



## 使用CDO部署威胁防御

本章对您适用吗？

要查看所有可用的应用和管理器，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) 的云交付的防火墙管理中心云的威胁防御。

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[Cisco Secure Firewall ASA 和 Secure Firewall Threat Defense 重新映像指南](#)。

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 3100/4200 的思科 FXOS 故障排除指南](#)。

**隐私收集声明** - 防火墙不要求或主动收集个人身份信息。但是，您可以在配置中使用个人身份信息，例如用户名。在这种情况下，管理员在执行配置或使用 SNMP 时可能会看到此信息。

- [关于CDO的威胁防御管理，第 2 页](#)
- [端到端任务，第 3 页](#)
- [中央管理员预配置，第 4 页](#)
- [通过激活向导部署防火墙，第 8 页](#)
- [配置基本安全策略，第 16 页](#)
- [访问威胁防御和FXOS CLI，第 29 页](#)
- [关闭防火墙电源，第 30 页](#)
- [后续操作，第 31 页](#)

# 关于CDO的威胁防御管理

## 关于 云交付的防火墙管理中心

云交付的防火墙管理中心 提供许多与内部部署 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。

您可以使用自行激活向导和 CLI 注册自行激活设备。

## 威胁防御管理器访问接口

本指南涵盖介绍外部接口访问，因为它是远程分支机构最可能遇到的场景。虽然管理器访问发生在外部接口上，但专用管理接口仍然相关。管理接口是一个与 威胁防御 数据接口分开配置的特殊接口，它有自己的网络设置。

- 即使您在数据接口上启用了管理器访问，也仍会使用管理接口网络设置。
- 所有管理流量会继续源自或发往管理接口。
- 如果在数据接口上启用了管理器访问，威胁防御 会将传入管理流量通过背板转发到管理接口。
- 对于传出管理流量，管理接口会通过背板将流量转发到数据接口。

