](#)。



第 3 章

使用远程管理中心部署威胁防御

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[哪种操作系统和管理器适合您？](#)，第 1 页。本章适用于在中央总部使用管理中心的远程分支机构的威胁防御。

每个威胁防御会控制、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。

- 中央总部的管理员在 CLI 上或使用设备管理器预配置威胁防御，然后将威胁防御发送到远程分支机构。
- 分支机构管理员连接并打开威胁防御电源。
- 中央管理员使用管理中心完成威胁防御的配置。



注释 远程分支机构部署要求使用 6.7 或更高版本。

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。

- [开始之前](#)，第 44 页
- [端到端程序](#)，第 44 页
- [远程管理的工作原理](#)，第 46 页
- [中央管理员预配置](#)，第 48 页

- [分支机构安装](#)，第 59 页
- [中央管理员后配置](#)，第 61 页

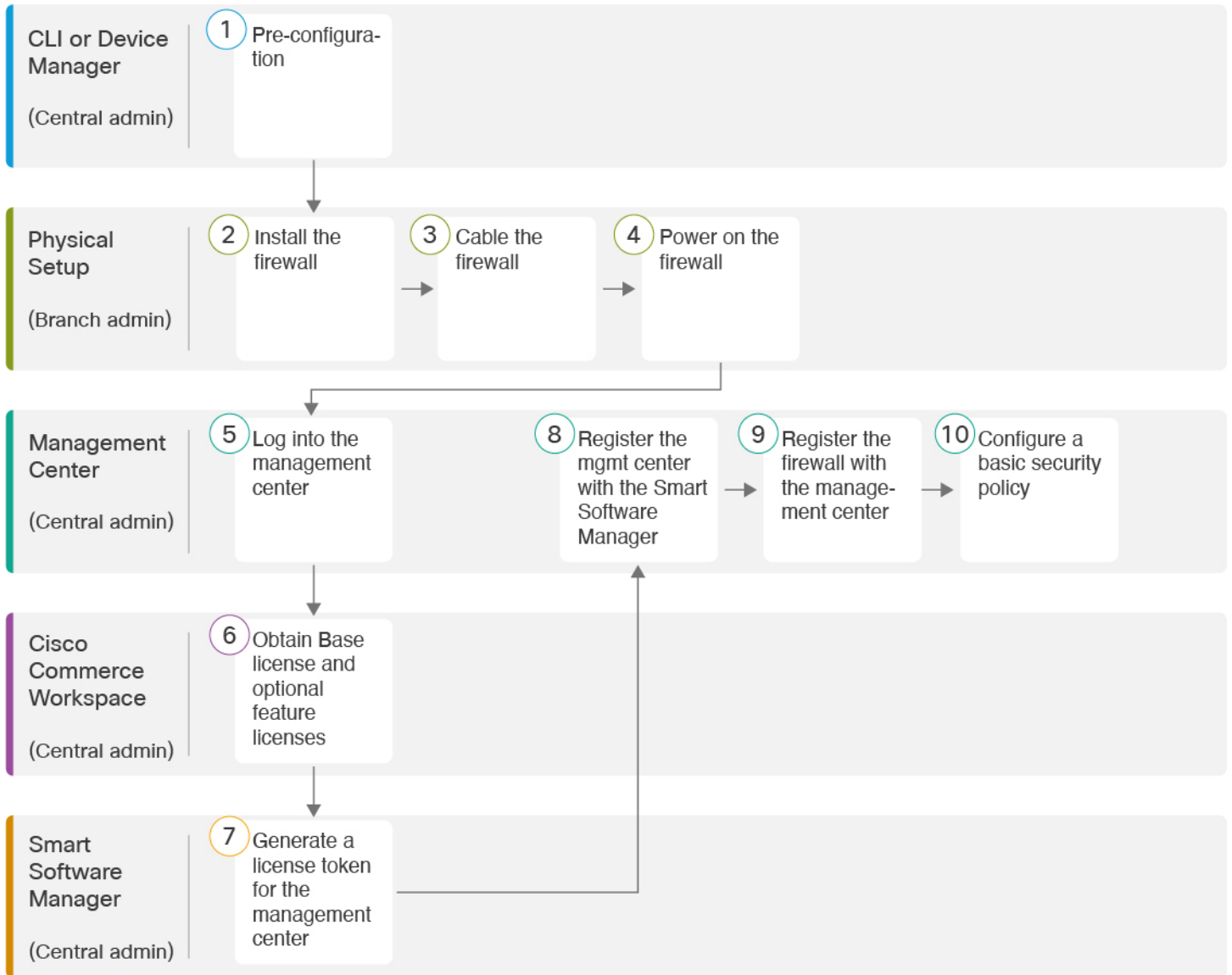
开始之前

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 [威胁防御](#) 和 [管理中心](#)。

图 15: 端到端程序



①	CLI 或 设备管理器 (中央管理员)	<ul style="list-style-type: none"> • (可选) 检查软件并安装新版本, 第 48 页 • 使用 CLI 进行预配置, 第 54 页。 • 使用设备管理器进行预配置, 第 50 页
②	物理设置 (分支机构管理员)	安装防火墙。请参阅 硬件安装指南 。
③	物理设置 (分支机构管理员)	连接防火墙的电缆 , 第 59 页。

4	物理设置 (分支机构管理员)	打开防火墙电源, 第 60 页
5	管理中心 (中央管理员)	登录管理中心, 第 23 页。
6	Cisco Commerce Workspace (中央管理员)	购买基本许可证和可选功能许可证 (获取管理中心的许可证, 第 62 页)。
7	智能软件管理器 (中央管理员)	为 管理中心 (获取管理中心的许可证, 第 62 页) 生成许可证令牌。
8	管理中心 (中央管理员)	向智能许可证服务器 (获取管理中心的许可证, 第 62 页) 注册管理中心。
9	管理中心 (中央管理员)	向管理中心注册威胁防御, 第 64 页。
10	管理中心 (中央管理员)	配置基本安全策略, 第 67 页。

远程管理的工作原理

要允许 管理中心 通过互联网管理 威胁防御, 请使用外部接口而不是管理接口进行 管理中心 管理。由于大多数远程分支机构都只有一个互联网连接, 因此外部管理中心访问让集中管理成为了可能。



注释 管理连接是信道自身与设备之间的 SSL 加密的安全通信信道。出于安全考虑, 您无需通过额外的加密隧道 (例如站点到站点 VPN) 来运行此流量。例如, 如果 VPN 发生故障, 您将失去管理连接, 因此建议使用简单的管理路径。



注释 您可以将任何数据接口用于管理器访问, 例如, 如果您有内部 管理中心, 则使用内部接口。但是, 本指南主要介绍外部接口访问, 因为它是远程分支机构最可能遇到的场景。

管理接口是一个与威胁防御数据接口分开配置的特殊接口, 它有自己的网络设置。即使您在数据接口上启用了管理器访问, 也仍会使用管理接口网络设置。所有管理流量会继续源自或发往管理接口。如果在数据接口上启用了管理器访问, 威胁防御 会将传入管理流量通过背板转发到管理接口。对于传出管理流量, 管理接口会通过背板将流量转发到数据接口。

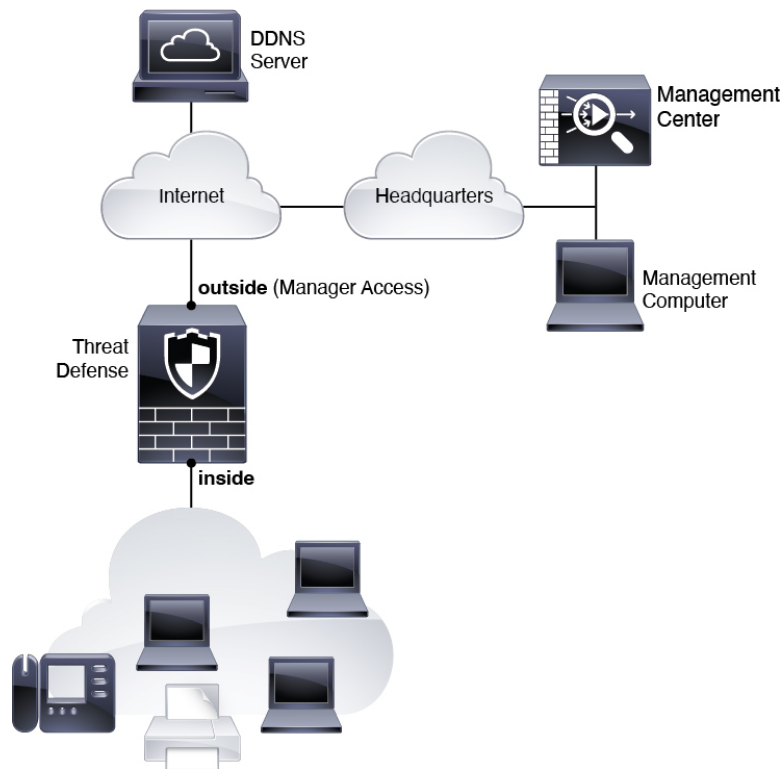
从数据接口进行管理器访问具有以下限制：

- 只能在物理数据接口上启用管理器访问。不能使用子接口或 EtherChannel。您还可以使用管理中心在单个辅助接口上启用管理器访问，以实现冗余。
- 此接口不能是仅管理接口。
- 仅路由防火墙模式，使用路由接口。
- 不支持 PPPoE。如果您的 ISP 需要 PPPoE，则必须在威胁防御与 WAN 调制解调器之间放入支持 PPPoE 的路由器。
- 接口只能位于全局 VRF 中。
- 默认不对数据接口启用 SSH，因此必须稍后使用管理中心来启用 SSH。由于管理接口网关将更改为数据接口，因此您也无法启动从远程网络到管理接口的 SSH 会话，除非您使用 **configure network static-routes** 命令为管理接口添加静态路由。
- 您不能使用单独的管理接口和仅事件接口。
- 不支持集群技术。在这种情况下，必须使用管理接口。
- 不支持高可用性。在这种情况下，必须使用管理接口。

下图显示了位于中央总部的管理中心和在外部接口上具有管理器访问权限的威胁防御。

威胁防御或管理中心需要公共 IP 地址或主机名以允许入站管理连接；您需要知道该 IP 地址以进行初始设置。您还可以选择为外部接口配置动态 DNS (DDNS)，以适应不断变化的 DHCP IP 分配。

图 16:



中央管理员预配置

您需要先手动预配置 威胁防御，然后再将其发送到分支机构。

（可选）检查软件并安装新版本

要检查软件版本并在必要时安装不同的版本，请执行以下步骤。我们建议您在配置防火墙之前安装目标版本。或者，您也可以在启动并运行后执行升级，但升级（保留配置）可能需要比按照此程序花费更长的时间。

我应该运行什么版本？

思科建议运行软件下载页面上的版本号旁边标有金色星号的 **Gold Star** 版本。您还可以参考 <https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html> 中所述的发布策略；例如，此公告描述短期版本编号（包含最新功能）、长期版本编号（较长时间的维护版本和补丁）或额外长期版本编号（最长期限的维护版本和补丁，用于政府认证）。

过程

步骤 1 连接到控制台端口。有关详细信息，请参阅[访问威胁防御和FXOS CLI](#)，第 77 页。

使用用户名 **admin** 和默认密码 **Admin123** 登录。

您连接到 FXOS CLI。第一次输入登录时，系统会提示您更改密码。此密码也用于 SSH 的威胁防御登录。

注释 如果密码已更改，但您不知道，则必须执行出厂重置以将密码重置为默认值。有关 [出厂重置程序](#) 的信息，请参阅 [FXOS 故障排除指南](#)。

示例:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: *****
Confirm new password: *****
Your password was updated successfully.

[...]

firepower#
```

步骤 2 在 FXOS CLI 中，显示正在运行的版本。

scope ssa

show app-instance

示例:

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name      Slot ID   Admin State   Operational State   Running Version Startup
Version Cluster Oper State
-----
ftd                   1         Enabled       Online               7.2.0.65           7.2.0.65
                        Not Applicable
```

步骤 3 如果要安装新版本，请执行这些步骤。

a) 如果要为管理接口设置静态 IP 地址，请参阅[使用 CLI 进行预配置](#)，第 54 页。默认情况下，管理接口将使用 DHCP。

您需要从可通过管理接口访问的服务器下载新的映像。

- b) 执行《FXOS 故障排除指南》中的重新映像程序。

使用设备管理器进行预配置

连接到设备管理器以执行威胁防御的初始设置。当您使用设备管理器执行初始设置时，如果您切换到管理中心进行管理，除管理接口和管理器访问设置外，在设备管理器中完成的所有接口配置都将保留。请注意，不会保留其他默认配置设置，例如访问控制策略或安全区。使用 CLI 时，只有管理接口和管理器访问设置会被保留（例如，不保留默认的内部接口配置）。

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》。在设置威胁防御之前，您需要知道管理中心 IP 地址或主机名。
- 使用 Firefox、Chrome、Safari、Edge 或 Internet Explorer 的当前版本。

过程

步骤 1 将管理计算机连接到内部（以太网 1/2）接口。

步骤 2 打开防火墙电源。

注释 首次启动威胁防御时，初始化大约需要 15 到 30 分钟。

步骤 3 登录设备管理器。

- a) 在浏览器中输入以下 URL: **https://192.168.95.1**
- b) 使用用户名 **admin** 和默认密码 **Admin123** 登录。
- c) 系统会提示您阅读和接受“最终用户许可协议”并更改管理员密码。

步骤 4 首次登录设备管理器以完成初始配置时，请使用设置向导。您可以选择通过点击页面底部的**跳过设备设置 (Skip device setup)** 来跳过安装向导。

完成安装向导后，除了内部接口 (Ethernet1/2) 的默认配置外，您还将拥有外部（以太网 1/1）接口的配置，该接口会在您切换到管理中心管理接口时进行维护。

a) 为外部接口和管理接口配置以下选项，然后点击**下一步 (Next)**。

1. **外部接口地址 (Outside Interface Address)** - 此接口通常是互联网网关，并且可用作管理器访问接口。在初始设备设置期间，您不能选择其他外部接口。第一个数据接口是默认的外部接口。

如果要使用与外部（或内部）不同的接口来进行管理器访问，则必须在完成安装向导后手动配置该接口。

配置 IPv4 - 外部接口的 IPv4 地址。可以使用 DHCP，也可以手动输入静态 IP 地址、子网掩码和网关。另外，也可以选择关，不配置 IPv4 地址。您无法使用安装向导配置 PPPoE。如果

接口连接到 DSL、电缆调制解调器或 ISP 的其他连接，并且 ISP 使用 PPPoE 来提供 IP 地址，则可能需要使用 PPPoE。您可以在完成向导后配置 PPPoE。

配置 Ipv6 - 外部接口的 Ipv6 地址可以使用 DHCP，也可以手动输入静态 IP 地址、前缀和网关。另外，也可以选择关，不配置 IPv6 地址。

2. 管理接口

如果在 CLI 中执行了初始设置，您将不会看到管理接口设置。

即使您在数据接口上启用了管理器访问，也仍会使用管理接口设置。例如，通过数据接口在背板上路由的管理流量将使用管理接口 DNS 服务器解析 FQDN，而非使用数据接口 DNS 服务器。

DNS 服务器 - 系统管理地址的 DNS 服务器。输入 DNS 服务器的一个或多个地址以解析名称。默认值为 OpenDNS 公共 DNS 服务器。如果您编辑字段并想要恢复默认值，请点击使用 **OpenDNS (Use OpenDNS)** 以重新将合适的 IP 地址载入字段。

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

b) 配置时间设置 (NTP) (Time Setting [NTP]) 并点击下一步 (Next)。

1. 时区 - 选择系统时区。

2. NTP 时间服务器 - 选择使用默认 NTP 服务器，还是手动输入 NTP 服务器的地址。可以添加多个服务器来提供备份。

c) 选择启动 90 日评估期而不注册。

不要向智能软件管理器注册威胁防御；所有许可均在管理中心上执行。

d) 点击完成。

e) 系统将提示您选择云管理 (Cloud Management) 或独立 (Standalone)。对于管理中心管理，请选择独立 (Standalone)，然后选择知道了 (Got It)。

步骤 5 (可能需要) 配置管理接口。请参阅设备 > 接口上的管理接口。

管理接口必须将网关设置为数据接口。默认情况下，管理接口从 DHCP 接收 IP 地址和网关。如果您没有从 DHCP 接收到网关（例如，您没有将此接口连接到网络），则网关将默认为数据接口，并且您无需进行任何配置。如果您从 DHCP 接收到了网关，则需要使用静态 IP 地址配置此接口，并将该网关设置为数据接口。

步骤 6 如果要配置其他接口，包括要用于管理器访问的外部或内部接口，请选择设备 (Device)，然后点击接口 (Interfaces) 摘要中的链接。

有关在设备管理器中配置接口的更多信息，请参阅在设备管理器中配置防火墙，第 105 页。在向管理中心注册设备时，不会保留其他设备管理器配置。

步骤 7 选择设备 > 系统设置 > 集中管理，然后点击继续设置管理中心管理。

步骤 8 配置管理中心/CDO 详细信息。

图 17: 管理中心/CDO 详细信息

Configure Connection to Management Center or CDO


Provide details to register to the management center/CDO.

Management Center/CDO Details

Do you know the Management Center/CDO hostname or IP address?

Yes No


Threat Defense



10.89.5.16
fe80::6a87:c6ff:fea6:4c00/64

→

Management Center/CDO



10.89.5.35

Management Center/CDO Hostname or IP Address

10.89.5.35

Management Center/CDO Registration Key

●●●● 👁

NAT ID

Required when the management center/CDO hostname or IP address is not provided. We recommend always setting the NAT ID even when you specify the management center/CDO hostname or IP address.

11203

Connectivity Configuration

Threat Defense Hostname

1120-3

DNS Server Group

CustomDNSServerGroup ▼

Management Center/CDO Access Interface

Data Interface

Please select an interface ▼

Management Interface [View details](#)

CANCEL
CONNECT

- a) 对于 **是否知道管理中心/CDO 主机名或 IP 地址**，如果您可以使用 IP 地址或主机名访问管理中心，请点击 **是**，如果管理中心位于 NAT 之后或没有公共 IP 地址或主机名，请点击 **否**。

必须至少有一个设备（管理中心或威胁防御设备）具有可访问的 IP 地址，才能在两个设备之间建立双向 SSL 加密的通信通道。

- b) 如果您选择是，则输入 **管理中心/CDO 主机名/IP 地址**。
- c) 指定 **管理中心/CDO 注册密钥**。

此密钥是您选择的一次性注册密钥，注册威胁防御设备时也要在管理中心上指定它。注册密钥不得超过 37 个字符。有效字符包括字母数字（A - Z、a - z、0 - 9）和连字符 (-)。此 ID 可用于将多台设备注册到管理中心。

- d) 指定 **NAT ID**。

此 ID 是您选择的唯一一次性字符串，您还需要在管理中心上指定它。如果仅在其中一台设备上指定 IP 地址，则此字段必填；但建议您即使在知道两台设备的 IP 地址时，仍指定 NAT ID。NAT ID 不得超过 37 个字符。有效字符包括字母数字（A - Z、a - z、0 - 9）和连字符 (-)。此 ID 不能用于将任何其他设备注册到管理中心。NAT ID 与 IP 地址结合使用，用于验证连接是否来自正确的设备；只有在对 IP 地址/NAT ID 进行身份验证后，才会检查注册密钥。

步骤 9 配置连接配置。

- a) 指定 **FTD 主机名**。

此 FQDN 将用于外部接口，或您为 **管理中心/CDO 访问接口 (Management Center/CDO Access Interface)** 选择的任何接口。

- b) 指定 **DNS 服务器组**。

选择现有组或创建一个新组。默认 DNS 组名为 **CiscoUmbrellaDNSServerGroup**，其中包括 OpenDNS 服务器。

此设置设定数据接口 DNS 服务器。您使用安装向导设置的管理 DNS 服务器用于管理流量。数据 DNS 服务器用于 DDNS（如果已配置）或适用于此接口的安全策略。您可能会选择用于管理的相同 DNS 服务器组，因为管理和数据流量都通过外部接口到达 DNS 服务器。

在管理中心上，数据接口 DNS 服务器在您分配给此威胁防御的平台设置策略中配置。当您威胁防御添加到管理中心时，本地设置将保留，并且 DNS 服务器不会添加到平台设置策略。但是，如果稍后将平台设置策略分配给包含 DNS 配置的威胁防御，则该配置将覆盖本地设置。我们建议您主动配置与此设置匹配的 DNS 平台设置，以使管理中心和威胁防御同步。

此外，仅当在初始注册时发现 DNS 服务器，管理中心才会保留本地 DNS 服务器。

- c) 对于 **管理中心/CDO 访问接口 (Management Center/CDO Access Interface)**，请选择外部 (**outside**)。

您可以选择任何已配置的接口，但本指南假定您使用的是外部接口。

步骤 10 如果您选择了外部之外的其他数据接口，那么请添加默认路由。

您将看到一条消息，要求您检查是否有通过接口的默认路由。如果您选择了外部接口，那么您已经在安装向导中配置了此路由。如果您选择了其他接口，那么需要在连接到管理中心之前手动配置默认路由。有关在设备管理器中配置静态路由的更多信息，请参阅在 [设备管理器中配置防火墙](#)，第 105 页。

步骤 11 点击添加动态 DNS (DDNS) 方法 (Add a Dynamic DNS [DDNS] method)。

如果威胁防御的 IP 地址发生变化，DDNS 可确保管理中心接通完全限定域名 (FQDN) 内的威胁防御。参阅 **设备 > 系统设置 > DDNS 服务配置** 动态 DNS。

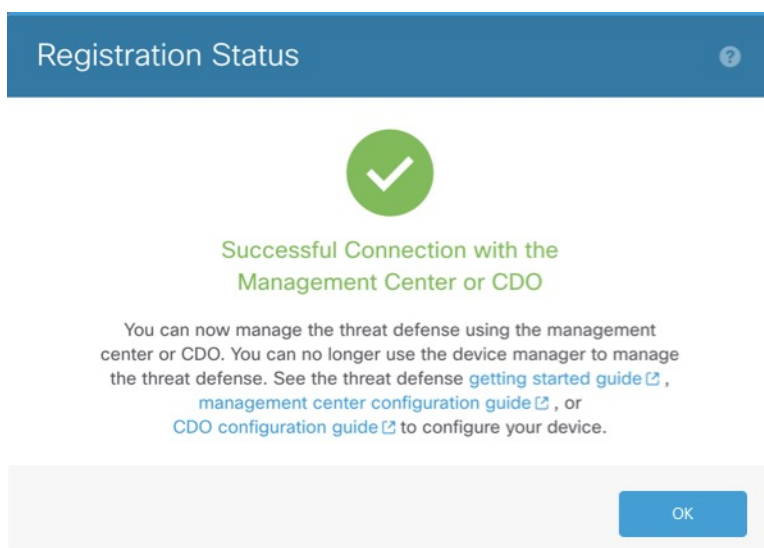
如果您在将威胁防御添加到管理中心之前配置 DDNS，则威胁防御会自动为思科受信任根 CA 捆绑包中的所有主要 CA 添加证书，以便威胁防御可以验证用于 HTTPS 连接的 DDNS 服务器证书。威胁防御支持使用 DynDNS 远程 API 规范 (<https://help.dyn.com/remote-access-api/>) 的任何 DDNS 服务器。

步骤 12 点击 **连接 (Connect)**。注册状态对话框显示切换到管理中心的当前状态。在 **保存管理中心/CDO 注册设置** 步骤后，转到管理中心，并添加防火墙。

如果要取消切换到管理中心，请点击 **取消注册**。否则，请在 **保存管理中心/CDO 注册设置** 步骤之后关闭设备管理器浏览器窗口。如果这样做，该过程将暂停，并且只有在您重新连接到设备管理器时才会恢复。

如果您在 **保存管理中心/CDO 注册设置** 步骤后保持连接到设备管理器，您最终将看到与管理中心的成功连接或 CDO 对话框。您将断开与设备管理器的连接。

图 18: 成功连接



使用 CLI 进行预配置

连接到威胁防御 CLI 以执行初始设置。使用 CLI 进行初始配置时，只有管理接口和管理器访问接口设置会被保留。当您使用设备管理器执行初始设置时，如果您切换到管理中心进行管理，除管理接口和管理器访问接口设置外，在设备管理器中完成的所有接口配置都将保留。请注意，不会保留其他默认配置设置，例如访问控制策略。

Before you begin

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](#)》。在设置威胁防御之前，您需要知道管理中心 IP 地址或主机名。

Procedure

步骤 1 打开防火墙电源。

Note 首次启动威胁防御时，初始化大约需要 15 到 30 分钟。

步骤 2 连接到控制台端口上的威胁防御 CLI。

控制台端口连接到 FXOS CLI。

步骤 3 使用用户名 **admin** 和密码 **Admin123** 登录。

第一次登录 FXOS 时，系统会提示您更改密码。此密码也用于 SSH 的威胁防御登录。

Note 如果密码已更改，但您不知道，则必须重新映像设备以将密码重置为默认值。有关[重新映像程序](#)的信息，请参阅 [FXOS 故障排除指南](#)。

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: *****
Confirm new password: *****
Your password was updated successfully.

[...]

firepower#
```

步骤 4 连接到威胁防御 CLI。

connect ftd

Example:

```
firepower# connect ftd
>
```

步骤 5 第一次登录威胁防御时，系统会提示您接受《最终用户许可协议》(EULA)和，如果使用 SSH 连接，则会提示您更改 admin 密码。然后，您将看到管理接口设置的 CLI 设置脚本。

即使您在数据接口上启用了管理器访问，也仍会使用管理接口设置。

Note 除非清除配置，否则无法重复 CLI 安装向导（例如，通过重新建立映像）。但是，可以稍后在 CLI 中使用 **configure network** 命令更改所有这些设置。请参阅 [Cisco Secure Firewall Threat Defense 命令参考](#)。

默认值或以前输入的值会显示在括号中。要接受之前输入的值，请按 **Enter** 键。

请参阅以下准则：

- **通过 DHCP 或手动配置 IPv4? (Configure IPv4 via DHCP or manually?)**— 选择 **manual**。虽然您不打算使用管理接口，但必须设置 IP 地址，例如专用地址。如果管理接口设置为 DHCP，则无法配置数据接口用于管理，因为默认路由（必须是 **data-interfaces**，请参阅下一个要点）可能会被接收自 DHCP 服务器的路由覆盖。
- **输入管理接口的 IPv4 默认网关 (Enter the IPv4 default gateway for the management interface)**— 将网关设置为 **data-interfaces**。此设置将在背板上转发管理流量，因此可路由通过管理器访问数据接口。
- **如果您的网络信息已更改，需要重新连接** - 如果您已建立 SSH 连接，则连接将断开。如果您的管理计算机在管理网络上，则可以使用新的 IP 地址和密码来重新连接。由于默认路由更改（通过数据接口），您将无法从远程网络重新连接。控制台连接不会受影响。
- **本地管理设备?** - 输入 **否** 以使用管理中心。回答 **yes** 意味着您将改为使用设备管理器。
- **配置防火墙模式? (Configure firewall mode?)**— 输入 **routed**。只有路由防火墙模式支持外部管理器访问。

Example:

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress. Please stand by.
You must change the password for 'admin' to continue.
Enter new password: *****
Confirm new password: *****
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]:
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...
```

```
Update policy deployment information
- add device configuration
- add network discovery
- add system policy
```

You can register the sensor to a Firepower Management Center and use the Firepower Management Center to manage it. Note that registering the sensor to a Firepower Management Center disables on-sensor Firepower Services management capabilities.

