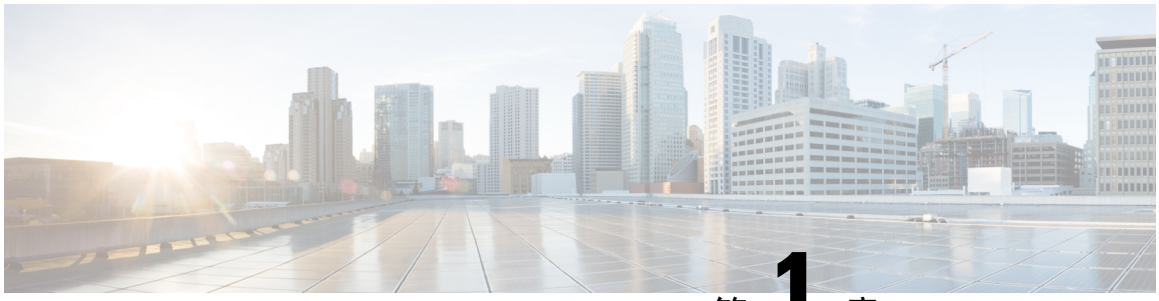
Cisco Secure Firewall 4200 威胁防御入门：云交付的防火墙管理中心

上次修改日期: 2025 年 1 月 20 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

在分支安装防火墙，并使用 安全云控制（以前称为 Cisco Defense Orchestrator）在外部接口上对其进行管理。

注释 集群不支持外部管理。在这种情况下，请使用管理接口进行 安全云控制访问。本指南专门介绍外部管理，但您可以参阅使用 思科安全云控制 中的云交付的防火墙管理中心来管理 Cisco Secure Firewall Threat Defense，以了解如何使用管理界面进行管理。另请参阅该指南，了解多实例部署。

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

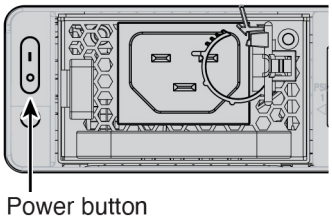
为防火墙提供可靠的电源（例如，使用不间断电源 (UPS)）非常重要。未事先关闭就断电可能会导致严重的文件系统损坏。后台始终有许多进程在运行，因此断电会使得系统无法正常关闭。

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。

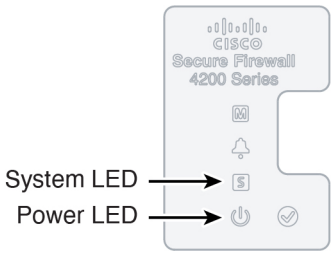
步骤 2 使用位于机箱背面电源线旁边的摇杆电源开关打开电源。

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。

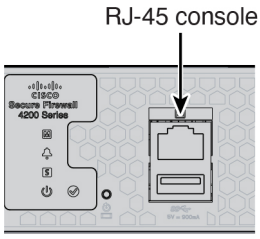
安装的哪个应用程序：威胁防御还是 ASA？

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

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。如果需要一直登录，请参阅访问威胁防御 CLI，第 3 页。

```
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。

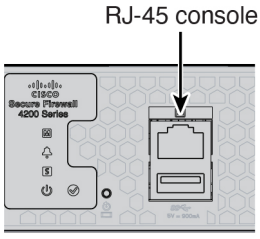
访问威胁防御 CLI

您可能需要访问 CLI 进行配置或故障排除。

过程

步骤 1 连接到控制台端口。

图 *4:* 控制台端口



步骤 2 连接到FXOS。使用 **admin** 用户名和密码（默认值为 **Admin123**）登录 CLI。第一次输入登录时，系统会提示您更改密码。

```
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 切换到 威胁防御 CLI。

注释
如果要使用 设备管理器 进行初始设置或使用 零接触调配，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。

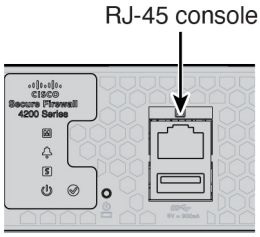
我应该运行什么版本？

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。

对于低接触调配，当您载入设备时，请务必为**密码重置 (Password Reset)** 区域选择 **否 (No)**，因为您已设置密码。

d) 关闭防火墙。请参阅（必要时）关闭防火墙电源，第 8 页。

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。

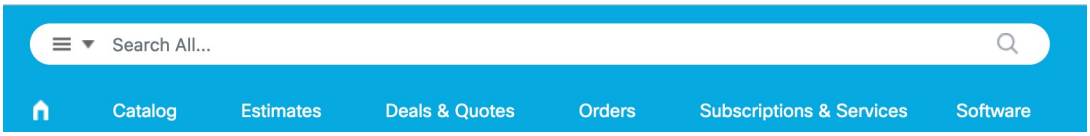
如果尚未注册，请向智能软件管理器注册 安全云控制。注册需要您在智能软件管理器中生成注册令牌。有关详细说明，请参阅 安全云控制 文档。

