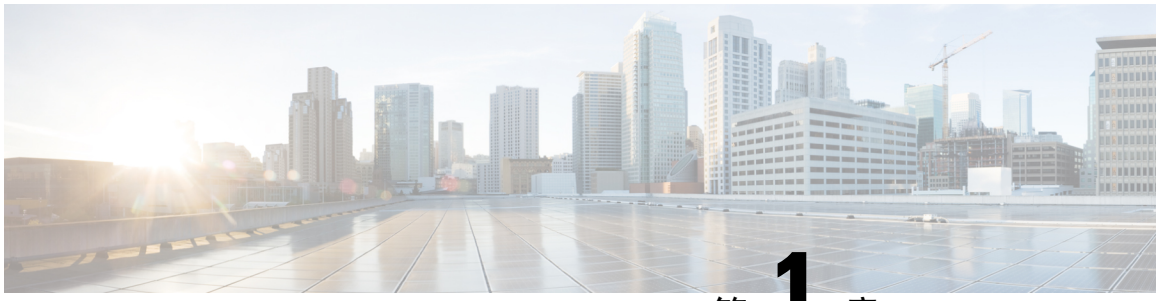
Cisco Secure Firewall 1210/20 威胁防御入门：设备管理器

上次修改日期: 2025 年 3 月 17 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



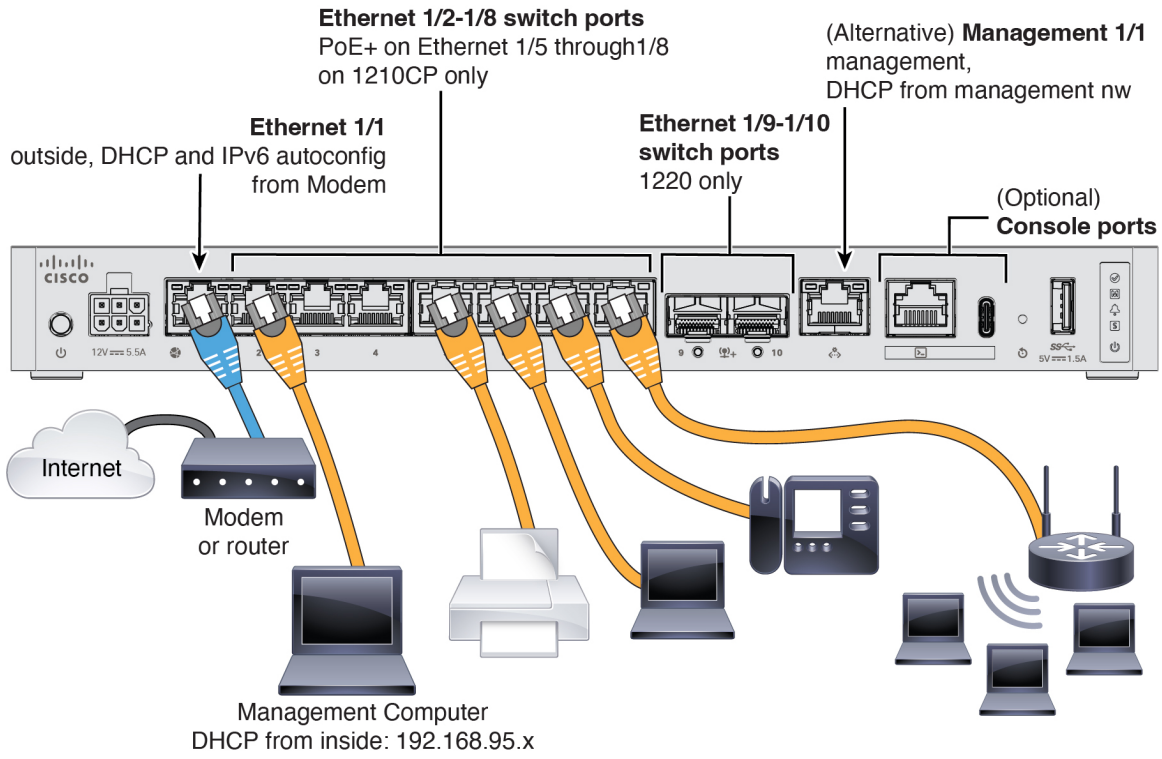
第 1 章

准备工作

使用本地 Cisco Secure Firewall 设备管理器 来管理防火墙。

连接防火墙的电缆

- 对于 Cisco Secure Firewall 1220，请将 SFP 安装到以太网 1/9 和 1/10 端口中。端口是需要使用 SFP/SFP+ 模块的 1/10-Gb SFP+ 端口。
- 有关详细信息，请参阅硬件安装指南。



打开防火墙电源

系统电源由位于防火墙后部的电源按钮控制。电源按钮提供软通知，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

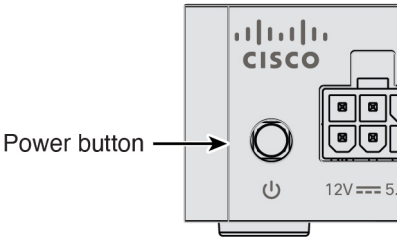
为防火墙提供可靠的电源（例如，使用不间断电源 (UPS)）非常重要。未事先关闭就断电可能会导致严重的文件系统损坏。后台始终有许多进程在运行，因此断电会使得系统无法正常关闭。

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。

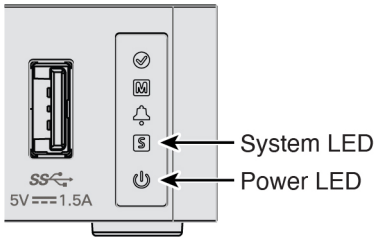
步骤 2 使用位于机箱背面电源线旁边的电源按钮打开电源。

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。

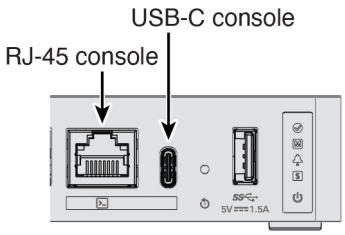
安装的哪个应用程序：威胁防御还是 ASA？

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 使用任一端口类型连接到控制台端口。

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 4 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。