When registering the sensor to a Firepower Management Center, a unique alphanumeric registration key is always required. In most cases, to register a sensor to a Firepower Management Center, you must provide the hostname or the IP address along with the registration key.

```
'configure manager add [hostname | ip address ] [registration key ]'
```

However, if the sensor and the Firepower Management Center are separated by a NAT device, you must enter a unique NAT ID, along with the unique registration key.

```
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'
```

Later, using the web interface on the Firepower Management Center, you must use the same registration key and, if necessary, the same NAT ID when you add this sensor to the Firepower Management Center.

```
>
```

步骤 6 配置用于管理器访问的外部接口。

configure network management-data-interface

然后，系统会提示您为外部接口配置基本网络设置。请参阅以下有关使用此命令的详细信息：

- 如果您要使用数据接口进行管理，则管理接口无法使用 DHCP。如果在初始设置期间没有手动设置 IP 地址，则可以使用 **configure network {ipv4 | ipv6} manual** 命令立即设置它。如果您尚未将管理接口网关设置为 **data-interfaces**，此命令将立即设置它。
- 当您 将威胁防御 添加到 管理中心时， 管理中心 会发现并维护接口配置，包括以下设置：接口名称和 IP 地址、网关静态路由、DNS 服务器和 DDNS 服务器。有关 DNS 服务器配置的详细信息，请参阅下文。在管理中心中，您可以稍后对管理器访问接口配置进行更改，但要确保更改不会阻止威胁防御或管理中心重新建立管理连接。如果管理连接中断，威胁防御将包含 **configure policy rollback** 命令以恢复以前的部署。
- 如果配置 DDNS 服务器更新 URL，则威胁防御会自动添加来自 Cisco 受信任根 CA 捆绑包的所有主要 CA 证书，以便威胁防御可以验证用于 HTTPS 连接的 DDNS 服务器证书。威胁防御支持使用 DynDNS 远程 API 规范 (<https://help.dyn.com/remote-access-api/>) 的任何 DDNS 服务器。
- 此命令设置数据接口 DNS 服务器。使用设置脚本（或使用 **configure network dns servers** 命令）设置的管理 DNS 服务器用于管理流量。数据 DNS 服务器用于 DDNS（如果已配置）或适用于此接口的安全策略。

在管理中心上，数据接口 DNS 服务器在您分配给此威胁防御的平台设置策略中配置。当您 将威胁防御 添加到 管理中心时，本地设置将保留，并且 DNS 服务器不会添加到平台设置策略。但是，如果稍后将平台设置策略分配给包含 DNS 配置的威胁防御，则该配置将覆盖本地设置。我们建议您主动配置与此设置匹配的 DNS 平台设置，以使管理中心和威胁防御同步。

此外，仅当在初始注册时发现 DNS 服务器，管理中心才会保留本地 DNS 服务器。例如，如果您使用管理接口注册了设备，但随后使用 **configure network management-data-interface** 命令配

置数据接口，则必须在管理中心中手动配置所有这些设置（包括 DNS 服务器），以便与威胁防御配置匹配。

- 将威胁防御注册到管理中心后，您可以将该管理接口更改为管理接口或另一数据接口。
- 您在安装向导中设置的 FQDN 将用于此接口。
- 您可以通过命令清除整个设备配置；在恢复场景中可使用此选项，但我们不建议您在初始设置或正常操作中使用它。
- 要禁用数据管理，请输入 **configure network management-data-interface disable** 命令。

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://deanwinchester:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

步骤 7 (Optional) 限制在特定网络上通过数据接口访问 管理中心。

configure network management-data-interface client ip_address netmask

默认情况下，允许所有网络。

步骤 8 确定将管理此威胁防御的管理中心。

configure manager add {hostname | IPv4_address | IPv6_address | **DONTRESOLVE**} regkey [nat_id]

- {hostname | IPv4_address | IPv6_address | **DONTRESOLVE**} - 指定管理中心的 FQDN 或 IP 地址。如果管理中心不是直接可寻址的，请使用 **DONTRESOLVE**。必须至少有一个设备（管理中心或威胁防御）具有可访问的 IP 地址，才能在两个设备之间建立双向 SSL 加密的通信通道。如果在此命令中指定 **DONTRESOLVE**，则威胁防御必须有可访问的 IP 地址或主机名。
- reg_key - 指定您选择的一次性注册密钥，注册威胁防御时也要在管理中心上指定它。注册密钥不得超过 37 个字符。有效字符包括字母数字（A - Z、a - z、0 - 9）和连字符 (-)。
- nat_id - 指定了您选择的唯一一次性字符串，您还需要在管理中心上指定它。如果使用数据接口进行管理，则必须同时在威胁防御和管理中心上指定注册用的 NAT ID。NAT ID 不得超过 37 个字符。有效字符包括字母数字（A - Z、a - z、0 - 9）和连字符 (-)。此 ID 不能用于将任何其他设备注册到管理中心。

Example:

```
> configure manager add fmc-1.example.com regk3y78 natid56
Manager successfully configured.
```

步骤 9 关闭威胁防御，以便将设备发送到远程分支机构。

正确关闭系统非常重要。仅拔掉电源或按下电源开关可能会导致文件系统严重损坏。请记住，有许多进程一直在后台运行，拔掉或关闭电源不能正常关闭系统。

- a) 输入 **shutdown** 命令。
- b) 观察电源 LED 和状态 LED 以验证机箱是否已断电（不亮）。
- c) 在机箱成功关闭电源后，您可以在必要时拔下电源插头以物理方式断开机箱的电源。

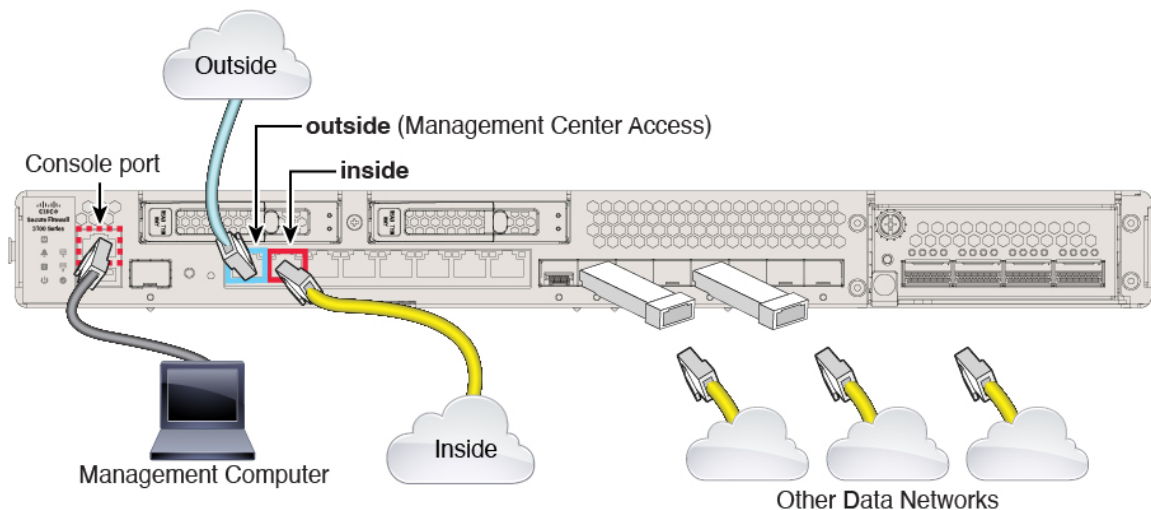
分支机构安装

收到来自中央总部的威胁防御后，您只需连接并打开防火墙电源，即可从外部接口访问互联网。然后，中央管理员即可完成配置。

连接防火墙的电缆

管理中心和您的管理计算机位于远程总部，可以通过互联网接通威胁防御。要在 Secure Firewall 3100 上进行布线，请参阅以下步骤。

图 19: 远程管理部署的布线



过程

步骤 1 安装机箱。请参阅[硬件安装指南](#)。

步骤 2 将外部接口（以太网 1/1）连接到外部路由器。

您可以将任何数据接口用于管理器访问，例如，如果您有内部管理中心，则使用内部接口。但是，本指南主要介绍外部接口访问，因为它是远程分支机构最可能遇到的场景。

步骤 3 将内部接口（例如，以太网 1/2）连接到内部交换机或路由器。

您可以为内部选择任何接口。

步骤 4 将其他网络连接其余接口。

步骤 5 （可选）将管理计算机连接到控制台端口。

在分支机构的日常工作中不需要使用控制台连接；但出于故障排除目的，可能需要此连接。

打开防火墙电源

系统电源由位于防火墙后部的摇杆电源开关控制。电源开关以软通知开关形式实施，支持平稳地关闭系统以降低系统软件及数据损坏的风险。



注释 首次启动威胁防御时，初始化大约需要 15 到 30 分钟。

开始之前

为防火墙提供可靠的电源（例如，使用不间断电源 (UPS)）非常重要。未事先关闭就断电可能会导致严重的文件系统损坏。后台始终有许多进程在运行，因此断电会使得系统无法正常关闭。

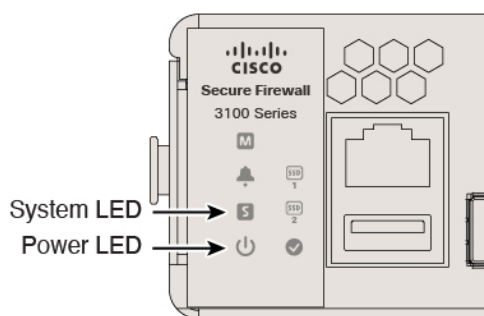
过程

步骤 1 将电源线一端连接到防火墙，另一端连接到电源插座。

步骤 2 使用位于机箱背面电源线旁边的标准摇杆型电源开关打开电源。

步骤 3 检查防火墙背面的电源 LED；如果该 LED 呈绿色稳定亮起，表示防火墙已接通电源。

图 20: 系统和电源 LED



步骤 4 检查防火墙背面的系统 LED；其呈绿色稳定亮起之后，系统已通过通电诊断。

注释 将开关从开切换到关时，系统可能需要几秒钟才会最终关闭。在此期间，机箱前面的电源 LED 将闪烁绿色。在电源 LED 完全关闭之前，请勿拔出电源。

中央管理员后配置

在远程分支机构管理员通过电缆连接威胁防御以便从外部接口访问互联网之后，您可以将威胁防御注册到管理中心并完成设备的配置。

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。您可以选择购买以下功能许可证：

- **基础版**-（必需）基础版 许可证。
- **IPS** - 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。

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

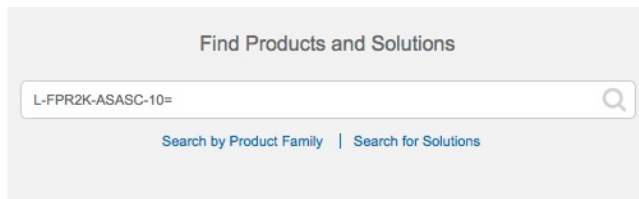
- 您的智能软件许可帐户必须符合强加密 (3DES/AES) 许可证的要求，才能使用某些功能（已使用导出合规性标志启用）。

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 21: 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。

- 基础版 许可证：
 - L-FPR3110-BSE=
 - L-FPR3120-BSE=
 - L-FPR3130-BSE=
 - L-FPR3140-BSE=

- IPS、恶意软件 防御和 URL 许可证组合：
 - L-FPR3110T-TMC =
 - L-FPR3120T-TMC =
 - L-FPR3130T-TMC =
 - L-FPR3140T-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-FPR3110T-TMC-1Y
- L-FPR3110T-TMC-3Y
- L-FPR3110T-TMC-5Y
- L-FPR3120T-TMC-1Y
- L-FPR3120T-TMC-3Y
- L-FPR3120T-TMC-5Y
- L-FPR3130T-TMC-1Y
- L-FPR3130T-TMC-3Y
- L-FPR3130T-TMC-5Y
- L-FPR3140T-TMC-1Y
- L-FPR3140T-TMC-3Y
- L-FPR3140T-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-FPR3K-FTD-CAR=

步骤 2 如果尚未注册，请向智能软件管理器注册管理中心。

注册需要您在智能软件管理器中生成注册令牌。有关详细指示，请参阅 [管理中心配置指南](#)。对低接触调配，您必须在向智能软件管理器注册时或在注册后启用低接触调配的云协助 (**Cloud Assistance for Low-Touch Provisioning**)。请参阅系统 (**System**) > 许可证 (**Licenses**) > 智能许可证 (**Smart Licenses**) 页面。

向管理中心注册威胁防御

使用设备 IP 地址或主机名将威胁防御手动注册到管理中心。

开始之前

- 收集您在威胁防御初始配置中设置的以下信息：
 - 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

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。

Add Device

Host:†
ftd-1.cisco.com

Display Name:
ftd-1.cisco.com

Registration Key:†
....

Group:
None

Access Control Policy:†
inside-outside

Smart Licensing

Malware
 Threat
 URL Filtering

Advanced

Unique NAT ID:†
natic56

Transfer Packets

Cancel Register

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 37 页。

图 22: 新建策略

- **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**)，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，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 management-data-interface** 命令。

- 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）。可以在威胁防御使用 **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。您在管理器访问设置中配置了外部接口的基本设置，但仍需要将其分配给安全区域。
- DHCP 服务器 - 在内部接口上为客户端使用 DHCP 服务器。
- 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。
- SSH - 在管理器访问接口上启用 SSH。

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。

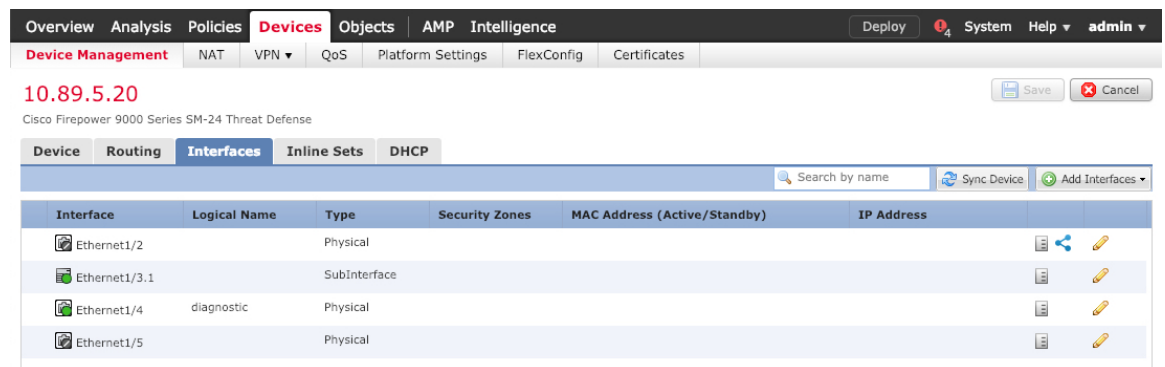
典型的边缘路由情况是通过 DHCP 从 ISP 获取外部接口地址，同时在内部接口上定义静态地址。

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 要从 40-Gb 接口（部分型号上可用）创建 4 x 10-Gb 分支接口，请点击接口的分支图标。

如果您已经在配置中使用了 40-Gb 接口，则必须在继续创建分支之前删除该配置。

步骤 4 点击要用于内部的接口的编辑 (✎)。

此时将显示一般 (**General**) 选项卡。

Edit Physical Interface ? X

General IPv4 IPv6 Advanced Hardware Configuration

Name: Enabled Management Only

Description:

Mode: ▼

Security Zone: ▼

Interface ID:

MTU: (64 - 9000)

OK Cancel

- 输入长度最大为 48 个字符的名称 (**Name**)。
例如，将接口命名为 **inside**。
- 选中启用 (**Enabled**) 复选框。
- 将模式 (**Mode**) 保留为无 (**None**)。
- 从安全区域 (**Security Zone**) 下拉列表选择一个现有的内部安全区域，或者点击新建 (**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。

- 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**

Edit Physical Interface

General **IPv4** IPv6 Advanced Hardware Configuration

IP Type: ▼

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

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

f) 点击**确定 (OK)**。

步骤 5 点击要用于外部的接口的 **编辑** (✎)。

此时将显示**一般 (General)** 选项卡。

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

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

您已经为该接口预配置了管理器访问，因此该接口就已经命名、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。您仍然必须在此屏幕上为直通流量策略配置安全区域。

- a) 从**安全区域 (Security Zone)** 下拉列表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。

b) 点击**确定 (OK)**。

步骤 6 点击**保存 (Save)**。

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 (Save)。

配置 NAT

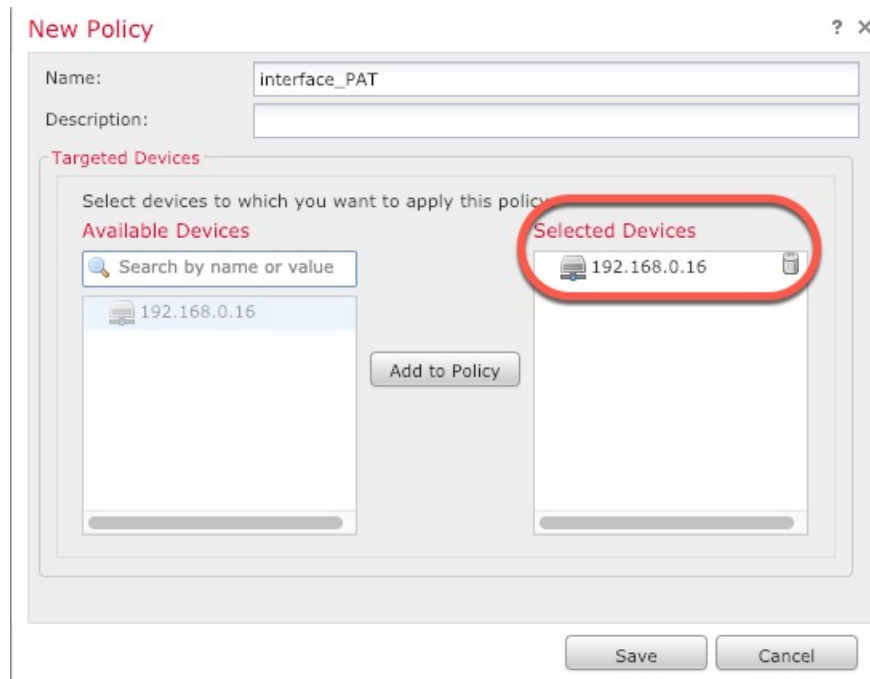
配置 NAT

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，然后点击新建策略 (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。

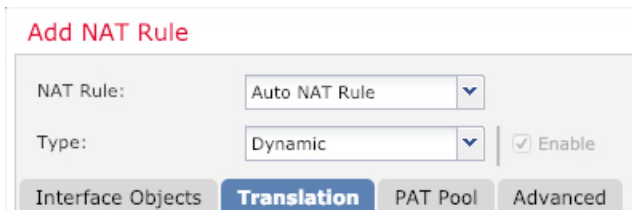


策略即已添加 管理中心。您仍然需要为策略添加规则。

步骤 3 点击添加规则 (**Add Rule**)。

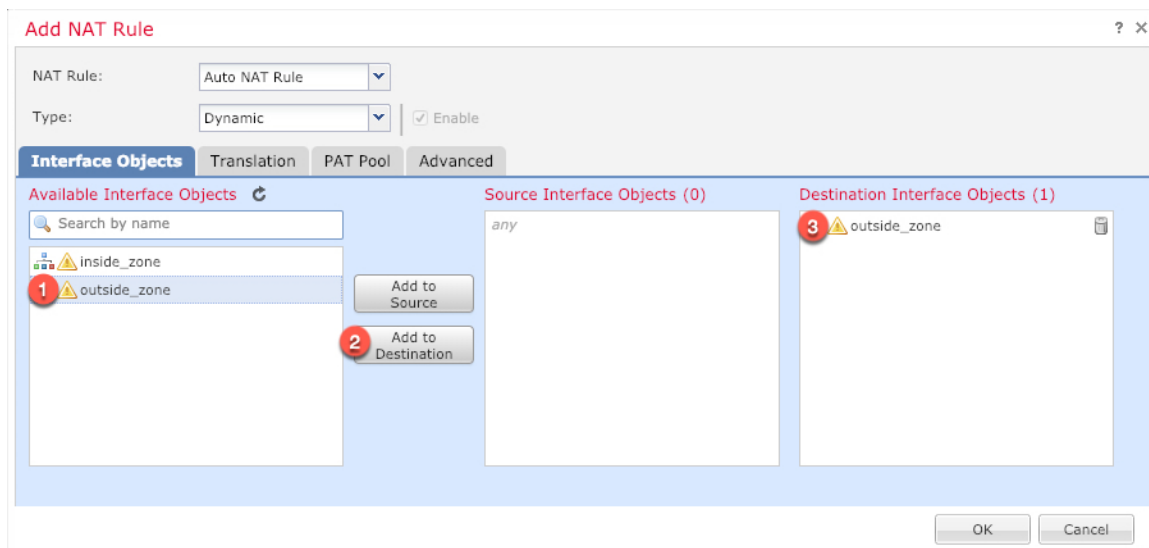
Add NAT Rule 对话框将显示。

步骤 4 配置基本规则选项：

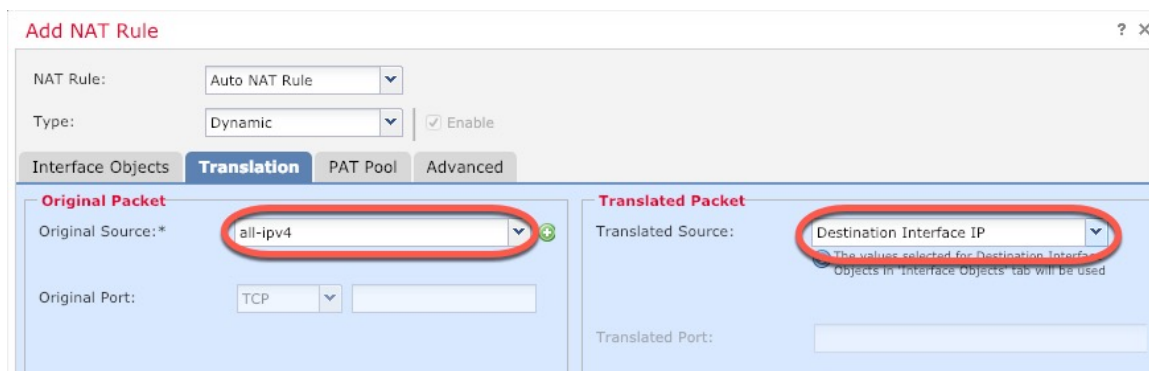


- **NAT 规则 (NAT Rule)** - 选择自动 NAT 规则 (**Auto NAT Rule**)。
- **类型 (Type)** - 选择动态 (**Dynamic**)。

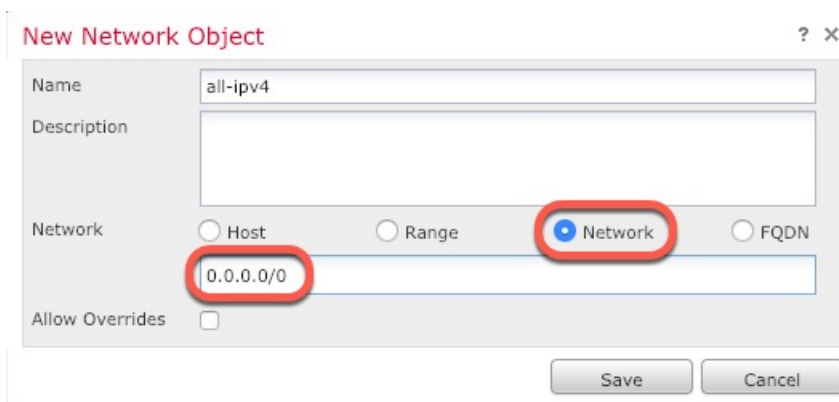
步骤 5 在 **Interface Objects** 页面，将 **Available Interface Objects** 区域中的外部区域添加到 **Destination Interface Objects** 区域。



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)。

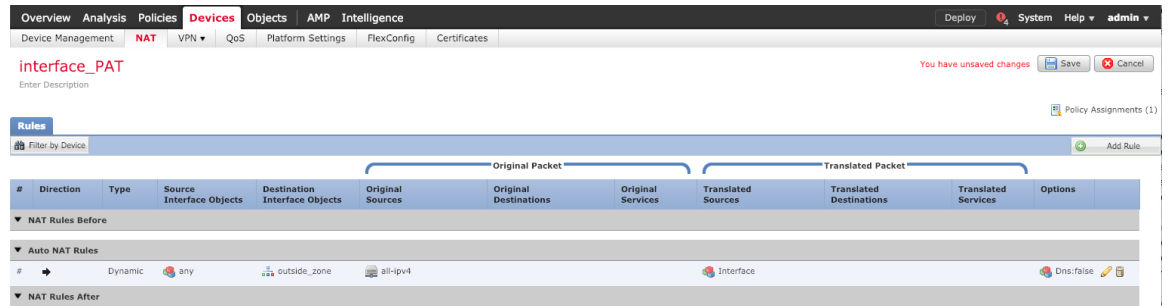


注释 您不能使用系统定义的 **any-ipv4** 对象，因为自动 NAT 规则在对象定义过程中添加 NAT，并且您无法编辑系统定义的对象。

- 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。

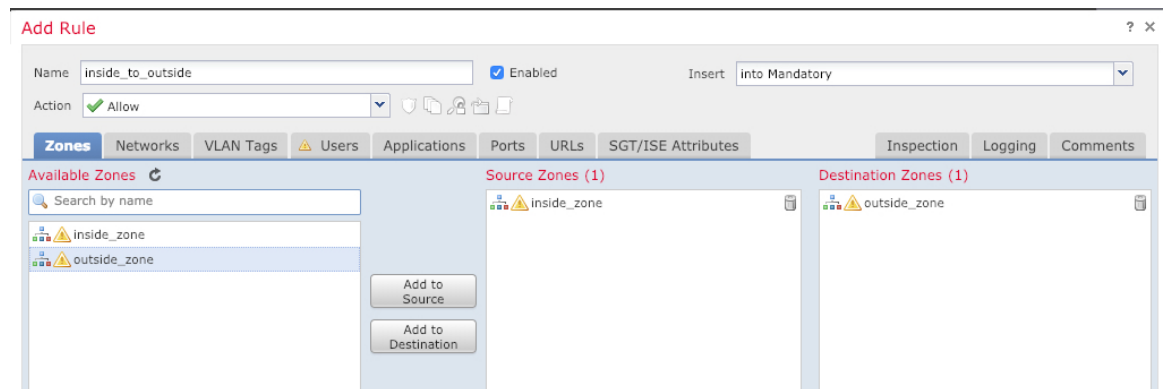
允许流量从内部传到外部

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：

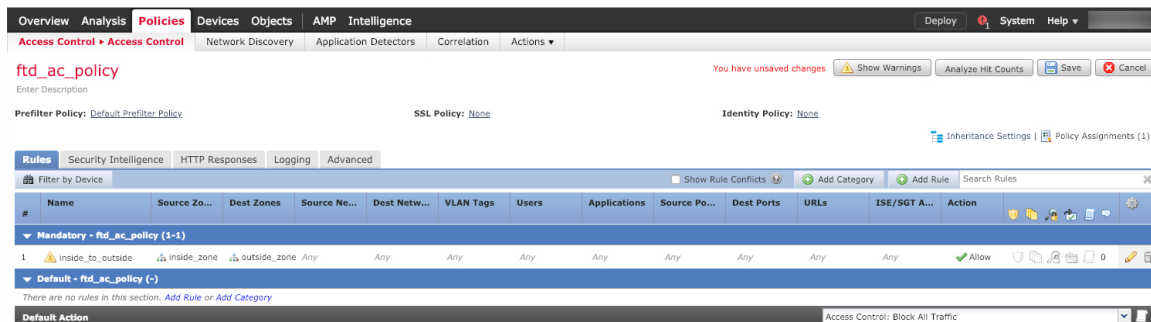


- 名称 (**Name**) - 为此规则命名，例如 **inside_to_outside**。
- 源区域 (**Source Zones**) - 从可用区域 (**Available Zones**) 中选择内部区域，然后点击添加到源 (**Add to Source**)。
- 目标区域 (**Destination Zones**) - 从可用区域 (**Available Zones**) 中选择外部区域，然后点击添加到目标 (**Add to Destination**)。

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 (Save)。

在管理器访问数据接口上配置 SSH

如果在数据接口（例如外部）上启用了管理中心访问，则应使用此程序在该接口上启用 SSH。本节介绍如何启用威胁防御上一个或多个数据接口的 SSH 连接。诊断逻辑接口上不支持 SSH。



注释 管理接口上默认已启用 SSH，但此屏幕不会影响管理 SSH 访问。

管理接口与设备上的其他接口分离。它用于设置设备并将其注册到管理中心。数据接口的 SSH 与管理接口的 SSH 共用内部和外部用户列表。其他设置单独进行配置：对于数据接口，使用此屏幕启用 SSH 和访问列表；数据接口的 SSH 流量使用常规路由配置，并不是所有静态路由均在设置时或 CLI 中配置。

对于管理接口，要配置 SSH 访问列表，请参阅 [Cisco Secure Firewall Threat Defense 命令参考](#) 中的 **configure ssh-access-list** 命令。要配置静态路由，请参阅 **configure network static-routes** 命令。默认情况下，在初始设置时通过管理接口配置默认路由。

要使用 SSH，您也不需要允许主机 IP 地址的访问规则。您只需按照本部分配置 SSH。

您只能 SSH 到可访问接口；如果 SSH 主机位于外部接口上，则只能直接向外部接口发起管理连接。



注释 在您连续三次尝试使用 SSH 登录 CLI 失败后，设备会终止 SSH 连接。

开始之前

- 可以使用 **configure user add** 命令。默认情况下，有一个您在初始设置期间为其配置密码的 **admin** 用户。还可以通过在平台设置中配置外部身份验证，在 LDAP 或 RADIUS 上配置外部用户。

- 您需要定义允许与设备建立 SSH 连接的主机或网络对象。您可以在此过程中添加对象，但如果要使用对象组标识一组 IP 地址，请确保规则中所需的组已经存在。选择 **对象 > 对象管理** 以配置对象。



注释 不能使用系统提供的 **any** 网络对象。而是使用 **any-ipv4** 或 **any-ipv6**。

过程

步骤 1 选择 **设备 > 平台设置**，并创建或编辑 **威胁防御** 策略。

步骤 2 选择 **安全外壳 (Secure Shell)**。

步骤 3 标识允许 SSH 连接的接口和 IP 地址。

使用此表可以限制哪些接口将接受 SSH 连接，以及允许建立这些连接的客户端的 IP 地址。您可以使用网络地址而不是单个 IP 地址。

a) 点击 **添加 (Add)** 以添加新规则，或点击 **编辑 (Edit)** 以编辑现有规则。

b) 配置规则属性：

- **IP 地址**-用于标识允许建立 HTTPS 连接的主机或网络的 **网络对象** 或 **组**。从下拉列表中选择 **一个对象**，或者点击 **+** 以添加新的网络对象。
- **安全区域 (Security Zones)** - 添加包含将允许进行 SSH 连接的接口的 **区域**。对于不在区域中的接口，可以在 **所选安全区域 (Selected Security Zones)** 列表下方的 **字段** 中键入接口名称，然后点击 **添加 (Add)**。仅当设备包含所选接口或区域时，才会将这些规则应用于该设备。

c) 点击 **确定 (OK)**。

步骤 4 点击 **保存 (Save)**。

此时，您可以转至 **部署 > 部署** 并将策略部署到所分配的设备。在部署更改之后，更改才生效。

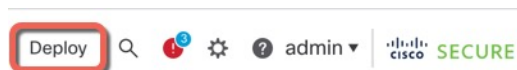
部署配置

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 23: 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 24: 全部部署

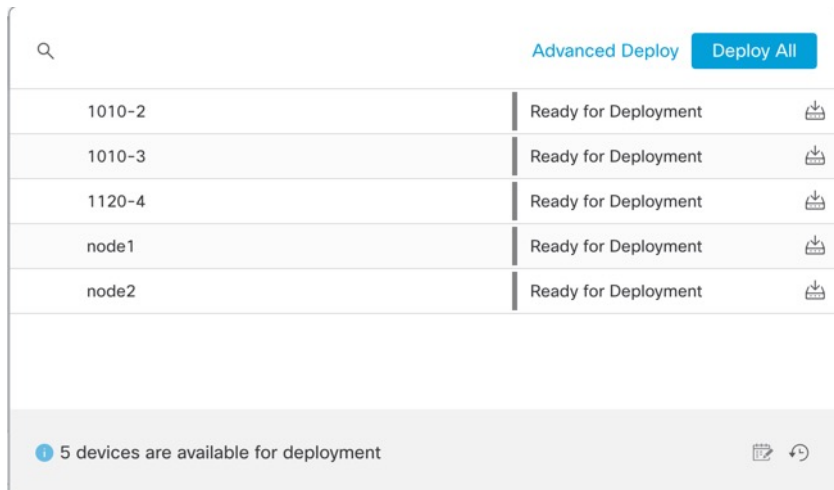
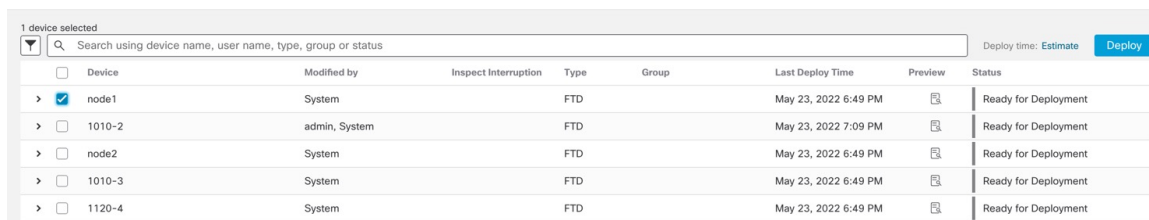
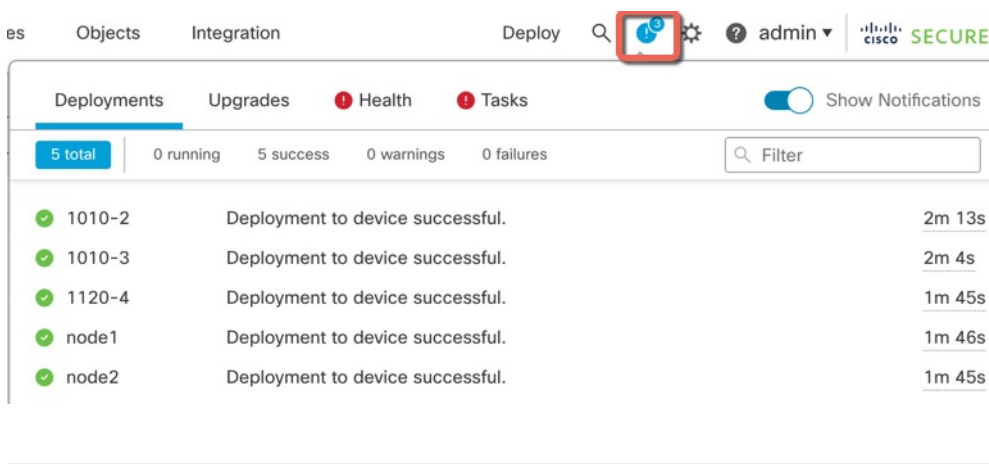


