



使用设备管理器部署威胁防御

本章对您适用吗？

要查看所有可用的操作系统和管理器，请参阅[哪种操作系统和管理器适合您？](#)。本章适用于威胁防御和设备管理器。

本章介绍如何使用基于 Web 的设备安装向导，完成威胁防御的初始设置和配置。

设备管理器可以配置小型网络最常用软件的基本功能。此产品专为包括一台或几台设备的网络而设计，在这种网络中，无需使用高功率多设备管理器来控制包含许多设备管理器设备的大型网络。

关于防火墙

硬件可以运行威胁防御软件或 ASA 软件。在威胁防御和 ASA 之间切换需要您对设备进行重新映像。如果您需要不同于当前安装的软件版本，则还应重新映像。请参阅[重新映像思科 ASA 或 Firepower 威胁防御设备](#)。

防火墙会运行被称为 Secure Firewall eXtensible 操作系统 (FXOS) 的底层操作系统。防火墙不支持 FXOS Cisco Secure Firewall 机箱管理器；出于故障排除目的，仅支持受限的 CLI。有关详细信息，请参阅[适用于具备 Firepower 威胁防御的 Firepower 1000/2100 和 Cisco Secure Firewall 3100 的思科 FXOS 故障排除指南](#)。

隐私收集声明-防火墙不要求或主动收集个人身份信息。但是，您可以在配置中使用个人身份信息，例如用户名。在这种情况下，管理员在执行配置或使用 SNMP 时可能会看到此信息。

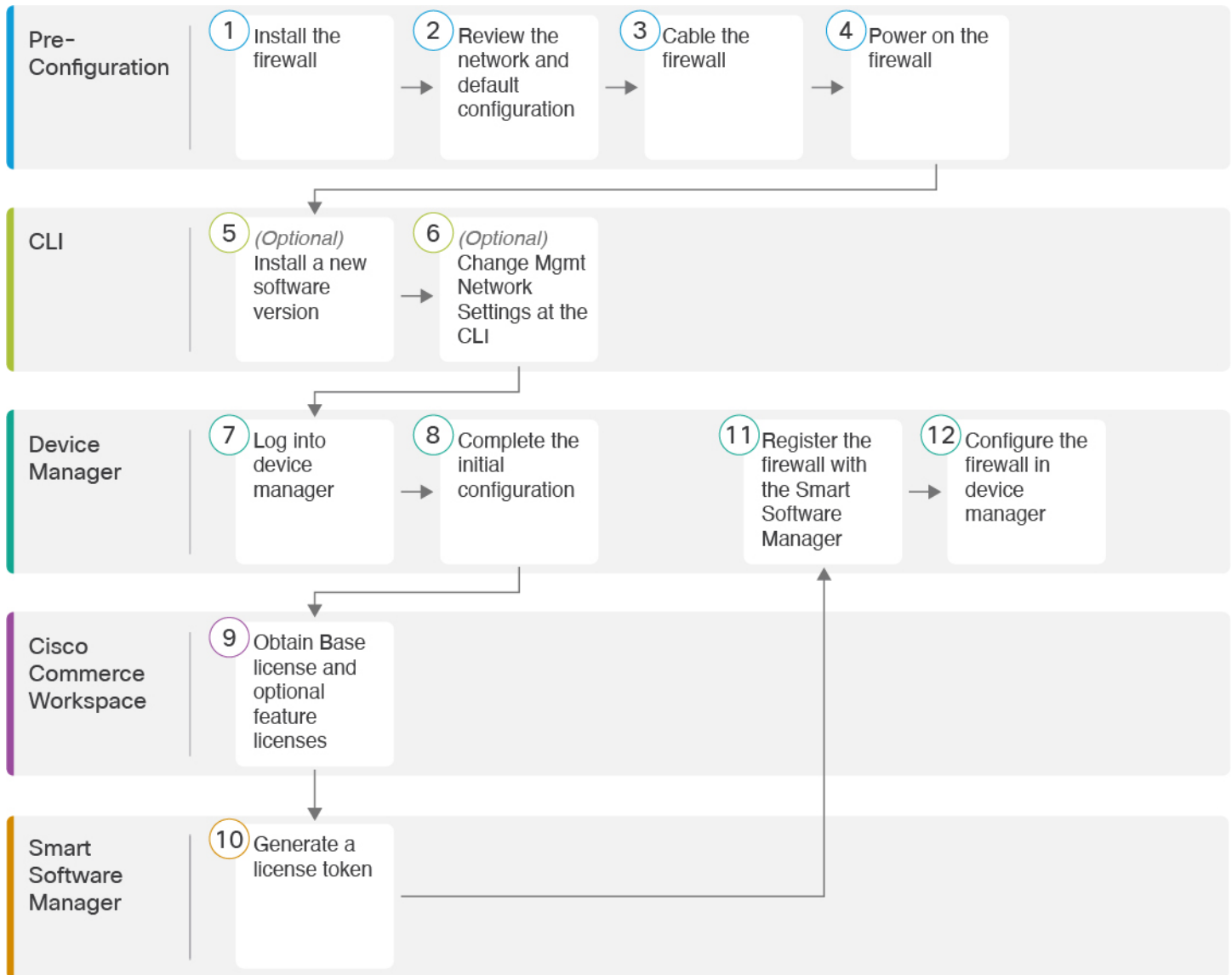
- [端到端程序，第 2 页](#)
- [查看网络部署和默认配置，第 3 页](#)
- [连接防火墙的电缆，第 5 页](#)
- [打开防火墙电源，第 6 页](#)
- [（可选）检查软件并安装新版本，第 7 页](#)
- [（可选）在 CLI 中更改管理网络设置，第 8 页](#)
- [登录设备管理器，第 10 页](#)
- [完成初始配置，第 11 页](#)
- [配置许可，第 12 页](#)
- [在设备管理器中配置防火墙，第 19 页](#)
- [访问威胁防御和 FXOS CLI，第 22 页](#)
- [关闭防火墙电源，第 24 页](#)

