



Cisco Secure Firewall 200

Cisco Secure Firewall Threat Defense
Updated NaN,

第 1

章

- :
- □□□□□□
- □□□□□□□
- □□□□□□□□□□□□□□**Firewall Threat Defense** □□ ASA□
- □□**Firewall Threat Defense CLI**
- □□□□□□□□□□
- □□□□□ **CLI** □□□□□□□□□□
- □□□□□□
- □□□□□□□□□□□□□□

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。

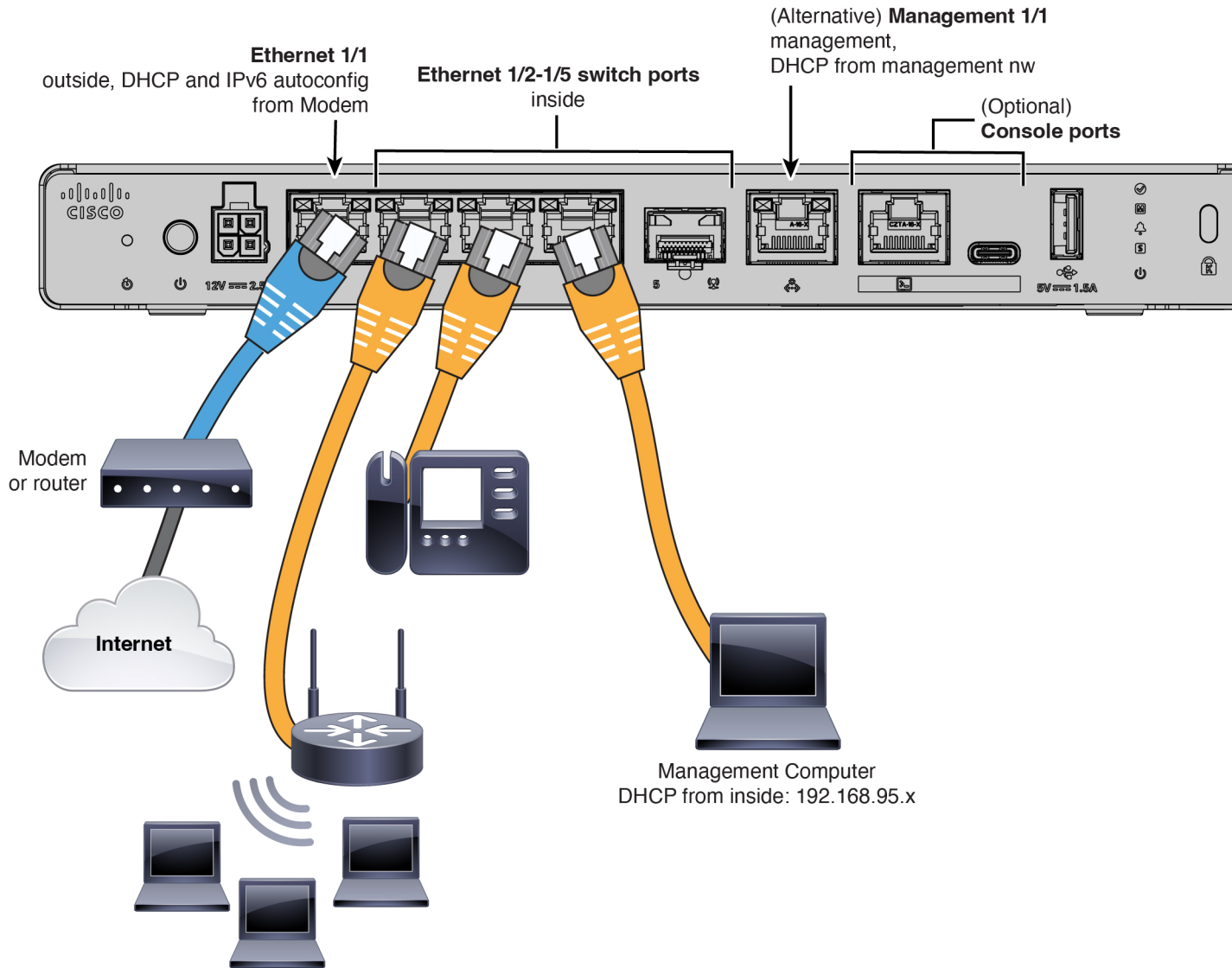
Cisco Secure Firewall 200 具备下一代防火墙功能，专为分布式企业和小型分支机构设计。它在紧凑的设备形态下提供强大、经济高效的安全防护和简化管理，确保网络边缘的安全优化连接。**Cisco Secure Firewall 200:**