图 25: 高级部署



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 26: 部署状态



访问威胁防御和FXOS CLI

使用命令行界面 (CLI) 可设置系统以及对系统进行基本的故障排除。无法通过 CLI 会话配置策略。可以连接到控制台端口以访问 CLI。

也可以访问FXOS CLI以进行故障排除。



注释 您也可以通过 SSH 连接到 威胁防御 设备的管理接口。与控制台会话不同，SSH 会话默认使用 威胁防御 CLI，由此可使用 **connect fxos** 命令连接到 FXOS CLI。如果您为 SSH 连接打开某个数据接口，稍后可以连接到该接口上的地址。默认情况下，禁用 SSH 数据接口访问。此程序介绍控制台端口的访问（默认使用 FXOS CLI）。

过程

步骤 1 要登录 CLI，请将管理计算机连接到控制台端口。Secure Firewall 3100 配有一条 DB-9 转 RJ-45 串行电缆，所以您需要第三方串行转 USB 电缆进行连接。确保为您的操作系统安装必要的 USB 串行驱动程序（请参阅 Secure Firewall 3100 [硬件指南](#)）。控制台端口默认为 FXOS CLI。使用以下串行设置：

- 9600 波特率
- 8 个数据位
- 无奇偶校验
- 1 个停止位

您连接到 FXOS CLI。使用 **admin** 用户名和初始设置时设置的密码（默认值为 **Admin123**）登录 CLI。

示例：

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

步骤 2 访问威胁防御 CLI。

connect ftd

示例：

```
firepower# connect ftd
>
```

登录后，如需了解 CLI 中可用命令的相关信息，请输入 **help** 或 **?**。有关使用信息，请参阅 [Cisco Secure Firewall Threat Defense 命令参考](#)。

步骤 3 要退出 威胁防御FTD CLI，请输入 **exit** 或 **logout** 命令。

此命令会将您重新导向至 FXOS CLI 提示。有关 FXOS CLI 中可用命令的相关信息，请输入 **?**。

示例：

```
> exit
firepower#
```

排除数据接口上的管理连接故障

当使用数据接口进行管理器访问而不是使用专用管理接口时，必须注意在 管理中心 中更改 威胁防御 的接口和网络设置，以免中断连接。如果在将 威胁防御 添加到 管理中心 后更改管理接口类型（从数据到管理，或从管理到数据），如果接口和网络设置未正确配置，则可能会丢失管理连接。

本主题可帮助您排除管理连接丢失的问题。

查看管理连接状态

在 管理中心 中，在 **设备 (Devices) > 设备管理 (Device Management) > 设备 (Device) > 管理 (Management) > 管理器访问 - 配置详细信息 (Manager Access - Configuration Details) > 连接状态 (Connection Status)** 页面上检查管理连接状态。

在 威胁防御 CLI，输入 **sftunnel-status-brief** 命令以查看管理连接状态。您还可以使用 **sftunnel-status** 查看更完整的信息。

请参阅以下有关关闭连接的输出示例；没有显示“连接至“信息，也没有显示心跳信息：

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

请参阅以下关于已建立连接的输出示例，其中显示了对等信道和心跳信息：

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

查看 威胁防御 网络信息

在 威胁防御 CLI 上，查看管理和管理器访问数据接口网络设置：

show network

```

> show network
===== [ System Information ] =====
Hostname                : 5516X-4
DNS Servers             : 208.67.220.220,208.67.222.222
Management port        : 8305
IPv4 Default route
  Gateway               : data-interfaces
IPv6 Default route
  Gateway               : data-interfaces

===== [ br1 ] =====
State                   : Enabled
Link                    : Up
Channels                : Management & Events
Mode                    : Non-Autonegotiation
MDI/MDIX                : Auto/MDIX
MTU                     : 1500
MAC Address             : 28:6F:7F:D3:CB:8D
----- [ IPv4 ] -----
Configuration          : Manual
Address                : 10.99.10.4
Netmask                 : 255.255.255.0
Gateway                 : 10.99.10.1
----- [ IPv6 ] -----
Configuration          : Disabled

===== [ Proxy Information ] =====
State                   : Disabled
Authentication          : Disabled

===== [ System Information - Data Interfaces ] =====
DNS Servers             :
Interfaces              : GigabitEthernet1/1

===== [ GigabitEthernet1/1 ] =====
State                   : Enabled
Link                    : Up
Name                    : outside
MTU                     : 1500
MAC Address             : 28:6F:7F:D3:CB:8F
----- [ IPv4 ] -----
Configuration          : Manual
Address                : 10.89.5.29
Netmask                 : 255.255.255.192
Gateway                 : 10.89.5.1
----- [ IPv6 ] -----
Configuration          : Disabled

```

检查向 管理中心注册 威胁防御

在 威胁防御 CLI 中，检查 管理中心 注册是否已完成。请注意，此命令不会显示管理连接的当前状态。

show managers

```

> show managers
Type                   : Manager
Host                   : 10.10.1.4
Display name           : 10.10.1.4

```

```

Identifier           : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration         : Completed
Management type     : Configuration

```

Ping 管理中心

在威胁防御 CLI 上，使用以下命令从数据接口对管理中心执行 ping 操作：

ping fmc_ip

在威胁防御 CLI 上，使用以下命令从管理接口对管理中心执行 ping 操作，该接口应通过背板路由到数据接口：

ping system fmc_ip

捕获威胁防御内部接口上的数据包

在威胁防御 CLI 上，捕获内部背板接口 (nlp_int_tap) 上的数据包，以查看是否发送了管理数据包：

capture 名称 interface nlp_int_tap trace detail match ip any any

show capture name trace detail

检查内部接口状态，统计信息和数据包计数

在威胁防御 CLI 上，查看有关内部背板接口 nlp_int_tap 的信息：

show interace detail

```

> show interface detail
[...]
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_ymtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
  (Full-duplex), (1000 Mbps)
  Input flow control is unsupported, output flow control is unsupported
  MAC address 0000.0100.0001, MTU 1500
  IP address 169.254.1.1, subnet mask 255.255.255.248
  37 packets input, 2822 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 pause input, 0 resume input
  0 L2 decode drops
  5 packets output, 370 bytes, 0 underruns
  0 pause output, 0 resume output
  0 output errors, 0 collisions, 0 interface resets
  0 late collisions, 0 deferred
  0 input reset drops, 0 output reset drops
  input queue (blocks free curr/low): hardware (0/0)
  output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
  37 packets input, 2304 bytes
  5 packets output, 300 bytes
  37 packets dropped
    1 minute input rate 0 pkts/sec,  0 bytes/sec
    1 minute output rate 0 pkts/sec,  0 bytes/sec
    1 minute drop rate, 0 pkts/sec
    5 minute input rate 0 pkts/sec,  0 bytes/sec
    5 minute output rate 0 pkts/sec,  0 bytes/sec
    5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
  Interface number is 14

```

```
Interface config status is active
Interface state is active
```

检查路由和 NAT

在威胁防御 CLI 中，检查是否已添加默认路由 (S*)，以及管理接口 (nlp_int_tap) 是否存在内部 NAT 规则。

show route

```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF

Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*      0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C       10.89.5.0 255.255.255.192 is directly connected, outside
L       10.89.5.29 255.255.255.255 is directly connected, outside

>
```

show nat

```
> show nat

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface service
  tcp 8305 8305
  translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface service
  tcp ssh
  translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
  ipv6 service tcp 8305 8305
  translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
  translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
  translate_hits = 0, untranslate_hits = 0

>
```

检查其他设置

请参阅以下命令以检查是否存在所有其他设置。您还可以在管理中心的 **设备 (Devices) > 设备管理 (Device Management) > 设备 (Device) > 管理 (Management) > 管理器访问 - 配置详细信息 (Manager Access - Configuration Details) > CLI 输出 (CLI Output)** 页面上看到许多这些命令。

show running-config sftunnel

```
> show running-config sftunnel
```

```
sftunnel interface outside
sftunnel port 8305
```

show running-config ip-client

```
> show running-config ip-client
ip-client outside
```

show conn address *fmc_ip*

```
> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
    preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap 10.89.5.29(169.254.1.2):51231 outside 10.89.5.35:8305, idle 0:00:04,
bytes 86684, flags UxIO
TCP nlp_int_tap 10.89.5.29(169.254.1.2):8305 outside 10.89.5.35:52019, idle 0:00:02,
bytes 1630834, flags UIO
>
```

检查 DDNS 更新是否成功

在威胁防御 CLI 中，检查 DDNS 更新是否成功：

debug ddns

```
> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfully updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
DDNS: IDB SB total = 0
```

如果更新失败，请使用 **debug http** 和 **debug ssl** 命令。对于证书验证失败，请检查是否已在设备上安装根证书：

show crypto ca certificates *trustpoint_name*

要检查 DDNS 操作，请执行以下操作：

show ddns update interface *fmc_访问_ifc_name*

```
> show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name Update Destination
  RBD_DDNS not available

Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

检查 管理中心 日志文件

请参阅 <https://cisco.com/go/fmc-reg-error>。

如果管理中心断开连接，则回滚配置

如果将威胁防御上的数据接口用于管理器访问，并从管理中心部署影响网络连接的配置更改，则可以将威胁防御上的配置回滚到上次部署的配置，以便恢复管理连接。然后，您可以调整管理中心中的配置设置，以便保持网络连接并重新部署。即使没有丢失连接，也可以使用回滚功能；它不仅限于此故障排除情况。

请参阅以下准则：

- 只有以前的部署可以在威胁防御上本地提供；您无法回滚到任何较早的部署。
- 支持回滚以实现高可用性，但不支持集群部署。
- 回滚只会影响您可以在管理中心中设置的配置。例如，回滚不会影响与专用管理接口相关的任何本地配置，您只能在威胁防御 CLI 中进行配置。请注意，如果您在上次管理中心部署后使用 **configure network management-data-interface** 命令更改了数据接口设置，然后使用了回滚命令，则这些设置将不会保留；它们将回滚到上次部署的管理中心设置。
- UCAPL/CC 模式无法回滚。
- 无法回滚上一次部署期间更新的带外 SCEP 证书数据。
- 在回滚期间，连接将被丢弃，因为当前配置将被清除。

过程

步骤 1 在威胁防御 CLI 中，回滚到之前的配置。

configure policy rollback

回滚后，威胁防御会通知管理中心已成功完成回滚。在管理中心中，部署屏幕将显示一条横幅，说明配置已回滚。

注释 如果回滚失败且管理中心管理已恢复，请参阅<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html>以了解常见的部署问题。在某些情况下，恢复管理中心管理访问权限后回滚可能会失败；在这种情况下，您可以解决管理中心配置问题，并从管理中心重新部署。

示例：

对于使用数据接口进行管理器访问的威胁防御：

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2020 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
```

```
Following is the rollback summary:
.....
.....
>
```

步骤 2 检查管理连接是否已重新建立。

在管理中心中，在 **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **管理 (Management)** > **管理器访问 - 配置详细信息 (Manager Access - Configuration Details)** > **连接状态 (Connection Status)** 页面上检查管理连接状态。

在威胁防御 CLI，输入 **sftunnel-status-brief** 命令以查看管理连接状态。

如果重新建立连接需要 10 分钟以上，则应排除连接故障。请参阅[排除数据接口上的管理连接故障，第 78 页](#)。

使用管理中心关闭防火墙电源

正确关闭系统非常重要。仅拔掉电源或按下电源开关可能会导致文件系统严重损坏。请记住，有许多进程一直在后台运行，拔掉或关闭电源不能正常关闭防火墙。

您可以使用管理中心正确关闭系统。

过程

步骤 1 选择设备 > 设备管理。

步骤 2 在要重新启动的设备旁边，点击编辑图标 (✎)。

步骤 3 点击设备 (Device) 选项卡。

步骤 4 点击系统 (System) 部分中的关闭设备图标 (🔴)。

步骤 5 出现提示时，确认是否要关闭设备。

步骤 6 如果您与防火墙建立了控制台连接，请在防火墙关闭时留意系统提示。您将看到以下提示：

```
System is stopped.
It is safe to power off now.

Do you want to reboot instead? [y/N]
```

如果没有控制台连接，请等待大约 3 分钟以确保系统已关闭。

步骤 7 您现在可以关闭电源开关并在必要时拔下电源插头以物理方式断开机箱的电源。

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》](#)。



第 4 章

使用设备管理器部署威胁防御

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[哪种操作系统和管理器适合您？](#)，第 1 页。本章适用于威胁防御和设备管理器。

本章介绍如何使用基于 Web 的设备安装向导，完成威胁防御的初始设置和配置。

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。

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。

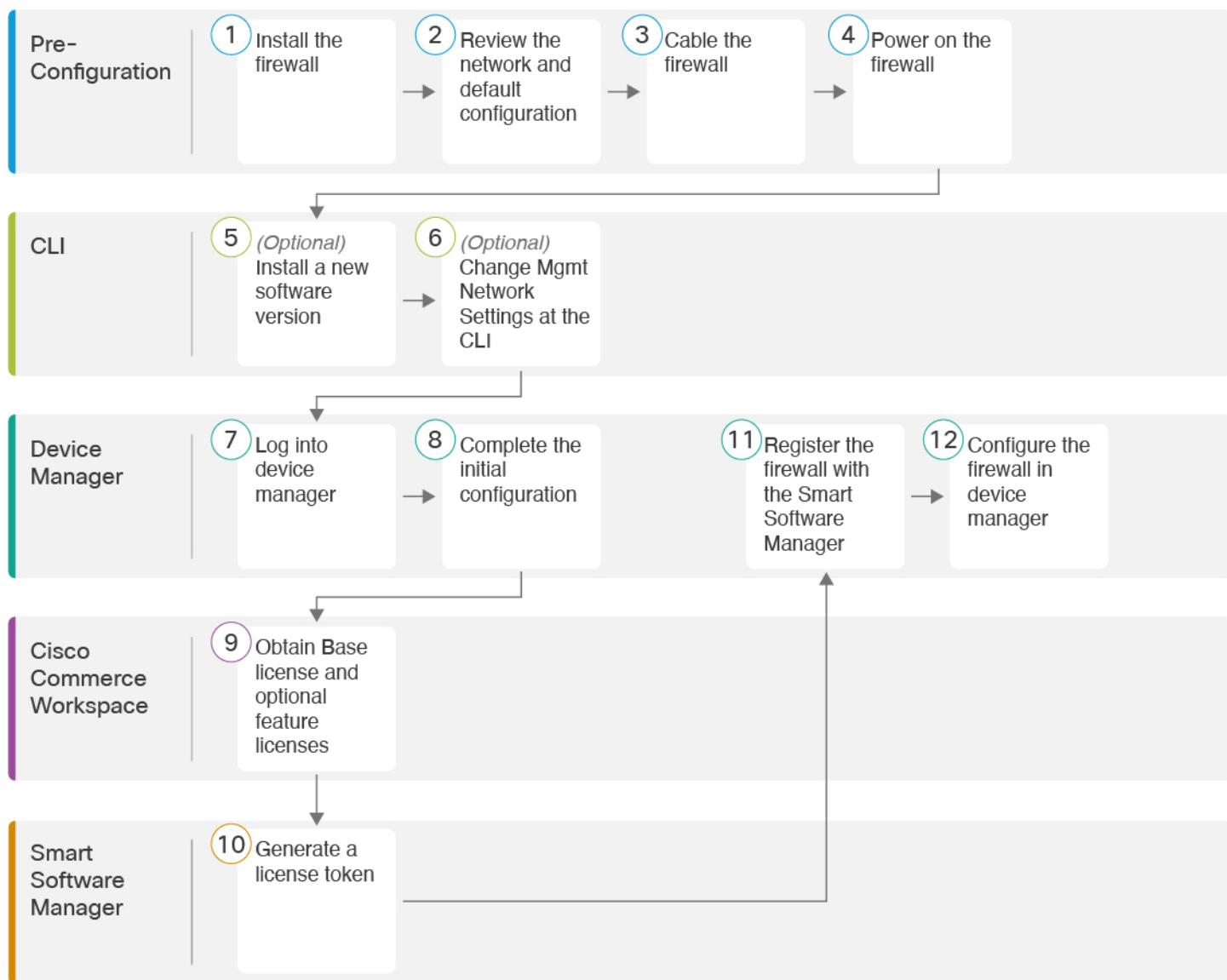
- [端到端程序](#)，第 88 页
- [查看网络部署和默认配置](#)，第 89 页
- [连接防火墙的电缆](#)，第 91 页
- [打开防火墙电源](#)，第 92 页
- [（可选）检查软件并安装新版本](#)，第 93 页
- [（可选）在 CLI 中更改管理网络设置](#)，第 94 页
- [登录设备管理器](#)，第 96 页
- [完成初始配置](#)，第 97 页
- [配置许可](#)，第 98 页
- [在设备管理器中配置防火墙](#)，第 105 页
- [访问威胁防御和 FXOS CLI](#)，第 108 页
- [关闭防火墙电源](#)，第 110 页

• 后续步骤，第 111 页

端到端程序

请参阅以下任务以在机箱上部署威胁防御和设备管理器。

图 27: 端到端程序



1	配置前准备工作	安装防火墙。请参阅 硬件安装指南 。
2	配置前准备工作	查看 网络部署和默认配置 ，第 89 页。

3	配置前准备工作	连接防火墙的电缆，第 91 页。
4	配置前准备工作	打开防火墙电源，第 92 页。
5	CLI	(可选) 检查软件并安装新版本，第 93 页。
6	CLI	(可选) 在 CLI 中更改管理网络设置，第 94 页。
7	设备管理器	登录设备管理器，第 96 页。
8	设备管理器	完成初始配置，第 97 页。
9	Cisco Commerce Workspace	获取基本许可证和可选功能许可证 (配置许可，第 98 页)。
10	智能软件管理器	生成许可证令牌 (配置许可，第 98 页)。
11	设备管理器	向智能许可证服务器 (配置许可，第 98 页) 注册防火墙。
12	设备管理器	在设备管理器中配置防火墙，第 105 页。

查看网络部署和默认配置

您可以从管理 1/1 接口或内部接口使用设备管理器管理威胁防御。专用管理接口是一种具有自己的网络设置的特殊接口。

下图显示了推荐用于网络部署。如果您将外部接口直接连接到电缆调制解调器或 DSL 调制解调器，我们建议您将调制解调器置于桥接模式，以便威胁防御为您的内部网络执行所有路由和 NAT。如果您需要为外部接口配置 PPPoE 以连接到您的 ISP，可以在设备管理器中完成初始设置后执行此操作。



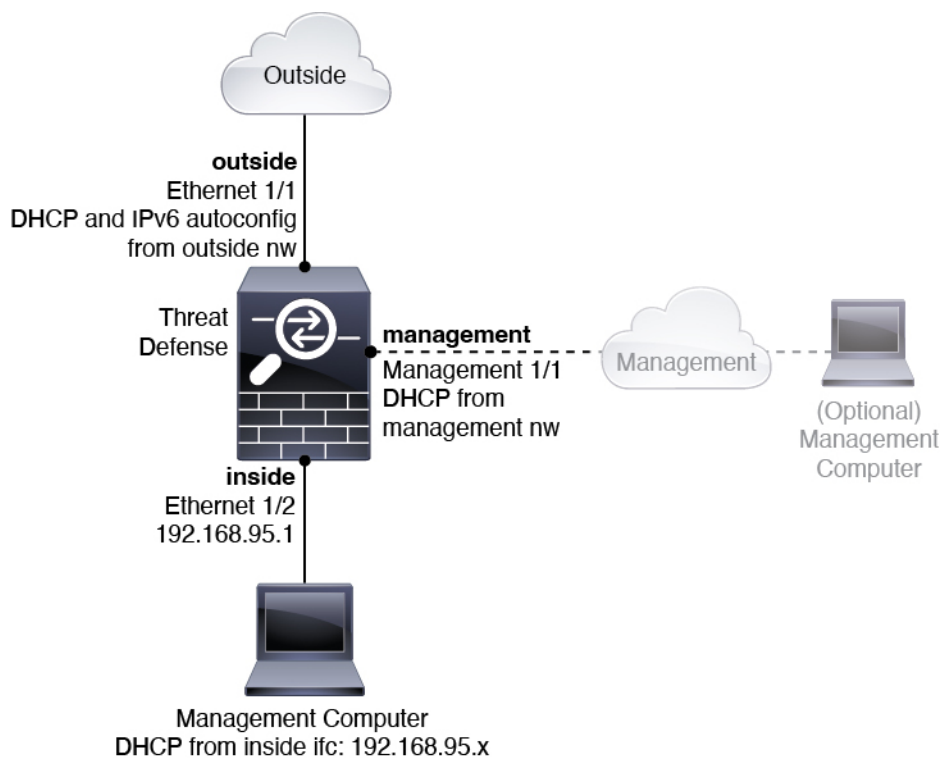
注释 如果您无法使用默认管理 IP 地址（例如，您的管理网络不包括 DHCP 服务器），可以连接到控制台端口并在 CLI 中执行初始设置，包括设置管理 IP 地址、网关和其他基本网络设置。

如果您需要更改内部 IP 地址，可以在设备管理器中完成初始设置后执行此操作。例如，在以下情况下，您可能需要更改内部 IP 地址：

- 内部 IP 地址为 192.168.95.1。
- 如果将威胁防御添加到现有内部网络中，需要将内部 IP 地址更改到现有网络上。

下图显示了在使用默认配置的设备管理器的威胁防御默认网络部署。

图 28: 建议的网络部署



默认配置

在初始设置后，防火墙配置包括以下内容：

- 内部 - 以太网 1/2、IP 地址 192.168.95.1。
- 外部 - 以太网 1/1，IP 地址来自 IPv4 DHCP 和 IPv6 自动配置
- 内部→外部流量
- 管理 - 管理 1/1（管理），IP 地址来自 DHCP



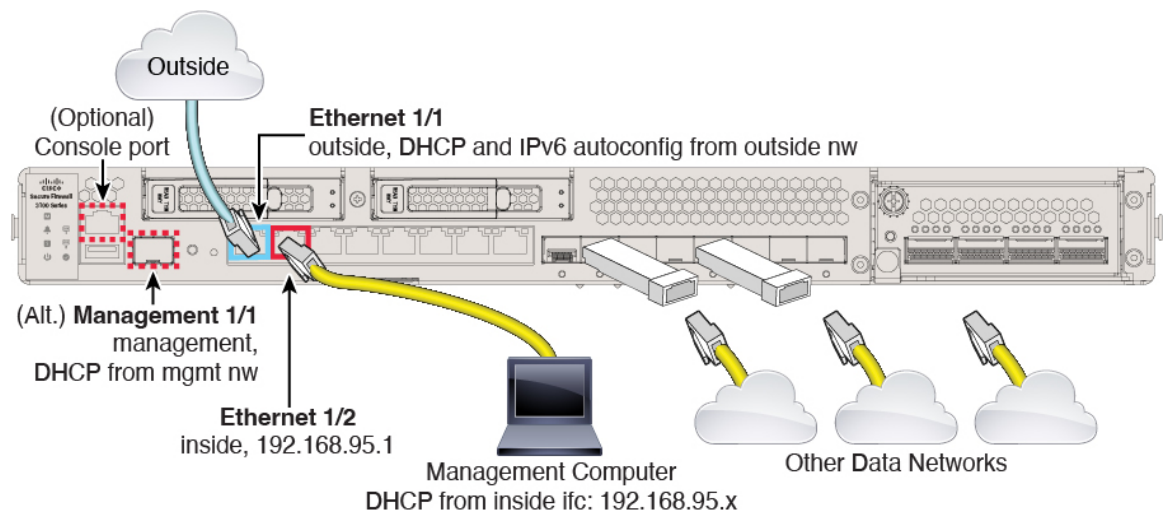
注释 管理 1/1 接口是不同于数据接口的特殊接口，用于管理、智能许可和数据库更新。物理接口与第二个逻辑接口（诊断接口）共享。诊断是一种数据接口，但仅限于其他类型的管理流量（发往设备和发自设备），例如 syslog 或 SNMP。通常不使用诊断接口。有关详细信息，请参阅《[Cisco Secure Firewall 设备管理器配置指南](#)》。

- 管理型 DNS 服务器 - OpenDNS: (IPv4) 208.67.222.222、208.67.220.220; (IPv6) 2620:119:35::35 或在设置过程中指定的服务器。系统从不使用从 DHCP 获取的 DNS 服务器。

- **NTP** - 思科 NTP 服务器: 0.sourcefire.pool.ntp.org、1.sourcefire.pool.ntp.org、2.sourcefire.pool.ntp.org 或您在设置过程中指定的服务器
- **默认路由**
 - **数据接口** - 从外部 DHCP 获取, 或在设置过程中指定的网关 IP 地址
 - **管理接口** - 从管理 DHCP 获取。如果没有收到网关, 则默认路由在背板上并通过数据接口。
请注意, 管理接口需要互联网访问, 以在背板上或使用单独的互联网网关获取许可和进行更新。请注意, 只有源自管理接口的流量才能通过背板; 否则, 管理接口不允许从网络进入管理接口的直通流量。
- **DHCP 服务器** - 在内部接口上启用
- **设备管理器 访问** - 管理和内部接口上允许的所有主机。
- **NAT** - 接口 PAT 用于所有从内部到外部的流量

连接防火墙的电缆

图 29: *Secure Firewall 3100* 布线



在管理 1/1 或以太网 1/2 上管理 Secure Firewall 3100。默认配置还会将以太网 1/1 配置为外部接口。

过程

步骤 1 安装机箱。请参阅[硬件安装指南](#)。

步骤 2 将您的管理计算机连接至以下任一接口:

- **以太网 1/2** - 将您的管理计算机直接连接至以太网 1/2 以进行初始配置, 或将以太网 1/2 连接至内部网络。以太网 1/2 具有默认 IP 地址 (192.168.95.1), 并且还会运行 DHCP 服务器以向客户端

(包括管理计算机) 提供 IP 地址, 因此, 请确保这些设置不会与任何现有内部网络设置冲突 (请参阅[默认配置](#), 第 90 页)。

- 管理 1/1 - 将管理 1/1 接口连接到管理网络, 并确保管理计算机位于管理网络上, 或者可以访问管理网络。管理 1/1 接口从管理网络上的 DHCP 服务器获取 IP 地址; 如果使用此接口, 则必须确定分配给防火墙的 IP 地址, 以便可以从管理计算机连接到 IP 地址。

如果需要将管理 1/1 IP 地址从默认值更改为配置静态 IP 地址, 还必须将管理计算机连接到控制台端口。请参阅 [\(可选\) 在 CLI 中更改管理网络设置](#), 第 94 页。

注释 管理 1/1 是需要 SFP 模块的 10 Gb 光纤接口。

可以稍后从其他接口配置设备管理器管理访问; 请参阅[FDM 配置指南](#)。

步骤 3 将外部网络连接到以太网 1/1 接口。

默认情况下, 使用 IPv4 DHCP 和 IPv6 自动配置获取 IP 地址, 但可以在初始配置期间设置静态地址。

步骤 4 将其他网络连接到其余接口。

打开防火墙电源

系统电源由位于防火墙后部的摇杆电源开关控制。电源开关以软通知开关形式实施, 支持平稳地关闭系统以降低系统软件及数据损坏的风险。



注释 首次启动威胁防御时, 初始化大约需要 15 到 30 分钟。

开始之前

为防火墙提供可靠的电源 (例如, 使用不间断电源 (UPS)) 非常重要。未事先关闭就断电可能会导致严重的文件系统损坏。后台始终有许多进程在运行, 因此断电会使得系统无法正常关闭。

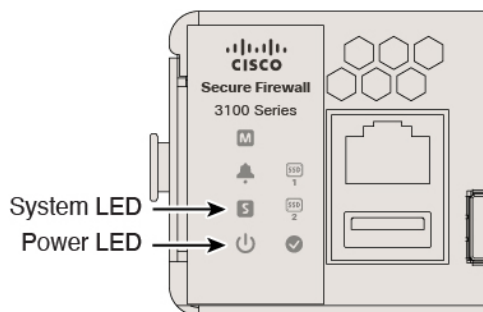
过程

步骤 1 将电源线一端连接到防火墙, 另一端连接到电源插座。

步骤 2 使用位于机箱背面电源线旁边的标准摇杆型电源开关打开电源。

步骤 3 检查防火墙背面的电源 LED; 如果该 LED 呈绿色稳定亮起, 表示防火墙已接通电源。

图 30: 系统和电源 LED



步骤 4 检查防火墙背面的系统 LED；其呈绿色稳定亮起之后，系统已通过通电诊断。

注释 将开关从开切换到关时，系统可能需要几秒钟才会最终关闭。在此期间，机箱前面的电源 LED 将闪烁绿色。在电源 LED 完全关闭之前，请勿拔出电源。

(可选) 检查软件并安装新版本

要检查软件版本并在必要时安装不同的版本，请执行以下步骤。我们建议您在配置防火墙之前安装目标版本。或者，您也可以在启动并运行后执行升级，但升级（保留配置）可能需要比按照此程序花费更长的时间。

我应该运行什么版本？

思科建议运行软件下载页面上的版本号旁边标有金色星号的 Gold Star 版本。您还可以参考 <https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html> 中所述的发布策略；例如，此公告描述短期版本编号（包含最新功能）、长期版本编号（较长时间的维护版本和补丁）或额外长期版本编号（最长期限的维护版本和补丁，用于政府认证）。

过程

步骤 1 连接到控制台端口。有关详细信息，请参阅[访问威胁防御和 FXOS CLI](#)，第 108 页。

使用用户名 **admin** 和默认密码 **Admin123** 登录。

您连接到 FXOS CLI。第一次输入登录时，系统会提示您更改密码。此密码也用于 SSH 的威胁防御登录。

注释 如果密码已更改，但您不知道，则必须执行出厂重置以将密码重置为默认值。有关 [出厂重置程序](#) 的信息，请参阅 [FXOS 故障排除指南](#)。

示例:

```
firepower login: admin
```

```

Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: *****
Confirm new password: *****
Your password was updated successfully.

[...]

firepower#

```

步骤 2 在 FXOS CLI 中，显示正在运行的版本。

scope ssa

show app-instance

示例:

```

Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name      Slot ID      Admin State      Operational State      Running Version Startup
Version Cluster Oper State
-----
ftd                   1            Enabled          Online                  7.2.0.65              7.2.0.65
                        Not Applicable

```

步骤 3 如果要安装新版本，请执行这些步骤。

- a) 如果要为管理接口设置静态 IP 地址，请参阅 [\(可选\) 在 CLI 中更改管理网络设置，第 94 页](#)。
默认情况下，管理接口将使用 DHCP。
您需要从可通过管理接口访问的服务器下载新的映像。
- b) 执行 [《FXOS 故障排除指南》](#) 中的 [重新映像程序](#)。

(可选) 在 CLI 中更改管理网络设置

如果您无法使用默认管理 IP 地址，可以连接到控制台端口并在 CLI 中执行初始设置，包括设置管理 IP 地址、网关和其他基本网络设置。您只能配置管理接口设置；而无法配置内部或外部接口，稍后可在 GUI 中配置它们。



注释 除非清除配置，否则无法重复 CLI 设置脚本（例如，通过重新建立映像）。但是，可以稍后在 CLI 中使用 **configure network** 命令更改所有这些设置。请参阅 [Cisco Secure Firewall Threat Defense 命令参考](#)。

过程

步骤 1 连接到威胁防御控制台端口。有关详细信息，请参阅[访问威胁防御和 FXOS CLI](#)，第 108 页。

使用用户名 **admin** 和默认密码 **Admin123** 登录。

您连接到 FXOS CLI。第一次输入登录时，系统会提示您更改密码。此密码也用于 SSH 的威胁防御登录。

注释 如果密码已更改，但您不知道，则必须执行出厂重置以将密码重置为默认值。有关 [出厂重置程序](#) 的信息，请参阅 [FXOS 故障排除指南](#)。

示例:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: *****
Confirm new password: *****
Your password was updated successfully.