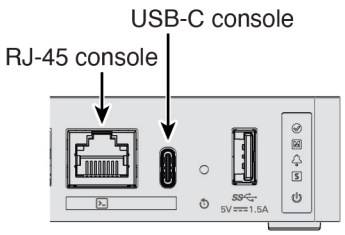
访问威胁防御 CLI

您可能需要访问 CLI 进行配置或故障排除。

过程

步骤 1 使用任一端口类型连接到控制台端口。

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，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。

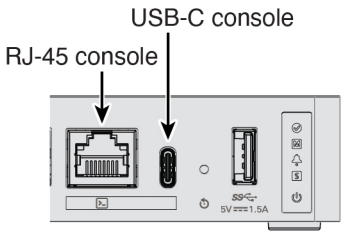
我应该运行什么版本？

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 使用任一端口类型连接到控制台端口。

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。

（可选）在 CLI 中更改管理网络设置

默认情况下，您可以通过以下任一接口来管理防火墙：

- 以太网 1/2 至以太网 1/8 或 1/10 - 192.168.95.1/24
- 管理 1/1 - DHCP 的 IP 地址

如果无法使用默认 IP 地址，则可以连接到控制台端口，通过 CLI 执行初始设置，将管理 1/1 IP 地址设置为静态地址。

过程

步骤 1 连接到控制台端口。请参阅安装的哪个应用程序：威胁防御还是 ASA？ ，第 3 页。

步骤 2 连接到 威胁防御 CLI。

connect ftd

示例：

```
firepower# connect ftd
>
```

步骤 3 完成管理界面设置的 CLI 设置脚本。

```
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]:
```

指南：选择**手动**以设置静态 IP 地址。

```
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
```

指南：设置网关的 IP 地址。

```
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]: yes

>
```

指南：输入 **yes** 以使用 设备管理器。

步骤 4 在新的管理 IP 地址上登录设备管理器 。

获取许可证

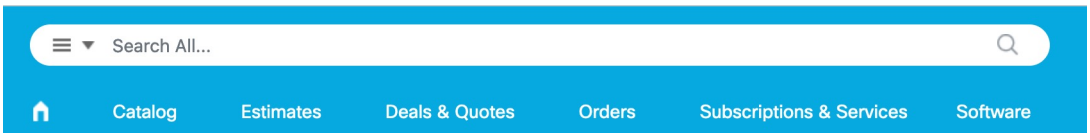
当您从思科或经销商那里购买设备时，您的许可证应该已链接到您的智能软件许可证帐户。如果您没有智能软件管理器账户，请点击链接建立新账户。

威胁防御 具有以下许可证：

- 标准版 — 必需
- IPS
- 恶意软件防御
- URL 过滤
- Cisco Secure Client

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。

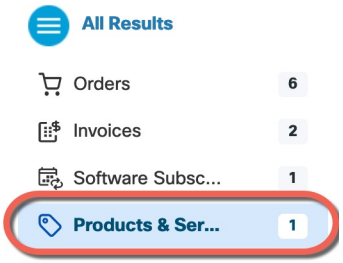
注释 如果未找到 PID，您可以手动将 PID 添加到订单中。

- Essentials：
  - 自动包含
- IPS、恶意软件防御和 URL 组合：
  - L-CSF1210CET-TMC=
  - L-CSF1210CPT-TMC=
  - L-CSF1220CXT-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-CSF1210CE-TMC-1Y
  - L-CSF1210CE-TMC-3Y
  - L-CSF1210CE-TMC-5Y
  - L-CSF1210CP-TMC-1Y
  - L-CSF1210CP-TMC-3Y
  - L-CSF1210CP-TMC-5Y
  - L-CSF1220CX-TMC-1Y
  - L-CSF1220CX-TMC-3Y
  - L-CSF1220CX-TMC-5Y
- 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。

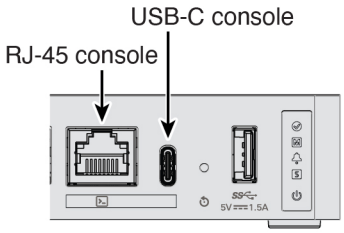
在 CLI 关闭防火墙电源

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 使用任一端口类型连接到控制台端口。

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。

使用设备管理器关闭防火墙

使用设备管理器正确关闭系统。

过程

步骤 1 关闭防火墙。

a) 点击**设备 (Device)**，然后点击**系统设置 (System Settings)** > **重新启动/关闭 (Reboot/Shutdown)** 链接。