• 后续步骤，第 25 页

端到端程序

请参阅以下任务以在机箱上部署威胁防御和设备管理器。

图 1: 端到端程序



1	配置前准备工作	安装防火墙。请参阅 硬件安装指南 。
2	配置前准备工作	查看网络部署和默认配置 ，第 3 页。

3	配置前准备工作	连接防火墙的电缆，第 5 页。
4	配置前准备工作	打开防火墙电源，第 6 页。
5	CLI	(可选) 检查软件并安装新版本，第 7 页。
6	CLI	(可选) 在 CLI 中更改管理网络设置，第 8 页。
7	设备管理器	登录设备管理器，第 10 页。
8	设备管理器	完成初始配置，第 11 页。
9	Cisco Commerce Workspace	获取基本许可证和可选功能许可证 (配置许可，第 12 页)。
10	智能软件管理器	生成许可证令牌 (配置许可，第 12 页)。
11	设备管理器	向智能许可证服务器 (配置许可，第 12 页) 注册防火墙。
12	设备管理器	在设备管理器中配置防火墙，第 19 页。

查看网络部署和默认配置

您可以从管理 1/1 接口或内部接口使用设备管理器管理威胁防御。专用管理接口是一种具有自己的网络设置的特殊接口。

下图显示了推荐用于网络部署。如果您将外部接口直接连接到电缆调制解调器或 DSL 调制解调器，我们建议您将调制解调器置于桥接模式，以便威胁防御为您的内部网络执行所有路由和 NAT。如果您需要为外部接口配置 PPPoE 以连接到您的 ISP，可以在设备管理器中完成初始设置后执行此操作。



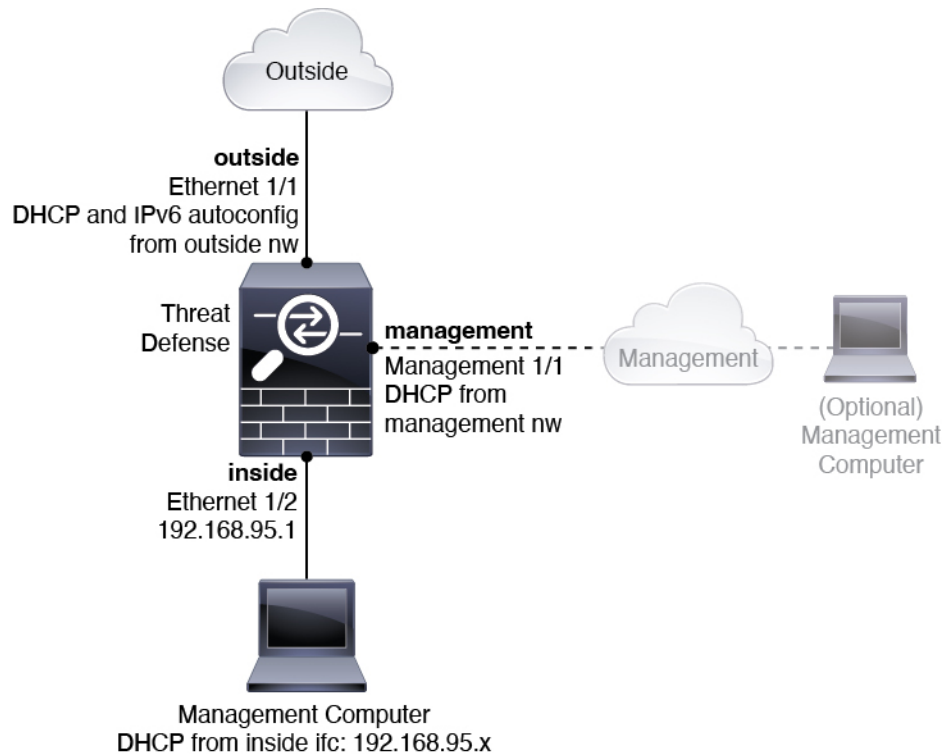
注释 如果您无法使用默认管理 IP 地址（例如，您的管理网络不包括 DHCP 服务器），可以连接到控制台端口并在 CLI 中执行初始设置，包括设置管理 IP 地址、网关和其他基本网络设置。

如果您需要更改内部 IP 地址，可以在设备管理器中完成初始设置后执行此操作。例如，在以下情况下，您可能需要更改内部 IP 地址：

- 内部 IP 地址为 192.168.95.1。
- 如果将威胁防御添加到现有内部网络中，需要将内部 IP 地址更改到现有网络上。

下图显示了在使用默认配置的设备管理器的威胁防御默认网络部署。

图 2: 建议的网络部署



默认配置

在初始设置后，防火墙配置包括以下内容：

- 内部 - 以太网 1/2、IP 地址 192.168.95.1。
- 外部 - 以太网 1/1，IP 地址来自 IPv4 DHCP 和 IPv6 自动配置
- 内部→外部流量
- 管理 - 管理 1/1（管理），IP 地址来自 DHCP