- 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。

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

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。

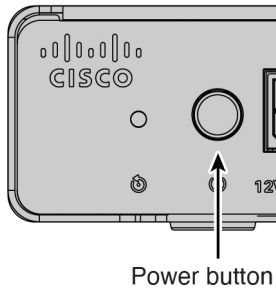
系统电源由位于防火墙后部的电源按钮控制。电源按钮提供软通知，支持平稳地关闭系统以降低系统软件及数据损坏的风险。

 注

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

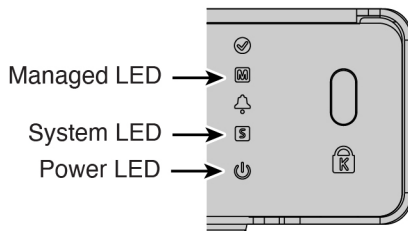
1. 将电源线一端连接到防火墙，另一端连接到电源插座。
2. 使用位于机箱背面电源线旁边的电源按钮打开电源。

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
琥珀色常亮 (错误条件)	应用加载失败。	15:00-30:00

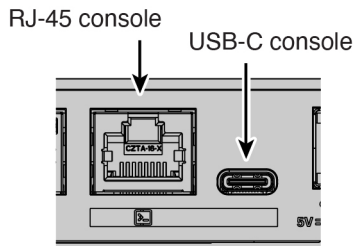
Firewall Threat Defense ASA

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](#)。

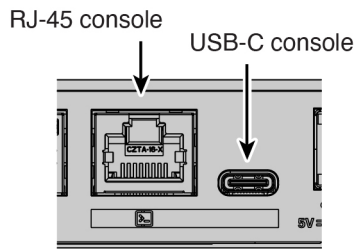
Firewall Threat Defense CLI

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。



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。

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。

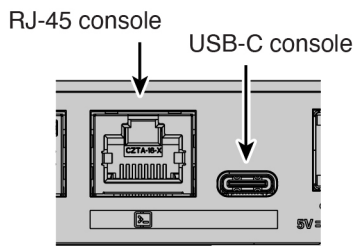
我们建议您在配置防火墙之前安装目标版本。或者，您也可以在启动并运行后执行升级，但升级（保留配置）可能需要比按照此程序花费更长的时间。

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。

CLI

当默认寻址不可用时，如何从 CLI 更改 Secure Firewall 200 管理 1/1 网络设置，以便您能在网络上访问 Cisco Secure Firewall 设备管理器。

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 及更高版本 - 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。

1. 连接到控制台端口。请参阅[安装的是哪个应用程序：Firewall Threat Defense 还是 ASA？](#) 在第 6 页。
2. 连接到 Firewall Threat Defense CLI。

connect ftd

```
firepower# connect ftd
>
```

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 防火墙设备管理器。

4. 在新的管理 IP 地址上登录防火墙设备管理器。

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**。

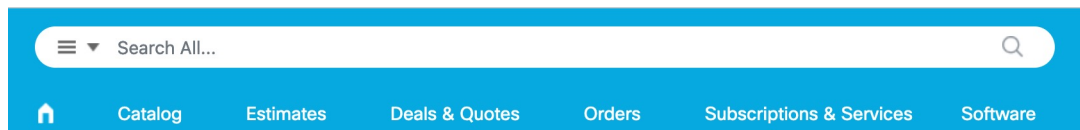
当您从思科或经销商那里购买设备时，您的许可证应该已链接到您的智能软件许可证帐户。如果您没有 [智能软件管理器](#) 帐户，请点击链接 [建立新帐户](#)。

