



准备工作

中端 Cisco Secure Firewall 3100 系列支持您不断发展的业务需求。它使混合工作和零信任变得可行，并具有确保高投资回报的灵活性。Cisco Secure Firewall 3100 是一款以威胁为核心的安全设备，具备业务弹性和卓越威胁防御能力。它在多种防火墙使用场景中均表现出色，即使启用高级威胁功能也不例外。现代 CPU 架构与可优化防火墙、加密和威胁检测功能的专用硬件相结合，可实现这些性能功能。Cisco Secure Firewall 3100 适用于从互联网边缘到数据中心和私有云的各类场景。Cisco Secure Firewall 3100 支持多实例和集群功能，可提升性能并随组织发展扩展以满足需求。

使用专用管理网络上的 Secure Firewall Management Center 来管理防火墙。

- [打开防火墙电源，第 1 页](#)
- [安装的是哪个应用程序：Firewall Threat Defense 还是 ASA？，第 3 页](#)
- [访问 Firewall Threat Defense CLI，第 3 页](#)
- [检查版本并重新映像，第 5 页](#)
- [获取许可证，第 6 页](#)
- [（必要时）关闭防火墙电源，第 8 页](#)

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。摇杆电源开关提供软通知，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

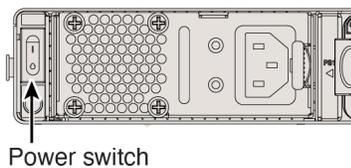
为防火墙提供可靠的电源（例如，使用不间断电源 (UPS)）非常重要。未事先关闭就断电可能会导致严重的文件系统损坏。后台始终有许多进程在运行，因此断电会使得系统无法正常关闭。

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。

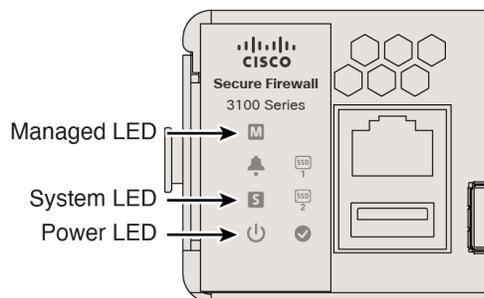
步骤 2 使用位于机箱背面电源线旁边的摇杆电源开关打开电源。

图 1: 电源开关



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

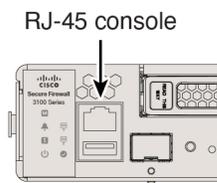
安装的是哪个应用程序：**Firewall Threat Defense** 还是 **ASA**？

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 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 3 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](#)。

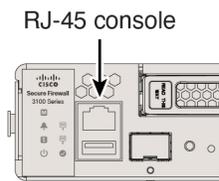
访问**Firewall Threat Defense CLI**

您可能需要访问 CLI 进行配置或故障排除。

过程

步骤 1 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。

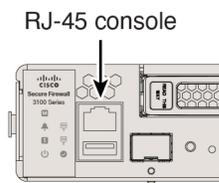
我应运行哪个版本？

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 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。

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](#)帐户，请点击链接[建立新帐户](#)。

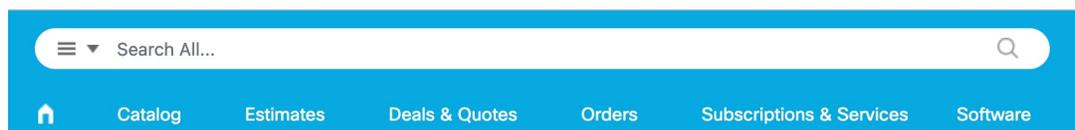
如果尚未注册，请向智能软件管理器注册 Firewall Management Center。注册需要您在智能软件管理器中生成注册令牌。有关详细说明，请参阅[Cisco Secure Firewall Management Center 管理指南](#)。

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
- 运营商 - Diameter、GTP/GPRS、M3UA、SCTP

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-FPR3110T-TMC =
 - L-FPR3120T-TMC =

- L-FPR3130T-TMC =
- L-FPR3140T-TMC =

当您上述 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-FPR3110T-TMC-1Y
 - L-FPR3110T-TMC-3Y
 - L-FPR3110T-TMC-5Y
 - L-FPR3120T-TMC-1Y
 - L-FPR3120T-TMC-3Y
 - L-FPR3120T-TMC-5Y
 - L-FPR3130T-TMC-1Y
 - L-FPR3130T-TMC-3Y
 - L-FPR3130T-TMC-5Y
 - L-FPR3140T-TMC-1Y
 - L-FPR3140T-TMC-3Y
 - L-FPR3140T-TMC-5Y
- 运营商：
 - L-FPR3K-FTD-CAR=
 - 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。

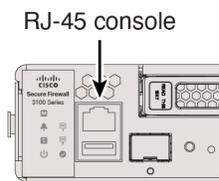
在 CLI 上关闭防火墙电源

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 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。

使用防火墙管理中心关闭防火墙电源

使用 Firewall Management Center 正确关闭系统。

过程

步骤 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。

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。