适用于 **Firepower 2100** 系列的思科 **ASA** 入门指南

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

本手册中有关产品的规格和信息如有更改，恕不另行通知。本手册中的所有声明、信息和建议均准确可靠，但我们不为其提供任何明示或暗示的担保。用户必须承担使用产品的全部责任。

随附产品的软件许可和有限担保在随产品一起提供的信息包中提供，且构成本文的一部分。如果您无法找到软件许可或有限担保，请与思科代表联系获取副本。

思科所采用的 TCP 报头压缩是加州大学伯克利分校 (UCB) 开发的一个程序的改版，是 UCB 的 UNIX 操作系统公共域版本的一部分。保留所有权利。版权所有 © 1981，加州大学董事会。

无论本手册中是否有任何其他保证，这些供应商的所有文档文件和软件均按“原样”提供，并可能包含缺陷。思科和上面所提及的供应商拒绝所有明示或暗示保证，包括（但不限于）适销性、特定用途适用性和无侵权保证，或者因买卖或使用以及商业惯例所引发的保证。

在任何情况下，对于任何间接、特殊、连带发生或偶发的损坏，包括（但不限于）因使用或无法使用本手册而导致的任何利润损失或数据损失或损坏，思科及其供应商概不负责，即使思科及其供应商已获知此类损坏的可能性也不例外。

本文档中使用的任何互联网协议 (IP) 地址和电话号码并非实际地址和电话号码。本文档中所含的任何示例、命令显示输出、网络拓扑图和其他图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表，请访问此网址：http://www.cisco.com/go/trademarks。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。(1110R)

目 录

第 1 章

使用入门

本章介绍如何在网络中的 Firepower 2100 上部署 ASA，以及如何执行初始配置。

关于适用于 Firepower 2100 的 ASA

Firepower 2100 硬件可以运行思科 ASA 软件或 Firepower 威胁防御软件。本指南介绍了如何在 Firepower 2100 上使用 ASA。

注释 在 ASA 和 Firepower 威胁防御之间切换需要您对设备进行重新映像。请参阅重新映像思科 ASA 或 Firepower 威胁防御设备。

ASA 如何与 Firepower 2100 配合使用

Firepower 2100 是适用于 ASA 的单一应用程序设备。Firepower 2100 运行名为 Firepower 可扩展操作系统 (FXOS) 的底层操作系统。您必须在 FXOS 中配置基本的操作参数和硬件接口设置。这些设置

包括启用接口、建立 EtherChannel、NTP、映像管理等。您可以使用 Firepower 机箱管理器 web 界面或 FXOS CLI。然后，您可以使用 ASDM 或 ASA CLI 在 ASA 操作系统中配置安全策略。

ASA 和 FXOS 管理

ASA 和 FXOS 操作系统共享管理 1/1 接口。此接口拥有单独的 IP 地址，用于连接到 ASA 和 FXOS。

注释 此接口在 ASA 中被称为管理 1/1；在 FXOS 中，您可能会看到它显示为 MGMT、management0 或其他类似名称。本指南将此接口称为管理 1/1，以保持一致性和简洁性。

某些功能必须在 FXOS 上进行监控，而其他功能则必须在 ASA 上进行监控，因此您需要利用这两个操作系统进行持续维护。对于 FXOS 上的初始配置，您可以使用 SSH 或您的浏览器 (https://192.168.45.45) 连接到默认的 192.168.45.45 IP 地址。

对于 ASA 的初始配置，您可以使用 ASDM 连接到 https://192.168.45.1/admin。在 ASDM 中，您可以以后从任何接口配置 SSH 访问。

这两个操作系统都可从控制台端口获得。初始连接将访问 FXOS CLI。您可以使用 **connect asa** 命令来访问 ASA CLI。

您还可以允许从 ASA 数据接口进行 FXOS 管理；配置 SSH、HTTPS 和 SNMP 访问。此功能对远程管理非常有用。

许可证要求

Firepower 2100 上的 ASA 使用思科智能软件许可。您可以使用常规智能软件许可，这需要互联网接入；或者对于离线管理，您可以配置永久许可证保留或卫星服务器。有关这些离线许可方法的更多信息，请参阅思科 ASA 系列功能许可证；本指南适用于常规智能软件许可。

在向许可证颁发机构注册之前，您将无法对需要特殊许可证的功能进行配置更改，但操作则不受影响。许可的功能包括：

- 安全情境（2 种以上）
- 强加密 (3DES/AES)（适用于通过流量）

您还需要“标准 (Standard)”许可证，但对于基本功能，设备可在评估模式下运行。

ASA 默认情况下包含 3DES 功能，仅用于管理访问，因此您可以连接到许可证颁发机构，还可以立即使用 ASDM。请注意，要访问 ASDM，必须将接口设置为仅管理，否则必须启用完整的“强加密 (Strong Encryption)”(3DES/AES) 许可证；默认配置包括设置为仅管理的管理 1/1 接口。当您向智能软件许可帐户请求 ASA 的注册令牌时，请选中**允许使用此令牌注册的产品上的导出控制功能 (Allow export-controlled functionaility on the products registered with this token)** 复选框，以便应用完整的“强加密 (Strong Encryption)”许可证（您的帐户必须符合其使用条件）。有关许可的更多详细信息，请参阅启动 ASDM 并配置许可，第 7 页。

注释 与 Firepower 4100/9300 机箱不同，您在 ASA 上执行所有许可配置，而不是在 FXOS 配置中执行。

不支持的功能

Firepower 2100 不支持以下功能：

- 集成路由和桥接
- 集群
- 无客户端 SSL VPN 与 KCD
- ASA REST API
- ASA FirePOWER 模块
- 僵尸网络流量过滤器
- 以下检查：

  SCTP 检查图（支持使用 ACL 的 SCTP 状态检查）

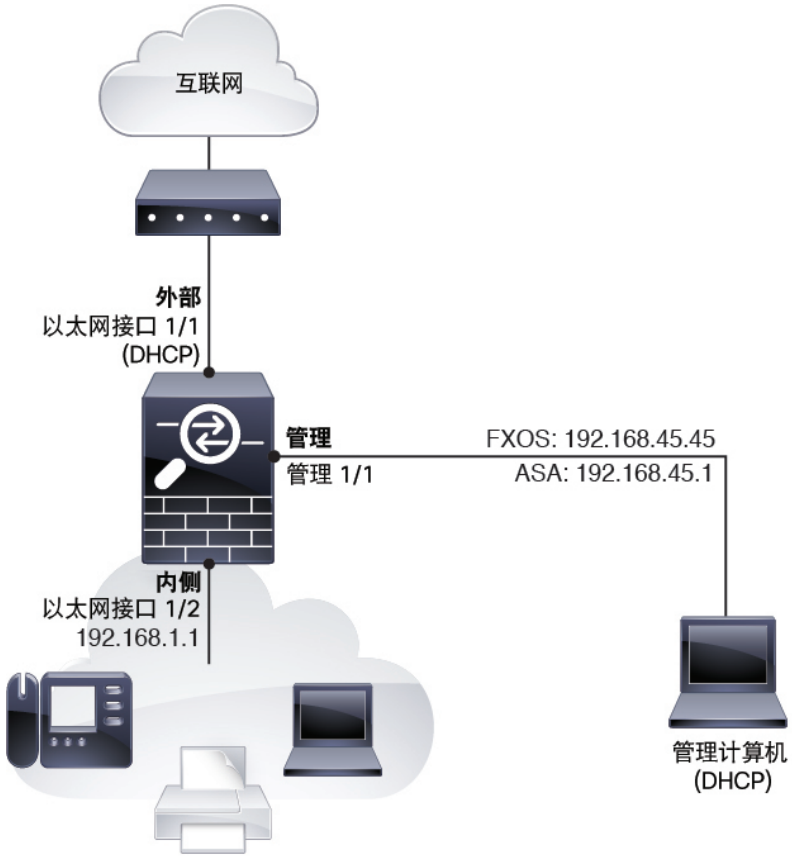
  Diameter

  GTP/GPRS

您的网络中的 Firepower 2100

下图显示了适用于 Firepower 2100 上的 ASA 的默认网络部署。

图 *1*：您的网络中的 *Firepower 2100* 上的 *ASA*



在完成本指南中所述的初始设置后，默认配置将启用上述网络部署，并具有以下行为：

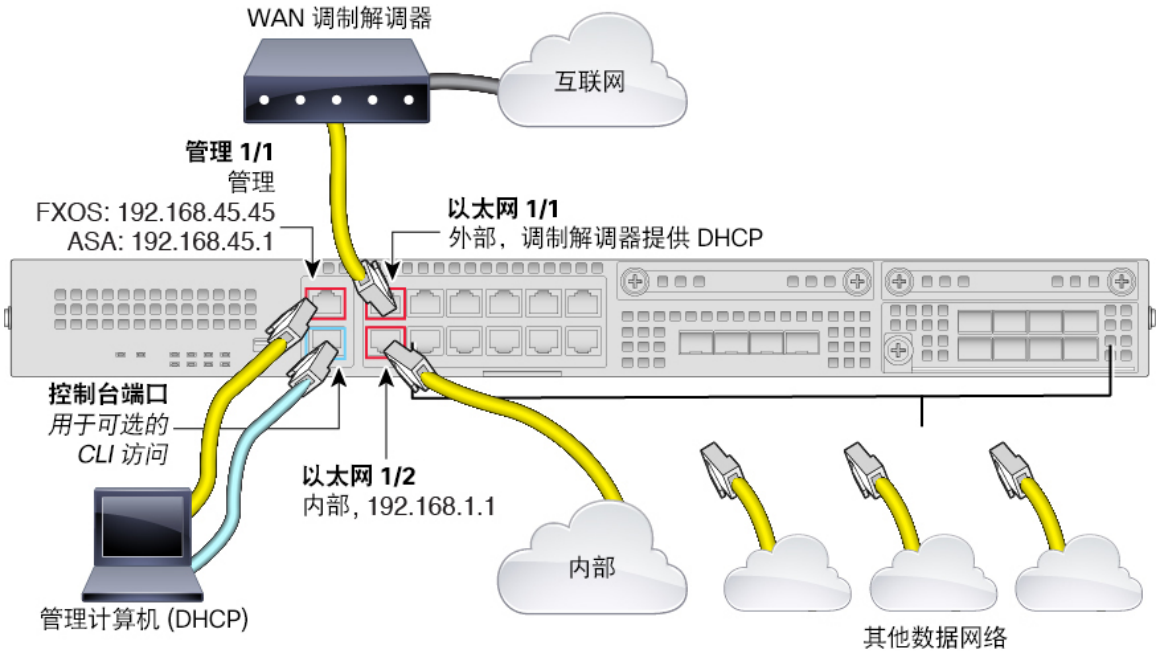
- 内部 --> 外部流量，包括 NAT
- 外部 **IP** 地址从 **DHCP** 获取
- 管理 **1/1** 用于 FXOS 和 ASA 管理。DHCP IP 地址由 FXOS 提供给此网络上的管理计算机。