b) 点击**关闭**。

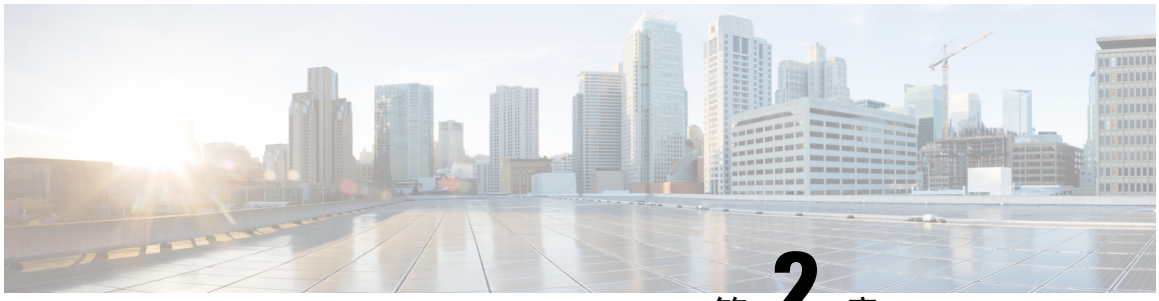
步骤 2 如果您与防火墙建立了控制台连接，请在防火墙关闭时留意系统提示。关闭完成后，您将看到以下提示。

```
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

配置基本策略

完成初始配置，然后配置其他接口和网络设置以及自定义策略。

登录设备管理器

登录设备管理器以配置威胁防御。

过程

步骤 1 根据计算机连接的接口，在浏览器中输入以下 URL。

- 以太网 1/2 至以太网 1/8 或 1/10 - **https://192.168.95.1**
- 管理 1/1 - **https://***management_ip*（从 DHCP）

步骤 2 使用用户名 **admin** 和默认密码 **Admin123** 登录。

完成初始配置

首次登录设备管理器以完成初始配置时，请使用设置向导。完成设置向导后，您的设备应该会正常工作并应部署了几个基本策略：

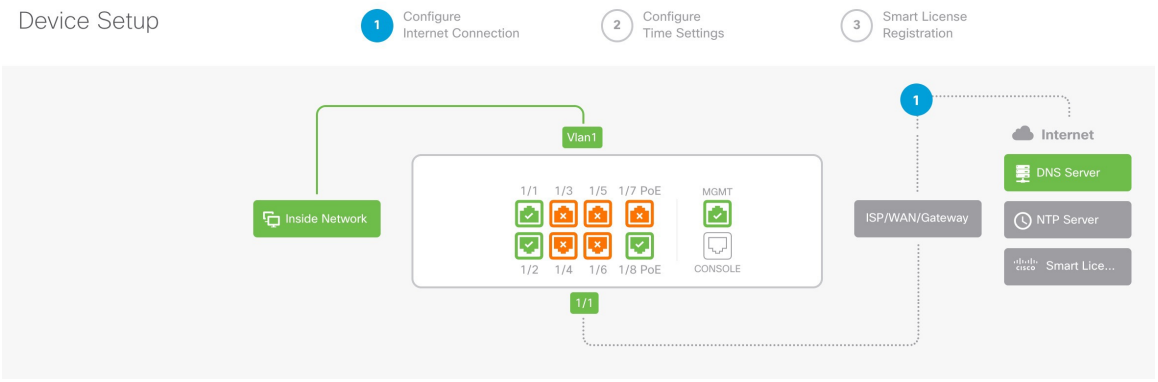
- 内部→外部流量
- 用于所有对外流量的接口 PAT。

过程

步骤 1 接受“一般条款”并更改管理员密码。

将出现**设备设置 (Device Setup)** 屏幕。

图 *9:* 设备设置

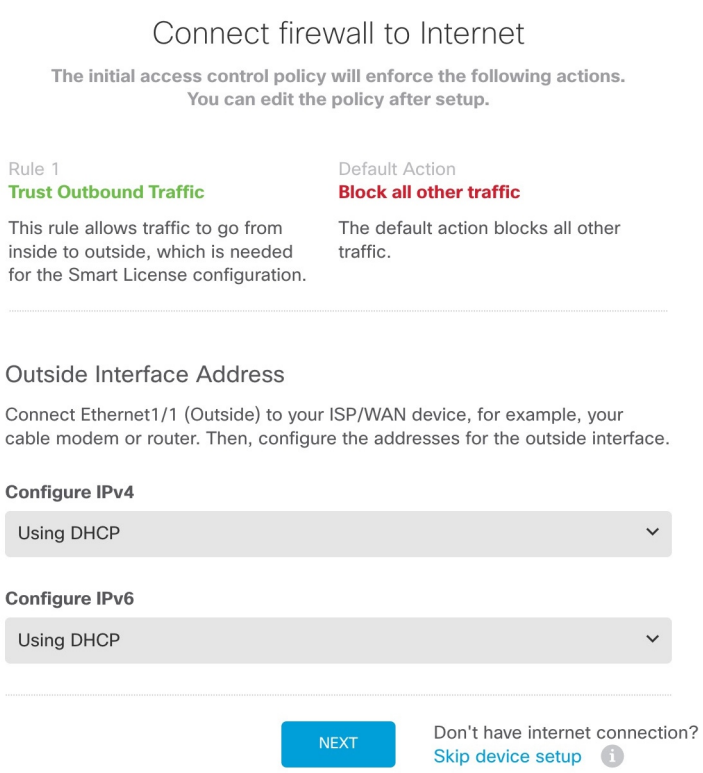


注释

具体的端口配置取决于您的型号。

步骤 2 为外部接口和管理接口配置网络设置。

图 *10:* 将防火墙连接到互联网



a) **外部接口 (Outside Interface)** - 以太网 1/1。在初始设备设置期间，您不能选择其他外部接口。

配置 IPv4 (Configure IPv4) - 如果需要 PPPoE，则可以在完成向导后进行配置。