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。

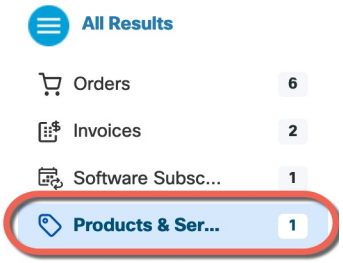
- Essentials：
  - 自动包含

- 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。

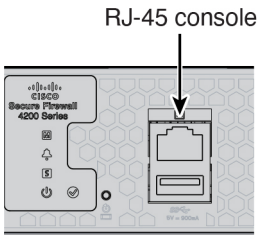
在 CLI 关闭防火墙电源

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。

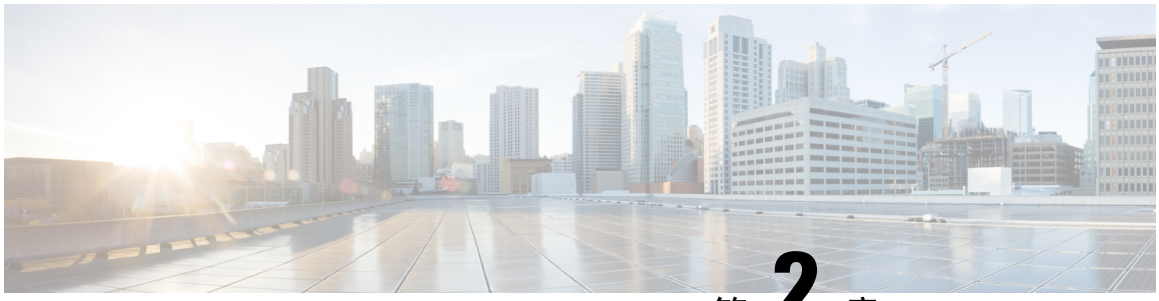
步骤 2 如果您与防火墙建立了控制台连接，请在防火墙关闭时留意系统提示。关闭完成后，您将看到以下提示。

```
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。



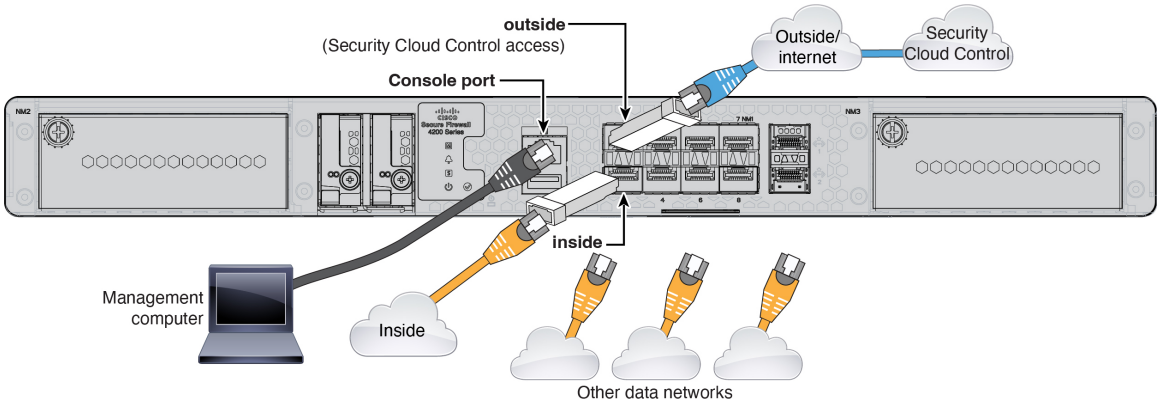
第 2 章

连接和载入防火墙

连接防火墙并载入到安全云控制。

连接防火墙的电缆

- 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。



通过手动调配载入防火墙

使用 CLI 注册密钥载入防火墙。

过程

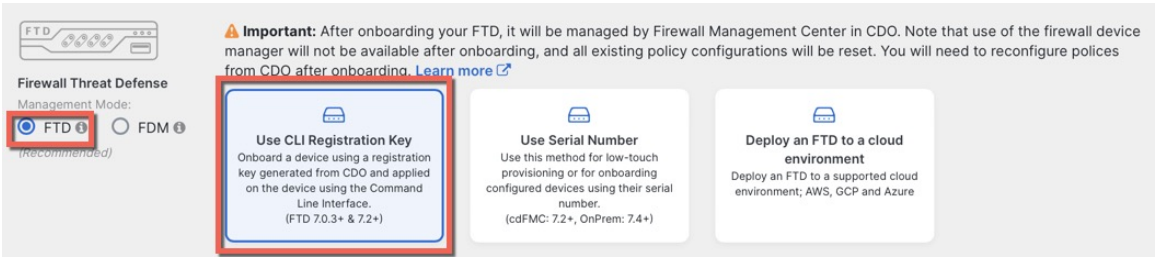
步骤 1 在 安全云控制 导航窗格中，点击 **安全设备 (Security Devices)**，然后点击蓝色加号按钮（  ）以便**载入**设备。

步骤 2 点击 **FTD** 磁贴。

步骤 3 在 **管理模式**下，确保选择 **FTD** 。

步骤 4 选择**使用 CLI 注册密钥 (Use CLI Registration Key)** 作为激活方法。

图 *9:* 使用 *CLI* 注册密钥

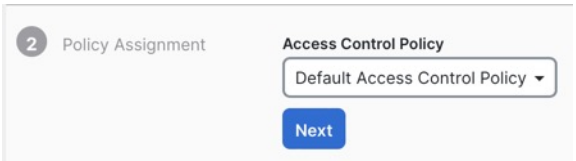


步骤 5 输入**设备名称 (Device Name)**，然后点击**下一步 (Next)**。

图 *10:* 设备名称

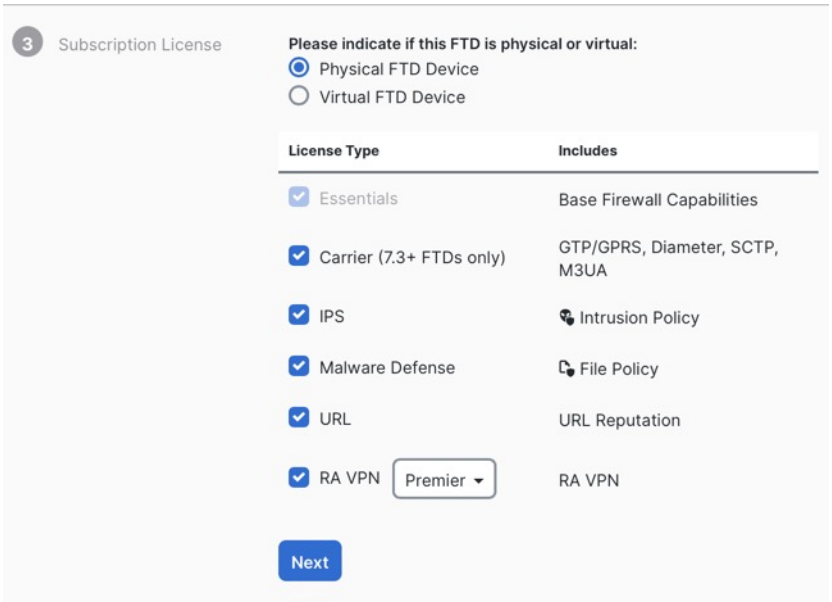
步骤 6 对于**策略分配 (Policy Assignment)**，请使用下拉菜单为设备选择访问控制策略。如果未配置策略，请选择**默认访问控制策略 (Default Access Control Policy)**。

图 *11:* 访问控制策略



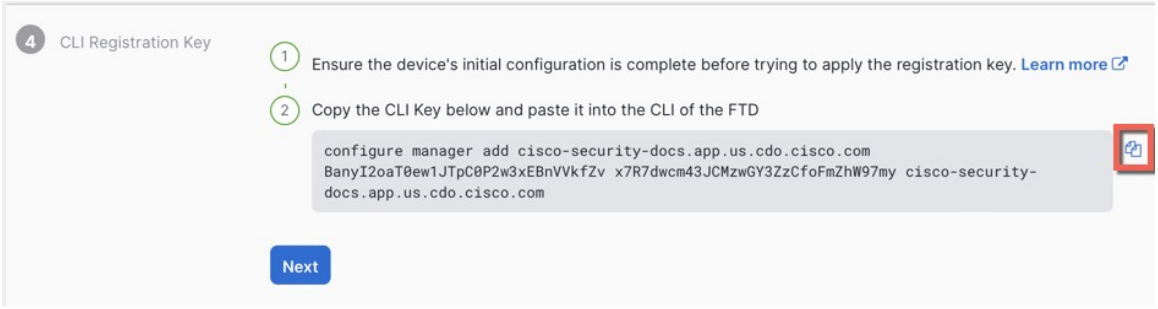
步骤 7 对于**订用许可证 (Subscription License)**，请点击**物理 FTD 设备 (Physical FTD Device)** 单选按钮，然后选中要启用的每个功能许可证。点击**下一步**。

图 *12:* 订用许可证



步骤 8 对于 **CLI 注册密钥**，安全云控制 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。

图 *13: CLI* 注册密钥



configure manager add 安全云控制*_hostname registration_key nat_id display_name*

完成启动脚本后，在 威胁防御 CLI 中复制此命令。请参阅初始配置：CLI，第 14 页。

示例：

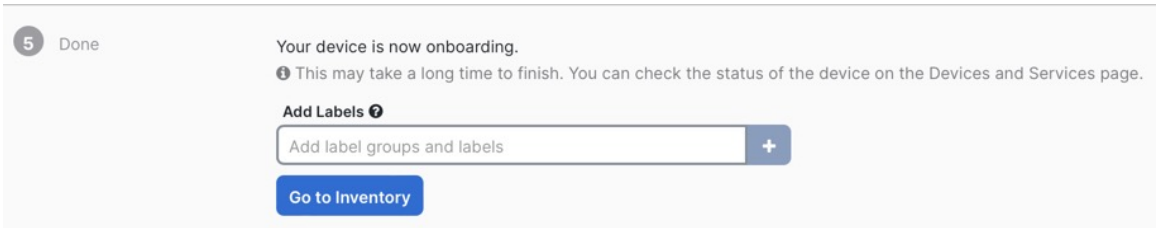
CLI 设置的命令示例：