连接接口

在管理 1/1 接口上管理 Firepower 2100。您可以对 FXOS 和 ASA 使用同一管理计算机。连接到 FXOS IP 地址上的 Firepower 机箱管理器以执行机箱配置。然后使用 ASDM 连接到 ASA IP 地址，以完成 ASA 配置。

默认配置还会将 Ethernet1/1 配置为外部，将 Ethernet1/2 配置为内部。

图 2：将线缆连接到 *Firepower 2100* 接口



过程

步骤 1 使用以太网将管理计算机连接到管理 1/1（标记为 MGMT）。

步骤 2 （可选） 将管理计算机连接到控制台端口。Firepower 2100 配有一条 DB-9 转 RJ-45 串行线缆，所以您需要第三方串行转 USB 线缆进行连接。确保为操作系统安装任何必要的 USB 串行驱动程序。

步骤 3 将外部网络连接到 Ethernet1/1 端口（标记为 WAN）。对于智能软件许可，ASA 需要互联网接入，以便它可以访问许可证颁发机构。

步骤 4 根据需要将内部网络连接到 Ethernet1/2 和其他数据接口。

启动 Firepower 2100

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。

过程

步骤 1 将电源线连接到 Firepower 2100，然后将其连接到电源插座。

步骤 2 将机箱背面的电源开关按到 1 位置。
要关闭机箱电源，请将机箱背面的电源开关按到 0 位置。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。

步骤 3 检查机箱正面的 PWR LED；如果绿灯常亮，表示机箱已接通电源。

步骤 4 检查机箱正面的 SYS LED；在其绿灯常亮后，表示系统已通过启动诊断。

（可选）在 Firepower 机箱管理器中启用其他接口

默认情况下，管理 1/1、以太网 1/1 和以太网 1/2 接口将以物理方式为机箱启用，并以逻辑方式在 ASA 配置中启用。要使用任何其他接口，必须使用此程序为机箱启用它，然后在 ASA 配置中启用它。您还可以添加 EtherChannel（也称为端口通道）。

开始之前

- Firepower 2100 仅在有效链路汇聚控制协议 (LACP) 模式下支持 EtherChannel。我们建议将连接交换机端口设置为“活动 (Active)”模式，以实现最佳兼容性。
- 要从默认值更改管理 IP 地址，请参阅更改 FXOS 管理 IP 地址或网关，第 15 页。

过程

步骤 1 在与管理 1/1 接口连接的管理计算机上，通过访问以下 URL 启动 Firepower 机箱管理器：**https://192.168.45.45**。

步骤 2 输入默认用户名：**admin** 和密码：**Admin123**。
思科建议您立即在**系统 (System)** > **用户管理 (User Management)** > **本地用户 (Local Users)** 页上更改密码。

要更改管理 IP 地址，请参阅更改 FXOS 管理 IP 地址或网关，第 15 页。

步骤 3 在 Firepower 机箱管理器中，点击**接口 (Interfaces)** 选项卡。

步骤 4 要启用或禁用接口，请点击**管理状态 (Admin State)** 滑块。复选标记表示已启用，而 X 则表示已禁用。

注释 管理 1/1 接口在该表中显示为 **MGMT**。

步骤 5 （可选） 添加 EtherChannel.

注释 EtherChannel 成员端口在 ASA 上可见，但您只能在 FXOS 中配置 EtherChannels 和端口成员身份。

a) 点击接口表上方的**添加端口通道 (Add Port Channel)**。
b) 在**端口通道 ID (Port Channel ID)** 字段中，输入端口通道的 ID。有效值介于 1 与 47 之间。
c) 选中**启用 (Enable)** 复选框以启用端口通道。
忽略**类型 (Type)** 下拉列表；唯一可用的类型是**数据 (Data)**。
d) 从**管理速度 (Admin Speed)** 下拉列表中，选择所有成员接口的速度。
如果您选择的接口无法达到所选速度（以及您选择的其他设置），则会自动应用尽可能最快的速度。
e) 为所有成员接口点击**自动协商 (Auto Negotiation) 是 (Yes)** 或**否 (No)** 单选按钮。
f) 在**管理双工 (Admin Duplex)** 下拉列表中，为所有成员接口选择双工。
g) 在**可用接口 (Available Interface)** 列表中，选择您要添加的接口，然后点击**添加接口 (Add Interface)**。
您最多可以添加 16 个同一类型和速度的接口。添加到通道组的第一个接口确定正确的类型和速度。

提示 一次可添加多个接口。要选择多个独立接口，请点击所需的接口，同时按住 **Ctrl** 键。要选择一个接口范围，请选择范围中的第一个接口，然后，在按住 **Shift** 键的同时，点击选择范围中的最后一个接口。

h) 点击**确定 (OK)**。

启动 ASDM 并配置许可

启动 ASDM 并将您的设备注册到智能软件许可证服务器。

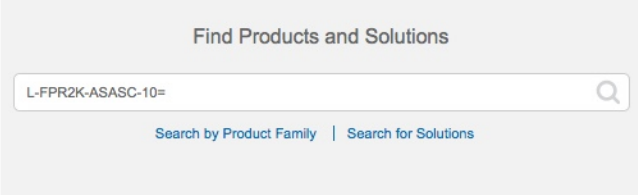
开始之前

- 请参阅 Cisco.com 上的 ASDM 版本说明了解运行 ASDM 的要求。
- 此程序假定您已将以太网 1/1 外部接口连接到互联网，并且您使用的是默认配置。请参阅您的网络中的 Firepower 2100，第 4 页。
- 拥有思科智能软件管理器主帐户。

  如果您还没有帐户，请点击此链接以设置新帐户。通过智能软件管理器，您可以为组织创建一个主帐户。
- 您的思科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）。
- 请确保您的帐户包含您所需的可用许可证，包括最低限度的标准许可证。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，则请使用思科商务工作空间上的**查找产品和解决方案 (Find Products and Solutions)**搜索字段。搜索以下许可证 PID：

图 *3*：许可证搜索



标准许可证 - L-FPR2100-ASA=。标准许可证是免费的，但您仍然需要将其添加到您的智能软件许可帐户中。

5 情景许可证 - L-FPR2K-ASASC-5=。情景许可证是附加的；请购买多份许可证以满足您的需要。

10 情景许可证 - L-FPR2K-ASASC-10=。情景许可证是附加的；请购买多份许可证以满足您的需要。

强加密 (3DES/AES) 许可证 - L-FPR2K-ENC-K9=。此许可证是免费的。虽然只有使用较旧的卫星服务器版本（2.3.0 以前的版本）的 ASA 需要此许可证，但您仍应将其添加到您的帐户中以进行跟踪。

注释 对于故障切换对，您必须将标准许可证（和相同的加密）应用于两台设备；对于情景许可证，只需将其应用于主设备。

过程

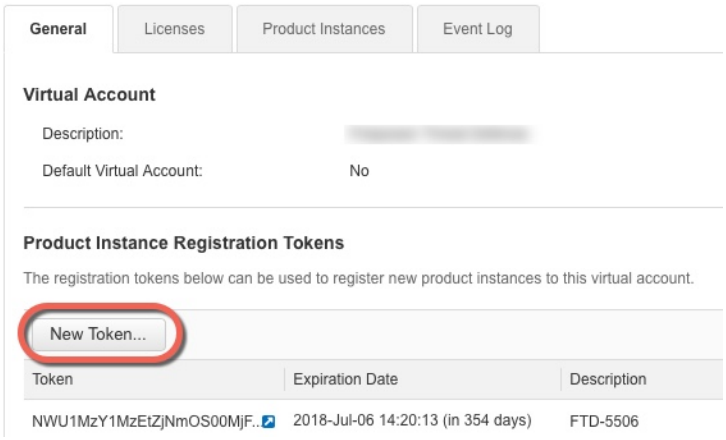
步骤 1 在智能软件管理器（思科智能软件管理器）中，为要将此设备添加到其中的虚拟帐户请求一个注册令牌并复制该令牌。

a) 点击**资产 (Inventory)**。

图 *4*：资产

b) 在常规 **(General)** 选项卡上，点击新建令牌 **(New Token)**。

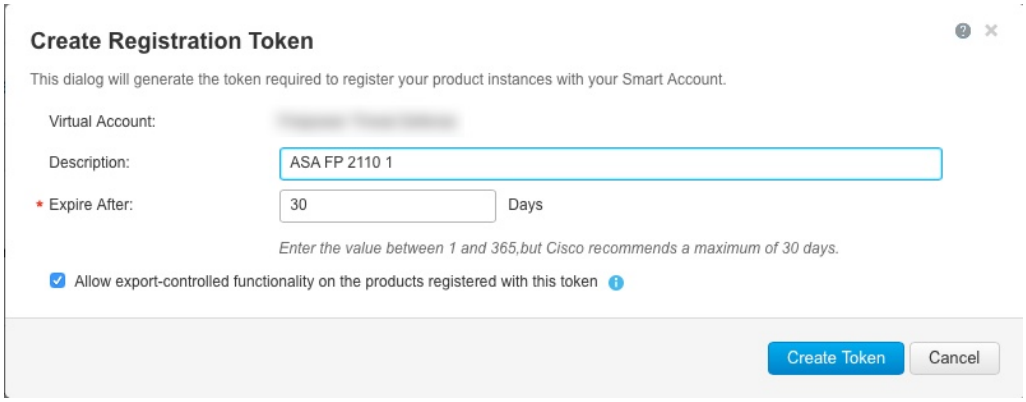
图 *5*：新建令牌



c) 在创建注册令牌 **(Create Registration Token)** 对话框中，输入以下设置，然后点击创建令牌 **(Create Token)**：