在接口上配置 IPv6

b) **管理接口 (Management Interface)** - 设置专用管理 1/1 接口的参数。如果您在 CLI 中更改了 IP 地址，则不会看到这些设置，因为您已经对其进行了配置。

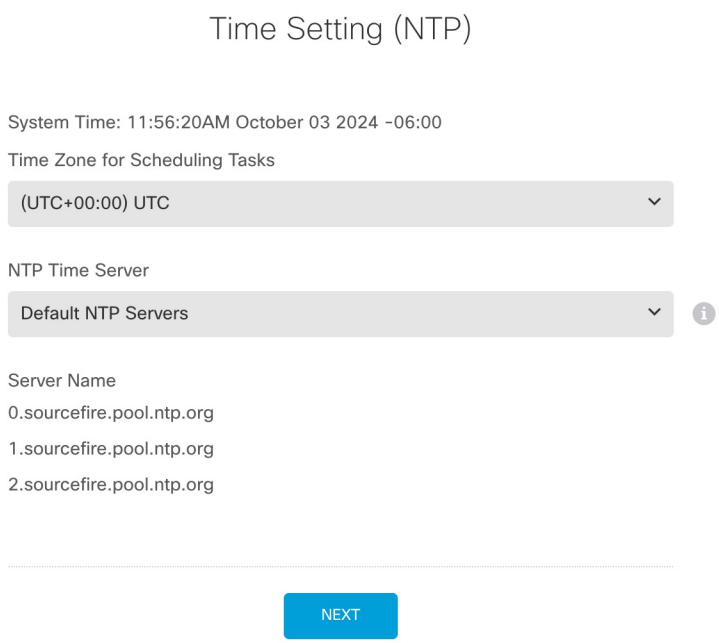
DNS 服务器 (DNS Servers) - 默认值为 OpenDNS 公共 DNS 服务器。

防火墙主机名

c) 点击**下一步**。

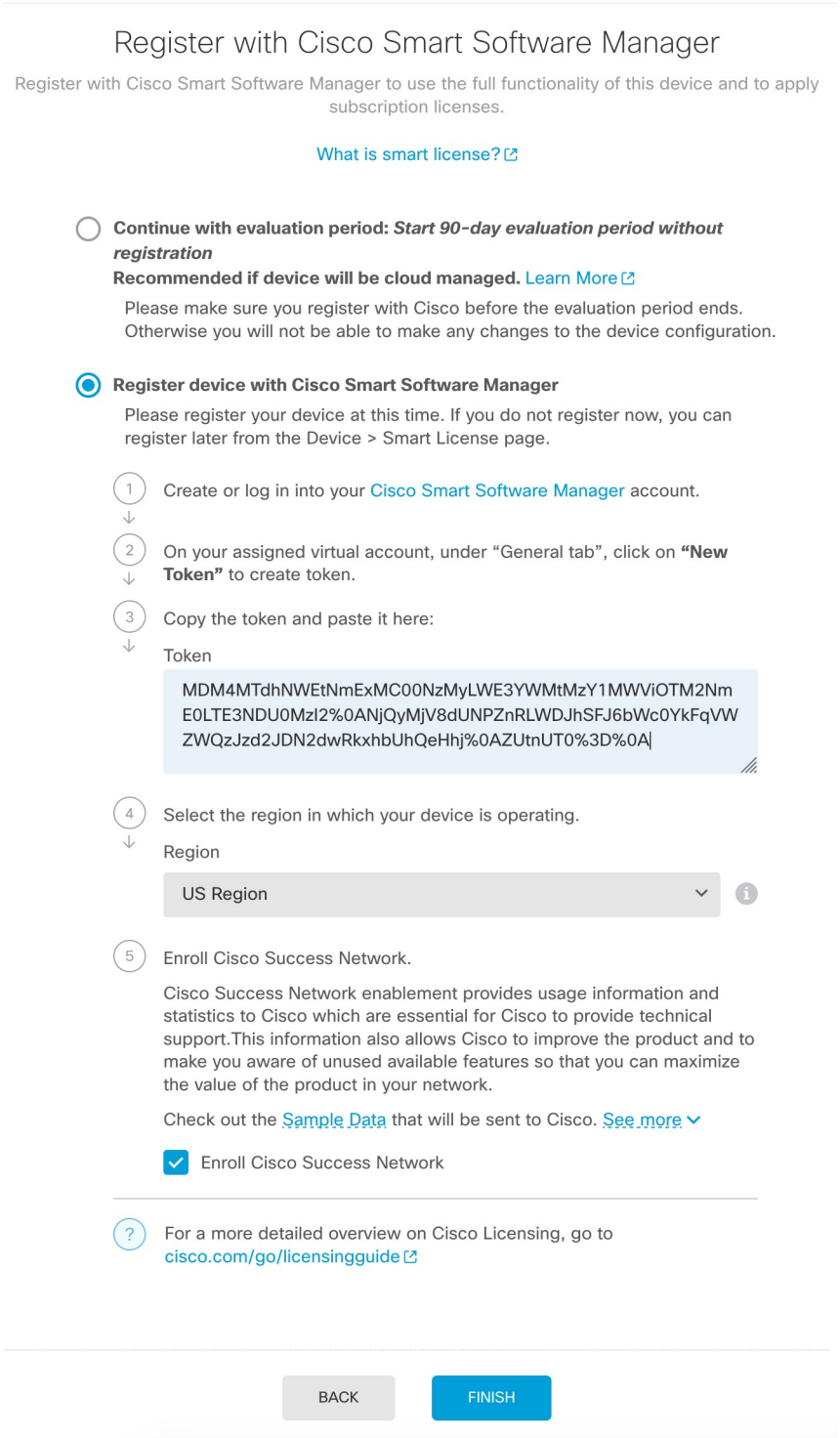
步骤 3 配置系统时间设置。

图 *11:* 时间设置 *(NTP)*



a) 时区
b) **NTP** 时间服务器
c) 点击**下一步**。

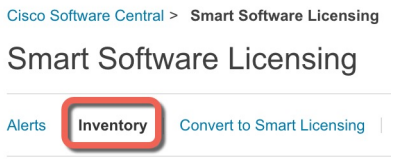
步骤 4 配置智能许可。



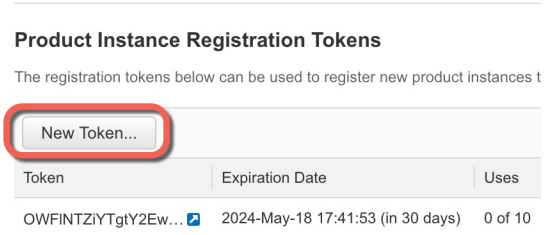
a) 点击向思科智能软件管理器注册设备 **(Register device with Cisco Smart Software Manager)**。

b) 点击思科智能软件管理器 (Cisco Smart Software Manager) 链接。

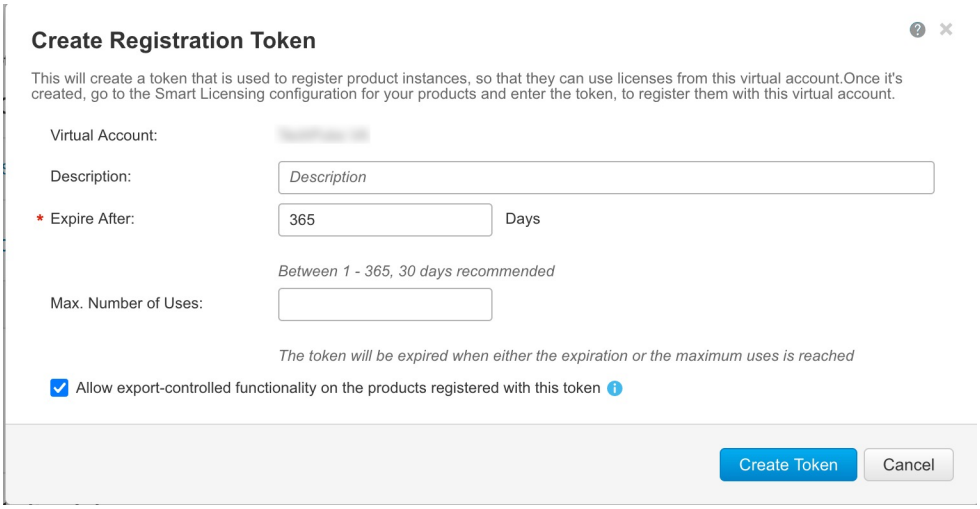
c) 点击清单 **(Inventory)**。



d) 在 **General** 选项卡上，点击 **New Token**。



e) 在 **Create Registration Token** 对话框中，输入以下设置，然后点击 **Create Token**：



- **Description**
- **Expire After** - 思科建议该时间为 30 天。
- **最大使用次数**
