Cisco Secure Firewall 200 Threat Defense

Cisco Secure Firewall Threat Defense
Updated NaN,

第

1

章

:

请检查您的软件版本，必要时重新进行映像，获取许可证，并确保能够正常连接。

Cisco Secure Firewall 200 具备下一代防火墙功能，专为分布式企业和小型分支机构设计。它在紧凑的设备形态下提供强大、经济高效的安全防护和简化管理，确保网络边缘的安全优化连接。Cisco Secure Firewall 200：

- 将思科混合网状防火墙架构扩展至分支边缘
- 提供人工智能驱动的检测和统一安全策略
- 集成 SD-WAN 功能，提升应用性能和用户访问可靠性
- 提供应用和用户控制、高效分段以及专为成本敏感型环境定制的高级安全特性。

在分支安装防火墙，并使用中央 在外部接口上对其进行管理。

> **注**
>
> 对于高可用性，如果使用 零接触调配，我们建议使用管理接口。如果您在外部使用 零接触调配，并希望使用高可用性，则必须在注册后将外部 IP 地址更改为静态地址。

如何开启 Secure Firewall 200 并通过检查前面板电源和系统状态 LED 确认启动成功。

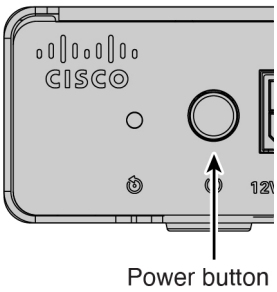
为防火墙提供可靠的电源（例如，使用不间断电源(UPS)）非常重要。未事先关闭就断电可能会导致严重的文件系统损坏。后台始终有许多进程在运行，因此断电会使得系统无法正常关闭。

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**
>
> 首次启动防火墙时，Firewall Threat Defense 初始化大约需要 15 到 30 分钟。

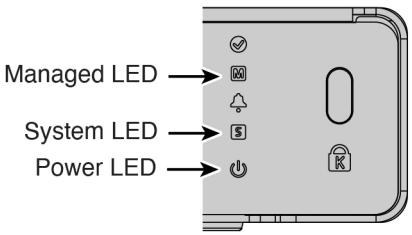
1. 将电源线一端连接到防火墙，另一端连接到电源插座。
2. 使用位于机箱背面电源线旁边的电源按钮打开电源。

1:



3. 检查 LED 的当前状态。

2: LED



- 电源 LED - 呈绿色常亮表示防火墙已通电。
- 系统 (S) LED - 请参阅以下行为：

1: (S) LED

LED 行为	说明	设备通电后的时间 （分:秒）
绿色快速闪烁	正在启动	01:00
琥珀色快速闪烁（错误状态）	未能启动	01:00
绿灯常亮	已加载应用	15:00-30:00

LED 行为	说明	设备通电后的时间 （分:秒）
琥珀色常亮 （错误条件）	应用加载失败。	15:00-30:00

- 托管 (M) LED — 将外部接口连接到互联网（请参阅为防火墙布线 在第 12 页）后，检查托管 LED 以检查零接触调配的云连接状态。

2: (M) LED

M LED	说明	设备通电后的时间 （分:秒）
绿色慢速闪烁	已连接到思科云，准备好载入	15:00 - 30:00
绿色和琥珀色交替闪烁 （错误情况）	设备无法连接到思科云。	15:00 - 30:00
绿灯常亮	已自行激活	20:00 - 45:00

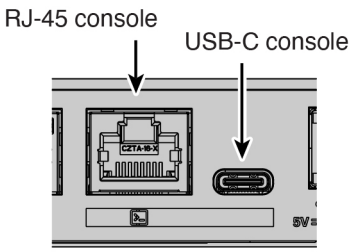
Firewall Threat Defense ASA

了解如何通过将控制台端口连接至设备并识别 CLI 提示符，判断您的 Secure Firewall 200 运行的是 Firewall Threat Defense 还是 ASA。

硬件上支持Firewall Threat Defense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。

1. 使用任一端口类型连接到控制台端口。

3:



2. 请参阅 CLI 提示，确定防火墙运行的是Firewall Threat Defense还是 ASA。

Firewall Threat Defense

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Firewall Threat Defense CLI 在第 6 页。

```
firepower login:
```

ASA

您将看到 ASA 提示。

```
ciscoasa>
```

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。

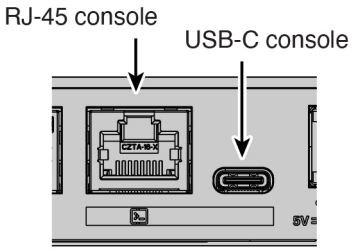
Firewall Threat Defense CLI

如何访问 Secure Firewall 200 上的 Firewall Threat Defense CLI 以进行执行设置与故障排除（包括登录 FXOS 并在需要时切换至 FTD CLI）。

您可能需要访问 CLI 进行配置或故障排除。

1. 使用任一端口类型连接到控制台端口。

   4:



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#
```

3. 切换到 Firewall Threat Defense CLI。

> **注**
>
> 如果要使用防火墙设备管理器进行初始设置或使用，请不要访问Firewall Threat Defense CLI，否则会启动 CLI 设置。
>
> 对于零接触调配，如果您必须访问 CLI 并运行设置脚本，请在系统出现以下提示时回答：**n**是否要配置 IPv4□(y/n) [y]：和是否要配置 IPv6□(y/n) [y]：。您还必须接受默认本地管理器：本地管理设备□(yes/no) [yes]：。

connect ftd

首次连接到 Firewall Threat Defense CLI 时，系统会提示您完成初始设置。

```
firepower# connect ftd
>
```

要退出 Firewall Threat DefenseFTD CLI，请输入 **exit** 或 **logout** 命令。此命令会将您重新导向至 FXOS 提示。

```
> exit
firepower#
```

了解如何在开始配置前检查当前 Firewall Threat Defense 软件版本，并决定是否将 Secure Firewall 200 重映像至目标版本。

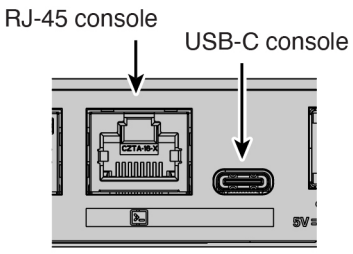
我们建议您在配置防火墙之前安装目标版本。或者，您也可以在启动并运行后执行升级，但升级（保留配置）可能需要比按照此程序花费更长的时间。

我应运行哪个版本？

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。

1. 使用任一端口类型连接到控制台端口。

   5:



2. 在 FXOS CLI 中，显示正在运行的版本。

   scope ssa

show app-instance

```
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
```

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

   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。

      对于零接触调配，当您载入设备时，请务必为**密码重置**区域选择**否**，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 在第 9 页。

了解如何在思科智能软件管理器和思科商务工作空间中获取 Secure Firewall 200 许可证，包括识别所需的许可证类型和用于订购额外权利的许可证 PID。

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。

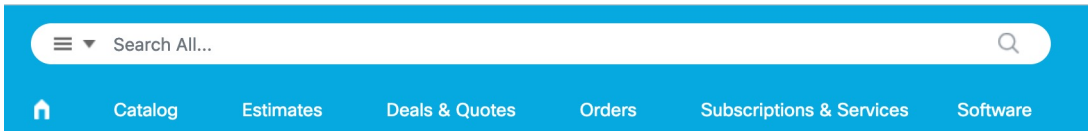
如果尚未注册，请向智能软件管理器注册 。注册需要您在智能软件管理器中生成注册令牌。有关详细说明，请参阅*Cisco Secure Firewall Management Center* 管理指南。

Firewall Threat Defense 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

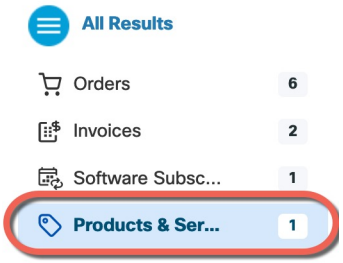
1. 如果您需要自己添加许可证，请前往思科商务工作空间并使用**搜索全部 (Search All)** 字段。

   6:



2. 搜索许可证 PID。咨询您的订购指南以了解您想要的 PID。
3. 从结果中选择**产品和服务 (Products & Services)**。

7:



如何使用 FXOS CLI shutdown 命令或 关机工作流安全关闭 Secure Firewall 200，以避免文件系统损坏。

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。

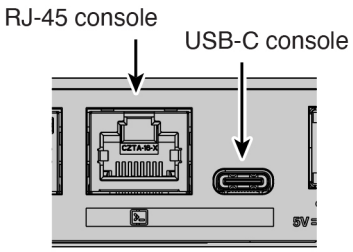
CLI

了解如何从 FXOS CLI 关闭 Secure Firewall 200，以便在断电或移动设备前干净地停止系统。

您可以使用 FXOS CLI 安全地关闭系统并关闭防火墙电源。

1. 使用任一端口类型连接到控制台端口。

8:



2. 在 FXOS CLI 中，连接到 local-mgmt 模式。

   firepower # connect local-mgmt

3. 关闭系统。

   firepower(local-mgmt) # shutdown

```
firepower(local-mgmt)# shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
```

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]
```

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。

如何从 关闭 Secure Firewall 200 以便安全关闭设备（即使是在对其进行远程管理也是如此）。

使用正确关闭系统。

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。
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。
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

：

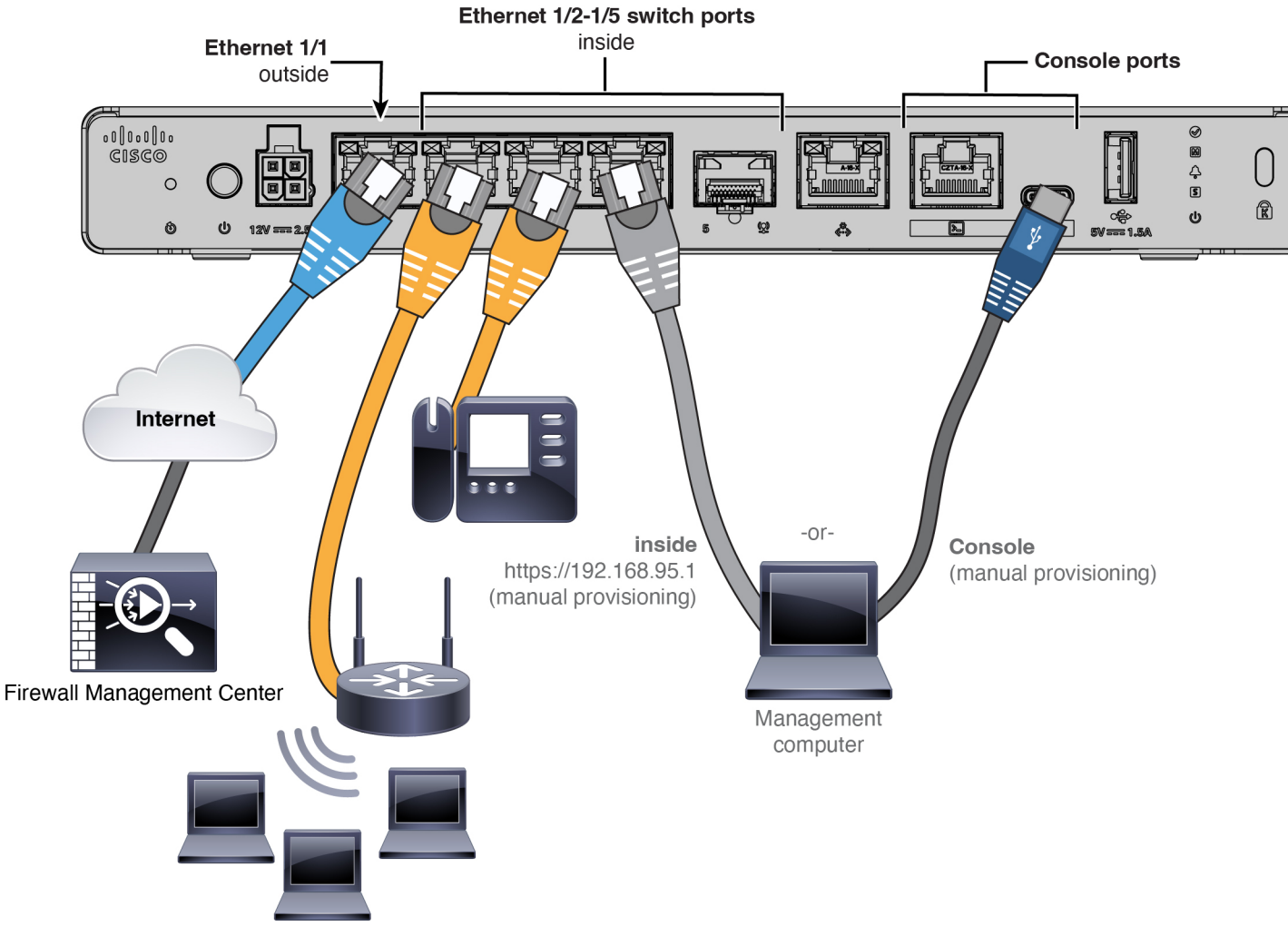
- □□□□□□
- □□□□□□□□□□□□
- □□□□□□□□□□□□□□

