使用 CDO 部署威胁防御

本章对您适用吗？

要查看所有可用的操作系统和管理器，请参阅哪种应用和管理器适合您？。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。

• 后续操作，第 28 页

关于通过 CDO 管理威胁防御

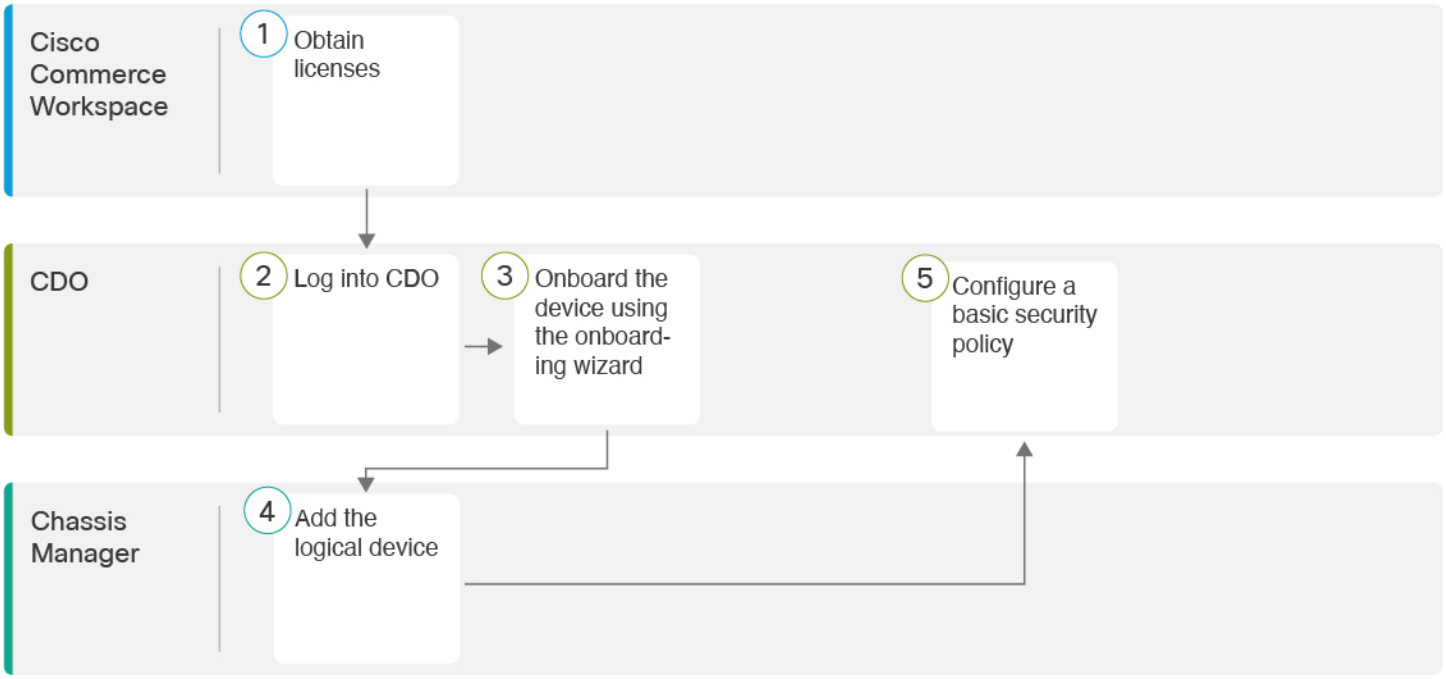
云交付的 管理中心 管理中心 提供许多与本地部署 管理中心 相同的功能，并且具有相同的外观。在将 CDO 用作主管理器时，您只能使用本地部署 管理中心 进行分析。本地部署 管理中心 不支持策略配置或升级。

注释 CDO 不支持容器实例或集群。

端到端程序

请参阅以下任务，使用激活向导在 CDO 中激活 威胁防御。

图 *1:* 端到端程序



1	Cisco Commerce Workspace	获取许可证，第 3 页。
2	CDO	登录 CDO，第 5 页。
3	CDO	使用激活向导激活设备，第 9 页。

4	机箱 管理器	机箱管理器：添加威胁防御逻辑设备，第 10 页。
5	CDO	配置基本安全策略。

获取许可证

所有许可证都由 CDO 提供给 威胁防御。您可以选择购买以下功能许可证：

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

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

开始之前

- 拥有 智能软件管理器主帐户。

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

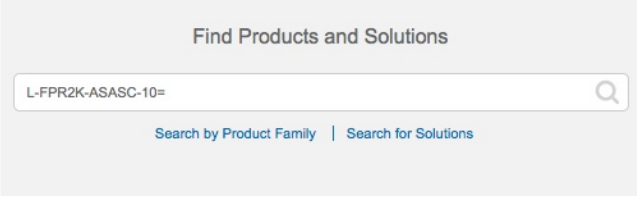
- 您的智能软件许可帐户必须符合强加密 (3DES/AES) 许可证的要求，才能使用某些功能（已使用导出合规性标志启用）。

过程

步骤 1 请确保智能许可帐户包含所需的可用许可证。

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

图 *2:* 许可证搜索



注释　　如果未找到 PID，您可以手动将 PID 添加到订单中。

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

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

步骤 2 如果尚未注册，请向智能软件管理器注册 CDO。

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

登录 CDO

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

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

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

- 如果您有 Cisco Secure Sign-On 帐户，请提前跳转至 使用 Cisco Secure Sign-On 登录 CDO，第 7 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 5 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

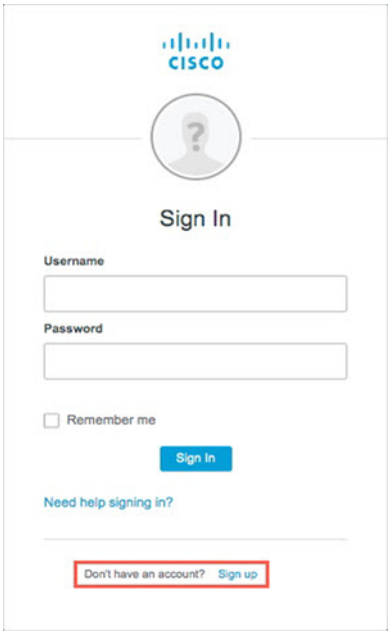
- **安装 DUO Security** - 我们建议您在手机上安装 Duo Security 应用。如果您对于如何安装 Duo 有疑问，请查看 Duo 双因素身份验证指南：注册指南。
- **时间同步** — 您要使用移动设备生成一次性密码。由于 OTP 是基于时间的，所以您的设备时钟与实时同步是非常重要的。请确保您的设备时钟设置为正确的时间。
- 使用当前版本的 Firefox 或 Chrome。