```
configure manager add account1.app.us.scc.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.scc.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**安全设备 (Security Devices)** 页面进行排序和过滤。输入标签，然后选择蓝色加号按钮（ + ）。标签会在设备载入 安全云控制后应用到设备。

图 *14:* 完成



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**。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。

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

指南：选择**手动**。使用外部接口访问管理器时，不支持DHCP。确保此接口与管理器访问接口位于不同的子网上，以防止出现路由问题。

```
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]:
```

指南：将网关设置为 **data-interfaces**。此设置可将管理流量转发到背板上，以便通过外部接口进行路由。

```
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
```

指南：设置管理接口 DNS 服务器。这些服务器很可能与您稍后设置的外部接口 DNS 服务器一致，因为它们都是从外部接口访问的。

```
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'
```

指南：输入 **routed**。只有路由防火墙模式支持外部管理器访问。

```
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 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。

手动 IP 地址

```
> 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
```

指南：要在注册后保留外部 DNS 服务器，您需要在 管理中心 中重新配置 DNS 平台设置。

```
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.

>
```

DHCP 的 IP 地址

```
> 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://dwinchester: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.

>
```

步骤 4 使用 安全云控制 生成的 **configure manager add** 命令确定将管理此 威胁防御 的 安全云控制。请参阅通过手动调配载入防火墙，第 11 页以生成命令。

示例：

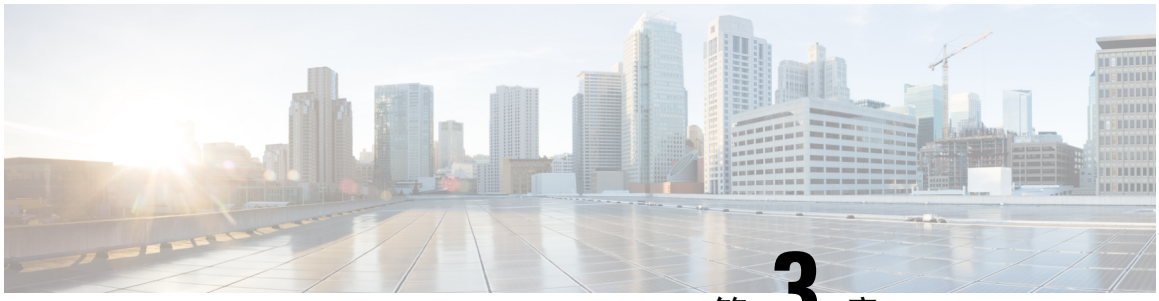
```
> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
Manager successfully configured.
```

步骤 5 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。



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 19 页
- 配置 DHCP 服务器， 第 23 页
- 配置 NAT， 第 24 页
- 配置访问控制规则， 第 27 页
- 在外部接口上启用 SSH， 第 30 页
- 部署配置， 第 31 页

配置接口

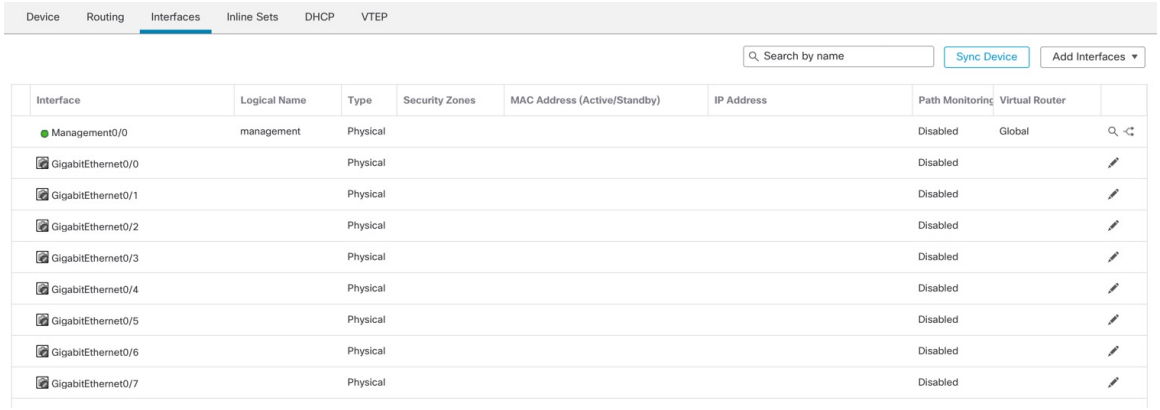
以下示例使用 DHCP 在接口内部配置了一个路由模式（含静态地址），并在接口外部配置了一个路由模式。它还会为内部 Web 服务器添加一个 DMZ 接口。

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 *15:* 接口

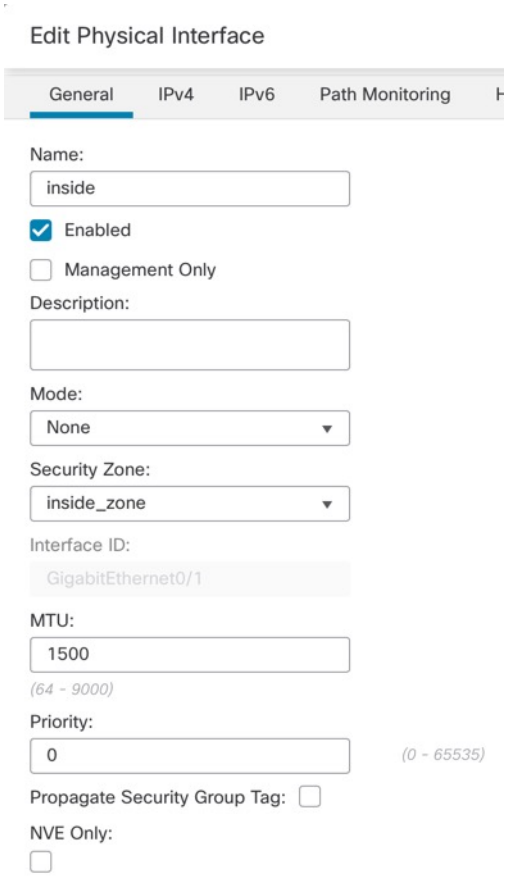


步骤 3 要从 40-Gb 或更大的接口创建分支端口，请点击该接口的 **中断** 图标。

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 *16:* “常规”选项卡



