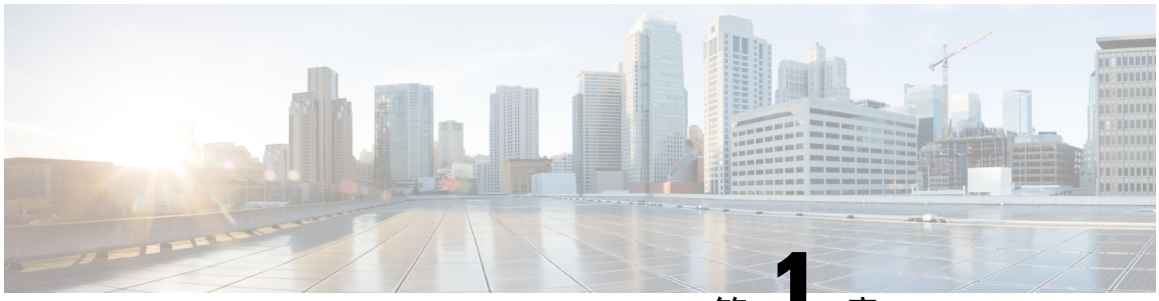
Cisco Secure Firewall 3100 威胁防御入门：云交付的防火墙管理中心

上次修改日期: 2025 年 1 月 21 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

准备工作

- 打开防火墙电源，第 1 页
- 安装的哪个应用程序：威胁防御还是 ASA？，第 1 页
- 访问 CLI，第 2 页
- 获取许可证，第 2 页

打开防火墙电源

系统电源由位于防火墙后部的控制。提供软通知，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。

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。

安装的哪个应用程序：威胁防御还是 ASA？

硬件上支持 FTD 或 ASA 两种应用。连接到控制台端口，并确定出厂时安装的应用。

过程

步骤 1 连接到控制台端口。

步骤 2 请参阅 CLI 提示，确定防火墙运行的是 FTD 还是 ASA。

FTD

您会看到 Firepower 登录 (FXOS) 提示。您无需登录和设置新密码即可断开连接。

```
firepower login:
```

ASA

您将看到 ASA 提示。

```
ciscoasa>
```

步骤 3 如果您运行的是错误的应用，请参阅Cisco Secure Firewall ASA 和 Secure Firewall Threat Defense 重新映像指南。

访问 CLI

您可能需要访问 CLI 进行配置或故障排除。

过程

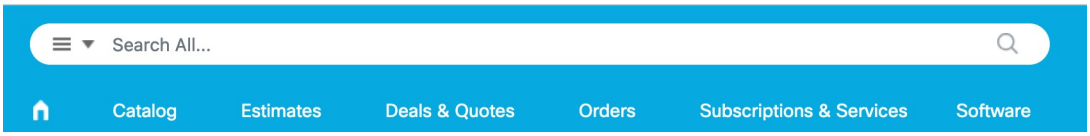
连接到控制台端口。

获取许可证

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。如果您没有智能软件管理器账户，请点击链接建立新账户。

1. 如果您需要自己添加许可证，请前往思科商务工作空间并使用**搜索全部 (Search All)** 字段。

   图 *1:* 许可证搜索

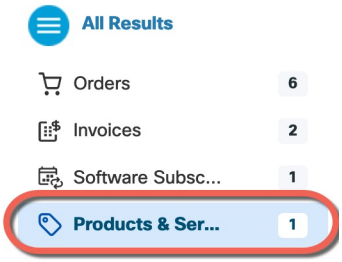
   

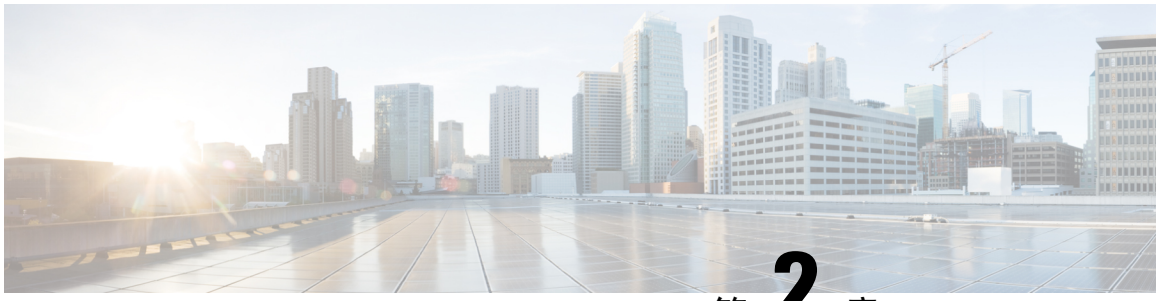
2. 搜索以下许可证 PID。

注释 如果未找到 PID，您可以手动将 PID 添加到订单中。

3. 从结果中选择产品和服务 **(Products & Services)**。

图 *2:* 结果





第 2 章

连接并防火墙

- 连接防火墙的电缆， 第 5 页
- 执行初始配置， 第 5 页

连接防火墙的电缆

执行初始配置

使用 Firepower 设备管理器 或 CLI 来执行行初始配置。

初始配置：设备管理器

使用这种方法，在注册防火墙后，除管理接口外还将预先配置以下接口：

- 以太网 1/1 - **outside**，IP 地址来自 DHCP、IPv6 自动配置
- - **inside**，192.168.95.1/24
- 默认路由 - 通过外部接口上的 DHCP 获取
- 其他接口 - 保留 FDM 中的任何接口配置。