[...]

firepower#
```

步骤 2 连接到威胁防御 CLI。

connect ftd

示例:

```
firepower# connect ftd
>
```

步骤 3 首次登录威胁防御时，系统会提示您接受“最终用户许可协议”(EULA)并。然后，系统将显示 CLI 设置脚本。

默认值或以前输入的值会显示在括号中。要接受之前输入的值，请按 **Enter** 键。

请参阅以下准则:

- **输入管理接口的 IPv4 默认网关** - 如果您设置手动 IP 地址，则可以输入网关路由器的数据接口或 IP 地址。**data-interfaces** 设置将通过背板发送出站管理流量，以退出数据接口。如果您没有可以访问互联网的单独管理网络，则此设置非常有用。源自管理接口的流量包括需要访问互联网的许可证注册和数据库更新。如果您使用 **data-interfaces**，在直接连接到管理网络的情况下，您仍可以在管理接口上使用设备管理器（或 SSH）但是，要对特定网络或主机进行远程管理，则应该使用 **configure network static-routes** 命令添加静态路由。请注意，数据接口上的设备管理器管理不受此设置的影响。如果使用 DHCP，则系统使用 DHCP 提供的网关，如果 DHCP 不提供网关，则使用数据接口作为回退方法。

- 如果网络信息已更改则需要重新连接 - 如果您已通过 SSH 连接到默认 IP 地址，但在初始设置时更改了 IP 地址，则会断开连接。使用新 IP 地址和密码重新进行连接。控制台连接不会受影响。
- 在本地管理设备？ - 输入是 (yes) 以使用设备管理器。回答否 (no) 表示您打算使用本地部署或云端交付管理中心来管理设备。

示例:

```

You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress. Please stand by.
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: yes

>

```

步骤 4 在新的管理 IP 地址上登录设备管理器。

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。

过程

步骤 1 在浏览器中输入以下 URL。

- 内部（以太网 1/2）—<https://192.168.95.1>。

- 管理 - https://management_ip。管理接口是 DHCP 客户端，因此 IP 地址取决于您的 DHCP 服务器。如果在 CLI 设置中更改了管理 IP 地址，则输入该地址。

步骤 2 使用用户名 **admin** 和默认密码 **Admin123** 登录。

下一步做什么

- 通过 设备管理器 安装向导运行；请参阅[完成初始配置](#)，第 97 页。

完成初始配置

首次登录设备管理器以完成初始配置时，请使用设置向导。完成安装向导后，您的设备应该会正常工作并部署了下列基本策略：

- 外部（Ethernet1/1）和内部接口（Ethernet1/2）。
- 内部和外部接口的安全区域。
- 信任所有内部到外部流量的访问规则。
- 接口 NAT 规则，用于将所有内部到外部流量转换到外部接口 IP 地址上的唯一端口。
- 在内部接口上运行的 DHCP 服务器。



注释 如果您执行了 [端到端程序](#)，第 88 页 程序，则这些任务中应该有一部分已经完成，特别是更改 admin 密码以及配置外部和管理接口。

过程

步骤 1 系统会提示您阅读和接受“最终用户许可协议”并更改管理员密码。

只有完成这些步骤，才能继续。

步骤 2 为外部接口和管理接口配置以下选项，然后点击下一步 (**Next**)。

注释 点击下一步后，您的设置将部署到设备中。该接口将命名为“outside”，并添加到“outside_zone”安全区。请确保您的设置准确无误。

- a) **外部接口** - 即连接到网关路由器的数据端口。在初始设备设置期间，您不能选择其他外部接口。第一个数据接口是默认的外部接口。

配置 IPv4 - 外部接口的 IPv4 地址。可以使用 DHCP，也可以手动输入静态 IP 地址、子网掩码和网关。另外，也可以选择**关**，不配置 IPv4 地址。您无法使用安装向导配置 PPPoE。如果接口连

接到 DSL、电缆调制解调器或 ISP 的其他连接，并且 ISP 使用 PPPoE 来提供 IP 地址，则可能需要使用 PPPoE。您可以在完成向导后配置 PPPoE。

配置 Ipv6 - 外部接口的 Ipv6 地址可以使用 DHCP，也可以手动输入静态 IP 地址、前缀和网关。另外，也可以选择关，不配置 IPv6 地址。

b) 管理接口

DNS 服务器 - 系统管理地址的 DNS 服务器。输入 DNS 服务器的一个或多个地址以解析名称。默认值为 OpenDNS 公共 DNS 服务器。如果您编辑字段并想要恢复默认值，请点击使用 **OpenDNS (Use OpenDNS)** 以重新将合适的 IP 地址载入字段。

防火墙主机名 - 系统管理地址的主机名。

步骤 3 配置系统时间设置，然后点击下一步。

a) 时区 - 选择系统时区。

b) **NTP 时间服务器** - 选择使用默认 NTP 服务器，还是手动输入 NTP 服务器的地址。可以添加多个服务器来提供备份。

步骤 4 (可选) 为系统配置智能许可证。

购买威胁防御设备会自动附带基本许可证。其他所有许可证均是可选的。

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

要立即注册设备，请点击链接登录智能软件管理器帐户，并参阅[配置许可](#)，第 98 页。

要使用评估许可证，请选择启动 **90 日评估期而不注册 (Start 90 day evaluation period without registration)**。

步骤 5 点击完成。

下一步做什么

- 尽管您可以继续使用评估许可证，但我们建议您注册并许可您的设备；请参阅[配置许可](#)，第 98 页。
- 您也可以选择使用设备管理器配置设备；请参阅[在设备管理器中配置防火墙](#)，第 105 页。

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

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：

- **基础版**-（必需）基础版 许可证。
- **IPS** - 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

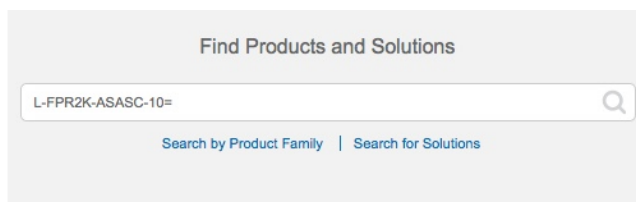
- 拥有 [智能软件管理器](#) 主帐户。
如果您还没有帐户，请点击此链接以 [设置新帐户](#)。通过智能软件管理器，您可以为组织创建一个主帐户。
- 您的智能软件许可帐户必须符合强加密 (3DES/AES) 许可证的要求，才能使用某些功能（已使用导出合规性标志启用）。

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 31: 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。

- 基础版 许可证：
 - L-FPR3110-BSE=
 - L-FPR3120-BSE=
 - L-FPR3130-BSE=
 - L-FPR3140-BSE=

- IPS、恶意软件防御和 URL 许可证组合：

- L-FPR3110T-TMC =
- L-FPR3120T-TMC =
- L-FPR3130T-TMC =
- L-FPR3140T-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-FPR3110T-TMC-1Y
- L-FPR3110T-TMC-3Y
- L-FPR3110T-TMC-5Y
- L-FPR3120T-TMC-1Y
- L-FPR3120T-TMC-3Y
- L-FPR3120T-TMC-5Y
- L-FPR3130T-TMC-1Y
- L-FPR3130T-TMC-3Y
- L-FPR3130T-TMC-5Y
- L-FPR3140T-TMC-1Y
- L-FPR3140T-TMC-3Y
- L-FPR3140T-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) 在常规 (**General**) 选项卡上，点击**新令牌 (New Token)**。

The screenshot shows the 'Product Instance Registration Tokens' section of a configuration page. It includes a 'New Token...' button circled in red, and a table with columns for Token, Expiration Date, and Description. The table contains one entry with a token ID, an expiration date of 2018-Jul-06 14:20:13 (in 354 days), and a description of FTD-5506.

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

The screenshot shows the 'Create Registration Token' dialog box. It contains fields for 'Virtual Account', 'Description', and 'Expire After' (set to 30 Days). There is a checkbox for 'Allow export-controlled functionality on the products registered with this token' which is checked. At the bottom right, there are 'Create Token' and 'Cancel' buttons.

- **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 functionality 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 32: 查看令牌

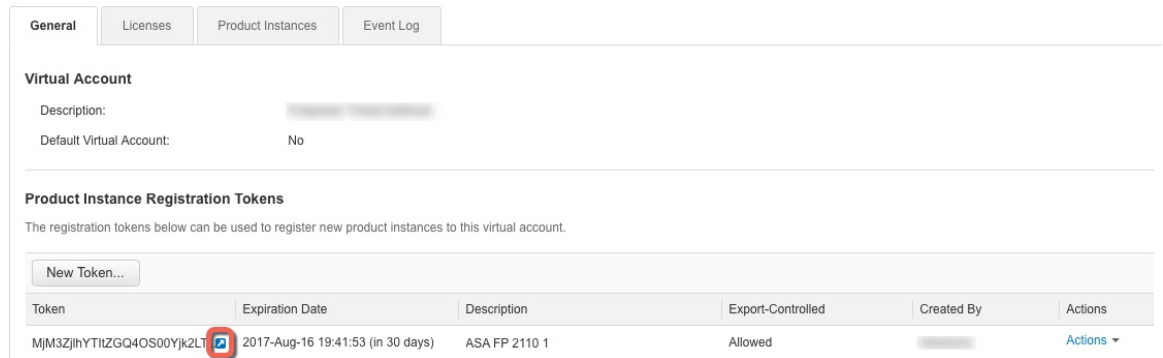
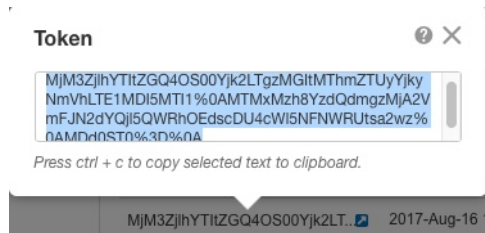


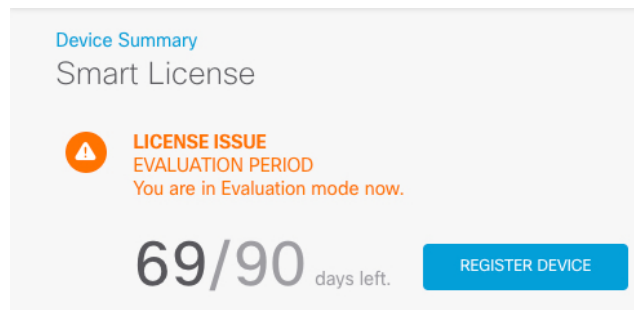
图 33: 复制令牌



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：

Smart License Registration ✕

- 1 Create or log in into your [Cisco Smart Software Manager](#) account.
- 2 On your assigned virtual account, under “General tab”, click on “**New Token**” to create token.
- 3 Copy the token and paste it here:

MGY2NzMwOGItODJiZi00NzFlWjNiNltYWMwNzU0ODY2ZGVlTE1NlUz
 Nzlv%0AODg5Mzh8SUQ5Vm5XbzZiSmN5M3I6K3owZ3ovVmpmc3Vtal
 JLQ2FFeGhFWmlW%0AWC9WTT0%3D%0A

- 4 Select Region

When you register the device, you are also registered with Cisco Security Services Exchange (SSE). Please select the region in which your device is operating. You will be able to see your device in the device list of the regional SSE portal.

Region

SSE US Region ▼ ⓘ

- 5 Cisco Success Network

Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.

Check out the [Sample Data](#) that will be sent to Cisco. [See more](#) ▼

Enable Cisco Success Network

CANCEL
REGISTER DEVICE

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：

Registration request sent on 10 Jul 2019. Please wait. Normally, it takes about one minute to complete the registration. You can check the task status in [Task List](#). Refresh this page to see the updated status.

在设备成功注册并刷新页面后，您会看到以下内容：

Device Summary

Smart License

✓

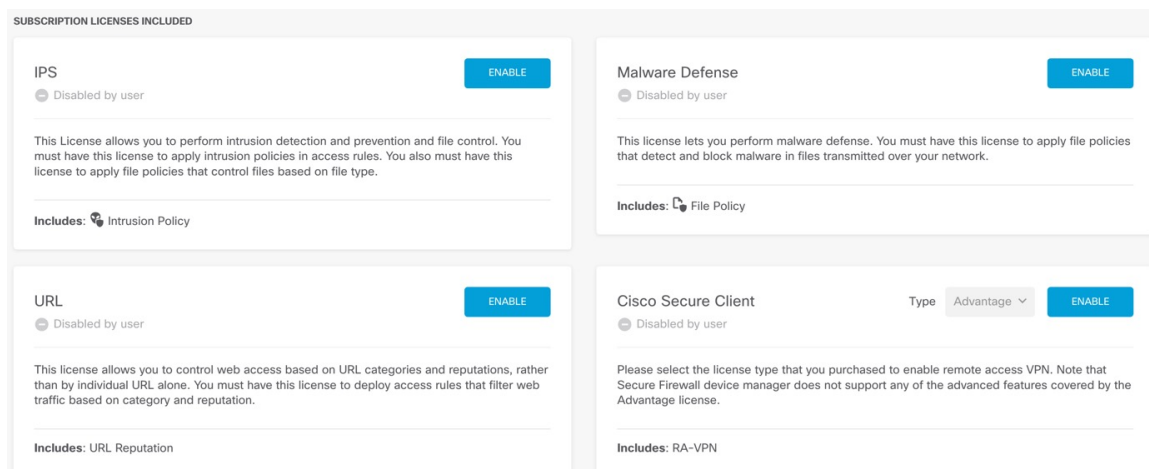
CONNECTED
SUFFICIENT LICENSE

Last sync: 10 Jul 2019 11:39 AM

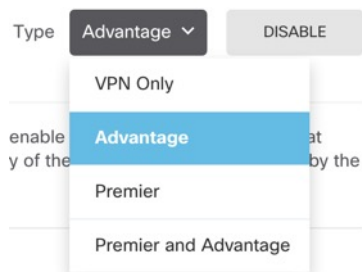
Next sync: 10 Jul 2019 11:49 AM

ⓘ

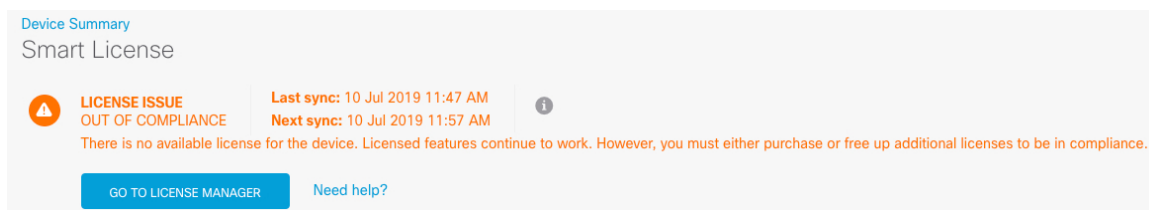
步骤 6 根据需要，点击每个可选许可证的启用/禁用控件。



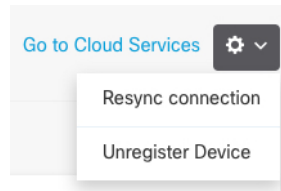
- **启用** - 将许可证注册到您的思科智能软件管理器帐户，并启用控制的功能。现在，您可以配置和部署该许可证控制的策略了。
- **禁用** - 取消许可证向思科智能软件管理器帐户的注册，并禁用控制的功能。新策略中无法配置这些功能，也不能再部署使用该功能的策略。
- 如果启用了 **Cisco Secure 客户端** 许可证，请选择要使用的许可证类型：**Advantage**、**Premier**、**VPN Only**或 **Premier** 和**Advantage**。



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。



在设备管理器中配置防火墙

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

过程

步骤 1 要从 40-Gb 接口（部分型号上可用）创建 4 x 10-Gb 分支接口，请选择**设备 (Device)**，然后点击**接口 (Interfaces)** 摘要中的链接。然后点击接口的分支图标。

如果您已经在配置中使用了 40-Gb 接口，则必须在继续创建分支之前删除该配置。

步骤 2 如果连接了其他接口，请选择**设备**，然后点击**接口摘要**中的链接。

点击每个接口的编辑图标 (✎)，以设置模式并定义 IP 地址和其他设置。

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

图 34: 编辑接口

A screenshot of the "Edit Physical Interface" configuration page. The page has a blue header with the title "Edit Physical Interface". Below the header, there are two input fields: "Interface Name" with the value "dmz" and "Status" with a toggle switch turned on. Below these is a "Description" field. At the bottom, there are three tabs: "IPv4 Address" (selected), "IPv6 Address", and "Advanced Options". Under the "IPv4 Address" tab, there is a "Type" dropdown menu set to "Static". Below that is an "IP Address and Subnet Mask" field with the value "192.168.6.1 / 24". At the very bottom, there is a small text example: "e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0".

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

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

以下示例显示如何为 DMZ 接口创建一个新的 DMZ 区域。

图 35: 安全区域对象

Add Security Zone

Name
dmz-zone

Description

Interfaces
+
dmz

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

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

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

图 36: DHCP 服务器

Add Server

Enabled DHCP Server

Interface
inside2

Address Pool
192.168.4.50-192.168.4.240
e.g. 192.168.45.46-192.168.45.254

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

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

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

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

图 37: 默认路由

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

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

步骤 6 选择策略 (Policies)，并为网络配置安全策略。

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

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

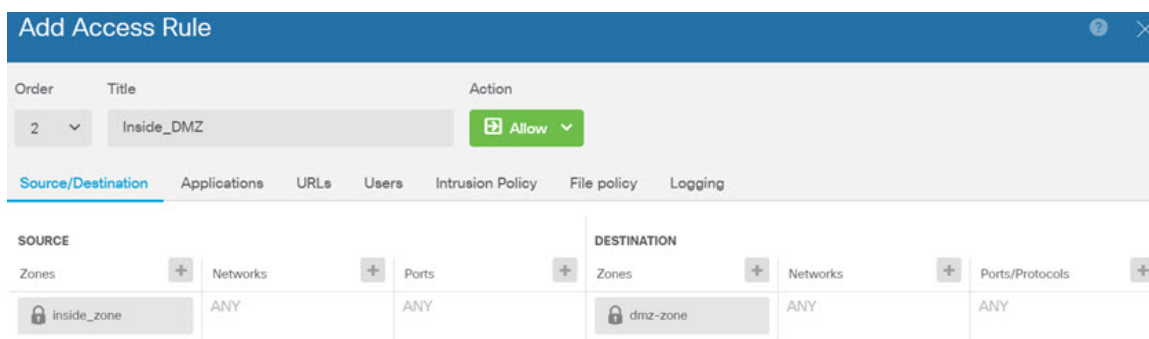
此外，您还可配置其他策略以提供附加服务，并对 NAT 和访问规则进行精细调整，以实现组织需要的结果。您可以配置以下策略：

- **SSL 解密 (SSL Decryption)** - 如果要检查加密连接（例如 HTTPS）是否存在入侵、恶意软件等，则必须解密连接。使用 SSL 解密策略确定需要解密的连接。系统检查连接后，会将其重新加密。
- **身份 (Identity)** - 如果要将网络活动与各个用户相关联，或根据用户或用户组成员身份控制网络访问，请使用身份策略确定与给定源 IP 地址关联的用户。

- **安全情报 (Security Intelligence)** - 使用安全情报策略快速丢弃进出列入黑名单的 IP 地址或 URL 的连接。将已知恶意站点列入黑名单后，在访问控制策略中即可无需考虑这些站点。思科提供定期更新的已知恶意地址和 URL 源，可使安全情报黑名单实现动态更新。使用情报源，无需通过编辑策略来添加或删除黑名单中的项目。
- **NAT (Network Address Translation)** - 使用 NAT 策略将内部 IP 地址转换为外部可路由地址。
- **访问控制 (Access Control)** - 使用访问控制策略确定网络上允许的连接。您可以按安全区域、IP 地址、协议、端口、应用、URL、用户或用户组进行过滤。您还可以使用访问控制规则来应用入侵策略和文件（恶意软件）策略。使用此策略实施 URL 过滤。
- **入侵 (Intrusion)** - 使用入侵策略检测已知威胁。即使使用访问控制规则应用入侵策略，也仍可以编辑入侵策略，以选择性地启用或禁用特定的入侵规则。


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

图 38: 访问控制策略



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

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

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

只有将更改部署至设备，更改才会生效。

访问威胁防御和 FXOS CLI

使用命令行界面 (CLI) 可设置系统以及对系统进行基本的故障排除。无法通过 CLI 会话配置策略。可以连接到控制台端口以访问 CLI。

也可以访问FXOS CLI以进行故障排除。



注释 您也可以通过 SSH 连接到 威胁防御 设备的管理接口。与控制台会话不同，SSH 会话默认使用 威胁防御 CLI，由此可使用 **connect fxos** 命令连接到 FXOS CLI。如果您为 SSH 连接打开某个数据接口，稍后可以连接到该接口上的地址。默认情况下，禁用 SSH 数据接口访问。此程序介绍控制台端口的访问（默认使用 FXOS CLI）。

过程

步骤 1 要登录 CLI，请将管理计算机连接到控制台端口。Secure Firewall 3100 配有一条 DB-9 转 RJ-45 串行电缆，所以您需要第三方串行转 USB 电缆进行连接。确保为您的操作系统安装必要的 USB 串行驱动程序（请参阅 Secure Firewall 3100 [硬件指南](#)）。控制台端口默认为 FXOS CLI。使用以下串行设置：

- 9600 波特率
- 8 个数据位
- 无奇偶校验
- 1 个停止位

您连接到 FXOS CLI。使用 **admin** 用户名和初始设置时设置的密码（默认值为 **Admin123**）登录 CLI。

示例：

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

步骤 2 访问威胁防御 CLI。

connect ftd

示例：

```
firepower# connect ftd
>
```

登录后，如需了解 CLI 中可用命令的相关信息，请输入 **help** 或 **?**。有关使用信息，请参阅 [Cisco Secure Firewall Threat Defense 命令参考](#)。

步骤 3 要退出 威胁防御 FTD CLI，请输入 **exit** 或 **logout** 命令。

此命令会将您重新导向至 FXOS CLI 提示。有关 FXOS CLI 中可用命令的相关信息，请输入 **?**。

示例：

```
> exit
firepower#
```

关闭防火墙电源

正确关闭系统非常重要。仅拔掉电源或按下电源开关可能会导致文件系统严重损坏。请记住，有许多进程一直在后台运行，拔掉或关闭电源不能正常关闭防火墙系统。

您可以使用设备管理器关闭防火墙，也可以使用FXOS CLI。

使用设备管理器关闭防火墙电源

您可以使用 设备管理器 正确关闭系统。

过程

步骤 1 使用 设备管理器 关闭防火墙。

- a) 点击设备 (**Device**)，然后点击系统设置 (**System Settings**) > 重新启动/关闭 (**Reboot/Shutdown**) 链接。
- b) 点击关闭。

步骤 2 如果您与防火墙建立了控制台连接，请在防火墙关闭时留意系统提示。您将看到以下提示：

```
System is stopped.
It is safe to power off now.

Do you want to reboot instead? [y/N]
```

如果没有控制台连接，请等待大约 3 分钟以确保系统已关闭。

步骤 3 您现在可以关闭电源开关并在必要时拔下电源插头以物理方式断开机箱的电源。

在 CLI 关闭防火墙电源

您可以使用FXOS CLI安全地关闭系统并关闭防火墙电源。您可以通过连接到控制台端口来访问CLI；请参阅[访问威胁防御和 FXOS CLI](#)，第 108 页。

过程

步骤 1 在 FXOS CLI 中，连接到 local-mgmt:


```
firepower # connect local-mgmt
```

步骤 2 发出 **shutdown** 命令：

```
firepower(local-mgmt) # shutdown
```

示例：

```
firepower(local-mgmt)# shutdown
This command will shutdown the system. Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense.....ok
```

步骤 3 留意防火墙关闭时的系统提示。您将看到以下提示：

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

步骤 4 您现在可以关闭电源开关并在必要时拔下电源插头以物理方式断开机箱的电源。

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](#)》。



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[哪种操作系统和管理器适合您？](#)，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 114 页
- [端到端程序：低接触调配](#)，第 115 页
- [端到端程序：激活向导](#)，第 117 页
- [中央管理员预配置](#)，第 119 页
- [通过低接触调配部署防火墙](#)，第 126 页
- [通过激活向导部署防火墙](#)，第 130 页
- [配置基本安全策略](#)，第 142 页
- [故障排除和维护](#)，第 153 页

- 后续操作，第 161 页

关于通过 CDO 管理威胁防御

云交付的 Cisco Secure Firewall Management Center

云交付的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。

CDO 激活方法

您可以通过以下方式来激活设备：

- 使用序列号进行低接触调配 -
 - 中央总部的管理员会将威胁防御发送到远程分支机构。无需预先配置。实际上，您不应在设备上配置任何内容，因为低接触调配不适用于预配置的设备。



注释 中心管理员可以在将设备发送到分支机构之前，使用威胁防御序列号在 CDO 上预注册威胁防御。

- 分支机构管理员连接并打开 威胁防御 电源。
- 中央管理员使用 CDO 完成 威胁防御 的配置。

如果您已开始配置设备，也可以使用序列号来激活设备管理器，但本指南并未介绍该方法。

- 使用 CLI 注册的激活向导 - 如果您需要执行任何预配置，或者如果您使用的是低接触调配不支持的管理器接口，请使用此手动方法。

威胁防御管理器访问接口

您可以使用管理接口或任何数据接口来进行管理器访问。但是，本指南介绍了外部接口访问。低接触调配仅支持外部接口。

管理接口是一个与威胁防御数据接口分开配置的特殊接口，它有自己的网络设置。即使您在数据接口上启用了管理器访问，也仍会使用管理接口网络设置。所有管理流量会继续源自或发往管理接口。如果在数据接口上启用了管理器访问，威胁防御会将传入管理流量通过背板转发到管理接口。对于传出管理流量，管理接口会通过背板将流量转发到数据接口。

从数据接口进行管理器访问具有以下限制：

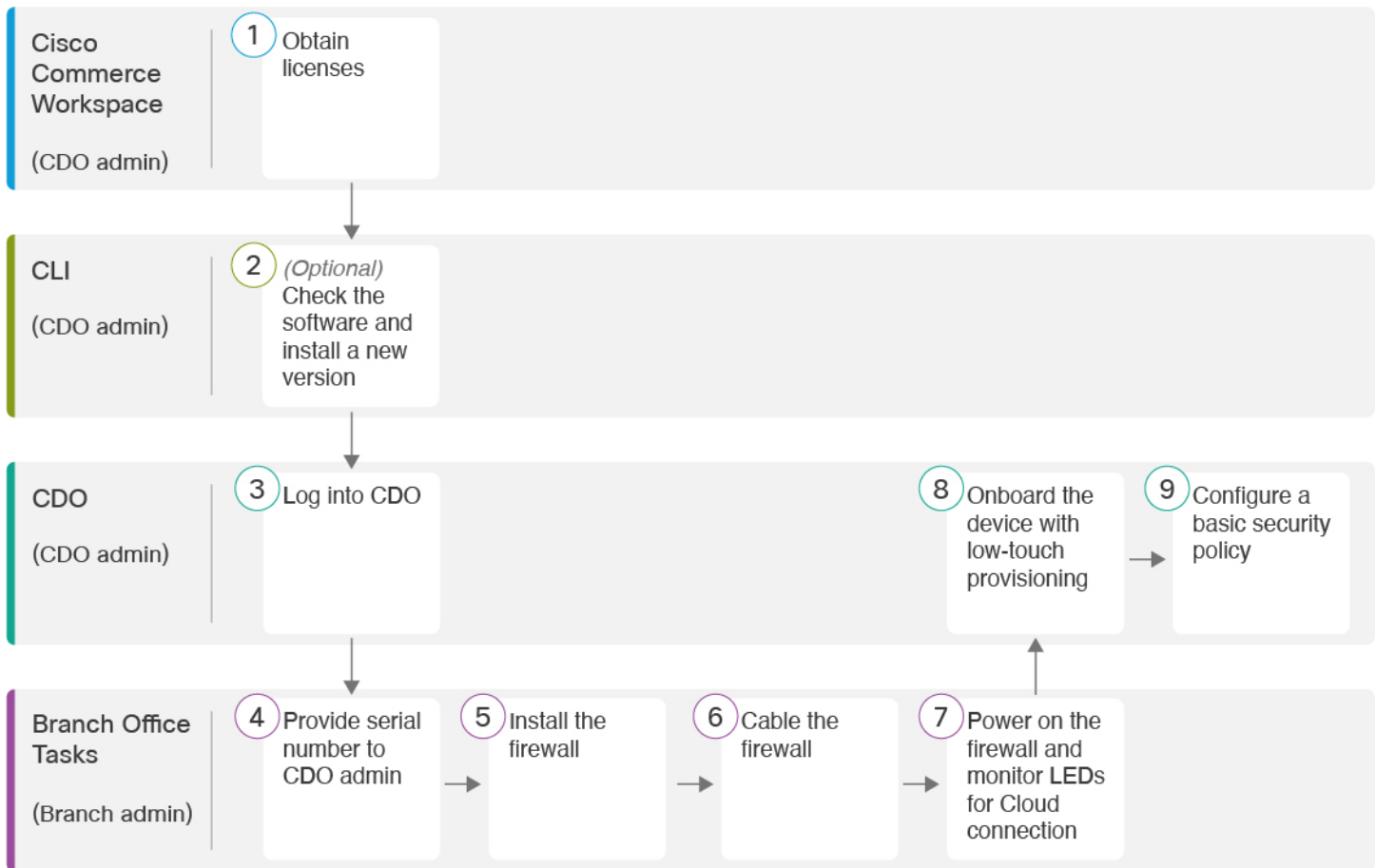
- 只能在物理数据接口上启用管理器访问。不能使用子接口或 EtherChannel。您还可以使用管理中心在单个辅助接口上启用管理器访问，以实现冗余。
- 此接口不能是仅管理接口。

- 仅路由防火墙模式，使用路由接口。
- 不支持 PPPoE。如果您的 ISP 需要 PPPoE，则必须在 威胁防御 与 WAN 调制解调器之间放入支持 PPPoE 的路由器。
- 接口只能位于全局 VRF 中。
- 默认不对数据接口启用 SSH，因此必须稍后使用 管理中心 来启用 SSH。由于管理接口网关将更改为数据接口，因此您也无法启动从远程网络到管理接口的 SSH 会话，除非您使用 **configure network static-routes** 命令为管理接口添加静态路由。
- 您不能使用单独的管理接口和仅事件接口。
- 不支持集群技术。在这种情况下，必须使用管理接口。
- 不支持高可用性。在这种情况下，必须使用管理接口。

端到端程序：低接触调配

请参阅以下任务以使用低接触调配部署带有 CDO 的 威胁防御。

图 39: 端到端程序：低接触调配



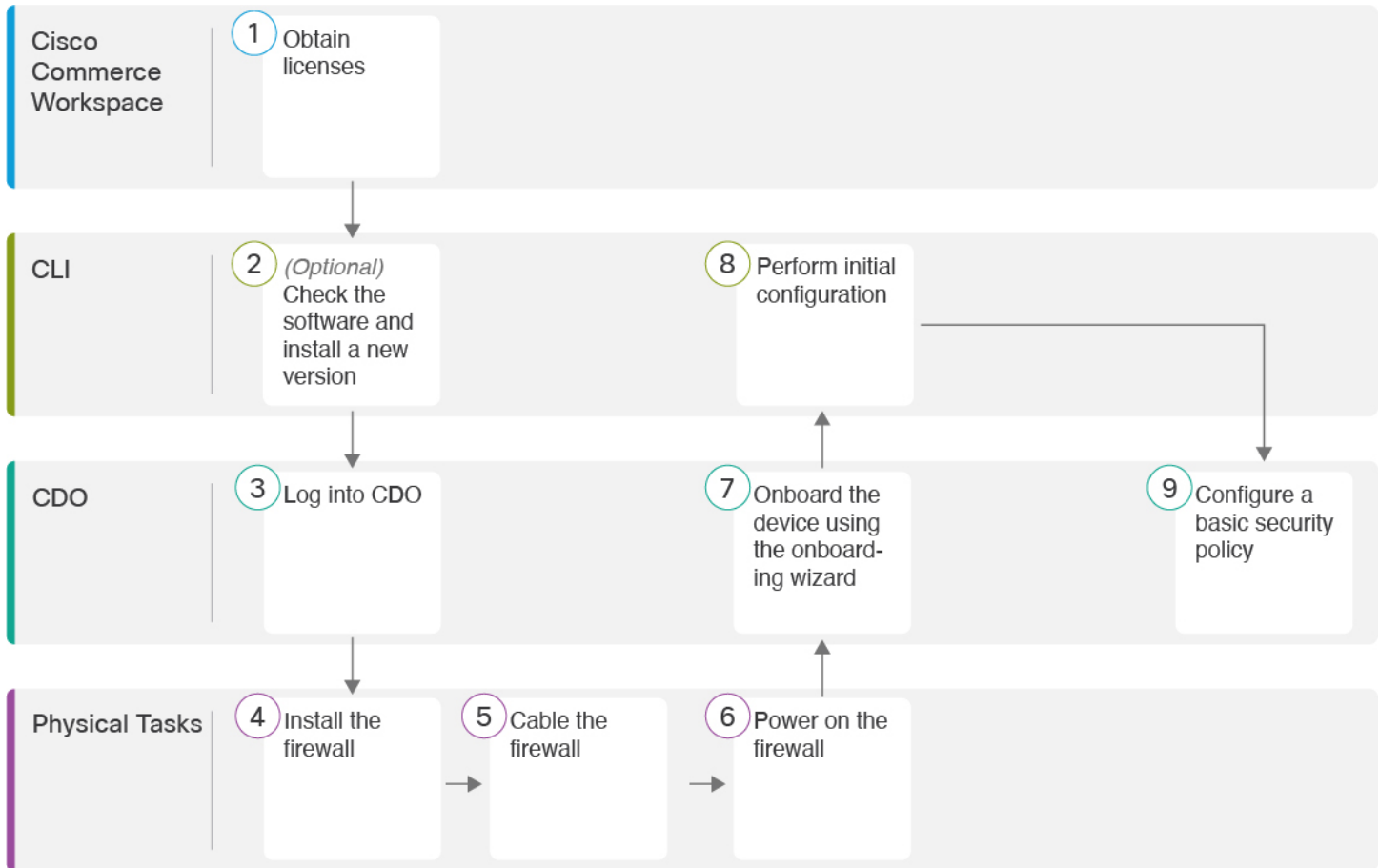
1	Cisco Commerce Workspace (CDO 管理员)	获取许可证，第 119 页。
2	CLI (CDO 管理员)	(可选) 检查软件并安装新版本，第 121 页。
3	CDO (CDO 管理员)	登录 CDO，第 122 页。
4	分支机构任务 (分支机构管理员)	向中央管理员提供防火墙序列号，第 126 页。
5	分支机构任务 (分支机构管理员)	安装防火墙。请参阅 硬件安装指南 。

⑥	分支机构任务 (分支机构管理员)	连接防火墙的电缆，第 127 页。
⑦	分支机构任务 (分支机构管理员)	打开防火墙电源，第 128 页。
⑧	CDO (CDO 管理员)	通过低接触调配激活设备，第 129 页。
⑨	CDO (CDO 管理员)	配置基本安全策略，第 142 页。

端到端程序：激活向导

请参阅以下任务，使用激活向导在 CDO 中激活 威胁防御。

图 40: 端到端程序：激活向导



1	Cisco Commerce Workspace	获取许可证，第 119 页。
2	CLI	(可选) 检查软件并安装新版本，第 121 页。
3	CDO	登录 CDO，第 122 页。
4	物理任务	安装防火墙。请参阅 硬件安装指南 。
5	物理任务	连接防火墙的电缆，第 130 页。
6	物理任务	打开防火墙电源，第 131 页。
7	CDO	使用激活向导激活设备，第 132 页。

8	CLI 或 设备管理器	<ul style="list-style-type: none"> • 使用 CLI 执行初始配置，第 133 页。 • 使用设备管理器执行初始配置，第 137 页。
9	CDO	配置基本安全策略，第 142 页。

中央管理员预配置

本节介绍如何获取防火墙的功能许可证；如何在部署之前安装新的软件版本；以及如何登录 CDO。

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：

- 基础版-（必需）基础版 许可证。
- IPS - 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

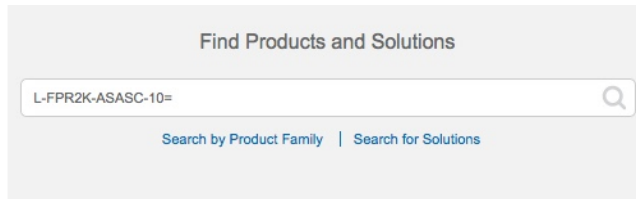
- 拥有智能软件管理器主帐户。
如果您还没有帐户，请点击此链接以[设置新帐户](#)。通过智能软件管理器，您可以为组织创建一个主帐户。
- 您的智能软件许可帐户必须符合强加密 (3DES/AES) 许可证的要求，才能使用某些功能（已使用导出合规性标志启用）。

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 41: 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。

- 基础版 许可证：
 - L-FPR3110-BSE=
 - L-FPR3120-BSE=
 - L-FPR3130-BSE=
 - L-FPR3140-BSE=
- IPS、恶意软件 防御和 URL 许可证组合：
 - L-FPR3110T-TMC =
 - L-FPR3120T-TMC =
 - L-FPR3130T-TMC =
 - L-FPR3140T-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-FPR3110T-TMC-1Y
- L-FPR3110T-TMC-3Y
- L-FPR3110T-TMC-5Y
- L-FPR3120T-TMC-1Y
- L-FPR3120T-TMC-3Y
- L-FPR3120T-TMC-5Y
- L-FPR3130T-TMC-1Y
- L-FPR3130T-TMC-3Y
- L-FPR3130T-TMC-5Y
- L-FPR3140T-TMC-1Y
- L-FPR3140T-TMC-3Y
- L-FPR3140T-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-FPR3K-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。

(可选) 检查软件并安装新版本

要检查软件版本并在必要时安装不同的版本，请执行以下步骤。我们建议您在配置防火墙之前安装目标版本。或者，您也可以在启动并运行后执行升级，但升级（保留配置）可能需要比按照此程序花费更长的时间。

我应该运行什么版本？

思科建议运行软件下载页面上的版本号旁边标有金色星号的 Gold Star 版本。您还可以参考 <https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html> 中所述的发布策略；例如，此公告描述短期版本编号（包含最新功能）、长期版本编号（较长时间的维护版本和补丁）或额外长期版本编号（最长期限的维护版本和补丁，用于政府认证）。

过程

步骤 1 打开防火墙电源，然后连接到控制台端口。有关详细信息，请参阅 [打开防火墙电源](#)，第 131 页和 [访问威胁防御和FXOS CLI](#)，第 153 页。

使用用户名 **admin** 和默认密码 **Admin123** 登录。

您连接到 FXOS CLI。第一次输入登录时，系统会提示您更改密码。此密码也用于 SSH 的威胁防御登录。

注释 如果密码已更改，但您不知道，则必须执行出厂重置以将密码重置为默认值。有关 [出厂重置程序](#) 的信息，请参阅 [FXOS 故障排除指南](#)。

示例:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: *****
Confirm new password: *****
Your password was updated successfully.
```

```
[...]
```

```
firepower#
```

步骤 2 在 FXOS CLI 中，显示正在运行的版本。

```
scope ssa
```

```
show app-instance
```

示例:

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name      Slot ID      Admin State      Operational State      Running Version Startup
Version Cluster Oper State
-----
ftd                   1            Enabled          Online                  7.2.0.65              7.2.0.65
                        Not Applicable
```

步骤 3 如果要安装新版本，请执行这些步骤。

a) 如果要为管理接口设置静态 IP 地址，请参阅[使用 CLI 执行初始配置](#)，第 133 页。默认情况下，管理接口将使用 DHCP。

您需要从可通过管理接口访问的服务器下载新的映像。

b) 执行《[FXOS 故障排除指南](#)》中的[重新映像程序](#)。

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 125 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 122 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

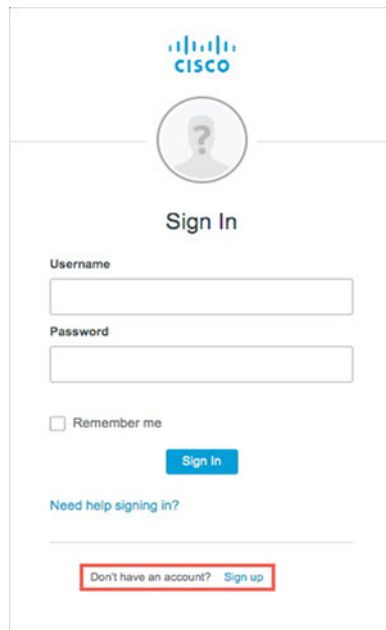
- **安装 DUO Security** - 我们建议您在手机上安装 Duo Security 应用。如果您对于如何安装 Duo 有疑问，请查看 [Duo 双因素身份验证指南：注册指南](#)。
- **时间同步** - 您要使用移动设备生成一次性密码。由于 OTP 是基于时间的，所以您的设备时钟与实时同步是非常重要的。请确保您的设备时钟设置为正确的时间。
- 使用当前版本的 Firefox 或 Chrome。

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 42: 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 43: 创建帐户

The screenshot shows a web form titled "Create Account" with the Cisco logo at the top. The form contains five input fields: "Email *", "Password *", "First name *", "Last name *", and "Organization *". Below the fields is a note: "* indicates required field". At the bottom of the form, there is a blue "Register" button and a "Back" link.

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。

- 在设置多因素身份验证屏幕中，点击配置。
- 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。

- 在向导结束时，点击继续登录。
- 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。

- 选择要与 Google Authenticator 配对的移动设备，然后点击下一步。
- 按照安装向导中的提示设置 Google Authenticator。

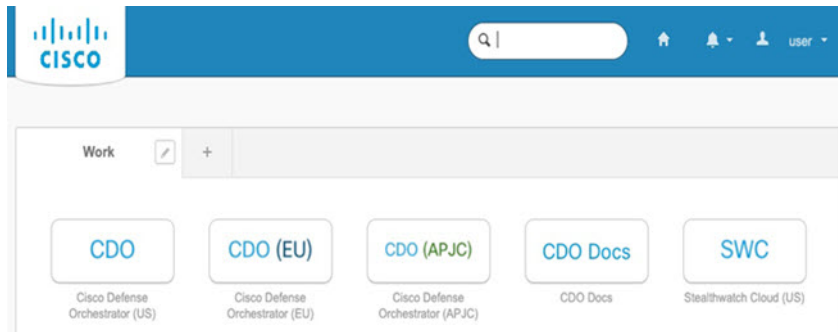
步骤 4 配置 Cisco Secure Sign-On 帐户的帐户恢复选项。

- 选择一个“忘记密码”问答。
- 选择恢复电话号码以使用 SMS 重置帐户。
- 选择安全图像。
- 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 44: 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

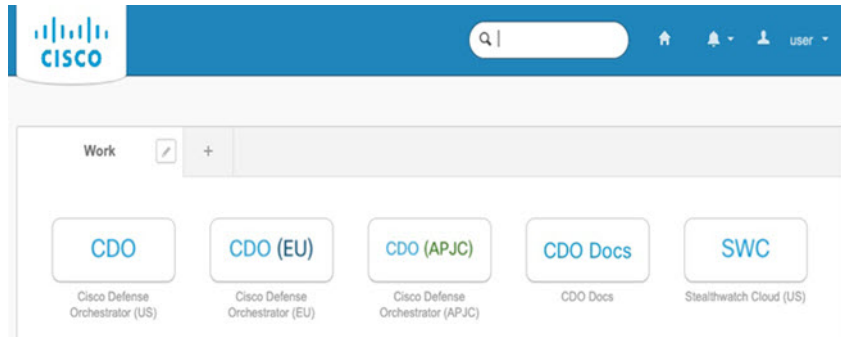
Cisco Defense Orchestrator (CDO) 使用 Cisco Secure Sign-On 作为身份提供商，并使用 Duo Security 进行多因素身份验证 (MFA)。

- 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 122 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 45: 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。

通过低接触调配部署防火墙

收到来自中央总部的威胁防御后，您只需连接并打开防火墙电源，即可从外部接口访问互联网。然后，中央管理员即可完成配置。

向中央管理员提供防火墙序列号

在安装防火墙或丢弃装运箱之前，请记下序列号，以便与中央管理员协调。

过程

步骤 1 打开机箱和机箱组件。

在连接任何电缆或打开防火墙电源之前，请清点防火墙和包装。您还应熟悉机箱布局、组件和 LED。

步骤 2 记录防火墙的序列号。

装运箱上有防火墙的序列号。它也可以在防火墙正面的拉出式卡舌的标签上找到。

步骤 3 将防火墙序列号发送给 IT 部门/中央总部的 CDO 网络管理员。

网络管理员需要您的防火墙序列号才能继续进行低接触调配、连接到防火墙并进行远程配置。

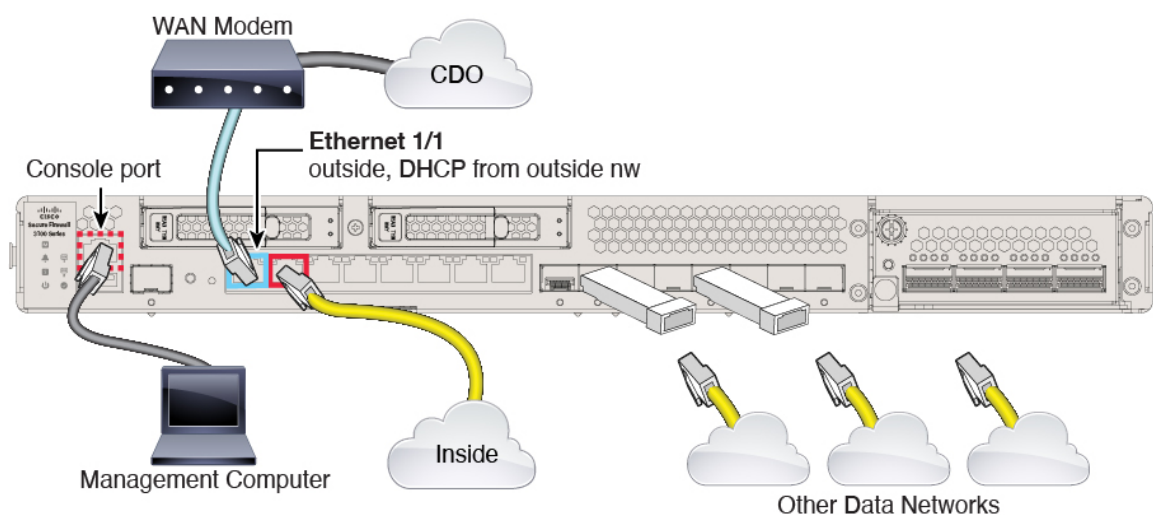
与 CDO 管理员沟通，制定激活时间表。

连接防火网的电缆

本主题介绍如何将 Secure Firewall 3100 连接到您的网络，以便由 CDO 进行管理。

如果您的分支机构收到了防火墙，并且您的工作是将其插入网络，[请观看此视频](#)。该视频介绍了您的防火墙上指示防火墙状态的 LED 顺序。如果需要，只需查看 LED 即可向 IT 部门确认防火墙的状态。

图 46: Secure Firewall 3100 布线



低接触调配支持连接到以太网 1/1（外部）上的 CDO。

过程

步骤 1 安装机箱。请参阅[硬件安装指南](#)。

步骤 2 将网线从以太网 1/1 接口连接到广域网 (WAN) 调制解调器。WAN 调制解调器是分支机构与互联网的连接，也将是防火墙与互联网的路由。

步骤 3 将内部接口（例如，以太网 1/2）连接到内部交换机或路由器。

您可以为内部选择任何接口。

步骤 4 将其他网络连接到其余接口。

步骤 5（可选）将管理计算机连接到控制台端口。

在分支机构的日常工作中不需要使用控制台连接；但出于故障排除目的，可能需要此连接。

打开防火墙电源

系统电源由位于防火墙后部的摇杆电源开关控制。电源开关以软通知开关形式实施，支持平稳地关闭系统以降低系统软件及数据损坏的风险。



注释 首次启动 威胁防御时，初始化大约需要 15 到 30 分钟。

开始之前

为防火墙提供可靠的电源（例如，使用不间断电源 (UPS)）非常重要。未事先关闭就断电可能会导致严重的文件系统损坏。后台始终有许多进程在运行，因此断电会使得系统无法正常关闭。

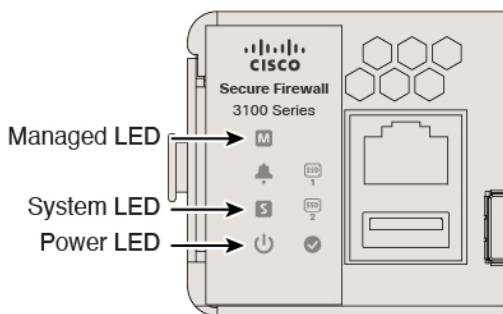
过程

步骤 1 将电源线一端连接到防火墙，另一端连接到电源插座。

步骤 2 使用位于机箱背面电源线旁边的标准摇杆型电源开关打开电源。

步骤 3 检查防火墙背面的电源 LED；如果该 LED 呈绿色稳定亮起，表示防火墙已接通电源。

图 47: 受管、电源和系统 LED



步骤 4 检查防火墙背面的系统 LED；其呈绿色稳定亮起之后，系统已通过通电诊断。

注释 将开关从开切换到关时，系统可能需要几秒钟才会最终关闭。在此期间，机箱前面的电源 LED 将闪烁绿色。在电源 LED 完全关闭之前，请勿拔出电源。

步骤 5 检查防火墙背面的受管 LED；当防火墙连接到思科云时，受管 LED 会呈绿色缓慢闪烁。

如果存在问题，受管 LED 会呈琥珀色和绿色闪烁，以表明防火墙无法访问思科云。如果看到这种情况，请确保将网线连接到以太网 1/1 接口和 WAN 调制解调器。在调整网络电缆后，如果防火墙在约 10 分钟后仍未连接到思科云，请致电您的 IT 部门。


下一步做什么

- 与您的 IT 部门沟通，确认您的激活时间表和活动。您应该与中央总部的 CDO 管理员制定通信计划。
- 完成此任务后，您的 CDO 管理员将能够远程配置和管理防火墙。就行了。

通过低接触调配激活设备

使用低接触调配和序列号激活 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。

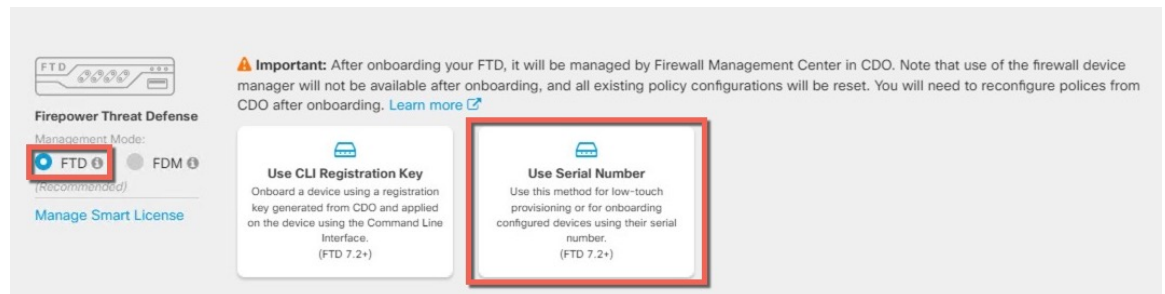
步骤 2 选择 **FTD** 磁贴。

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 119 页以查看可用的许可证。

步骤 4 选择使用序列号 (**Use Serial Number**) 作为激活方法。

图 48: 使用序列号



步骤 5 在 **连接 (Connection)** 区域中，输入设备序列号 (**Device Serial Number**) 和设备名称 (**Device Name**)，然后点击下一步 (**Next**)。

步骤 6 在 **密码重置 (Password Reset)** 区域中，点击是，此新设备从未登录或配置管理器 (**Yes, this new device has never been logged into or configured for a manager**) 单选按钮，然后点击下一步 (**Next**)。

步骤 7 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 8 对于 **订阅许可证 (Subscription License)**，请选中要启用的每个功能许可证。点击下一步。

步骤 9 (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，选择您刚刚激活的设备，然后选择位于右侧的**管理 (Management)** 窗格下列出的任何选项。

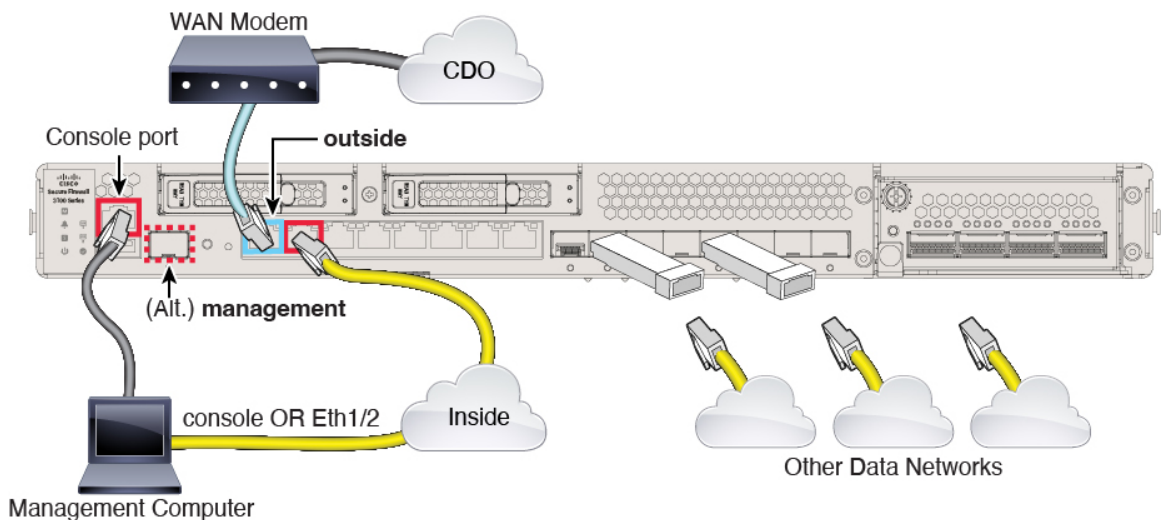
通过激活向导部署防火墙

本节介绍如何使用 CDO 激活向导来配置防火墙，以便进行激活。

连接防火墙的电缆

本主题介绍如何将 Secure Firewall 3100 连接到您的网络，以便由 CDO 进行管理。

图 49: Secure Firewall 3100 布线



您可以在任何数据接口或管理接口上连接到 CDO，具体取决于在初始设置期间为管理器访问设置的接口。本指南将介绍外部接口。

过程

步骤 1 安装机箱。请参阅[硬件安装指南](#)。

步骤 2 将外部接口（例如，以太网 1/1）连接到外部路由器。

您可以使用任何数据接口或管理接口来进行管理器访问。但是，本指南主要介绍外部接口访问，因为它是远程分支机构最可能遇到的场景。

步骤 3 将内部接口（例如，以太网 1/2）连接到内部交换机或路由器。

您可以为内部选择任何接口。

步骤 4 将其他网络连接到其余接口。

步骤 5 将管理计算机连接到控制台端口或以太网 1/2 接口。

如果使用 CLI 来执行初始设置，则需要连接到控制台端口。出于故障排除目的，也可能需要使用控制台端口。如果使用设备管理器来执行初始设置，请连接到以太网 1/2 接口。

打开防火墙电源

系统电源由位于防火墙后部的摇杆电源开关控制。电源开关以软通知开关形式实施，支持平稳地关闭系统以降低系统软件及数据损坏的风险。



注释 首次启动威胁防御时，初始化大约需要 15 到 30 分钟。

开始之前

为防火墙提供可靠的电源（例如，使用不间断电源 (UPS)）非常重要。未事先关闭就断电可能会导致严重的文件系统损坏。后台始终有许多进程在运行，因此断电会使得系统无法正常关闭。

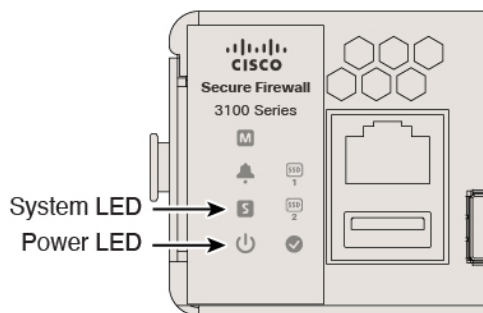
过程

步骤 1 将电源线一端连接到防火墙，另一端连接到电源插座。

步骤 2 使用位于机箱背面电源线旁边的标准摇杆型电源开关打开电源。

步骤 3 检查防火墙背面的电源 LED；如果该 LED 呈绿色稳定亮起，表示防火墙已接通电源。

图 50: 系统和电源 LED




步骤 4 检查防火墙背面的系统 LED；其呈绿色稳定亮起之后，系统已通过通电诊断。

注释 将开关从开切换到关时，系统可能需要几秒钟才会最终关闭。在此期间，机箱前面的电源 LED 将闪烁绿色。在电源 LED 完全关闭之前，请勿拔出电源。

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。

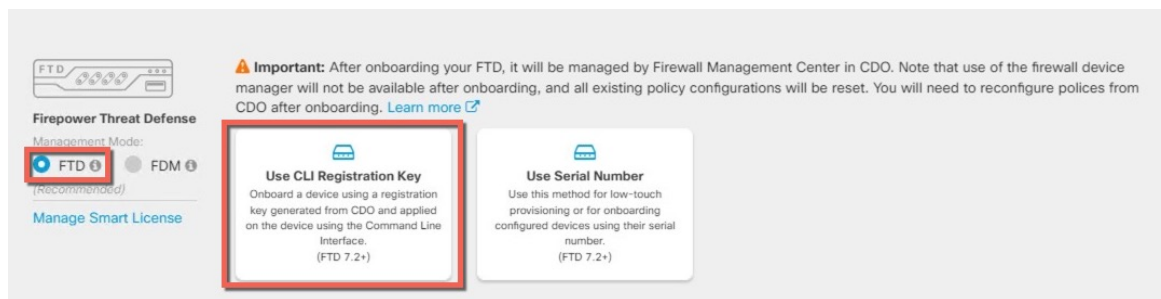
步骤 2 选择 **FTD** 磁贴。

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 119 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)** 作为激活方法。

图 51: 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 对于订阅许可证 (**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 CLI 或使用设备管理器完成初始配置：

- 使用 CLI 执行初始配置，第 133 页 - 完成启动脚本后，在 FTD CLI 中复制此命令。
- 使用设备管理器执行初始配置，第 137 页 - 将命令的 *cdo_hostname*、*registration_key* 和 *nat_id* 部分复制到管理中心/CDO 主机名/IP 地址 (**Management Center/CDO Hostname/IP Address**)、管理中心/CDO 注册密钥 (**Management Center/CDO Registration Key**) 和 NAT ID 字段中。

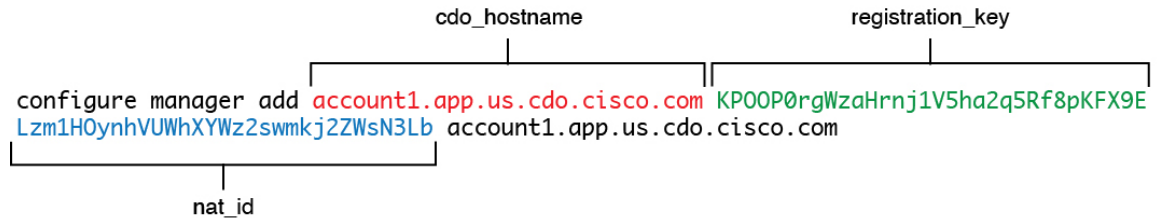
示例：

CLI 设置的命令示例：

```
configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsn3Lb account1.app.us.cdo.cisco.com
```

GUI 设置的命令组件示例：

图 52: 配置管理器添加命令组件



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，选择您刚刚激活的设备，然后选择位于右侧的管理 (Management) 窗格下列出的任何选项。

执行初始配置

使用 CLI 或使用 设备管理器 执行 威胁防御 的初始配置。

使用 CLI 执行初始配置

连接到威胁防御 CLI 以执行初始设置。在对初始配置使用 CLI 时，仅保留管理接口和管理器访问设置。当您使用设备管理器执行初始设置时，如果您切换到 CDO 进行管理，除管理接口和管理器访问接口设置外，在设备管理器中完成的所有接口配置都将保留。请注意，不会保留其他默认配置设置，例如访问控制策略。

Procedure

步骤 1 连接到控制台端口上的 威胁防御 CLI。

控制台端口连接到 FXOS CLI。

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

第一次登录 FXOS 时，系统会提示您更改密码。此密码也用于 SSH 的威胁防御登录。

Note 如果密码已更改，但您不知道，则必须重新映像设备以将密码重置为默认值。有关 [重新映像程序](#) 的信息，请参阅 [FXOS 故障排除指南](#)。

Example:

```

firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: *****
Confirm new password: *****
Your password was updated successfully.