## 管理器访问要求

从数据接口进行管理器访问具有以下限制：

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

## 高可用性要求

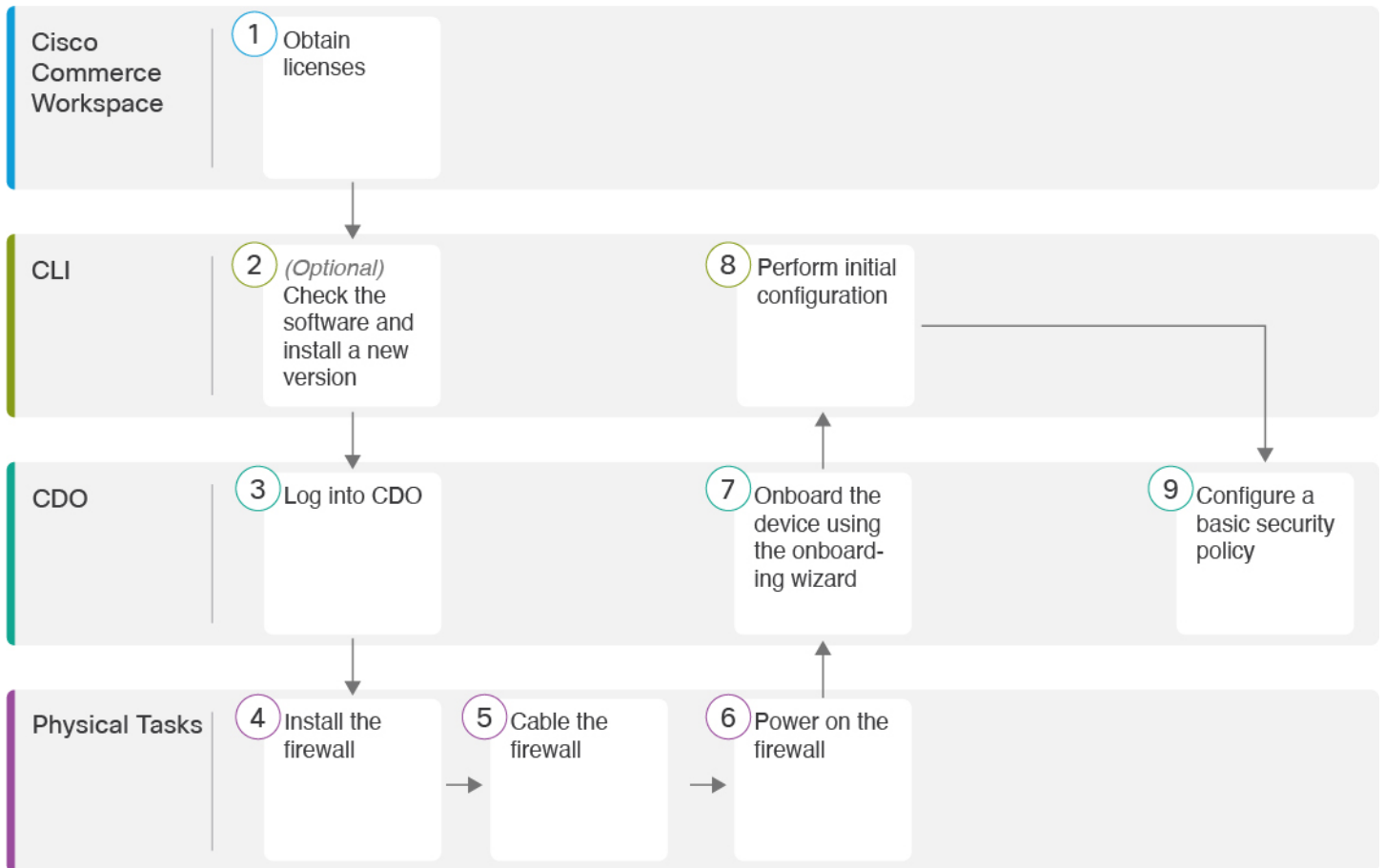
将数据接口与设备高可用性配合使用时，请参阅以下要求。

- 在两台设备上使用相同的数据接口进行管理器访问。
- 不支持冗余管理器访问数据接口。
- 不能使用 DHCP；仅支持静态 IP 地址。无法使用依赖 DHCP 的功能，包括 DDNS 和零接触调配。
- 在同一子网中有不同的静态 IP 地址。
- 使用 IPv4 或 IPv6；不能同时设置。
- 使用相同的管理器配置（`configure manager add` 命令）确保连接相同。
- 不能将数据接口用作故障转移链路或状态链路。

## 端到端任务

请参阅以下任务，使用激活向导在 CDO 中激活 威胁防御。

图 1: 端到端任务



1	Cisco Commerce Workspace	获取许可证，第 4 页。
2	CLI	(可选) 检查软件并安装新版本，第 6 页。
3	CDO	登录 CDO，第 8 页。
4	物理任务	安装防火墙。请参阅硬件安装指南。
5	物理任务	连接防火墙的电缆，第 8 页。
6	物理任务	打开防火墙电源，第 9 页。
7	CDO	使用激活向导激活设备，第 9 页。
8	CLI	使用 CLI 执行初始配置，第 12 页。
9	CDO	配置基本安全策略，第 16 页。

## 中央管理员预配置

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

### 获取许可证

所有许可证都由 CDO 提供给威胁防御。您可以选择购买以下功能许可证：

- 基础版- (必需) 基础版 许可证。
- **IPS** - 安全情报和下一代 IPS
- 恶意软件 防御-恶意软件 防御
- **URL 过滤**—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](https://www.cisco.com/go/licensingguide)

## 开始之前

- 拥有一个[智能软件管理器](#)帐户。

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

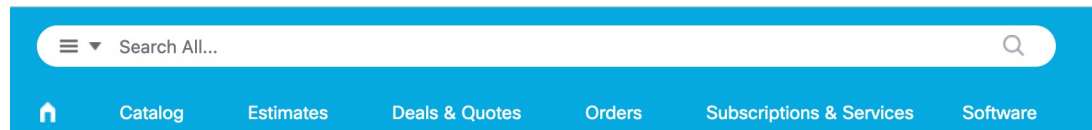
- 您的智能软件许可帐户必须符合强加密 (3DES/AES) 许可证的要求，才能使用某些功能（已使用导出合规性标志启用）。

## 过程

**步骤 1** 请确保智能许可帐户包含所需的可用许可证。

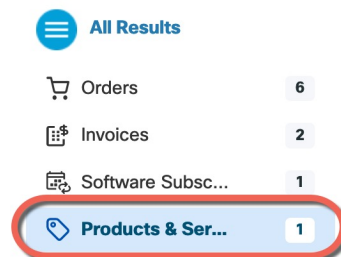
当您从思科或经销商那里购买设备时，您的许可证应该已链接到您的智能软件许可帐户。但是，如果您需要自己添加许可证，则请使用[思科商务工作空间](#)上的[搜索全部 \(Search All\)](#) 字段。

图 2: 许可证搜索



从结果中选择[产品和服务 \(Products & Services\)](#)。

图 3: 成果



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。

- 基础版 许可证:
  - L-FPR4215-BSE=
  - L-FPR4225-BSE=
  - L-FPR4245-BSE=
- IPS、恶意软件 防御和 URL 许可证组合:
  - 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
- 运营商许可证：
    - L-FPR4200K-FTD-CAR=
  - Cisco Secure 客户端-请参阅 [思科安全客户端订购指南](#)。

**步骤 2** 如果尚未注册，请向智能软件管理器注册 CDO。

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

---

## (可选) 检查软件并安装新版本

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

我应该运行什么版本？

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

## 过程

**步骤 1** 打开防火墙电源，然后连接到控制台端口。有关详细信息，请参阅 [打开防火墙电源](#)，第 9 页和 [访问威胁防御和FXOS CLI](#)，第 29 页。

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

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

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

### 示例:

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

[...]