不会保留其他设置，如内部的 DHCP 服务器、访问控制策略或安全区域。

过程

步骤 1 将计算机连接到内部接口。

步骤 2 登录FDM。

a) 转至https://192.168.95.1。

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

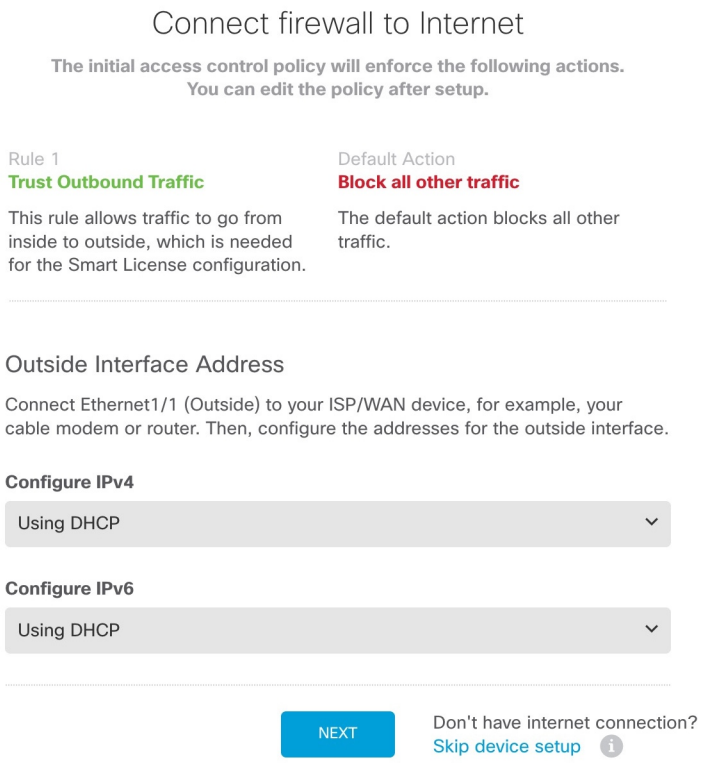
c) 系统会提示您阅读并接受“一般条款”并更改管理员密码。

步骤 3 使用设置向导。

注释
具体的端口配置取决于您的型号。

a) 配置外部接口和管理接口。

图 *3:* 将防火墙连接到互联网



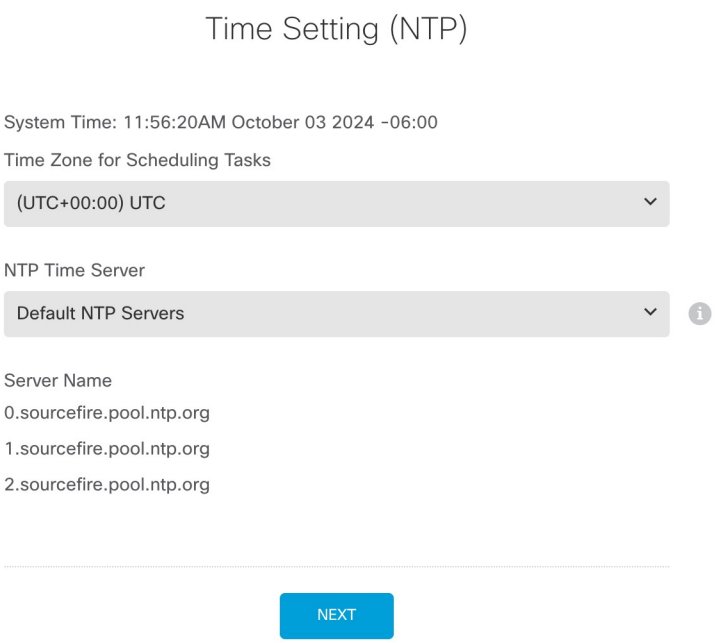
1. **外部接口地址** - 如果您计划实现高可用性，请使用静态 IP 地址。您不能使用设置向导配置 PPPoE；您可以在完成向导后配置 PPPoE。
2. **管理接口**

