



Cisco Secure Firewall 4200 威胁防御入门：本地管理网络上的管理中心

上次修改日期: 2025 年 3 月 25 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

使用专用管理网络上的 Cisco Secure Firewall Management Center 来管理防火墙。

- 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 2 页
- 访问威胁防御 CLI，第 3 页
- 检查版本和重新映像，第 4 页
- 获取许可证，第 5 页
- （必要时）关闭防火墙电源，第 7 页

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。摇杆电源开关提供软通知，支持平稳地关闭系统以降低系统软件及数据损坏的风险。



注释 首次启动防火墙时，威胁防御 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。

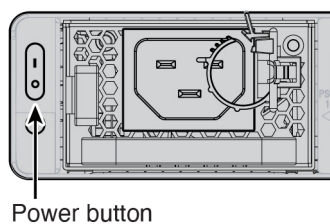
过程

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摇杆电源开关打开电源。

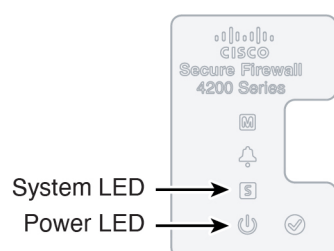
安装的哪个应用程序：威胁防御还是 **ASA**？

图 1: 电源按钮



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 2: 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。

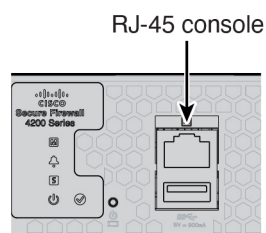
安装的哪个应用程序：威胁防御还是 **ASA**？

硬件上支持威胁防御或 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。

图 3: 控制台端口



步骤 2 请参阅 CLI 提示，确定防火墙运行的是威胁防御还是 ASA。

威胁防御

```
firepower login:
```

您将看到 ASA 提示。

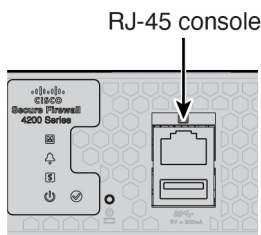
```
ciscoasa>
```

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](#)。

您可能需要访问 CLI 进行配置或故障排除。

过程

图 4: 控制台端口



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

$$[\dots]$$

```
firepower#
```

步骤 3 切换到 威胁防御 CLI。

注释

如果要使用 设备管理器 进行初始设置，请不要访问 威胁防御 CLI，否则会启动 CLI 设置。

connect ftd

首次连接到 威胁防御 CLI 时，系统会提示您完成初始设置。

示例：

```
firepower# connect ftd
>
```

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 提示。

示例：

```
> exit
firepower#
```

检查版本和重新映像

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。

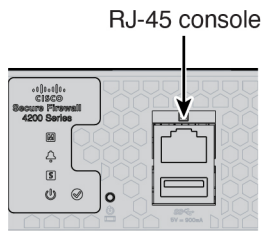
我应该运行什么版本？

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> 中介绍的发布策略。

过程

步骤 1 连接到控制台端口。

图 5: 控制台端口



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	7.6.0.65	7.6.0.65	Not Applicable

步骤 3 如果要安装新版本，请执行这些步骤。

a) 默认情况下，管理接口将使用 DHCP。如果需要为管理界面设置静态 IP 地址，请输入以下命令。

scope fabric-interconnect a

set out-of-band static ip ip netmask 网络掩码 gw 网关

commit-buffer

注释

如果遇到以下错误，必须在提交更改之前禁用 DHCP。使用以下命令来禁用 DHCP。

```
firepower /fabric-interconnect* # commit-buffer
Error: Update failed: [Management ipv4 address (IP <ip> / net mask <netmask> ) is not
in the same network of current DHCP server IP range <ip - ip>].
Either disable DHCP server first or config with a different ipv4 address.]
firepower /fabric-interconnect* # exit
firepower* # scope system
firepower /system* # scope services
firepower /system/services* # disable dhcp-server
firepower /system/services* # commit-buffer
```

b) 执行《[FXOS 故障排除指南](#)》中的[重新映像程序](#)。

您需要从可通过管理接口访问的服务器下载新的映像。

防火墙重新启动后，您可以再次连接到 FXOS CLI。

c) 在 FXOS CLI 中，系统会提示您再次设置管理员密码。

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](#)。

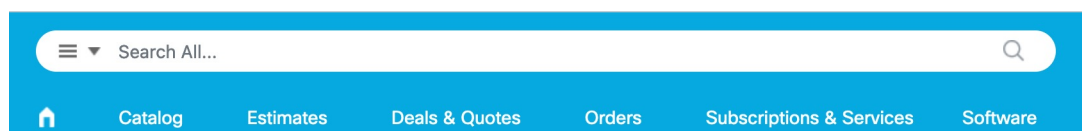
如果尚未注册，请向智能软件管理器注册 管理中心。注册需要您在智能软件管理器中生成注册令牌。有关详细说明，请参阅《[Cisco Secure Firewall Management Center 管理指南](#)》。