将您的Secure Firewall 200连接到网络并注册至管理中心。

连接防火墙，然后将防火墙注册到。

了解如何为 Secure Firewall 200 布线，以便在配置前完成初始硬件设置并为网络连接准备好所需端口。

- 将 SFP 安装到以太网 1/5 - 该端口是需要 SFP 模块的 1 Gbps SFP 端口。
- 有关详细信息，请参阅硬件安装指南。
- 如果使用 零接触调配，请勿同时使用电缆连接外部接口和管理接口。本指南介绍了外部接口上的管理，但您可能希望在具有高可用性的管理上使用 零接触调配。如果您在外部使用 零接触调配，并希望使用高可用性，则必须在注册后将外部 IP 地址更改为静态地址。



如何完成手动配置的初始 Secure Firewall 200 设置，以便设备具有基本网络设置并准备好注册到 。

对于手动调配，请使用 Cisco Secure Firewall 设备管理器 或 CLI 来执行行初始配置。

了解使用 防火墙设备管理器 在 Secure Firewall 200 上运行初始设置向导，在将设备注册到 之前准备好外接口和管理连接。

使用这种方法，在注册防火墙后，除管理接口外还将预先配置以下接口：

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

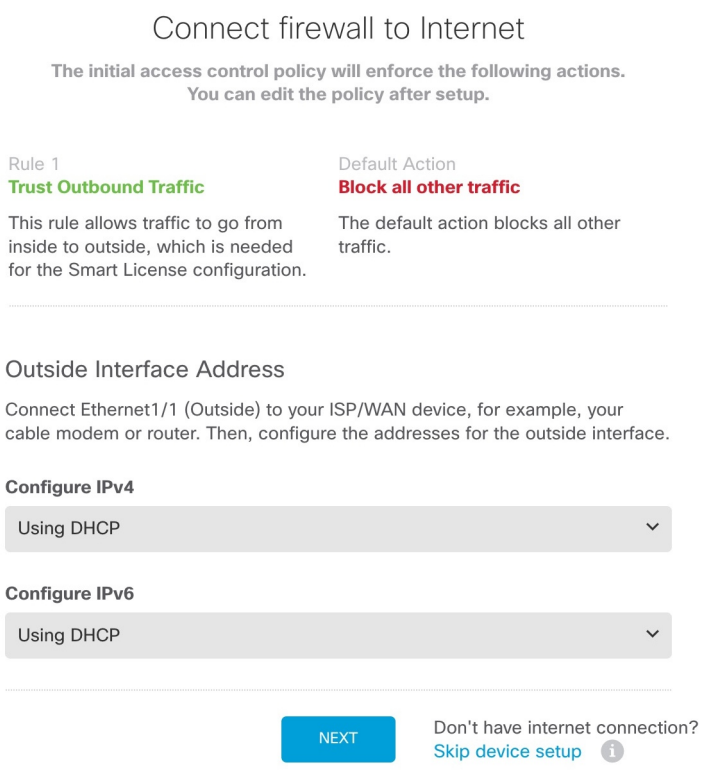
不会保留其他设置，如内部的 DHCP 服务器、访问控制策略或安全区域。

1. 将计算机连接到内部接口。
2. 登录防火墙设备管理器。
   a) 转至https://192.168.95.1。
   b) 使用用户名 **admin** 和默认密码 **Admin123** 登录。
   c) 系统会提示您阅读并接受“一般条款”并更改管理员密码。
3. 使用设置向导。

> **注**
>
> 具体的端口配置取决于您的型号。

   a) 配置外部接口和管理接口。

9:



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

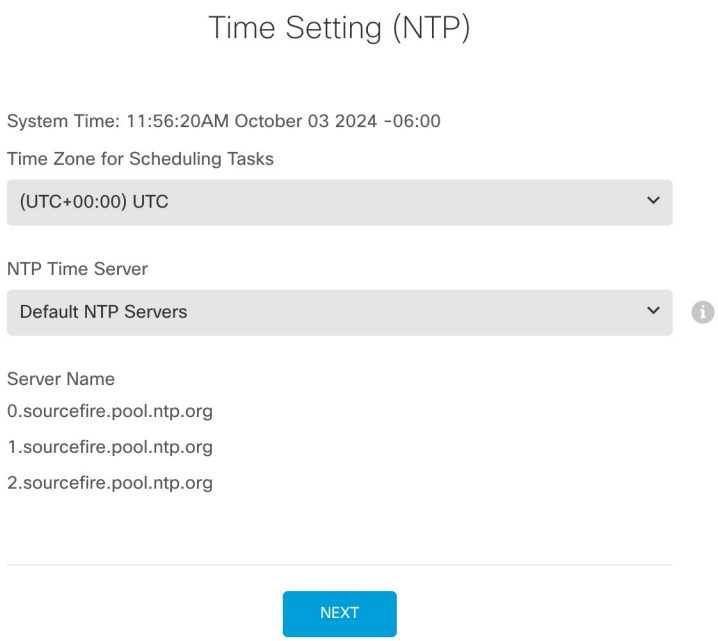
2. **管理接口 -** 即使在外部接口上使用管理器访问，也会使用管理接口设置。例如，通过外部接口在背板上路由的管理流量将使用这些管理接口 DNS 服务器，而不是外部接口 DNS 服务器解析 FQDN。

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

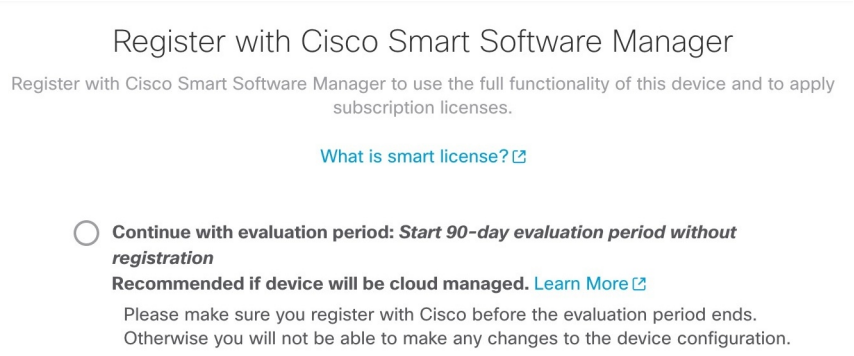
   防火墙主机名

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

10: (NTP)



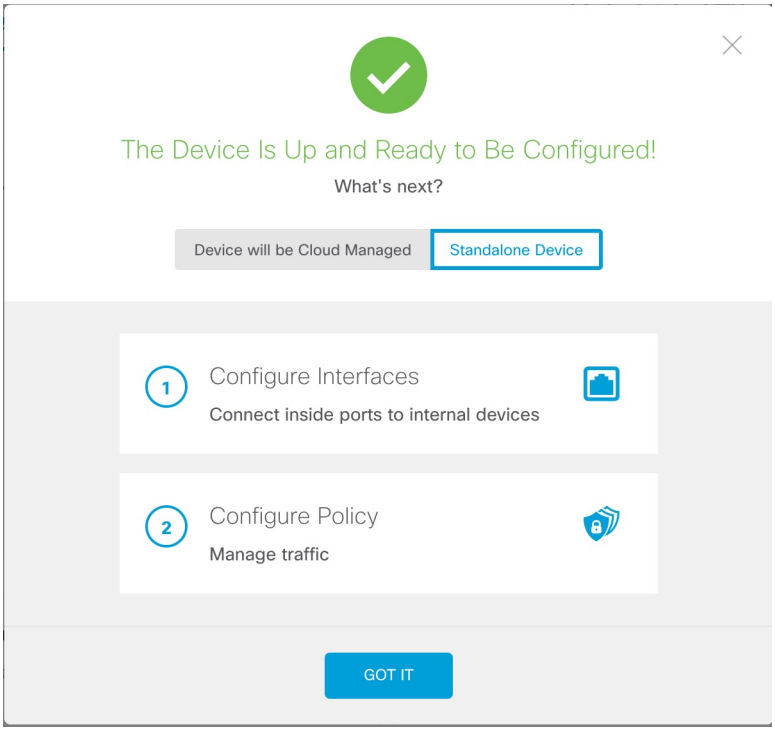
c) 选择启动 **90** 日评估期而不注册。



不要向智能软件管理器注册 Firewall Threat Defense；所有许可均在 Security Cloud Control 上执行。

d) 点击完成。

11:



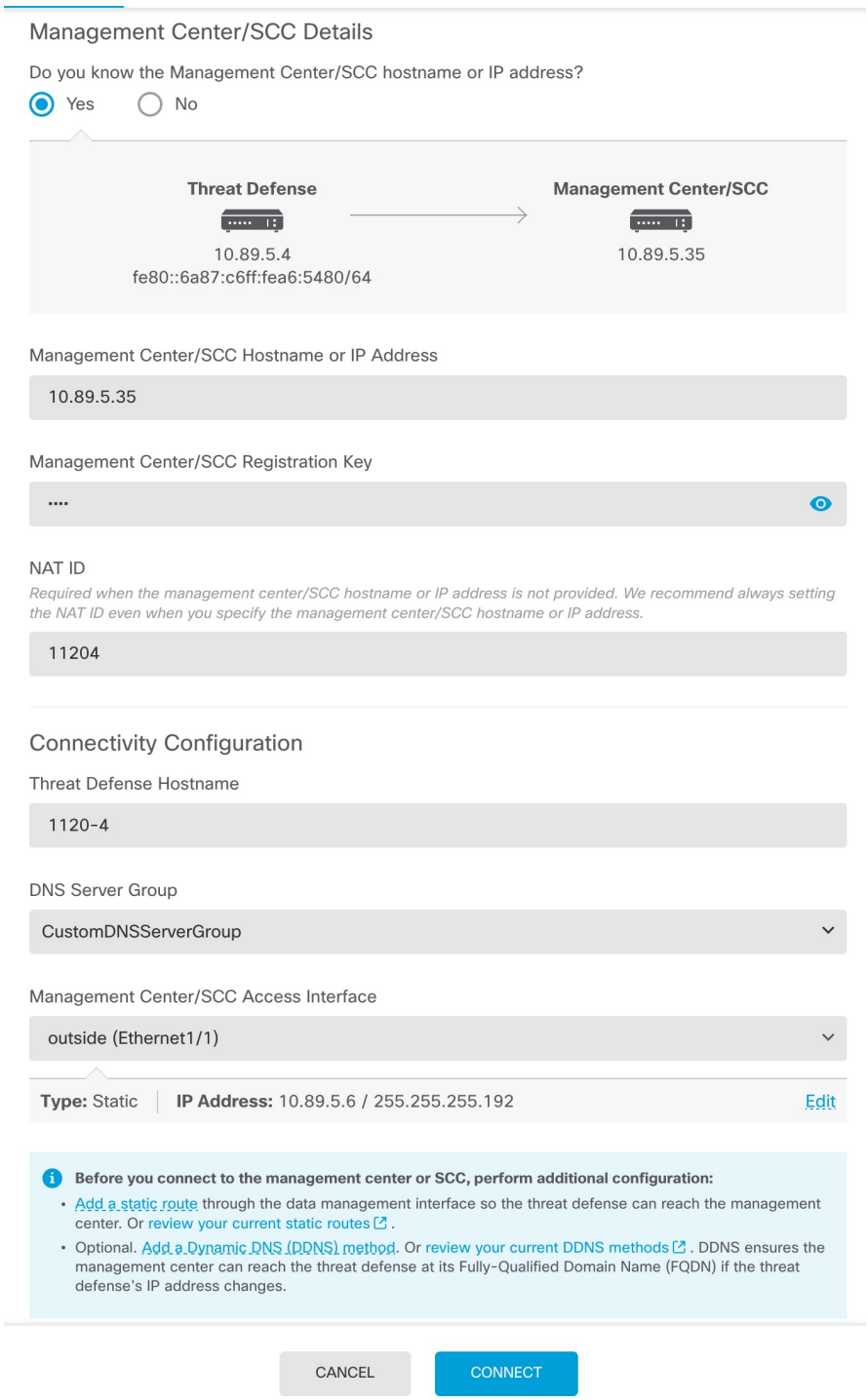
e) 依次选择**独立设备 (Standalone Device)** 和 **明白 (Got It)**。

