适用于使用 Firepower 设备管理器的 Firepower 2100 系列的思科 Firepower 威胁防御快速入门指南

版本 6.2.1 （或更高版本）

首次发布日期：2017 年 4 月 24 日

本指南适用对象

本指南介绍使用 Firepower 威胁防御安全设备上附带的基于 Web 的 Firepower 设备管理器设备设置向导如何完成 Firepower 威胁防御安全设备的初始配置。

通过 Firepower 设备管理器，可以配置小型网络最常用软件的基本功能。此产品专门为包括一台或几台安全设备的网络而设计，在此类网络中，无需使用高功率的多设备管理器来控制包含许多 Firepower 威胁防御设备的大型网络。

如果要管理大量安全设备或要使用 Firepower 威胁防御支持的更复杂的功能和配置，请使用 Firepower 管理中心 （而不是集成的 Firepower 设备管理器）来配置安全设备。

使用 CLI 设置向导，可按照适用于使用 Firepower 管理中心的 Firepower 2100 系列的思科 Firepower 威胁防御快速入门指南中所述为 Firepower 威胁防御安全设备配置网络连接并将其注册到 Firepower 管理中心。

许可证要求

Firepower 威胁防御安全设备需要思科智能许可。通过智能许可，可以集中管理许可证池。与产品授权密钥 (PAK) 许可证不同的是，智能许可证未绑定到特定序列号或许可证密钥。通过智能许可，可以直观地评估许可证使用情况和需求。

此外，智能许可不会阻止您使用尚未购买的产品功能。只要注册到思科智能软件管理器，然后再购买一个许可证，立即就能使用该许可证。这样即可部署和使用某项功能，同时避免采购订单审批造成的延迟。

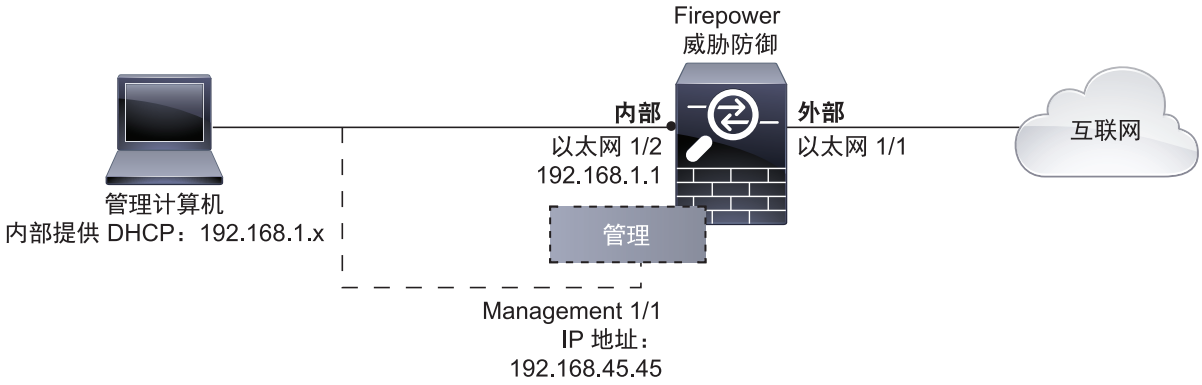
在为 Firepower 功能购买一个或多个智能许可证后，可在思科智能软件管理器中对其进行管理：http://www.cisco.com/web/ordering/smart-software-manager/index.html。通过智能软件管理器，您可以为组织创建一个主帐户。有关思科智能软件管理器的更多信息，请参阅*思科智能软件管理器用户指南*。

购买 Firepower 威胁防御安全设备或 Firepower 威胁防御虚拟会自动附带基本许可证。所有其他许可证 （威胁、恶意软件或 URL 过滤）均为可选。有关 Firepower 威胁防御许可的更多信息，请参阅*适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南*中的 “为系统授予许可”。

在网络中部署 Firepower 威胁防御

下图显示 Firepower 2100 系列中建议的 Firepower 威胁防御网络部署。

图 1 部署方案示例



该配置示例支持上述网络部署执行以下行为：

- 网络流量**从内部到外部**
- **外部 IP** 地址从 **DHCP** 获取
- **内部**客户端的 **DHCP** 内部接口上有 DHCP 服务器。您可以将管理计算机直接插入内部接口，并获取 192.168.1.0/24 网络中的地址。