威胁防御 具有以下许可证：

- 基础版 — 必需
- IPS
- 恶意软件防御
- URL 过滤
- Cisco Secure Client
- 运营商 - Diameter、GTP/GPRS、M3UA、SCTP

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 6: 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。

- Essentials:
 - 自动包含
- IPS、恶意软件防御和 URL 组合:
 - L-FPR4215T-TMC=
 - L-FPR4225T-TMC=
 - L-FPR4245T-TMC=

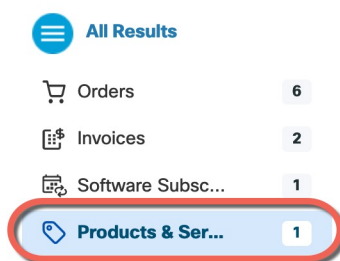
当您将上述 PID 之一添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：

- L-FPR4215T-TMC-1Y
- L-FPR4215T-TMC-3Y
- L-FPR4215T-TMC-5Y
- L-FPR4225T-TMC-1Y
- L-FPR4225T-TMC-3Y
- L-FPR4225T-TMC-5Y
- L-FPR4245T-TMC-1Y

- L-FPR4245T-TMC-3Y
- L-FPR4245T-TMC-5Y
- 运营商:
 - L-FPR4200K-FTD-CAR=
- Cisco Secure 客户端 — 请参阅 [Cisco Secure 客户端订购指南](#)。

3. 从结果中选择产品和服务 (Products & Services)。

图 7: 结果



(必要时) 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。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。