   DNS 服务器 - 系统管理地址的 DNS 服务器。默认值为 OpenDNS 公共 DNS 服务器。

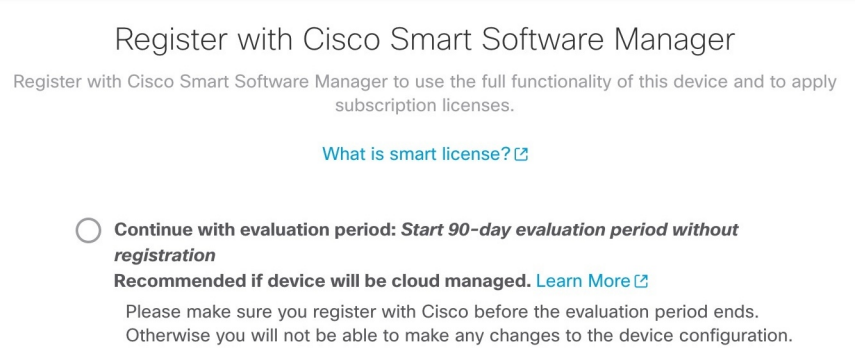
   防火墙主机名

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

图 *4:* 时间设置 ***(NTP)***



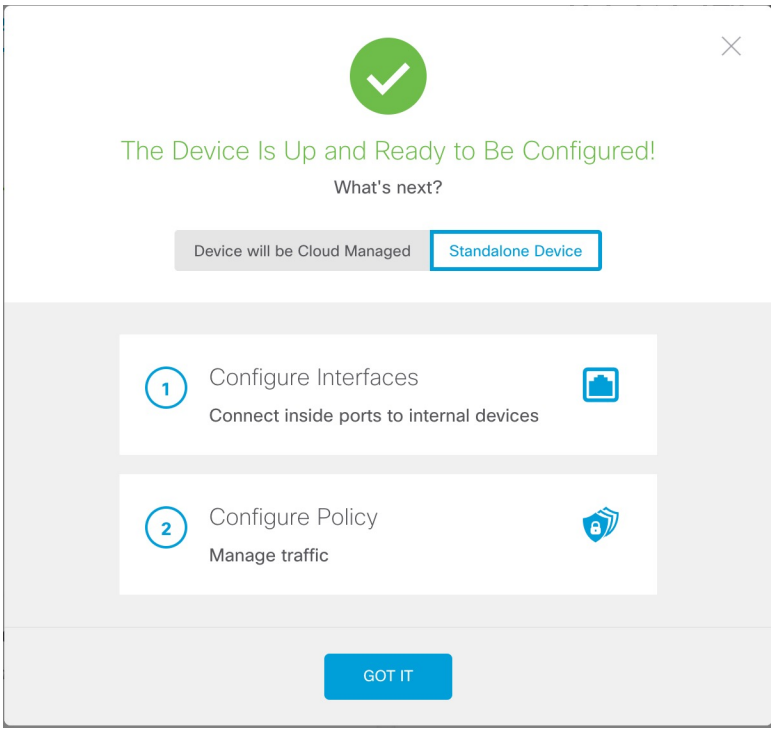
c) 选择**启动 90 日评估期而不注册**。



不要向智能软件管理器注册 FTD；所有许可均在 上执行。

d) 点击**完成**。

图 *5:* 后续操作



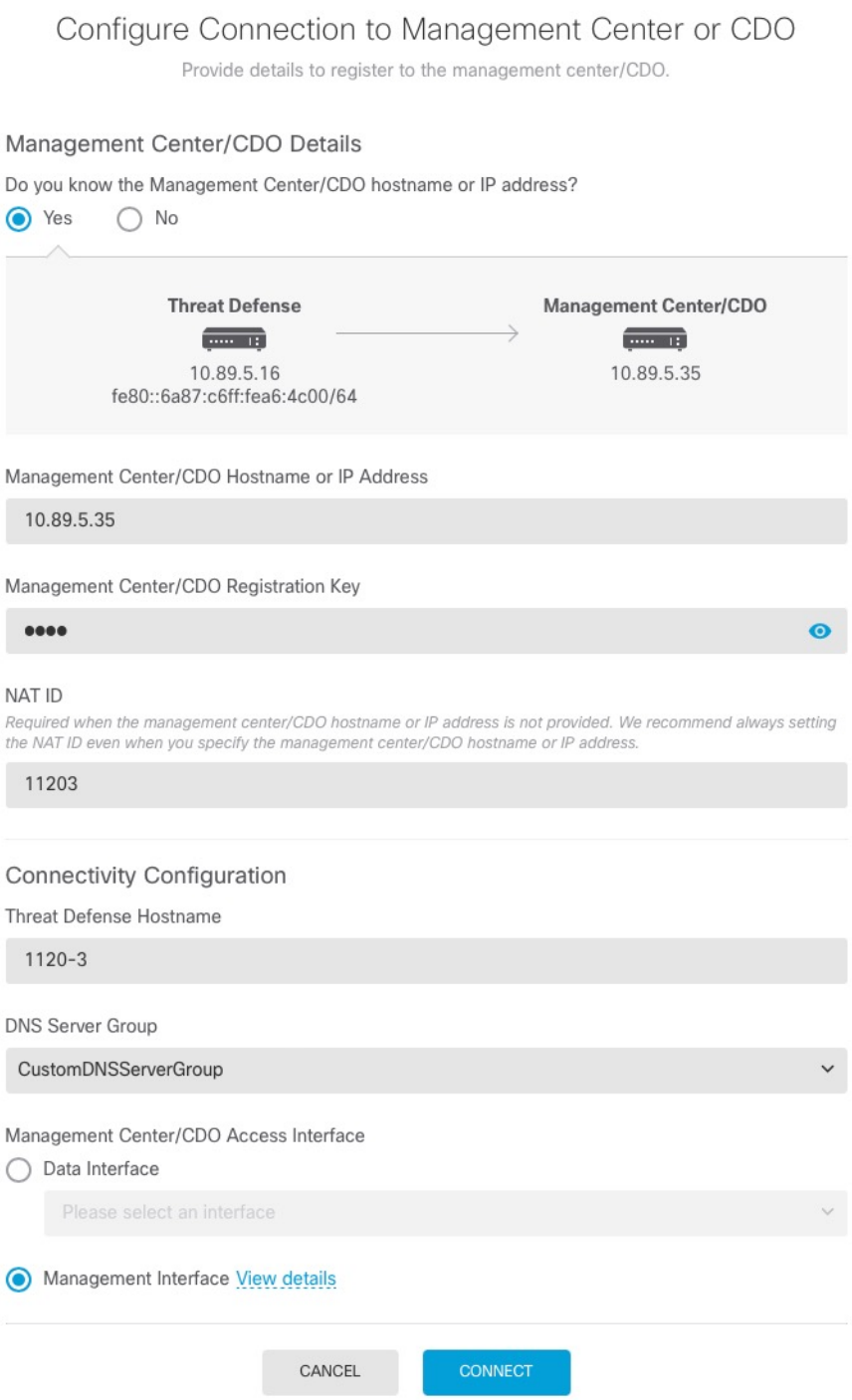
e) 依次选择**独立设备 (Standalone Device)** 和 **明白 (Got It)**。

步骤 4 如果要配置其他接口，请选择**设备 (Device)**，然后点击**接口 (Interfaces)** 摘要中的链接。

步骤 5 通过选择**设备 (Device)** 、 > **系统设置 (System Settings)** 、 > **集中管理 (Central Management)** 并点击**继续 (Proceed)**，向 注册

配置**管理中心/CDO** 详细信息。

图 *6:* 管理中心/*CDO* 详细信息



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 FMC，请点击**是 (Yes)**。

步骤 6 配置**连接配置**。

a) 指定**威胁防御主机名**。

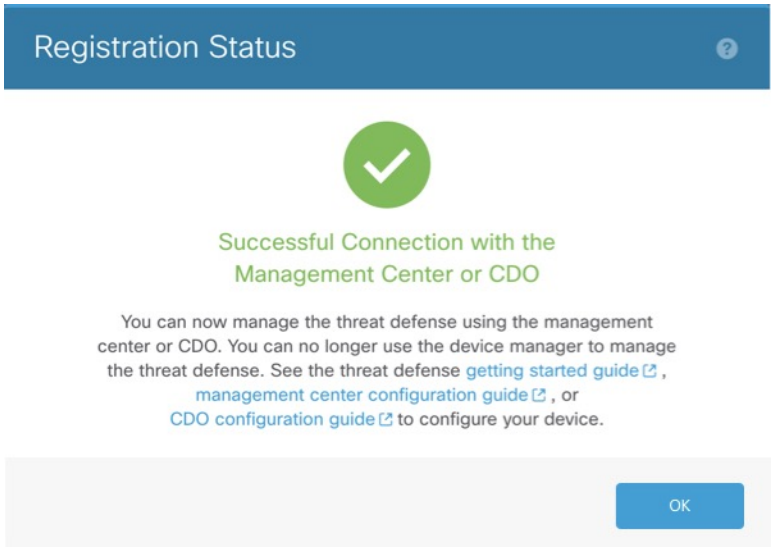
b) 指定 **DNS 服务器组**。

选择一个现有组，或创建一个新组。默认 DNS 组名为 **CiscoUmbrellaDNSServerGroup**，其中包括 OpenDNS 服务器。

步骤 7 点击**连接 (Connect)**。

注册状态 (Registration Status) 对话框将显示 注册的当前状态。

图 7: 成功连接



步骤 8 在**保存管理中心/CDO 注册设置**步骤之后，转到 ，然后添加防火墙。请参阅。

初始配置： CLI

使用 CLI 设置脚本设置专用管理 IP 地址、网关和其他基本网络设置。

过程

步骤 1 连接控制台端口并访问 FTD CLI。请参阅访问 CLI， 第 2 页。

步骤 2 完成管理界面设置的 CLI 设置脚本。

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。

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
Cisco General Terms
```

```
[...]