Firewall Threat Defense 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。

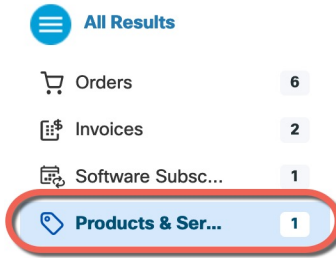
6:



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 防火墙设备管理器 关机 workflow 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。

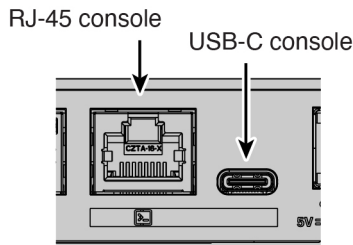
CLI

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 防火墙设备管理器 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）。

使用防火墙设备管理器正确关闭系统。

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。

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

:

- □□□□□□□□□□
- □□□□□□
- □□□□□□□□□□

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。

如何使用默认内部 URL 或 Management 1/1 地址登录 Secure Firewall 200 上的 Secure Firewall 设备管理器，以便开始配置。

登录防火墙设备管理器以配置 Firewall Threat Defense。

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 及更高接口—<https://192.168.95.1>
- 管理 1/1 - https://management_ip (从 DHCP)

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

了解如何在 Secure Firewall 设备管理器中完成初始 Secure Firewall 200 设置，使设备具备基本的外部连接能力和可用的内到外策略。

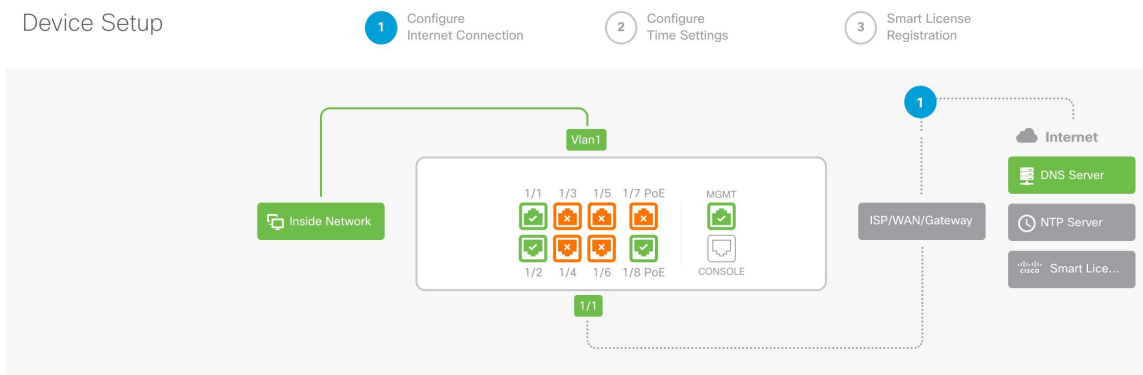
首次登录防火墙设备管理器以完成初始配置时，请使用设置向导。完成设置向导后，您的设备应该会正常工作并部署了几个基本策略：

- 内部→外部流量
- 用于所有对外流量的接口 PAT。

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。

9:



 注

具体的端口配置取决于您的型号。

2. 为外部接口和管理接口配置网络设置。

10:

Connect firewall to Internet

The initial access control policy will enforce the following actions.
You can edit the policy after setup.

<p>Rule 1</p> <p>Trust Outbound Traffic</p> <p>This rule allows traffic to go from inside to outside, which is needed for the Smart License configuration.</p>	<p>Default Action</p> <p>Block all other traffic</p> <p>The default action blocks all other traffic.</p>
---	---

Outside Interface Address

Connect Ethernet1/1 (Outside) to your ISP/WAN device, for example, your cable modem or router. Then, configure the addresses for the outside interface.