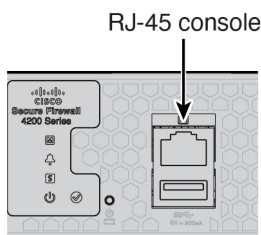
在 CLI 关闭防火墙电源

您可以使用 FXOS CLI 安全地关闭系统并关闭防火墙电源。

过程

步骤 1 连接到控制台端口。

图 8: 控制台端口



步骤 2 在 FXOS CLI 中，连接到 local-mgmt 模式。

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

步骤 3 关闭系统。

```
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 4 留意防火墙关闭时的系统提示。关闭完成后，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 5 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。

使用管理中心关闭防火墙

使用管理中心正确关闭系统。

过程

步骤 1 关闭防火墙。

- a) 选择设备 > 设备管理。
- b) 在要重新启动的设备旁边，点击 编辑 (✎)。
- c) 点击设备 (Device) 选项卡。
- d) 在系统 (System) 部分中点击 关闭设备 (🔌)。
- e) 出现提示时，确认是否要关闭设备。

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。关闭完成后，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。



第 2 章

连接并注册防火墙

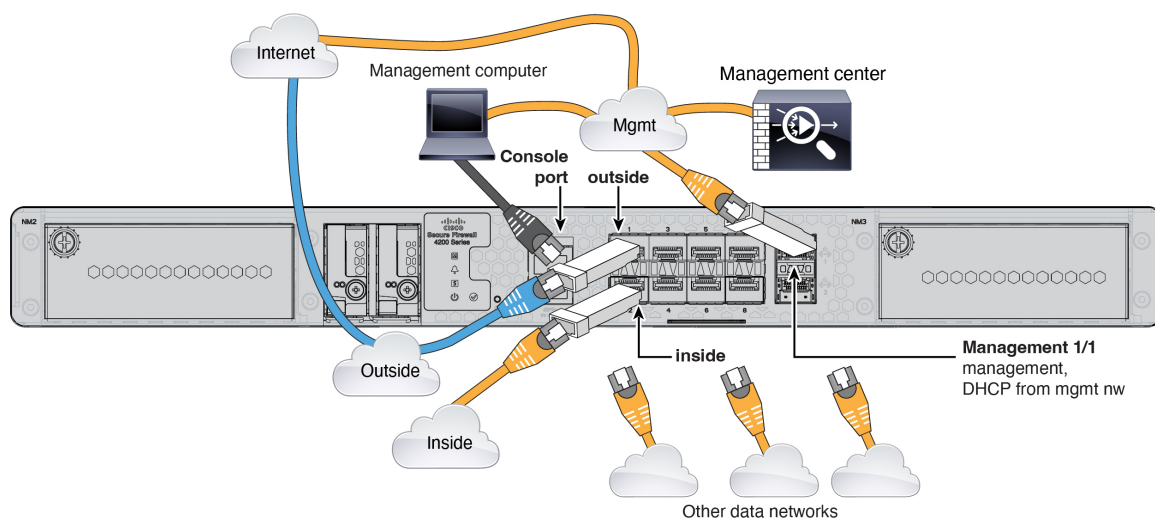
连接防火墙，然后将防火墙注册到管理中心。

- 连接防火墙的电缆，第 9 页
- 初始配置：CLI，第 10 页
- 向管理中心注册防火墙，第 11 页

连接防火墙的电缆

将管理中心 连接到专用管理 1/1 接口。管理网络需要访问互联网以进行更新。例如，您可以通过防火墙本身将管理网络与互联网连接（如连接到内部网络）。

- 获取控制台电缆-默认情况下，防火墙不随附控制台电缆，因此您需要购买第三方USB转RJ-45串行电缆。
- 将 SFP 安装到数据接口端口 - 内置端口是需要 1/10/25-Gb SFP28 模块的 1/10/25-Gb SFP28 端口。
- 有关详细信息，请参阅[硬件安装指南](#)。



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 威胁防御 CLI。请参阅[访问威胁防御 CLI](#)，第 3 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 the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
```

```
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'
```

```
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.

>

步骤 3 识别 管理中心。

configure manager add {主机名 | IPv4_address | IPv6_address | **DONTRESOLVE**} reg_key nat_id

- {hostname | IPv4_address | IPv6_address | **DONTRESOLVE**} - 指定管理中心的 FQDN 或 IP 地址。如果管理中心无法直接寻址，请使用 **DONTRESOLVE**，在这种情况下，防火墙必须具有可访问的 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。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。

示例：

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

向管理中心注册防火墙

将防火墙手动注册到 管理中心。

过程

步骤 1 登录管理中心。

a) 输入以下 URL。

`https://fmc_ip_address`

b) 输入您的用户名和密码。

c) 点击**登录**。

步骤 2 选择**设备 > 设备管理**。

步骤 3 从添加下拉列表中，选择**添加设备**。

图 9: 使用注册密钥添加设备

Add Device ?

☐ CDO Managed Device

Host:

Display Name:

Registration Key:*

Group:

Access Control Policy:*

Smart Licensing

Note: All virtual Firewall Threat Defense devices require a performance tier license. Make sure your Smart Licensing account contains the available licenses you need. It's important to choose the tier that matches the license you have in your account. Click [here](#) for information about the Firewall Threat Defense performance-tiered licensing. Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.

Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):

☒ Carrier
☒ Malware Defense
☒ IPS
☒ URL

Advanced

Unique NAT ID:

☒ Transfer Packets

Cancel Register

设置以下参数:

- **主机 (Host)** - 输入要添加的防火墙的 IP 地址或主机名 (如果可用)。如果不可用, 请将此字段留空。
- **显示名称 (Display Name)** - 输入要在 管理中心 中显示的防火墙名称。之后将无法更改该名称。
- **注册密钥 (Registration Key)** - 输入您在防火墙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[配置访问控制规则](#)，第 29 页。

图 10: 新建策略

New Policy

Name:
ftd-ac-policy

Description:

Select Base Policy:
None

Default Action:
☒ Block all traffic
☐ Intrusion Prevention
☐ Network Discovery

Cancel Save

- **智能许可**—为要部署的功能分配所需的智能许可证。**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)** - 指定您在防火墙初始配置中指定的 NAT ID。
- **传输数据包 (Transfer Packets)** - 选中**传输数据包 (Transfer Packets)** 复选框，以便对于每个入侵事件，设备将数据包传输到 管理中心 进行检查。

默认情况下，此选项已启用。对于每个入侵事件，设备会将事件信息和触发事件的数据包发送到 管理中心 进行检查。如果禁用此选项，则只会向 管理中心 发送事件信息，而不会发送数据包。

步骤 4 点击 **Register**。

如果 威胁防御注册失败，请检查以下项：

- **Ping** - 访问 威胁防御 CLI（请参阅[访问威胁防御 CLI](#)，第 3 页），然后使用以下命令 ping 管理中心 IP 地址：
ping system fmc_ip_address

如果 ping 不成功，使用 **show network** 命令检查网络设置。如果需要更改防火墙管理 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。可以在防火墙上使用 **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>。



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。

- [配置接口，第 17 页](#)
- [配置 DHCP 服务器，第 22 页](#)
- [添加默认路由，第 23 页](#)
- [配置 NAT，第 26 页](#)
- [配置访问控制规则，第 29 页](#)
- [部署配置，第 31 页](#)

配置接口

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。它还会为内部 Web 服务器添加一个 DMZ 接口。

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)。

图 11: 接口