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.
Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [y]: n
```

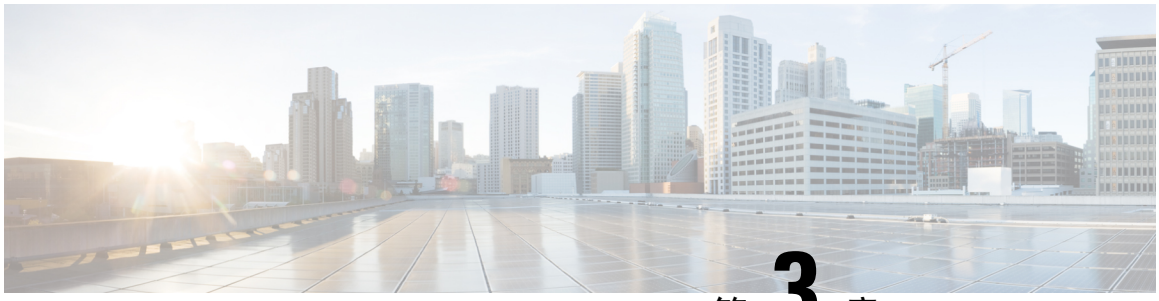
指南：为至少其中一种地址类型输入 **y**。

```
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:

Enter an IPv4 address for the management interface [192.168.45.61]: 10.89.5.17
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192


Enter a fully qualified hostname for this system [firepower]: 1010-3
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220,2620:119:35::35]:
Enter a comma-separated list of search domains or 'none' []: cisco.com
If your networking information has changed, you will need to reconnect.
Disabling IPv6 configuration: management0
Setting DNS servers: 208.67.222.222,208.67.220.220,2620:119:35::35
Setting DNS domains:cisco.com

Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: data on management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'

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

指南：输入 **no** 以使用 FMC。

```
Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: data on management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'

Configuring firewall mode ...


Device is in OffBox mode - disabling/removing port 443 from iptables.
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.
>
```



第 3 章

配置基本策略

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。

您还可以自定义安全策略，以包括更高级的检查。

- 配置 DHCP 服务器， 第 13 页
- 配置 NAT， 第 15 页
- 配置访问控制规则， 第 18 页
- 部署配置， 第 20 页

配置 DHCP 服务器

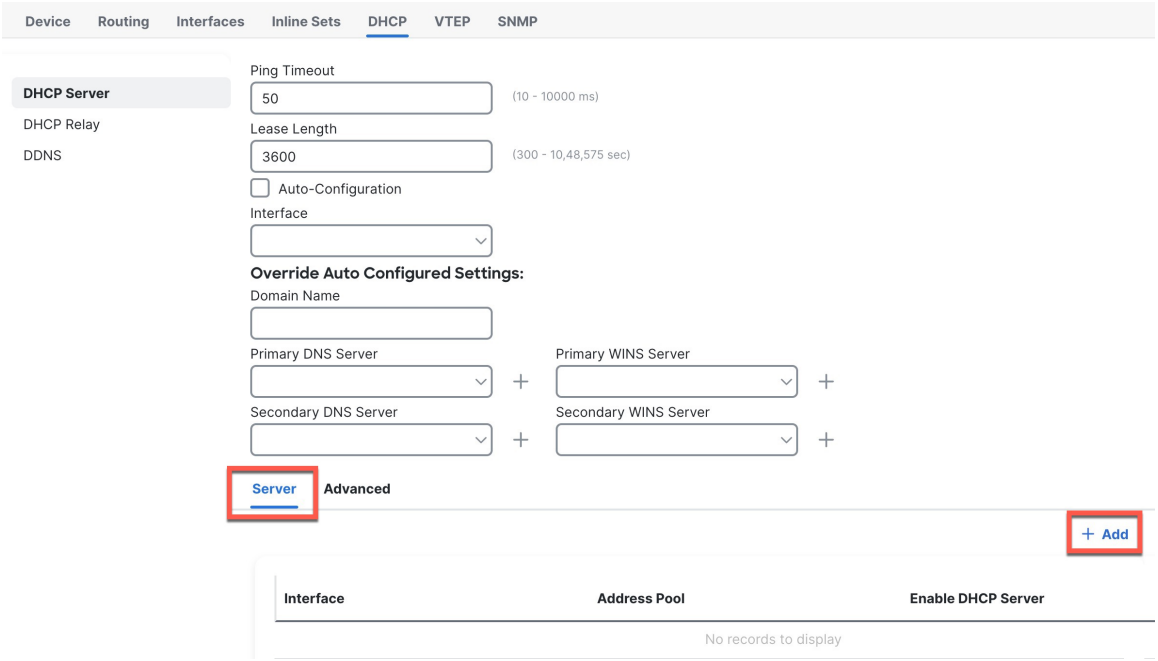
如果希望客户端使用 DHCP 从防火墙获取 IP 地址，请启用 DHCP 服务器。

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** ( )。

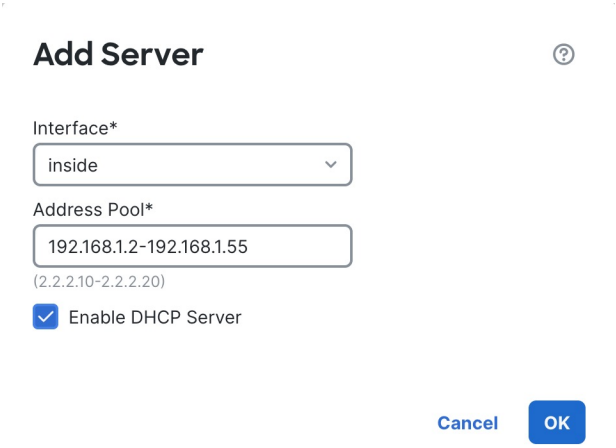
步骤 2 选择 **DHCP** > **DHCP 服务器 (DHCP Server)**。