Configure IPv4

Using DHCP ▼

Configure IPv6

Using DHCP ▼

NEXT

Don't have internet connection?

[Skip device setup](#) ⓘ

- 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。
3. 配置系统时间设置。
- 11: (NTP)

Time Setting (NTP)

System Time: 11:56:20AM October 03 2024 -06:00

Time Zone for Scheduling Tasks

(UTC+00:00) UTC

NTP Time Server

Default NTP Servers



Server Name

0.sourcefire.pool.ntp.org

1.sourcefire.pool.ntp.org

2.sourcefire.pool.ntp.org

NEXT

- a) 时区
 - b) **NTP** 时间服务器
 - c) 点击下一步。
4. 配置智能许可。

Register with Cisco Smart Software Manager

Register with Cisco Smart Software Manager to use the full functionality of this device and to apply subscription licenses.

[What is smart license? ↗](#)

- Continue with evaluation period: Start 90-day evaluation period without registration**
Recommended if device will be cloud managed. [Learn More ↗](#)
 Please make sure you register with Cisco before the evaluation period ends. Otherwise you will not be able to make any changes to the device configuration.

- Register device with Cisco Smart Software Manager**
 Please register your device at this time. If you do not register now, you can register later from the Device > Smart License page.

1 Create or log in into your [Cisco Smart Software Manager](#) account.



2 On your assigned virtual account, under “General tab”, click on “**New Token**” to create token.



3 Copy the token and paste it here:



Token

```
MDM4MTdhNWEtNmExMC00NzMyLWE3YWtMzY1MWViOTM2Nm
E0LTE3NDU0MzI2%0ANjQyMjV8dUNPZnRLWDJhSFJ6bWc0YkFqVW
ZWQzJzd2JDN2dwRkxhbUhQeHhj%0AZUtnUT0%3D%0A|
```

4 Select the region in which your device is operating.



Region

US Region

5 Enroll Cisco Success Network.

Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.

Check out the [Sample Data](#) that will be sent to Cisco. [See more](#) ▾

Enroll Cisco Success Network

? For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide ↗

BACK

FINISH

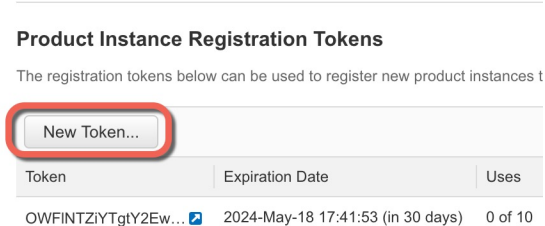
- 点击向思科智能软件管理器注册设备 (**Register device with Cisco Smart Software Manager**)。
- 点击思科智能软件管理器 ([Cisco Smart Software Manager](#)) 链接。
- 点击清单 (**Inventory**)。

[Cisco Software Central](#) > [Smart Software Licensing](#)

Smart Software Licensing

Alerts **Inventory** [Convert to Smart Licensing](#) |

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**：

- 说明
- **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 functionality 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。

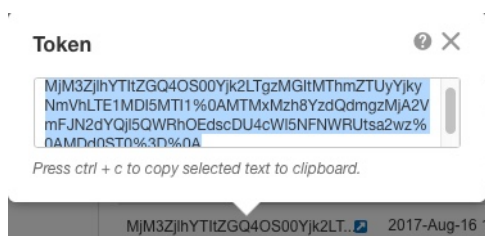
系统将令牌添加到您的清单中。

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 **Firewall Threat Defense** 时，请准备好此令牌，以在该程序后面的部分使用。

12:

General	Licenses	Product Instances	Event Log
Virtual Account			
Description:	[Redacted]		
Default Virtual Account:	No		
Product Instance Registration Tokens			
The registration tokens below can be used to register new product instances to this virtual account.			
New Token...			
Token	Expiration Date	Uses	Export-Controlled
OWFINTZYtY2Ew...	2024-May-18 17:41:53 (in 30 days)	0 of 10	Allowed