- **在使用此令牌注册的产品上允许导出控制的功能 (Allow export-controlled functionaility on the products registered with this token** — 在您所在的国家/地区允许进行强加密的情况下启用导出合规性标志。如果打算使用此功能，则须立即选择该选项。如果稍后启用此功能，则需要使用新产品密钥重新注册设备并重新加载设备。如果您没有看到此选项，则您的帐户不支持出口控制功能。

系统将令牌添加到您的清单中。

f) 点击令牌右侧的箭头图标可以打开 **Token** 对话框，可以从中将令牌 ID 复制到剪贴板。当需要注册威胁防御时，请准备好此令牌，以在该程序后面的部分使用。

图 *12:* 查看令牌

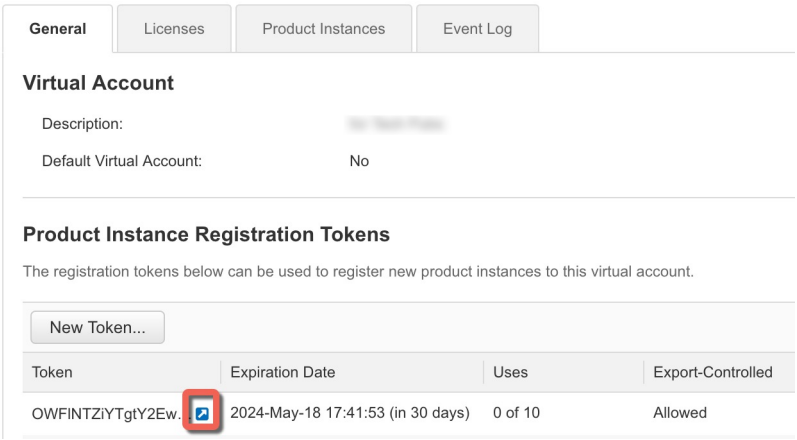
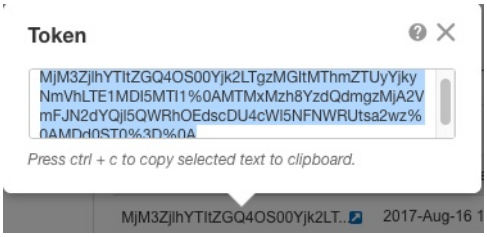


图 *13:* 复制令牌

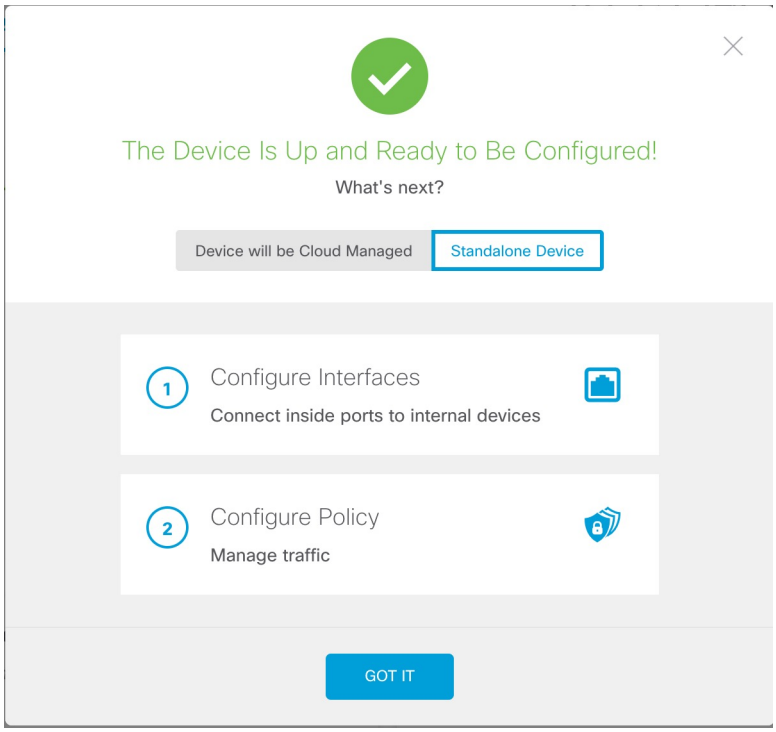


g) 在 设备管理器 中，将令牌粘贴到令牌字段中。

h) 设置其他选项，然后点击**完成 (Finish)**

步骤 5 完成设置向导。

图 *14:* 后续操作



a) 点击**独立设备 (Standalone Device)** 以使用 设备管理器。

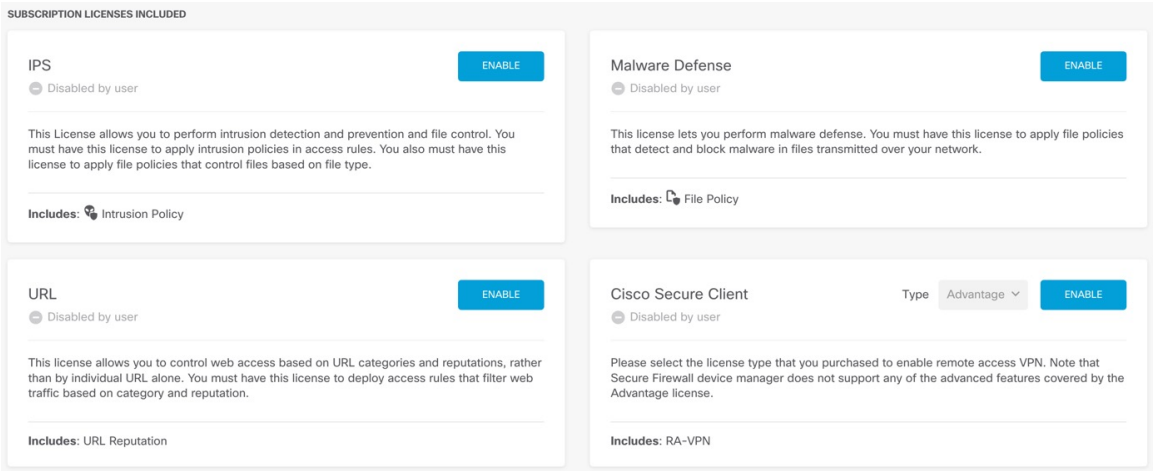
b) 点击**配置接口 (Configure Interfaces)** 直接转至**接口 (Interfaces)** 页面，点击**配置策略 (Configure Policy)** 转至**策略 (Policies)** 页面，或者点击**知道了 (Got It)** 转至**设备 (Device)** 页面。

有关接口或策略配置，请参阅配置网络设置和策略，第 21 页。