过程

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

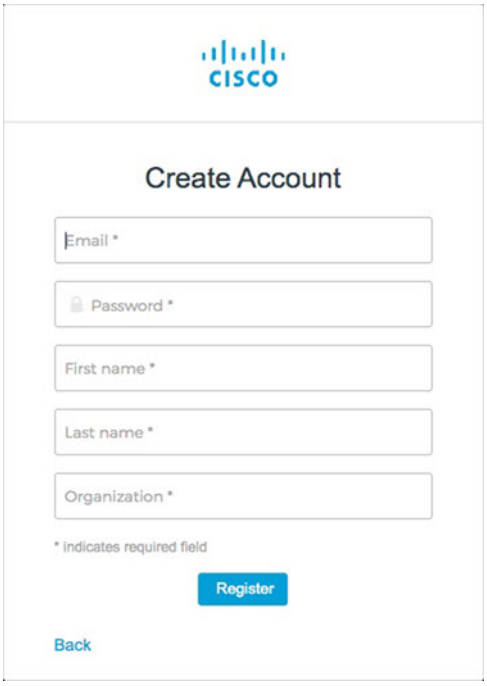
a) 浏览到 https://sign-on.security.cisco.com。
b) 在“登录”屏幕的底部，点击**注册**。

图 *3: 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 *4:* 创建帐户



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

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

步骤 2 使用 **Duo** 设置多因素身份验证。

a) 在**设置多因素身份验证**屏幕中，点击**配置**。

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

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

c) 在向导结束时，点击**继续登录**。

d) 通过双因素身份验证登录 Cisco Secure Sign-On。

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

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

b) 按照安装向导中的提示设置 Google Authenticator。

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

a) 选择一个“忘记密码”问答。

b) 选择恢复电话号码以使用 SMS 重置帐户。

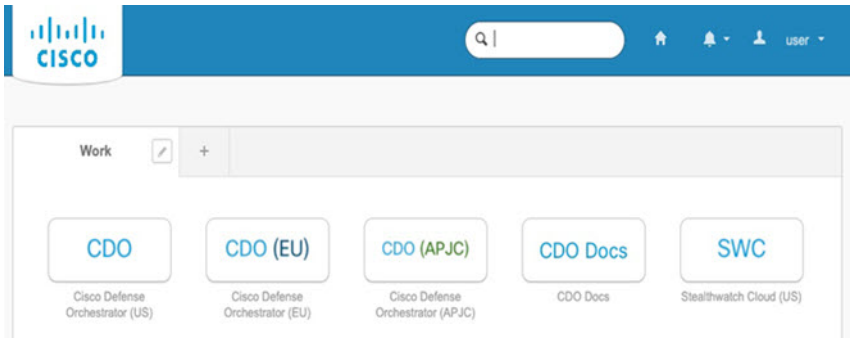
c) 选择安全图像。

d) 点击**创建帐户**。

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

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

图 *5: 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 5 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/。

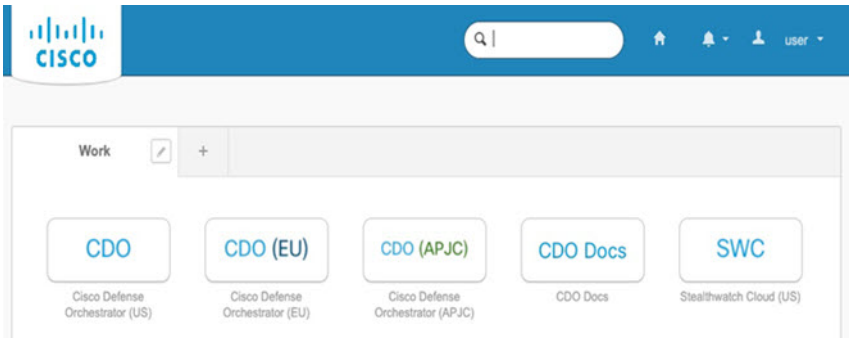
步骤 2 输入您的**用户名**和**密码**。

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 *6: Cisco SSO* 控制板



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

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

使用激活向导激活设备

通过 CDO 的激活向导使用 CLI 注册键激活威胁防御。

过程

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

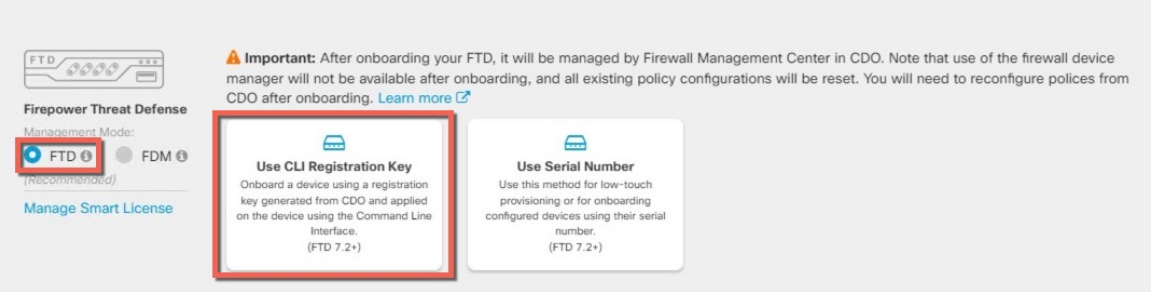
步骤 2 选择 **FTD** 磁贴。

步骤 3 在 **管理模式**下，确保选择 **FTD** 。

选择 **FTD** 作为管理模式后，您可以随时点击 **管理智能许可证** 注册或修改设备可用的现有智能许可证。请参阅获取许可证，第 3 页以查看可用的许可证。

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

图 7: 使用 *CLI* 注册密钥



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

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

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

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

configure manager add *cdo_hostname registration_key nat_id display_name*

在 机箱管理器 中，在部署逻辑设备时（请参阅机箱管理器：添加威胁防御逻辑设备，第 10 页），将命令的这一复制到**CDO 激活 (CDO Onboard)** 和**确认 CDO 激活 (Confirm CDO Onboard)** 字段中。

示例：

命令示例：

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

步骤 9 在激活向导中点击**下一步 (Next)**，以便开始注册设备。

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

下一步做什么

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

机箱管理器：添加威胁防御逻辑设备

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

您可以通过此程序配置逻辑设备特性，包括应用程序使用的引导程序配置。

开始之前

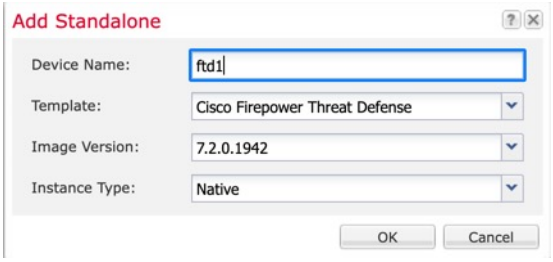
- 配置与 威胁防御一起使用的管理接口；请参阅配置接口。管理接口是必需的。您可以稍后从数据接口启用管理；但必须将管理接口分配给逻辑设备，即使您不打算在启用数据管理后使用该接口。请注意，此管理接口与仅用于机箱管理的机箱管理端口（并且该端口在**接口**选项卡的顶部显示为 **MGMT**）不同。
- 您还必须至少配置一个数据接口。
- 收集以下信息：
  - 此设备的接口 ID
  - 管理接口 IP 地址和网络掩码
  - 网关 IP 地址
  - CDO 生成的 CDO 主机名、注册密钥和 NAT ID。请参阅 使用激活向导激活设备，第 9 页。
  - DNS 服务器 IP 地址