  内部接口启用了 HTTPS 访问，因此可以通过默认地址 192.168.1.1 的内部接口打开 Firepower 设备管理器。

  注意：在初始配置期间仅启用了外部 （以太网 1/1）和内部 （以太网 1/2）接口。若要在配置后更改接口分配，请编辑接口和 DHCP 设置。

- 或者，可以连接到**管理 1/1** ，使用 Firepower 设备管理器来设置和管理安全设备。管理接口上有 DHCP 服务器。您可以将管理计算机直接插入此接口，并获取 192.168.45.0/24 网络中的地址。

  管理接口上启用了 HTTPS 访问，因此可以通过默认地址 192.168.45.45 的管理接口打开 Firepower 设备管理器。

  注意：管理逻辑接口与诊断逻辑接口之间共用物理管理接口；请参阅*适用于 Firepower 设备管理器的 Firepower 威胁防御配置指南*中的 “接口”。

- Firepower 威胁防御系统需要访问互联网才能获得许可和进行更新。管理 IP 地址的默认网关使用数据接口路由到互联网。因此，您不需要将管理物理接口连接到网络。

  但是，如果您希望使用单独的管理网络，则可以设置特定的网关。完成初始配置后，依次选择**设备 (Device) > 系统设置 (System Settings) > 管理接口 (Management Interface)**。

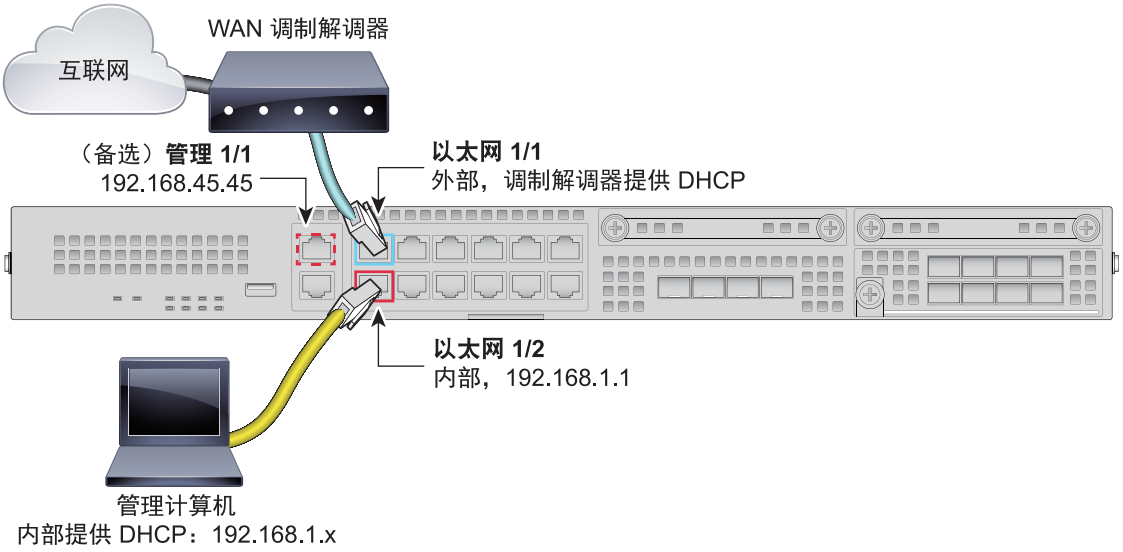
  注意：有关默认配置和初始设置选项的完整信息，请参阅*适用于 Firepower 设备管理器的 Firepower 威胁防御配置指南*中的 “使用入门”。

连接接口

默认配置假定某些接口用于内部和外部网络。如果基于上述预期将网线连接至接口，初始配置将变得更易于完成。要在 Firepower 2100 系列上按上述方案进行布线，请参阅下图。

注意：下图显示使用连接至内部网络的管理计算机的简单拓扑。也可以使用其他拓扑，而部署情况会因基本逻辑网络连接、端口、地址和配置要求有所不同。

图 2　默认配置的接口连接



程序

1. 将以太网 1/1 （外部）接口连接到 ISP/WAN 调制解调器或其他外部设备。默认情况下，使用 DHCP 获取 IP 地址，但可以在初始配置期间设置静态地址。
2. 将用于配置安全设备的本地管理工作站连接到内部接口：以太网 1/2。
3. 将工作站配置为使用 DHCP 获取 IP 地址。工作站将获得 192.168.1.0/24 网络中的地址。

   注意：可以使用其他选项来连接管理工作站。可以直接将其连接到管理端口。工作站将通过 DHCP 获得 192.168.45.0/24 网络中的地址。或者，可以将工作站连接到交换机，再将该交换机连接到 GigabitEthernet1/2。不过，必须确保该交换机的网络中没有其他设备运行 DHCP 服务器，否则就会与内部接口 192.168.1.1 上运行的 DHCP 服务器冲突。