- 说明 **(Description)**
- 在以下时间后到期 **(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 functionaility on the products registered with this token)** - 启用导出合规性标志。

图 *6*：创建注册令牌



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**令牌 (Token)** 对话框，可以从中将令牌 ID 复制到剪贴板。当需要注册 ASA 时，请准备好此令牌，以在该程序后面的部分使用。

图 7：查看令牌

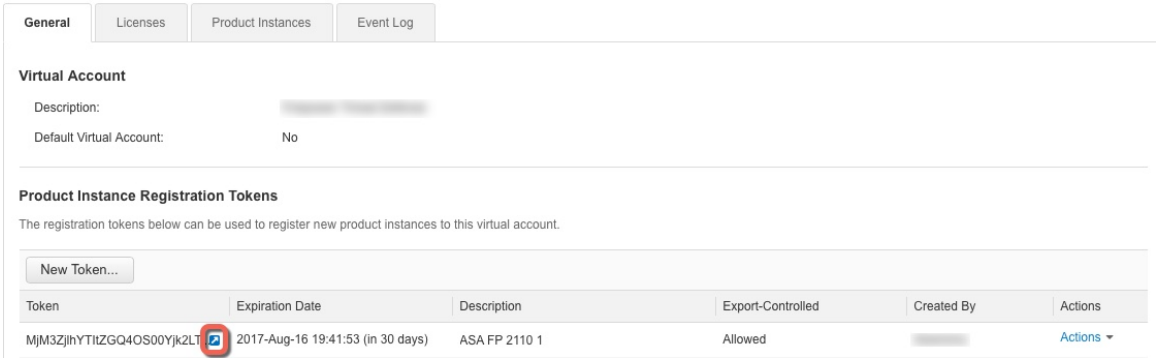
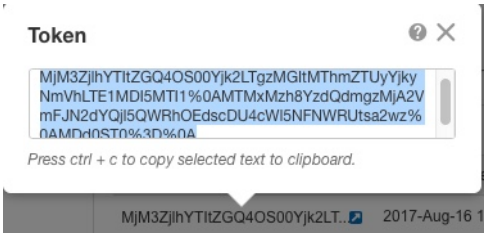


图 8：复制令牌



步骤 2 在连接到管理 1/1 的管理计算机上，启动网络浏览器并转到以下 URL：**https://192.168.45.1/admin**。此时将显示**思科 ASDM (Cisco ASDM)** 网页。

步骤 3 点击以下可用选项之一：**安装 ASDM 启动器 (Install ASDM Launcher)** 或**运行 ASDM (Run ASDM)**。

步骤 4 根据您选择的选项，按照屏幕上的说明启动 ASDM。系统将显示**思科 ASDM-IDM 启动程序 (Cisco ASDM-IDM Launcher)**。

步骤 5 将用户名和密码字段留空，然后点击**确定 (OK)**。系统将显示 ASDM 主窗口。

步骤 6 依次选择**配置 (Configuration)** > **设备管理 (Device Management)** > **许可 (Licensing)** > **智能许可 (Smart Licensing)**。

步骤 7 选中**启用智能许可证配置 (Enable Smart license configuration)**。

步骤 8 从**功能层 (Feature Tier)** 下拉菜单中，选择**标准 (Standard)**。
仅标准层可用。

步骤 9 （可选） 对于**情景 (Context)** 许可证，输入情景的数目。
情景的最大数目取决于您的型号。您可以在没有许可证的情况下使用 2 种情景。

- Firepower 2110 - 25 种情景
- Firepower 2120 - 25 种情景
- Firepower 2130 - 30 种情景

- Firepower 2140 - 40 种情景

步骤 10 点击**应用 (Apply)**。

步骤 11 点击**注册 (Register)**。

步骤 12 在 **ID 令牌 (ID Token)** 字段中输入注册令牌。

步骤 13 点击**注册 (Register)**。

ASA 使用预先配置的外部接口向许可证颁发机构注册，并请求对已配置的许可证授权进行授权。如果您的帐户允许，则许可证颁发机构还会应用强加密 (3DES/AES) 许可证。依次选择**监控 (Monitoring) > 属性 (Properties) > 智能许可证 (Smart License)** 以检查许可证状态。

配置 ASA

利用 ASDM，您可以使用向导来配置基本功能和高级功能。您还可以手动配置向导中未包括的功能。

过程

步骤 1 依次选择**向导 (Wizards) > 启动向导 (Startup Wizard)**，然后点击**修改现有配置 (Modify existing configuration)** 单选按钮。

步骤 2 **启动向导 (Startup Wizard)** 将引导您完成配置：

- 启用密码
- 接口，包括更改内部和外部接口 IP 地址，以及启用您在第 6 页的“（可选）在 Firepower 机箱管理器中启用其他接口”中配置的接口 （可选）在 Firepower 机箱管理器中启用其他接口，第 6 页
- 静态路由
- DHCP 服务器（不会为管理 1/1 接口设置 DHCP 服务器）
- 其他...

步骤 3 （可选） 在**向导 (Wizards)** 菜单中，运行其他向导。

步骤 4 要继续配置 ASA，请参阅浏览思科 ASA 系列文档中适合您的软件版本的文档。

ASA 和 FXOS CLI 访问

本节介绍如何连接到 FXOS 和 ASA 控制台；在 ASA 数据接口上配置 FXOS SSH、HTTPS 和 SNMP 访问，并使用 SSH 连接到 FXOS。

连接到 ASA 或 FXOS 控制台

Firepower 2100 控制台端口会将您连接到 FXOS CLI。您可以从 FXOS CLI 中连接到 ASA 控制台，然后再次返回。

开始之前

每次只能有 1 个控制台连接。当您从 FXOS 控制台连接到 ASA 控制台时，此连接是一个持久控制台连接，而不像 Telnet 或 SSH 连接那样。

过程

步骤 1 将管理计算机连接到控制台端口。Firepower 2100 配有一条 DB-9 转 RJ-45 串行线缆，所以您需要第三方串行转 USB 线缆进行连接。确保为操作系统安装任何必要的 USB 串行驱动程序。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

您将连接到 FXOS CLI。

步骤 2 连接到 ASA：
connect asa

示例：

```
firepower-2100# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

步骤 3 要返回到 FXOS 控制台，请输入 **Ctrl+a**, **d**。

在数据接口上配置对 FXOS 的管理访问

如果要从数据接口管理 Firepower 2100 上的 FXOS，可以配置 SSH、HTTPS 和 SNMP 访问。如果要远程管理设备，并且保持管理 1/1 位于独立网络中，则此功能非常有用。您可以继续使用管理 1/1 进行本地访问；不能在将流量转发到 ASA 数据接口的同时，允许从管理 1/1 对 FXOS 进行远程访问，因为您只能指定一个网关。默认情况下，FXOS 管理网关是到 ASA 的内部路径。

ASA 使用非标准端口进行 FXOS 访问；标准端口将被保留以供同一接口上的 ASA 使用。当 ASA 将流量转发到 FXOS 时，它会针对每个协议将非标准目标端口转换为 FXOS 端口（不会更改 FXOS 中

的 HTTPS 端口）。数据包目标 IP 地址（即 ASA 接口 IP 地址）也会被转换为内部地址，供 FXOS 使用。源地址保持不变。为了返回流量，ASA 使用其数据路由表来确定正确的出口接口。当您访问管理应用的 ASA 数据 IP 地址时，必须使用 FXOS 用户名登录；ASA 用户名只适用于 ASA 管理访问。

您还可以在 ASA 数据接口上启用 FXOS 管理流量启动，这是 SNMP 陷阱或进行 NTP 和 DNS 服务器等所需的。默认情况下，将为 ASA 外部接口启用 FXOS 管理流量启动，以进行 DNS 和 NTP 服务器通信（这是进行智能软件许可通信所必需的）。

开始之前

- 仅限单一情景模式。
- 不包括 ASA 仅管理接口。
- 不能直接通过 VPN 隧道连接至 ASA 数据接口，也不能直接访问 FXOS。作为 SSH 的一种变通方法，您可以通过 VPN 连接到 ASA，访问 *ASA* CLI，然后使用 **connect fxos** 命令访问 FXOS CLI。请注意，SSH、HTTPS 和 SNMPv3 已经加密/可以加密，因此直接连接到数据接口是安全的。

过程

步骤 1 在 ASDM 中，依次选择**配置 (Configuration)** > **防火墙 (Firewall)** > **高级 (Advanced)** > **FXOS 远程管理 (FXOS Remote Management)**。

步骤 2 启用 FXOS 远程管理。

a) 从导航窗格中选择 **HTTPS**、**SNMP** 或 **SSH**。

b) 点击**添加 (Add)**，并设置要允许管理的**接口 (Interface)**，设置允许连接的 **IP 地址 (IP Address)**，然后点击**确定 (OK)**。
您可以为每个协议类型创建多个条目。如果不想使用以下默认值，请设置**端口 (Port)**：

- HTTPS 默认端口 - 3443
- SNMP 默认端口 - 3061
- SSH 默认端口 - 3022

步骤 3 允许 FXOS 从 ASA 接口启动管理连接。

a) 从导航窗格中选择 **FXOS 流量启动 (FXOS Traffic Initiation)**。

b) 点击**添加 (Add)**，并启用发送 FXOS 管理流量所需的 ASA 接口。默认情况下，外部接口处于启用状态。

步骤 4 点击**应用 (Apply)**。

步骤 5 连接到 Firepower 机箱管理器（默认情况下网址为 https://192.168.45.45，用户名为 **admin**，密码为 **Admin123**）。

步骤 6 点击**平台设置 (Platform Settings)** 选项卡，然后启用 **SSH**、**HTTPS** 或 **SNMP**。
默认情况下，SSH 和 HTTPS 处于启用状态。

步骤 7 将**平台设置 (Platform Settings)** 选项卡上的**访问列表 (Access List)** 配置为允许您的管理地址。默认情况下，SSH 和 HTTPS 只允许管理 1/1 192.168.45.0 网络。您需要允许在 ASA 上的 **FXOS 远程管理 (FXOS Remote Management)** 配置中指定的任何地址。

使用 SSH 连接到 FXOS

您可以使用默认 IP 地址 192.168.45.45 连接到管理 1/1 上的 FXOS。如果配置远程管理（在数据接口上配置对 FXOS 的管理访问，第 12 页），则还可以连接到非标准端口（默认情况下为 3022）上的数据接口 IP 地址。

要使用 SSH 连接到 ASA，必须首先根据 ASA 通用操作配置指南配置 SSH 访问。

您可以从 FXOS 连接到 ASA CLI，反之亦然。

FXOS 最多允许 8 条 SSH 连接。

开始之前

要更改管理 IP 地址，请参阅更改 FXOS 管理 IP 地址或网关，第 15 页。

过程

步骤 1 在连接到管理 1/1 的管理计算机上，将 SSH 连接到管理 IP 地址（默认情况下为 https://192.168.45.45，使用用户名：**admin** 和密码：**Admin123**）。
可以使用任何用户名登录（请参阅添加用户，第 42 页）。如果配置远程管理，则将 SSH 连接到端口 3022 上的 ASA 数据接口 IP 地址（默认端口）。

步骤 2 连接到 ASA CLI。
connect asa

要返回到 FXOS CLI，请输入 **Ctrl+a**, **d**。

示例：