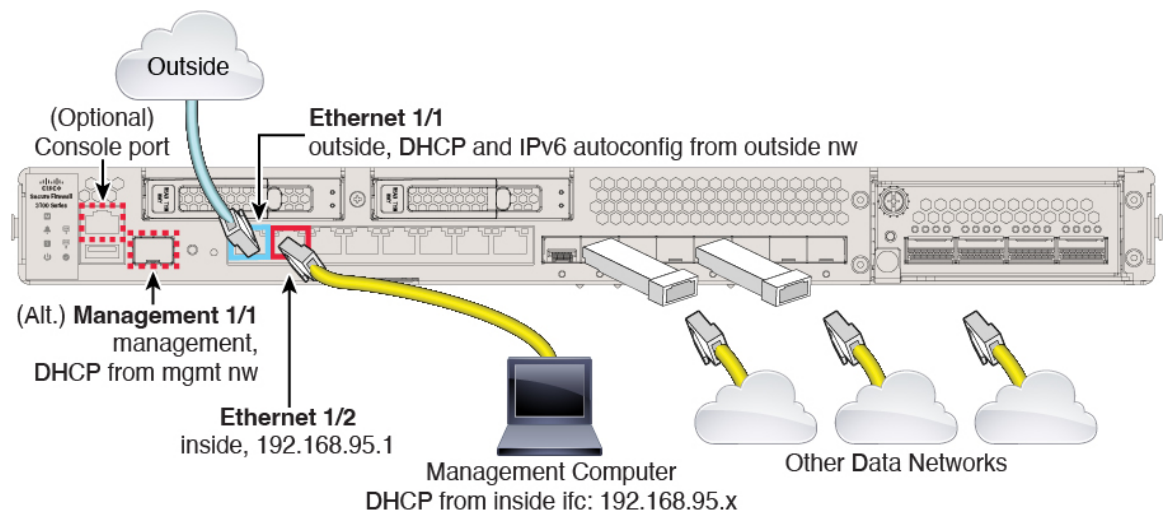
注释 管理 1/1 接口是不同于数据接口的特殊接口，用于管理、智能许可和数据库更新。物理接口与第二个逻辑接口（诊断接口）共享。诊断是一种数据接口，但仅限于其他类型的管理流量（发往设备和发自设备），例如 syslog 或 SNMP。通常不使用诊断接口。有关详细信息，请参阅《[Cisco Secure Firewall 设备管理器配置指南](#)》。

- 管理型 DNS 服务器 - OpenDNS: (IPv4) 208.67.222.222、208.67.220.220; (IPv6) 2620:119:35::35 或在设置过程中指定的服务器。系统从不使用从 DHCP 获取的 DNS 服务器。

- **NTP** - 思科 NTP 服务器: 0.sourcefire.pool.ntp.org、1.sourcefire.pool.ntp.org、2.sourcefire.pool.ntp.org 或您在设置过程中指定的服务器
- **默认路由**
 - **数据接口** - 从外部 DHCP 获取, 或在设置过程中指定的网关 IP 地址
 - **管理接口** - 从管理 DHCP 获取。如果没有收到网关, 则默认路由在背板上并通过数据接口。
请注意, 管理接口需要互联网访问, 以在背板上或使用单独的互联网网关获取许可和进行更新。请注意, 只有源自管理接口的流量才能通过背板; 否则, 管理接口不允许从网络进入管理接口的直通流量。
- **DHCP 服务器** - 在内部接口上启用
- **设备管理器 访问** - 管理和内部接口上允许的所有主机。
- **NAT** - 接口 PAT 用于所有从内部到外部的流量

连接防火墙的电缆

图 3: *Secure Firewall 3100* 布线



在管理 1/1 或以太网 1/2 上管理 Secure Firewall 3100。默认配置还会将以太网 1/1 配置为外部接口。

过程

步骤 1 安装机箱。请参阅[硬件安装指南](#)。

步骤 2 将您的管理计算机连接至以下任一接口:

- **以太网 1/2** - 将您的管理计算机直接连接至以太网 1/2 以进行初始配置, 或将以太网 1/2 连接至内部网络。以太网 1/2 具有默认 IP 地址 (192.168.95.1), 并且还会运行 DHCP 服务器以向客户端

(包括管理计算机) 提供 IP 地址, 因此, 请确保这些设置不会与任何现有内部网络设置冲突 (请参阅[默认配置](#), 第 4 页)。

- 管理 1/1 - 将管理 1/1 接口连接到管理网络, 并确保管理计算机位于管理网络上, 或者可以访问管理网络。管理 1/1 接口从管理网络上的 DHCP 服务器获取 IP 地址; 如果使用此接口, 则必须确定分配给防火墙的 IP 地址, 以便可以从管理计算机连接到 IP 地址。

如果需要将管理 1/1 IP 地址从默认值更改为配置静态 IP 地址, 还必须将管理计算机连接到控制台端口。请参阅 [\(可选\) 在 CLI 中更改管理网络设置](#), 第 8 页。

注释 管理 1/1 是需要 SFP 模块的 10 Gb 光纤接口。

可以稍后从其他接口配置设备管理器管理访问; 请参阅 [FDM 配置指南](#)。

步骤 3 将外部网络连接到以太网 1/1 接口。

默认情况下, 使用 IPv4 DHCP 和 IPv6 自动配置获取 IP 地址, 但可以在初始配置期间设置静态地址。

步骤 4 将其他网络连接到其余接口。

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。电源开关以软通知开关形式实施, 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 首次启动威胁防御时, 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。

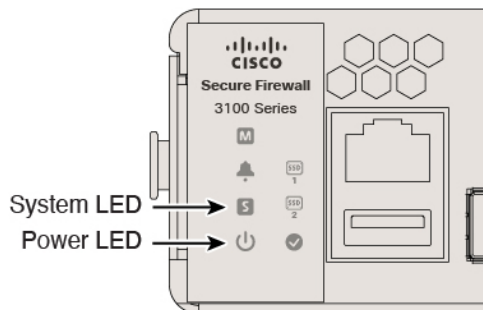
过程

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标准摇杆型电源开关打开电源。

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 4: 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。

注释 将开关从开切换到关时，系统可能需要几秒钟才会最终关闭。在此期间，机箱前面的电源 LED 将闪烁绿色。在电源 LED 完全关闭之前，请勿拔出电源。

(可选) 检查软件并安装新版本

要检查软件版本并在必要时安装不同的版本，请执行以下步骤。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> 中所述的发布策略；例如，此公告描述短期版本编号（包含最新功能）、长期版本编号（较长时间的维护版本和补丁）或额外长期版本编号（最长期限的维护版本和补丁，用于政府认证）。