启动 Firepower 2100 安全设备

系统电源由位于机箱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。

程序

1. 将电源线连接到 Firepower 2100 安全设备，并将其连接到电源插座。
2. 按下安全设备后部的电源开关。
3. 检查安全设备前面的 PWR LED；如果显示纯绿色，则安全设备已启动。
4. 检查安全设备前面的 SYS LED；在该指示灯显示纯绿色后，表示系统已通过启动诊断。

注意：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 PWR LED 将闪烁绿色。在 PWD LED 完全关闭之前，请勿拔出电源。

初始配置

您必须完成初始配置，才能使系统在网络中正常运行，其中包括配置将安全设备插入网络所需的地址，以及将设备连接到互联网或其他上游路由器。您可以通过以下两种方式之一来执行 Firepower 威胁防御应用的初始配置：

- 使用 Firepower 设备管理器 Web 界面 （推荐）。

  Firepower 设备管理器在网络浏览器中运行。使用该界面可配置、管理和监控系统。

- 使用命令行界面 (CLI) 设置向导 （可选）。

  可以使用 CLI 设置向导 （而不是 Firepower 设备管理器）进行初始配置，并可以使用 CLI 执行故障排除。也可以使用 Firepower 设备管理器来配置、管理和监控系统；请参阅 （可选）启动 Firepower 威胁防御 CLI 向导 （第 5 页）。

以下主题介绍如何使用这些界面来执行系统初始配置。

启动 Firepower 设备管理器

首次登录 Firepower 设备管理器时，设备设置向导会指引您完成初始系统配置。

准备工作

确保将数据接口连接到网关设备 （例如电缆调制解调器或路由器）。对于边缘部署，网关设备可能是面向互联网的网关。对于数据中心部署，可能是主干路由器。使用在网络中部署 Firepower 威胁防御 （第 2 页）中标识的默认 “外部” 接口。

然后，将管理计算机连接到默认 “内部” 接口。或者，可以连接到管理物理接口。

程序

1. 打开浏览器，并登录 Firepower 设备管理器。假定您未在 CLI 中进行初始配置，请在 **https://***ip-address* 中打开 Firepower 设备管理器，其中地址为以下项目之一：
   - 如果连接到内部接口，则地址为：**https://192.168.1.1**。
   - 如果连接到管理物理接口，则地址为：**https://192.168.45.45**。
2. 使用用户名 **admin** 和密码 **Admin123** 登录。
3. 如果这是您首次登录系统且未使用 CLI 设置向导，系统会提示您阅读并接受 “最终用户许可协议” 以及更改管理员密码。只有完成这些步骤，才能继续。

   注意：如果要手动配置安全设备，可以选择跳过设备设置向导。
4. 为外部接口和管理接口配置以下选项，然后点击**下一步 (Next)**。

   注意：点击**下一步 (Next)** 后，您的设置即会部署到安全设备中。该接口将命名为 “outside”，并添加到 “outside_zone” 安全区。确保您的设置正确。

   a. **外部接口 (Outside Interface)** - 即连接到网关调制解调器或路由器的数据端口。在初始设备设置期间无法选择备选外部接口。第一个数据接口是默认的外部接口。

      配置 Ipv4 (Configure 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。

      配置 Ipv6 (Configure 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. **管理界面**

      DNS 服务器 (DNS Servers) - 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** 以重新将合适的 IP 地址加载到字段。

      防火墙主机名 (Firewall Hostname) - 系统管理地址的主机名。

注意：使用设备设置向导配置 Firepower 威胁防御安全设备时，系统会为出站和入站流量提供两个默认访问规则。完成初始设置后，可以编辑这些访问规则。

5. 配置系统时间设置，然后点击**下一步 (Next)**。
   a. **时区 (Time Zone)** - 为系统选择时区。
   b. **NTP 时间服务器 (NTP Time Server)** - 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。
6. 为系统配置智能许可证。

   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。

   要立即注册安全设备，请点击链接以登录您的智能软件管理器帐户，生成新的令牌并将该令牌复制到编辑框中。

   要使用评估许可证，请点击**开始 90 天试用期，暂不注册 (Start 90 day evaluation period without registration)**。若要以后注册安全设备及获取智能许可证，请点击菜单中的设备名称以访问**设备控制面板 (Device Dashboard)**，然后点击**智能许可证 (Smart Licenses)** 组中的链接。
7. 点击 **Finish**。