Device Routing Interfaces Inline Sets DHCP VTEP								
Search by name Sync Device Add Interfaces								
Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
Management0/0	management	Physical				Disabled	Global	
GigabitEthernet0/0		Physical				Disabled		
GigabitEthernet0/1		Physical				Disabled		
GigabitEthernet0/2		Physical				Disabled		
GigabitEthernet0/3		Physical				Disabled		
GigabitEthernet0/4		Physical				Disabled		
GigabitEthernet0/5		Physical				Disabled		
GigabitEthernet0/6		Physical				Disabled		
GigabitEthernet0/7		Physical				Disabled		

步骤 3 要从 40-Gb 或更大的接口创建分支端口，请点击该接口的 **中断** 图标。

如果您已经在配置中使用了全接口，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** 图标。

图 12: “常规”选项卡

Edit Physical Interface

General

IPv4

IPv6

Path Monitoring

Name:

inside

☒ Enabled

☐ Management Only

Description:

Mode:

None

Security Zone:

inside_zone

Interface ID:

GigabitEthernet0/1

MTU:

1500

(64 - 9000)

Priority:

0

(0 - 65535)

Propagate Security Group Tag:

☐

NVE Only:

☐

- a) 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。您可以根据区域或组应用安全策略。例如，配置访问控制策略，使流量可以从内部区域进入外部区域，但不能从外部进入内部区域。

- b) 输入长度最大为 48 个字符的名称 (Name)。

例如，将接口命名为 **inside**。

- c) 选中启用 (Enabled) 复选框。

- d) 将模式 (Mode) 保留为无 (None)。

- 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**

图 13: IPv4 选项卡

Edit Physical Interface

General IPv4 IPv6 Path Monitoring

IP Type:
Use Static IP

IP Address:
192.168.1.1/24

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。

图 14: IPv6 选项卡

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Hardware Configu

Basic Address Prefixes Settings DHCP

Enable IPV6: ☐

Enforce EUI 64: ☐

Link-Local address:

Autoconfiguration: ☒

Obtain Default Route: ☐

- f) 点击**确定 (OK)**。

步骤 5 点击要用于外部的接口的 **编辑** (✎)。

图 15: “常规”选项卡

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Hardware

Name:
outside

☒ Enabled
☐ Management Only

Description:

Mode:
None

Security Zone:
outside_zone

Interface ID:
GigabitEthernet0/0

MTU:
1500
(64 - 9000)

Priority:
0 (0 - 65535)

Propagate Security Group Tag: ☐

NVE Only:
☐