过程

步骤 1 在 机箱管理器中，选择**逻辑设备**。

步骤 2 点击**添加** > **独立设备**，并设置以下参数：

图 *8:* 添加独立设备



a) 提供**设备名称**。

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

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

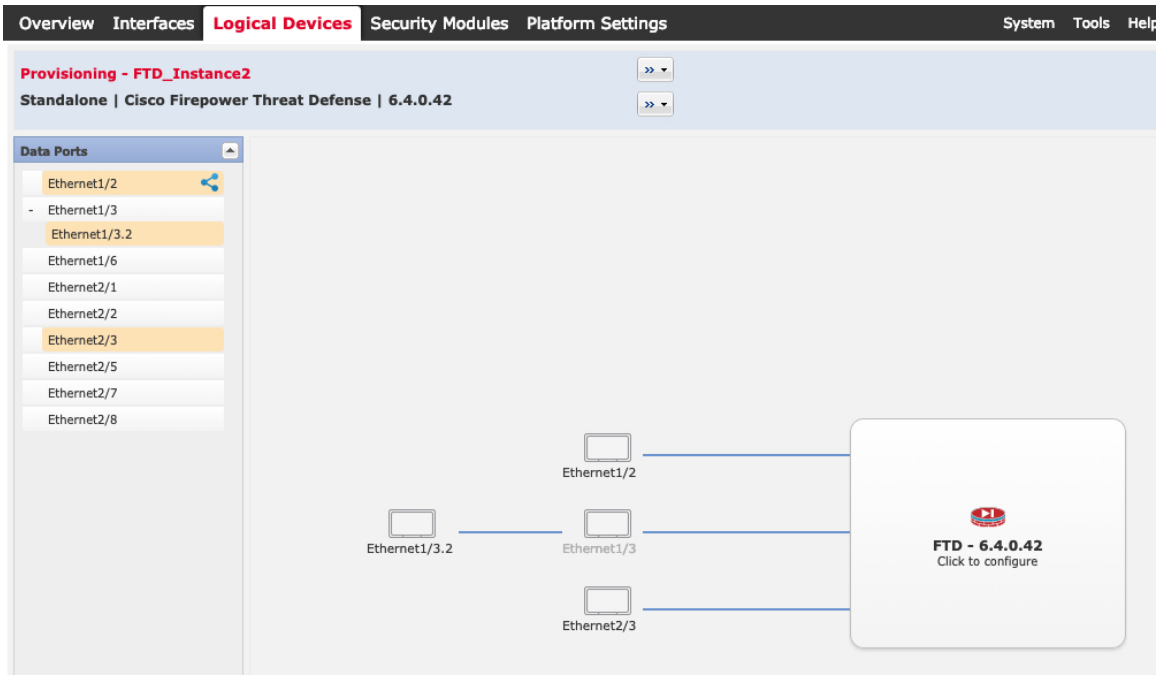
c) 选择**映像版本**。

d) 选择**实例类型：本地**。

e) 点击**确定 (OK)**。

屏幕会显示调配 - 设备名称窗口。

步骤 3 展开**数据端口**区域，然后点击要分配给设备的每个接口。



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

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

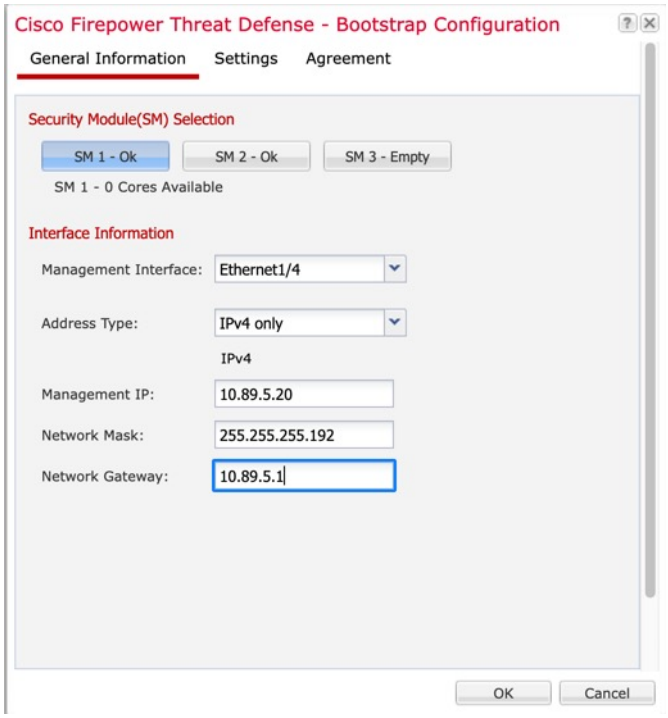
告消息，确认您是故意这样分配。您不需要使用硬件旁路功能，因此如果您愿意，可以分配单个接口。