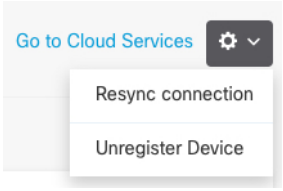
步骤 6 启用功能许可证。

a) 在**设备 (Device)** 页面中，点击**智能许可证 (Smart License)** > > **查看配置 (View Configuration)**。

b) 点击每个可选许可证的**启用/禁用 (Enable/Disable)** 控件。



c) 从齿轮下拉列表中选择 **Resync Connection**（再同步连接），将许可证信息与思科智能软件管理器同步。



配置网络设置和策略

配置其他接口和 DHCP 服务器，并自定义安全策略。

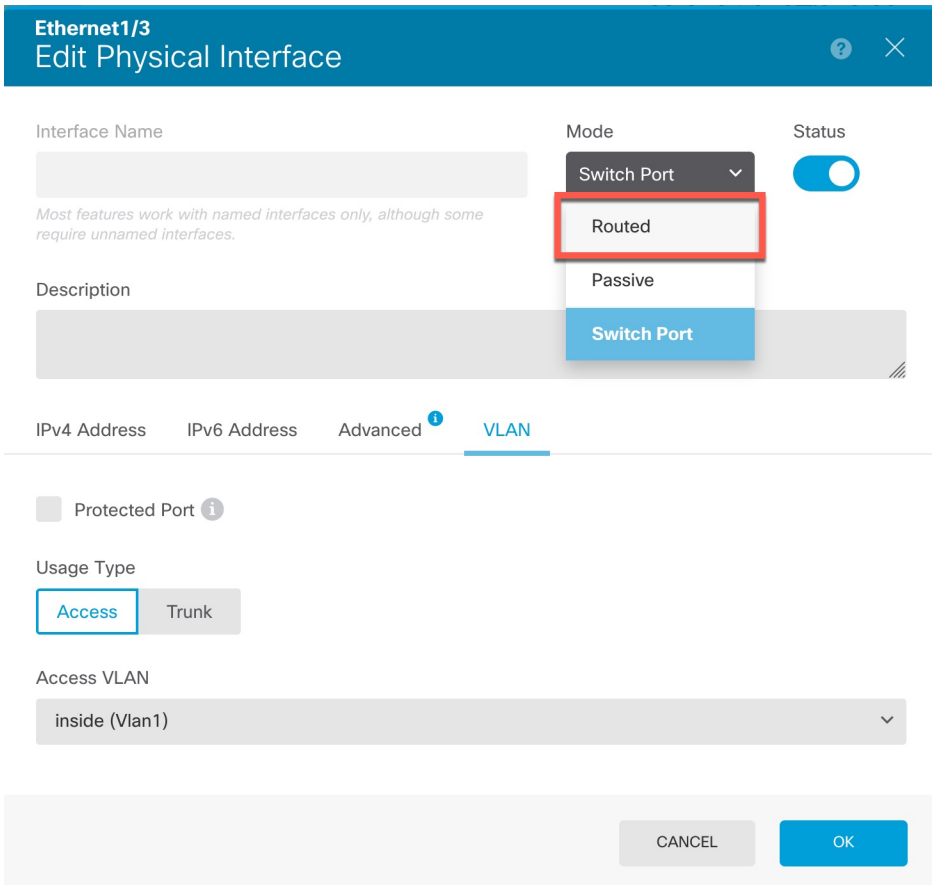
过程

步骤 1 如果要将交换机端口转换为防火墙接口，请选择**设备 (Device)**，然后点击**接口 (Interfaces)** 摘要中的链接。

a) 点击交换机端口的编辑图标 ( )。

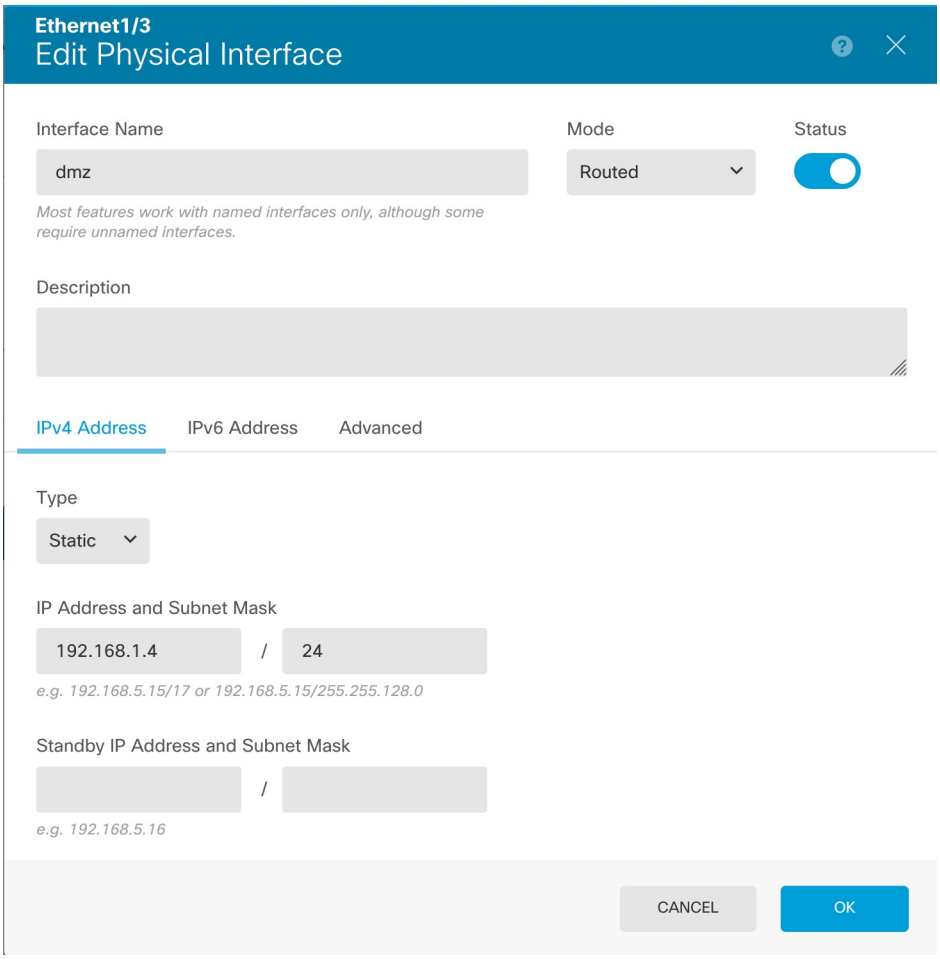
b) 将模式从**交换机端口 (Switch Port)** 更改为**已路由 (Routed)**。

图 *15:* 更改模式



c) 设置名称和 IP 地址。

图 *16:* 编辑接口



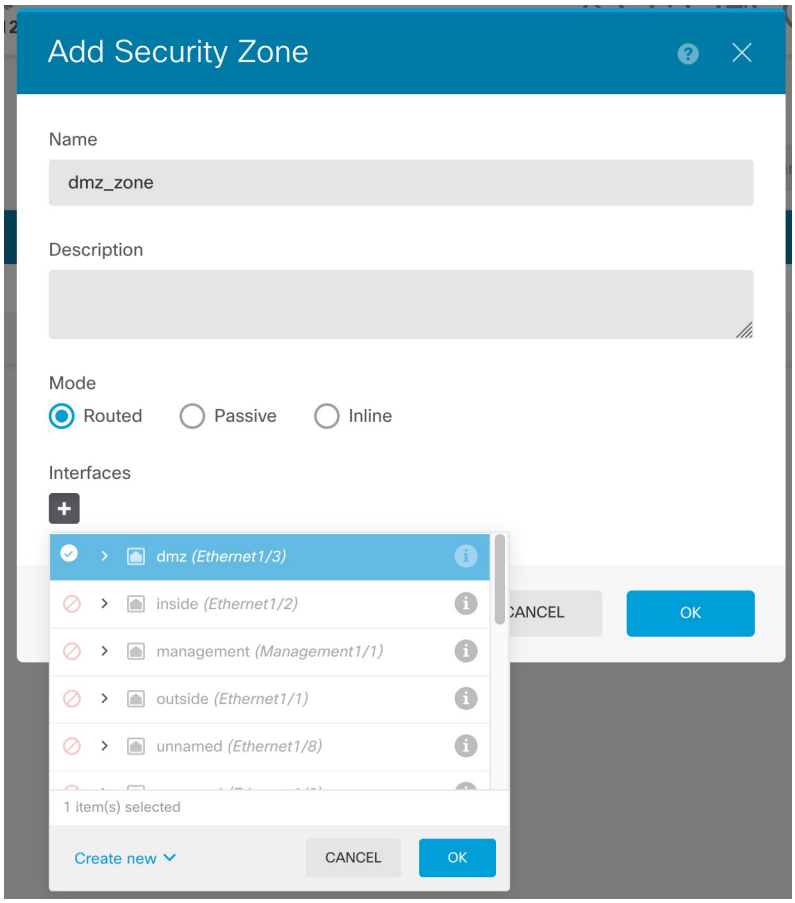
d) 点击**确定 (OK)**。

步骤 2 如果已配置新的防火墙接口，请选择**对象 (Objects)**，然后选择**安全区域 (Security Zones)**。

根据情况编辑或创建新区域，并将接口分配给该区域。每个接口都必须属于您为其配置策略的区域。

以下示例创建了一个新的 dmz_zone，然后将 dmz 接口分配给它。

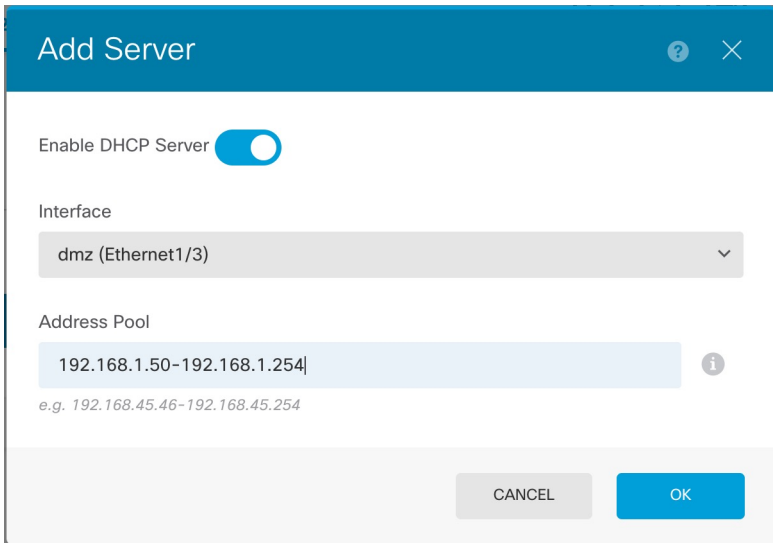
图 *17:* 安全区域对象