- 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。

如果预配置了外部接口，则其余字段为可选。

- b) 输入长度最大为 48 个字符的 **Name**。

例如，将接口命名为 **outside**。

- c) 选中**启用 (Enabled)**复选框。

- d) 将模式 (Mode) 保留为无 (None)。

- 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。

图 16: IPv4 选项卡

Edit Physical Interface

General IPv4 IPv6 Path Monitoring

IP Type:
Use DHCP

Obtain default route using DHCP: ☒

DHCP route metric:
1

(1 - 255)

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

图 17: IPv6 选项卡

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Hardware Configuration

Basic Address Prefixes Settings DHCP

Enable IPV6: ☐

Enforce EUI 64: ☐

Link-Local address:

Autoconfiguration: ☒

Obtain Default Route: ☐

f) 点击**确定 (OK)**。

步骤 6 例如，配置 DMZ 接口以托管 Web 服务器。

- 点击您要使用的接口的 **编辑** (🔗)。
- 从**安全区域 (Security Zone)** 下拉列表选择一个现有的 DMZ 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 **dmz_zone** 的区域。

- 输入长度最大为 48 个字符的**名称 (Name)**。

例如，将接口命名为 **dmz**。

- 选中**启用 (Enabled)** 复选框。
- 将**模式 (Mode)** 保留为**无 (None)**。
- 点击 **IPv4** 和/或 **IPv6** 选项卡并配置所需的 IP 地址。
- 点击**确定 (OK)**。

步骤 7 点击**保存 (Save)**。

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)。

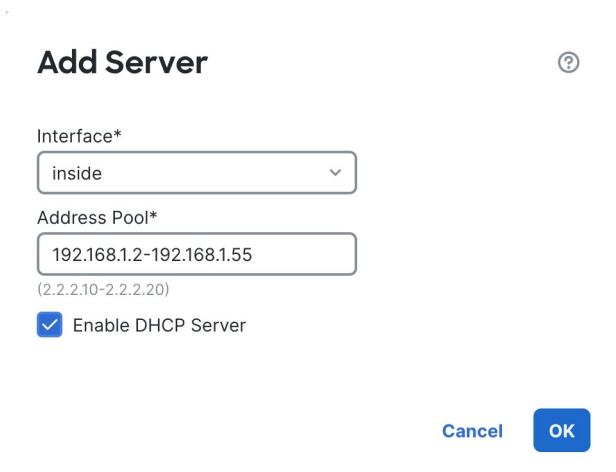
图 18: DHCP 服务器

The screenshot displays the DHCP Server configuration page. The left sidebar shows the navigation menu with 'DHCP Server' selected. The main content area includes the following fields and sections:

- Ping Timeout:** A text input field with the value '50' and a range '(10 - 10000 ms)'.
- Lease Length:** A text input field with the value '3600' and a range '(300 - 10,48,575 sec)'.
- Auto-Configuration:** A checkbox that is currently unchecked.
- Interface:** A dropdown menu.
- Override Auto Configured Settings:**
 - Domain Name:** A text input field.
 - Primary DNS Server:** A dropdown menu.
 - Secondary DNS Server:** A dropdown menu.
 - Primary WINS Server:** A dropdown menu.
 - Secondary WINS Server:** A dropdown menu.
- Server/Advanced tabs:** The 'Server' tab is selected and highlighted with a red box.