4. 如果要配置其他接口，请选择**设备 (Device)**，然后点击**接口 (Interfaces)** 摘要中的链接。
5. 通过选择**设备 > 系统设置 > 集中管理**并点击**继续**，向 Security Cloud Control 注册。

   配置 **管理中心/SCC/详细信息 (Management Center/SCC/Details)**。

> **注**
>
> 较早的版本可能会显示“CDO”而不是“SCC”。

12: **/SCC**



a) 对于 **是否知道管理中心/SCC 主机名或 IP 地址**，如果您可以使用 IP 地址或主机名访问 ，请点击**是 (Yes)**，如果 位于 NAT 之后或没有公共 IP 地址或主机名，请点击**否 (No)**。

b) 如果选择**是**，则输入 **管理中心/SCC 主机名/IP 地址**。

c) 指定 **管理中心/SCC 注册密钥**。

此密钥是您选择的一次性注册密钥，注册 防火墙时也要在 上指定它。注册密钥必须为 2 到 36 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 可用于将多个防火墙注册到 。

d) 指定 **NAT ID**。

此 ID 是您选择的唯一一次性字符串，您还需要在 上指定它。即使您知道两台设备的 IP 地址，我们仍建议您指定 NAT ID。NAT ID 必须介于 2 到 36 个字符之间。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防火墙注册到 。NAT ID 与 IP 地址结合使用，用于验证连接是否来自正确的设备；只有在对 IP 地址/NAT ID 进行身份验证后，才会检查注册密钥。

6. 配置**连接配置**。
   a) 指定**威胁防御主机名**。

      此 FQDN 将用于外部接口。

   b) 指定 **DNS 服务器组**。

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

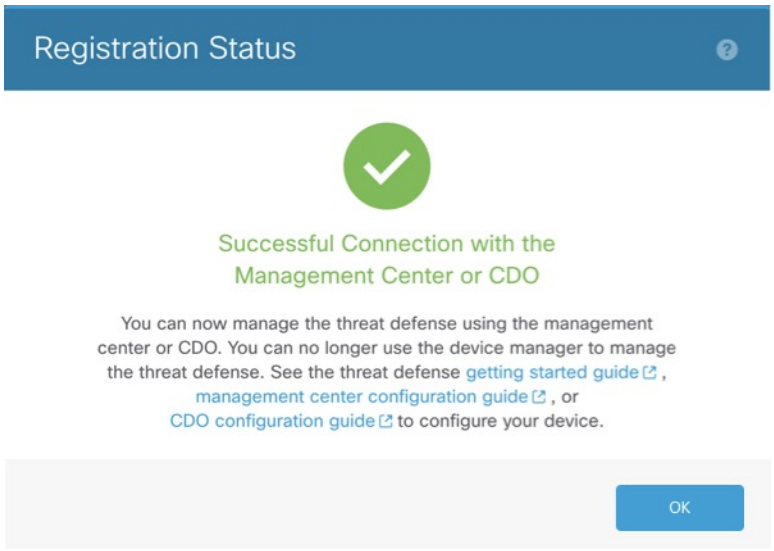
      要在注册后保留外部 DNS 服务器设置，您需要在 中重新配置 DNS 平台设置。

   c) 对于 **管理中心/SCC 访问接口**，点击 **数据接口**，然后选择 **外部**。
7. 可选： 点击**添加动态 DNS (DDNS) 方法 (Add a Dynamic DNS [DDNS] method)**。

   如果 Firewall Threat Defense 的 IP 地址发生变化，DDNS 将确保 可访问其 FQDN 内的 Firewall Threat Defense。
8. 点击**连接 (Connect)**。

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

   13:



9. 在状态屏幕上完成 **保存管理中心/SCC 注册设置** 步骤之后，转到Security Cloud Control，然后添加防火墙。请参阅使用手动调配添加防火墙 在第 26 页。

CLI

如何使用 CLI 设置脚本配置 Secure Firewall 200 管理寻址并设置外接口管理器访问，以便将设备注册到 。

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。

1. 连接控制台端口并访问 Firewall Threat Defense CLI。请参阅访问Firewall Threat Defense CLI 在第 6 页。
2. 完成管理界面设置的 CLI 设置脚本。

> **注**
>
> 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'
```

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

指南： 输入 **no** 以使用 。

```
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.
>
```

3. 配置用于管理器访问的外部接口。

   configure network management-data-interface

   按下 **Enter** 键后，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 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.

>
```

4. 识别 。

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

   - {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} - 指定 的 FQDN 或 IP 地址。如果 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Firewall Threat Defense时也要在上指定它。注册密钥必须为 2 到 36 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 上指定它。NAT ID 必须介于 2 到 36 个字符之间。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 。

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

5. 关闭 Firewall Threat Defense，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。

了解如何使用 零接触调配 或手动注册将 Secure Firewall 200 注册到，以开始集中管理。

根据您使用的部署方法向 注册防火墙。

如何使用 零接触调配 和设备序列号将设备添加到，以便您可以在无需本地预配置的情况下注册设备。

- 如果设备没有公共 IP 地址或 FQDN，请为 设置公共 IP 地址/FQDN（例如，如果它在 NAT 之后），以便设备可以发起管理连接。请参阅**管理 > 配置 > 管理器远程访问**。
- 为管理或以太网 1/1 提供 IP 地址和默认网关的 DHCP 服务器。
- 通过网络访问 OpenDNS 公共 DNS 服务器。IPv4：208.67.220.220 和 208.67.222.222；IPv6：2620:119:35::35。系统从不使用从 DHCP 获取的 DNS 服务器。

  需要解析以下名称：

  3: FQDN

FQDNs
*.cisco.com（多个 FQDN）
defenseorchestrator.com
*.defenseorchestrator.eu（供欧盟地区使用，许多 FQDN）
0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org, 3.sourcefire.pool.ntp.org
1.200.159.162.in-addr.arpa
60.19.239.178.in-addr.arpa
connected.by.freedominter.net
time.cloudflare.com
udc.neo4j.org

通过零接触调配，您可以按序列号将设备注册到，而无需在设备上执行任何初始设置。Security Cloud Control 集成以实现此功能。

> 注
>
> 对于 版本 7.4，您需要使用 Security Cloud Control 来添加设备；有关详细信息，请参阅 7.4 指南。7.6 中添加了本地 工作流程。此外，对于 7.4 中的云集成，请参阅中的 **SecureX 集成**页面。

注册后的默认配置

使用零接触调配时，系统会预配置以下接口：请注意，不会保留其他配置设置，例如访问控制策略或安全区。请注意，诸如内部的 DHCP 服务器、访问控制策略或安全区域等其他设置均未配置。

- 以太网 1/1—“外部”，IP 地址来自 DHCP、IPv6 自动配置
- 以太网 1/2（或对于 200，为 VLAN1 接口）-“内部”，192.168.95.1/24
- 默认路由 - 通过外部接口上的 DHCP 获取

要求

当您使用外部接口进行管理器访问时，它会默认使用DHCP。在启用高可用性之前，需要将IP地址更改为静态地址。或者，您可以改用管理接口；在高可用性管理上支持 DHCP。

1. 首次使用序列号添加设备时，请将 与Security Cloud Control集成。

   > 注
   >
   > 对于 高可用性对，您还需要将辅助 与Security Cloud Control集成。

   a) 选择**集成 > 安全云控制**。
   b) 点击**启用安全云控制**打开单独的浏览器选项卡，让您登录Security Cloud Control帐户并确认显示的代码。

      确保此页面未被弹出窗口阻止程序阻止。如果您还没有Security Cloud Control 帐户，您可以在程序期间添加一个。

      有关此集成的详细信息，请参阅 *Cisco Secure Firewall Management Center* 管理指南中的“系统配置”一章。

      Security Cloud Control 会在您将 与Security Cloud Control集成后载入本地 。Security Cloud Control 需要其清单中的，以便 零接触调配 运行。但是，您不需要直接使用 Security Cloud Control。如果您使用 Security Cloud Control，其 支持仅限于设备载入、查看其托管设备、查看与 关联的对象，以及交叉启动 。

   c) 确保选中**启用零接触调配 (Enable Zero-Touch Provisioning)** 。
   d) 点击**保存**。

2. 获取设备的序列号。

   设备包含两个序列号：机箱序列号和 PCB（电路板）序列号。任一序列号均可使用。

   - 如果您有装运箱，则可以在标签上看到机箱序列号。
   - 机箱序列号位于设备。
   - PCB 序列号位于机箱上名为“S/N”的标签上。
   - 您可以使用以下 CLI 命令查看序列号：
     - FXOS CLI - **show chassis detail**显示两个序列号。

- Firewall Threat Defense - **show inventory**显示机箱序列号。**show serial-number**显示 PCB 序列号。