[...]

firepower#

```

步骤 3 连接到 威胁防御 CLI。**connect ftd****Example:**

```

firepower# connect ftd
>

```

步骤 4 首次登录威胁防御时，系统会提示您接受“最终用户许可协议” (EULA)。然后，您将看到管理接口设置的 CLI 设置脚本。

即使您在数据接口上启用了管理器访问，也仍会使用管理接口设置。

Note 除非清除配置，否则无法重复 CLI 安装向导（例如，通过重新建立映像）。但是，可以稍后在 CLI 中使用 **configure network** 命令更改所有这些设置。请参阅 [Cisco Secure Firewall Threat Defense 命令参考](#)。

默认值或以前输入的值会显示在括号中。要接受之前输入的值，请按 **Enter** 键。

请参阅以下准则：

- **通过 DHCP 或手动配置 IPv4? (Configure IPv4 via DHCP or manually?)**— 选择 **manual**。虽然您不打算使用管理接口，但必须设置 IP 地址，例如专用地址。如果管理接口设置为 DHCP，则无法配置数据接口用于管理，因为默认路由（必须是 **data-interfaces**，请参阅下一个要点）可能会被接收自 DHCP 服务器的路由覆盖。
- **输入管理接口的 IPv4 默认网关 (Enter the IPv4 default gateway for the management interface)** — 将网关设置为 **data-interfaces**。此设置将在背板上转发管理流量，因此可路由通过管理器访问数据接口。
- **本地管理设备? (Manage the device locally?)** — 输入 **no** 以使用 CDO。回答 **yes** 意味着您将改为使用设备管理器。
- **配置防火墙模式? (Configure firewall mode?)** — 输入 **routed**。只有路由防火墙模式支持外部管理器访问。

Example:

```

You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress. Please stand by.
You must change the password for 'admin' to continue.
Enter new password: *****
Confirm new password: *****
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]:
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...

Update policy deployment information
- add device configuration
- add network discovery
- add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required. In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>

```

步骤 5 配置用于管理器访问的外部接口。

configure network management-data-interface

然后，系统会提示您为外部接口配置基本网络设置。请参阅以下有关使用此命令的详细信息：

- 如果您要使用数据接口进行管理，则管理接口无法使用 DHCP。如果在初始设置期间没有手动设置 IP 地址，则可以使用 **configure network {ipv4 | ipv6} manual** 命令立即设置它。如果您尚未将管理接口网关设置为 **data-interfaces**，此命令将立即设置它。
- 当您威胁防御添加到 CDO 时，CDO 会发现并维护接口配置，包括以下设置：接口名称和 IP 地址、网关静态路由、DNS 服务器和 DDNS 服务器。有关 DNS 服务器配置的详细信息，请参阅下文。在 CDO 中，您可以稍后对管理器访问接口配置进行更改，但要确保更改不会阻止威胁防御或 CDO 重新建立管理连接。如果管理连接中断，威胁防御将包含 **configure policy rollback** 命令以恢复以前的部署。
- 如果配置 DDNS 服务器更新 URL，则威胁防御会自动添加来自 Cisco 受信任根 CA 捆绑包的所有主要 CA 证书，以便威胁防御可以验证用于 HTTPS 连接的 DDNS 服务器证书。威胁防御支持使用 DynDNS 远程 API 规范 (<https://help.dyn.com/remote-access-api/>) 的任何 DDNS 服务器。
- 此命令设置数据接口 DNS 服务器。使用设置脚本（或使用 **configure network dns servers** 命令）设置的管理 DNS 服务器用于管理流量。数据 DNS 服务器用于 DDNS（如果已配置）或适用于此接口的安全策略。

在 CDO 上，数据接口 DNS 服务器在您分配给此威胁防御的平台设置策略中配置。当您威胁防御添加到 CDO 时，本地设置将保留，并且 DNS 服务器不会添加到平台设置策略。但是，如果稍后将平台设置策略分配给包含 DNS 配置的威胁防御，则该配置将覆盖本地设置。我们建议您主动配置与此设置匹配的 DNS 平台设置，以使 CDO 和威胁防御同步。

此外，仅当在初始注册时发现 DNS 服务器，CDO 才会保留本地 DNS 服务器。例如，如果您使用管理接口注册了设备，但随后使用 **configure network management-data-interface** 命令配置数据接口，则必须在 CDO 中手动配置所有这些设置（包括 DNS 服务器），以便与威胁防御配置匹配。

- 将威胁防御注册到 CDO 后，您可以将该管理接口更改为管理接口或另一数据接口。
- 您在安装向导中设置的 FQDN 将用于此接口。
- 您可以通过命令清除整个设备配置；在恢复场景中可使用此选项，但我们不建议您在初始设置或正常操作中使用它。
- 要禁用数据管理，请输入 **configure network management-data-interface disable** 命令。

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://deanwinchester:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.
```

>

Example:

```

> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>

```

步骤 6 使用 CDO 生成的 **configure manager add** 命令确定将管理此威胁防御的 CDO。请参阅[使用激活向导激活设备, on page 132](#)以生成命令。

Example:

```

> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
LzmlHOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
Manager successfully configured.

```

使用设备管理器执行初始配置

连接到设备管理器以执行威胁防御的初始设置。当您使用设备管理器执行初始设置时，如果您切换到 CDO 进行管理，除管理接口和管理器访问设置外，在设备管理器中完成的所有接口配置都将保留。请注意，不会保留其他默认配置设置，例如访问控制策略或安全区。使用 CLI 时，只有管理接口和管理器访问设置会被保留（例如，不保留默认的内部接口配置）。

过程

-
- 步骤 1** 将管理计算机连接到 Ethernet1/2 接口。
- 步骤 2** 登录设备管理器。
- 在浏览器中输入以下 URL: **https://192.168.95.1**
 - 使用用户名 **admin** 和默认密码 **Admin123** 登录。
 - 系统会提示您阅读和接受“最终用户许可协议”并更改管理员密码。
- 步骤 3** 首次登录设备管理器以完成初始配置时，请使用设置向导。您可以选择通过点击页面底部的**跳过设备设置 (Skip device setup)** 来跳过安装向导。

完成安装向导后，除了内部接口 (Ethernet1/2) 的默认配置外，您还将拥有外部（以太网 1/1）接口的配置，该接口会在您切换到 CDO 管理接口时进行维护。

a) 为外部接口和管理接口配置以下选项，然后点击**下一步 (Next)**。

1. **外部接口地址 (Outside Interface Address)** - 此接口通常是互联网网关，并且可用作管理器访问接口。在初始设备设置期间，您不能选择其他外部接口。第一个数据接口是默认的外部接口。

如果要使用与外部（或内部）不同的接口来进行管理器访问，则必须在完成安装向导后手动配置该接口。

配置 IPv4 - 外部接口的 IPv4 地址。可以使用 DHCP，也可以手动输入静态 IP 地址、子网掩码和网关。另外，也可以选择**关**，不配置 IPv4 地址。您无法使用安装向导配置 PPPoE。如果接口连接到 DSL、电缆调制解调器或 ISP 的其他连接，并且 ISP 使用 PPPoE 来提供 IP 地址，则可能需要使用 PPPoE。您可以在完成向导后配置 PPPoE。

配置 Ipv6 - 外部接口的 Ipv6 地址可以使用 DHCP，也可以手动输入静态 IP 地址、前缀和网关。另外，也可以选择**关**，不配置 IPv6 地址。

2. **管理接口**

如果在 CLI 中执行了初始设置，您将不会看到管理接口设置。

即使您在数据接口上启用了管理器访问，也仍会使用管理接口设置。例如，通过数据接口在背板上路由的管理流量将使用管理接口 DNS 服务器解析 FQDN，而非使用数据接口 DNS 服务器。

DNS 服务器 - 系统管理地址的 DNS 服务器。输入 DNS 服务器的一个或多个地址以解析名称。默认值为 OpenDNS 公共 DNS 服务器。如果您编辑字段并想要恢复默认值，请点击**使用 OpenDNS (Use OpenDNS)** 以重新将合适的 IP 地址载入字段。

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

b) 配置**时间设置 (NTP) (Time Setting [NTP])** 并点击**下一步 (Next)**。

1. **时区** - 选择系统时区。
2. **NTP 时间服务器** - 选择使用默认 NTP 服务器，还是手动输入 NTP 服务器的地址。可以添加多个服务器来提供备份。

c) 选择**启动 90 日评估期而不注册**。

不要向智能软件管理器注册威胁防御；所有许可均在 CDO 上执行。

d) 点击**完成**。

e) 系统将提示您选择**云管理 (Cloud Management)** 或**独立 (Standalone)**。对于 CDO 云交付管理中心，选择**独立 (Standalone)**，然后选择**明白了 (Got It)**。

云管理 (Cloud Management) 选项适用于传统 CDO/FDM 功能。

步骤 4 （可能需要）配置管理接口。请参阅**设备 > 接口**上的管理接口。

管理接口必须将网关设置为数据接口。默认情况下，管理接口从 DHCP 接收 IP 地址和网关。如果您没有从 DHCP 接收到网关（例如，您没有将此接口连接到网络），则网关将默认为数据接口，并且您无需进行任何配置。如果您从 DHCP 接收到了网关，则需要使用静态 IP 地址配置此接口，并将该网关设置为数据接口。

步骤 5 如果要配置其他接口，包括要用于管理器访问的外部或内部接口，请选择**设备 (Device)**，然后点击**接口 (Interfaces)** 摘要中的链接。

有关在设备管理器中配置接口的更多信息，请参阅[在设备管理器中配置防火墙，第 105 页](#)。在向 CDO 注册设备时，不会保留其他设备管理器配置。

步骤 6 选择 **设备 > 系统设置 > 集中管理**，然后点击 **继续** 设置管理中心管理。

步骤 7 配置管理中心/CDO 详细信息 (**Management Center/CDO Details**)。

图 53: 管理中心/CDO 详细信息

Configure Connection to Management Center or CDO


Provide details to register to the management center/CDO.

Management Center/CDO Details

Do you know the Management Center/CDO hostname or IP address?

Yes No


Threat Defense



10.89.5.16
fe80::6a87:c6ff:fea6:4c00/64

→

Management Center/CDO



10.89.5.35

Management Center/CDO Hostname or IP Address

10.89.5.35

Management Center/CDO Registration Key

●●●● 👁

NAT ID

Required when the management center/CDO hostname or IP address is not provided. We recommend always setting the NAT ID even when you specify the management center/CDO hostname or IP address.

11203

Connectivity Configuration

Threat Defense Hostname

1120-3

DNS Server Group

CustomDNSServerGroup ▾

Management Center/CDO Access Interface

Data Interface

Please select an interface ▾

Management Interface [View details](#)

CANCEL
CONNECT

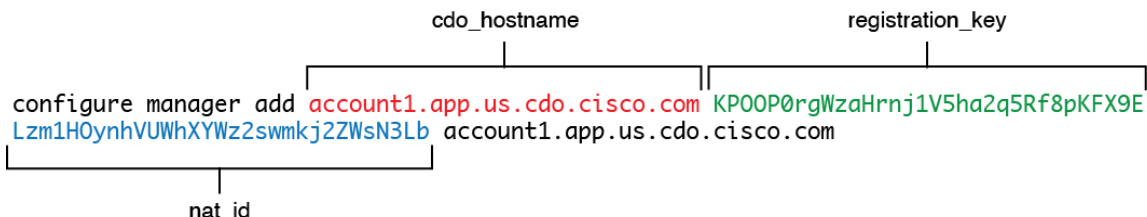
- a) 对于您知道管理中心/CDO 主机名或 IP 地址吗 (Do you know the Management Center/CDO hostname or IP address), 点击是 (Yes)。

CDO 会生成 `configure manager add` 命令。请参阅[使用激活向导激活设备](#)，第 132 页以生成命令。

```
configure manager add cdo_hostname registration_key nat_id display_name
```

示例:

图 54: 配置管理器添加命令组件



- b) 将命令的 `cdo_hostname`、`registration_key` 和 `nat_id` 部分复制到管理中心/CDO 主机名/IP 地址 (Management Center/CDO Hostname/IP Address)、管理中心/CDO 注册密钥 (Management Center/CDO Registration Key) 和 NAT ID 字段中。

步骤 8 配置连接配置。

- a) 指定 **FTD** 主机名。

此 FQDN 将用于外部接口，或您为管理中心/CDO 访问接口 (Management Center/CDO Access Interface) 选择的任何接口。

- b) 指定 **DNS** 服务器组。

选择现有组或创建一个新组。默认 DNS 组名为 **CiscoUmbrellaDNSServerGroup**，其中包括 OpenDNS 服务器。

此设置设定数据接口 DNS 服务器。您使用安装向导设置的管理 DNS 服务器用于管理流量。数据 DNS 服务器用于 DDNS（如果已配置）或适用于此接口的安全策略。您可能会选择用于管理的相同 DNS 服务器组，因为管理和数据流量都通过外部接口到达 DNS 服务器。

在 CDO 上，数据接口 DNS 服务器在您分配给此威胁防御的平台设置策略中配置。当您威胁防御添加到 CDO 时，本地设置将保留，并且 DNS 服务器不会添加到平台设置策略。但是，如果稍后将平台设置策略分配给包含 DNS 配置的威胁防御，则该配置将覆盖本地设置。我们建议您主动配置与此设置匹配的 DNS 平台设置，以使 CDO 和威胁防御同步。

此外，仅当在初始注册时发现 DNS 服务器，CDO 才会保留本地 DNS 服务器。

- c) 对于管理中心/CDO 访问接口 (Management Center/CDO Access Interface)，请选择外部 (**outside**)。

您可以选择任何已配置的接口，但本指南假定您使用的是外部接口。

步骤 9 如果您选择了外部之外的其他数据接口，那么请添加默认路由。

您将看到一条消息，要求您检查是否有通过接口的默认路由。如果您选择了外部接口，那么您已经在安装向导中配置了此路由。如果您选择了其他接口，那么需要在连接到 CDO 之前手动配置默认路由。有关在设备管理器中配置静态路由的更多信息，请参阅[在设备管理器中配置防火墙](#)，第 105 页。

步骤 10 点击添加动态 DNS (DDNS) 方法 (Add a Dynamic DNS [DDNS] method)。

如果威胁防御的 IP 地址发生变化，DDNS 可确保 CDO 接通完全限定域名 (FQDN) 内的威胁防御。参阅设备 > 系统设置 > DDNS 服务配置动态 DNS。

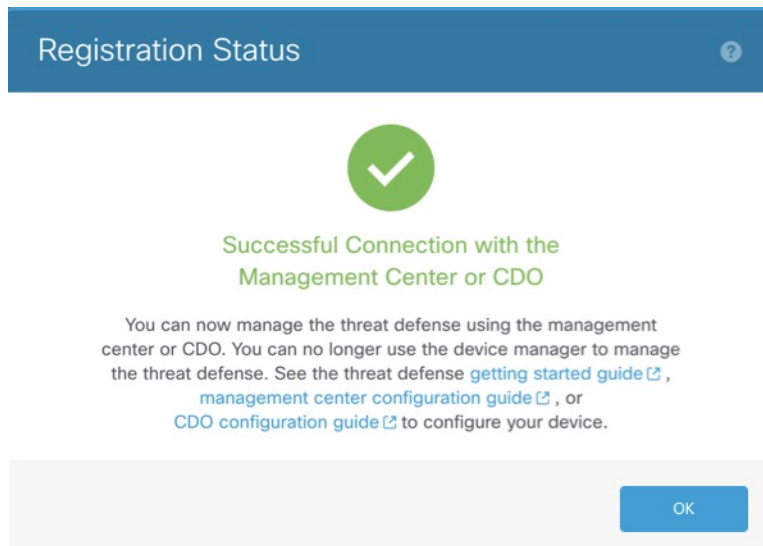
如果您在将威胁防御添加到 CDO 之前配置 DDNS，则威胁防御会自动为思科受信任根 CA 捆绑包中的所有主要 CA 添加证书，以便威胁防御可以验证用于 HTTPS 连接的 DDNS 服务器证书。威胁防御支持使用 DynDNS 远程 API 规范 (<https://help.dyn.com/remote-access-api/>) 的任何 DDNS 服务器。

步骤 11 点击连接 (Connect)。注册状态对话框显示切换到 CDO 的当前状态。在保存管理中心/CDO 注册设置 (Saving Management Center/CDO Registration Settings) 步骤之后，转到 CDO，然后添加防火墙。

如果要取消切换到 CDO，请点击取消注册 (Cancel Registration)。否则，在保存管理中心/CDO 注册设置 (Saving Management Center/CDO Registration Settings) 步骤之前不要关闭设备管理器浏览器窗口。如果这样做，该过程将暂停，并且只有在您重新连接到设备管理器时才会恢复。

如果在保存管理中心/CDO 注册设置 (Saving Management Center/CDO Registration Settings) 步骤后仍与设备管理器保持连接，最终您会看到与管理中心或 CDO 成功连接 (Successful Connection with Management Center or CDO) 对话框，在此之后将与设备管理器断开连接。

图 55: 成功连接



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。您在管理器访问设置中配置了外部接口的基本设置，但仍需要将其分配给安全区域。
- DHCP 服务器 - 在内部接口上为客户端使用 DHCP 服务器。

- 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。
- SSH - 在管理器访问接口上启用 SSH。

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。

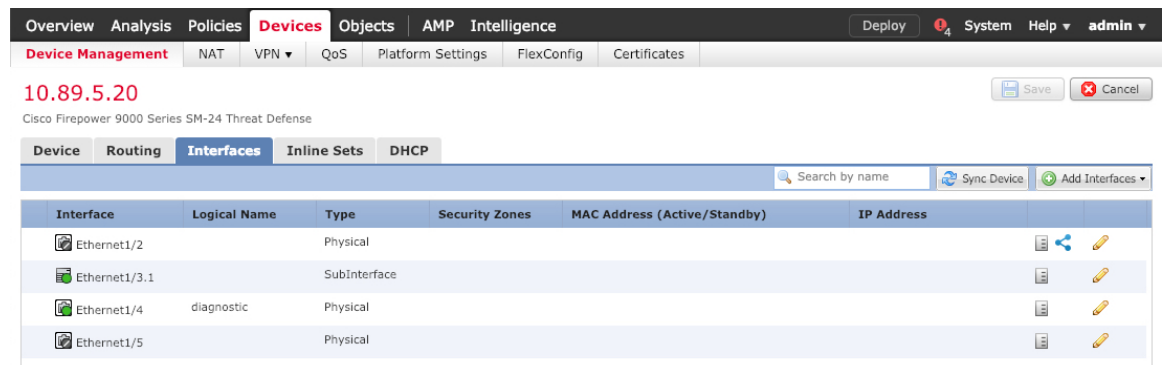
典型的边缘路由情况是通过 DHCP 从 ISP 获取外部接口地址，同时在内部接口上定义静态地址。

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**)。




The screenshot shows the Cisco Firepower 9000 Series SM-24 Threat Defense configuration interface. The top navigation bar includes tabs for Overview, Analysis, Policies, **Devices**, Objects, AMP, and Intelligence. Below this, there are sub-tabs for NAT, VPN, QoS, Platform Settings, FlexConfig, and Certificates. The main content area shows the configuration for a Cisco Firepower 9000 Series SM-24 Threat Defense device. The **Interfaces** tab is selected, displaying a table of interfaces:

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

步骤 3 要从 40-Gb 接口（部分型号上可用）创建 4 x 10-Gb 分支接口，请点击接口的分支图标。

如果您已经在配置中使用了 40-Gb 接口，则必须在继续创建分支之前删除该配置。

步骤 4 点击要用于内部的接口的编辑 ()。

此时将显示一般 (**General**) 选项卡。

Edit Physical Interface ? X

General IPv4 IPv6 Advanced Hardware Configuration

Name: Enabled Management Only

Description:

Mode: ▼

Security Zone: ▼

Interface ID:

MTU: (64 - 9000)

OK Cancel

- 输入长度最大为 48 个字符的名称 (Name)。

例如，将接口命名为 **inside**。
- 选中启用 (Enabled) 复选框。
- 将模式 (Mode) 保留为无 (None)。
- 从安全区域 (Security Zone) 下拉列表选择一个现有的内部安全区域，或者点击新建 (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。

- 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**

Edit Physical Interface

General **IPv4** IPv6 Advanced Hardware Configuration

IP Type: ▼

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

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

f) 点击**确定 (OK)**。

步骤 5 点击要用于外部的接口的 **编辑** (✎)。

此时将显示**一般 (General)** 选项卡。

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

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

您已经为该接口预配置了管理器访问，因此该接口就已经命名、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。您仍然必须在此屏幕上为直通流量策略配置安全区域。

- a) 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。

b) 点击**确定 (OK)**。

步骤 6 点击**保存 (Save)**。

配置 DHCP 服务器

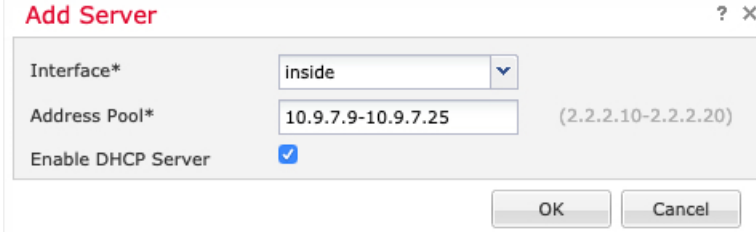
如果希望客户端使用 DHCP 从威胁防御处获取 IP 地址，请启用 DHCP 服务器。

过程

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

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

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



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

步骤 4 单击确定 (OK)。

步骤 5 单击保存 (Save)。

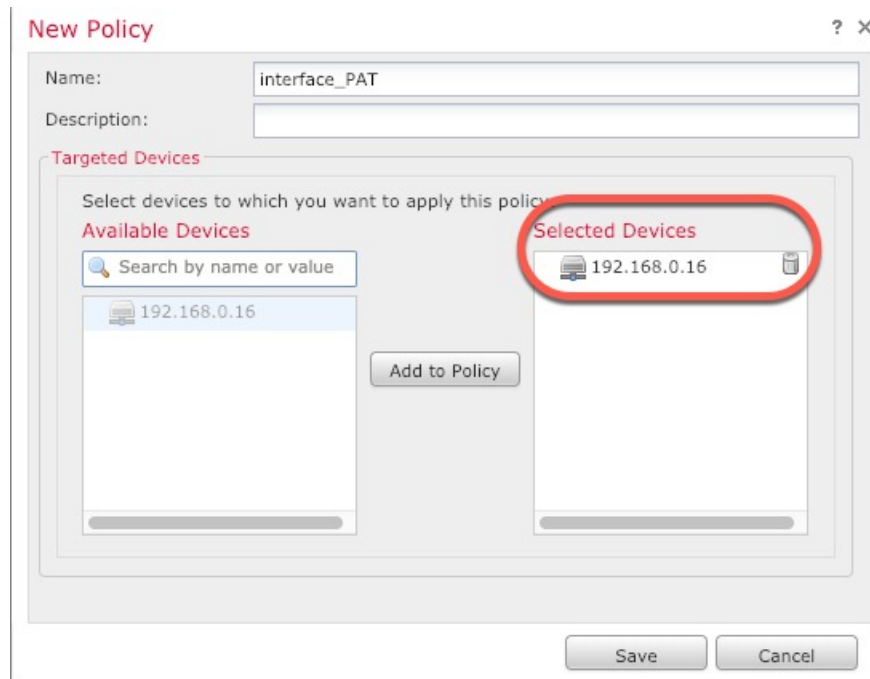
配置 NAT

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，然后单击新建策略 (New Policy) > 威胁防御 NAT (Threat Defense NAT)。

步骤 2 为策略命名，选择要使用策略的设备，然后单击 Save。

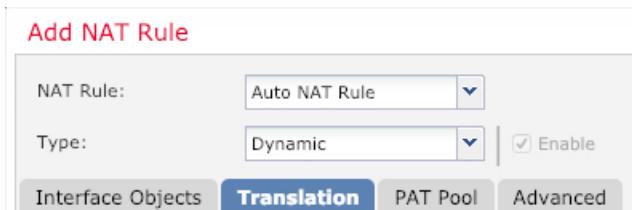


策略即已添加 管理中心。您仍然需要为策略添加规则。

步骤 3 点击添加规则 (**Add Rule**)。

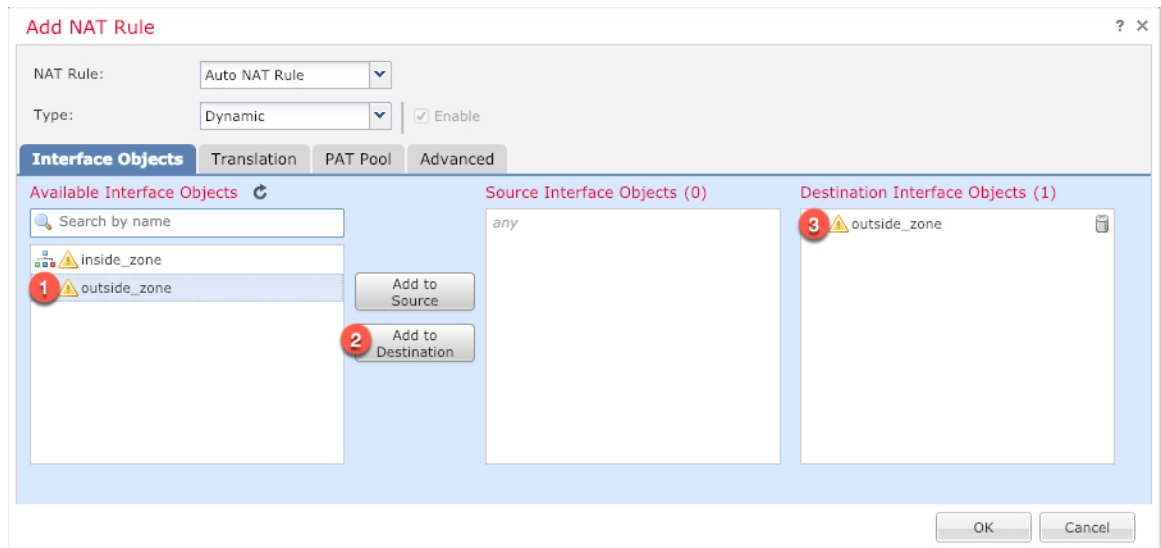
Add NAT Rule 对话框将显示。

步骤 4 配置基本规则选项：

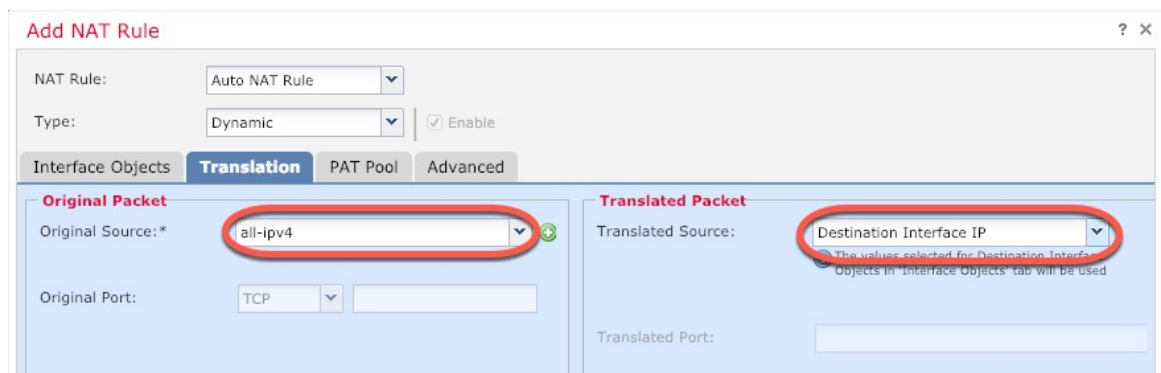


- **NAT 规则 (NAT Rule)** - 选择自动 NAT 规则 (**Auto NAT Rule**)。
- **类型 (Type)** - 选择动态 (**Dynamic**)。