- + Add button:** A button to add a new DHCP server, highlighted with a red box.
- Table:** A table with columns 'Interface', 'Address Pool', and 'Enable DHCP Server'. It currently shows 'No records to display'.

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

图 19: 添加服务器



The image shows a dialog box titled "Add Server" with a help icon (question mark) in the top right corner. It contains three main fields: "Interface*" with a dropdown menu showing "inside"; "Address Pool*" with a text box containing "192.168.1.2-192.168.1.55" and a smaller text "(2.2.2.10-2.2.2.20)" below it; and a checkbox labeled "Enable DHCP Server" which is checked. At the bottom right, there are "Cancel" and "OK" buttons.

- 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)。

添加默认路由

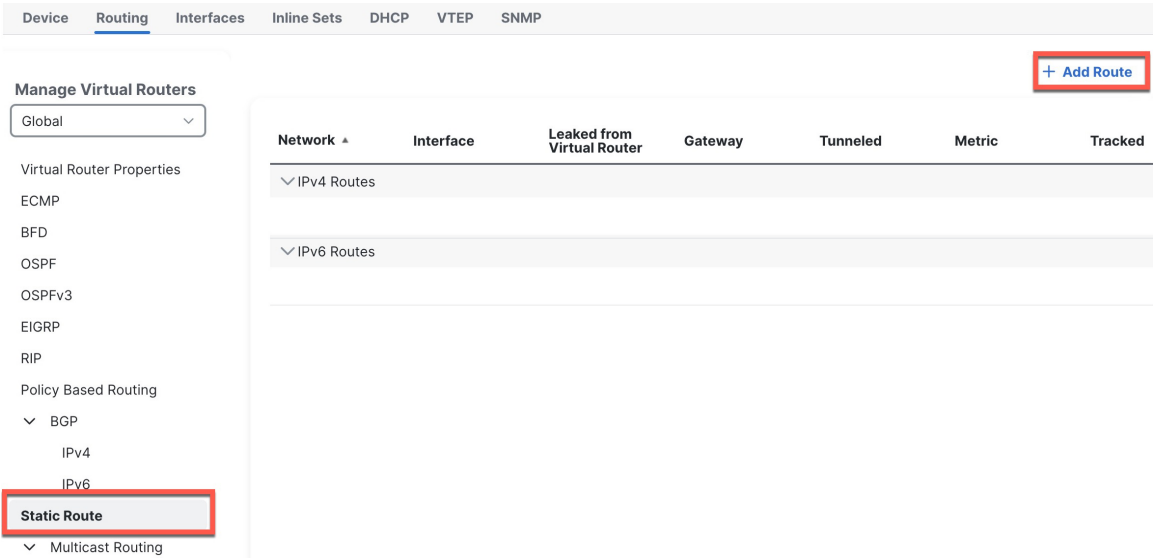
默认路由通常指向可从外部接口访问的上游路由器。如果您从 DHCP 获取外部地址，则设备可能已经收到了默认路由。如果需要手动添加路由，则遵照此程序执行。

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 > 静态路由。

图 20: 静态路由



如果从 DHCP 服务器收到默认路由，它将显示在此表中。

步骤 3 点击添加路由 (Add Route)，然后设置以下选项。

图 21: 添加静态路由配置

Add Static Route Configuration

Type: ☒ IPv4 ☐ IPv6

Interface*: outside

(Interface starting with this icon signifies it is available for route leak)

Available Network +

Search

any-ipv4
gateway
IPv4-Benchmark-Tests
IPv4-Link-Local
IPv4-Multicast
IPv4-Private-10.0.0.0-8

Add

Selected Network

any-ipv4

Gateway*: gateway +

Metric: 1

(1 - 254)

Tunneled: ☐ (Used only for default Route)

Route Tracking: +

Cancel OK

- **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。

步骤 4 点击确定 (**OK**)。

路由即已添加至静态路由表。

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 22: 新建策略

New Policy

Name:
FTD_policy

Description:

Targeted Devices
Select devices to which you want to apply this policy.

Available Devices and Templates
192.168.0.124
192.168.0.155

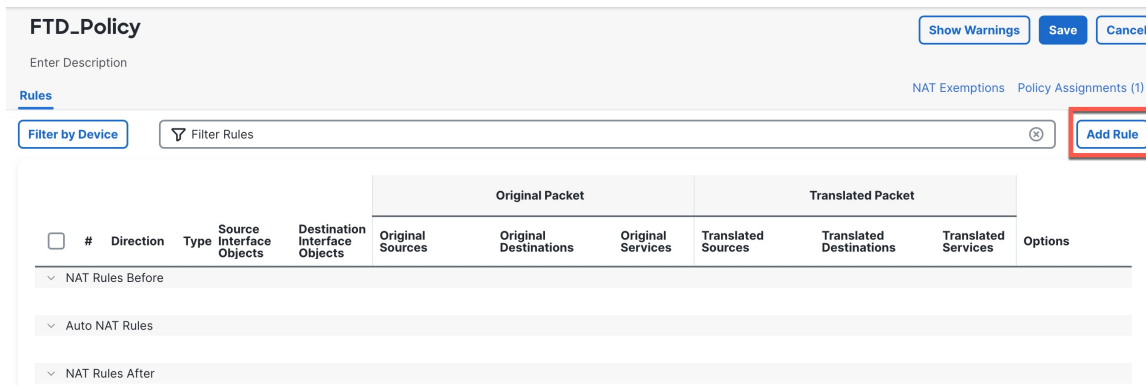
Selected Devices and Templates
192.168.0.124
192.168.0.155

Add to Policy

Cancel Save

策略即已添加 管理中心。您仍然需要为策略添加规则。

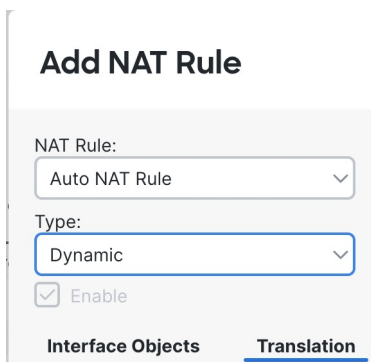
图 23: NAT 策略



步骤 3 点击添加规则 (Add Rule)。

步骤 4 配置基本规则选项：

