适用于 Firepower 4100 的思科 FirePower 威胁防御：快速入门指南

首次发布日期：2016 年 3 月 10 日

最后更新日期：2017 年 7 月 18 日

1. 关于 Firepower 威胁防御安全服务

思科 Firepower 4100 安全设备是适用于网络和内容安全解决方案的独立安全服务平台，可以运行 Firepower 威胁防御应用。

您可以在数据中心使用 Firepower 威胁防御部署 Firepower 4100，提供下一代防火墙服务，包括状态防火墙、路由、下一代入侵防御系统 (NGIPS)、应用可视性与可控性 (AVC)、URL 过滤和高级恶意软件保护 (AMP)。您可以在单情景模式、路由模式或透明模式下使用威胁防御设备。

Firepower 威胁防御如何与 Firepower 4100 配合使用

Firepower 4100 安全设备在管理引擎上运行其操作系统，即 Firepower 可扩展操作系统 (FXOS)。Firepower 机箱管理器提供基于 GUI 的简便管理功能。您可以使用 Firepower 机箱管理器 Web 界面或 CLI 在管理引擎上配置硬件接口设置、智能许可和其他基本运行参数。

所有物理接口操作（包括建立外部 EtherChannel）均由管理引擎负责。您可以为运行 Firepower 威胁防御的逻辑设备分配接口，支持的接口有三种类型：数据接口、管理接口和 Firepower 事件接口。Firepower 事件接口专门用于传送事件流量。您可以根据需要，在部署时或部署后为具备 Firepower 威胁防御的 Firepower 4100 分配接口。这些接口在管理引擎中使用的 ID 与具备 Firepower 威胁防御的 Firepower 4100 配置中的 ID 相同。

部署具备 Firepower 威胁防御的 Firepower 4100 时，管理引擎将下载您选择的应用映像，并创建默认配置。您只能将具备 Firepower 威胁防御的 Firepower 4100 作为独立逻辑设备部署；不支持集群。

Firepower 管理中心支持和 CLI 访问

在部署具备 Firepower 威胁防御的 Firepower 4100 时，您可以为管理 Firepower 管理中心指定管理接口和注册信息，以便允许 Firepower 管理中心的访问。Firepower 威胁防御设备的注册步骤与其他受管设备相同。此外，您还可以进行策略配置和策略部署。

您还可以使用内部 Telnet 连接从 Firepower 4100 管理引擎 CLI 访问 Firepower 威胁防御 CLI。在 Firepower 4100 安全设备内，您随后可以通过其任意管理接口或数据接口配置 SSH 或 Telnet 访问；请参阅 6. 访问 Firepower 威胁防御 CLI（第 9 页）。

管理/诊断接口和网络部署

物理管理接口由管理逻辑接口与诊断逻辑接口共用。

Firepower 威胁防御设备可使用设置的 IP 地址（以及相关的网关路由）实现基于 Firepower 管理中心的管理。管理 IP 地址和路由**不包含**在 Firepower 管理中心 Web 界面上的设备接口或静态路由列表中，只能通过设置脚本和 CLI 设置。您需要在执行初始设置后，使用 Firepower 管理中心配置安全与访问策略、设备设置及接口。

请注意，如果您选择通过物理管理端口执行系统日志或 SNMP 报告，则必须使用 Firepower 管理中心 Web 界面为 Diagnostic 0/0 或 Diagnostic 1/1 接口配置单独的 IP 地址和路由以及外部身份验证。但是为了简化部署，思科建议将数据端口用于报告功能。

有关管理/诊断接口的更多信息，请参阅《*Firepower 管理中心配置指南*》的“Firepower 威胁防御接口”一章。

Firepower 威胁防御的许可要求

在 Firepower 4100 上运行的 Firepower 威胁防御需要智能软件许可。机箱中安全模块上的 Firepower 威胁防御实例都必须有自己的的许可证。所有安全服务的许可证授权均在 Firepower 管理中心中配置。

您购买的 Firepower 威胁防御设备自动包含一个基础许可证。所有其他许可证（威胁、恶意软件或 URL 过滤）均为可选。一个基础许可证将添加到您注册的每个 Firepower 威胁防御设备的 Firepower 管理中心。