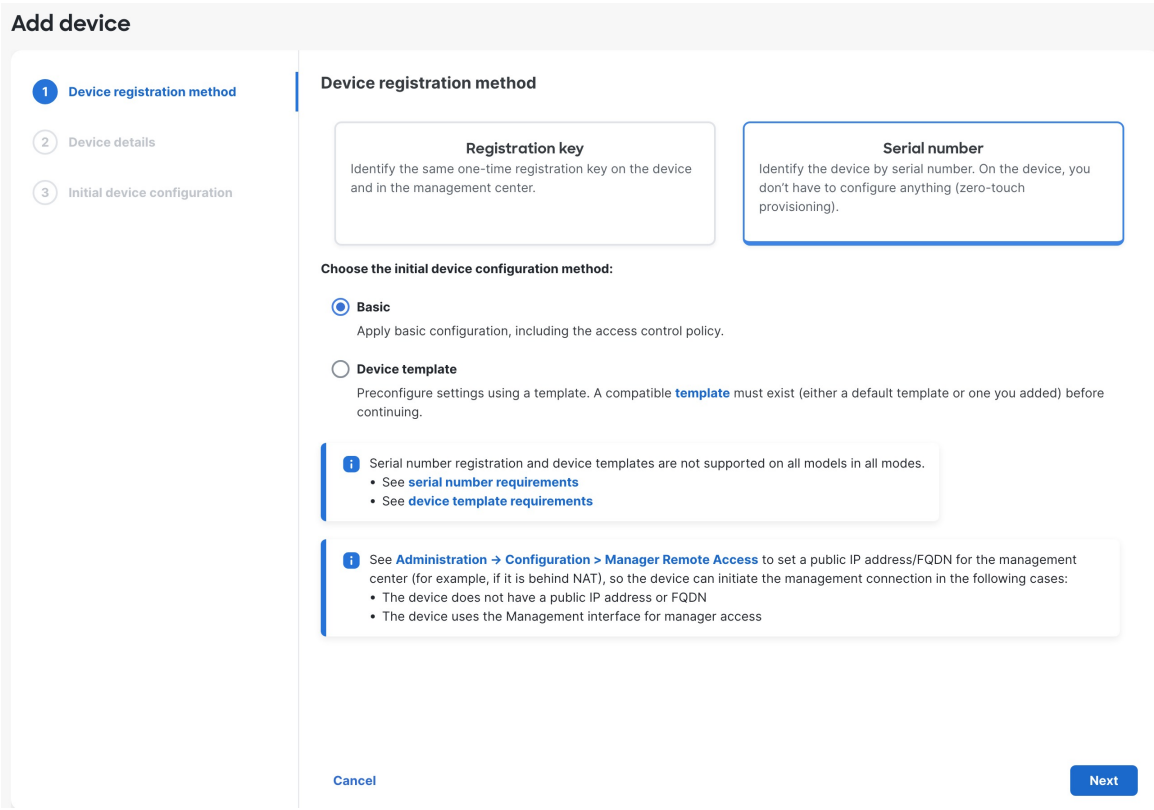
3. 检查 LED，确保防火墙已准备好注册。

4: (M) LED

M LED	说明	设备通电后的时间 （分:秒）
绿色慢速闪烁	已连接到思科云，准备好载入	15:00 - 30:00
绿色和琥珀色交替闪烁（错误情况）	设备无法连接到思科云。	15:00 - 30:00
绿灯常亮	已自行激活	20:00 - 45:00

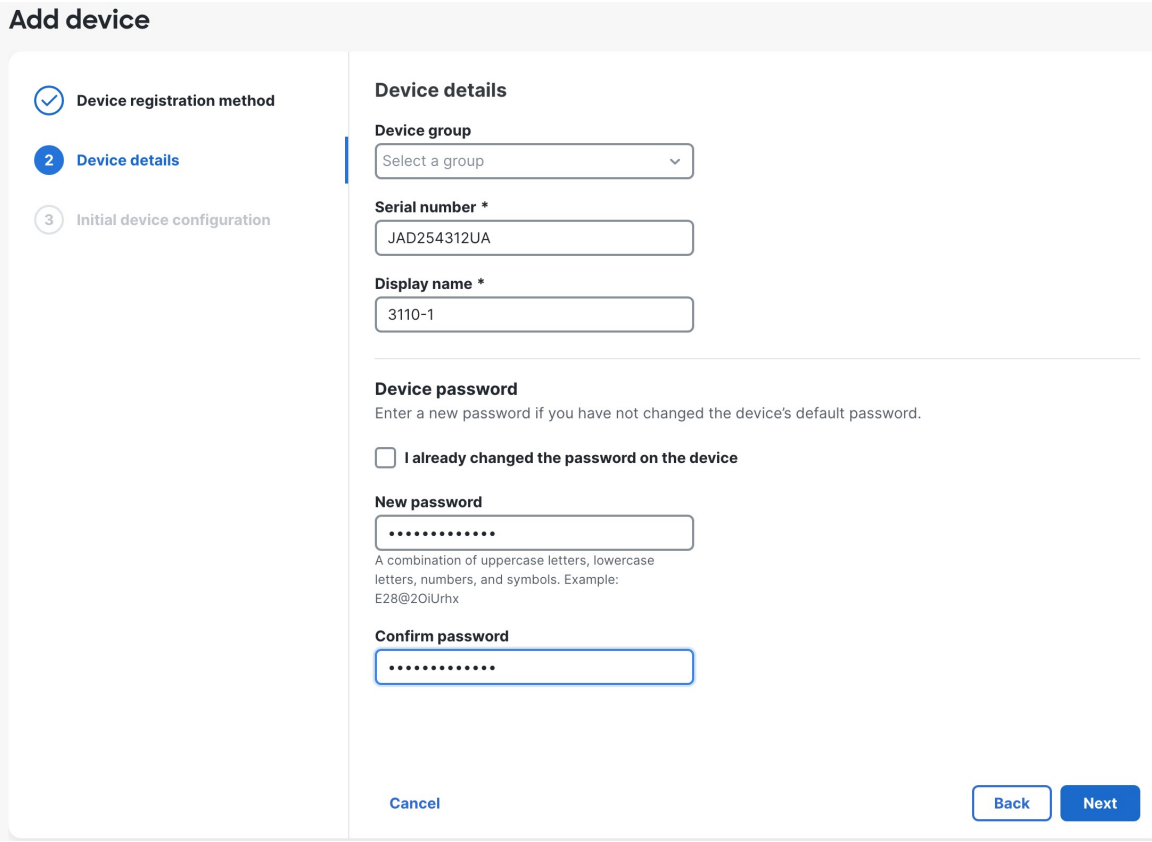
4. 选择**设备 > 设备管理**。
5. 从**添加**下拉菜单中，选择**设备**。
6. 依次点击**序列号**、**基本**和**下一步**。

14:



7. 配置设备详细信息并点击**下一步**。

15:

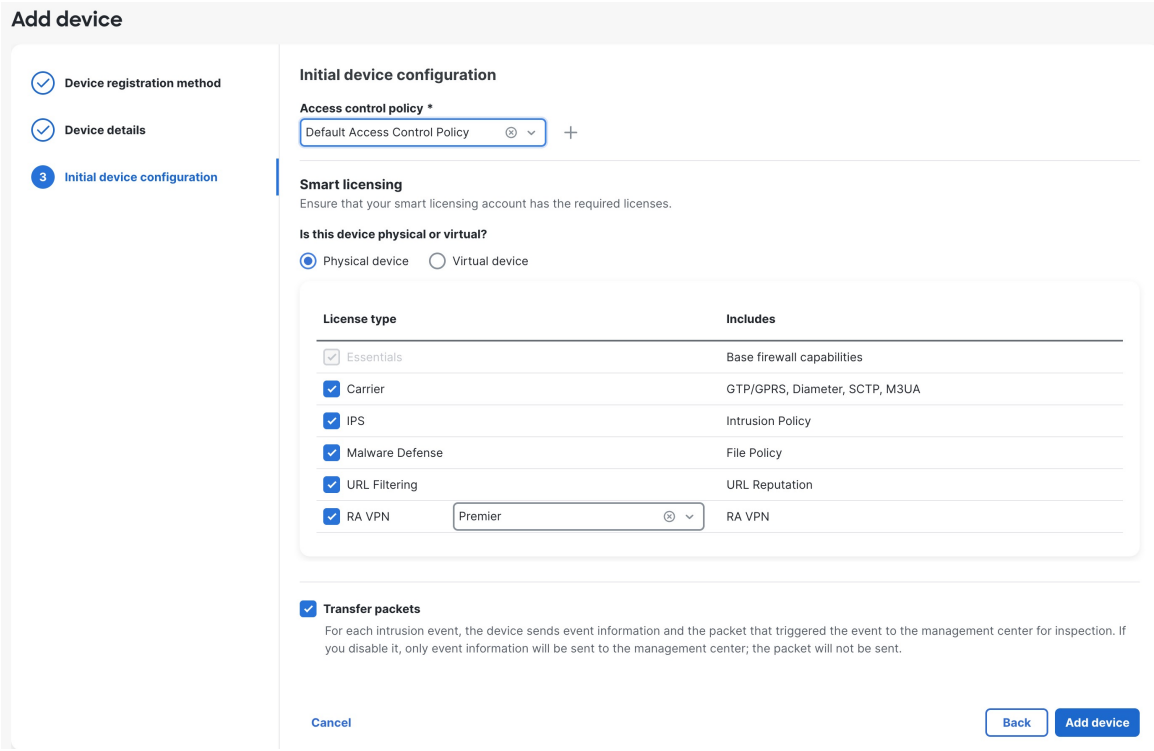


- **域 (Domain)-** 在多域环境中，选择分叶域。
- **设备组-** 在单域环境中，将设备添加到 **设备组**。
- **序列号 -** 输入要添加设备的 IP 地址或主机名。如果您不知道设备的 IP 地址（例如，它位于 NAT 后），请将此字段留空。
- **显示名称 -** 输入要在 中显示的设备名称。之后将无法更改该名称。
- **设备密码 -** 如果此设备未配置或全新安装，则需要设置**新密码**并进行确认。

  仅当您已登录并更改 **密码时，才可检查我已在设备上** 更改密码。否则，注册将失败。

8. 配置初始设备配置。

   16:



- **访问控制策略 -** 选择初始访问控制策略以在注册时部署到设备，或创建一个新策略。 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**添加**(+)，然后选择**阻止所有流量**。之后您可以更改此设置以允许流量通过。
- **智能许可-** 选择您的许可证。
  - **此设备是物理设备还是虚拟设备？-** 选择 **物理设备**
  - **许可证类型-** 选中要分配给设备的每个许可证类型。

  在添加设备后应用许可证。
- **传输数据包 -** 启用此选项，以便对于每个入侵事件，设备会将数据包传输到 进行检查。

  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 进行检查。如果禁用此选项，则只会向 发送事件信息，而不会发送数据包。

9. 点击**添加设备**。

   可能需要长达两分钟来验证设备的心跳并建立通信。

   在外部接口上使用零接触调配时，Security Cloud Control 会充当 DDNS 提供商并执行以下操作：

   - 使用**仅限 FMC (FMC Only)** 方法在外部启用 DDNS。此方法仅支持零接触调配设备。
   - 使用以下主机名映射外部 IP 地址： *serial-number*.**local**。
   - 提供到 的 IP 地址/主机名映射，以便将主机名解析为正确的 IP 地址。
   - 如果 IP 地址发生变化（例如 DHCP 租用更新），则会向 发送通知。