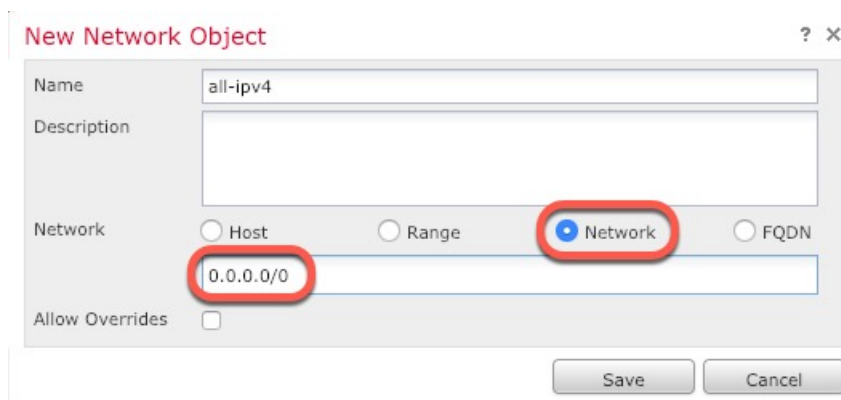
步骤 5 在 **Interface Objects** 页面，将 **Available Interface Objects** 区域中的外部区域添加到 **Destination Interface Objects** 区域。



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)。

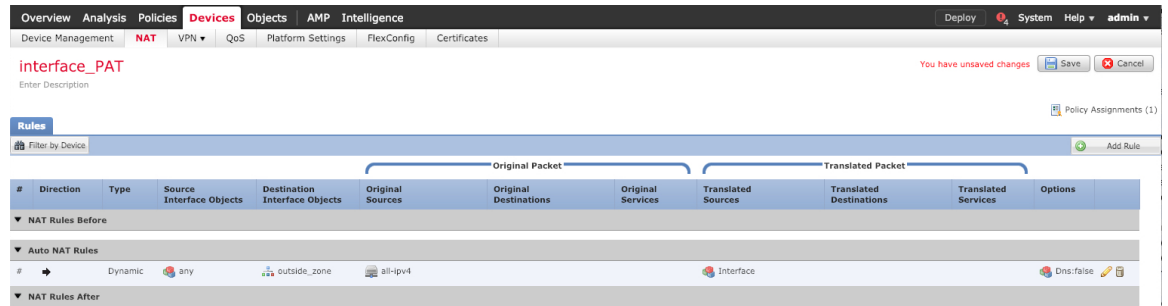


注释 您不能使用系统定义的 **any-ipv4** 对象，因为自动 NAT 规则在对象定义过程中添加 NAT，并且您无法编辑系统定义的对象。

- 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。

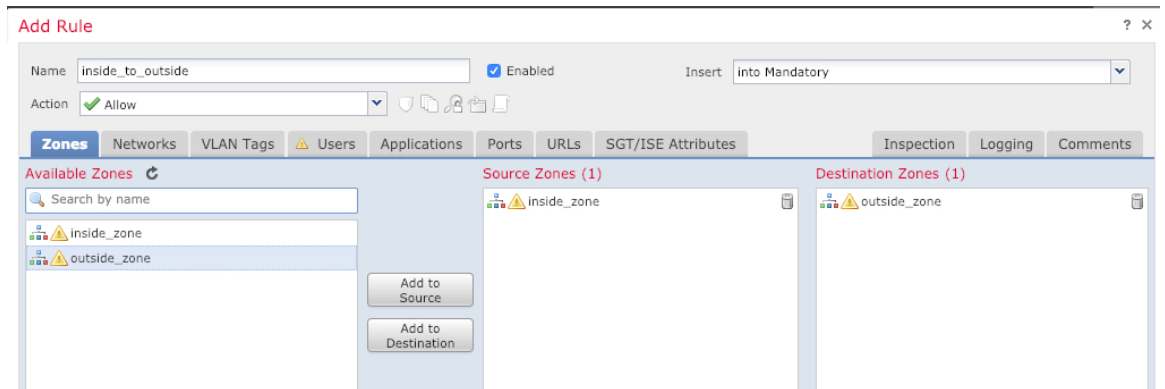
允许流量从内部传到外部

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：



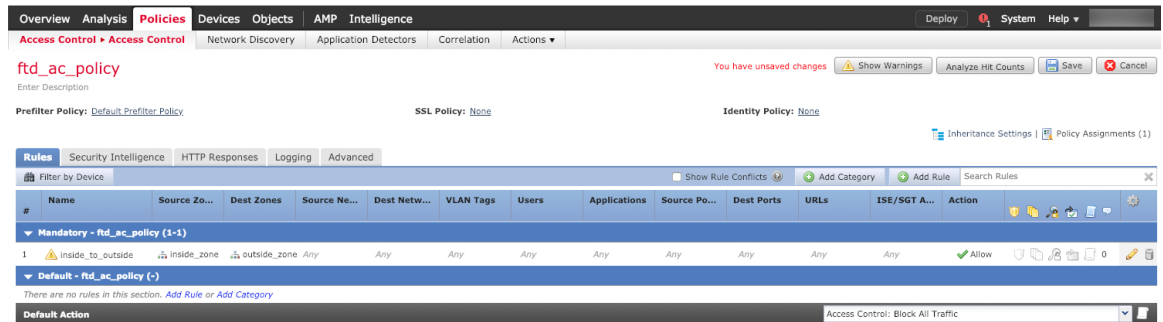
- 名称 (Name) - 为此规则命名，例如 **inside_to_outside**。
- 源区域 (Source Zones) - 从可用区域 (Available Zones) 中选择内部区域，然后点击添加到源 (Add to Source)。

- 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 (**Save**)。

在管理器访问数据接口上配置 SSH

如果在数据接口（例如外部）上启用了管理中心访问，则应使用此程序在该接口上启用 SSH。本节介绍如何启用 威胁防御上一个或多个 数据 接口的 SSH 连接。诊断逻辑接口上不支持 SSH。



注释 管理接口上默认已启用 SSH，但此屏幕不会影响管理 SSH 访问。

管理接口与设备上的其他接口分离。它用于设置设备并将其注册到管理中心。数据接口的 SSH 与管理接口的 SSH 共用内部和外部用户列表。其他设置单独进行配置：对于数据接口，使用此屏幕启用 SSH 和访问列表；数据接口的 SSH 流量使用常规路由配置，并不是所有静态路由均在设置时或 CLI 中配置。

对于管理接口，要配置 SSH 访问列表，请参阅 [Cisco Secure Firewall Threat Defense 命令参考](#) 中的 **configure ssh-access-list** 命令。要配置静态路由，请参阅 **configure network static-routes** 命令。默认情况下，在初始设置时通过管理接口配置默认路由。

要使用 SSH，您也不需要允许主机 IP 地址的访问规则。您只需按照本部分配置 SSH。

您只能 SSH 到可访问接口；如果 SSH 主机位于外部接口上，则只能直接向外部接口发起管理连接。



注释 在您连续三次尝试使用 SSH 登录 CLI 失败后，设备会终止 SSH 连接。

开始之前

- 可以使用 **configure user add** 命令。默认情况下，有一个您在初始设置期间为其配置密码的 **admin** 用户。还可以通过在平台设置中配置**外部身份验证**，在 LDAP 或 RADIUS 上配置外部用户。
- 您需要定义允许与设备建立 SSH 连接的主机或网络对象。您可以在此过程中添加对象，但如果要使用对象组标识一组 IP 地址，请确保规则中所需的组已经存在。选择**对象 > 对象管理**以配置对象。



注释 不能使用系统提供的 **any** 网络对象。而是使用 **any-ipv4** 或 **any-ipv6**。

过程

步骤 1 选择 **设备 > 平台设置**，并创建或编辑 **威胁防御** 策略。

步骤 2 选择**安全外壳 (Secure Shell)**。

步骤 3 标识允许 SSH 连接的接口和 IP 地址。

使用此表可以限制哪些接口将接受 SSH 连接，以及允许建立这些连接的客户端的 IP 地址。您可以使用网络地址而不是单个 IP 地址。

a) 点击**添加 (Add)** 以添加新规则，或点击**编辑 (Edit)** 以编辑现有规则。

b) 配置规则属性：

- **IP 地址**-用于标识允许建立 HTTPS 连接的主机或网络的**网络对象** 或**组**。从下拉列表中选择**一个对象**，或者点击 **+** 以添加新的网络对象。
- **安全区域 (Security Zones)** - 添加包含将允许进行 SSH 连接的接口的区域。对于不在区域中的接口，可以在所选**安全区域 (Selected Security Zones)** 列表下方的字段中键入接口名称，然后点击**添加 (Add)**。仅当设备包含所选接口或区域时，才会将这些规则应用于该设备。

c) 点击**确定 (OK)**。

步骤 4 点击**保存 (Save)**。

此时，您可以转至**部署 > 部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

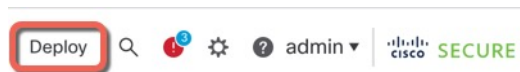
部署配置

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 56: 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 57: 全部部署

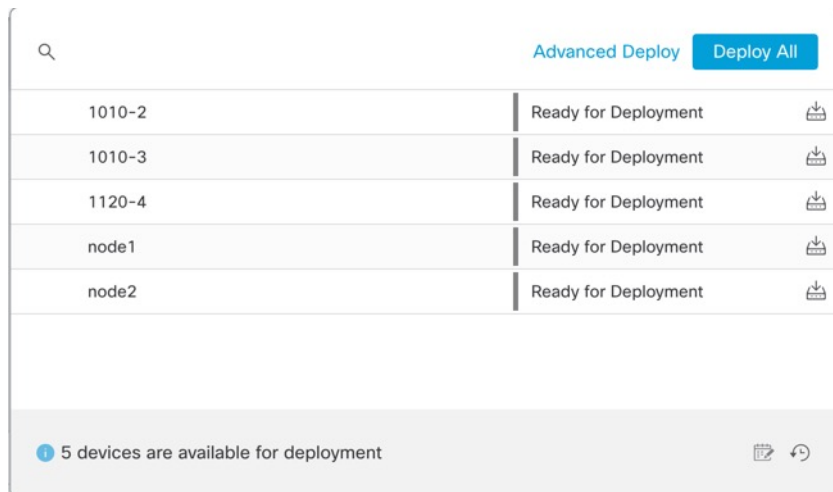
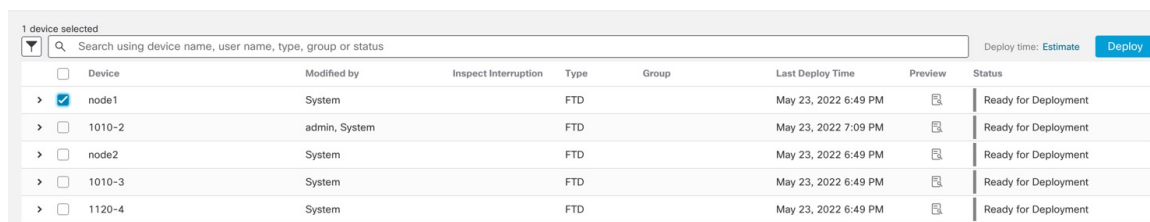
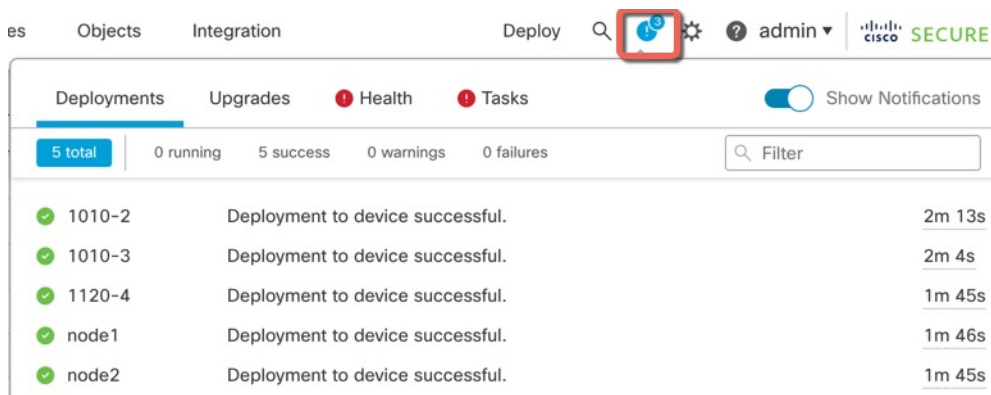


图 58: 高级部署



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 59: 部署状态



Deployment ID	Status	Message	Time
1010-2	Success	Deployment to device successful.	2m 13s
1010-3	Success	Deployment to device successful.	2m 4s
1120-4	Success	Deployment to device successful.	1m 45s
node1	Success	Deployment to device successful.	1m 46s
node2	Success	Deployment to device successful.	1m 45s

故障排除和维护

访问威胁防御和FXOS CLI

使用命令行界面 (CLI) 可设置系统以及对系统进行基本的故障排除。无法通过 CLI 会话配置策略。可以连接到控制台端口以访问 CLI。

也可以访问FXOS CLI以进行故障排除。



注释 您也可以通过 SSH 连接到威胁防御设备的管理接口。与控制台会话不同，SSH 会话默认使用威胁防御 CLI，由此可使用 `connect fxos` 命令连接到 FXOS CLI。如果您为 SSH 连接打开某个数据接口，稍后可以连接到该接口上的地址。默认情况下，禁用 SSH 数据接口访问。此程序介绍控制台端口的访问（默认使用 FXOS CLI）。

过程

步骤 1 要登录 CLI，请将管理计算机连接到控制台端口。Secure Firewall 3100 配有一条 DB-9 转 RJ-45 串行电缆，所以您需要第三方串行转 USB 电缆进行连接。确保为您的操作系统安装必要的 USB 串行驱动程序（请参阅 Secure Firewall 3100 [硬件指南](#)）。控制台端口默认为 FXOS CLI。使用以下串行设置：

- 9600 波特率
- 8 个数据位
- 无奇偶校验
- 1 个停止位

您连接到 FXOS CLI。使用 **admin** 用户名和初始设置时设置的密码（默认值为 **Admin123**）登录 CLI。

示例：

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

步骤 2 访问威胁防御 CLI。

connect ftd

示例：

```
firepower# connect ftd
>
```

登录后，如需了解 CLI 中可用命令的相关信息，请输入 **help** 或 **?**。有关使用信息，请参阅 [Cisco Secure Firewall Threat Defense 命令参考](#)。

步骤 3 要退出 威胁防御 FTD CLI，请输入 **exit** 或 **logout** 命令。

此命令会将您重新导向至 FXOS CLI 提示。有关 FXOS CLI 中可用命令的相关信息，请输入 **?**。

示例：

```
> exit
firepower#
```

排除数据接口上的管理连接故障

当使用数据接口进行管理器访问而不是使用专用管理接口时，必须注意在 CDO 中更改 威胁防御 的接口和网络设置，以免中断连接。如果在将 威胁防御 添加到 CDO 后更改管理接口类型（从数据到管理，或从管理到数据），如果接口和网络设置未正确配置，则可能会丢失管理连接。

本主题可帮助您排除管理连接丢失的问题。

查看管理连接状态

在 CDO 中，在设备 (**Devices**) > 设备管理 (**Device Management**) > 设备 (**Device**) > 管理 (**Management**) > 管理器访问 - 配置详细信息 (**Manager Access - Configuration Details**) > 连接状态 (**Connection Status**) 页面上检查管理连接状态。

在 威胁防御 CLI，输入 **sftunnel-status-brief** 命令以查看管理连接状态。您还可以使用 **sftunnel-status** 查看更完整的信息。

请参阅以下有关关闭连接的输出示例；没有显示“连接至“信息，也没有显示心跳信息：

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

请参阅以下关于已建立连接的输出示例，其中显示了对等信道和心跳信息：

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

查看 威胁防御 网络信息

在 威胁防御 CLI 上，查看管理和管理器访问数据接口网络设置：

show network

```
> show network
===== [ System Information ] =====
Hostname           : 5516X-4
DNS Servers        : 208.67.220.220,208.67.222.222
Management port    : 8305
IPv4 Default route
  Gateway           : data-interfaces
IPv6 Default route
  Gateway           : data-interfaces

===== [ br1 ] =====
State              : Enabled
Link               : Up
Channels           : Management & Events
Mode               : Non-Autonegotiation
MDI/MDIX          : Auto/MDIX
MTU                : 1500
MAC Address        : 28:6F:7F:D3:CB:8D
----- [ IPv4 ] -----
Configuration      : Manual
Address            : 10.99.10.4
Netmask            : 255.255.255.0
Gateway            : 10.99.10.1
----- [ IPv6 ] -----
Configuration      : Disabled

===== [ Proxy Information ] =====
State              : Disabled
Authentication     : Disabled

===== [ System Information - Data Interfaces ] =====
DNS Servers        :
Interfaces         : GigabitEthernet1/1
```

```

===== [ GigabitEthernet1/1 ] =====
State                : Enabled
Link                 : Up
Name                 : outside
MTU                  : 1500
MAC Address          : 28:6F:7F:D3:CB:8F
----- [ IPv4 ] -----
Configuration        : Manual
Address              : 10.89.5.29
Netmask               : 255.255.255.192
Gateway              : 10.89.5.1
----- [ IPv6 ] -----
Configuration        : Disabled

```

检查向 CDO 注册 威胁防御

在威胁防御 CLI 中，检查 CDO 注册是否已完成。请注意，此命令不会显示管理连接的当前状态。

show managers

```

> show managers
Type                : Manager
Host                : account1.app.us.cdo.cisco.com
Display name        : account1.app.us.cdo.cisco.com
Identifier           : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration         : Completed
Management type     : Configuration

```

对 CDO 执行 ping 操作

在威胁防御 CLI 上，使用以下命令从数据接口对 CDO 执行 ping 操作：

ping cdo_hostname

在威胁防御 CLI 上，使用以下命令从管理接口对 CDO 执行 ping 操作，该接口应通过背板路由到数据接口：

ping system cdo_hostname

捕获 威胁防御 内部接口上的数据包

在威胁防御 CLI 上，捕获内部背板接口 (nlp_int_tap) 上的数据包，以查看是否发送了管理数据包：

capture 名称 interface nlp_int_tap trace detail match ip any any

show capture name trace detail

检查内部接口状态，统计信息和数据包计数

在威胁防御 CLI 上，查看有关内部背板接口 nlp_int_tap 的信息：

show interace detail

```

> show interface detail
[...]
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec

```

```

(Full-duplex), (1000 Mbps)
Input flow control is unsupported, output flow control is unsupported
MAC address 0000.0100.0001, MTU 1500
IP address 169.254.1.1, subnet mask 255.255.255.248
37 packets input, 2822 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 pause input, 0 resume input
0 L2 decode drops
5 packets output, 370 bytes, 0 underruns
0 pause output, 0 resume output
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
input queue (blocks free curr/low): hardware (0/0)
output queue (blocks free curr/low): hardware (0/0)
Traffic Statistics for "nlp_int_tap":
37 packets input, 2304 bytes
5 packets output, 300 bytes
37 packets dropped
    1 minute input rate 0 pkts/sec,  0 bytes/sec
    1 minute output rate 0 pkts/sec,  0 bytes/sec
    1 minute drop rate, 0 pkts/sec
    5 minute input rate 0 pkts/sec,  0 bytes/sec
    5 minute output rate 0 pkts/sec,  0 bytes/sec
    5 minute drop rate, 0 pkts/sec
Control Point Interface States:
Interface number is 14
Interface config status is active
Interface state is active

```

检查路由和 NAT

在威胁防御 CLI 中，检查是否已添加默认路由 (S *)，以及管理接口 (nlp_int_tap) 是否存在内部 NAT 规则。

show route

```

> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*      0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C       10.89.5.0 255.255.255.192 is directly connected, outside
L       10.89.5.29 255.255.255.255 is directly connected, outside

>

```

show nat

```

> show nat

```

```

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface service
  tcp 8305 8305
  translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface service
  tcp ssh ssh
  translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
  ipv6 service tcp 8305 8305
  translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
  translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
  translate_hits = 0, untranslate_hits = 0
>

```

检查其他设置

请参阅以下命令以检查是否存在所有其他设置。您还可以在 CDO 的 **设备 (Devices) > 设备管理 (Device Management) > 设备 (Device) > 管理 (Management) > 管理器访问 - 配置详细信息 (Manager Access - Configuration Details) > CLI 输出 (CLI Output)** 页面上看到许多这些命令。

show running-config sftunnel

```

> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305

```

show running-config ip-client

```

> show running-config ip-client
ip-client outside

```

show conn address fmc_ip

```

> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
  preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap 10.89.5.29(169.254.1.2):51231 outside 10.89.5.35:8305, idle 0:00:04,
  bytes 86684, flags UxIO
TCP nlp_int_tap 10.89.5.29(169.254.1.2):8305 outside 10.89.5.35:52019, idle 0:00:02,
  bytes 1630834, flags UIO
>

```

检查 DDNS 更新是否成功

在威胁防御 CLI 中，检查 DDNS 更新是否成功：

debug ddns

```

> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfully updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
DDNS: IDB SB total = 0

```

如果更新失败，请使用 **debug http** 和 **debug ssl** 命令。对于证书验证失败，请检查是否已在设备上安装根证书：


```
show crypto ca certificates trustpoint_name
```

要检查 DDNS 操作，请执行以下操作：

```
show ddns update interface fmc_访问_ifc_name
```

```
> show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name Update Destination
  RBD_DDNS not available

Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

检查 CDO 日志文件

请参阅 <https://cisco.com/go/fmc-reg-error>。

如果 CDO 断开连接则回滚配置

如果将威胁防御上的数据接口用于管理器访问，并从 CDO 部署影响网络连接的配置更改，则可以将威胁防御上的配置回滚到上次部署的配置，以便恢复管理连接。然后，您可以调整 CDO 中的配置设置，以便保持网络连接并重新部署。即使没有丢失连接，也可以使用回滚功能；它不仅限于此故障排除情况。

请参阅以下准则：

- 只有以前的部署可以在威胁防御上本地提供；您无法回滚到任何较早的部署。
- 回滚只会影响您可以在 CDO 中设置的配置。例如，回滚不会影响与专用管理接口相关的任何本地配置，您只能在威胁防御 CLI 中进行配置。请注意，如果您在上次 CDO 部署后使用 **configure network management-data-interface** 命令更改了数据接口设置，然后使用了回滚命令，则这些设置将不会保留；它们将回滚到上次部署的 CDO 设置。
- 无法回滚上一次部署期间更新的带外 SCEP 证书数据。
- 在回滚期间，连接将被丢弃，因为当前配置将被清除。

过程

步骤 1 在威胁防御 CLI 中，回滚到之前的配置。

```
configure policy rollback
```

回滚后，威胁防御会通知 CDO 已成功完成回滚。在 CDO 中，部署屏幕将显示一条横幅，说明配置已回滚。

注释 如果回滚失败且 CDO 管理已恢复，请参阅<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html>以了解常见的部署问题。在某些情况下，恢复 CDO 管理访问权限后回滚可能会失败；在这种情况下，您可以解决 CDO 配置问题，并从 CDO 重新部署。

示例:

对于使用数据接口进行管理器访问的 威胁防御:

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2022 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
.....
.....
>
```

步骤 2 检查管理连接是否已重新建立。

在 CDO 中，在设备 (**Devices**) > 设备管理 (**Device Management**) > 设备 (**Device**) > 管理 (**Management**) > 管理器访问 - 配置详细信息 (**Manager Access - Configuration Details**) > 连接状态 (**Connection Status**) 页面上检查管理连接状态。

在 威胁防御 CLI，输入 **sftunnel-status-brief** 命令以查看管理连接状态。

如果重新建立连接需要 10 分钟以上，则应排除连接故障。请参阅[排除数据接口上的管理连接故障，第 154 页](#)。

使用 CDO 关闭防火墙

正确关闭系统非常重要。仅拔掉电源或按下电源开关可能会导致文件系统严重损坏。请记住，有许多进程一直在后台运行，拔掉或关闭电源不能正常关闭防火墙。

您可以使用 CDO 正确关闭系统。

过程

步骤 1 选择设备 > 设备管理。

步骤 2 在要重新启动的设备旁边，点击编辑图标 (✎)。

步骤 3 点击设备 (**Device**) 选项卡。

步骤 4 点击系统 (**System**) 部分中的关闭设备图标 (🔴)。

步骤 5 出现提示时，确认是否要关闭设备。

步骤 6 如果您与防火墙建立了控制台连接，请在防火墙关闭时留意系统提示。您将看到以下提示：

```
System is stopped.  
It is safe to power off now.  
Do you want to reboot instead? [y/N]
```

如果没有控制台连接，请等待大约 3 分钟以确保系统已关闭。

步骤 7 您现在可以关闭电源开关并在必要时拔下电源插头以物理方式断开机箱的电源。

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？

要查看所有可用的操作系统和管理器，请参阅[哪种操作系统和管理器适合您？](#)，第 1 页。本章适用于使用 ASDM 的 ASA。

本章不涉及以下部署，请参考《[ASA 配置指南](#)》了解相关内容：

- 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。

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 ASA](#)，第 164 页
- [端到端程序](#)，第 165 页
- [查看网络部署和默认配置](#)，第 167 页
- [连接防火墙的电缆](#)，第 169 页
- [打开防火墙电源](#)，第 170 页
- [（可选）更改 IP 地址](#)，第 171 页
- [登录 ASDM](#)，第 172 页
- [配置许可](#)，第 173 页
- [配置 ASA](#)，第 178 页
- [访问 ASA 和 FXOS CLI](#)，第 180 页

- 后续步骤，第 181 页

关于 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（本指南中已介绍）- 设备中包含的单个设备管理器。
- CLI
- CDOF - 一个简化的、基于云的多设备管理器。
- 思科安全管理器 - 位于单独的服务器上的多设备管理器。

迁移 ASA 5500-X 配置

您可以将 ASA 5500-X 配置复制并粘贴到 Cisco Secure Firewall 3100 中。但是，您需要修改配置。另请注意平台之间的一些行为差异。

1. 要复制配置，请在 ASA 5500-X 上输入 **more system:running-config** 命令。
2. 根据需要编辑配置（请参阅下文）。
3. 连接至 Cisco Secure Firewall 3100 的控制台端口，然后进入全局配置模式：