图 *8: DHCP* 服务器



步骤 3 在服务器 **(Server)** 区域中，点击添加 **(Add)** 并配置以下选项。

图 *9:* 添加服务器



- **接口 (Interface)** - 从下拉列表中选择接口名称。
- **地址池 (Address Pool)** - 设置 IP 地址的范围。IP 地址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

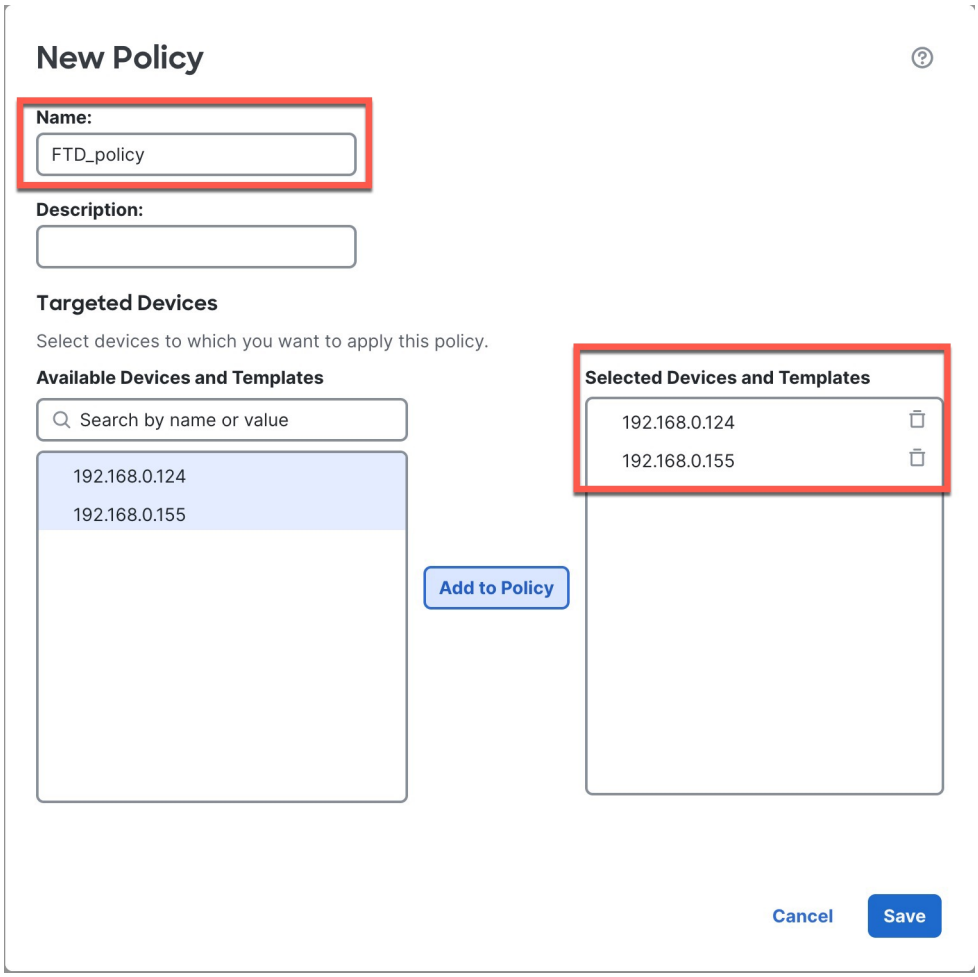
此步骤将为内部客户端创建一条 NAT 规则，以便将内部地址转换为外部接口 IP 地址上的端口。这类 NAT 规则称为接口端口地址转换 *(PAT)*。