步骤 4 点击屏幕中心的设备图标。

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

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

图 *9:* 常规信息



a) 选择**管理接口**。

此接口用于管理逻辑设备。此接口独立于机箱管理端口。

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

c) 配置**管理 IP** 地址。

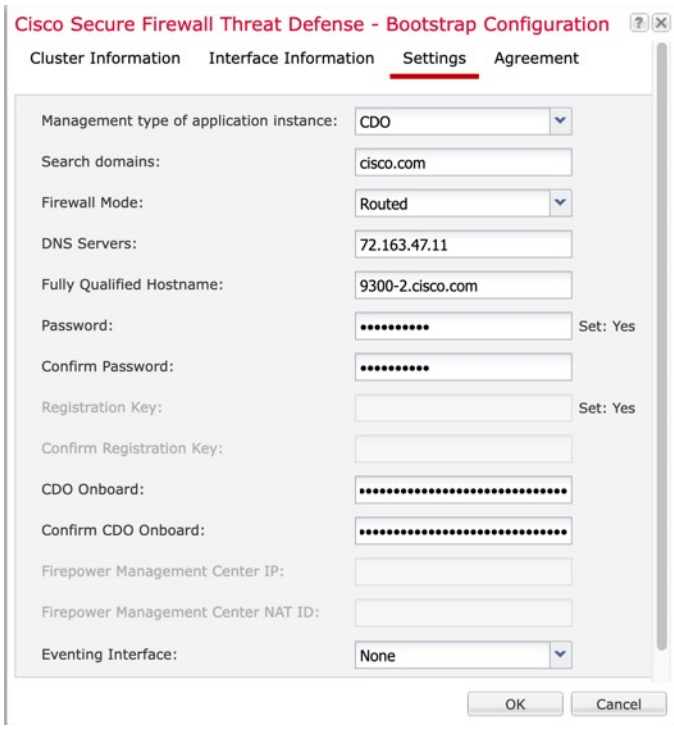
设置用于此接口的唯一 IP 地址。

d) 输入**网络掩码**或**前缀长度**。

e) 输入**网络网关**地址。

步骤 6 在**设置**选项卡上，完成下列操作：

图 *10:* 设置



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

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

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

d) 输入逗号分隔列表形式的 **DNS 服务器**。

例如，如果指定 管理中心 主机名，则 威胁防御 使用 DNS。

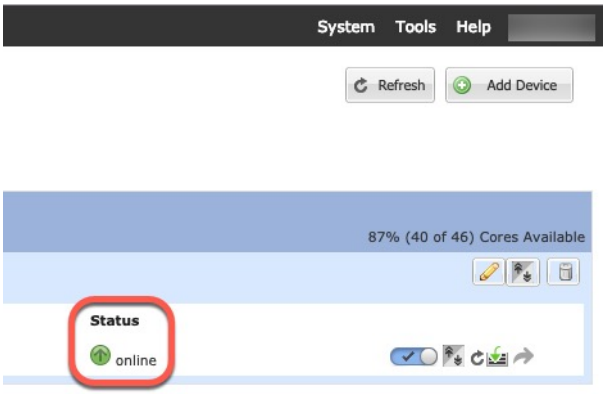
e) 输入 威胁防御 的**完全限定主机名**。
f) 输入供威胁防御管理员用户用于 CLI 访问的**密码**。
g) 将 CDO 生成的命令复制到**CDO 激活 (CDO Onboard)** 和**确认 CDO 激活 (Confirm CDO Onboard)** 字段中。
h) CDO 不支持单独的**事件接口**，因此将忽略此设置。

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

步骤 8 点击**确定 (OK)** 关闭配置对话框。

步骤 9 点击**保存 (Save)**。

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



配置基本安全策略

本部分介绍如何使用以下设置配置基本安全策略：

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

要配置基本安全策略，需完成以下任务。

1	配置接口。
2	配置 DHCP 服务器。
3	添加默认路由。
4	配置 NAT。
5	允许流量从内部传到外部。
6	部署配置。

配置接口

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

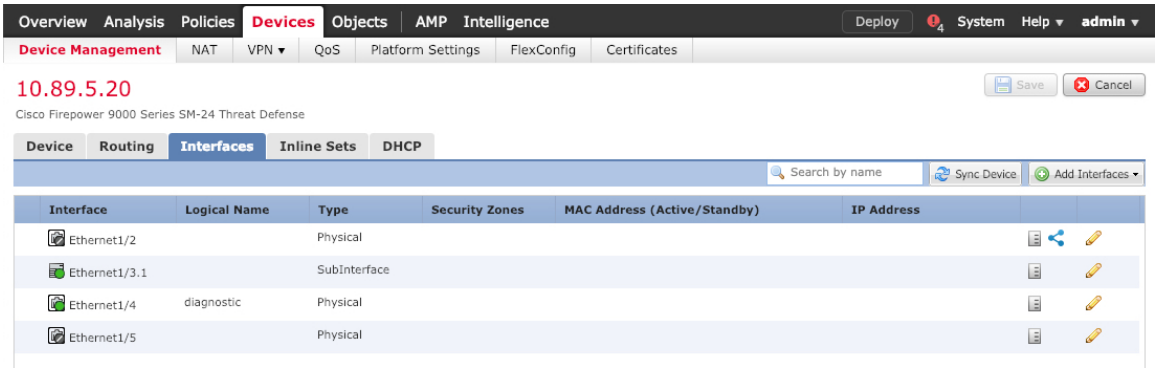
典型的边缘路由情况是通过 DHCP 从 ISP 获取外部接口地址，同时在内部接口上定义静态地址。

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

过程

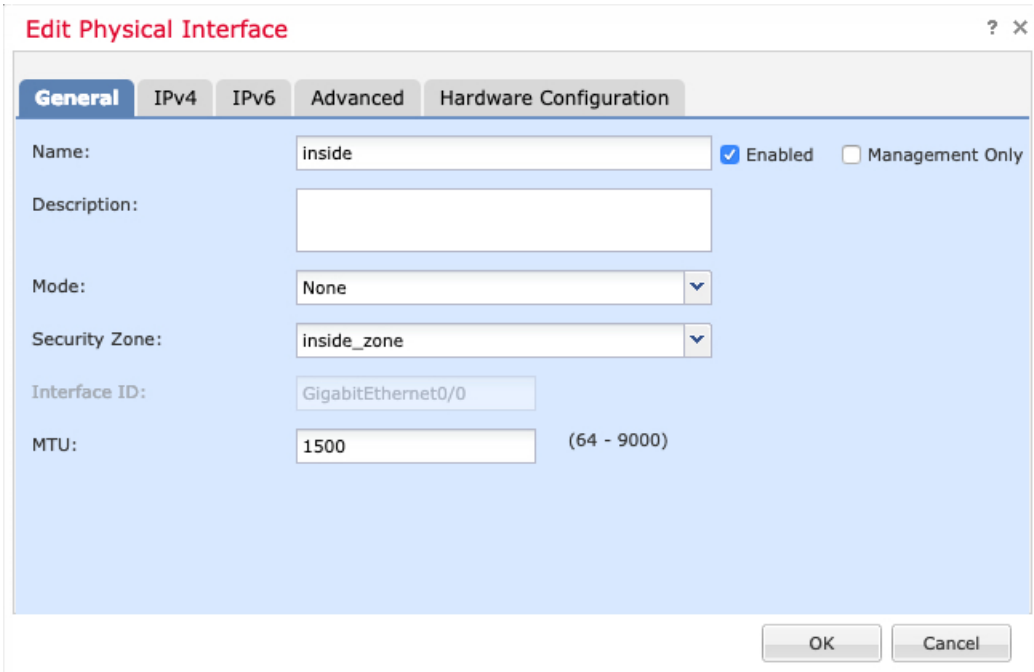
步骤 1 选择**设备 (Devices)** > **设备管理 (Device Management)**，然后点击防火墙的**编辑**（ ）。