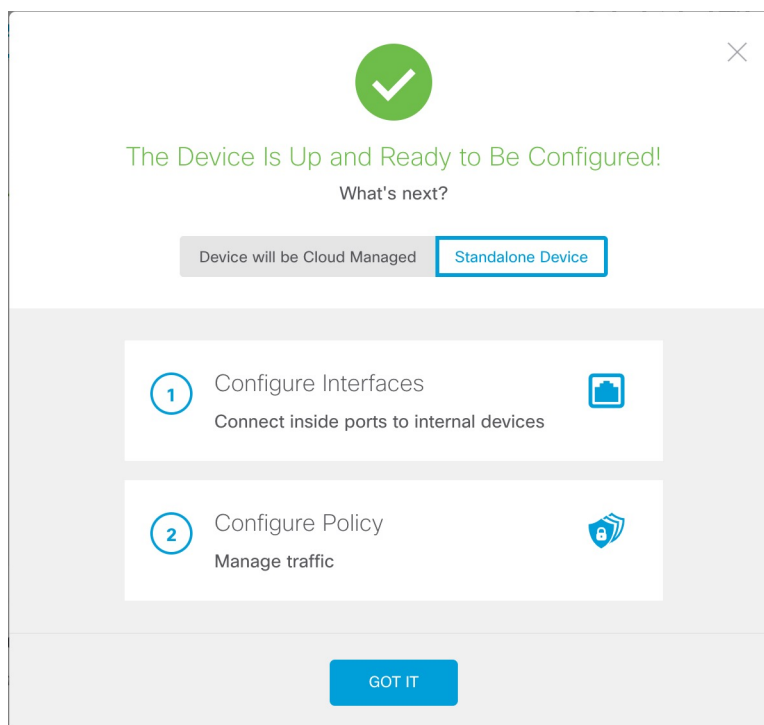
13:



- g) 在 防火墙设备管理器 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)**

5. 完成设置向导。

14:

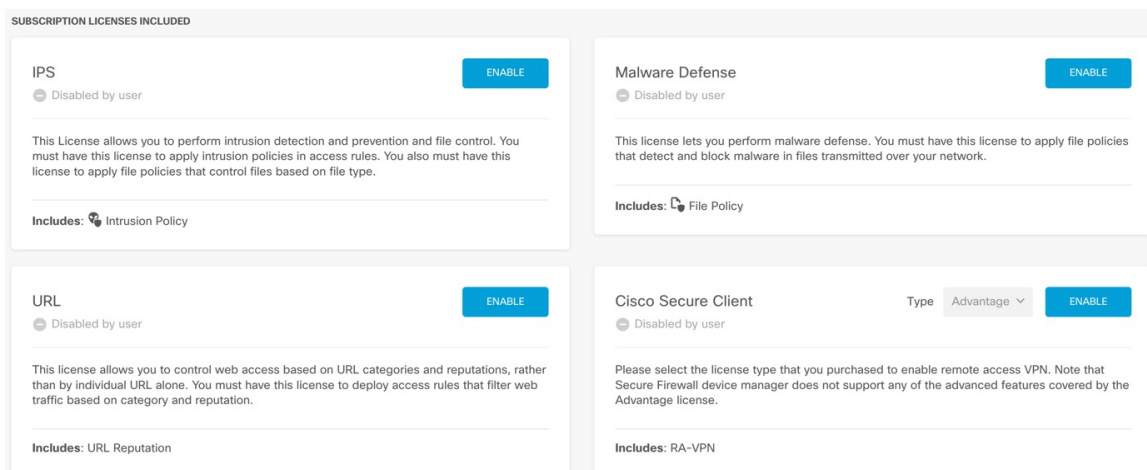


- a) 点击**独立设备 (Standalone Device)** 以使用 防火墙设备管理器。
b) 点击**配置接口 (Configure Interfaces)** 直接转至接口 (**Interfaces**) 页面，点击**配置策略 (Configure Policy)** 转至策略 (**Policies**) 页面，或者点击**知道了 (Got It)** 转至设备 (**Device**) 页面。