过程

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

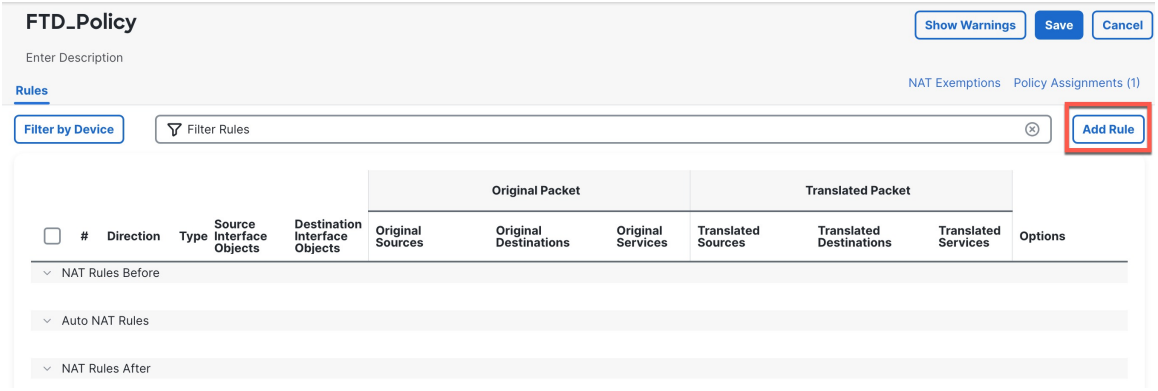
步骤 2 为策略命名，选择要使用策略的设备，然后点击保存 (Save)。

图 *10:* 新建策略



策略即已添加 FMC。您仍然需要为策略添加规则。

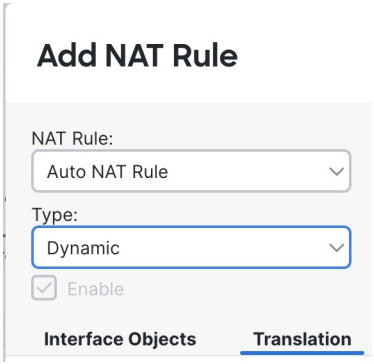
图 *11: NAT* 策略



步骤 3 点击添加规则 **(Add Rule)**。

步骤 4 配置基本规则选项：

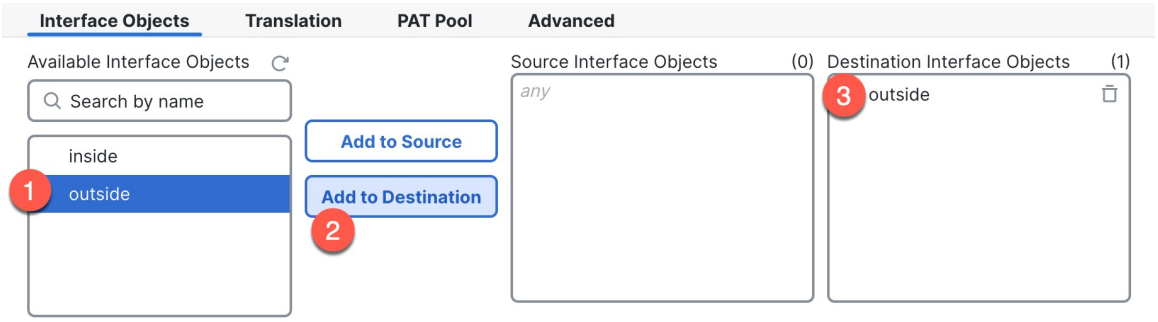
图 *12:* 基本规则选项



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

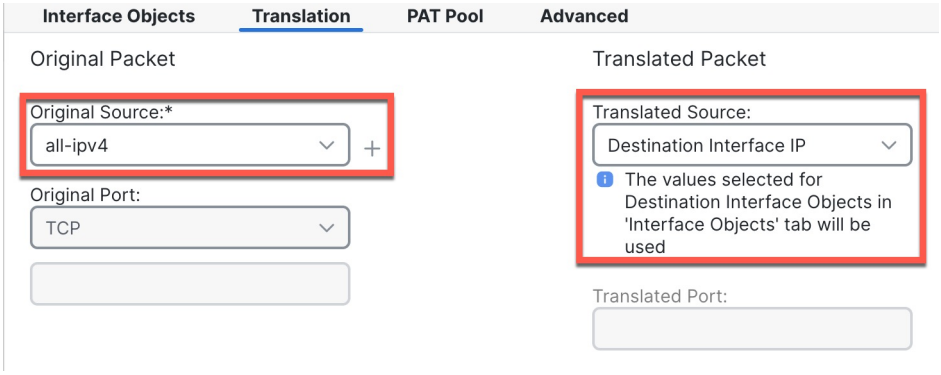
步骤 5 在 **Interface Objects** 页面，将 **Available Interface Objects** 区域中的外部区域添加到 **Destination Interface Objects** 区域。

图 *13:* 接口对象



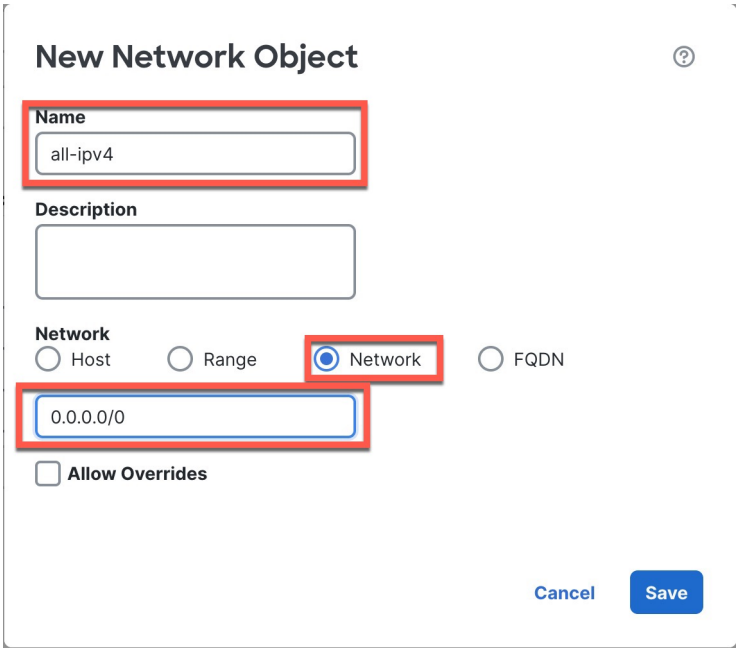
步骤 6 在**转换 (Translation)** 页面上配置以下选项：

图 *14:* 转换



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

  图 *15:* 新的网络对象



  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。

配置访问控制规则

如果您在注册设备时创建了基本的**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。访问控制策略可包括按顺序评估的多个规则。