步骤 2 点击**接口 (Interfaces)**。



步骤 3 点击要用于内部的接口的**编辑**（ ）。

此时将显示**一般 (General)** 选项卡。



a) 输入长度最大为 48 个字符的 **Name**。

例如，将接口命名为 **inside**。

b) 选中 **Enabled** 复选框。

c) 将 **Mode** 保留为 **None**。

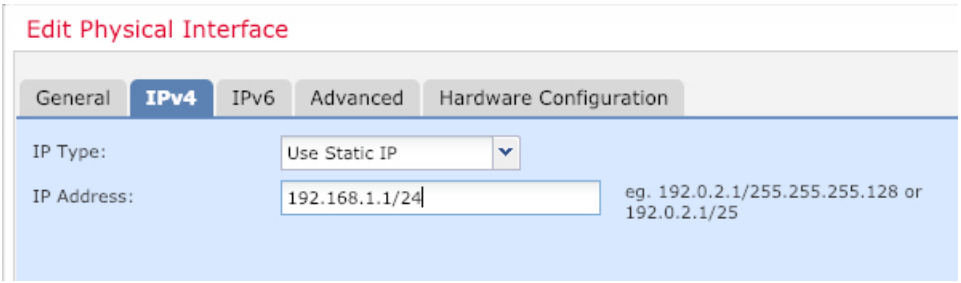
d) 从**安全区域 (Security Zone)** 下拉列表中选择一个现有的内部安全区域，或者点击**新建 (New)** 添加一个新的安全区域。

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

e) 点击 **IPv4** 和/或 **IPv6** 选项卡。

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

  例如，输入 **192.168.1.1/24**

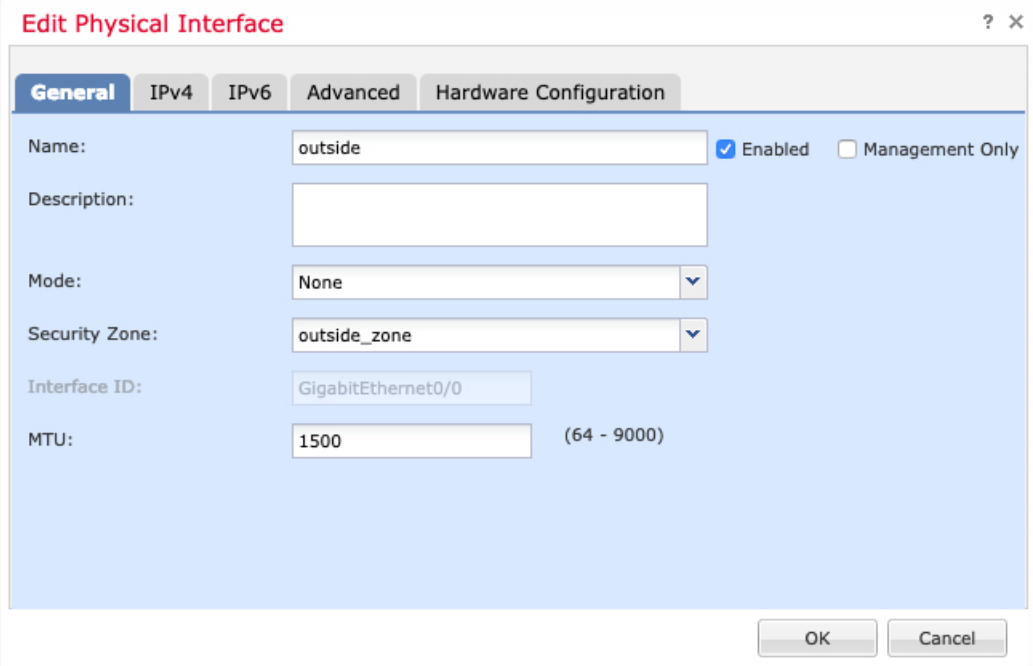


- **IPv6** - 为无状态自动配置选中**自动配置 (Autoconfiguration)** 复选框。

f) 点击**确定 (OK)**。

步骤 4 点击要用于外部的接口的 **编辑**（ ）。

此时将显示**一般 (General)** 选项卡。



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

a) 输入长度最大为 48 个字符的 **Name**。

例如，将接口命名为 **outside**。

b) 选中 **Enabled** 复选框。

c) 将 **Mode** 保留为 **None**。

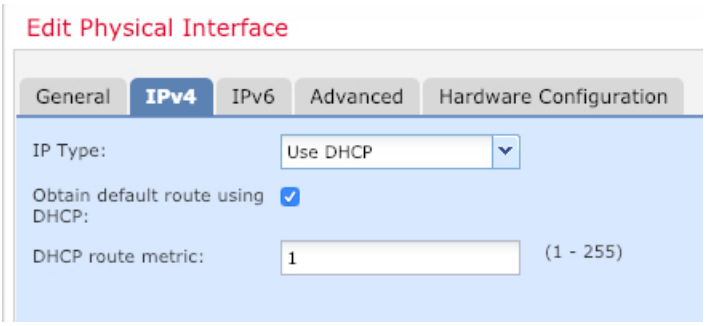
d) 从**安全区域 (Security Zone)** 下拉列表中选择一个现有的外部安全区域，或者点击**新建 (New)** 添加一个新的安全区域。

例如，添加一个名为 **outside_zone** 的区域。

e) 点击 **IPv4** 和/或 **IPv6** 选项卡。

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

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



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

f) 点击**确定 (OK)**。

步骤 5 点击**保存**。

配置 DHCP 服务器

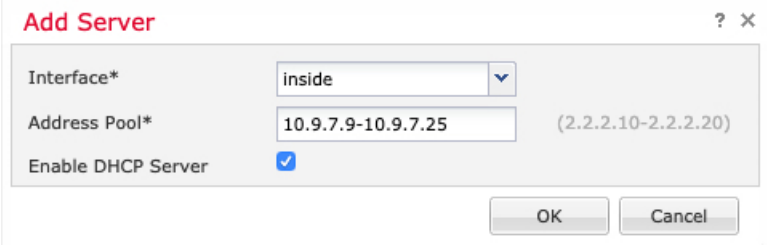
如果希望客户端使用 DHCP 从 威胁防御处获取 IP 地址，请启用 DHCP 服务器。