   如果在管理接口上使用零接触调配，则不支持 DDNS。 必须可公开访问，以便设备能够发起管理连接。

   您可以继续使用 Security Cloud Control 作为 DDNS 提供商，也可以稍后将 中的 DDNS 配置更改为其他方法。

如何使用设备主机名或 IP 地址加上注册密钥和 NAT ID 将设备添加到 中。

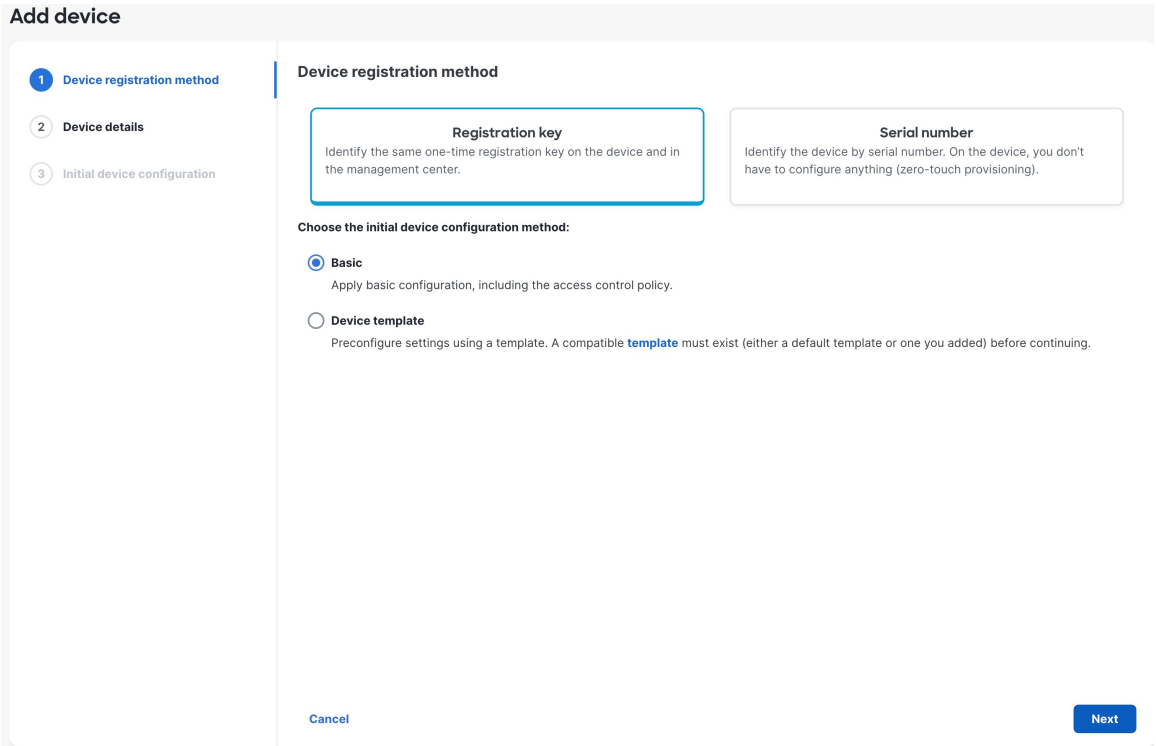
使用设备 IP 地址或主机名以及注册密钥将防火墙手动注册到。

1. 登录。
   a) 输入以下 URL。

      https://*fmc_ip_address*

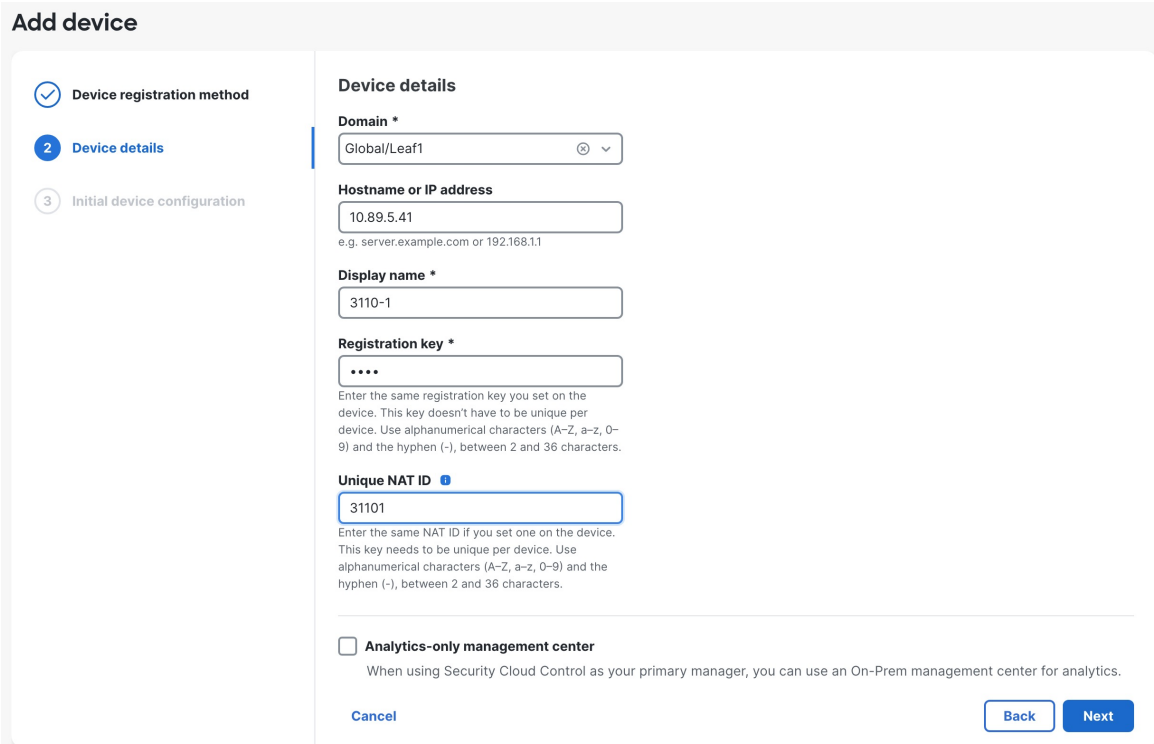
   b) 输入您的用户名和密码。
   c) 点击**登录**。
2. 选择**设备 > 设备管理**。
3. 从**添加**下拉菜单中，选择**设备**。
4. 依次点击**注册密钥**、**基本**和**下一步**。

   17:



5. 配置设备详细信息并点击**下一步**。

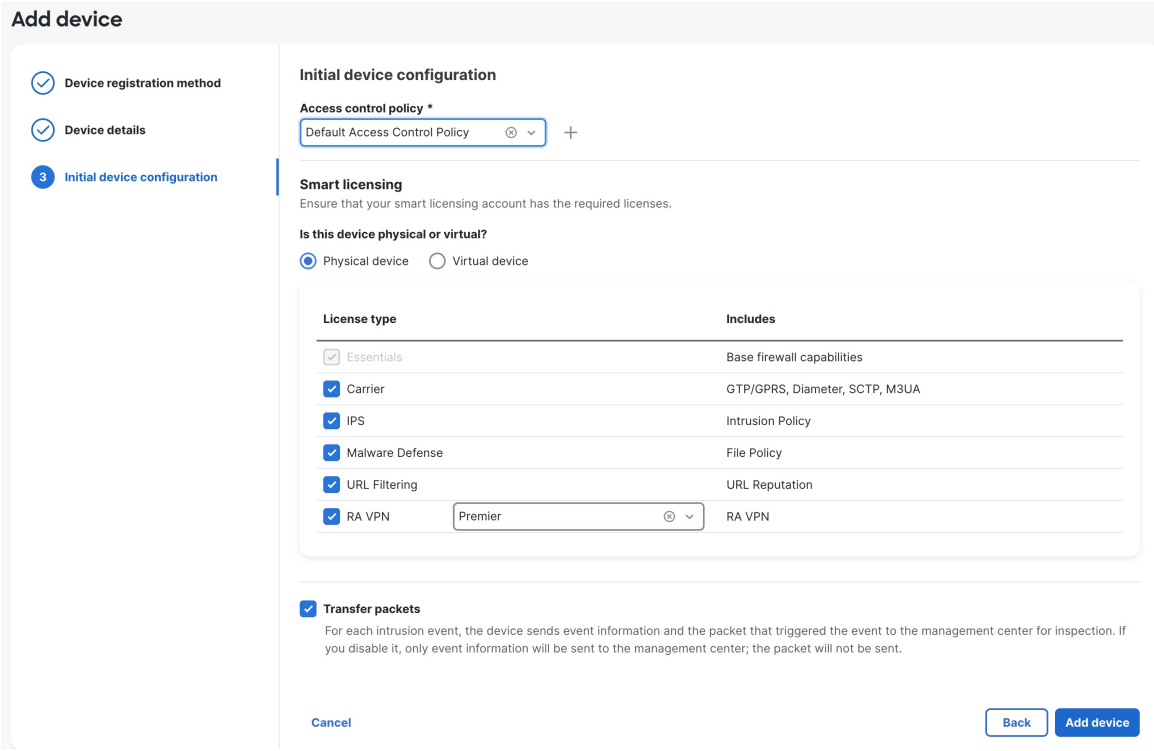
   18:



- **域 (Domain)-** 在多域环境中，选择分叶域。
- **设备组-** 在单域环境中，将设备添加到 **设备组**。
- **主机名或 IP 地址 -** 对于主机，输入要添加设备的 IP 地址或主机名。如果您不知道设备的 IP 地址（例如，它位于 NAT 后），请将此字段留空。
- **显示名称 -** 输入要在 中显示的设备名称。之后将无法更改该名称。
- **注册密钥 -** 输入初始配置中相同的注册密钥。
- **唯一 NAT ID -** 输入初始配置中相同的 ID。
- **仅分析管理中心 -** 除非您知道设备由云交付的防火墙管理中心管理，。

6. 配置初始设备配置。

19:



- **访问控制策略** - 选择初始访问控制策略以在注册时部署到设备，或创建一个新策略。 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**添加**(+)，然后选择**阻止所有流量**。之后您可以更改此设置以允许流量通过。
- **智能许可**- 选择您的许可证。
  - **此设备是物理设备还是虚拟设备？** - 选择 **物理设备**
  - **许可证类型**- 选中要分配给设备的每个许可证类型。

  在添加设备后应用许可证。
- **传输数据包** - 启用此选项，以便对于每个入侵事件，设备会将数据包传输到 进行检查。

  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 进行检查。如果禁用此选项，则只会向 发送事件信息，而不会发送数据包。

7. 点击**添加设备**。

   可能需要长达两分钟来验证设备的心跳并建立通信。如果注册成功，设备将添加到列表中。如果注册失败，您会看到一则错误消息。如果设备注册失败，请检查以下项：

   - Ping - 访问设备 CLI，然后使用以下命令 ping IP 地址：

     ping system *ip_address*

     如果 ping 不成功，使用 **show network** 命令检查网络设置。如果需要更改设备 IP 地址，使用 **configure network {ipv4 | ipv6} manual** 命令。
   - 注册密钥、NAT ID 和 IP 地址 - 确保在两个设备上使用相同的注册密钥和 NAT ID（如有使用）。可以在设备上使用 **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

:

配置基本安全策略以使Secure Firewall 200启动并运行。

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。

了解如何配置 Secure Firewall 200 接口，包括分配内部和外部区域，以及为路由部署设置 IP 地址。

使用 零接触调配 或 防火墙设备管理器 而不是 CLI 进行初始设置时，系统会预配置以下接口：

- 以太网 1/1 - **outside**，IP 地址来自 DHCP、IPv6 自动配置
- VLAN1 - **inside**，192.168.95.1/24
- 默认路由 - 通过外部接口上的 DHCP 获取

如果在向 注册之前在 防火墙设备管理器 中执行其他特定于接口的配置，则会保留该配置。

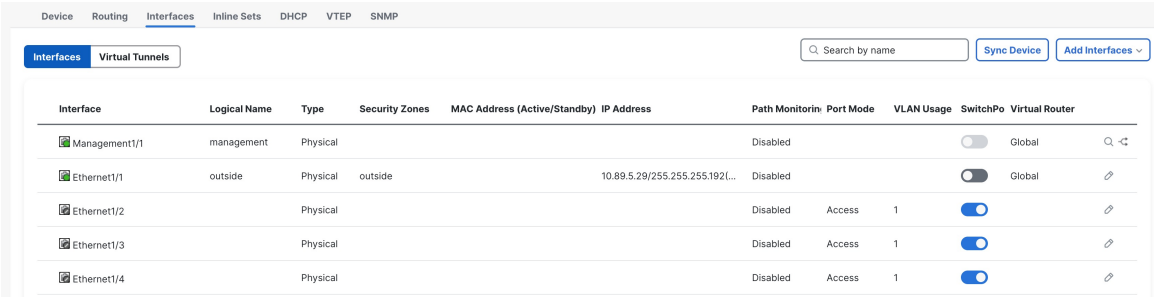
如果使用 CLI 进行初始设置，则无需对设备进行预配置。

在两种情况下，您都需要在注册设备后执行其他接口配置。要进行CLI初始设置，必须为内部交换机端口添加 VLAN1 接口。其他配置包括根据需要将交换机端口转换为防火墙接口、将接口分配给安全区域以及更改 IP 地址。

以下示例配置了一个含静态地址的路由模式内部接口 (VLAN1)，以及一个使用 DHCP 的路由模式外部接口 （以太网 1/1）。它还会为内部 Web 服务器添加一个 DMZ 接口。