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

[...]

firepower#
```

**步骤 2** 在 FXOS CLI 中，显示正在运行的版本。

```
scope ssa
```

```
show app-instance
```

### 示例:

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

Application Name      Slot ID   Admin State   Operational State   Running Version Startup
Version Cluster Oper State
-----
ftd                   1         Enabled       Online               7.6.0.65         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) 如果要为管理接口设置静态 IP 地址，请参阅 [使用 CLI 执行初始配置](#)，第 12 页。默认情况下，管理接口将使用 DHCP。

您需要从可通过管理接口访问的服务器下载新的映像。

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

防火墙重新启动后，您可以再次连接到 FXOS CLI。

## 登录 CDO

有关创建 CDO 租户和登录的详细信息，请参阅 CDO 文档：<https://docs.defenseorchestrator.com>。

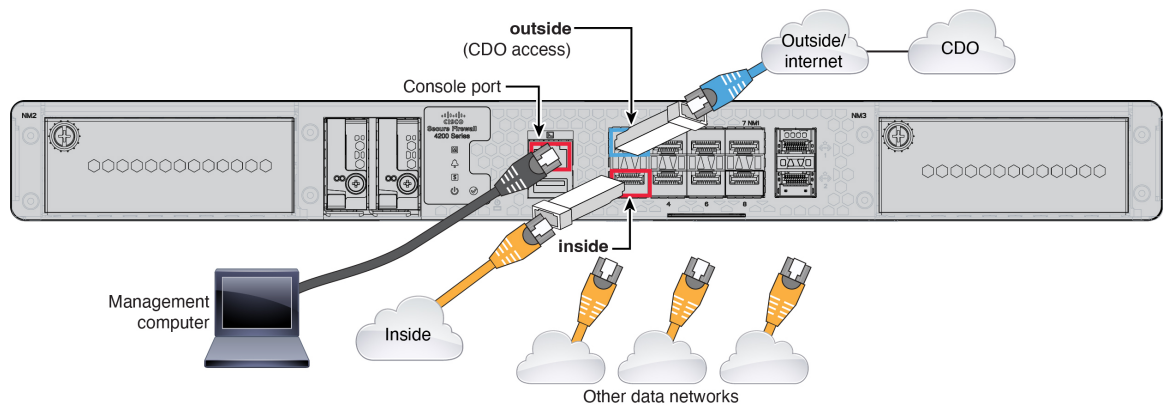
## 通过激活向导部署防火墙

本节介绍如何使用 CDO 激活向导来配置防火墙，以便进行激活。

### 连接防火墙的电缆

本主题介绍如何将 Cisco Secure Firewall 4200 连接到您的网络，以便由 CDO 进行管理。

图 4: 布线 *Cisco Secure Firewall 4200*



#### 开始之前

- 将 SFP 安装到数据接口端口 - 内置端口是需要 SFP 模块的 1/10/25-Gb SFP 端口。
- 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。

#### 过程

**步骤 1** 安装机箱。请参阅[硬件安装指南](#)。

**步骤 2** 将外部接口（例如，以太网 1/1）连接到外部路由器。

**步骤 3** 将内部接口（例如，以太网 1/2）连接到内部交换机或路由器。

**步骤 4** 将其他网络连接到其余接口。



**步骤 5** 将管理计算机连接到控制台端口。

您需要使用 CLI 执行初始设置。出于故障排除目的，也可能需要使用控制台端口。

## 打开防火墙电源

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



**注释** 首次启动 威胁防御时，初始化大约需要 15 到 30 分钟。

### 开始之前

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

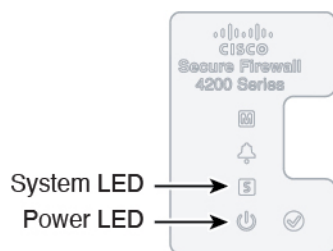
### 过程

**步骤 1** 将电源线一端连接到防火墙，另一端连接到电源插座。

**步骤 2** 使用位于机箱背面电源线旁边的标准摇杆型电源开关打开电源。

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

图 5: 系统和电源 LED



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

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

## 使用激活向导激活设备

通过 CDO 的激活向导使用 CLI 注册键激活 威胁防御。

## 过程

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

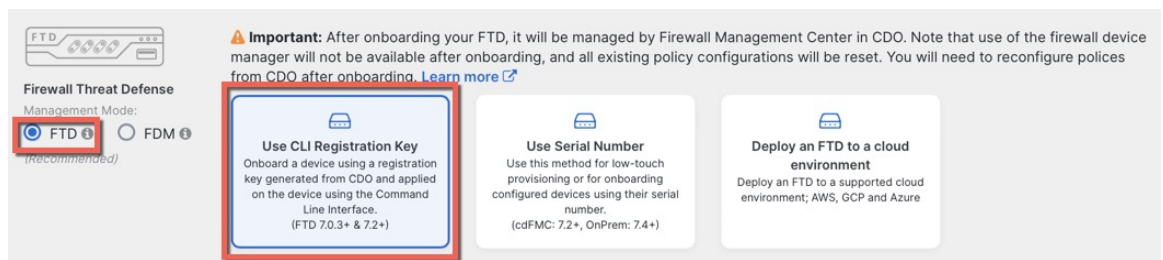
**步骤 2** 点击 **FTD** 磁贴。

**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 4 页以查看可用的许可证。

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

图 6: 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 7: 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 8: 访问控制策略

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

图 9: 订阅许可证

License Type	Includes
<input checked="" type="checkbox"/> Essentials	Base Firewall Capabilities
<input checked="" type="checkbox"/> Carrier (7.3+ FTDs only)	GTP/GPRS, Diameter, SCTP, M3UA
<input checked="" type="checkbox"/> IPS	Intrusion Policy
<input checked="" type="checkbox"/> Malware Defense	File Policy
<input checked="" type="checkbox"/> URL	URL Reputation
<input checked="" type="checkbox"/> RA VPN <span>Premier ▾</span>	RA VPN

**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。

图 10: CLI 注册密钥

- Ensure the device's initial configuration is complete before trying to apply the registration key. [Learn more](#)
- Copy the CLI Key below and paste it into the CLI of the FTD