a) 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。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。

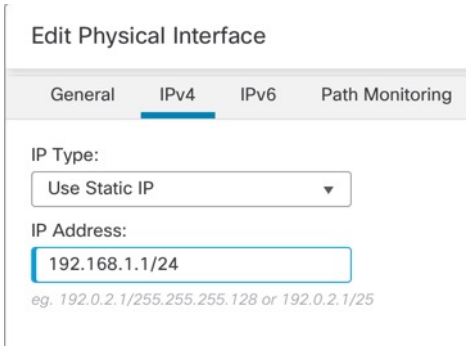
d) 将**模式 (Mode)** 保留为**无 (None)**。

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。

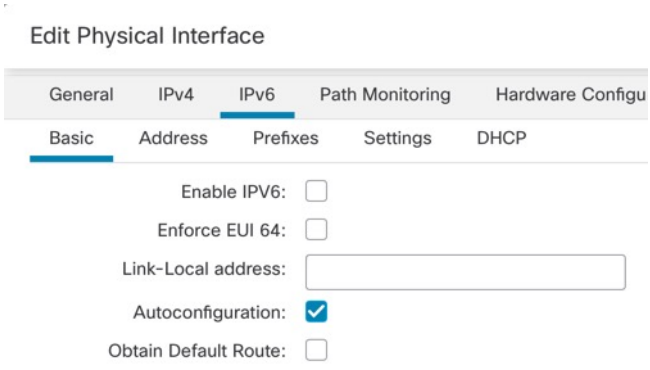
  例如，输入 **192.168.1.1/24**

  图 ***17: IPv4*** 选项卡



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

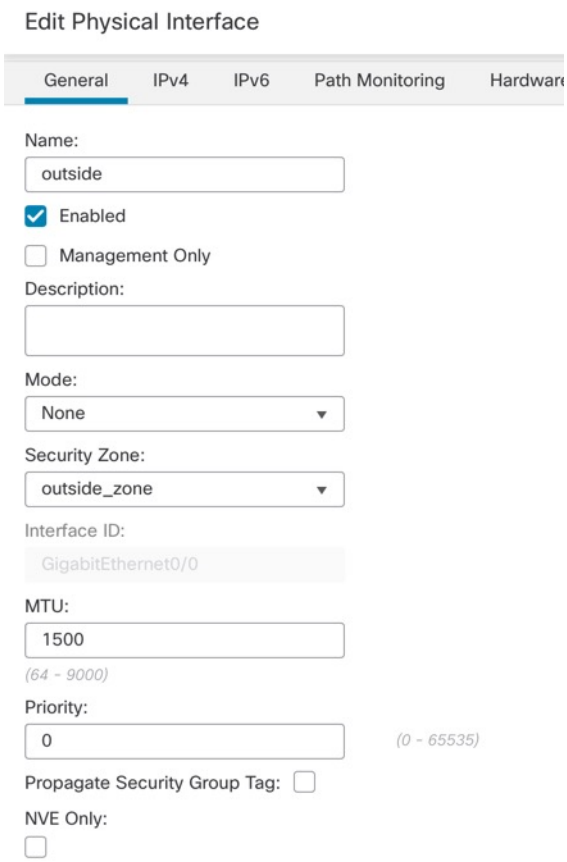
  图 ***18: IPv6*** 选项卡



f) 点击**确定 (OK)**。

步骤 5 点击要用于外部的接口的 **编辑** (✎)。

图 *19:*“常规”选项卡



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。

您不应更改任何其他基本设置，因为这样做会中断 管理中心 管理连接。

b) 点击**确定 (OK)**。

步骤 6 例如，配置 DMZ 接口以托管 Web 服务器。

a) 点击您要使用的接口的 **编辑** (✎)。

b) 从**安全区域 (Security Zone)** 下拉列表中选择一个现有的 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。

c) 输入长度最大为 48 个字符的**名称 (Name)**。

例如，将接口命名为 **dmz**。

d) 选中**启用 (Enabled)** 复选框。

e) 将**模式 (Mode)** 保留为**无 (None)**。

f) 点击 **IPv4** 和/或 **IPv6** 选项卡并配置所需的 IP 地址。
g) 点击**确定 (OK)**。

步骤 7 点击**保存 (Save)**。

配置 DHCP 服务器

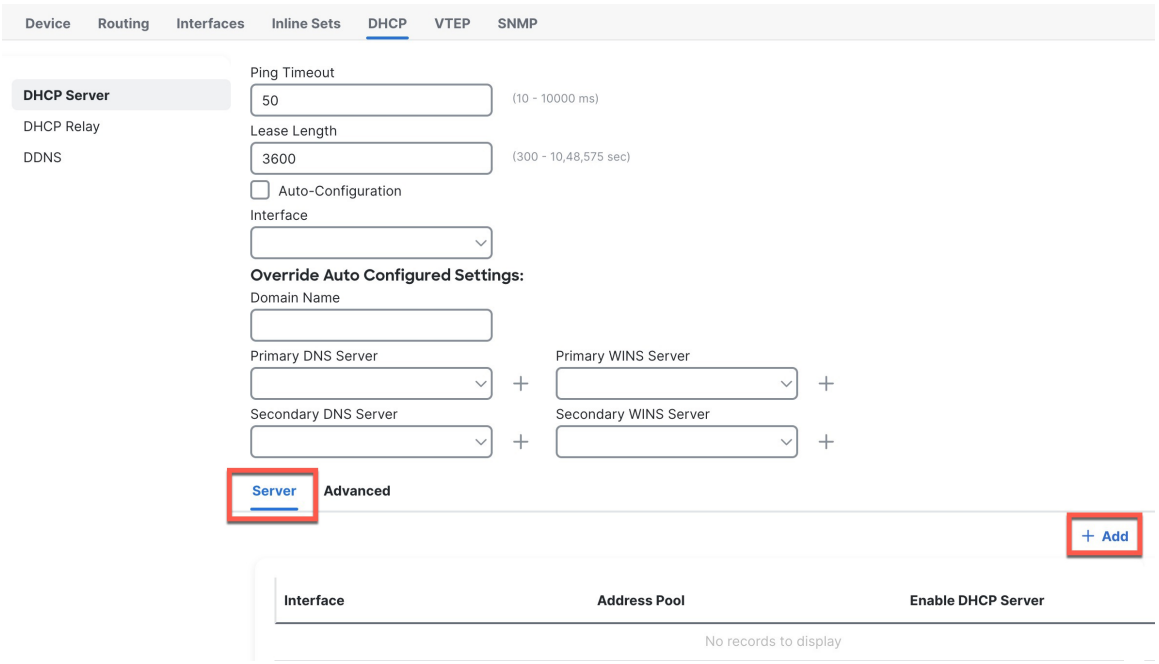
如果希望客户端使用 DHCP 从防火墙获取 IP 地址，请启用 DHCP 服务器。