过程

步骤 1 连接到控制台端口。有关详细信息，请参阅[访问威胁防御和 FXOS CLI](#)，第 22 页。

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

您连接到 FXOS CLI。第一次输入登录时，系统会提示您更改密码。此密码也用于 SSH 的威胁防御登录。

注释 如果密码已更改，但您不知道，则必须执行出厂重置以将密码重置为默认值。有关 [出厂重置程序](#) 的信息，请参阅 [FXOS 故障排除指南](#)。

示例：

```
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 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                  7.2.0.65              7.2.0.65
                        Not Applicable

```

步骤 3 如果要安装新版本，请执行这些步骤。

- a) 如果要为管理接口设置静态 IP 地址，请参阅 [\(可选\) 在 CLI 中更改管理网络设置，第 8 页](#)。
默认情况下，管理接口将使用 DHCP。
您需要从可通过管理接口访问的服务器下载新的映像。
- b) 执行 [《FXOS 故障排除指南》](#) 中的 [重新映像程序](#)。

(可选) 在 CLI 中更改管理网络设置

如果您无法使用默认管理 IP 地址，可以连接到控制台端口并在 CLI 中执行初始设置，包括设置管理 IP 地址、网关和其他基本网络设置。您只能配置管理接口设置；而无法配置内部或外部接口，稍后可在 GUI 中配置它们。



注释 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](#)。

过程

步骤 1 连接到 威胁防御 控制台端口。有关详细信息，请参阅[访问威胁防御和 FXOS CLI](#)，第 22 页。

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

您连接到 FXOS CLI。第一次输入登录时，系统会提示您更改密码。此密码也用于 SSH 的威胁防御登录。

注释 如果密码已更改，但您不知道，则必须执行出厂重置以将密码重置为默认值。有关 [出厂重置程序](#) 的信息，请参阅 [FXOS 故障排除指南](#)。

示例:

```
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 2 连接到 威胁防御 CLI。

connect ftd

示例:

```
firepower# connect ftd
>
```

步骤 3 首次登录威胁防御时，系统会提示您接受“最终用户许可协议”(EULA)并。然后，系统将显示 CLI 设置脚本。

默认值或以前输入的值会显示在括号中。要接受之前输入的值，请按 **Enter** 键。

请参阅以下准则：

- **输入管理接口的 IPv4 默认网关** - 如果您设置手动 IP 地址，则可以输入网关路由器的数据接口或 IP 地址。**data-interfaces** 设置将通过背板发送出站管理流量，以退出数据接口。如果您没有可以访问互联网的单独管理网络，则此设置非常有用。源自管理接口的流量包括需要访问互联网的许可证注册和数据库更新。如果您使用 **data-interfaces**，在直接连接到管理网络的情况下，您仍可以在管理接口上使用设备管理器（或 SSH）但是，要对特定网络或主机进行远程管理，则应该使用 **configure network static-routes** 命令添加静态路由。请注意，数据接口上的设备管理器管理不受此设置的影响。如果使用 DHCP，则系统使用 DHCP 提供的网关，如果 DHCP 不提供网关，则使用数据接口作为回退方法。

- 如果网络信息已更改则需要重新连接 - 如果您已通过 SSH 连接到默认 IP 地址，但在初始设置时更改了 IP 地址，则会断开连接。使用新 IP 地址和密码重新进行连接。控制台连接不会受影响。
- 在本地管理设备？ - 输入是 (yes) 以使用设备管理器。回答否 (no) 表示您打算使用本地部署或云端交付管理中心来管理设备。

示例:

```

You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

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.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
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
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