- 有关可用于 Firepower 系统的功能许可证的概述，请参阅《思科 Firepower 系统功能许可证》。
- 有关如何在 Firepower 管理中心管理许可证的更多信息，请参阅《*Firepower 管理中心配置指南*》中的“Firepower 系统许可”。
- 有关 FXOS 机箱上许可证管理的一般信息，请参阅《*思科 FXOS Firepower 机箱管理器配置指南*》中的“许可证管理”。

访问 Firepower 机箱管理器 Web 界面

您可以使用 Firepower 机箱管理器 Web 界面管理应用映像，并配置硬件接口设置以及管理引擎上的其他基本操作参数。

程序

1. 登录 Firepower 机箱管理器 Web 界面：
   a. 使用支持的浏览器，在地址栏中输入以下 URL：

   `https://<chassis_mgmt_ip_address>`

   其中 *<chassis_mgmt_ip_address>* 是您在初始配置期间输入的 Firepower 4100 IP 地址或主机名。有关详细信息，请参阅初始配置（第 3 页）。

   b. 输入您的用户名和密码。

   c. 点击**登录 (Login)**。

   成功登录后，屏幕将显示 Firepower 机箱管理器 Web 界面，并进入“概述”(Overview) 页面。
2. 要退出 Firepower 机箱管理器 Web 界面，请选择**管理 (admin)** > **退出 (Logout)**。您将退出 Firepower 机箱管理器 Web 界面，并回到登录屏幕。

2. 部署 Firepower 威胁防御

Firepower 4100 使用两种基本类型的映像：平台捆绑包和应用。平台捆绑包包含管理引擎所需的 Firepower FXOS 软件包；应用映像是您需要在安全引擎上部署的软件映像。

Firepower 威胁防御作为应用映像部署在 Firepower 4100 的安全引擎上。应用映像作为思科安全数据包文件 (CSP) 提供，在部署到安全引擎之前存储在管理引擎中，用于创建逻辑设备，或者为今后创建逻辑设备做准备。您可以在管理引擎上存储同一个应用映像类型的多个不同版本。

通过**系统 (System)** 菜单的**更新 (Updates)** 页面，您可以从 Cisco.com 下载 FXOS 平台捆绑包、Firepower 威胁防御应用映像和最新的更新。然后，您可以将 Firepower 威胁防御映像上传到 Firepower 4100，以便在创建或更新逻辑设备时使用。请确保使用与管理引擎上运行的 FXOS 版本兼容的 Firepower 威胁防御映像版本。

有关详细信息，请参阅《*思科 FXOS Firepower 机箱管理器配置指南*》。

任务概述

开始在 Firepower 4100 安全设备上部署 Firepower 威胁防御之前，请先阅读以下准则和要求。

- 按照初始配置（第 3 页）中的说明，使用初始设置向导执行 Firepower 4100 安全设备的初始配置。
- 按照配置 NTP（第 4 页）中的说明，在 Firepower 机箱管理器中配置 NTP。
- 按照配置接口（第 5 页）中的说明，配置一个管理接口和至少一个数据接口。
- 按照部署Firepower 威胁防御逻辑设备（第 5 页）中的说明，配置一个 Firepower 威胁防御独立逻辑设备。
- 按照 3. 向 Firepower 管理中心注册（第 6 页）中的说明，在 Firepower 管理中心执行 Firepower 威胁防御单元发现。

如果要升级 Firepower 威胁防御 或 FXOS，或者要部署另一个应用，则需要从 Cisco.com 获得最新的 FXOS 平台捆绑包、应用映像和最新的更新；请参阅 5. 升级注意事项（第 7 页）。

初始配置

必须先使用可通过控制台端口访问的 FXOS CLI 执行一些初始配置任务，然后才能使用 Firepower 机箱管理器或 FXOS CLI 来配置和管理系统。首次使用 FXOS CLI 访问 FXOS 机箱时，您将会看到可用于配置系统的设置向导。