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** ()。

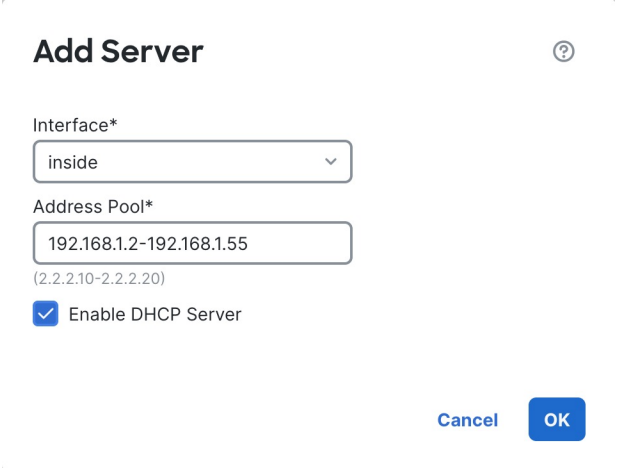
步骤 2 选择 **DHCP** > **DHCP 服务器 (DHCP Server)**。

图 *20: 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 *21:* 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

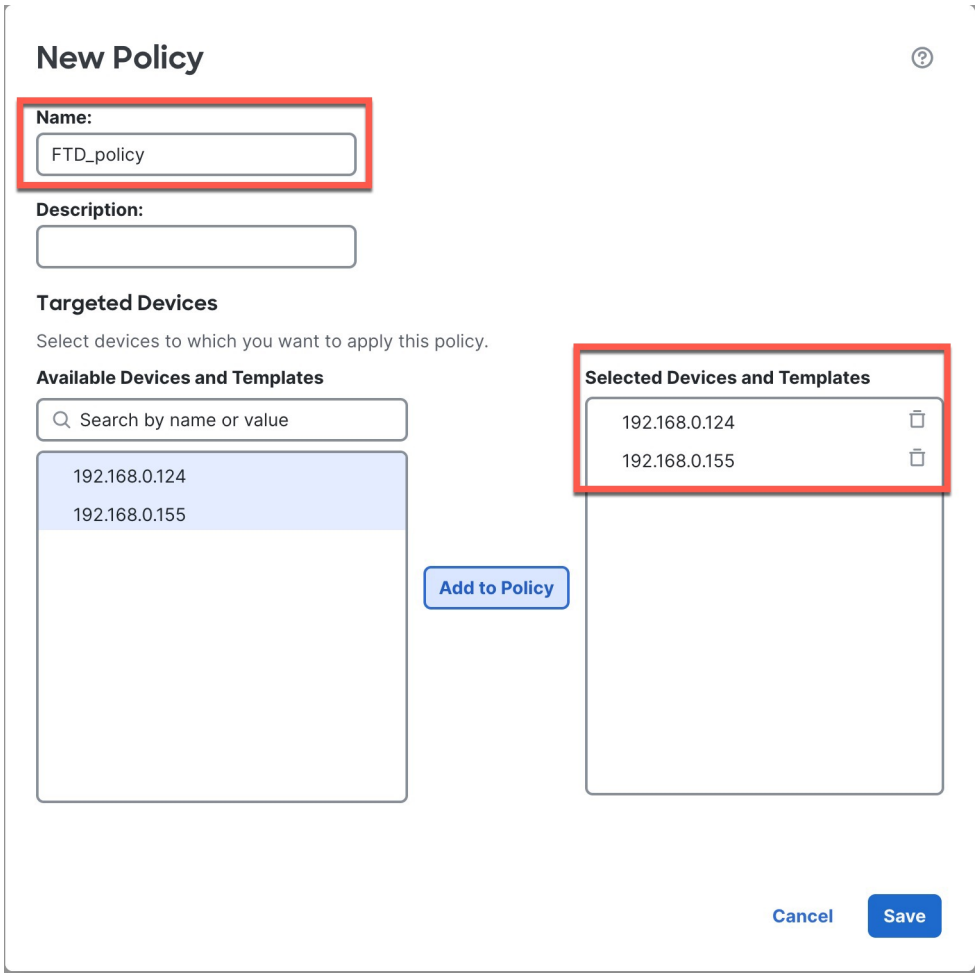
此步骤将为内部客户端创建一条 NAT 规则，以便将内部地址转换为外部接口 IP 地址上的端口。这类 NAT 规则称为接口端口地址转换 *(PAT)*。

过程

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

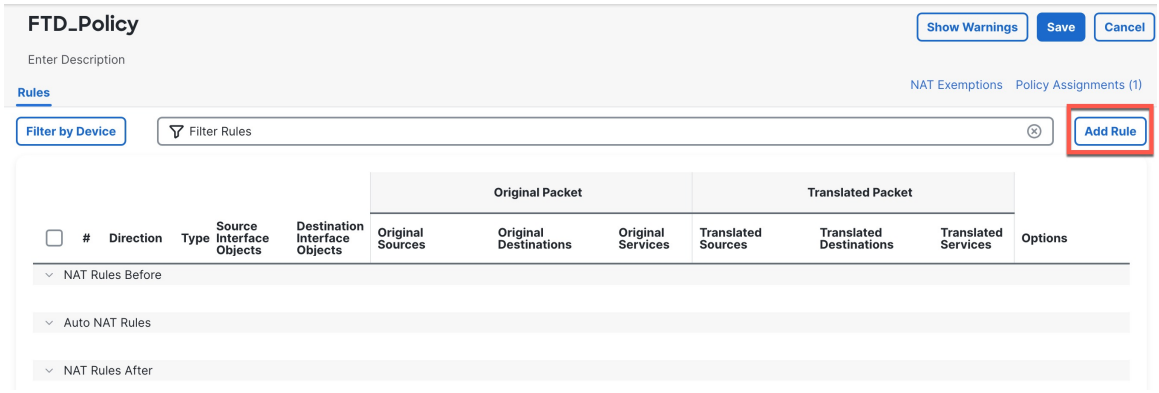
步骤 2 为策略命名，选择要使用策略的设备，然后点击**保存 (Save)**。

图 *22:* 新建策略



策略即已添加 管理中心。您仍然需要为策略添加规则。

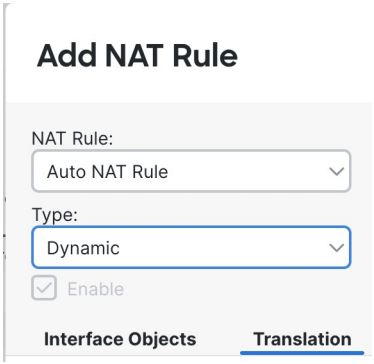
图 *23: NAT* 策略



步骤 3 点击添加规则 **(Add Rule)**。

步骤 4 配置基本规则选项：

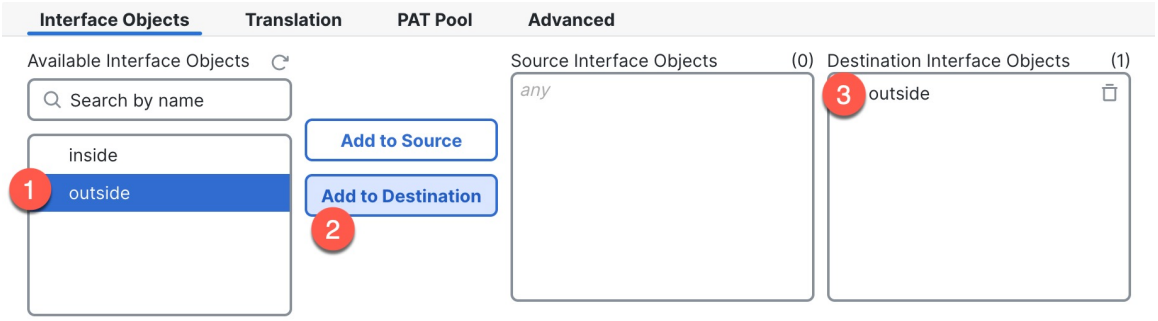
图 *24:* 基本规则选项



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

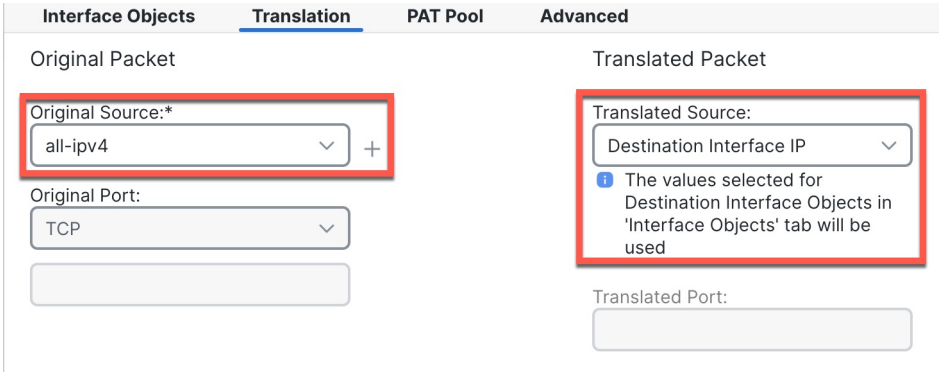
步骤 5 在 **Interface Objects** 页面，将 **Available Interface Objects** 区域中的外部区域添加到 **Destination Interface Objects** 区域。

图 *25:* 接口对象



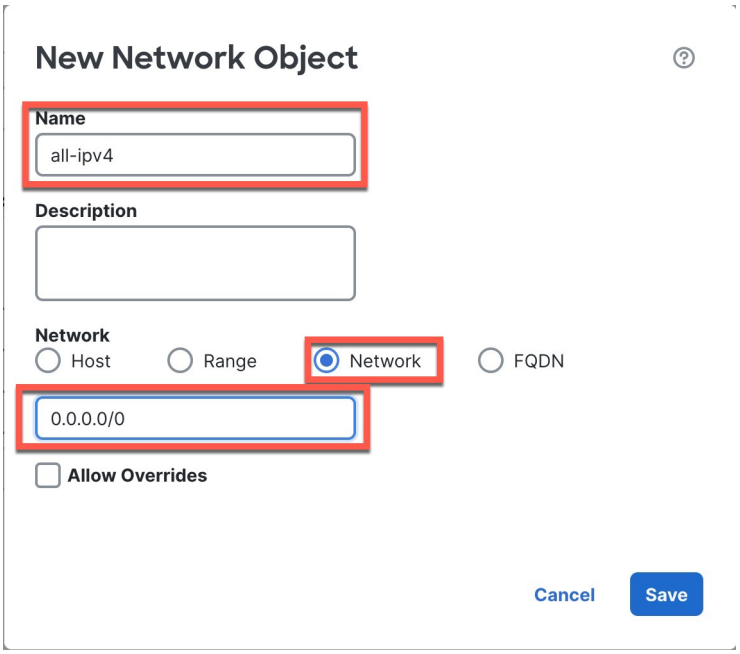
步骤 6 在**转换 (Translation)** 页面上配置以下选项：