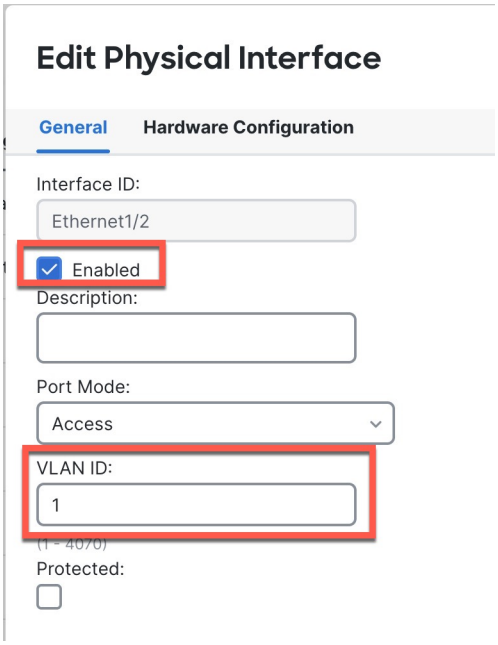
1. 选择**设备 (Devices) > 设备管理 (Device Management)**，然后点击设备的**编辑** (✎)。
2. 点击**接口 (Interfaces)**。

20:



3. 如果使用 CLI 进行初始设置，请启用交换机端口。
   a) 点击交换机端口的 **编辑** (✎)。

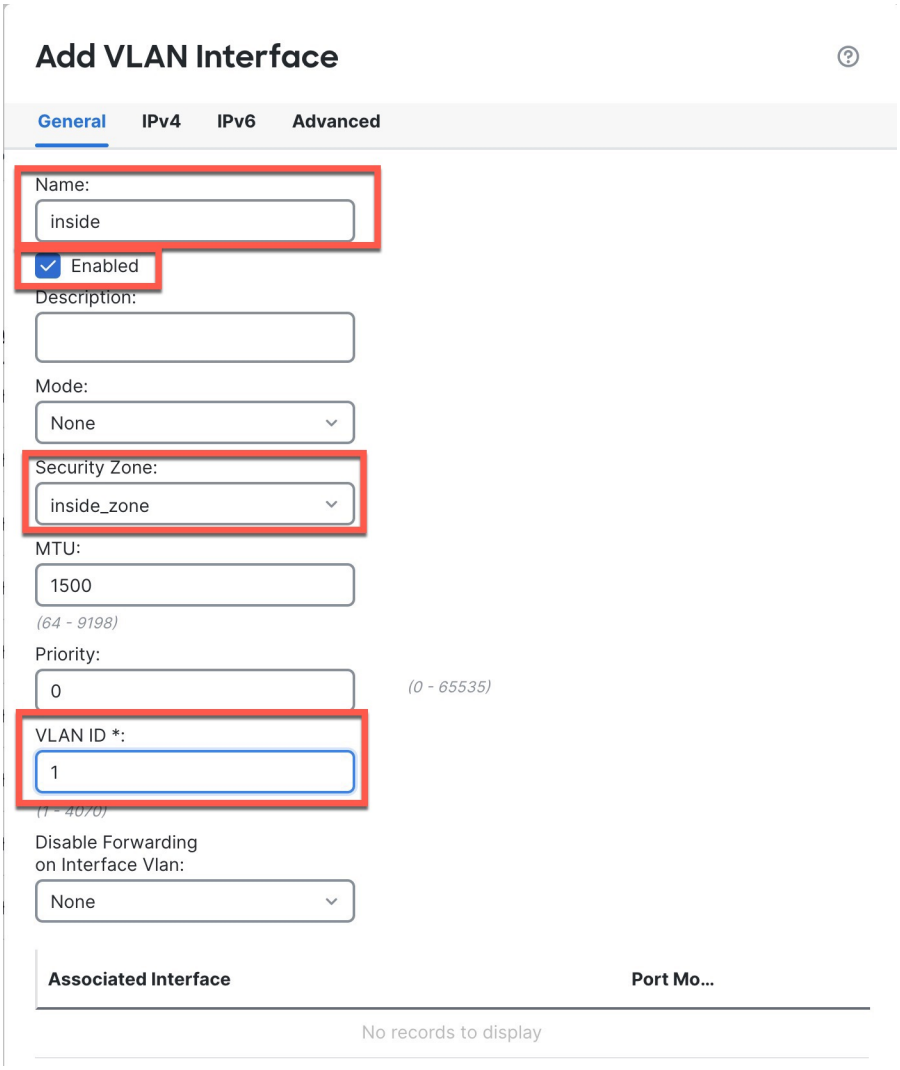
21:



b) 选中**启用**复选框以启用此接口。
c) 可选： 更改 VLAN ID；默认值为 1。接下来，您将添加一个 VLAN 接口来匹配此 ID。
d) 点击**确定**。

4. 添加（或编辑）内部 VLAN 接口。
a) 点击**添加接口 (Add Interfaces)** > **VLAN 接口 (VLAN Interface)**；如果此接口已存在，请点击该接口的 **编辑** ()。

22： VLAN



b) 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。

如果 VLAN1 已预配置，则其余字段为可选。

c) 输入长度最大为 48 个字符的**名称 (Name)**。

例如，将接口命名为 **inside**。

d) 选中**启用 (Enabled)** 复选框。

e) 将**模式 (Mode)** 保留为**无 (None)**。

f) 将 **VLAN ID** 设置为 **1**。

默认情况下，所有交换机端口都设置为 VLAN 1；如果在此处选择不同的 VLAN ID，还需要编辑每个交换机端口，使其位于新 VLAN ID 所对应的 VLAN 上。

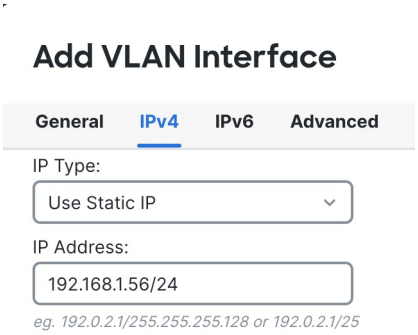
保存接口后，无法更改 VLAN ID；VLAN ID 既是使用的 VLAN 标记，也是您的配置中的接口 ID。

g) 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 **192.168.1.56/24**

23: IP



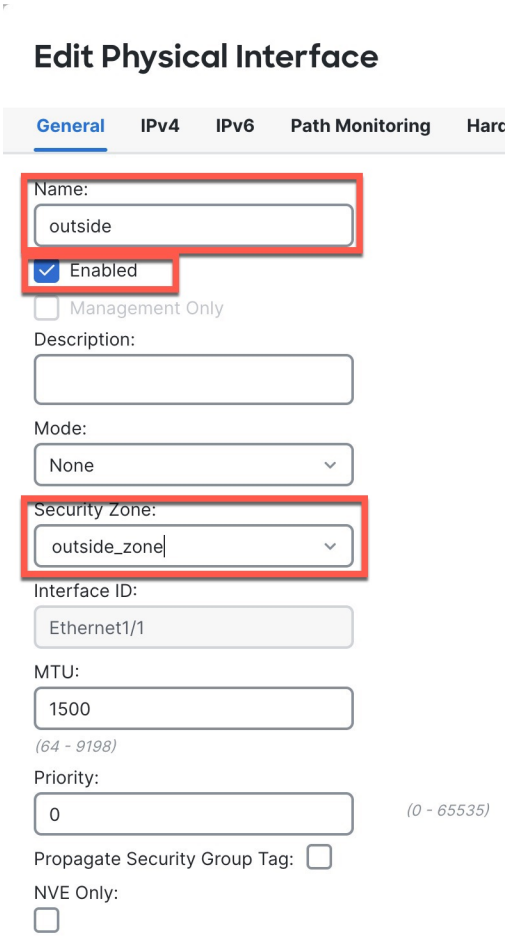
- **IPv6** - 为无状态自动配置选中**自动配置 (Autoconfiguration)** 复选框。

h) 点击**确定**。

5. 点击要用于**外部**的以太网 1/1 的 **编辑** (✎)。

系统将显示**一般 (General)** 窗格。

24:



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 管理连接。

b) 点击**确定**。

6. 例如，配置 DMZ 接口以托管 Web 服务器。
   a) 点击 **SwitchPort** 列中的滑块，禁用要用于 DMZ 的交换机端口的交换机端口模式（ ）。
   b) 点击接口的 **编辑** ()。
   c) 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。

   d) 输入长度最大为 48 个字符的**名称 (Name)**。

      例如，将接口命名为 **dmz**。

   e) 选中**启用 (Enabled)** 复选框。
   f) 将**模式 (Mode)** 保留为**无 (None)**。
   g) 点击 **IPv4** 和/或 **IPv6** 选项卡并配置所需的 IP 地址。
   h) 点击**确定**。
7. 点击**保存**。

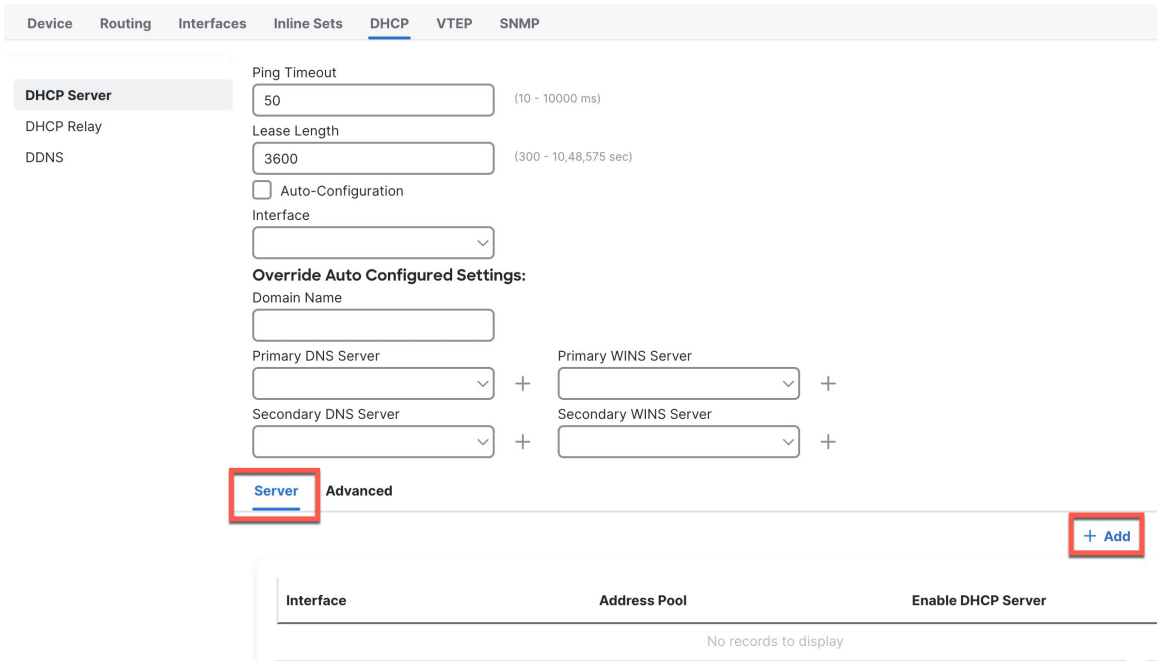
DHCP

如何在 Secure Firewall 200 接口上启用 DHCP 服务器，以便内部客户端可以自动接收 IP 地址和相关网络设置。

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。

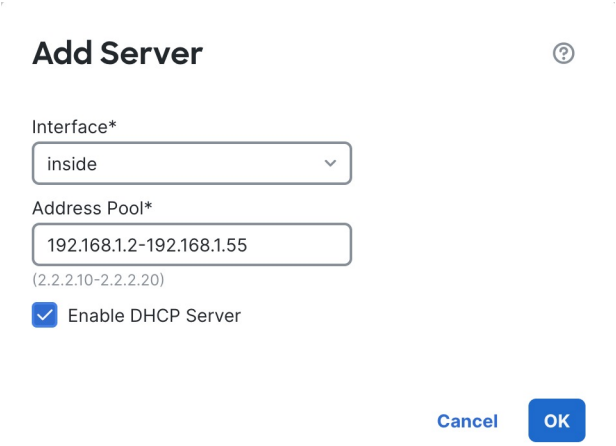
1. 选择**设备 (Devices)** > **设备管理 (Device Management)**，然后点击设备的**编辑** ()。
2. 选择 **DHCP** > **DHCP 服务器 (DHCP Server)**。