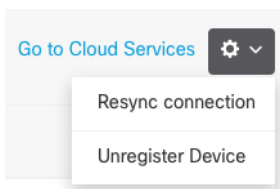
有关接口或策略配置，请参阅[配置网络设置和策略](#) 在第 20 页。

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。



如何在 **Secure Firewall** 设备管理器中配置接口、安全区域、DHCP 和安全策略，使您的 **Secure Firewall 200** 符合网络设计和流量要求。

配置其他接口和 DHCP 服务器，并自定义安全策略。

1. 如果要交换端口转换为防火墙接口，请选择设备 (**Device**)，然后单击接口 (**Interfaces**) 摘要中的链接。
 - a) 单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**)。

15:

Ethernet1/3

Edit Physical Interface

Interface Name

Mode: Switch Port (dropdown menu with options: Routed, Passive, Switch Port) Status

Description

Protected Port

Usage Type: Access (selected), Trunk

Access VLAN: inside (Vlan1)

CANCEL OK

c) 设置名称和 IP 地址。

16:

Ethernet1/3
? ×

Interface Name

Mode
Routed ▼

Status

Most features work with named interfaces only, although some require unnamed interfaces.

Description

IPv4 Address
IPv6 Address
Advanced

Type
Static ▼

IP Address and Subnet Mask
 /
e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

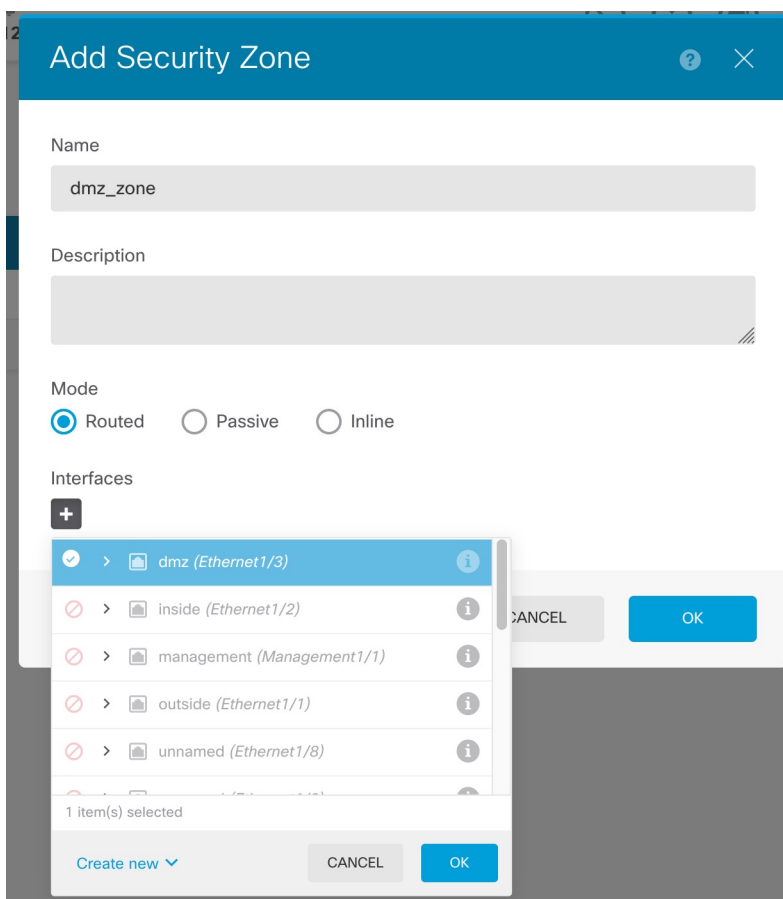
Standby IP Address and Subnet Mask
 /
e.g. 192.168.5.16