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。

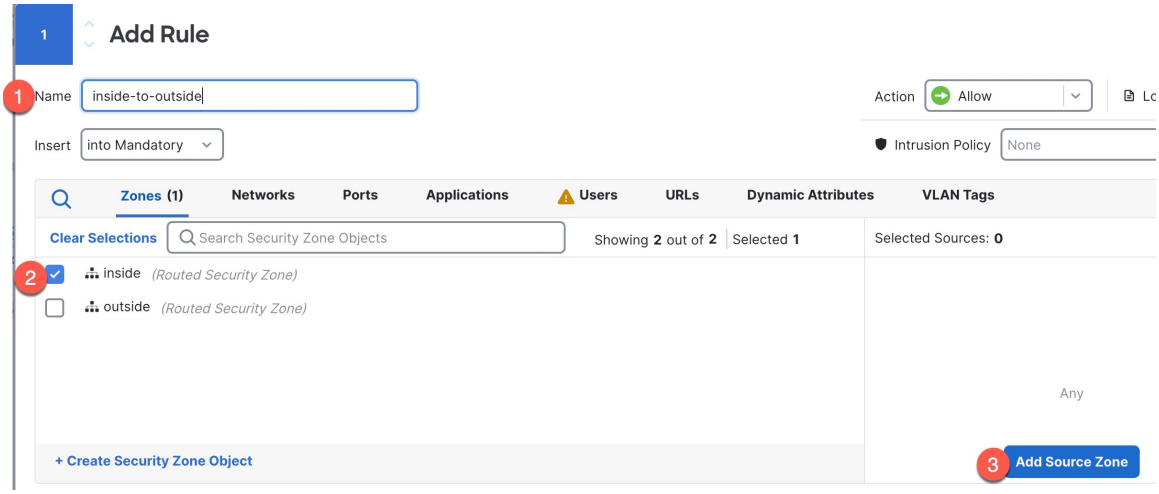
此过程将创建一个访问控制规则，以允许从内部区域到外部区域的所有流量。

过程

步骤 1 选择**策略 (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** (✎)。

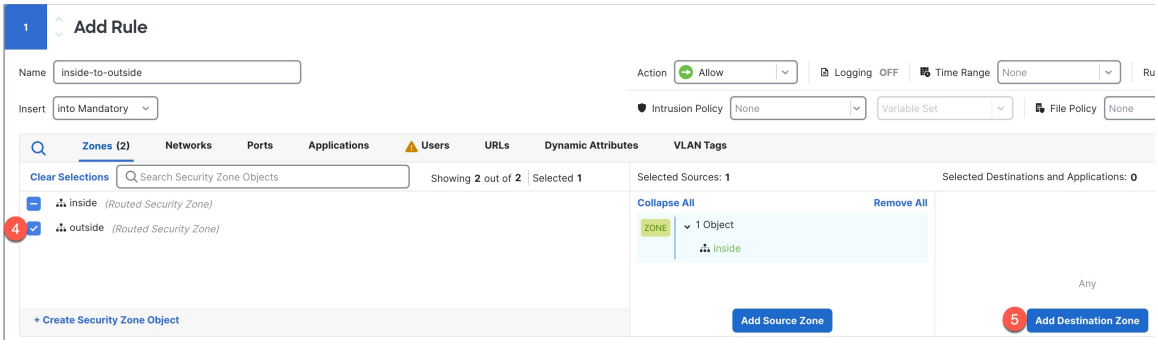
步骤 2 点击**添加规则 (Add Rule)** 并设置以下参数。

图 ***28:*** 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 ***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。

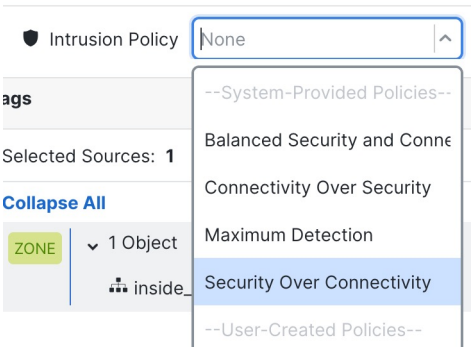
- **身份** - 默认情况下不应用身份。在允许访问控制策略处理流量之前，可以要求用户进行身份验证。

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

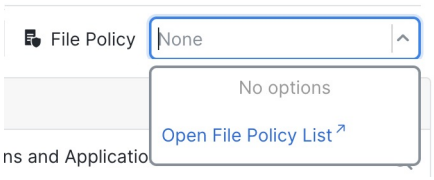


b) 从列表中选择一个系统提供的策略。

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)**。

在外部接口上启用 SSH

本部分介绍如何启用与外部接口的 SSH 连接。

默认情况下，您可以使用在初始设置期间为其配置密码的 **admin** 用户。

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 **SSH 访问 (SSH Access)**。

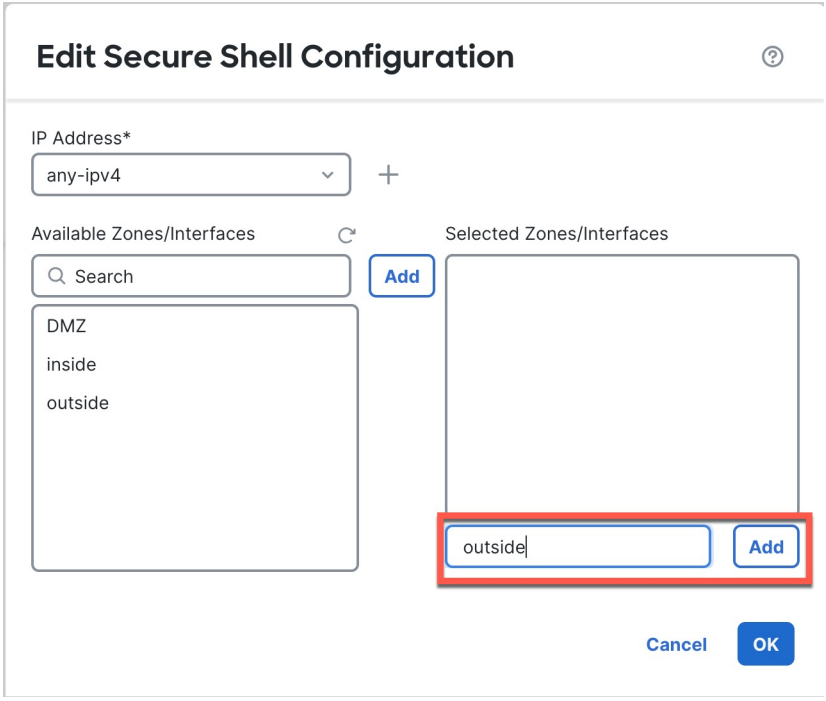
步骤 3 标识允许 SSH 连接的外部接口和 IP 地址。

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。
- **可用区域/接口 (Available Zones/Interfaces)** - 添加外部区域或者在**所选区域/接口 (Selected Zones/Interfaces)** 列表下的字段中键入**外部**接口名称，然后点击**添加 (Add)**。