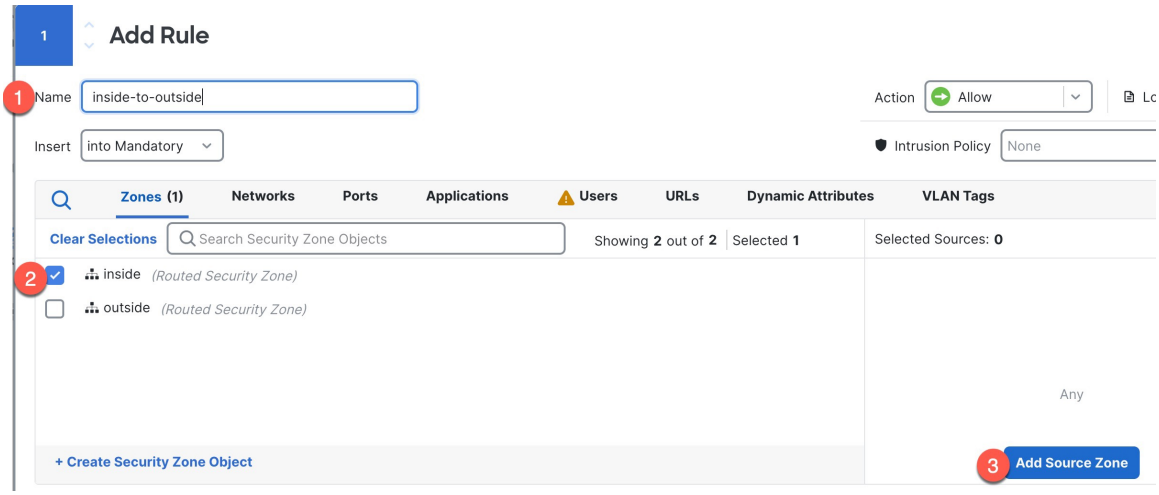
此过程将创建一个访问控制规则，以允许从内部区域到外部区域的所有流量。

过程

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

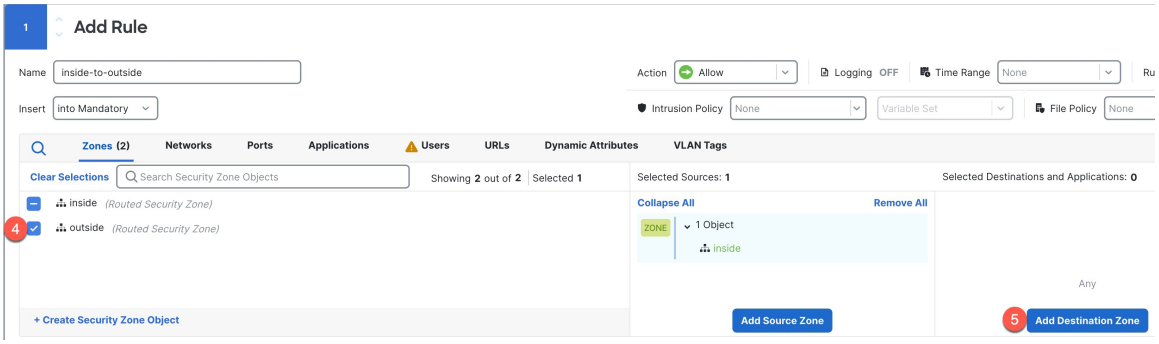
步骤 2 点击**添加规则 (Add Rule)** 并设置以下参数。

图 *16:* 源区域



1. 为此规则命名，例如 **inside-to-outside**。
2. 从**区域 (Zones)** 中选择内部区域
3. 点击**添加源区域 (Add Source Zone)**。

图 *17:* 目标区域



4. 从区域 **(Zones)** 中选择外部区域。

5. 点击添加目标区域 **(Add Destination Zone)**。

其他设置保留原样。

步骤 3 （可选） 点击数据包流程图中的策略类型，以便自定义相关策略。

预过滤器、解密、安全智能和身份策略在访问控制规则之前应用。不需要自定义这些策略，但在了解网络需求后，这些策略可通过快速路由受信任流量（绕过处理）或阻止流量以避免进一步处理，从而提高网络性能。

图 *18:* 在访问控制之前应用政策

- **预过滤器规则** - 默认预过滤器策略通过所有流量，以便其他规则执行操作（分析）。您可以对默认策略进行的唯一更改是**阻止**隧道流量。否则，您可以创建新的预过滤器策略，以便与可以分析（传递）、快速路径（绕过进一步检查）或阻止的访问控制策略关联。

  预过滤功能可在流量到达更远的地方之前，通过拦截或快速路径来处理流量，从而提高性能。在新策略中，您可以添加隧道规则和预过滤器规则。通过隧道规则，您可以对明文（非加密）直通隧道进行快速路由、阻止或重新分区。预过滤器规则可让您快速路由或阻止通过 IP 地址、端口和协议识别的非隧道流量。

  例如，如果知道要阻止网络上的所有 FTP 流量，但不阻止来自管理员的快速 SSH 流量，则可以添加一个新的预过滤器策略。

- **解密** - 默认情况下不应用解密。解密是让网络流量接受深度检查的一种方法。大多数情况下都不要对流量进行解密，只有在法律允许的情况下才能这样做。为了最大限度地保护网络，对于前往关键服务器或来自不信任网段的流量，解密策略可能是一个好主意。

- **安全智能** - （需要 IPS 许可证）默认启用安全智能。安全智能是在将连接传递到访问控制策略进行进一步处理之前应用的另一项针对恶意活动的早期防御措施。安全智能使用信誉情报快速阻止与思科威胁情报组织 Talos 提供的 IP 地址、URL 和域名之间的连接。您可以根据需要添加或删除其他 IP 地址、URL 或域。

  注释
  如果没有 IPS 许可证，即使访问控制策略中显示该策略已启用，也不会部署该策略。

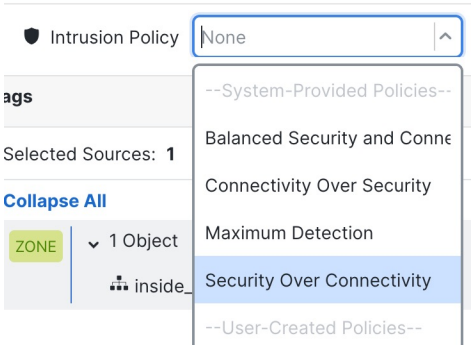
- **身份** - 默认情况下不应用身份。在允许访问控制策略处理流量之前，可以要求用户进行身份验证。

步骤 4 （可选）添加在访问控制规则之后应用的入侵策略。

入侵策略是一组已定义的入侵检测和防御配置，用于检查流量是否违反安全规定。FMC 包括许多系统提供的策略，您可以按原样启用或自定义这些策略。此步骤可启用系统提供的策略。

a) 点击**入侵策略 (Intrusion Policy)** 下拉列表。

图 *19:* 系统提供的入侵策略

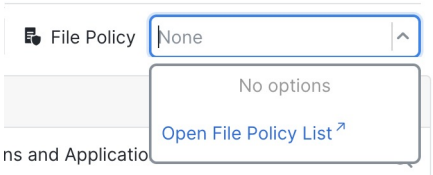


b) 从列表中选择一个系统提供的策略。

步骤 5 （可选）添加在访问控制规则之后应用的文件策略。

a) 点击**文件策略 (File Policy)** 下拉列表，然后选择现有策略或通过选择**打开文件策略列表 (Open File Policy List)** 添加一个策略。