准备工作

- 在 FXOS 机箱上验证下列物理连接：
  - 控制台端口以物理方式连接到计算机终端或控制台服务器。
  - 1 Gbps 以太网管理端口连接到外部集线器、交换机或路由器。

  有关详细信息，请参阅《*思科 Firepower 机箱管理器配置指南*》。

程序

1. 通过控制台端口或使用 SSH（或通过其他方式）连接至 Firepower 4100 CLI。
2. 使用用户名 **admin** 和密码 **cisco123** 登录。
3. 根据提示完成系统配置。

   例如：

```
Enter the setup mode; setup newly or restore from backup. (setup/restore) ? setup
You have chosen to setup a new Security Appliance. Continue? (y/n): y
Enforce strong password? (y/n): n
Enter the password for "admin": <new password>
```

```
Confirm the password for "admin": <repeat password>
Enter the system name: FTD-SSP-4100
Physical Switch Mgmt0 IP address : 10.127.56.61
Physical Switch Mgmt0 IPv4 netmask : 255.255.255.0
IPv4 address of default gateway : 10.127.56.1
Configure the DNS Server IP address? (yes/no) [n]: n
Configure the default domain name? (yes/no) [n]: n

Following configurations will be applied:
   Switch Fabic=A
   System Name=FTD-SSP-4100
   Enforced Strong Password=no
   Physical Switch Mgmt0 IP Address=10.127.56.61
   Physical Switch Mgmt0 IP Netmask=255.255.255.0
   Default Gateway=10.127.56.1
   Ipv6 value=0

Apply and save the configuration (select 'n' if you want to re-enter)? (yes/no): yes
Applying configuration. 请稍候。
```

4. 使用新的登录凭证启动 Firepower 机箱管理器 Web 界面，检查能否连接。

   a. 使用支持的浏览器，在地址栏中输入以下 URL：

   `https://<chassis_mgmt_ip_address>`

   其中 <*chassis_mgmt_ip_address*> 是您在初始配置期间输入的 Firepower 4100 IP 地址或主机名。

   b. 输入您的用户名和密码。

   c. 点击**登录 (Login)**。

   成功登录后，屏幕将显示 Firepower 机箱管理器 Web 界面，并进入“概述”(Overview) 页面。

配置 NTP

要在 Firepower 4100 上部署 Firepower 威胁防御，您需要在 Firepower 机箱管理器上配置 NTP。为了确保智能许可正常工作且设备注册采用正确的时间戳，必须在 Firepower 机箱管理器上设置 NTP 服务器。

程序

1. 从 Firepower 机箱管理器界面中，选择**平台设置 (Platform Settings) > NTP**。
2. 从**时区 (Time Zone)** 下拉列表中为 Firepower 机箱选择适当的时区。
3. 在**设置时间来源 (Set Time Source)** 下面，点击**使用 NTP 服务器 (Use NTP Server)**，然后在 **NTP 服务器 (NTP Server)** 字段中输入想要使用的 NTP 服务器的 IP 地址或主机名。
4. 点击**保存 (Save)**。

   使用指定的 NTP 服务器配置 Firepower 机箱。

   注： 如果修改系统时间的过程超过 10 分钟，系统会将您注销，您需要重新登录 Firepower 机箱管理器。

配置接口

在 Firepower 4100 Firepower 威胁防御部署配置中涉及的管理引擎上配置管理类型的接口。您还必须至少配置一个数据类型的接口。

程序

1. 在 Firepower 机箱管理器界面中，选择**接口 (Interfaces)** 打开“接口”(Interfaces) 页面。
2. 添加一个 EtherChannel：
   a. 点击**添加端口通道 (Add Port Channel)**。
   b. 在“端口通道 ID”(Port Channel ID) 字段中，输入一个介于 1 和 47 之间的值。
   c. 选中**启用 (Enable)**。
   d. 对于类型，选择**管理 (Management)**、**数据 (Data)** 或 **Firepower 事件 (Firepower Eventing)**。每个逻辑设备只能包括一个管理接口。