图 *33:* 在外部接口上启用 ***SSH***



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。

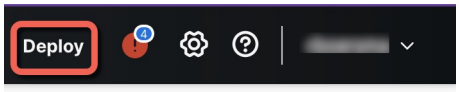
部署配置

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

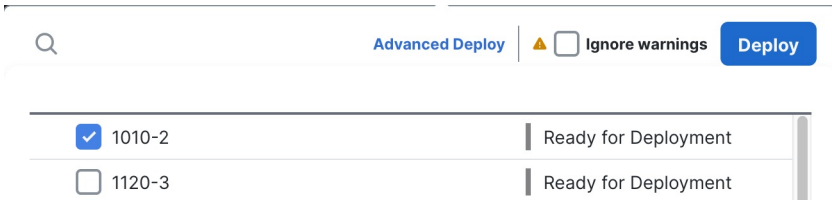
步骤 1 点击右上方的**部署 (Deploy)**。

图 *34:* 部署



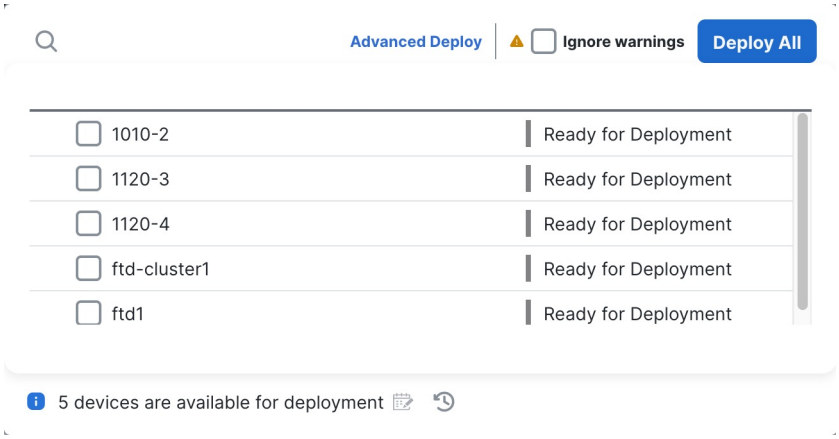
步骤 2 要快速部署，请选中特定设备，然后点击**部署 (Deploy)**。

图 *35:* 部署所选



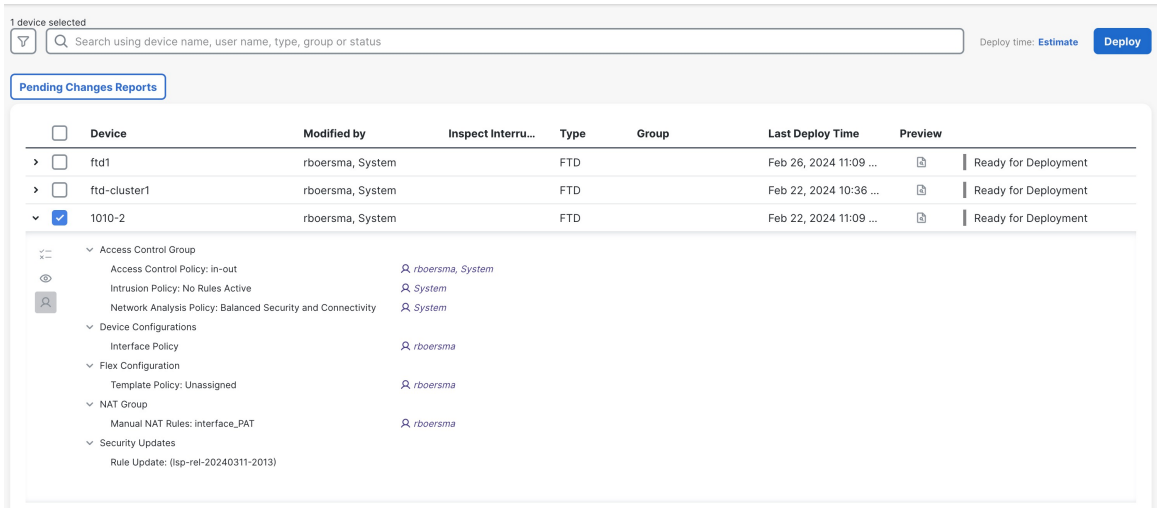
或者，点击**全部部署 (Deploy All)** 以部署到所有设备。

图 *36:* 全部部署



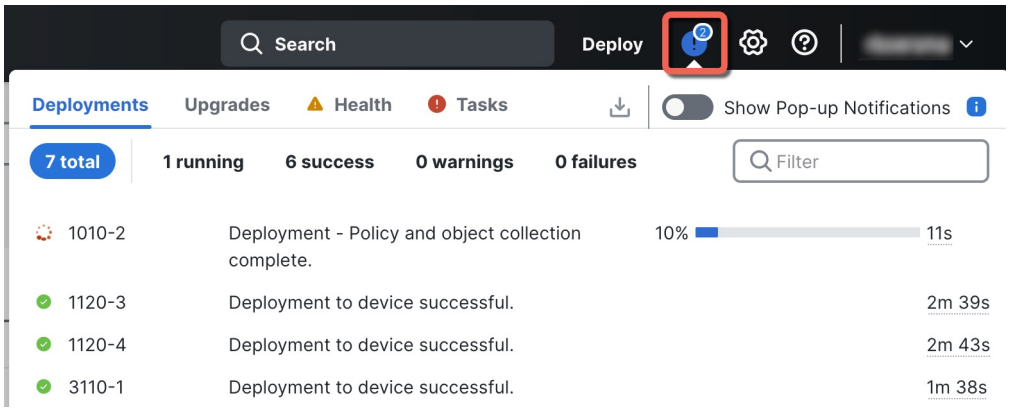
否则，对于其他部署选项，请点击**高级部署 (Advanced Deploy)**。

图 *37:* 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 *38:* 部署状态


Search
Deploy
Deployments
Upgrades
Health
Tasks
Show Pop-up Notifications
7 total
1 running
6 success
0 warnings
0 failures
Filter
1010-2
Deployment - Policy and object collection complete.
10%
11s
1120-3
Deployment to device successful.
2m 39s
1120-4
Deployment to device successful.
2m 43s
3110-1
Deployment to device successful.
1m 38s

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。