图 *20:* 文件策略



对于新策略，系统将在单独的选项卡中打开**策略 (Policies)** > **恶意软件和文件 (Malware & File)** 页面。

b) 有关创建策略的详细信息，请参阅《适用于 Firepower 设备的 Cisco Firepower Threat Defense 配置指南》。

c) 返回**添加规则 (Add Rule)** 页面，从下拉列表中选择新创建的策略。

步骤 6 点击**应用 (Apply)**。

规则即已添加至 **Rules** 表。

步骤 7 点击**保存 (Save)**。

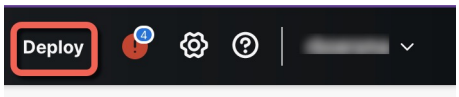
部署配置

将配置更改部署到设备；在部署之前，您的所有更改都不会在设备上生效。

过程

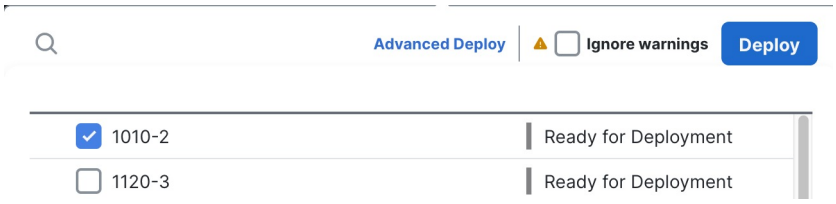
步骤 1 点击右上方的**部署 (Deploy)**。

图 *21:* 部署



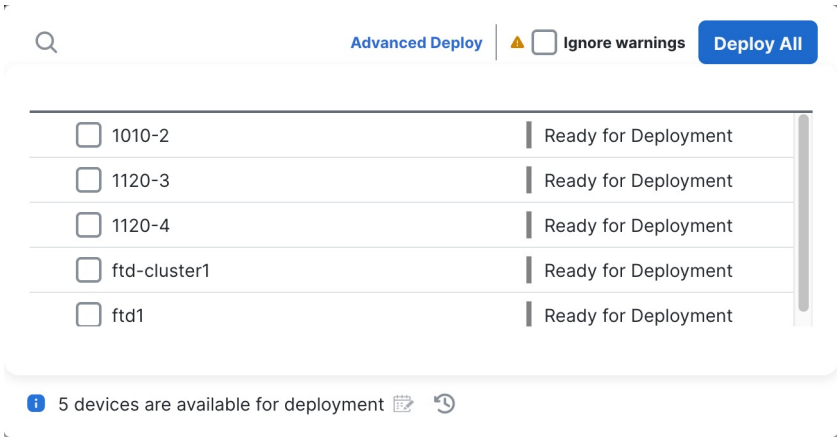
步骤 2 要快速部署，请选中特定设备，然后点击**部署 (Deploy)**。

图 *22:* 部署所选



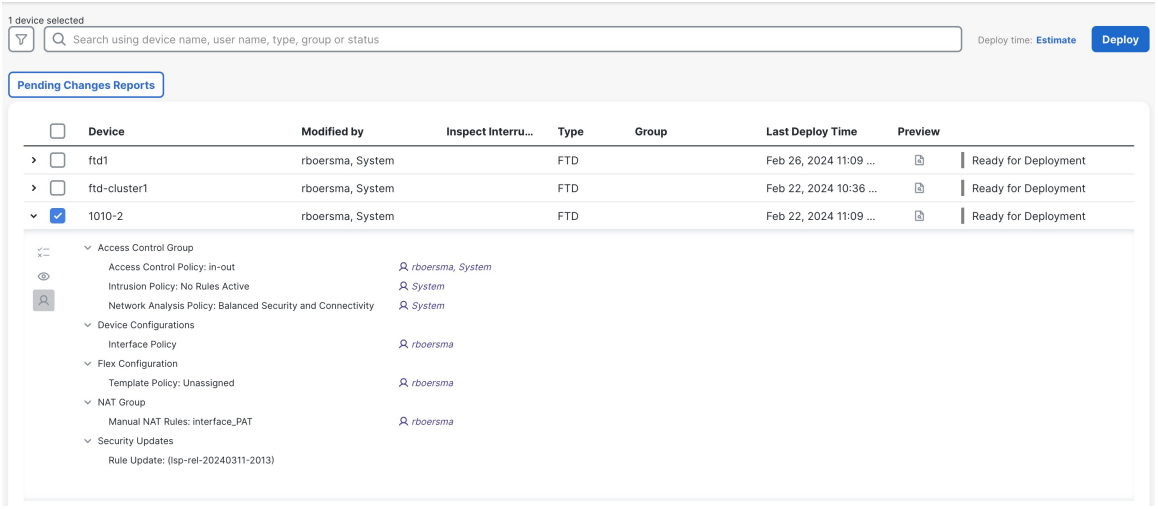
或者，点击**全部部署 (Deploy All)** 以部署到所有设备。

图 *23:* 全部部署



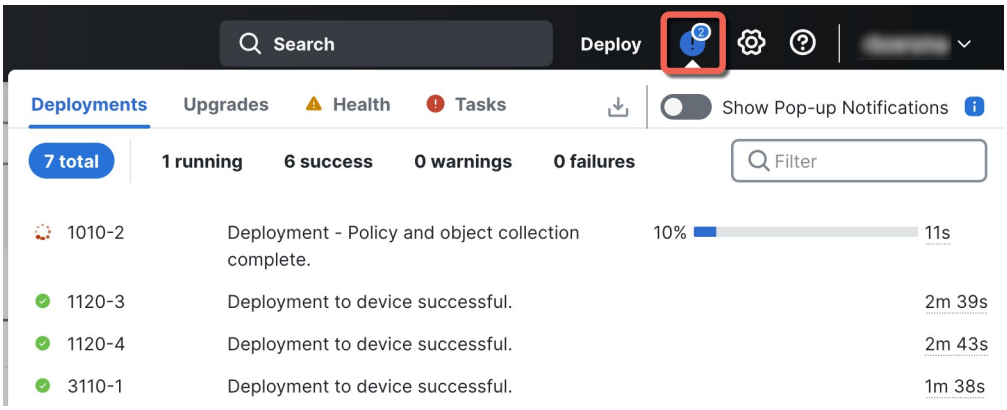
否则，对于其他部署选项，请点击**高级部署 (Advanced Deploy)**。

图 *24:* 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 *25:* 部署状态



© 2025 Cisco Systems, Inc. 保留所有权利。

当地语言翻译版本说明

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