# 准备工作

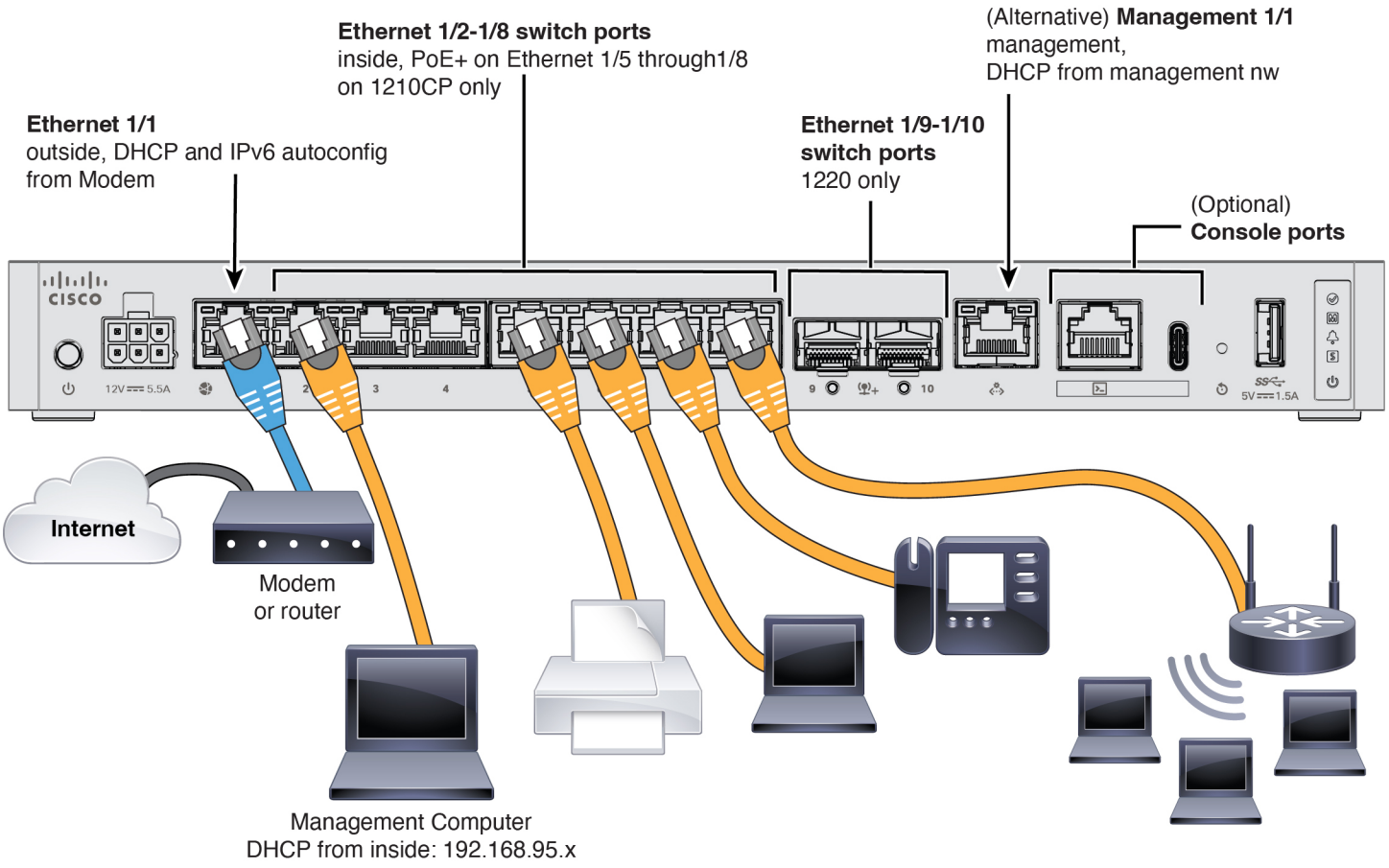
Cisco Secure Firewall 1200 为分布式企业提供连接和安全防护。它将思科企业安全策略和威胁检测扩展至分支机构和小型站点的用户及设备。借助高效网络处理器，Cisco Secure Firewall 1200 在不影响用户体验的前提下，提供高级别的安全策略和威胁防御。

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



# 为防火墙布线

- 对于 Cisco Secure Firewall 1220，请将 SFP 安装到以太网 1/9 和 1/10 - 这些是需要 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，Firewall Threat Defense 初始化大约需要 15 到 30 分钟。