25: DHCP



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

26:



- **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。

4. 点击**确定**。
5. 点击**保存**。

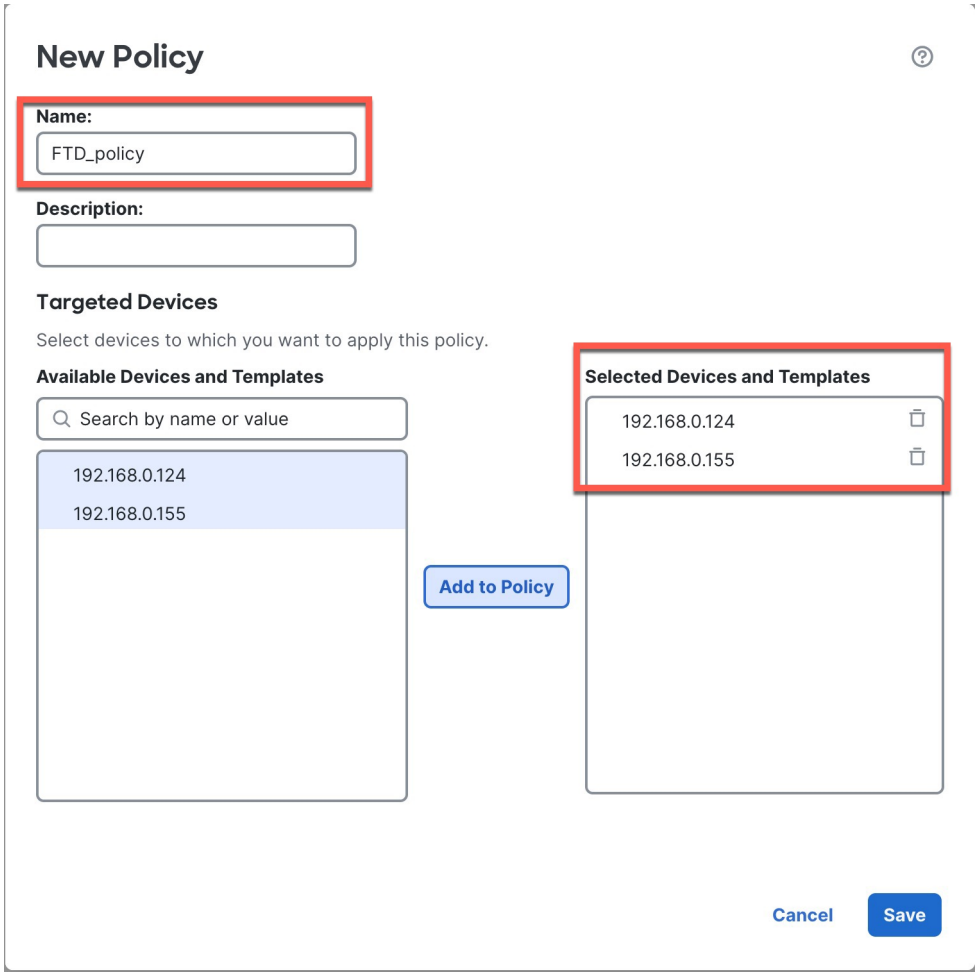
NAT

学习如何创建接口 PAT (NAT) 策略，以便内部客户端可以使用外部接口 IP 地址访问外部网络。

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)*。

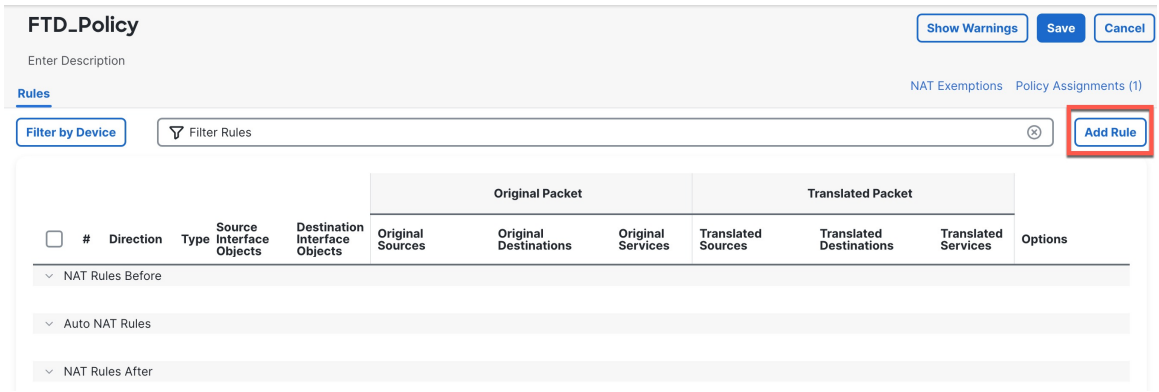
1. 选择**设备 (Devices)** > **NAT**，然后点击**新建策略 (New Policy)**。
2. 为策略命名，选择要使用策略的设备，然后点击**保存**。

27:



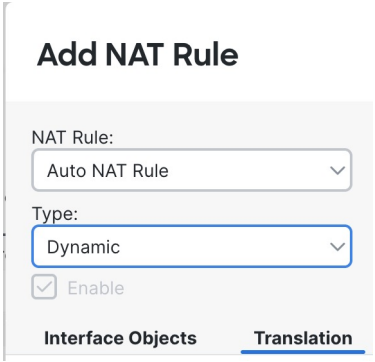
策略即已添加 。您仍然需要为策略添加规则。

28: NAT



3. 点击添加规则 **(Add Rule)**。
4. 配置基本规则选项：

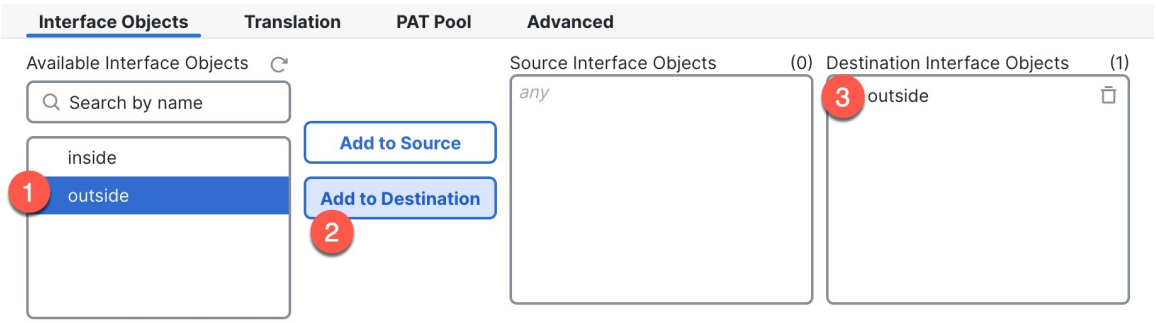
29:



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

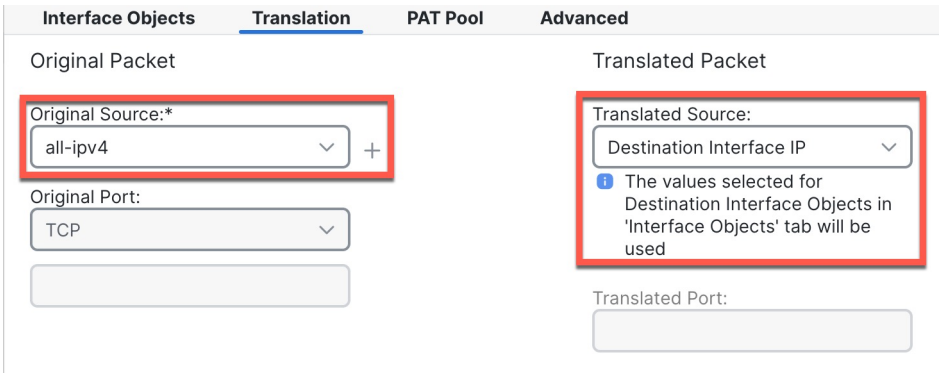
5. 在 **Interface Objects** 页面，将 **Available Interface Objects** 区域中的外部区域添加到 **Destination Interface Objects** 区域。

   30:



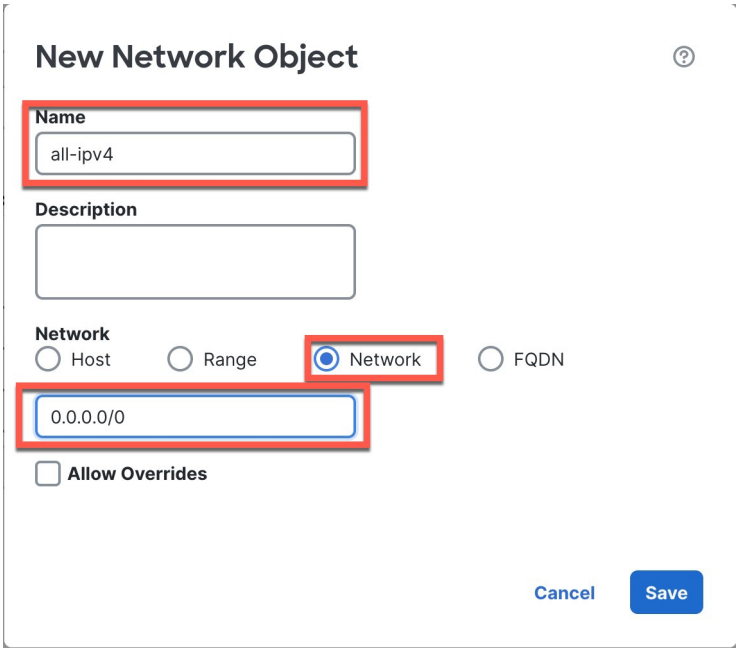
6. 在**转换 (Translation)** 页面上配置以下选项：

   31:



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

  32:



注

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)**。

7. 点击**保存** 以添加规则。

   规则即已保存至 **Rules** 表。

8. 点击 **NAT** 页面上的**保存** 以保存更改。

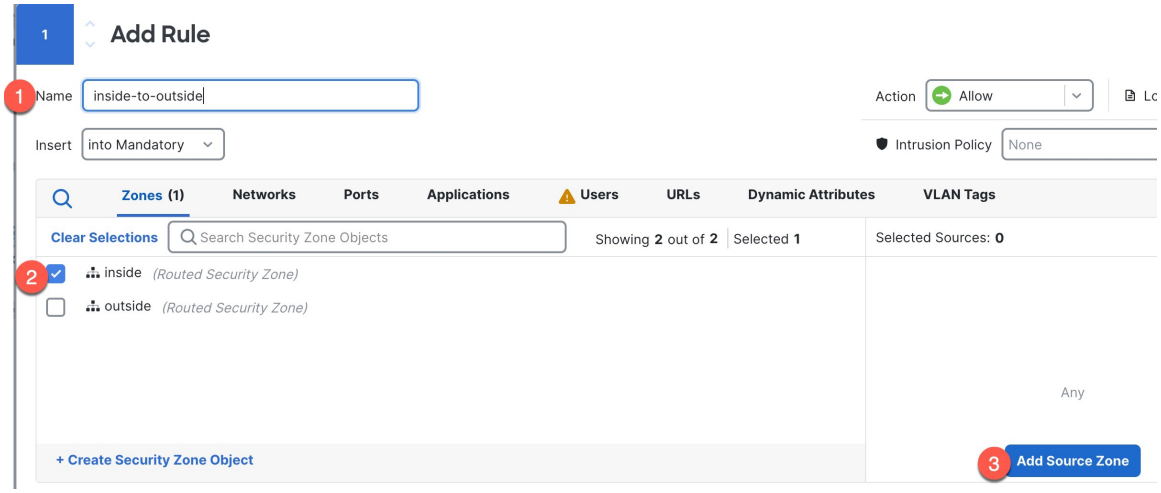
如何添加访问控制规则以允许流量在 Secure Firewall 200 上从内部区域传输到外部区域，并应用可选的安全检测策略。