过程

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

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

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



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

步骤 4 点击**确定 (OK)**。

步骤 5 点击保存。

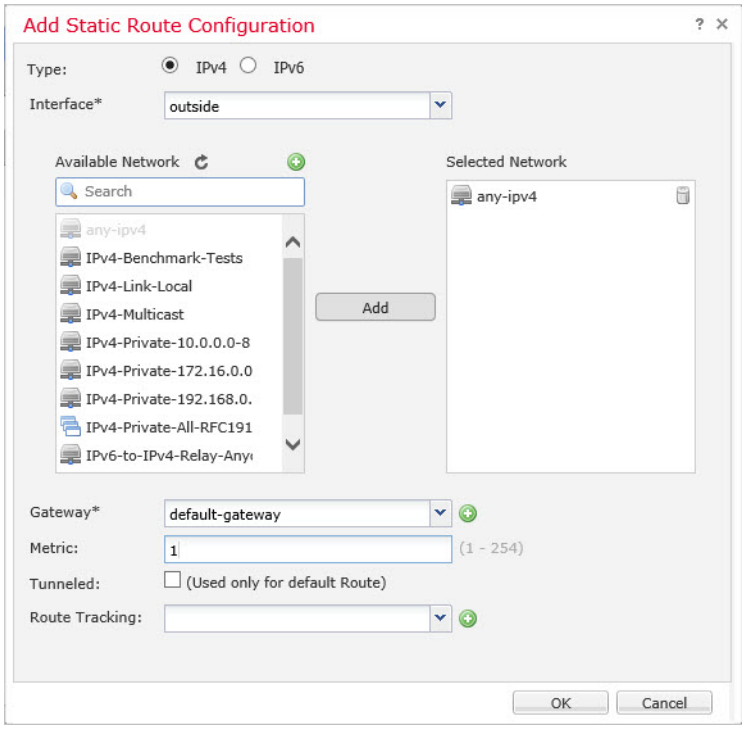
添加默认路由

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

过程

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

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

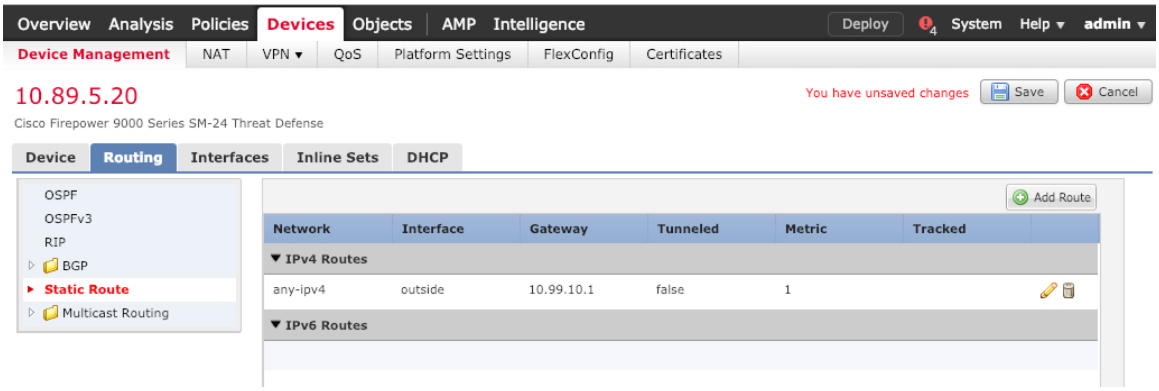


- **类型 (Intrusion)** - 根据要添加静态路由的类型，点击 **IPv4** 或 **IPv6** 单选按钮。
- **接口 (Interface)** - 选择出口接口；通常是外部接口。
- **Available Network** - 为 IPv4 默认路由选择 **any-ipv4**，为 IPv6 默认路由选择 **any-ipv6**，然后点击 **Add** 将其移至 **Selected Network** 列表。
- **网关 (Gateway)** 或 **IPv6 网关 (IPv6 Gateway)** - 输入或选择作为此路由的下一个跃点的网关路由器。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