```
configure manager add cisco-security-docs.app.us.cdo.cisco.com
BanyI2oaT0ew1JTpC0P2w3xEbnVvkfZv x7R7dwcM43JCMzwGY3ZzCfoFmZhW97my cisco-security-
docs.app.us.cdo.cisco.com
```

**configure manager add cdo\_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[使用 CLI 执行初始配置](#)，第 12 页。

示例：

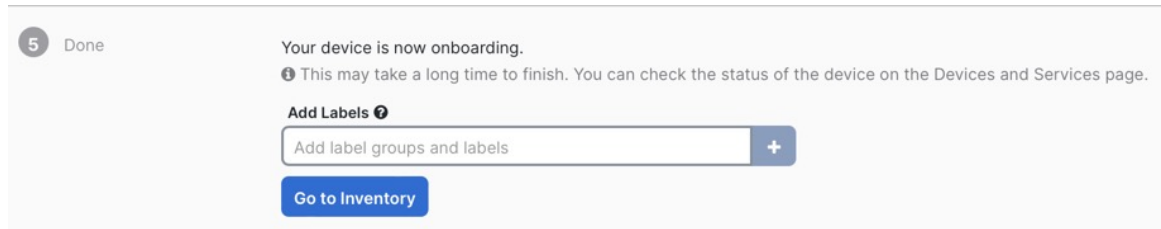
CLI 设置的命令示例：

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

**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。

图 11: 完成



### 下一步做什么

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

## 使用 CLI 执行初始配置

连接到 威胁防御 CLI 以执行初始设置。

### Procedure

**步骤 1** 连接到控制台端口上的 威胁防御 CLI。

控制台端口连接到 FXOS CLI。

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

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

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

### Example:

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

[...]

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

[...]

firepower#
```

**步骤 3** 连接到 威胁防御 CLI。

**connect ftd****Example:**

```
firepower# connect ftd
>
```

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

即使您在数据接口上启用了管理器访问，也仍会使用管理接口设置。

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

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

请参阅以下准则：

- 是否要配置 IPv4？ 和/或 是否要配置 IPv6？ - 为至少一种地址类型输入 **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。
- 通过 DHCP 还是手动配置 IPv4？ 和/或 通过 DHCP、路由器还是手动配置 IPv6？ - 选择 **手动**。如果管理接口设置为 DHCP，则无法配置数据接口用于管理，因为默认路由（必须是 **data-interfaces**，请参阅下一个要点）可能会被接收自 DHCP 服务器的路由覆盖。
- 输入管理接口的 IPv4 默认网关 和/或 输入管理接口的 IPv6 网关—将网关设置为 **data-interfaces**。此设置将在背板上转发管理流量，因此可路由通过管理器访问数据接口。
- 配置防火墙模式？ (**Configure firewall mode?**) — 输入 **routed**。只有路由防火墙模式支持外部管理器访问。

**Example:**

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

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
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]:
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'
```

```
DHCP server is already disabled
DHCP Server Disabled
Configure firewall mode? (routed/transparent) [routed]:
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 5 配置用于管理器访问的外部接口。

### **configure network management-data-interface**

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

- 如果您要使用数据接口进行管理，则管理接口无法使用 DHCP。如果在初始设置期间没有手动设置 IP 地址，则可以使用 **configure network {ipv4 | ipv6} manual** 命令立即设置它。如果您尚未将管理接口网关设置为 **data-interfaces**，此命令将立即设置它。
- 当您威胁防御添加到 CDO 时，CDO 会发现并维护接口配置，包括以下设置：接口名称和 IP 地址、网关静态路由、DNS 服务器和 DDNS 服务器。有关 DNS 服务器配置的详细信息，请参阅下文。在 CDO 中，您可以稍后对管理器访问接口配置进行更改，但要确保更改不会阻止威胁防御或 CDO 重新建立管理连接。如果管理连接中断，威胁防御将包含 **configure policy rollback** 命令以恢复以前的部署。

- 如果配置 DDNS 服务器更新 URL，则威胁防御会自动添加来自 Cisco 受信任根 CA 捆绑包的所有主要 CA 证书，以便威胁防御可以验证用于 HTTPS 连接的 DDNS 服务器证书。威胁防御支持使用 DynDNS 远程 API 规范 (<https://help.dyn.com/remote-access-api/>) 的任何 DDNS 服务器。
- 此命令设置数据接口 DNS 服务器。使用设置脚本（或使用 **configure network dns servers** 命令）设置的管理 DNS 服务器用于管理流量。数据 DNS 服务器用于 DDNS（如果已配置）或适用于此接口的安全策略。

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

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

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

#### Example:

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

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

Setting IPv4 network configuration.
Network settings changed.