   注： 接口类型一旦分配给调配的逻辑设备，便无法更改。

   e. 根据需要添加成员接口。
   f. 点击**确定 (OK)**。
3. 对单个接口执行以下操作：
   a. 点击接口行中的**编辑 (Edit)** 图标，打开“编辑接口”(Edit Interface) 对话框。
   b. 选中**启用 (Enable)**。
   c. 对于“类型”(Type)，点击**管理 (Management)**、**数据 (Data)** 或 **Firepower 事件 (Firepower Eventing)**。每个逻辑设备只能包括一个管理接口。
   d. 点击**确定 (OK)**。

部署Firepower 威胁防御逻辑设备

您可以将 Firepower 威胁防御配置为独立逻辑设备。您需要配置以下逻辑设备信息：

- 设备信息和地址
- 设备设置，包括 Firepower 管理中心注册信息、防火墙模式和事件
- 接口信息和地址
- 终端用户许可协议

程序

1. 在 Firepower 机箱管理器界面中，选择**逻辑设备 (Logical Devices)** 以打开“逻辑设备”(Logical Devices) 页面。
2. 点击**添加设备 (Add Device)** 打开“添加设备”(Add Device) 对话框。
3. 在**设备名称 (Device Name)** 字段中，为逻辑设备提供一个名称。此名称由 Firepower 4100 管理引擎用于配置管理设置和分配接口；它不是安全模块配置中使用的设备名称。
4. 对于**模板 (Template)**，选择 **Firepower 威胁防御 (Firepower Threat Defense)**。
5. 对于**映像版本 (Image Version)**，选择 Firepower 威胁防御软件版本。

6. 对于**设备模式 (Device Mode)**，点击**独立 (Standalone)** 单选按钮。
7. 点击**确定 (OK)**。屏幕将显示 *调配 - 设备名称 (Provisioning - device name)* 窗口。
8. 展开**数据端口 (Data Ports)** 区域，然后点击要分配给 Firepower 威胁防御的各个接口。
9. 点击屏幕中心的设备图标。系统将显示配置对话框。
10. 为“配置”(Configuration) 对话框中的每个选项卡配置部署选项：
    a. 逻辑设备信息 (Logical Device Information) - 输入此逻辑设备的管理设置。

    注： 虚拟 IPv4 或 IPv6 地址可以在完成设备注册后从 Firepower 管理中心进行配置。如果您要使用系统日志，此设置非常重要。

    b. 设置 (Settings) - 为管理 Firepower 管理中心输入注册密钥、密码和 IP 地址；然后选择防火墙模式、Firepower 事件接口（如果已配置）和 DNS 信息。

    注： 注册密钥是由用户生成的一次性使用密钥，长度不超过 37 个字符。有效字符包括字母数字（A–Z、a–z、0–9）和连字符 (-)。当您将设备添加到 Firepower 管理中心时，需要记住此注册密钥。

    c. 接口信息 (Interface Information) - 输入此逻辑设备的管理设置。

    注： 安全模块都必须有自己的 IP 地址，在注册设备时，Firepower 管理中心会使用该地址。将模块添加到 Firepower 管理中心时必须使用该 IP 地址。

    d. 同意 (Agreement) - 阅读并接受《终端用户许可协议》(EULA)。
11. 点击**确定 (OK)** 关闭配置对话框。
12. 点击**保存 (Save)**。Firepower 4100 管理引擎通过下载指定的软件版本，并将引导程序配置和管理接口设置推送到安全模块来部署逻辑设备。

3. 向 Firepower 管理中心注册

准备工作

- 对于您计划注册的 Firepower 威胁防御安全模块，在 Firepower 机箱管理器中检查其设置。
- 在 Firepower 4100 上运行的 Firepower 威胁防御需要智能软件许可，可以从 Firepower 管理中心进行配置。

程序

1. 在浏览器中，使用已配置的 Firepower 管理中心的主机名或地址通过 HTTPS 连接登录 Firepower 管理中心。例如，https://MC.example.com。
2. 在管理中心 Web 界面上，选择**设备 (Devices)** > **设备管理 (Device Management)**。
3. 从 **Add** 下拉菜单中，选择 **Add Device**。
4. 在**主机 (Host)** 字段中，键入要添加的 Firepower 威胁防御设备的 IP 地址。
5. 在**显示名称 (Display Name)** 字段中，键入要在管理中心显示的 Firepower 威胁防御设备名称。
6. 在**注册密钥 (Registration Key)** 字段中，键入在 Firepower 机箱管理器中配置 Firepower 威胁防御设备时使用的同一注册密钥。
7. 如果要在多域环境中添加设备，请从**域 (Domain)** 下拉列表中选择一个值，将设备分配到枝叶域。