```
firepower-2100# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

步骤 3 如果您将 SSH 连接到 ASA（在 ASA 中配置 SSH 访问后），请连接到 FXOS CLI。
connect fxos

系统会提示您对 FXOS 进行身份验证；使用默认用户名：**admin** 和密码：**Admin123**。要返回到 ASA CLI，请输入 **exit** 或键入 **Ctrl-Shift-6**, **x**。

示例：

```
ciscoasa# connect fxos
Connecting to fxos.
```

```
Connected to fxos. Escape character sequence is 'CTRL-^X'.

FXOS 2.2(2.32) kp2110

kp2110 login: admin
Password: Admin123
Last login: Sat Jan 23 16:20:16 UTC 2017 on pts/1
Successful login attempts for user 'admin' : 4
Cisco Firepower Extensible Operating System (FX-OS) Software

[…]

kp2110#
kp2110# exit
Remote card closed command session. Press any key to continue.
Connection with fxos terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

更改 FXOS 管理 IP 地址或网关

您可以从 FXOS CLI 更改 Firepower 2100 机箱上的管理 IP 地址。默认地址为 192.168.45.45。您还可以更改默认网关。默认网关设置为 0.0.0.0，它将流量发送到 ASA。如果要改为在管理 1/1 网络中使用路由器，则可以更改网关 IP 地址。此外，您还必须更改管理连接的访问列表以匹配新网络。

通常，FXOS 管理 1/1 IP 地址将与 ASA 管理 1/1 IP 地址在同一网络上；请确保也更改 ASA 上的 ASA IP 地址。

开始之前

- 更改管理 IP 地址后，需要使用新地址重新建立所有 Firepower 机箱管理器和 SSH 连接。
- 由于默认情况下在管理 1/1 上启用了 DHCP 服务器，因此在更改管理 IP 地址之前必须禁用 DHCP。

过程

步骤 1 连接到控制台端口（请参阅 ASA 和 FXOS CLI 访问，第 11 页）。我们建议您连接到控制台端口，以避免连接断开。

步骤 2 禁用 DHCP 服务器。

scope system

scope services

disable dhcp-server

commit-buffer

更改管理 IP 地址后，可以使用新客户端 IP 地址重新启用 DHCP。您还可以通过**平台设置 (Platform Settings)** > **DHCP** 在 Firepower 机箱管理器中启用或禁用 DHCP 服务器。

示例：

```
firepower-2100# scope system
firepower-2100 /system # scope services
firepower-2100 /system/services # disable dhcp-server
firepower-2100 /system/services* # commit-buffer
```

步骤 3 配置 IPv4 管理 IP 地址，还可以配置网关（可选）。

a) 设置交换矩阵互联 a 的范围。
scopefabric-interconnecta

示例：

```
firepower-2100# scope fabric-interconnect a
firepower-2100 /fabric-interconnect #
```

b) 查看当前的管理 IP 地址。
show

示例：

```
firepower-2100 /fabric-interconnect # show

Fabric Interconnect:
    ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
 Prefix Operability
   ---- --------------- --------------- --------------- ---------------- ----------------
 ------ -----------
    A    192.168.45.45    0.0.0.0         0.0.0.0          ::               ::
     64     Operable
```

c) 配置新管理 IP 地址，还可以配置新的默认网关（可选）。
setout-of-band staticip *ip_address***netmask** *network_mask***gw** *gateway_ip_address*

要保留当前设置的网关，请省略关键字 **gw**。同样，要在更改网关时保留现有的管理 IP 地址，请省略关键字 **ip** 和 **netmask**。

示例：

```
firepower-2100 /fabric-interconnect # set out-of-band static ip 192.168.4.1 netmask
255.255.255.0
Warning: When committed, this change may disconnect the current CLI session
firepower-2100 /fabric-interconnect* #
```

步骤 4 配置 IPv6 管理 IP 地址和网关。

a) 设置交换矩阵互联 a 的范围，然后设置 IPv6 配置的范围。
scopefabric-interconnecta

scopeipv6-config

示例：

```
firepower-2100# scope fabric-interconnect a
firepower-2100 /fabric-interconnect # scope ipv6-config
```

```
firepower-2100 /fabric-interconnect/ipv6-config #
```

b) 查看当前的管理 IPv6 地址。
show ipv6-if

示例：

```
firepower-2100 /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
    IPv6 Address                       Prefix     IPv6 Gateway
    ---------------------------------- ---------- ------------
    ::                                 ::         ::
```

c) 配置新的管理 IPv6 地址和网关：
Firepower-chassis /fabric-interconnect/ipv6-config # **setout-of-band staticipv6** *ipv6_address***ipv6-prefix** *prefix_length***ipv6-gw** *gateway_address*

要保留当前设置的网关，请省略关键字 **ipv6-gw**。同样，要在更改网关时保留现有的管理 IP 地址，请省略关键字 **ipv6** 和 **ipv6-prefix**。

示例：

```
firepower-2100 /fabric-interconnect/ipv6-config # set out-of-band static ipv6 2001:DB8::34
 ipv6-prefix 64 ipv6-gw 2001:DB8::1
firepower-2100 /fabric-interconnect/ipv6-config* #
```

步骤 5 更改 HTTPS、SSH 和 SNMP 的访问列表，以允许来自新网络的管理连接。
scope system

scope services

IPv4：

enterip-block *ip_address* 前缀 [**http** | **snmp** | **ssh**]

IPv6：

enteripv6-block *ipv6_address* 前缀 [**https** | **snmp** | **ssh**]

对于 IPv4，请输入 **0.0.0.0** 和前缀 **0** 以允许所有网络。对于 IPv6，请输入 **::** 和前缀 **0** 以允许所有网络。还可以通过**平台设置 (Platform Settings)** > **访问列表 (Access List)** 在 Firepower 机箱管理器中添加访问列表。

示例：

```
firepower-2100# scope system
firepower-2100 /system # scope services
firepower-2100 /system/services # enter ip-block 192.168.4.0 24 https
firepower-2100 /system/services/ip-block* # exit
firepower-2100 /system/services* # enter ip-block 192.168.4.0 24 ssh
firepower-2100 /system/services/ip-block* # exit
firepower-2100 /system/services* # enter ip-block 192.168.4.0 24 snmp
firepower-2100 /system/services/ip-block* # exit
firepower-2100 /system/services* # enter ipv6-block 2001:DB8:: 64 https
firepower-2100 /system/services/ip-block* # exit
firepower-2100 /system/services* # enter ipv6-block 2001:DB8:: 64 ssh
firepower-2100 /system/services/ip-block* # exit
firepower-2100 /system/services* # enter ipv6-block 2001:DB8:: 64 snmp
```

```
firepower-2100 /system/services/ip-block* # exit
firepower-2100 /system/services* #
```

步骤 6 （可选） 重新启用 IPv4 DHCP 服务器。

scope system

scope services

enable dhcp-server *start_ip_address end_ip_address*

您还可以通过**平台设置 (Platform Settings)** > **DHCP** 在 Firepower 机箱管理器中启用或禁用 DHCP 服务器。

示例：

```
firepower-2100# scope system
firepower-2100 /system # scope services
firepower-2100 /system/services # enable dhcp-server 192.168.4.10 192.168.4.20
```

步骤 7 保存配置。

commit-buffer

示例：

```
firepower-2100 /system/services* # commit-buffer
```

以下示例配置 IPv4 管理接口和网关：

```
firepower-2100# scope fabric-interconnect a
firepower-2100 /fabric-interconnect # show

Fabric Interconnect:
    ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
 Prefix Operability
    ---- --------------- --------------- --------------- ---------------- ----------------
 ------ -----------
    A    192.168.2.112    192.168.2.1     255.255.255.0   2001:DB8::2     2001:DB8::1
  64     Operable
firepower-2100 /fabric-interconnect # set out-of-band static ip 192.168.2.111 netmask
255.255.255.0 gw 192.168.2.1
Warning: When committed, this change may disconnect the current CLI session
firepower-2100 /fabric-interconnect* # commit-buffer
firepower-2100 /fabric-interconnect #
```

以下示例配置 IPv6 管理接口和网关：