CANCEL
OK

d) 点击确定 (OK)。

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。

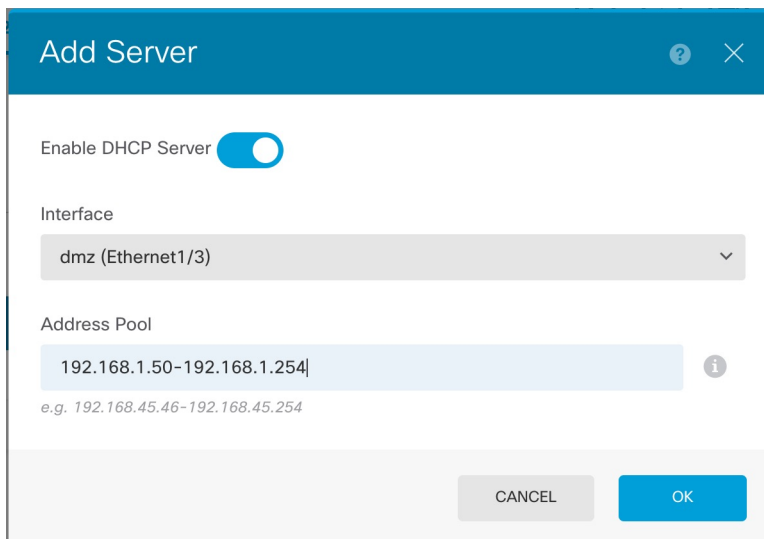
17:



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。

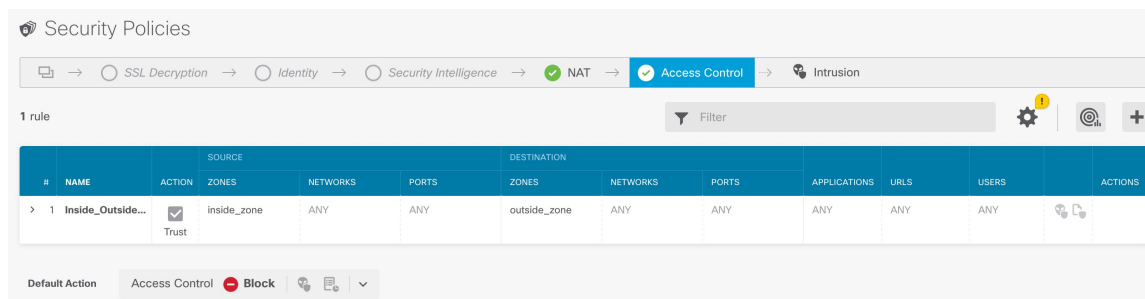
18: DHCP



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。

19:



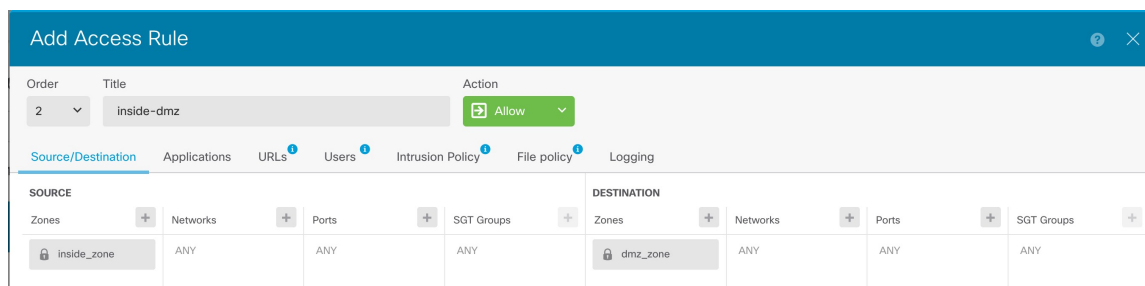
但是，如果在不同的区域都有接口，则需要访问控制规则来允许流量进出这些区域。

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。

20:



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。

6. 点击菜单中的**部署**按钮，然后点击**立即部署**按钮（即 ），将更改部署到设备。
只有将更改部署至设备，更改才会生效。



© 2023-2025 Cisco Systems, Inc. All rights reserved.

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。