步骤 3 如果要让内部客户端使用 DHCP 从设备获取 IP 地址，请选择**设备 (Device)** > **系统设置 (System Settings)** > **DHCP 服务器 (DHCP Server)**，然后选择**DHCP 服务器 (DHCP Server)** 选项卡。

内部接口已经配置了 DHCP 服务器。

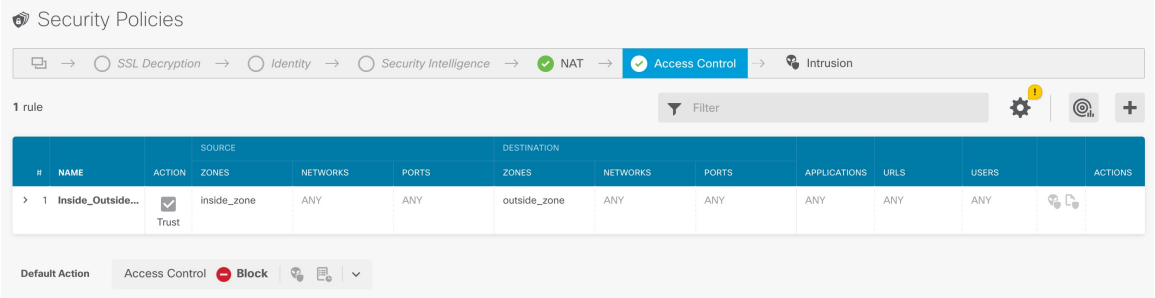
图 *18: DHCP* 服务器



步骤 4 选择**策略 (Policies)**，并为网络配置安全策略。

设备设置向导可使用信任规则在内部区域和外部区域之间实现流量流动。信任规则不会应用入侵策略。要使用入侵，请为规则指定“允许”操作。在连接外部接口时，该策略还包括所有接口的接口 PAT。

图 *19:* 默认安全策略



但是，如果在不同的区域都有接口，则需要访问控制规则来允许流量进出这些区域。

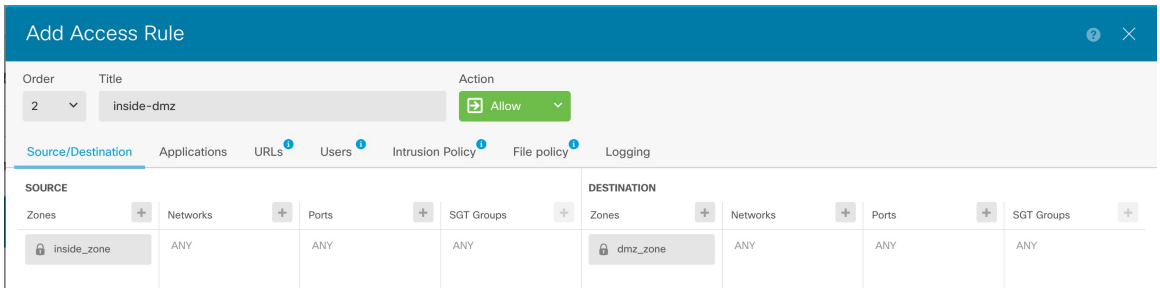
此外，您还可配置其他策略以提供附加服务，并对 NAT 和访问规则进行精细调整，以实现组织需要的结果。点击工具栏中的策略类型，即可配置以下策略：

- **SSL 解密 (SSL Decryption)** - 如果要检查加密连接（例如 HTTPS）是否存在入侵、恶意软件等，则必须解密连接。使用 SSL 解密策略确定需要解密的连接。系统检查连接后，会将其重新加密。
- **身份 (Identity)** - 如果要将网络活动与各个用户相关联，或根据用户或用户组成员身份控制网络访问，请使用身份策略确定与给定源 IP 地址关联的用户。
- **安全智能 (Security Intelligence)** -（需要 IPS 许可证）使用安全智能策略快速丢弃进出列入黑名单的 IP 地址或 URL 的连接。将已知恶意站点列入黑名单后，在访问控制策略中即可无需考虑这些站点。思科提供定期更新的已知恶意地址和 URL 源，可使安全智能黑名单实现动态更新。使用情报源，无需通过编辑策略来添加或删除黑名单中的项目。