```
firepower-2100# scope fabric-interconnect a
firepower-2100 /fabric-interconnect # scope ipv6-config
firepower-2100 /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
    IPv6 Address                            Prefix     IPv6 Gateway
    --------------------------------------- ---------- ------------
    2001:DB8::2                              64         2001:DB8::1
firepower-2100 /fabric-interconnect/ipv6-config # set out-of-band static ipv6 2001:DB8::2
ipv6-prefix 64 ipv6-gw 2001:DB8::1
firepower-2100 /fabric-interconnect/ipv6-config* # commit-buffer
firepower-2100 /fabric-interconnect/ipv6-config #
```

后续操作

- 要继续配置 ASA，请参阅浏览思科 ASA 系列文档中适合您的软件版本的文档。
- 要配置机箱设置，请参阅 Firepower 机箱管理器设置，第 21 页。

第 2 章

Firepower 机箱管理器设置

Firepower 2100 运行 FXOS 来控制设备的基本操作。您可以使用 GUI Firepower 机箱管理器或 FXOS CLI 来配置这些功能；本文档涵盖了 Firepower 机箱管理器的内容。请注意，所有安全策略和其他操作都是在 ASA OS 中配置的（使用 CLI 或 ASDM）。

概述

在**概述 (Overview)** 选项卡上，您可以轻松监控 Firepower 2100 的状态。**概述 (Overview)** 选项卡提供下列元素：

- 设备信息 (Device Information) - **概述 (Overview)** 选项卡顶部包含下列有关 Firepower 2100 的信息：

  机箱名称 (Chassis name) - 显示分配给机箱的名称。默认情况下，该名称为 **firepower-**型号，例如 firepower-2140。此名称显示在 CLI 提示符中。要更改机箱名称，请使用 FXOS CLI **scope system / set name** 命令。

  IP 地址 (IP address) - 显示分配给机箱的管理 IP 地址。

  型号 (Model) - 显示 Firepower 2100 的型号。

  版本 (Version) - 显示在机箱上运行的 ASA 的版本号。

  运行状态 (Operational State) - 显示机箱的运行状态。

  机箱正常运行时间 (Chassis uptime) - 显示自从系统上次重新启动后经过的时间。

正常运行时间信息 (Uptime Information) 图标 - 将光标悬停在该图标上可以查看机箱和 ASA 安全引擎的正常运行时间。

- 直观状态显示 (Visual Status Display) -“设备信息 (Device Information)”部分下面是机箱的直观展示图，显示机箱中安装的组件，并提供这些组件的常规状态。您可以将光标悬停在“直观状态显示 (Visual Status Display)”中显示的端口上，以获取更多信息，例如接口名称、速度、类型、管理状态和运行状态。
- 详细状态信息 (Detailed Status Information) -“直观状态显示 (Visual Status Display)”下面有一个表，其中包含机箱的详细状态信息。状态信息分为以下部分：“故障 (Faults)”、“接口 (Interfaces)”、“设备 (Devices)”和“资产 (Inventory)”。您可以看到表上面各个部分的摘要，点击您想要查看信息的摘要区域，可以看到每个部分的更多详细信息。

  系统为机箱提供以下详细状态信息：

  故障 (Faults) - 列出系统中发生的故障。故障按严重性排序：“严重 (Critical)”、“主要 (Major)”、“次要 (Minor)”、“警告 (Warning)”和“信息 (Info)”。对于所列的每个故障，可以查看严重性、故障说明、原因、出现次数以及最新出现时间。您还可以查看是否已确认故障。

  点击任何故障，可查看故障的更多详细信息或确认故障。

  注释 在消除了故障根源后，系统会在下个轮询间隔内自动将故障从列表中清除。如果用户正在想办法解决特定故障，他们可以确认故障，以便让其他用户了解当前正在处理故障。

  接口 (Interfaces) - 列出系统中安装的接口，并显示接口名称、运行状态、管理状态、收到的字节数和传输的字节数。

  您可以点击任何接口，查看以图形显示的最近 15 分钟内该接口的输入和输出字节数。

  设备 (Devices) - 显示 ASA，并提供以下详细信息：设备名称、设备状态、应用、运行状态、管理状态、映像版本和管理 IP 地址。

  资产 (Inventory) - 列出机箱中安装的组件，并提供这些组件的相关详细信息，如：**组件**名称、核心数量、安装位置、运行状态、可操作性、容量、功率、温度、序列号、型号、部件号和供应商。

接口

您可以在 FXOS 中管理物理接口。要使用某一接口，必须在 FXOS 中以物理方式启用它，并在 ASA 中以逻辑方式启用它。

Firepower 2100 默认启用巨帧支持。最大 MTU 为 9184。

有关管理接口的信息，请参阅 ASA 和 FXOS 管理，第 2 页。

配置接口

您可以通过物理方式启用和禁用接口，并设置接口速度和双工。要使用某一接口，必须在 FXOS 中以物理方式启用它，并在 ASA 中以逻辑方式启用它。

过程

步骤 1 点击**接口 (Interface)** 选项卡。

步骤 2 要启用或禁用接口，请点击**管理状态 (Admin State)** 滑块。复选标记表示已启用，而 X 则表示已禁用。

注释 管理 1/1 接口在该表中显示为 **MGMT**。

步骤 3 点击要编辑其速度或双工的接口对应的**编辑 (Edit)** 铅笔图标。

注释 您只能启用或禁用管理 1/1 接口；但不能编辑其属性。

步骤 4 选中**启用 (Enable)** 复选框以启用该接口。

步骤 5 从**管理速度 (Admin Speed)** 下拉列表中，选择接口的速度。

步骤 6 点击**自动协商 (Auto Negotiation) 是 (Yes)** 或**否 (No)** 单选按钮。

步骤 7 从**管理双工 (Admin Duplex)** 下拉列表中，选择该接口的双工。

步骤 8 点击**确定 (OK)**。

添加 EtherChannel

EtherChannel（也称为端口通道）最多可以包含 16 个同一类型和速度的成员接口。

注释 EtherChannel 成员端口在 ASA 上可见，但您只能在 FXOS 中配置 EtherChannels 和端口成员身份。

开始之前

Firepower 2100 在活动或开启链路汇聚控制协议 (LACP) 模式下支持 EtherChannel。默认情况下，LACP 模式设置为“活动 (Active)”；您可以在 CLI 中将该模式更改为“开启 (On)”。我们建议将连接交换机端口设置为“活动 (Active)”模式，以实现最佳兼容性。

过程

步骤 1 点击**接口 (Interface)** 选项卡。

步骤 2 点击接口表上方的**添加端口通道 (Add Port Channel)**。

步骤 3 在**端口通道 ID (Port Channel ID)** 字段中，输入端口通道的 ID。有效值介于 1 与 47 之间。

步骤 4 选中**启用 (Enable)** 复选框以启用端口通道。
忽略**类型 (Type)** 下拉列表；唯一可用的类型是**数据 (Data)**。

步骤 5 从**管理速度 (Admin Speed)** 下拉列表中，选择所有成员接口的速度。
如果您选择的接口无法达到所选速度（以及您选择的其他设置），则会自动应用尽可能最快的速度。

步骤 6 为所有成员接口点击**自动协商 (Auto Negotiation) 是 (Yes)** 或**否 (No)** 单选按钮。

步骤 7 在**管理双工 (Admin Duplex)** 下拉列表中，为所有成员接口选择双工。

步骤 8 在**可用接口 (Available Interface)** 列表中，选择您要添加的接口，然后点击**添加接口 (Add Interface)**。
您最多可以添加16个同一类型和速度的接口。添加到通道组的第一个接口确定正确的类型和速度。

提示 一次可添加多个接口。要选择多个独立接口，请点击所需的接口，同时按住 **Ctrl** 键。要选择一个接口范围，请选择范围中的第一个接口，然后，在按住 **Shift** 键的同时，点击选择范围中的最后一个接口。

步骤 9 点击**确定 (OK)**。

监控接口

在**接口 (Interfaces)** 选项卡上，可以查看机箱上已安装的接口的状态。下半部分包含安装在 Firepower 机箱中的接口的表。上面部分显示 Firepower 机箱中安装的接口的直观表示。您可以将鼠标悬停在上半部分中任何接口上方，以获取有关该接口的其他信息。

接口带有色标，表示其当前状态：

- 绿色 - 运行状态为“开启 (Up)”。
- 暗灰色 - 管理状态为“已禁用 (Disabled)”。
- 红色 - 运行状态为“关闭 (Down)”。
- 浅灰色 - 未安装 SFP。

逻辑设备

逻辑设备 (Logical Devices) 页显示有关 ASA 的信息和状态。您还可以使用滑块禁用或重新启用 ASA 以进行故障排除（选中标记表示它已被启用，而 X 则表示它已被禁用）。

ASA 的标题提供了**状态 (Status)**：

- **正常 (ok)** - 逻辑设备配置已完成。
- **未完成配置 (incomplete-configuration)** - 逻辑设备配置未完成。

逻辑设备区域还为 ASA 提供了更详细的**状态 (Status)**：

- **在线 (Online)** - ASA 正在运行和操作。
- **离线 (Offline)** - ASA 已停止且无法操作。
- **正在安装 (Installing)** - 正在进行 ASA 安装。
- **未安装 (Not Installed)** - 未安装 ASA。
- **安装失败 (Install Failed)** - ASA 安装失败。
- **正在启动 (Starting)** - ASA 正在启动。
- **启动失败 (Start Failed)** - ASA 未能启动。
- **已启动 (Started)** - ASA 已成功启动，并且正在等待应用代理心跳。
- **正在停止 (Stopping)** - ASA 正在停止。
- **停止失败 (Stop Failed)** - ASA 无法进入离线状态。
- **没有响应 (Not Responding)** - ASA 没有响应。
- **正在更新 (Updating)** - 正在进行 ASA 软件升级。