8. 从**访问控制策略 (Access Control Policy)** 下拉列表中选择要部署到安全模块的初始策略：
   - **Default Access Control** 策略阻止所有流量进入网络。
   - **Default Intrusion Prevention** 策略允许也通过 Balanced Security 和 Connectivity 入侵策略传递的所有流量。
   - **Default Network Discovery** 策略允许仅通过网络发现进行检查的所有流量。
   - 可以选择用户定义的任何现有的访问控制策略。有关详细信息，请参阅《*Firepower 管理中心配置指南*》中的“管理访问控制策略”一节。
9. 选择要应用到设备的许可证。请注意：
   - 控制、恶意软件和 URL 过滤许可证需要保护许可证。
10. 点击**注册 (Register)**，并确认注册成功。

4. 配置策略和设备设置

安装 Firepower 威胁防御并将设备添加到管理中心后，您可以使用 Firepower 管理中心用户界面为 Firepower 4100 上运行的 Firepower 威胁防御配置设备管理设置，还可以使用该界面配置并应用访问控制策略和其他相关策略，以利用 Firepower 威胁防御安全模块管理流量。

安全策略可对 Firepower 威胁防御提供的服务进行控制（例如下一代 IPS 过滤和应用过滤）。您可以使用 Firepower 管理中心配置 Firepower 威胁防御上的安全策略。有关如何配置安全策略的详细信息，请参阅《*思科 Firepower 配置指南*》或 Firepower 管理中心中的在线帮助。

5. 升级注意事项

如果要升级 Firepower 威胁防御部署或 Firepower 管理引擎，或者要部署另一个应用，则需要从 Cisco.com 获得最新的 FXOS 平台捆绑包、应用映像和最新的更新。

注： 必须使用 Firepower 管理中心升级 Firepower 威胁防御逻辑设备。不要使用 Firepower 机箱管理器或 FXOS CLI 升级 Firepower 威胁防御逻辑设备。请参阅《Firepower 系统版本说明》，了解详细信息。

下列操作程序介绍了如何使用**系统 (System)** 菜单的**更新 (Updates)** 页面从 Cisco.com 下载 FXOS 平台捆绑包、应用映像（例如 Firepower 威胁防御 或其他应用）和最新的更新，并介绍了如何上传映像和升级管理引擎。

- 要获得必要的 FXOS 软件包和应用映像，请参阅从 Cisco.com 下载软件映像（第 7 页）。
- 要上传应用或平台捆绑包，请参阅将软件映像上传到 Firepower 4100（第 8 页）。
- 要删除现有的逻辑设备或配置，请参阅删除现有逻辑设备和应用配置（第 8 页）。
- 要升级管理引擎软件捆绑包，请参阅升级 Firepower 管理引擎平台（第 9 页）。

从 Cisco.com 下载软件映像

准备工作

- 必须拥有 Cisco.com 帐户。
- 应熟悉设置所需的兼容平台捆绑包和 Firepower 威胁防御应用映像版本。
- 必须能够访问互联网。

程序

1. 在 Firepower 机箱管理器界面中，选择**系统 (System) > 更新 (Updates)**。“可用更新 (Available Updates)”页面显示机箱上可用的 Firepower 4100 平台捆绑包映像和应用映像列表。
2. 点击页面底部的**从 CCO 下载最新更新 (Download latest updates from CCO)** 链接。Firepower 4100的软件下载页面可在浏览器中的新标签中打开。
3. 找到适当的软件映像，并将其下载到您的本地计算机。