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

>

```

步骤 4 在新的管理 IP 地址上登录设备管理器。

登录设备管理器

登录设备管理器以配置威胁防御。

开始之前

- 使用 Firefox、Chrome、Safari、Edge 或 Internet Explorer 的当前版本。

过程

步骤 1 在浏览器中输入以下 URL。

- 内部（以太网 1/2）—<https://192.168.95.1>。

- 管理 - https://management_ip。管理接口是 DHCP 客户端，因此 IP 地址取决于您的 DHCP 服务器。如果在 CLI 设置中更改了管理 IP 地址，则输入该地址。

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

下一步做什么

- 通过 设备管理器 安装向导运行；请参阅[完成初始配置](#)，第 11 页。

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。完成安装向导后，您的设备应该会正常工作并部署了下列基本策略：

- 外部（Ethernet1/1）和内部接口（Ethernet1/2）。
- 内部和外部接口的安全区域。
- 信任所有内部到外部流量的访问规则。
- 接口 NAT 规则，用于将所有内部到外部流量转换到外部接口 IP 地址上的唯一端口。
- 在内部接口上运行的 DHCP 服务器。



注释 如果您执行了 [端到端程序](#)，第 2 页 程序，则这些任务中应该有一部分已经完成，特别是更改 admin 密码以及配置外部和管理接口。

过程

步骤 1 系统会提示您阅读和接受“最终用户许可协议”并更改管理员密码。

只有完成这些步骤，才能继续。

步骤 2 为外部接口和管理接口配置以下选项，然后点击下一步 (Next)。

注释 点击下一步后，您的设置将部署到设备中。该接口将命名为“outside”，并添加到“outside_zone”安全区。请确保您的设置准确无误。

- a) **外部接口** - 即连接到网关路由器的数据端口。在初始设备设置期间，您不能选择其他外部接口。第一个数据接口是默认的外部接口。

配置 IPv4 - 外部接口的 IPv4 地址。可以使用 DHCP，也可以手动输入静态 IP 地址、子网掩码和网关。另外，也可以选择关，不配置 IPv4 地址。您无法使用安装向导配置 PPPoE。如果接口连

接到 DSL、电缆调制解调器或 ISP 的其他连接，并且 ISP 使用 PPPoE 来提供 IP 地址，则可能需要使用 PPPoE。您可以在完成向导后配置 PPPoE。

配置 Ipv6 - 外部接口的 Ipv6 地址可以使用 DHCP，也可以手动输入静态 IP 地址、前缀和网关。另外，也可以选择关，不配置 IPv6 地址。

b) 管理接口

DNS 服务器 - 系统管理地址的 DNS 服务器。输入 DNS 服务器的一个或多个地址以解析名称。默认值为 OpenDNS 公共 DNS 服务器。如果您编辑字段并想要恢复默认值，请点击 **使用 OpenDNS (Use OpenDNS)** 以重新将合适的 IP 地址载入字段。

防火墙主机名 - 系统管理地址的主机名。

步骤 3 配置系统时间设置，然后点击下一步。

- a) 时区 - 选择系统时区。
- b) **NTP 时间服务器** - 选择使用默认 NTP 服务器，还是手动输入 NTP 服务器的地址。可以添加多个服务器来提供备份。

步骤 4 (可选) 为系统配置智能许可证。

购买威胁防御设备会自动附带基本许可证。其他所有许可证均是可选的。

只有具有智能许可证帐户，才能获取和应用系统需要的许可证。最初，可以使用为期 90 天的评估许可证，以后再设置智能许可。

要立即注册设备，请点击链接登录智能软件管理器帐户，并参阅 [配置许可](#)，第 12 页。

要使用评估许可证，请选择启动 **90 日评估期而不注册 (Start 90 day evaluation period without registration)**。

步骤 5 点击完成。

下一步做什么

- 尽管您可以继续使用评估许可证，但我们建议您注册并许可您的设备；请参阅 [配置许可](#)，第 12 页。
- 您也可以选择使用设备管理器配置设备；请参阅 [在设备管理器中配置防火墙](#)，第 19 页。

配置许可

威胁防御使用智能软件许可，这使得您可以集中购买和管理许可证池。

注册机箱时，智能软件管理器会为机箱和智能软件管理器之间的通信颁发 ID 证书。它还会将机箱分配到相应的虚拟帐户。

有关思科许可的更详细概述，请访问 cisco.com/go/licensingguide

智能许可不会阻止您使用尚未购买的产品功能。只要您向智能软件管理器进行了注册，即可立即开始使用许可证，并在以后购买该许可证。这使您能够部署和使用功能，并避免由于采购订单审批造成延迟。请参阅以下许可证：

- **基础版**-（必需）基础版 许可证。
- **IPS** - 安全情报和下一代 IPS
- **恶意软件 防御**-恶意软件 防御
- **URL** - URL 过滤
- **Cisco Secure 客户端**-Secure Client Advantage、Secure Client Premier 或 Secure Client VPN Only

开始之前

- 拥有 [智能软件管理器](#) 主帐户。

如果您还没有账户，请点击此链接以 [设置新账户](#)。通过智能软件管理器，您可以为组织创建一个主帐户。

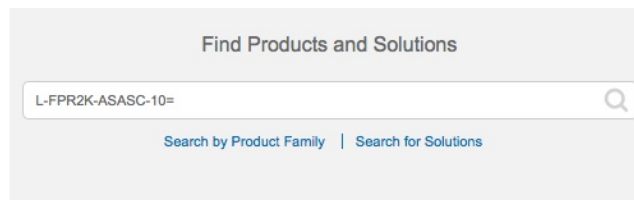
- 您的智能软件许可帐户必须符合强加密 (3DES/AES) 许可证的要求，才能使用某些功能（已使用导出合规性标志启用）。

过程

步骤 1 请确保智能许可帐户包含所需的可用许可证。