- **更新失败 (Update Failed)** - ASA 软件升级失败。
- **更新成功 (Update Succeeded)** - ASA 软件升级成功。

平台设置

平台设置 (Platform Settings) 选项卡允许您为 FXOS 设置基本操作，包括时间和管理访问。

NTP：设置时间

您可以手动设置时钟，或使用 NTP 服务器（推荐）。您最多可以配置 4 个 NTP 服务器。

开始之前

- 默认情况下，NTP 配置为以下思科 NTP 服务器：0.sourcefire.pool.ntp.org、1.sourcefire.pool.ntp.org、2.sourcefire.pool.ntp.org。
- 如果您要将主机名用于 NTP 服务器，则必须配置 DNS 服务器。请参阅 DNS：配置 DNS 服务器，第 37 页。

过程

步骤 1 点击**平台设置 (Platform Settings)** 选项卡，然后点击左侧导航窗格中的 **NTP**。
默认情况下，将选择**时间同步 (Time Synchronization)** 选项卡。

步骤 2 要使用 NTP 服务器：

a) 点击**使用 NTP 服务器 (Use NTP Server)** 单选按钮。

b) 点击**添加 (Add)** 以通过 IP 地址或主机名标识最多四个 NTP 服务器。
如果您要将主机名用于 NTP 服务器，请在完成此程序后配置 DNS 服务器。

步骤 3 要手动设置时间：

a) 点击**手动设置时间 (Set Time Manually)** 单选按钮。

b) 点击**日期 (Date)** 下拉列表，以显示日历，然后使用日历中的可用控件设置日期。

c) 使用对应的下拉列表将时间指定为小时、分钟和 **AM/PM**。

步骤 4 点击**当前时间 (Current Time)** 选项卡，然后从**时区 (Time Zone)** 下拉列表中，为机箱选择适当的时区。

步骤 5 点击**保存 (Save)**。

注释 如果系统时间修改超过 10 分钟，系统会将您注销，稍后，您需要再次登录 Firepower 机箱管理器。

SSH：配置 SSH

以下程序说明如何启用或禁用对 Firepower 机箱的 SSH 访问，以及如何将机箱作为 SSH 客户端启用。默认情况下，SSH 服务器和客户端处于启用状态。

开始之前

过程

步骤 1 依次选择**平台设置 (Platform Settings)** > **SSH** > **SSH 服务器 (SSH Server)**。

步骤 2 要启用 SSH 服务器，以提供对 Firepower 机箱的 SSH 访问，请勾选**启用 SSH (Enable SSH)** 复选框。

步骤 3 对于服务器**加密算法 (Encryption Algorithm)**，请选中每种允许的加密算法对应的复选框。

步骤 4 对于服务器**密钥交换算法 (Key Exchange Algorithm)**，请选中每种允许的 Diffie-Hellman (DH) 密钥交换对应的复选框。
DH 密钥交换提供无法由任何一方单独确定的共享密钥。密钥交换与签名和主机密钥进行组合以提供主机身份验证。此密钥交换方法提供显式服务器身份验证。有关使用 DH 密钥交换方法的详细信息，请参阅 RFC 4253。

步骤 5 对于服务器 **Mac 算法 (Mac Algorithm)**，请选中每种允许的完整性算法的复选框。

步骤 6 对于服务器**主机密钥 (Host Key)**，请为 RSA 密钥对输入模量大小。

模量值（以位为单位）是 8 的倍数，范围介于 1024 至 2048 之间。指定的密钥模量大小越大，生成 RSA 密钥对所需的时间就越长。建议值为 2048。

步骤 7 对于服务器**密钥更新数量限制 (Volume Rekey Limit)**，请设置在 FXOS 断开会话连接之前允许通过该连接的流量（以 KB 为单位）。

步骤 8 对于服务器**密钥更新时间限制 (Time Rekey Limit)**，请设置在 FXOS 断开会话连接之前 SSH 会话可以保持空闲的分钟数。

步骤 9 点击**保存 (Save)**。

步骤 10 点击 **SSH 客户端 (SSH Client)** 选项卡，以自定义 FXOS 机箱 SSH 客户端。

步骤 11 对于**严格主机密钥检查 (Strict Host Keycheck)**，请选择**启用 (enable)**、**禁用 (disable)** 或**提示 (prompt)** 来控制 SSH 主机密钥检查。

- **启用 (enable)** - 如果 FXOS 已知的主机文件中不包括主机密钥，连接将被拒绝。您必须在 FXOS CLI 中使用系统/服务范围的 **enter ssh-host** 命令手动添加主机。
- **提示 (prompt)** - 对于机箱中未存储的主机密钥，系统会提示您接受或拒绝该主机密钥。
- **禁用 (disable)** - （默认）机箱将自动接受以前未存储的主机密钥。

步骤 12 对于客户端**加密算法 (Encryption Algorithm)**，请选中每种允许的加密算法对应的复选框。

步骤 13 对于客户端**密钥交换算法 (Key Exchange Algorithm)**，请选中每种允许的 Diffie-Hellman (DH) 密钥交换对应的复选框。
DH 密钥交换提供无法由任何一方单独确定的共享密钥。密钥交换与签名和主机密钥进行组合以提供主机身份验证。此密钥交换方法提供显式服务器身份验证。有关使用 DH 密钥交换方法的详细信息，请参阅 RFC 4253。

步骤 14 对于客户端 **Mac 算法 (Mac Algorithm)**，请选中每种允许的完整性算法对应的复选框。

步骤 15 对于客户端**密钥更新数量限制 (Volume Rekey Limit)**，请设置在 FXOS 断开会话连接之前允许通过该连接的流量（以 KB 为单位）。

步骤 16 对于客户端**密钥更新时间限制 (Time Rekey Limit)**，请设置在 FXOS 断开会话连接之前 SSH 会话可以保持空闲的分钟数。

步骤 17 点击**保存 (Save)**。

SNMP

使用 **SNMP** 页在 Firepower 机箱上配置简单网络管理协议 (SNMP)。

关于 SNMP

SNMP 是一种应用层协议，提供 SNMP 管理器和代理之间的通信消息格式。SNMP 提供了标准化的框架和通用语言，可用于监控和管理网络中的设备。

SNMP 框架由三个部分组成：

- SNMP 管理器 - 用于通过 SNMP 来控制和监控网络设备的活动的系统。
- SNMP 代理 - Firepower 机箱内的软件组件，用于维护 Firepower 机箱的数据并根据需要向 SNMP 管理器报告数据。Firepower 机箱包含代理和 MIB 集合。
- 管理信息库 (MIB) - SNMP 代理上的受管对象集合。

Firepower 机箱支持 SNMPv1、SNMPv2c 和 SNMPv3。SNMPv1 和 SNMPv2c 都使用基于社区形式的安全性。

SNMP 通知

SNMP 的一个关键功能是能够生成来自 SNMP 代理的通知。这些通知不要求从 SNMP 管理器发送请求。通知可以指示不恰当的用户验证、重新启动、连接断开、到相邻路由器的连接丢失或其他重要事件。

Firepower 机箱将 SNMP 通知生成为陷阱或通知。陷阱不如通知可靠，因为 SNMP 管理器在收到陷阱时不发送任何确认，并且 Firepower 机箱无法确定是否已收到陷阱。收到通告请求的 SNMP 管理器使用一个 SNMP 响应协议数据单元 (PDU) 来确认消息。如果 Firepower 机箱不接收 PDU，则其可以再次发送通知请求。

SNMP 安全级别和权限

SNMPv1、SNMPv2c 和 SNMPv3 分别表示不同的安全模型。安全模型与所选安全级别结合来确定处理 SNMP 消息时应用的安全机制。

安全级别确定查看与 SNMP 陷阱关联的消息时所需的权限。权限级别确定是否需要防范消息泄露或免受身份验证。受支持的安全级别取决于实施的安全模式。SNMP 安全级别支持以下一个或多个权限：

- noAuthNoPriv - 无身份验证或加密
- authNoPriv - 身份验证，但无加密
- authPriv - 身份验证和加密

SNMPv3 同时提供了安全模型和安全级别。安全模型是为用户和用户所处的角色设置的身份验证策略。安全级别是安全模型中允许的安全级别。安全模型和安全级别相结合来确定在处理 SNMP 数据包时采用的安全机制。

支持的 SNMP 安全模型和级别组合

下表确定安全模型和级别的组合含义。

表 *1*：*SNMP* 安全模型和级别

型号	级别	身份验证	加密	状况
v1	noAuthNoPriv	社区字符串	否	使用社区字符串匹配进行身份验证。

型号	级别	身份验证	加密	状况
v2c	noAuthNoPriv	社区字符串	否	使用社区字符串匹配进行身份验证。
V3	noAuthNoPriv	用户名	否	使用用户名匹配进行身份验证。
V3	authNoPriv	HMAC-SHA	否	提供基于 HMAC 安全散列算法 (SHA) 的身份验证。
V3	authPriv	HMAC-SHA	DES	提供基于 HMAC-SHA 算法的身份验证。除基于密码块链 (CBC) DES (DES-56) 标准的身份验证外，还提供数据加密标准 (DES) 56 位加密。

SNMPv3 安全功能

SNMPv3 通过将在网络上对帧进行身份验证和加密相结合来提供对设备的安全接入。SNMPv3 仅按已配置的用户来授权管理操作，并会加密 SNMP 消息。SNMPv3 基于用户的安全模型 (USM) 是指 SNMP 消息级别安全，并提供以下服务：

- 消息完整性 - 确保消息未在未经授权的情况下进行修改或销毁，并且数据序列未修改至超出可以非恶意形式出现的程度。
- 消息来源身份验证 - 确保对用户（系统代表该用户发出此已接收数据）的声明身份进行确认。
- 消息机密性和加密 - 确保不向未经授权的个人、实体或流程提供或披露信息。

SNMP 支持

Firepower 机箱为 SNMP 提供下列支持：

针对 MIB 的支持

Firepower 机箱支持对 MIB 的只读访问。

适用于 SNMPv3 用户的身份验证协议

Firepower 机箱针对 SNMPv3 用户支持 HMAC-SHA-96 (SHA) 身份验证协议。

适用于 SNMPv3 用户的 AES 隐私协议

除了基于SHA的身份验证，Firepower机箱还提供了使用AES-128位高级加密标准的隐私。Firepower机箱使用隐私密码生成128位AES密钥。AES隐私密码至少可具有八个字符。如果口令用明文指定，您可以指定最多80个字符。

配置 SNMP

启用 SNMP，添加陷阱和 SNMPv3 用户。

过程

步骤 1 选择**平台设置 (Platform Settings)** > **SNMP**。

步骤 2 在 **SNMP** 区域中，填写以下字段：

名称	描述
管理状态 (Admin State) 复选框	SNMP 已启用还是已禁用。仅当系统包含与 SNMP 服务器的集成时才启用此服务。
端口 (Port) 字段	Firepower 机箱与 SNMP 主机通信时使用的端口。无法更改默认端口。