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: *****
Repeat Password: *****
ciscoasa# configure terminal
ciscoasa(config)#
```

4. 使用 **clear configure all** 命令清除当前配置。
5. 在 ASA CLI 上粘贴已修改的配置。

本指南假设采用出厂默认配置，因此，如果在现有配置下粘贴，则本指南中的某些程序将不适用于您的 ASA。

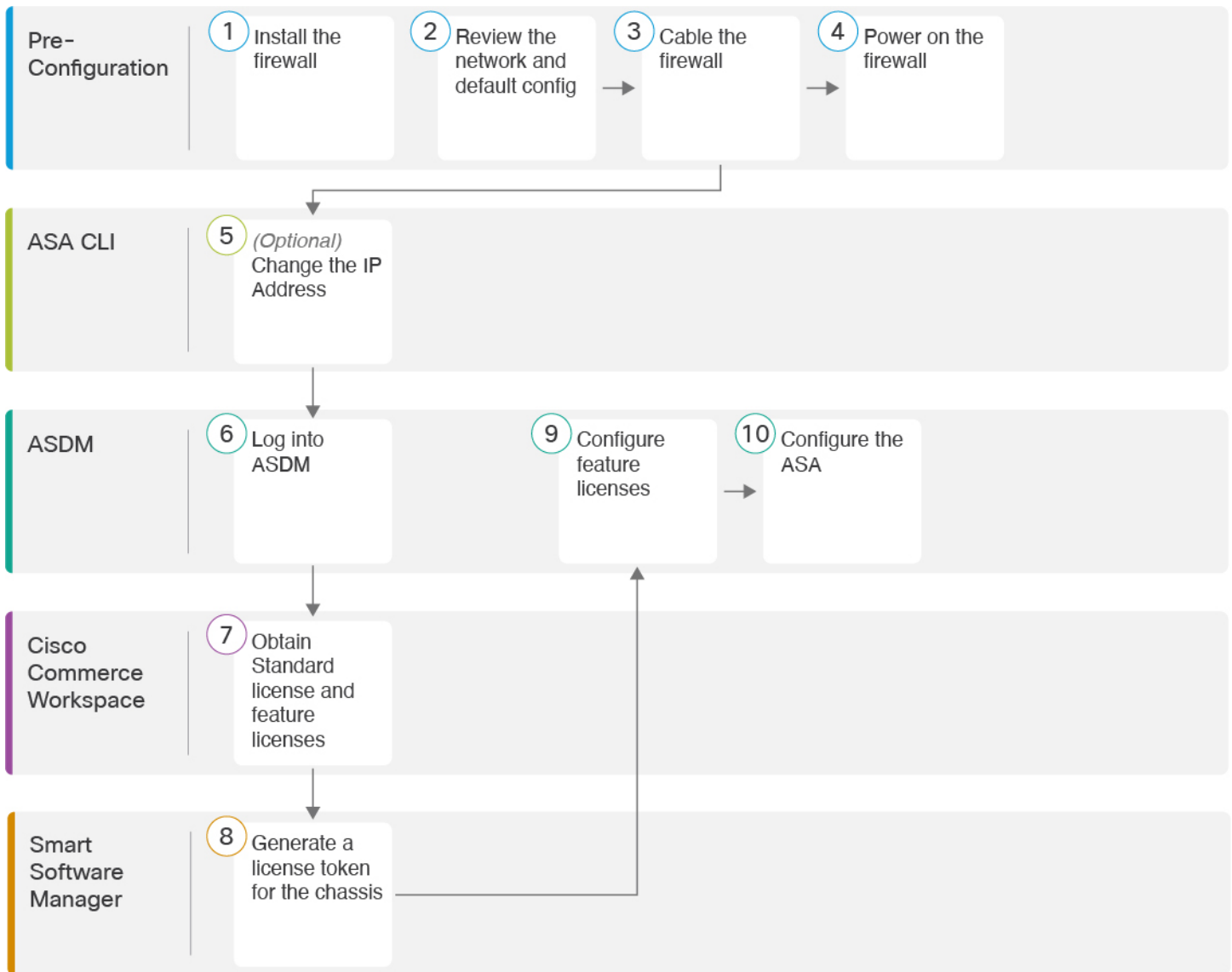
ASA 5500-X 配置	Cisco Secure Firewall 3100 配置
PAK 许可证	智能许可证 复制和粘贴配置时，不会应用 PAK 许可。默认情况下没有已安装的许可证。智能许可要求连接到智能许可服务器以获取许可证。智能许可还会影响 ASDM 或 SSH 访问（请参阅下文）。

ASA 5500-X 配置	Cisco Secure Firewall 3100 配置
初始 ASDM 访问	<p>如果无法连接 ASDM 或向智能许可服务器注册，请删除任何 VPN 或其他强加密功能配置（即使仅配置了弱加密）。您可以在获取强加密 (3DES) 许可证后重新启用这些功能。</p> <p>此问题的原因是，ASA 默认情况下仅包含用于管理访问的 3DES 功能。如果启用强加密功能，则系统会阻止 ASDM 和 HTTPS 流量（例如，与智能许可服务器之间的流量）。此规则的例外是您连接到仅限管理的接口，例如管理 1/1。SSH 不受影响。</p>
接口 ID	<p>确保更改接口 ID 以便与新硬件 ID 匹配。例如，ASA 5525-X 包括管理 0/0 和千兆以太网 0/0 至 0/5。Firepower 1120 包括管理 1/1 和以太网 1/1 至 1/8。</p>
<p>boot system commands</p> <p>ASA 5500-X 最多允许四个 boot system 命令指定要使用的启动映像。</p>	<p>Cisco Secure Firewall 3100 仅允许一个 boot system 命令，因此在粘贴之前应删除多余的命令，只剩下一个命令。实际上在配置中不需要存在任何 boot system 命令，因为启动时不会读取它来确定启动映像。最后加载的启动图像将始终在重新加载时运行。</p> <p>此 boot system 命令会在您输入时执行操作：系统验证并解压缩映像，并将其复制到引导位置（FXOS 管理的 disk0 上的内部位置）。重新加载 ASA 时，系统将加载新图像。</p>

端到端程序

请参阅以下任务以在机箱上部署和配置 ASA。

图 60: 端到端程序



①	配置前准备工作	安装防火墙。请参阅 硬件安装指南 。
②	配置前准备工作	查看网络部署和默认配置 ，第 167 页。
③	配置前准备工作	连接防火墙的电缆 ，第 169 页。
④	配置前准备工作	打开防火墙电源 ，第 170 页。
⑤	ASA CLI	(可选) 更改 IP 地址 ，第 171 页。

6	ASDM	登录 ASDM，第 172 页。
7	Cisco Commerce Workspace	获取标准许可证和可选功能许可证 (配置许可，第 173 页)。
8	智能软件管理器	为机箱生成许可证令牌 (配置许可，第 173 页)。
9	ASDM	配置功能许可证 (配置许可，第 173 页)。
10	ASDM	配置 ASA，第 178 页。

查看网络部署和默认配置

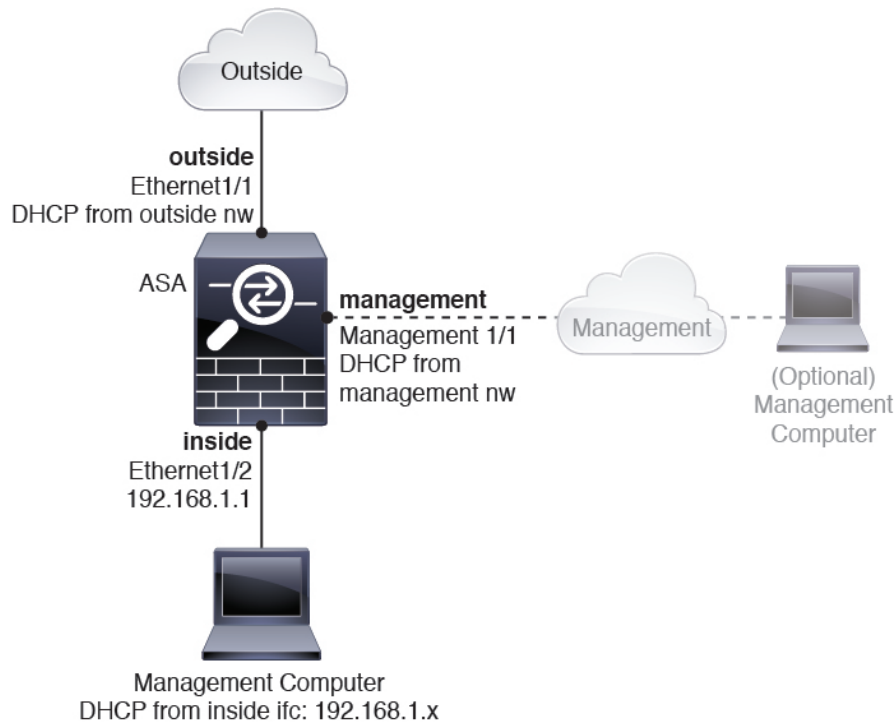
下图显示了在使用默认配置的 ASA 的默认网络部署。

如果您将外部接口直接连接到电缆调制解调器或 DSL 调制解调器，我们建议您将调制解调器置于桥接模式，以便 ASA 为您的内部网络执行所有路由和 NAT。如果您需要为外部接口配置 PPPoE 以连接到您的 ISP，可以在 ASDM 启动向导中执行此操作。



注释 如果不能使用默认内部 IP 地址进行 ASDM 访问，可以在 ASA CLI 上设置内部 IP 地址。请参阅 [\(可选\) 更改 IP 地址，第 171 页](#)。例如，在以下情况下，您可能需要更改内部 IP 地址：

- 如果外部接口尝试获取 192.168.1.0 网络（这是一个通用默认网络）上的 IP 地址，DHCP 租用将失败，外部接口不会获得 IP 地址。出现此问题的原因在于 ASA 在同一网络上不能有两个接口。在这种情况下，您必须将内部 IP 地址更改到新网络上。
- 如果将 ASA 添加到现有内部网络中，需要将内部 IP 地址更改到现有网络上。



Secure Firewall 3100 默认配置

Secure Firewall 3100 的默认出厂配置用于配置以下内容：

- 内部→外部流量 - 以太网 1/1（外部），以太网 1/2（内部）
- 外部 IP 地址来自 DHCP，内部 IP 地址—192.168.1.1
- 管理—管理 1/1（管理），IP 地址来自 DHCP
- DHCP 服务器在内部接口上
- 默认路由 来自外部 DHCP，管理 DHCP
- ASDM 访问 - 允许管理和内部主机。内部主机限制为 192.168.1.0/24 网络。
- NAT - 从内部到外部所有流量的接口 PAT。
- DNS 服务器 - OpenDNS 服务器已预配置。

配置由以下命令组成：

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
!
```

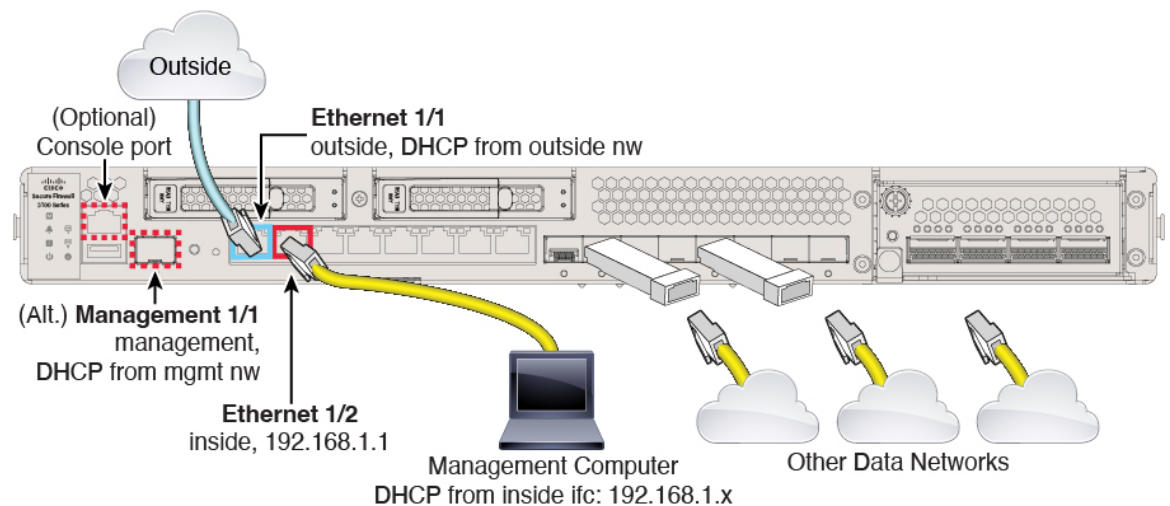
```

interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
  name-server 208.67.222.222 outside
  name-server 208.67.220.220 outside
!

```

连接防火墙的电缆

图 61: *Secure Firewall 3100* 的布线



在管理 1/1 或以太网 1/2 上管理 Secure Firewall 3100。默认配置还会将以太网 1/1 配置为外部接口。

过程

步骤 1 安装机箱。请参阅[硬件安装指南](#)。

步骤 2 将您的管理计算机连接至以下任一接口：

- 管理 1/1 - 将管理 1/1 接口连接到管理网络，并确保管理计算机位于管理网络上，或者可以访问管理网络。管理 1/1 是需要 SFP 模块的光纤接口。管理 1/1 接口从管理网络上的 DHCP 服务器获取 IP 地址；如果使用此接口，则必须确定分配给 ASA 的 IP 地址，以便可以从管理计算机连接到 IP 地址。
- 以太网 1/2 - 将管理计算机直接连接至以太网 1/2 以进行初始配置。或者将以太网 1/2 连接到内部网络；请确保管理计算机位于内部网络上，因为只有该网络上的客户端才能访问 ASA。以太网 1/2 具有默认 IP 地址 (192.168.1.1)，并且还会运行 DHCP 服务器以向客户端（包括管理计算机）提供 IP 地址，因此，请确保这些设置不会与任何现有内部网络设置冲突（请参阅[Secure Firewall 3100 默认配置](#)，第 168 页）。

如果需要将以太网 1/2 IP 地址从默认值更改为其他值，还必须将管理计算机连接至控制台端口。请参阅[（可选）更改 IP 地址](#)，第 171 页。

可以稍后从其他接口配置 ASA 管理访问；请参阅[ASA 常规操作配置指南](#)。

步骤 3 将外部网络连接到以太网 1/1 接口。

对于智能软件许可，ASA 需要互联网接入，以便它可以访问许可证颁发机构。

步骤 4 将其他网络连接到其余接口。

打开防火墙电源

系统电源由位于防火墙后部的摇杆电源开关控制。电源开关以软通知开关形式实施，支持平稳地关闭系统以降低系统软件及数据损坏的风险。

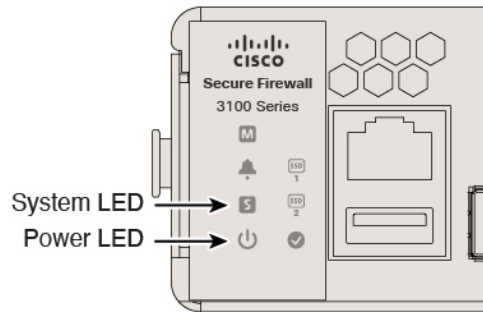
过程

步骤 1 将电源线一端连接到防火墙，另一端连接到电源插座。

步骤 2 使用位于机箱背面电源线旁边的标准摇杆型电源开关打开电源。

步骤 3 检查防火墙背面的电源 LED；如果该 LED 呈绿色稳定亮起，表示防火墙已接通电源。

图 62: 系统和电源 LED



步骤 4 检查防火墙背面的系统 LED；其呈绿色稳定亮起之后，系统已通过通电诊断。

注释 将开关从开切换到关时，系统可能需要几秒钟才会最终关闭。在此期间，机箱前面的电源 LED 将闪烁绿色。在电源 LED 完全关闭之前，请勿拔出电源。

(可选) 更改 IP 地址

如果不能使用默认 IP 地址进行 ASDM 访问，可以在 ASA CLI 上设置 inside 接口的 IP 地址。



注释 此程序恢复默认配置并设置您选择的 IP 地址，所以如果有任何要保留的 ASA 配置更改，请不要使用此程序。

过程

步骤 1 连接到 ASA 控制台端口，然后进入全局配置模式。有关详细信息，请参阅[访问 ASA 和 FXOS CLI](#)，第 180 页。

步骤 2 恢复默认配置和您选择的 IP 地址。

```
configure factory-default [ip_address [mask]]
```

示例:

```
ciscoasa(config)# configure factory-default 10.1.1.151 255.255.255.0
Based on the management IP address and mask, the DHCP address
pool size is reduced to 103 from the platform limit 256
```

```
WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.
```

```

Begin to apply factory-default configuration:
Clear all configuration
Executing command: interface ethernet1/2
Executing command: nameif inside
INFO: Security level for "inside" set to 100 by default.
Executing command: ip address 10.1.1.151 255.255.255.0
Executing command: security-level 100
Executing command: no shutdown
Executing command: exit
Executing command: http server enable
Executing command: http 10.1.1.0 255.255.255.0 management
Executing command: dhcpd address 10.1.1.152-10.1.1.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#

```

步骤 3 将默认配置保存到闪存。

write memory

登录 ASDM

启动 ASDM 以便配置 ASA。

ASA 默认情况下包含 3DES 功能，仅用于管理访问，因此您可以连接到智能软件管理器，还可以立即使用 ASDM。如果之后在 ASA 上配置了 SSH 访问，也可以使用 SSH 和 SCP。其他需要强加密（例如 VPN）的功能必须启用强加密，这要求您先向智能软件管理器注册。



注释 如果您在注册之前尝试配置任何可使用强加密的功能（即使您仅配置了弱加密），您的 HTTPS 连接会在该接口上断开，并且您无法重新连接。此规则的例外是您连接到仅限管理的接口，例如管理 1/1。SSH 不受影响。如果您丢失了 HTTPS 连接，可以连接到控制台端口以重新配置 ASA、连接到仅管理接口，或者连接到没有为强加密功能配置的接口。

开始之前

- 请参阅 Cisco.com 上的 [ASDM 发行说明](#) 了解运行 ASDM 的要求。

过程

步骤 1 在浏览器中输入以下 URL。

- **https://192.168.1.1**- 内部接口 IP 地址。
- **https://management_ip** - 从 DHCP 分配的管理接口 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 单击以下可用选项之一：**安装 ASDM 启动器 (Install ASDM Launcher)** 或 **运行 ASDM (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 时设置的启用密码，然后单击**确定 (OK)**。

系统将显示 ASDM 主窗口。

配置许可

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

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

ASA 默认情况下包含 3DES 功能，仅用于管理访问，因此您可以连接到智能软件管理器，还可以立即使用 ASDM。如果之后在 ASA 上配置了 SSH 访问，也可以使用 SSH 和 SCP。其他需要强加密（例如 VPN）的功能必须启用强加密，这要求您先向智能软件管理器注册。



注释 如果您在注册之前尝试配置任何可使用强加密的功能（即使您仅配置了弱加密），您的 HTTPS 连接会在该接口上断开，并且您无法重新连接。此规则的例外是您连接到仅限管理的接口，例如管理 1/1。SSH 不受影响。如果您丢失了 HTTPS 连接，可以连接到控制台端口以重新配置 ASA、连接到仅管理接口，或者连接到没有为强加密功能配置的接口。

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 functionality 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。

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。

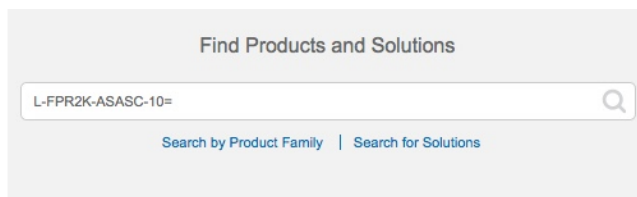
- 您的智能软件管理器帐户必须符合强加密 (3DES/AES) 许可证的要求，才能使用某些功能（已使用导出合规性标志启用）。

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 63: 许可证搜索



- 基础许可证 — L-FPR3110-BSE=。基础许可证是必需的许可证。
- 基础许可证 — L-FPR3120-BSE=。基础许可证是必需的许可证。
- 基础许可证 — L-FPR3130-BSE=。基础许可证是必需的许可证。
- 基础许可证 — L-FPR3140-BSE=。基础许可证是必需的许可证。
- 5 情景许可证 - L-FPR3K-ASASC-5=。情景许可证是附加的；请购买多份许可证以满足您的需要。
- 10 情景许可证 - L-FPR3K-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。
- 运营商 (Diameter, GTP/GPRS, M3UA, SCTP) — L-FPR3K-ASA-CAR=
- 强加密 (3DES/AES) 许可证 - L-FPR3K-ENC-K9=。仅当帐户未获授权使用强加密时需要。

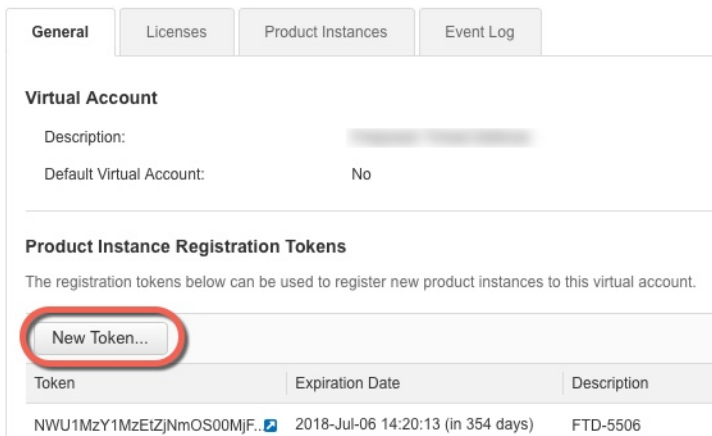
- Cisco Secure 客户端 - 请参阅[思科安全客户端订购指南](#)。您不能直接在 ASA 中启用此许可证。

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。

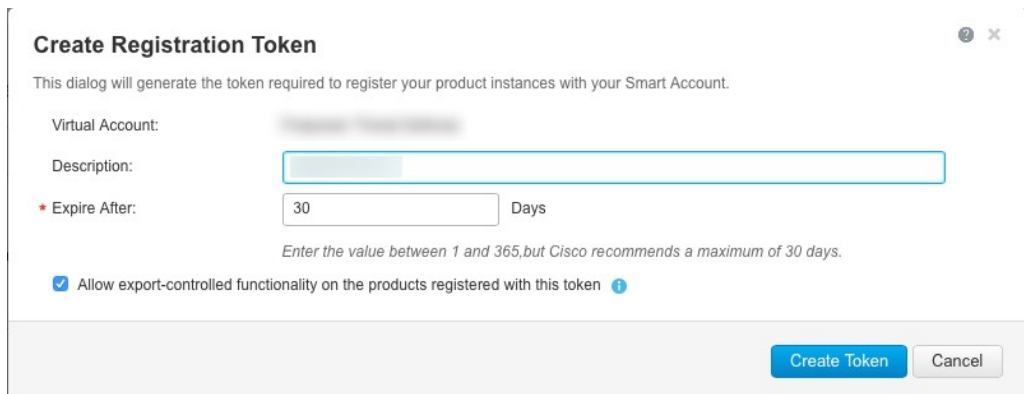
a) 点击 **Inventory**。



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 functionality 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 64: 查看令牌

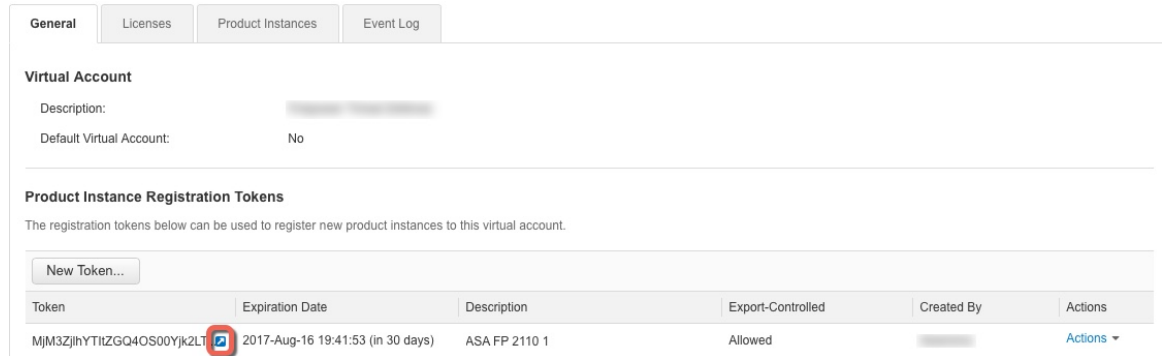
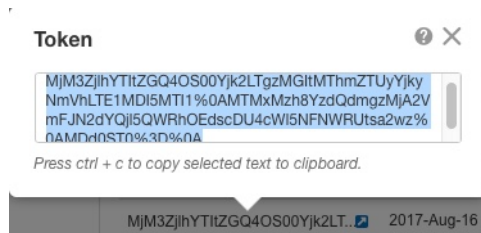


图 65: 复制令牌



步骤 3 在 ASDM 中，依次选择 **Configuration > Device Management > Licensing > Smart Licensing**。

步骤 4 点击 **Register**。

Configuration > Device Management > Licensing > Smart Licensing

To configure an HTTP proxy for smart licensing, see the [Smart Call-Home](#) page. Note that Smart Call Home is automatically enabled and is required for smart licensing.

Enable Smart license configuration

Feature Tier:

Throughput Level:

Privacy Host Name Version

Transport Call Home Smart Transport

Configure Transport URL

Default URL

Registration

Utility

Proxy URL

Proxy Port

Configure Utility Mode

Enable Standard Utility Mode

Custom ID

Customer Company Identifier

Customer Company Name

Customer Street

Customer City

Customer State

Customer Country

Customer Postal Code

Registration Status: UNREGISTERED

Effective Running Licenses

License Feature	License Value
Maximum VLANs	200
Inside Hosts	Unlimited
Failover	Active/Active
Encryption-DES	Enabled
Encryption-3DES-AES	Enabled
Security Contexts	2
Carrier	Disabled

步骤 5 在 ID Token 字段中输入注册令牌。

Smart License Registration

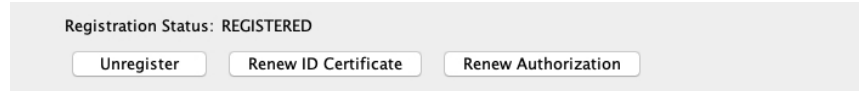
ID Token:

Force registration

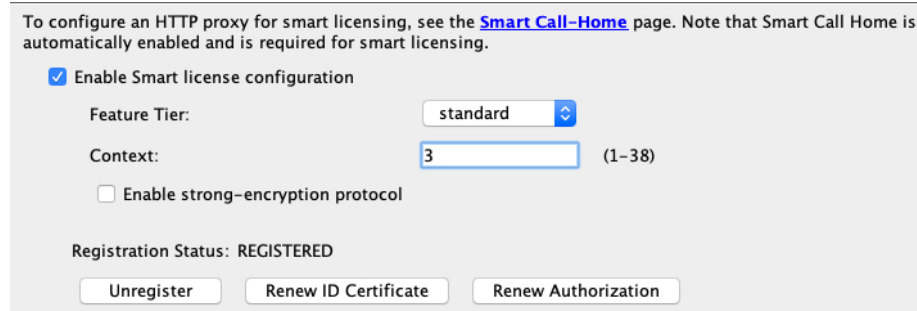
您可以勾选强制注册 (**Force registration**) 复选框，注册已注册但可能与智能软件管理器不同步的 ASA。例如，如果从智能软件管理器中意外删除了 ASA，请使用强制注册 (**Force registration**)。

步骤 6 点击 **Register**。

ASA 使用预先配置的外部接口向智能软件管理器注册，并请求对已配置的许可证授权进行授权。如果您的帐户允许，则智能软件管理器还会应用强加密(3DES/AES)许可证。当许可状态更新时，ASDM 会刷新页面。您还可以选择**监控 (Monitoring) > 属性 (Properties) > 智能许可证 (Smart License)**以检查许可证状态，尤其是注册失败时。



步骤 7 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 2 种情景。情景的最大数目取决于您的型号：

- Cisco Secure Firewall 3100 — 100 个情景

例如，对于 Cisco Secure Firewall 3110 而言，要使用最大值 - 25 种情景，请为情景数输入 23；此值将与默认值 2 相加。

步骤 8 点击 **Apply**。

步骤 9 点击工具栏中的 **Save** 图标。

步骤 10 退出并重新启动 ASDM。

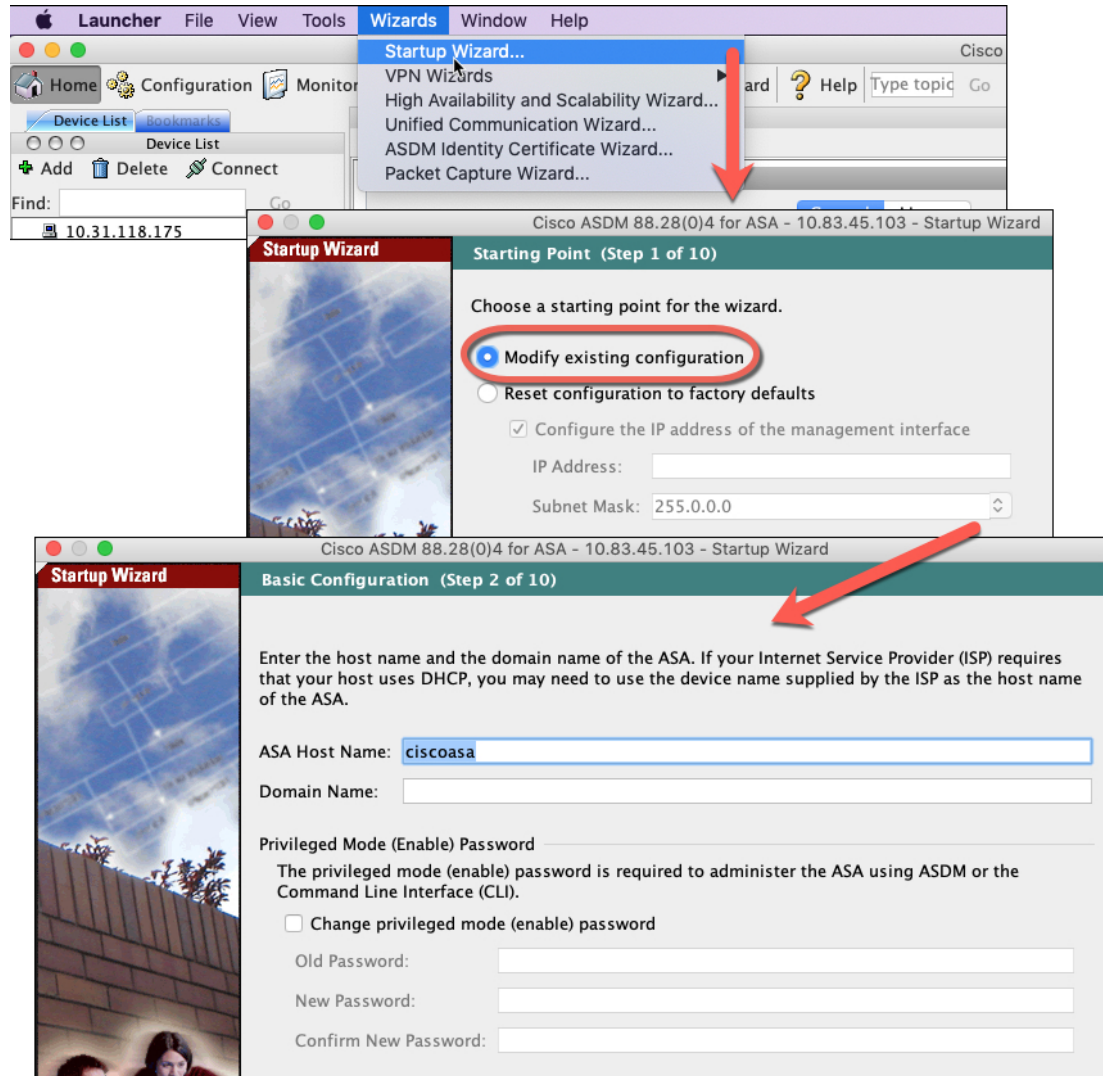
当您更改许可证时，您需要重新启动 ASDM 才能显示更新屏幕。

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和FXOS CLI

您可以使用 ASA CLI（而非 ASDM）对 ASA 进行故障排除或配置。可以连接到控制台端口以访问 CLI。您可以稍后在任何接口上配置对 ASA 的 SSH 访问；在默认情况下，SSH 访问是禁用的。有关更多信息，请参阅[ASA 一般操作配置指南](#)。

也可以从ASA CLI 访问FXOS CLI，以便进行故障排除。

过程

步骤 1 将管理计算机连接到控制台端口。Secure Firewall 3100 配有一条 DB-9 转 RJ-45 串行电缆，所以您需要第三方串行转 USB 电缆进行连接。确保为您的操作系统安装必要的 USB 串行驱动程序Secure Firewall 3100 [硬件指南](#)。使用以下串行设置：

- 9600 波特率
- 8 个数据位
- 无奇偶校验
- 1 个停止位

连接到 ASA CLI。默认情况下，访问控制台时不需要提供用户凭证。

步骤 2 访问特权 EXEC 模式。

enable

第一次输入 **enable** 命令时，系统会提示您更改密码。

示例：

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: *****
Repeat Password: *****
ciscoasa#
```

如果 ASA 无法启动，并且您进入 FXOS 故障保护模式，则您在 ASA 上设置的启用密码也是 FXOS 管理员用户密码。

在特权 EXEC 模式中，所有非配置命令均可用。还可从特权 EXEC 模式进入配置模式。

要退出特权 EXEC 模式，请输入 **disable**、**exit** 或 **quit** 命令。

步骤 3 访问全局配置模式。

configure terminal

示例:

```
ciscoasa# configure terminal
ciscoasa(config)#
```

可从全局配置模式开始配置 ASA。要退出全局配置模式，请输入 **exit**、**quit** 或 **end** 命令。

步骤 4（可选）连接到 FXOS CLI。

connect fxos [admin]

- **admin**- 提供管理员级的访问权限。如果不选择此选项，用户将拥有只读访问权限。请注意，即使在管理员模式下，也没有任何配置命令可用。

系统不会提示您提供用户凭证。当前的 ASA 用户名将传递给 FXOS，无需其他登录。要返回到 ASA CLI，请输入 **exit** 或键入 **Ctrl-Shift-6、x**。

在 FXOS 中，您可以使用 **scope security/show audit-logs** 命令查看用户活动。

示例:

```
ciscoasa# connect fxos admin
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
firepower#
firepower# exit
Connection with FXOS terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

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。
- 有关故障排除，请参阅《[FXOS 故障排除指南](#)》。

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。