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。但是，如果您需要自己添加许可证，则请使用 [Cisco Commerce Workspace](#) 上的 **Find Products and Solutions** 搜索字段。搜索以下许可证 PID：

图 5: 许可证搜索



注释 如果未找到 PID，您可以手动将 PID 添加到订单中。

- 基础版 许可证：
 - L-FPR3110-BSE=
 - L-FPR3120-BSE=
 - L-FPR3130-BSE=
 - L-FPR3140-BSE=

- IPS、恶意软件防御和 URL 许可证组合：

- L-FPR3110T-TMC =
- L-FPR3120T-TMC =
- L-FPR3130T-TMC =
- L-FPR3140T-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-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

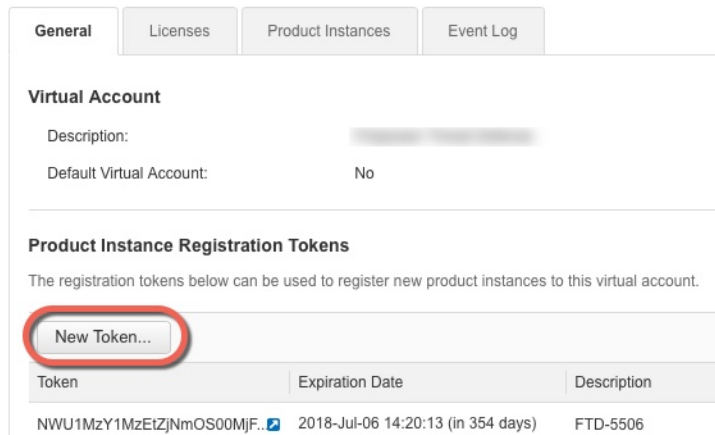
- Cisco Secure 客户端-请参阅 [思科安全客户端订购指南](#)。

步骤 2 在 [智能软件管理器](#) 中，为要将此设备添加到的虚拟帐户请求并复制注册令牌。

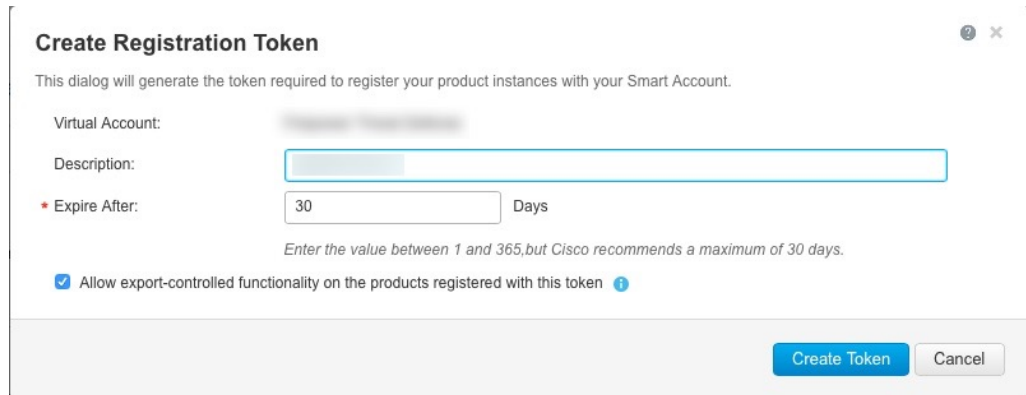
- a) 点击 **Inventory**。



- b) 在常规 (**General**) 选项卡上，点击**新令牌 (New Token)**。



c) 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。

- 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资产中。

d) 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 6: 查看令牌

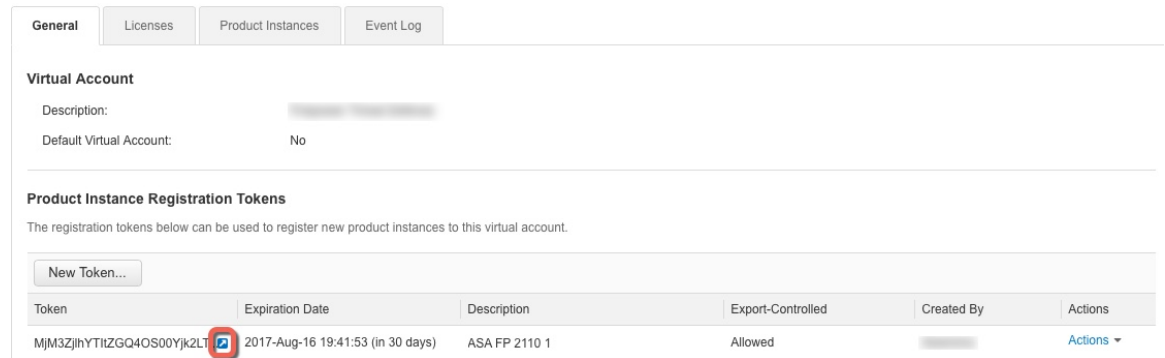
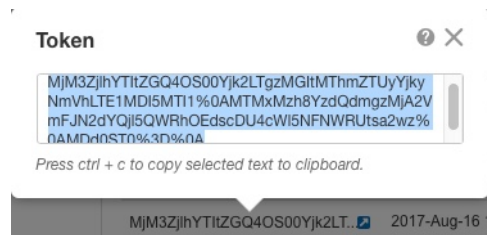


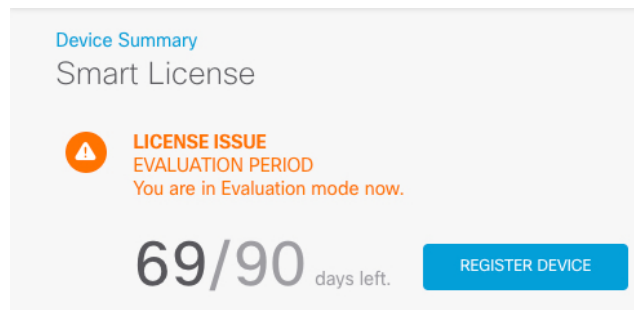
图 7: 复制令牌



步骤 3 在设备管理器中，点击 **设备**，然后在 **智能许可证** 摘要中，点击 **查看配置**。

您会看到智能许可证页面。

步骤 4 点击 **Register Device**。



然后，按照智能许可证注册对话框中的说明粘贴令牌：

Smart License Registration
✕

- 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:

MGY2NzMwOGitODJiZi00NzFiLWJiNiltYWMwNzU0ODY2ZGVlTE1NlUz
 Nzlv%0AODg5Mzh8SUQ5Vm5XbzZiSmN5M3I6K3owZ3ovVmpmc3Vtal
 JLQ2FFeGhFWmlW%0AWC9WTT0%3D%0A
- 4 Select Region

↓

When you register the device, you are also registered with Cisco Security Services Exchange (SSE). Please select the region in which your device is operating. You will be able to see your device in the device list of the regional SSE portal.

Region

SSE US Region
▼
i
- 5 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](#) ▼

Enable Cisco Success Network

CANCEL
REGISTER DEVICE

步骤 5 点击 **Register Device**。

您会返回到**智能许可证**页面。在设备注册时，您会看到以下消息：

Registration request sent on 10 Jul 2019. Please wait. Normally, it takes about one minute to complete the registration. You can check the task status in [Task List](#). Refresh this page to see the updated status.

在设备成功注册并刷新页面后，您会看到以下内容：

Device Summary
Smart License

✓

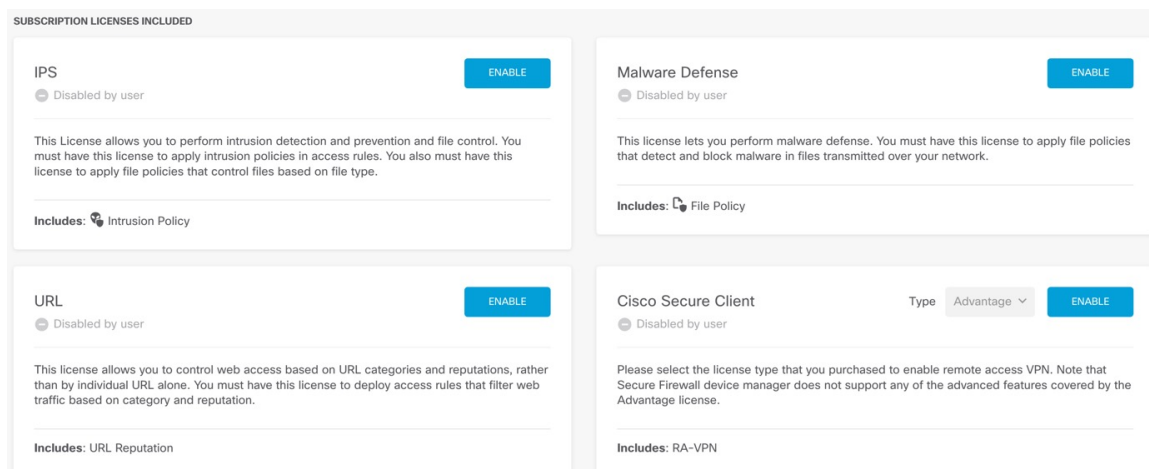
CONNECTED
SUFFICIENT LICENSE

Last sync: 10 Jul 2019 11:39 AM

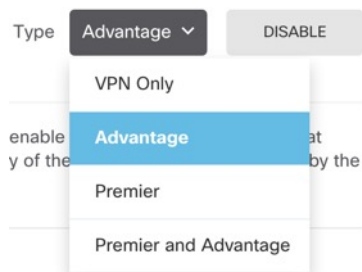
Next sync: 10 Jul 2019 11:49 AM

i

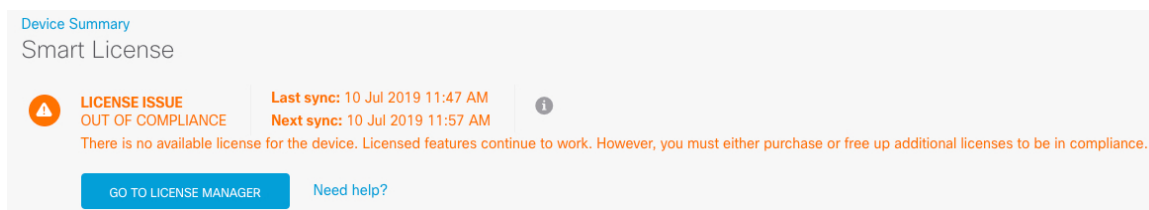
步骤 6 根据需要，点击每个可选许可证的启用/禁用控件。



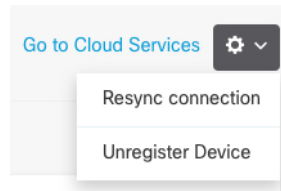
- **启用** - 将许可证注册到您的思科智能软件管理器帐户，并启用控制的功能。现在，您可以配置和部署该许可证控制的策略了。
- **禁用** - 取消许可证向思科智能软件管理器帐户的注册，并禁用控制的功能。新策略中无法配置这些功能，也不能再部署使用该功能的策略。
- 如果启用了 **Cisco Secure 客户端** 许可证，请选择要使用的许可证类型：**Advantage**、**Premier**、**VPN Only**或 **Premier** 和**Advantage**。