社区/用户名 (Community/Username) 字段	Firepower 机箱在它发送给 SNMP 主机的任何陷阱消息中包含的默认 SNMP v1 或 v2 社区名或 SNMP v3 用户名。 输入介于 1 和 32 个字符之间的字母数字字符串。请勿使用 @（at 号）、\（反斜线）、"（双引号）、?（问号）或空格。默认值为 public。 请注意，如果**社区/用户名 (Community/Username)** 字段已设置，空字段右侧会显示文本**已设置：是 (Set: Yes)**。如果**社区/用户名 (Community/Username)** 字段尚未填充值，空字段右侧会显示文本**已设置：否 (Set: No)**。
系统管理员名称 (System Administrator Name) 字段	负责 SNMP 实施的联系人。 输入一个字符串，最多 255 个字符，例如邮件地址或姓名和电话号码。
位置 (Location) 字段	SNMP 代理（服务器）运行所在的主机的位置。 输入一个字母数字字符串，最多 510 个字符。

步骤 3 在 **SNMP 陷阱 (SNMP Traps)** 区域中，点击**添加 (Add)**。

步骤 4 在**添加 SNMP 陷阱 (Add SNMP Trap)** 对话框中，填写以下字段：

名称	描述
主机名 (Host Name) 字段	Firepower机箱应向其发送陷阱的SNMP主机的主机名或IP地址。

名称	描述
社区/用户名 (Community/Username) 字段	向 SNMP 主机发送陷阱时，Firepower 机箱包含的 SNMP v1 或 v2 社区名或 SNMP v3 用户名。这必须与为 SNMP 服务配置的社区或用户名相同。 输入介于 1 和 32 个字符之间的字母数字字符串。请勿使用 @（at 号）、\（反斜线）、"（双引号）、?（问号）或空格。
端口 (Port) 字段	Firepower 机箱与 SNMP 主机通信以布设陷阱时使用的端口。 输入 1 和 65535 之间的整数。
版本 (Version) 字段	用于陷阱的 SNMP 版本和型号。这可以是以下其中一项： • **V1** • **V2** • **V3**
类型 (Type) 字段	如果为版本选择 **V2** 或 **V3**，则是要发送的陷阱类型。这可以是以下其中一项： • **陷阱** • **通知**
v3 权限 (v3 Privilege) 字段	如果为版本选择 **V3**，与陷阱相关联的权限。这可以是以下其中一项： • **身份验证 (Auth)** - 有身份验证，但没有加密 • **无身份验证 (Noauth)** - 没有身份验证和加密 • **权限 (Priv)** - 有身份验证和加密

步骤 5 点击**确定 (OK)**，可关闭**添加 SNMP 陷阱 (Add SNMP Trap)** 对话框。

步骤 6 在 **SNMP 用户 (SNMP Users)** 区域中，点击**添加 (Add)**。

步骤 7 在**添加 SNMP 用户 (Add SNMP User)** 对话框中，填写以下字段：

名称	描述
名称 (Name) 字段	分配给 SNMP 用户的用户名。 输入最多 32 个字母或数字。名称必须以字母开头，您还可以指定 _（下划线）、.（句号）、@（at 号）和 -（连字符）。
授权类型 (Auth Type) 字段	授权类型：**SHA**。

名称	描述
使用 AES-128 (Use AES-128) 复选框	如果选中，该用户将使用 AES-128 加密。
密码 (Password) 字段	该用户的密码：
确认密码 (Confirm Password) 字段	用于确认目的的再次输入的密码。
隐私密码 (Privacy Password) 字段	该用户的隐私密码。
确认隐私密码 (Confirm Privacy Password) 字段	用于确认目的的再次输入的隐私密码。

步骤 8 点击**确定 (OK)**，可关闭**添加 SNMP 用户 (Add SNMP User)** 对话框。

步骤 9 点击**保存 (Save)**。

HTTPS：更改端口

默认情况下，在端口 443 上启用 HTTPS 服务。您无法禁用 HTTPS，但可以更改端口，将其用于 HTTPS 连接。

开始之前

如果在 ASA 数据接口上启用 HTTPS 访问，则不要从 443 更改 HTTPS 端口；仅支持默认端口。

过程

步骤 1 依次选择**平台设置 (Platform Settings)** > **HTTPS**。

步骤 2 在**端口 (Port)** 字段中输入要用于 HTTPS 连接的端口。指定一个介于 1 和 65535 之间的整数。默认情况下，在端口 443 上启用此服务。

步骤 3 点击**保存 (Save)**。
使用指定的 HTTPS 端口配置 Firepower 机箱。

更改 HTTPS 端口后，所有当前 HTTPS 会话都将关闭。用户需要使用新端口重新登录 Firepower 机箱管理器，如下所示：

https://<*chassis_mgmt_ip_address*>:<*chassis_mgmt_port*>

其中 <*chassis_mgmt_ip_address*> 是您在初始配置期间输入的 Firepower 机箱的 IP 地址或主机名，<*chassis_mgmt_port*> 是您刚刚配置的 HTTPS 端口。

DHCP：为管理客户端配置 DHCP 服务器

您可以为连接到管理 1/1 接口的客户端启用 DHCP 服务器。默认情况下，使用以下地址范围启用服务器：192.168.45.10-192.168.45.12。如果要更改管理 IP 地址，则必须禁用 DHCP（请参阅更改 FXOS 管理 IP 地址或网关，第 15 页）。然后，您可以为新网络重新启用 DHCP。

过程

步骤 1 依次选择**平台设置 (Platform Settings)** > **DHCP**。

步骤 2 选中**启用 DNS 服务 (Enable DHCP service)** 复选框。

步骤 3 输入**起始 IP (Start IP)** 和**结束 IP (End IP)** 地址。

步骤 4 点击**保存 (Save)**。

系统日志：配置系统日志消息传送

系统日志记录是将来自设备的消息收集到运行系统日志守护程序的服务器的一种方法。将信息记录到中央系统日志服务器有助于汇聚日志和提醒。日志对常规故障排除及事件处理均有帮助。

这些系统日志消息仅适用于 FXOS 机箱。对于 ASA 系统日志消息，必须在 ASA 配置中配置日志记录。

过程

步骤 1 依次选择**平台设置 (Platform Settings)** > **系统日志 (Syslog)**。

步骤 2 配置本地目标：

a) 点击**本地目标 (Local Destinations)** 选项卡。

b) 填写以下字段：

名称	描述
控制台 (Console)	
管理状态 (Admin State)	勾选**启用 (Enable)** 复选框可在控制台上显示系统日志消息。

名称	描述
级别 (Level)	点击要在控制台上显示的最低消息级别。Firepower 机箱将显示该级别及以上级别的消息。 • **紧急 (Emergencies)** • **警报 (Alerts)** • **严重 (Critical)**
平台 (Platform)	
管理状态 (Admin State)	平台系统日志始终处于启用状态。
级别 (Level)	选择要显示的最低消息级别。Firepower 机箱将显示该级别及以上级别的消息。默认值为**信息 (Informational)**。 • **紧急 (Emergencies)** • **警报 (Alerts)** • **严重 (Critical)** • **错误 (Error)** • **警告 (Warnings)** • **通知 (Notifications)** • **信息 (Information)** • **调试 (Debugging)**
文件 (File)	
管理状态 (Admin State)	勾选**启用 (Enable)** 复选框可将系统日志消息保存到文件中。

名称	描述
级别 (Level)	选择要保存的最低消息级别。系统将保存该级别及以上级别的消息。 • **紧急 (Emergencies)** • **警报 (Alerts)** • **严重 (Critical)** • **错误 (Error)** • **警告 (Warnings)** • **通知 (Notifications)** • **信息 (Information)** • **调试 (Debugging)**
名称 (Name)	设置文件的名称，最多 16 个字符。
大小 (Size)	在系统开始用最新消息覆写最旧消息之前，请指定最大文件大小（以字节为单位）。范围为 4096 到 4194304 字节。

c) 点击**保存 (Save)**。

步骤 3 配置远程目标：

a) 点击**远程目标 (Remote Destinations)** 选项卡。

b) 在**远程目标 (Remote Destinations)** 选项卡上，为最多三个外部日志填写下列字段，这些日志可以存储 Firepower 机箱生成的消息：
通过将系统日志消息发送到远程目标，您可以根据外部系统日志服务器上的可用磁盘空间存档消息，并在保存日志记录数据后对其进行处理。例如，可以指定在记录特定类型的系统日志消息后要执行的操作，从日志提取数据并将记录保存到其他文件以进行报告，或者使用特定于站点的脚本跟踪统计信息。

名称	描述
管理状态 (Admin State)	勾选**启用 (Enable)** 复选框可将系统日志消息存储在远程日志文件中。

名称	描述
级别 (Level)	选择您想让系统存储的最低消息级别。系统在远程文件中存储此级别及以上消息。 • **紧急 (Emergencies)** • **警报 (Alerts)** • **严重 (Critical)** • **错误 (Error)** • **警告 (Warnings)** • **通知 (Notifications)** • **信息 (Information)** • **调试 (Debugging)**
主机名/IP 地址 (Hostname/IP Address)	为系统日志服务器设置主机名或 IP 地址。 注释 如果使用主机名而不使用 IP 地址，必须配置 DNS 服务器。
设施 (Facility)	为系统日志服务器选择要用作文件消息基础的系统日志设备。 • **Local0** • **Local1** • **Local2** • **Local3** • **Local4** • **Local5** • **Local6** • **Local7**

c) 点击**保存 (Save)**。

步骤 4 配置本地来源：

a) 点击**本地源 (Local Sources)** 选项卡。

b) 填写以下字段：

名称	描述
故障管理状态 (Faults Admin State)	是否启用系统故障日志记录。如果选中**启用 (Enable)** 复选框，Firepower 机箱将记录所有系统故障。

名称	描述
审核管理状态 (Audits Admin State)	是否启用审核日志记录。如果选中**启用 (Enable)** 复选框，Firepower 机箱将记录所有审核日志事件。
事件管理状态 (Events Admin State)	是否启用系统事件日志记录。如果选中 **启用 (Enable)** 复选框，Firepower 机箱将记录所有系统事件。

c) 点击**保存 (Save)**。

DNS：配置 DNS 服务器

如果系统要求将主机名解析为 IP 地址，则您需要指定 DNS 服务器。您最多可以配置 4 个 DNS 服务器。配置多个 DNS 服务器时，系统仅以任意随机顺序搜索服务器。