>
```

#### Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
```

```

DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

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

Setting IPv4 network configuration.
Network settings changed.

>

```

**步骤 6** 使用 CDO 生成的 `configure manager add` 命令确定将管理此威胁防御的 CDO。请参阅[使用激活向导激活设备, on page 9](#)以生成命令。

**Example:**

```

> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
LzmlHOynhVUWhXYWz2swmkj2ZWsn3Lb account1.app.us.cdo.cisco.com
Manager successfully configured.

```

## 配置基本安全策略

本部分介绍如何使用以下设置配置基本安全策略:

- 内部和外部接口 - 为内部接口分配静态 IP 地址。您在管理器访问设置中配置了外部接口的基本设置，但仍需要将其分配给安全区域。
- DHCP 服务器 - 在内部接口上为客户端使用 DHCP 服务器。
- NAT - 在外部接口上使用接口 PAT。
- 访问控制 - 允许流量从内部传到外部。
- SSH - 在管理器访问接口上启用 SSH。

## 配置接口

启用 威胁防御接口，为其分配安全区域并设置 IP 地址。还要配置分支接口。。

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。

### 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 12: 接口

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

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

**步骤 4** 点击要用于内部的接口的编辑（✎）。

此时将显示一般 (**General**) 选项卡。

图 13: “常规”选项卡

Edit Physical Interface

General IPv4 IPv6 Path Monitoring

Name:

Enabled  
 Management Only

Description:

Mode:

Security Zone:

Interface ID:

MTU:  
  
(64 - 9000)

Priority:  
 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

- 输入长度最大为 48 个字符的名称 (Name)。  
 例如，将接口命名为 **inside**。
- 选中启用 (Enabled) 复选框。
- 将模式 (Mode) 保留为无 (None)。
- 从安全区域 (Security Zone) 下拉列表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。
- 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 14: 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 15: 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 (✎)。

此时将显示一般 (General) 选项卡。

图 16: “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:

您已经为该接口预配置了管理器访问，因此该接口就已经命名、启用和寻址。您不应更改任何这些基本设置，因为这样做会中断管理中心管理连接。您仍然必须在此屏幕上为直通流量策略配置安全区域。

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

例如，添加一个名为 `outside_zone` 的区域。

- b) 点击确定 (OK)。

步骤 6 点击保存 (Save)。

## 配置 DHCP 服务器

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

## 过程

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

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

图 17: DHCP 服务器

The screenshot shows the DHCP Server configuration page. The left sidebar lists 'DHCP Server', 'DHCP Relay', and 'DDNS'. The main area has tabs for 'Device', 'Routing', 'Interfaces', 'Inline Sets', 'DHCP', and 'VTEP'. Under the 'DHCP' tab, there are input fields for 'Ping Timeout' (50), 'Lease Length' (3600), and a checkbox for 'Auto-Configuration'. Below that is an 'Interface' dropdown menu. The 'Override Auto Configured Settings' section includes fields for 'Domain Name', 'Primary DNS Server', 'Secondary DNS Server', 'Primary WINS Server', and 'Secondary WINS Server'. At the bottom, there are tabs for 'Server' and 'Advanced', and a '+ Add' button highlighted in a red box.

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

图 18: 添加服务器

The screenshot shows the 'Add Server' dialog box. It has a title bar with a question mark icon. The 'Interface\*' field is a dropdown menu with 'inside' selected. The 'Address Pool\*' field is a text input with '10.9.7.9-10.9.7.25' and '(2.2.2.10-2.2.2.20)' below it. There is a checked checkbox for 'Enable DHCP Server'. At the bottom, there are 'Cancel' and 'OK' buttons.