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

步骤 3 点击**确定 (OK)**。

路由即已添加至静态路由表。



步骤 4 点击**保存**。

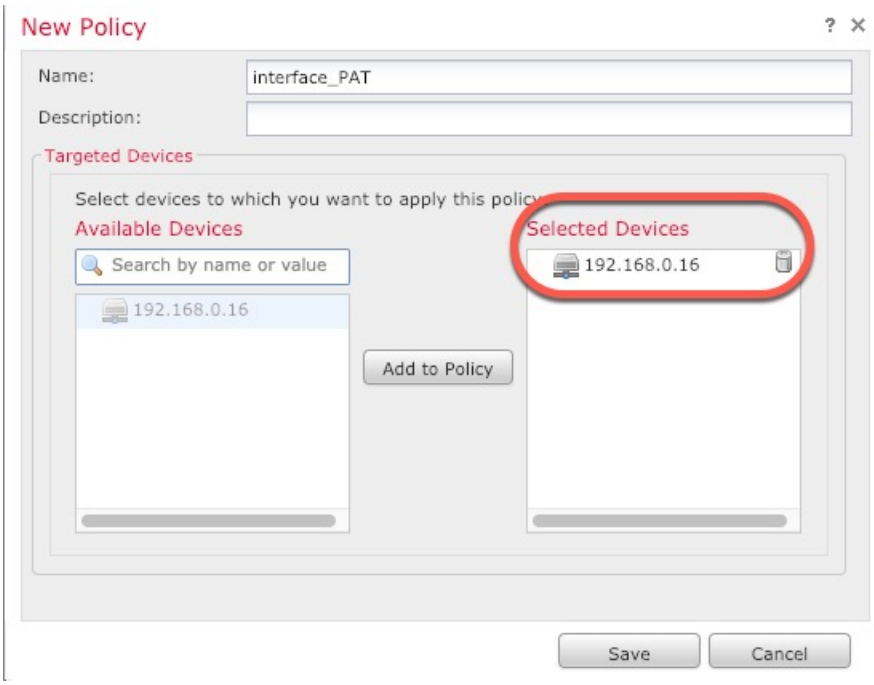
配置 NAT

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

过程

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

步骤 2 为策略命名，选择要使用策略的设备，然后点击**Save**。



策略即已添加 管理中心。您仍然需要为策略添加规则。

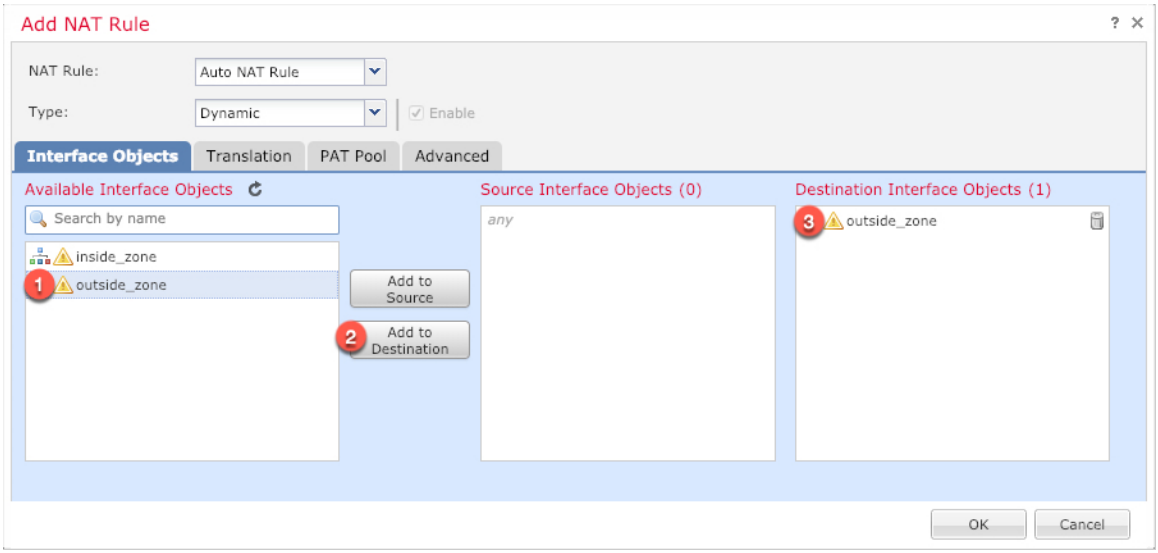
步骤 3 点击**添加规则 (Add Rule)**。

Add NAT Rule 对话框将显示。

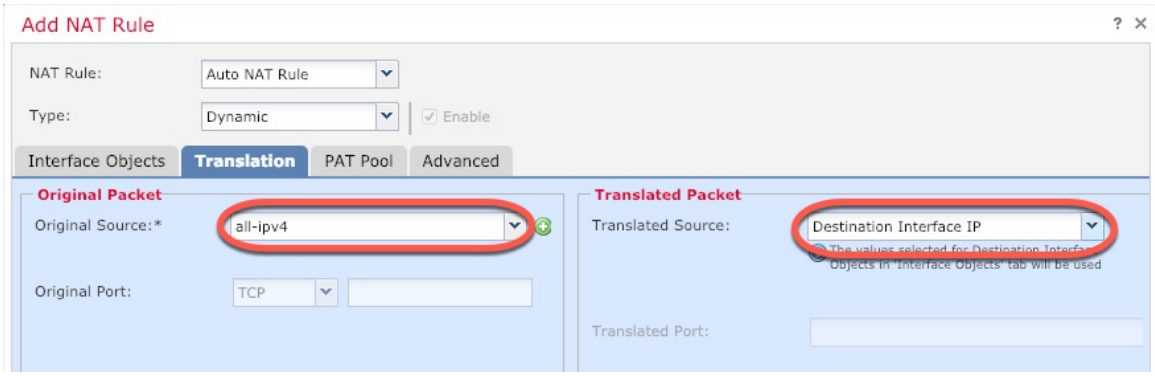
步骤 4 配置基本规则选项：

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

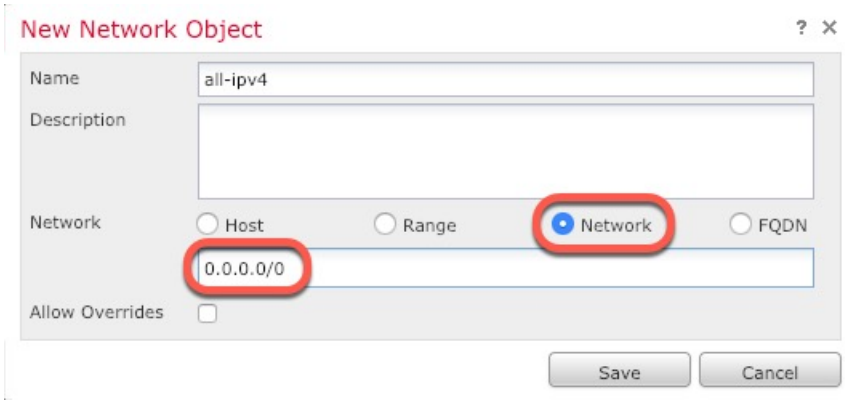
步骤 5 在 **Interface Objects** 页面，将 **Available Interface Objects** 区域中的外部区域添加到 **Destination Interface Objects** 区域。