- **NAT (Network Address Translation)** - 使用 NAT 策略将内部 IP 地址转换为外部可路由地址。
- **访问控制 (Access Control)** - 使用访问控制策略确定网络上允许的连接。您可以按安全区域、IP 地址、协议、端口、应用、URL、用户或用户组进行过滤。您还可以使用访问控制规则来应用入侵策略和文件（恶意软件）策略。使用此策略实施 URL 过滤。
- **入侵 (Intrusion)** - 使用入侵策略检测已知威胁。即使使用访问控制规则应用入侵策略，也仍可以编辑入侵策略，以选择性地启用或禁用特定的入侵规则。

以下示例显示了如何在访问控制策略中允许 inside_zone 和 dmz_zone 之间的流量。在此示例中，任何其他选项卡上均未设置任何选项，**日志记录 (Logging)** 除外，其中**在连接结束时 (At End of Connection)** 选项已被选中。

图 *20:* 访问控制策略



步骤 5 选择**设备 (Device)**，然后点击**更新 (Updates)** 组中的**查看配置 (View Configuration)**，为系统数据库配置更新计划。

如果使用入侵策略，请为“规则”和“VDB”数据库设置定期更新。如果使用安全智能源，请为“规则”和“VDB”数据库设置更新计划。如果在任何安全策略中使用地理位置作为匹配条件，请为“规则”和“VDB”数据库设置更新计划。

步骤 6 点击菜单中的**部署 (Deploy)** 按钮，然后点击**立即部署 (Deploy Now)** 按钮 ( )，以部署对设备的更改。

只有将更改部署至设备，更改才会生效。

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。