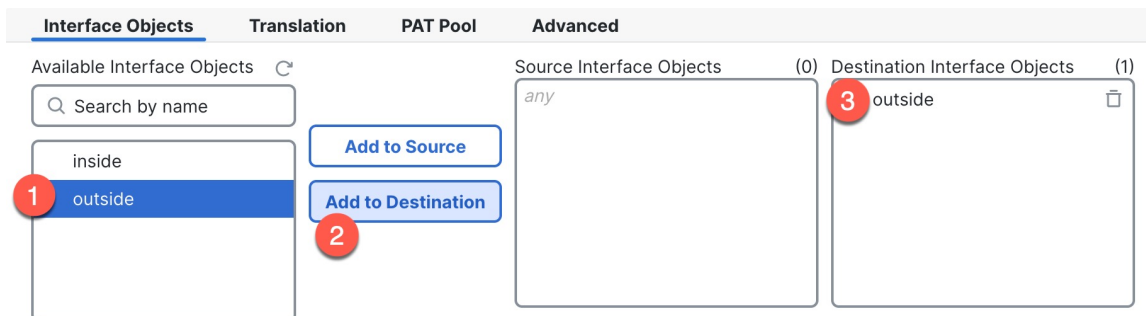
图 24: 基本规则选项



- 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 25: 接口对象



步骤 6 在转换 (Translation) 页面上配置以下选项：

图 26: 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 27: 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 > 访问控制标题 > 访问控制**，然后点击分配给设备的访问控制策略对应的 **编辑** (✎)。

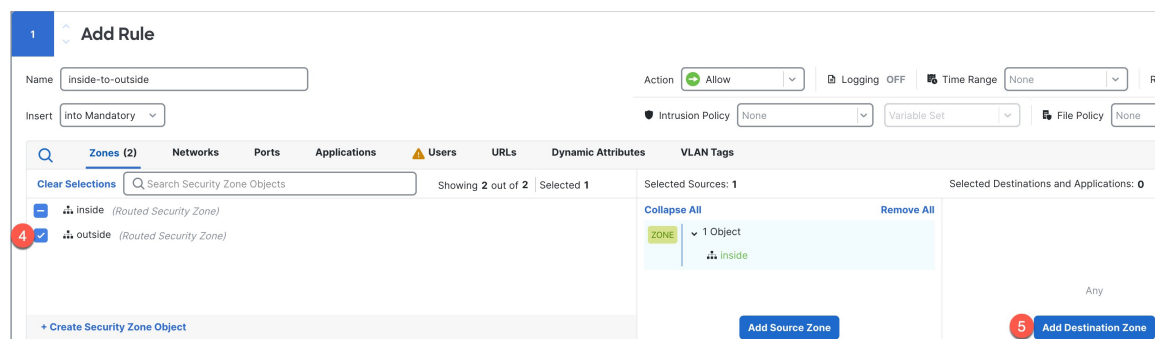
步骤 2 点击**添加规则 (Add Rule)** 并设置以下参数。

图 28: 源区域

The screenshot shows the 'Add Rule' configuration page. The 'Name' field is set to 'inside-to-outside'. The 'Action' is set to 'Allow'. The 'Intrusion Policy' is set to 'None'. The 'Zones (1)' tab is selected, showing a list of zones: 'inside (Routed Security Zone)' and 'outside (Routed Security Zone)'. The 'inside' zone is selected. The 'Add Source Zone' button is highlighted with a red circle and the number 3.

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 29: 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 30: 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。

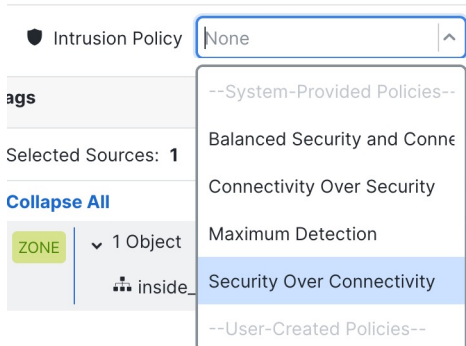
- **身份** - 默认情况下不应用身份。在允许访问控制策略处理流量之前，可以要求用户进行身份验证。

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。管理中心 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 31: 系统提供的入侵策略

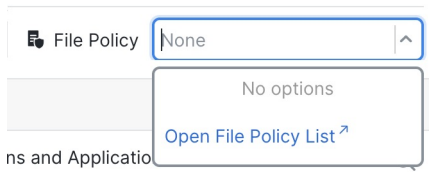


b) 从列表中选择一个系统提供的策略。

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 32: 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《[Cisco Secure Firewall 设备管理器配置指南](#)》。

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)**。

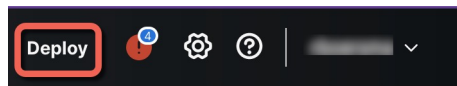
部署配置

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

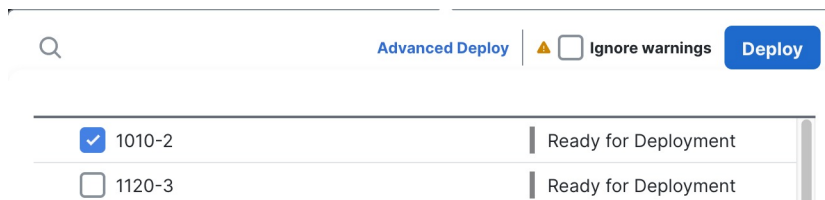
步骤 1 点击右上方的部署 (Deploy)。

图 33: 部署



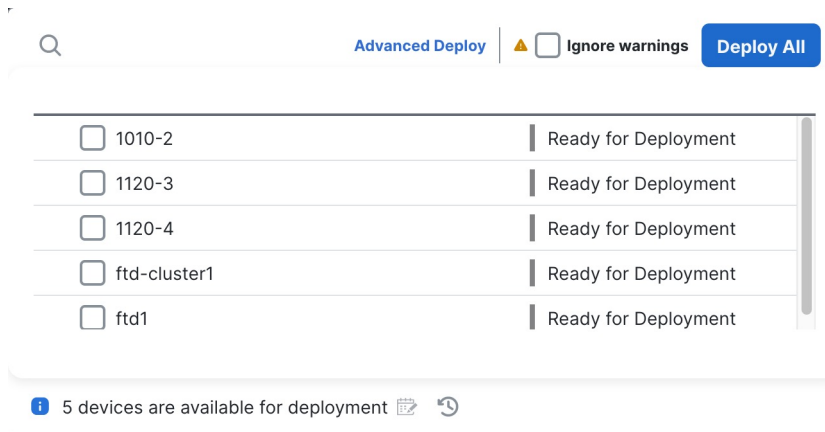
步骤 2 要快速部署，请选中特定设备，然后点击部署 (Deploy)。

图 34: 部署所选



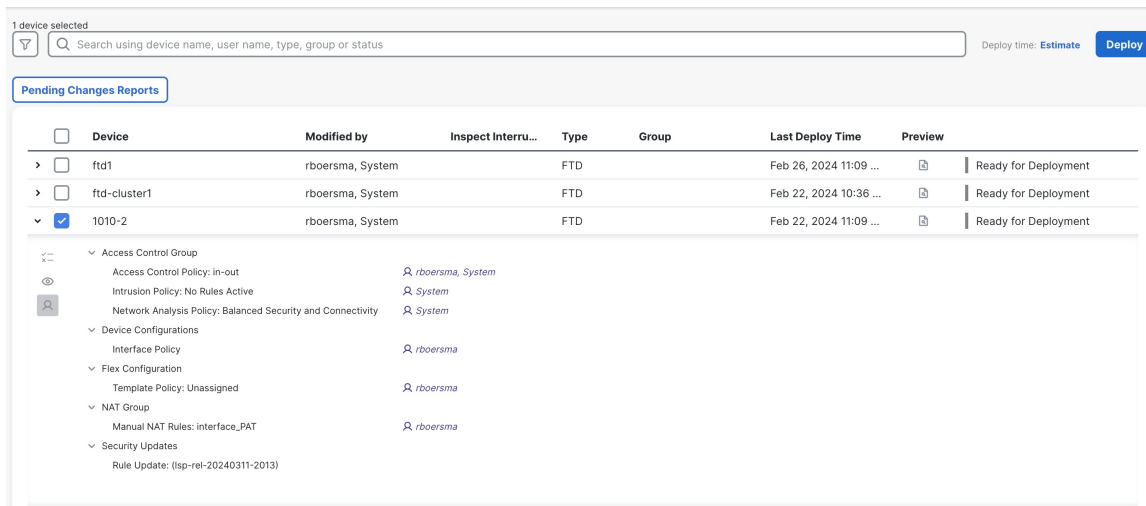
或者，点击全部部署 (Deploy All) 以部署到所有设备。

图 35: 全部部署



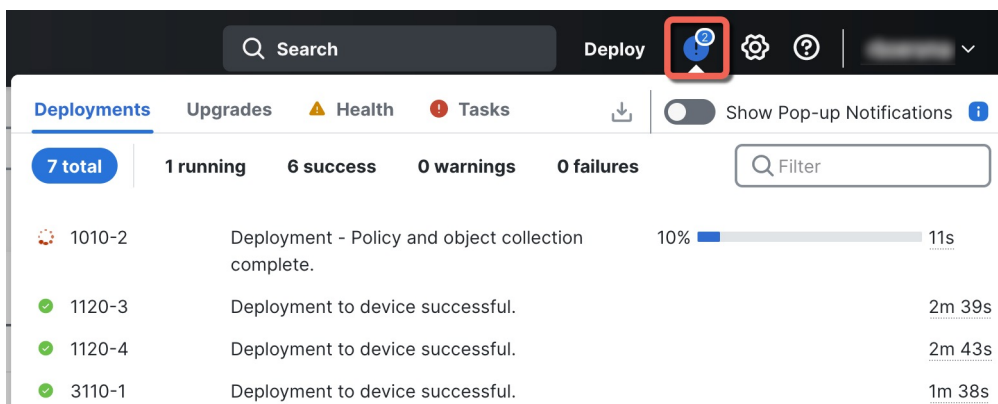
否则，对于其他部署选项，请点击高级部署 (Advanced Deploy)。

图 36: 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 37: 部署状态



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。