将软件映像上传到 Firepower 4100

准备工作

- 确保您要上传的所有映像均已在本地计算机上准备就绪。

程序

1. 在 Firepower 机箱管理器界面中，选择**系统 (System) > 更新 (Updates)**。“可用更新 (Available Updates)”页面显示机箱上可用的 Firepower 4100 平台捆绑包映像和应用映像列表。
2. 点击**上传映像 (Upload Image)**，可打开“上传映像”(Upload Image) 对话框。
3. 点击**浏览 (Browse)**，寻找并选择需要上传的映像。
4. 点击**上传**。已选中的映像被上传到 Firepower 4100。
5. 请按照系统提示接受任何终端用户许可协议，然后继续。

删除现有逻辑设备和应用配置

要升级 Firepower 威胁防御逻辑设备或部署其他逻辑设备，您必须删除现有设备，然后使用已更新的映像创建新设备。如果要升级 FXOS 平台捆绑包映像和应用，必须首先升级 FXOS 平台捆绑包。

程序

1. 在 Firepower 机箱管理器界面中，选择**逻辑设备 (Logical Devices)** 以打开“逻辑设备”(Logical Devices) 页面。

   “逻辑设备 (Logical Devices)”页面显示在机箱上配置的逻辑设备列表。如果尚未配置任何逻辑设备，则系统将显示一条表明此情况的消息。
2. 点击每个逻辑设备对应的**删除 (Delete)** 图标。
3. 当系统提示时，点击**是 (Yes)** 删除逻辑设备。
4. 当系统提示时，点击**是 (Yes)** 删除应用配置。这最后一步对于成功安装 Firepower 威胁防御非常必要。

后续操作

- 检查当前在机箱中运行的 Firepower FXOS 软件版本，确定是否需要进行升级，才能在安全引擎上运行 Firepower 威胁防御或其他任何应用。

升级 Firepower 管理引擎平台

FXOS 的运行版本显示在 Firepower 机箱管理器 Web 界面上的**概述 (Overview)** 页面的顶部。您需要确定当前在机箱中运行的 FXOS 版本是否足以支持在安全引擎上运行您的应用。您可以从**系统 (System)** 菜单的**更新 (Updates)** 页面升级 FXOS 平台捆绑包。

程序

1. 在 Firepower 机箱管理器界面中，选择**系统 (System) > 更新 (Updates)**。“可用更新 (Available Updates)”页面显示机箱上可用的 Firepower 4100 平台捆绑包映像和应用映像列表。
2. 浏览**映像名称 (Image Name)** 列，找到需要加载的 FXOS 平台捆绑包。
3. 点击与需要加载的 FXOS 平台捆绑包关联的上传/下载图标。
4. 在**更新捆绑包映像 (Update Bundle Image)** 对话框中，点击“是”(Yes) 确认所选版本。点击“是”(Yes) 后，系统将安装所选版本，并重新启动设备。

6. 访问 Firepower 威胁防御 CLI

在进行初始配置或故障排除时，可以从 Firepower 4100 FXOS 管理引擎 CLI 访问 Firepower 威胁防御 CLI。

程序

1. 通过控制台端口或使用 SSH（或通过其他方式）连接至管理引擎 CLI。
2. 连接到其中一个安全模块。

   connect module *slot* **console**

   示例：

   ```
   cisco-ssp-A# connect module 1 console
   firepower>
   ```

3. 首次连接到该模块时，您会进入 Firepower 机箱管理器模块 CLI（按照 FirePower 的提示操作）。您必须手动连接到 Firepower 威胁防御 CLI：

   connect ftd

   示例：

   ```
   firepower> connect ftd
   >
   ```

   此后，所有连接都将直接跳转到 Firepower 威胁防御 CLI。
4. 要退出 Firepower 威胁防御连接，请键入 **exit**。

   示例：

   ```
   > exit
   firepower>
   ```

5. 要访问系统诊断信息，请键入 **system support diagnostic-cli**。

   示例：

   ```
   firepower> system support diagnostic-cli
   ```

6. 要退出控制台连接，请键入 ~。您将退出至 Telnet 应用。输入 **quit** 退出到管理引擎 CLI。

   示例：

```
firepower> ~
telnet> quit
cisco-ssp-A#
```

7. 后续步骤

- 您可以在 Firepower 4100 文档页面找到所有 Firepower 4100 相关文档的链接。