步骤 6 在**转换 (Translation)** 页面上配置以下选项：



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

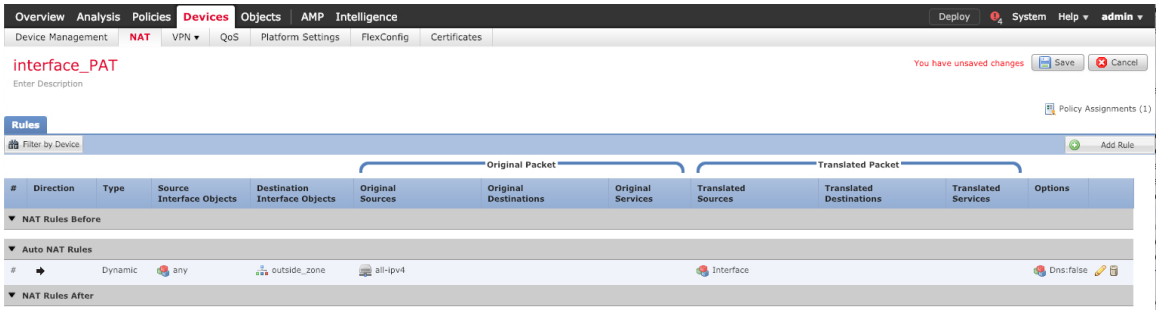


注释　　您不能使用系统定义的 **any-ipv4** 对象，因为自动 NAT 规则在对象定义过程中添加 NAT，并且您无法编辑系统定义的对象。

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

步骤 7 点击**保存 (Save)** 以添加规则。

规则即已保存至 **Rules** 表。



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

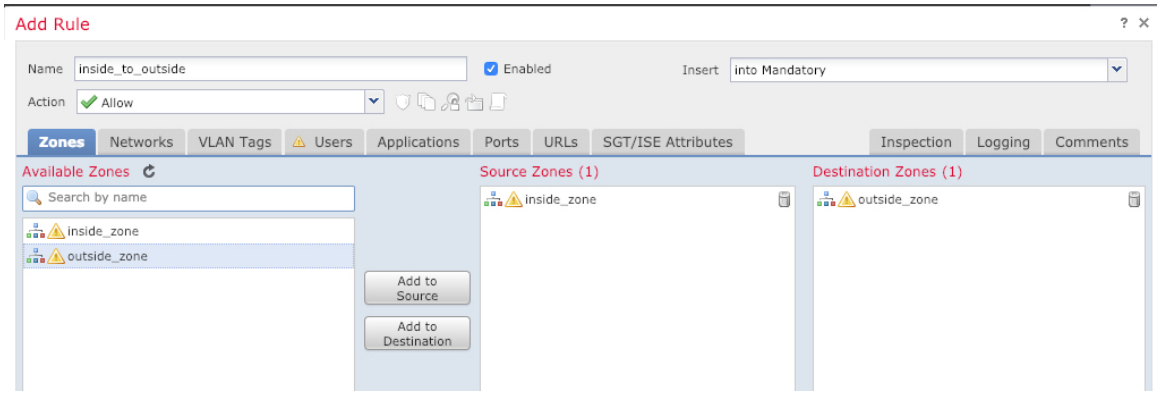
允许流量从内部传到外部

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

过程

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

步骤 2 点击**添加规则 (Add Rule)** 并设置以下参数：



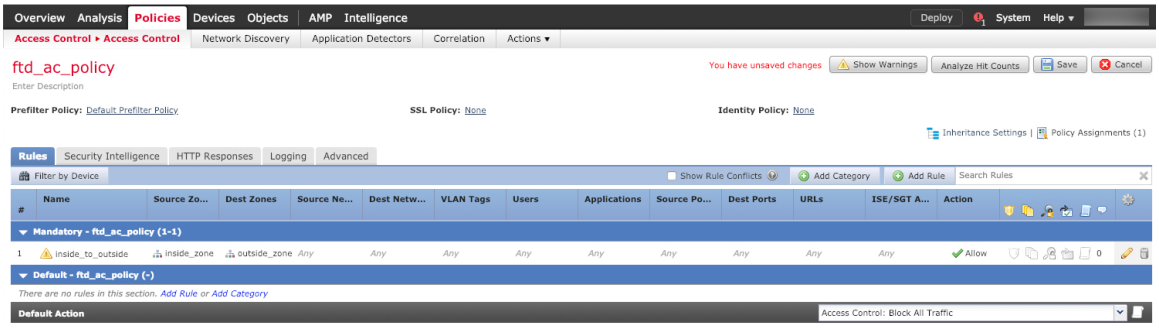
- **名称 (Name)** - 为此规则命名，例如 **inside_to_outside**。
- **源区域 (Source Zones)** - 从**可用区域 (Available Zones)** 中选择内部区域，然后点击**添加到源 (Add to Source)**。

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

其他设置保留原样。

步骤 3 点击添加 **(Add)**。

规则即已添加至 **Rules** 表。



步骤 4 点击保存。

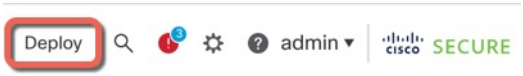
部署配置

将配置更改部署到 威胁防御；在部署之前，您的所有更改都不会在设备上生效。

过程

步骤 1 点击右上方的部署 **(Deploy)**。

图 *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

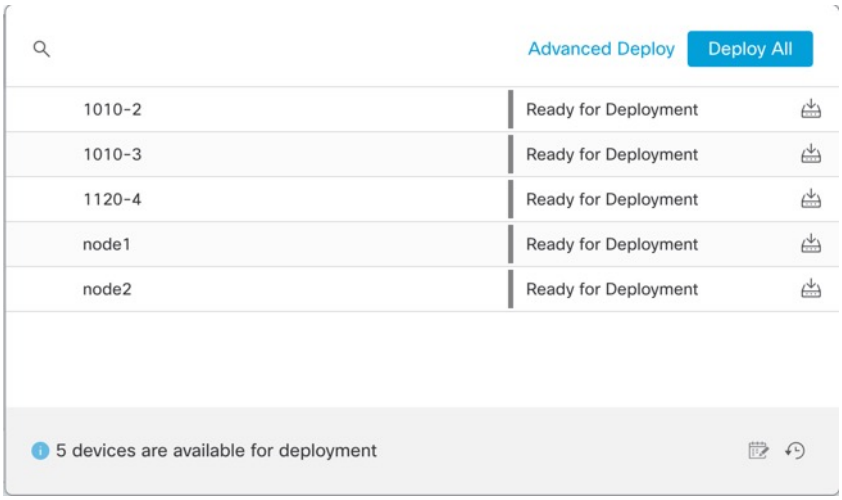
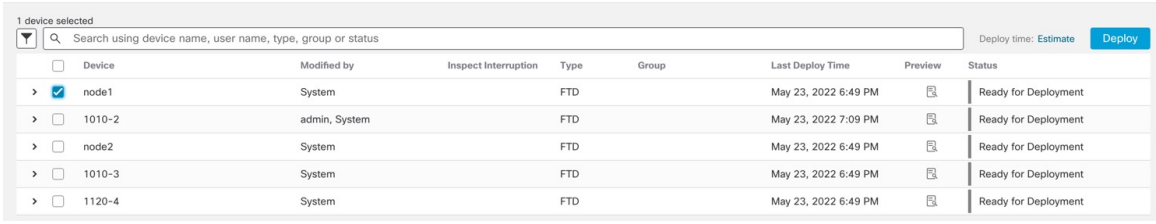
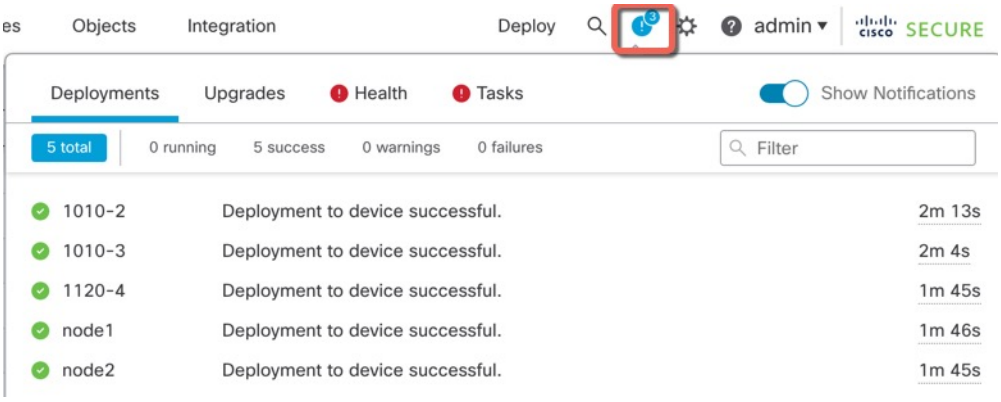


图 *13:* 高级部署



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

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

过程

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

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

如果忘记密码，可以通过编辑 机箱管理器 中的逻辑设备来更改密码。

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

a) 连接到 安全引擎。

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

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

示例：

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

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) 连接到 威胁防御控制台。

connect ftd *name*

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

示例：

```
Firepower-module1> connect ftd FTD_Instance1

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

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

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

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

注释　　对于 6.3 之前的版本，输入 **Ctrl-a, d**。

d) 返回 FXOS CLI的管理引擎层。

要退出控制台：

1. 输入 **~**

   您将退出至 Telnet 应用。

2. 要退出 Telnet 应用，请输入：

   telnet>**quit**

要退出 Telnet 会话：

输入 **Ctrl-],**。

示例

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

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

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect ftd FTD_Instance1

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

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

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

后续操作

要使用 CDO 继续配置 威胁防御，请参阅 思科防御协调器 主页。

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。