后续操作

完成设备设置向导后，系统会弹出一个窗口，为您提供后续选项。

- 如果将其他接口连接到了网络，请选择**配置接口 (Configure Interfaces)** 来配置连接的各个接口。
- 如果要修改默认访问规则，请选择**配置策略 (Configure Policy)** 来配置和管理流量策略。

您可以选择任一选项，也可以关闭弹出窗口返回到**设备控制面板 (Device Dashboard)**。

（可选）启动 Firepower 威胁防御 CLI 向导

首次启动时或执行系统重新映像后，可以使用 CLI 设置向导（而不是 Firepower 设备管理器）来执行初始配置，并可使用 CLI 进行故障排除。在使用 CLI 设置系统时，只能配置管理接口的 IP 地址。但无法通过 CLI 会话配置策略。也可以使用 Firepower 设备管理器来配置、管理和监控系统；请参阅启动 Firepower 设备管理器 （第 4 页）。

要登录到 CLI，请执行以下一项操作：

- 使用安全设备自带的控制台电缆将 PC 连接到使用终端仿真（设置为 9600 波特、8 个数据位、无奇偶校验、1 个停止位、无流控制）的控制台。有关控制台电缆的更多信息，请参阅安全设备的硬件指南。

  注意：控制台端口上的 CLI 默认为 FXOS CLI 登录提示。可以使用 **connect ftd** 命令来访问 Firepower 威胁防御 CLI。
- 使用 SSH 客户端连接到管理 IP 地址 （默认为 192.168.45.45）。使用 **admin** 用户名 （默认密码为 **Admin123**）进行登录。

登录后，如需了解 CLI 中可用命令的相关信息，请输入 **help** 或 ?。

程序

1. 在 **firepower login** 提示符下，使用默认凭据 （用户名 **admin**，密码 **Admin123**）登录。

   示例：

```
firepower login: admin
Password:
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2015, Cisco Systems, Inc. All rights reserved.
.
<...output truncated...>
.
firepower #
```

2. 连接到 Firepower 威胁防御应用。

   示例：

```
firepower #: connect ftd
```

3. 在 Firepower 威胁防御系统启动后，设置向导会提示您输入配置系统所需的以下信息：
   - 接受 EULA （最终用户许可协议）
   - 新管理员密码
   - IPv4 或 IPv6 配置
   - IPv4 或 IPv6 DHCP 设置
   - 管理端口 IPv4 地址和子网掩码，或者 IPv6 地址和前缀
   - 系统名称
   - 默认网关 IPv4、 IPv6 或数据接口设置
   - DNS 设置
   - HTTP 代理
   - 管理模式 （需要进行本地管理）
4. 查看设置向导设置。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。

   示例：

```
Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password:
Confirm new password:
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]: y
Do you want to configure IPv6? (y/n) [n]: y
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]: manual
Enter an IPv4 address for the management interface [192.168.45.45]: 192.168.0.43
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.0
Enter the IPv4 default gateway for the management interface [data-interfaces]: data-interfaces
Configure IPv6 via DHCP, router, or manually? (dhcp/router/manual) [disable]: manual
Enter the IPv6 address for the management interface []: 2001:420:1402:200f:e400::22
Enter the IPv6 address prefix for the management interface []: 76
Enter the IPv6 gateway for the management interface [data-interfaces]: data-interfaces
Enter a fully qualified hostname for this system [firepower]: FDM-FP2100
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
208.67.222.222
Enter a comma-separated list of search domains or 'none' []: cisco.com
If your networking information has changed, you will need to reconnect.
Setting IPv6: 2001:420:1402:200f:e400::22 prefix: 76 gateway: 2001:420:1402:200f:e400::1 on
management0
Setting DNS servers: 72.163.47.11
Setting DNS domains:cisco.com
Setting hostname as FDM-FP2100
DCHP Server Disabled
Setting static IPv4: 192.168.0.43 netmask: 255.255.255.0 gateway: 192.168.0.254 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
Configuring firewall mode to routed


Update policy deployment information
    - add device configuration
Successfully performed firstboot initial configuration steps for Firepower Device Manager for
Firepower Threat Defense.
```

后续操作

使用 Firepower 设备管理器可配置、管理和监控系统。通过浏览器可配置的功能不能通过 CLI 配置；必须使用 Web 界面来实施安全策略。

下一步是什么

- 有关使用 Firepower 设备管理器管理 Firepower 威胁防御的更多信息，请参阅 Firepower 威胁防御配置指南或 Firepower 设备管理器联机帮助。
- 在思科 Firepower 系统文档一览中可找到指向所有 Firepower 系统文档的链接。