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

**步骤 4** 点击确定 (OK)。

步骤 5 点击保存 (Save)。

## 配置 NAT

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

### 过程

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

步骤 2 为策略命名，选择要使用策略的设备，然后点击 Save。

图 19: 新建策略

New Policy

Name:  
interface\_PAT

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

Search by name or value

10.10.0.6  
10.10.0.7

Add to Policy

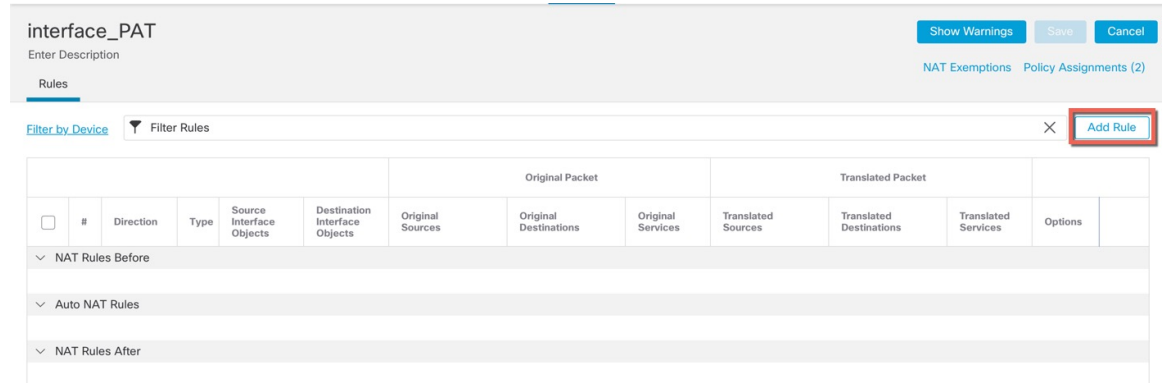
Selected Devices

10.10.0.6  
10.10.0.7

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 20: NAT 策略

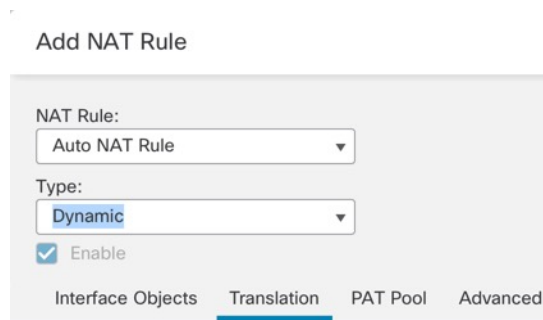


步骤 3 点击添加规则 (Add Rule)。

Add NAT Rule 对话框将显示。

步骤 4 配置基本规则选项：

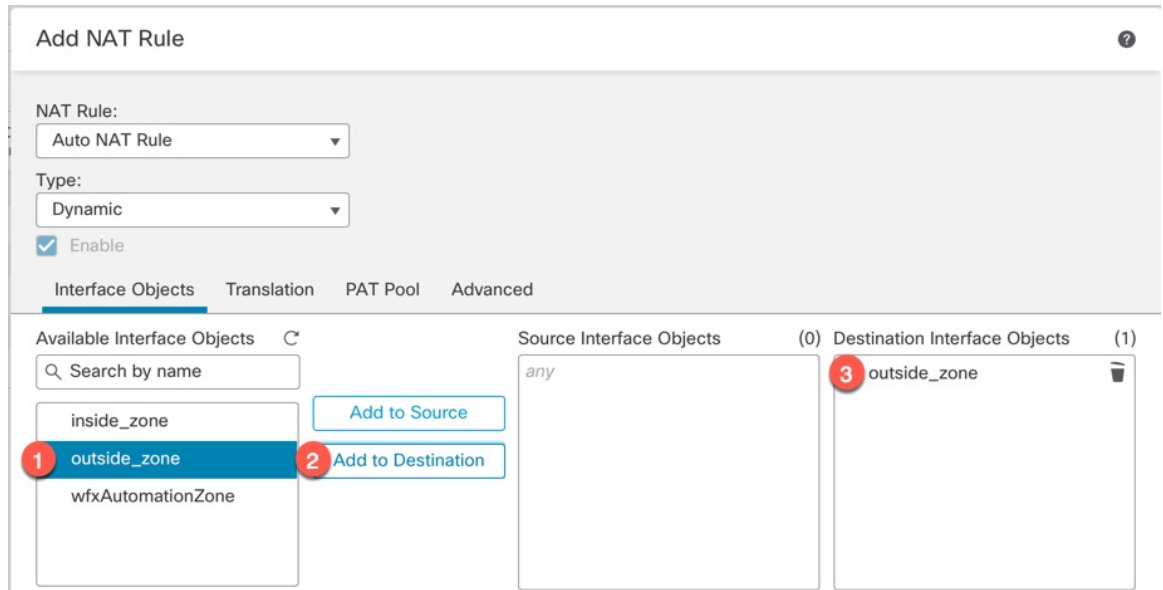
图 21: 基本规则选项



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

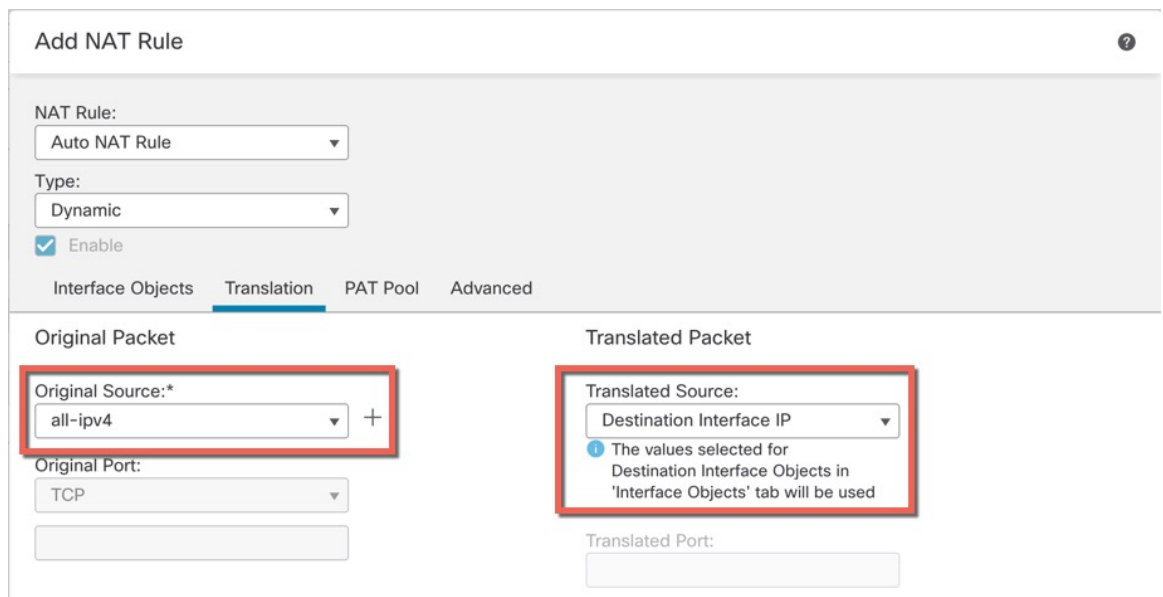
步骤 5 在 Interface Objects 页面，将 Available Interface Objects 区域中的外部区域添加到 Destination Interface Objects 区域。