如果您在注册防火墙时创建了基本的**阻止所有流量**访问控制策略，则需要向该策略添加规则以允许流量通过防火墙。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。

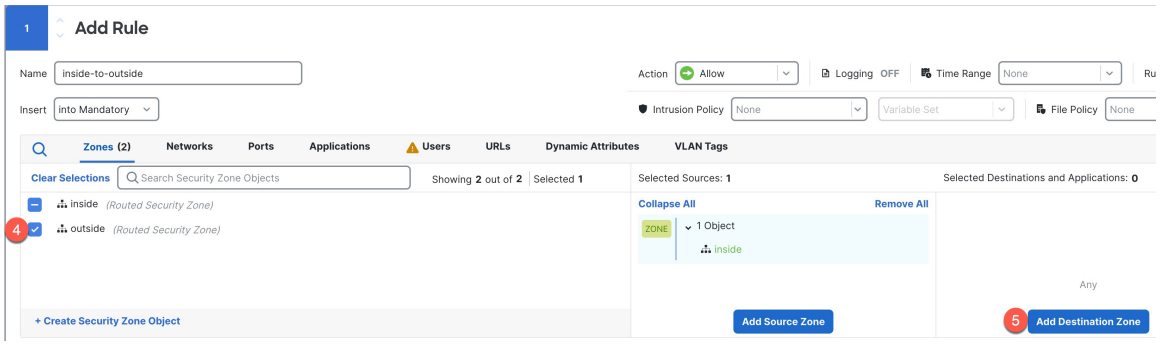
1. 选择 **策略 > 安全策略 > 访问控制**，然后点击分配给设备的访问控制策略对应的 **编辑** ()。
2. 点击**添加规则 (Add Rule)** 并设置以下参数。

33:



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)**。

34:



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。

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。

35:

- **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。安全智能使用信誉智能快速阻止与思科威胁智能组织 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**
>
> 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。

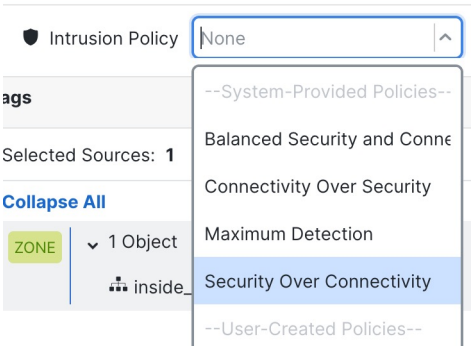
- **身份 -** 默认情况下不应用身份。在允许访问控制策略处理流量之前，可以要求用户进行身份验证。

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。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。

   36:



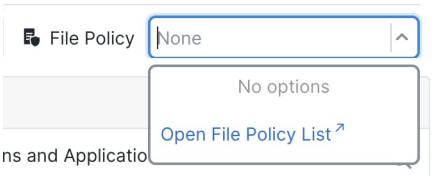
   b) 从列表中选择一个系统提供的策略。

   对于大多数使用场景，我们建议选择**平衡安全与连接** 。

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。

   37:



   对于新策略，系统将在单独的选项卡中打开**策略 > 安全策略 > 恶意软件和文件** 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。

6. 点击**应用 (Apply)**。

   规则即已添加至 **Rules** 表。

7. 点击**保存**。

SSH

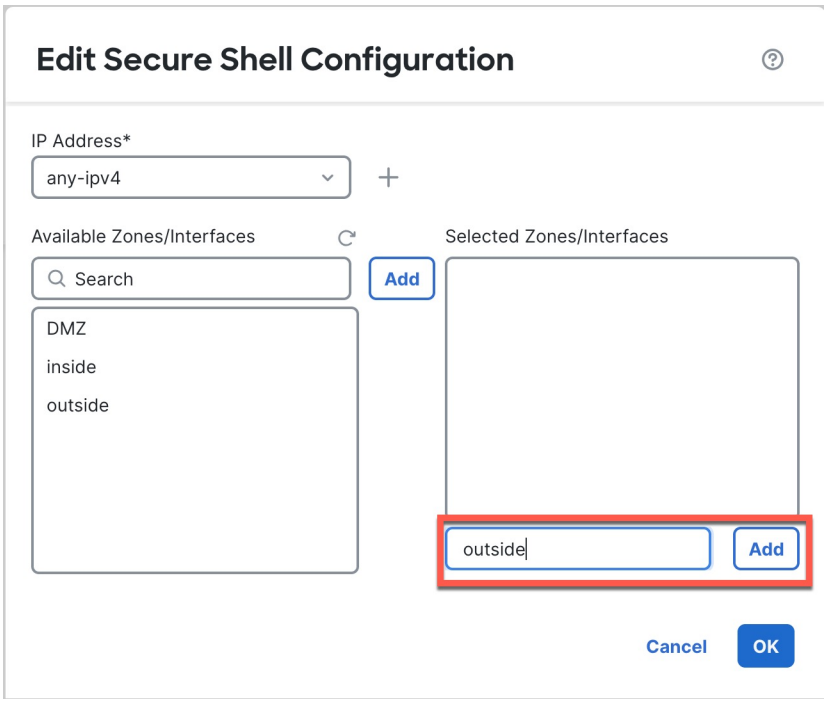
了解如何启用对 Secure Firewall 200 外部接口的 SSH 访问，以便从批准的 IP 地址远程管理设备。

本部分介绍如何启用到外部接口的 SSH 连接，以便远程管理防火墙。

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。

1. 选择 **设备 > 平台设置** 并创建或编辑 Firewall Threat Defense 策略。
2. 选择 **SSH 访问 (SSH Access)**。
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)**。

38: SSH



   c) 点击**确定**。

4. 点击**保存**。

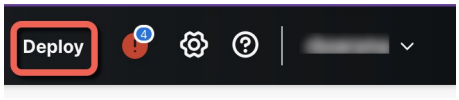
   此时，您可以转至**部署 > 部署**部署并将策略部署到所分配的设备。在部署更改之后，更改才生效。

如何将策略更改部署到 Secure Firewall 200 上，以便接口、NAT、DHCP 和访问控制更新在设备上生效。

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。

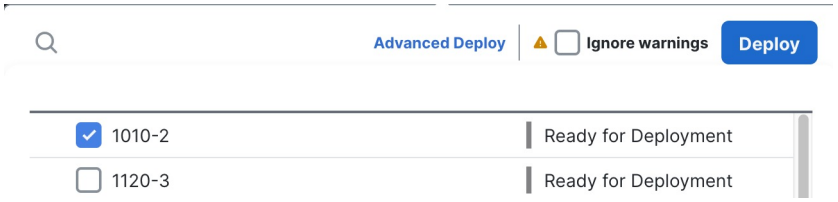
1. 点击右上方的**部署 (Deploy)**。

39:



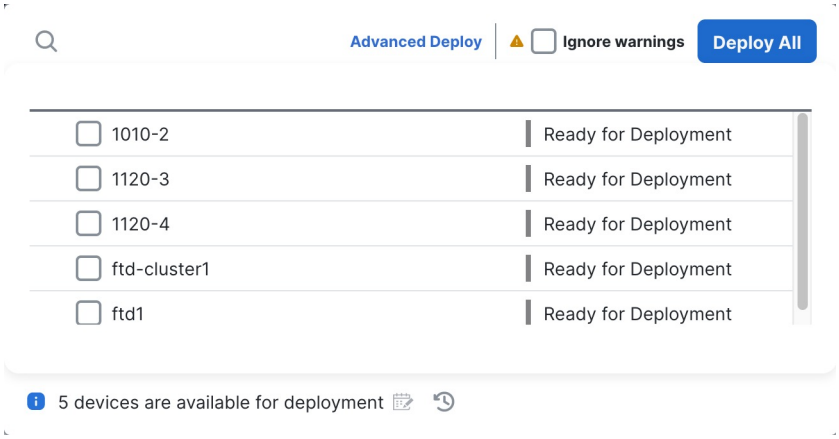
2. 要快速部署，请选中特定设备，然后点击**部署 (Deploy)**。

40:



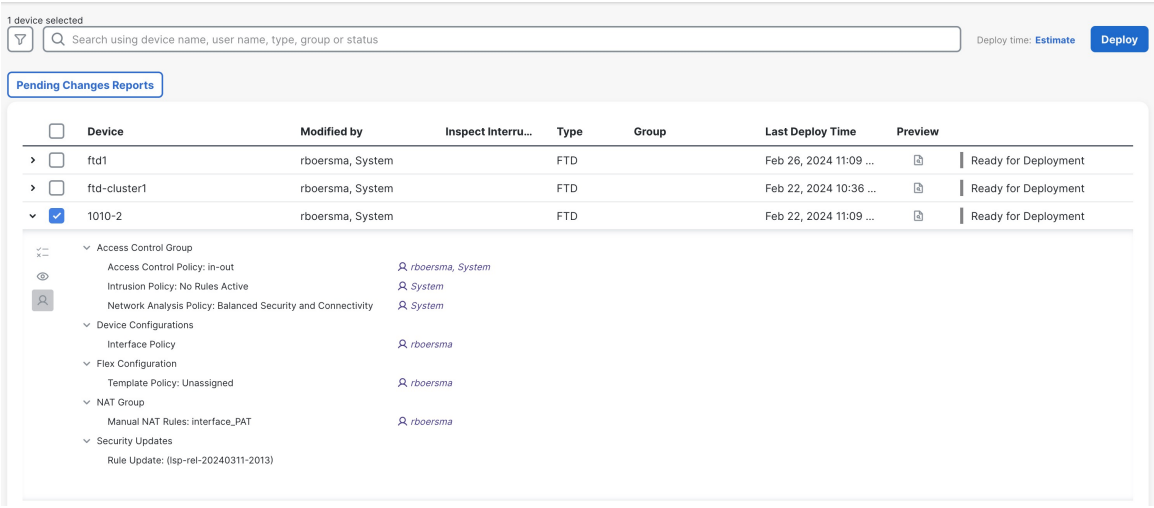
或者，点击**全部部署 (Deploy All)** 以部署到所有设备。

41:



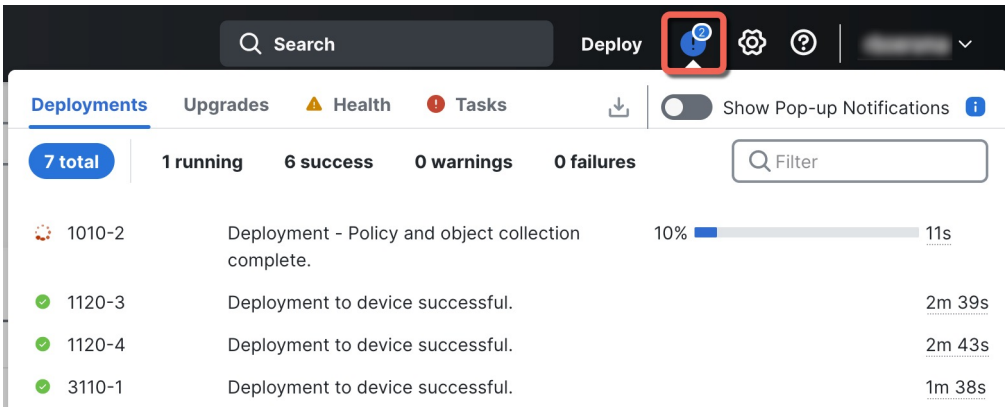
否则，对于其他部署选项，请点击**高级部署 (Advanced Deploy)**。

42:



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。

43:



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。

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。

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。