### 开始之前

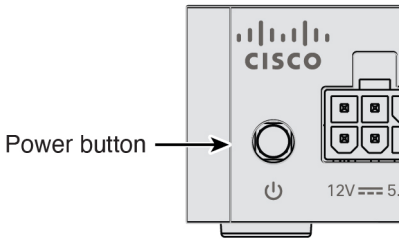
为防火墙提供可靠的电源（例如，使用不间断电源 (UPS)）非常重要。未事先关闭就断电可能会导致严重的文件系统损坏。后台始终有许多进程在运行，因此断电会使得系统无法正常关闭。

### 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。

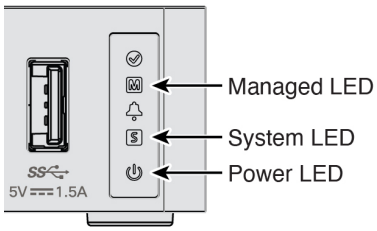
**步骤 2** 使用位于机箱背面电源线旁边的电源按钮打开电源。

**图 *1:* 电源按钮**




**步骤 3** 检查 LED 的当前状态。

**图 *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：

**表 *1:* 系统 *(S) LED* 行为**

| LED 行为 | 说明 | 设备通电后的时间 （分钟：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 |

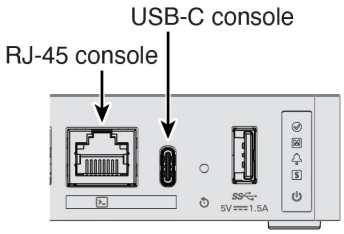
# 安装的是哪个应用程序： Firewall Threat Defense 还是 ASA？

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。

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，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。

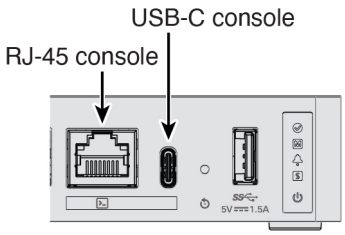
# 访问Firewall Threat Defense CLI

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 Firewall Threat Defense CLI。

**注释**
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。

**示例：**

```
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。

**示例：**

```
> exit
firepower#
```

# 检查版本并重新映像

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。

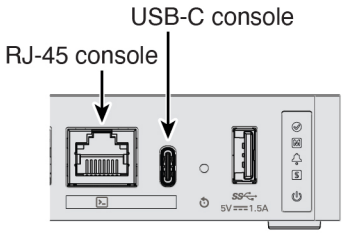
**我应运行哪个版本？**

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。

## 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**

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 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。

**过程**

**步骤 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？ ，第 3 页。

**步骤 2** 连接到 Firewall Threat Defense 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 防火墙设备管理器。

**步骤 4** 在新的管理 IP 地址上登录防火墙设备管理器 。

# 获取许可证

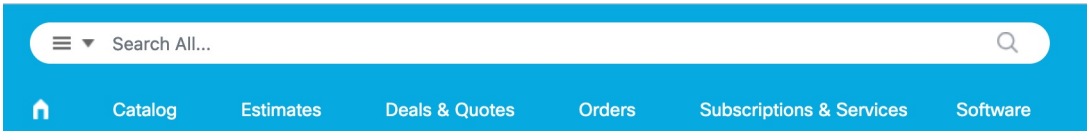
当您从思科或经销商那里购买设备时，您的许可证应该已链接到您的智能软件许可证帐户。如果您没有智能软件管理器账户，请点击链接建立新账户。

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。

图 *6:* 许可证搜索




2. 搜索以下许可证 PID。

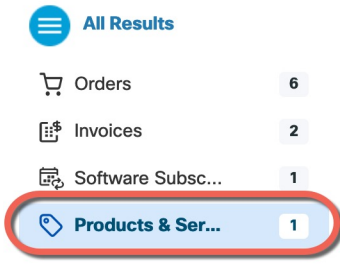
注释 如果未找到 PID，您可以手动将 PID 添加到订单中。

- 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 Client — 请参阅 Cisco Secure Client 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。

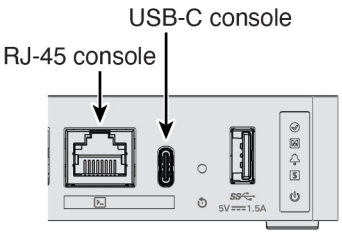
## 在 CLI 上关闭防火墙电源

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。

# 使用防火墙设备管理器关闭防火墙电源

使用防火墙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。

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。