图 22: 接口对象



步骤 6 在转换 (Translation) 页面上配置以下选项:

图 23: 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 24: 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。

## 允许流量从内部传到外部

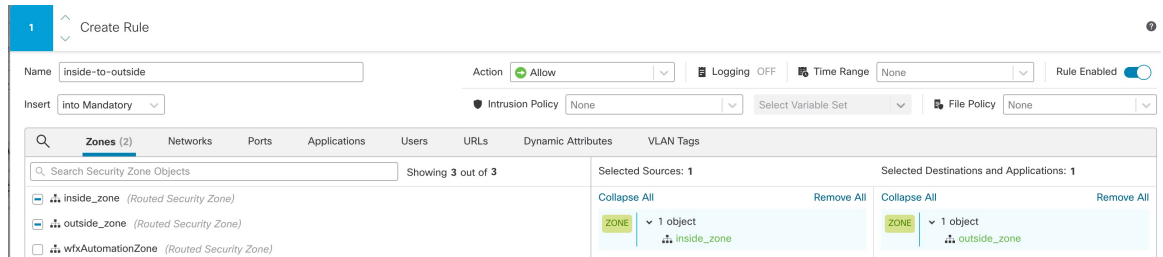
如果您在注册威胁防御时创建了基本的封锁所有流量访问控制策略，则需要向策略添加规则以允许流量通过设备。以下程序可添加规则以允许从内部区域到外部区域的流量。如有其他区域，请务必添加允许流量到适当网络的规则。

### 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：

图 25: 添加规则



- 名称 (Name) - 为此规则命名，例如 **inside-to-outside**。
- 所选择的源 (Selected Sources) - 从 区域 (Zones) 中选择内部区域，然后点击 添加到源 (Add to Source)。
- 所选择目标区域 (Selected Destination Zones) - 从 区域 (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** 点击应用 (Apply)。

规则即已添加至 **Rules** 表。

**步骤 4** 点击保存 (Save)。

## 在管理器访问数据接口上配置 SSH

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



**注释** 管理接口上默认已启用 SSH，但此屏幕不会影响管理 SSH 访问。

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

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

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

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

SSH 支持以下密码和密钥交换：

- Encryption—aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr
- Integrity—hmac-sha2-256
- Key exchange—dh-group14-sha256