启用功能后，如果帐户中没有许可证，则在刷新页面后，您会看到以下不合规消息：



步骤 7 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。



在设备管理器中配置防火墙

以下步骤概述了可能需要配置的其他功能。请点击页面上的帮助按钮(?)，获取有关每个步骤的详细信息。

过程

步骤 1 要从 40-Gb 接口（部分型号上可用）创建 4 x 10-Gb 分支接口，请选择**设备 (Device)**，然后点击**接口 (Interfaces)** 摘要中的链接。然后点击接口的分支图标。

如果您已经在配置中使用了 40-Gb 接口，则必须在继续创建分支之前删除该配置。

步骤 2 如果连接了其他接口，请选择**设备**，然后点击**接口摘要**中的链接。

点击每个接口的编辑图标 (🔗)，以设置模式并定义 IP 地址和其他设置。

以下示例将一个接口配置为用作“隔离区”(DMZ)，可以将可公开访问的资产（例如 Web 服务器）放在该区域中。完成后点击**保存 (Save)**。

图 8: 编辑接口

A screenshot of the "Edit Physical Interface" configuration page. The page has a blue header with the title "Edit Physical Interface". Below the header, there are two input fields: "Interface Name" with the value "dmz" and "Status" with a toggle switch turned on. Below these is a "Description" field. At the bottom, there are three tabs: "IPv4 Address" (selected), "IPv6 Address", and "Advanced Options". Under the "IPv4 Address" tab, there is a "Type" dropdown menu set to "Static". Below that is an "IP Address and Subnet Mask" field with the value "192.168.6.1 / 24". At the very bottom, there is a small text example: "e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0".

步骤 3 如果已配置新接口，请选择对象 (Objects)，然后从目录中选择安全区域 (Security Zones)。

根据需要编辑或创建新区域。每个接口都必须属于一个区域，因为需要根据安全区域而不是接口来配置策略。配置接口时不能将其放在区域中，因此每当创建新接口或更改现有接口的用途之后，都必须编辑区域对象。

以下示例显示如何为 DMZ 接口创建一个新的 DMZ 区域。

图 9: 安全区域对象

步骤 4 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。

内部接口已配置了 DHCP 服务器，但可以编辑地址池或甚至将其删除。如果配置了其他内部接口，则在这些接口上设置 DHCP 服务器是非常典型的做法。点击 +，为每个内部接口配置服务器和地址池。

此外，您还可以在配置 (Configuration) 选项卡中对为客户端提供的 WINS 和 DNS 列表进行精细调整。以下示例显示如何在 inside2 接口（地址池为 192.168.4.50-192.168.4.240）上设置 DHCP 服务器。

图 10: DHCP 服务器

步骤 5 选择设备 (Device)，然后点击路由 (Routing) 组中的查看配置 (View Configuration)（或创建第一个静态路由 (Create First Static Route)），配置默认路由。

默认路由通常指向位于外部接口之外的上游或 ISP 路由器。默认的 IPv4 路由适用于 any-ipv4 (0.0.0.0/0)，而默认的 IPv6 路由适用于 any-ipv6 (:::0/0)。为所使用的每个 IP 版本创建路由。如果使用 DHCP 获取外部接口的地址，则可能已经拥有所需的默认路由。

注释 此页面上定义的路由仅适用于数据接口，而不会影响管理接口。在 **设备 > 系统设置 > 管理接口** 上设置管理网关。

以下示例显示 IPv4 的默认路由。在此示例中，isp-gateway 是用于标识 ISP 网关 IP 地址的网络对象（必须从 ISP 中获取地址）。可以通过点击 **网关 (Gateway)** 下拉菜单底部的 **创建新网络 (Create New Network)**，来创建该对象。

图 11: 默认路由



The screenshot shows the 'Add Static Route' configuration interface. It includes the following fields and options:

- Protocol:** Radio buttons for IPv4 (selected) and IPv6.
- Gateway:** A text input field containing 'isp-gateway'.
- Interface:** A text input field containing 'outside'.
- Metric:** A text input field containing '1'.
- Networks:** A section with a '+' button and a list containing 'any-ipv4'.

步骤 6 选择策略 (Policies)，并为网络配置安全策略。