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

### 开始之前

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



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

### 过程

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

**步骤 2** 选择**SSH 访问 (SSH Access)**。

**步骤 3** 标识允许 SSH 连接的接口和 IP 地址。

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

- a) 点击**添加 (Add)** 以添加新规则，或点击**编辑 (Edit)** 以编辑现有规则。
- b) 配置规则属性：

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

- c) 点击**确定 (OK)**。

**步骤 4** 点击**保存 (Save)**。

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

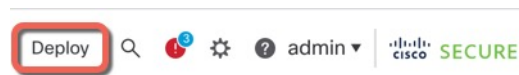
## 部署配置

将配置更改部署到威胁防御；在部署之前，您的所有更改都不会在设备上生效。

### 过程

**步骤 1** 点击右上方的部署 (Deploy)。

图 26: 部署



**步骤 2** 要快速部署，请选中特定设备，然后点击部署 (Deploy)，或者点击全部部署 (Deploy All) 以部署到所有设备。否则，对于其他部署选项，请点击高级部署 (Advanced Deploy)。

图 27: 全部部署

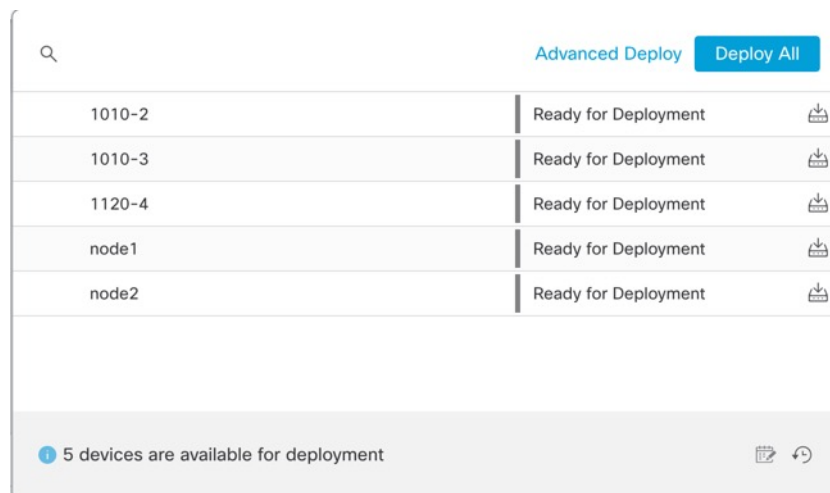
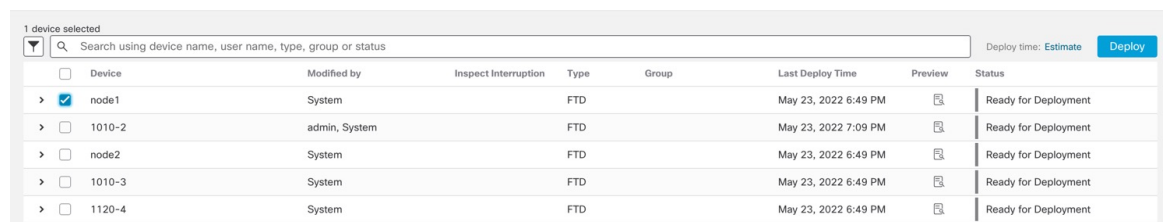
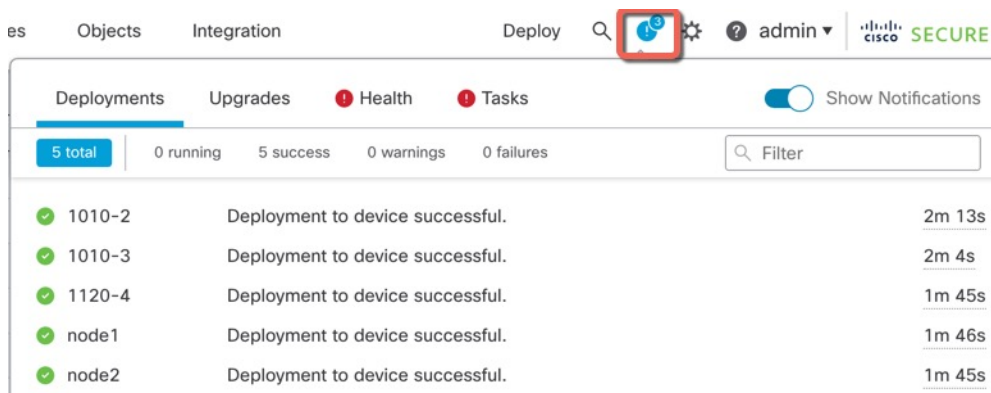


图 28: 高级部署



**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 29: 部署状态



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

## 访问威胁防御和FXOS CLI

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

也可以访问FXOS CLI以进行故障排除。



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

### 过程

**步骤 1** 要登录 CLI，请将管理计算机连接到控制台端口。默认情况下，安全防火墙 4200 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。确保为操作系统安装任何必要的 USB 串行驱动程序。控制台端口默认为 FXOS CLI。使用以下串行设置：

- 9600 波特率
- 8 个数据位
- 无奇偶校验
- 1 个停止位

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

示例：

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

firepower#
```

**步骤 2** 访问威胁防御 CLI。

**connect ftd**

示例:

```
firepower# connect ftd
>
```

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

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

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

示例:

```
> exit
firepower#
```

## 关闭防火墙电源

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

您可以使用管理中心设备管理页面来关闭设备电源，也可以使用FXOS CLI。

## 使用 CDO 关闭防火墙

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

您可以使用 管理中心 正确关闭系统。

过程

**步骤 1** 选择设备 > 设备管理。

**步骤 2** 在要重新启动的设备旁边，点击 **编辑** (✎)。

**步骤 3** 点击设备 (Device) 选项卡。

**步骤 4** 在系统 (System) 部分中点击 关闭设备 (✕)。

**步骤 5** 出现提示时，确认是否要关闭设备。

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

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

如果没有控制台连接，请等待大约 3 分钟以确保系统已关闭。

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

---

## 使用 CDO 关闭防火墙

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

您可以使用 管理中心 正确关闭系统。

### 过程

---

**步骤 1** 选择设备 > 设备管理。

**步骤 2** 在要重新启动的设备旁边，点击 编辑 (✎)。

**步骤 3** 点击设备 (Device) 选项卡。

**步骤 4** 在系统 (System) 部分中点击 关闭设备 (✕)。

**步骤 5** 出现提示时，确认是否要关闭设备。

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

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

如果没有控制台连接，请等待大约 3 分钟以确保系统已关闭。

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

---

## 后续操作

要使用 CDO 继续配置 威胁防御，请参阅 [思科防御协调器 主页](#)。





## 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。