设备安装向导设置允许内部区域与外部区域之间存在流量流动，并对所有接口上流向外部接口的流量启用网络地址转换 (NAT)。即使配置了新接口，如果将其添加到内部区域对象中，访问控制规则也将自动应用于这些接口。

但是，如果有多个内部接口，则需要一条访问控制规则来允许内部区域之间的流量。如要添加其他安全区域，则需要规则来允许这些区域之间的流量。这是您需要进行的最低限度的更改。

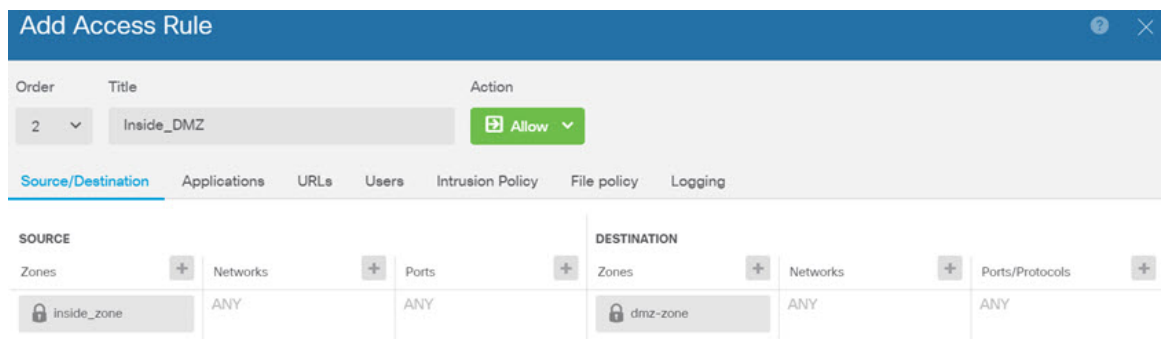
此外，您还可配置其他策略以提供附加服务，并对 NAT 和访问规则进行精细调整，以实现组织需要的结果。您可以配置以下策略：

- **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。

- **安全情报 (Security Intelligence)** - 使用安全情报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，可使安全情报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。


以下示例显示如何在访问控制策略中允许内部区域与 DMZ 区域之间的流量。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 12: 访问控制策略



步骤 7 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。如果使用安全情报源，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 8 点击菜单中的部署 (Deploy) 按钮，然后点击立即部署按钮 ()，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。

访问威胁防御和 FXOS CLI

使用命令行界面 (CLI) 可设置系统以及对系统进行基本的故障排除。无法通过 CLI 会话配置策略。可以连接到控制台端口以访问 CLI。

也可以访问FXOS CLI以进行故障排除。



注释 您也可以通过 SSH 连接到 威胁防御 设备的管理接口。与控制台会话不同，SSH 会话默认使用 威胁防御 CLI，由此可使用 **connect fxos** 命令连接到 FXOS CLI。如果您为 SSH 连接打开某个数据接口，稍后可以连接到该接口上的地址。默认情况下，禁用 SSH 数据接口访问。此程序介绍控制台端口的访问（默认使用 FXOS CLI）。

过程

步骤 1 要登录 CLI，请将管理计算机连接到控制台端口。Secure Firewall 3100 配有一条 DB-9 转 RJ-45 串行电缆，所以您需要第三方串行转 USB 电缆进行连接。确保为您的操作系统安装必要的 USB 串行驱动程序（请参阅 Secure Firewall 3100 [硬件指南](#)）。控制台端口默认为 FXOS CLI。使用以下串行设置：

- 9600 波特率
- 8 个数据位
- 无奇偶校验
- 1 个停止位

您连接到 FXOS CLI。使用 **admin** 用户名和初始设置时设置的密码（默认值为 **Admin123**）登录 CLI。

示例：

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

步骤 2 访问威胁防御 CLI。

connect ftd

示例：

```
firepower# connect ftd
>
```

登录后，如需了解 CLI 中可用命令的相关信息，请输入 **help** 或 **?**。有关使用信息，请参阅 [Cisco Secure Firewall Threat Defense 命令参考](#)。

步骤 3 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 CLI 提示。有关 FXOS CLI 中可用命令的相关信息，请输入 **?**。

示例：

```
> exit
firepower#
```

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。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防火墙系统。

您可以使用设备管理器关闭防火墙，也可以使用FXOS CLI。

使用设备管理器关闭防火墙电源

您可以使用 设备管理器 正确关闭系统。

过程

步骤 1 使用 设备管理器 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。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。

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。您可以通过连接到控制台端口来访问CLI；请参阅[访问威胁防御和 FXOS CLI](#)，第 22 页。

过程

步骤 1 在 FXOS CLI 中，连接到 local-mgmt:


```
firepower # connect local-mgmt
```

步骤 2 发出 **shutdown** 命令：

```
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 3 留意防火墙关闭时的系统提示。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 4 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。

后续步骤

要继续配置 威胁防御，请参阅适用于您的软件版本的文档：[导航思科 Firepower 文档](#)。

有关使用设备管理器的信息，请参阅《[适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南](#)》。

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。