开始之前

- 默认情况下，DNS 配置为以下 OpenDNS 服务器：208.67.222.222、208.67.220.220。

过程

步骤 1 依次选择**平台设置 (Platform Settings)** > **DNS**。

步骤 2 选中**启用 DNS 服务器 (Enable DNS Server)** 复选框。

步骤 3 对于要添加的每个 DNS 服务器（最多四个），请在 **DNS 服务器 (DNS Server)** 字段中输入 DNS 服务器的 IP 地址，然后点击**添加 (Add)**。

步骤 4 点击**保存 (Save)**。

步骤 5 点击**域名配置 (Domain Name Configuration)** 选项卡，输入要将 Firepower 机箱作为后缀附加到非限定名称的**域名 (Domain name)**，然后点击**添加 (Add)**。
例如，如果您将域名设置为“example.com”并通过不受限定的名称“jupiter”来指定系统日志服务器，则 Firepower 机箱会将名称限定为“jupiter.example.com”。

FIPS 和通用标准：启用 FIPS 和通用标准模式

执行以下步骤可在 Firepower 2100 上启用 FIPS 或“通用标准 (CC) ”模式。

您还必须使用 **fips enable** 命令在 ASA 上单独启用 FIPS 模式。在 ASA 上没有用于通用标准模式的单独设置；对 CC 或 UCAPL 法规合规性的任何其他限制都必须按照思科安全策略文档进行配置。

我们建议您首先在 ASA 上设置 FIPS 模式，等待设备重新加载，然后在 FXOS 中设置 FIPS 模式。

过程

步骤 1 依次选择**平台设置 (Platform Settings)** > **FIPS 和通用标准 (FIPS and Common Criteria)**。

步骤 2 通过选中**启用 (Enable)** 复选框启用 **FIPS**。

步骤 3 通过选中**启用 (Enable)** 复选框启用**通用标准 (Common Criteria)**。
在启用“通用标准 (Common Criteria)”后，默认情况下将启用 **FIPS 启用 (FIPS Enable)** 复选框。

步骤 4 点击**保存 (Save)**。

步骤 5 按照提示重新启动系统。

访问列表：配置管理访问

默认情况下，Firepower 2100 允许对 Firepower 机箱管理器进行 HTTPS 访问，和在管理 1/1 192.168.45.0/24 网络上进行 SSH 访问。如果您要允许从其他网络进行访问，或者允许 SNMP，则必须添加或更改访问列表。

对于每个 IP 地址块（v4 或 v6），最多可为每项服务配置 25 个不同子网。

过程

步骤 1 依次选择**平台设置 (Platform Settings)** > **访问列表 (Access List)**。

步骤 2 在 **IPv4 访问列表 (IPv4 Access List)** 区域中：

a) 点击**添加 (Add)**。

b) 输入以下字段的值：

- **IP 地址 (IP Address)** - 设置 IP 地址。输入 **0.0.0.0** 以允许所有网络。
- **前缀长度 (Prefix Length)** - 设置子网掩码。输入 **0** 以允许所有网络。
- **协议 (Protocol)** - 选择 **HTTPS**、**SNMP** 或 **SSH**。

c) 点击**确定 (OK)**。

d) 重复这些步骤为每项服务添加其他网络。

步骤 3 在 **IPv6 访问列表 (IPv6 Access List)** 区域中：

a) 点击**添加 (Add)**。

b) 输入以下字段的值：

- **IP 地址 (IP Address)** - 设置 IP 地址。输入 :: 以允许所有网络。
- **前缀长度 (Prefix Length)** - 设置前缀长度。输入 **0** 以允许所有网络。

- **协议 (Protocol)** - 选择 **HTTPS**、**SNMP** 或 **SSH**。

c) 点击**确定 (OK)**。

d) 重复这些步骤为每项服务添加其他网络。

步骤 4 点击**保存 (Save)**。

系统更新

此任务适用于独立 ASA。如果要升级故障切换对，请参阅思科 ASA 升级指南。升级过程通常需要 20 到 30 分钟。

ASA、ASDM 和 FXOS 映像被捆绑成一个单一的包。包更新由 FXOS 管理；不能在 ASA 操作系统中升级 ASA。不能单独升级 ASA 和 FXOS；它们始终捆绑在一起。

不过 ASDM 是个例外，此时您可以从 ASA 操作系统中升级，因此无需只使用捆绑的 ASDM 映像。手动上传的 ASDM 映像不会出现在 FXOS 映像列表中；您必须从 ASA 管理 ASDM 映像。

注释 在升级捆绑包时，捆绑包中的 ASDM 映像将替换以前的 ASDM 捆绑包映像，因为它们具有相同的名称 (**asdm.bin**)。但是，如果您手动选择了您上传的其他 ASDM 映像（例如，**asdm-782.bin**），那么即使捆绑包升级之后，您仍可继续使用该映像。为了确保您运行的是兼容版本的 ASDM，您应该在升级捆绑包之前先升级 ASDM，或者应该在升级 ASA 捆绑包之前，或将 ASA 重新配置为使用捆绑的 ASDM 映像 (**asdm.bin**)。

开始之前

确保您要上传的映像在本地计算机上可用。

过程

步骤 1 依次选择**系统 (System)** > **更新 (Updates)**。
可用更新 (Available Updates) 页面将显示机箱上可用的包的列表。

步骤 2 点击**上传映像 (Upload Image)**。

步骤 3 点击**浏览 (Browse)**，可导航到并选择想要上传的映像。

步骤 4 点击**上传 (Upload)**。
所选映像将上传到机箱。新映像添加至机箱后，系统将自动验证映像的完整性。如果要手动验证其完整性，请点击**验证 (Verify)**（勾选标记图标）。

步骤 5 选择要升级到的 ASA 包，然后点击**升级 (Upgrade)**。

步骤 6 点击**是 (Yes)**，确认您想要继续安装，或者点击**否 (No)** 取消安装。
升级过程中，系统会将您从 Firepower 机箱管理器注销。

用户管理

用户帐户用于访问 Firepower 2100 机箱。这些帐户用于 Firepower 机箱管理器和 SSH 访问。ASA 拥有单独的用户帐户和身份验证。

关于用户帐户

您最多可配置 48 个本地用户帐户。每个用户帐户必须具有唯一的用户名和密码。

帐户类型

管理员帐户

管理员帐户是默认用户帐户，并且无法修改或删除。此帐户是系统管理员或超级用户帐户并具有完整权限。默认密码为 **Admin123**。

管理员帐户始终处于活动状态，并且不会到期。无法将管理员帐户配置为非活动状态。

本地身份验证的用户帐户

本地身份验证用户帐户直接通过机箱进行身份验证，并且可以由具有管理员权限的任何用户来启用或禁用。一旦本地用户帐户被禁用，该用户将无法登录。已禁用本地用户帐户的详细配置信息不会被数据库删除。如果重新启用已禁用的本地用户帐户，此帐户将再次处于活动状态，且采用现有配置（包括用户名和密码）。

用户角色

系统包含以下用户角色：

管理员

完成对整个系统的读写访问。默认情况下，为默认管理员帐户分配此角色，不能更改。

只读

对系统配置的只读权限，无权修改系统状态。

用户帐户的到期

您可以配置用户帐户在预定时间过期。当到达到期时间时，系统将会禁用用户帐户。

默认情况下，用户帐户不会到期。

在为用户帐户配置过期日期后，无法将帐户重新配置为不过期。然而，您可以为帐户配置可用的最新过期日期。

用户帐户的准则

用户名

用户名用作 Firepower 机箱管理器和 FXOS CLI 的登录 ID。将登录 ID 分配到用户帐户时，请考虑以下准则和限制：

- 登录 ID 可以包含 1 到 32 个字符，包括以下字符：

  任意字母字符

  任意数字

  _（下划线）

  -（短划线）

  .（点）

- 登录 ID 必须唯一。
- 登录 ID 必须以字母字符开头。它不能以数字或特殊字符开头，例如下划线。
- 登录 ID 区分大小写。
- 不能创建全数字登录 ID。
- 创建用户帐户后，不能更改登录 ID。必须删除该用户帐户，创建新的用户帐户。

密码

密码对于每个本地认证的用户帐户都是必需的。具有管理员或AAA权限的用户可以配置系统，以对用户密码执行密码强度检查。如果密码强度检查已启用，则每个用户必须使用强密码。

建议每个用户都使用强密码。如果对本地身份验证的用户启用密码强度检查，则 FXOS 将拒绝不符合以下要求的任何密码：

- 必须包含最少 8 个字符，最多 80 个字符。

注释 您可以选择在系统上配置 15 个字符（最小密码长度）的密码，以符合通用标准需求。有关详细信息，请参阅配置用户设置，第 43 页。

- 必须包含至少一个大写字母字符。
- 必须包含至少一个小写字母字符。
- 必须包含至少一个非字母数字（特殊）字符。

- 不能包含连续重复 3 次的字符，例如 aaabbb。
- 不得包含三个以任何顺序排列的连续数字或字母，例如 passwordABC 或 password321。
- 不能与用户名相同，或与用户名正好相反。
- 必须通过密码词典检查。例如，密码不可以是标准词典单词。
- 不能包含以下符号：$（美元符号）、?（问号）和 =（等号）。
- 本地用户和管理员帐户的密码不得为空。

添加用户

为 Firepower 机箱管理器和 FXOS CLI 访问添加本地用户。

过程

步骤 1 依次选择**系统 (System)** > **用户管理 (User Management)**。

步骤 2 点击**本地用户 (Local Users)** 选项卡。

步骤 3 点击**添加用户 (Add User)**，可打开**添加用户 (Add User)** 对话框。

步骤 4 使用关于用户的必填信息，填写下列字段：

名称	描述
用户名 (User Name) 字段	登录此帐户时使用的帐户名称。此名称必须唯一，并满足用户帐户名称的准则和限制（请参阅用户帐户的准则，第 41 页）。 保存用户后，不能更改登录 ID。必须删除该用户帐户，创建新的用户帐户。
名字 (First Name) 字段	用户的名字。该字段最多包含 32 个字符。
姓氏 (Last Name) 字段	用户的姓氏。该字段最多包含 32 个字符。
邮件 (Email) 字段	用户的邮件地址。
电话号码 (Phone Number) 字段	用户的电话号码。
密码 (Password) 字段	与此帐户关联的密码。如果启用了密码强度检查，则用户的密码必须为强密码，FXOS 会拒绝任何不满足强度检查要求的密码（请参阅用户帐户的准则，第 41 页）。
确认密码 (Confirm Password) 字段	第二次用于确认目的的密码。

名称	描述
帐户状态 (Account Status) 字段	如果状态设置为**活动 (Active)**，用户可以登录使用此登录 ID 和密码登录 Firepower 机箱管理器和 FXOS CLI。
用户角色 (User Role) 列表	代表要分配给用户帐户的权限的角色（请参阅用户角色，第 40 页）。 所有用户均默认分配了“只读 (Read-Only)”角色，并且此角色无法取消选择。要分配多个角色，请按住 Ctrl 键并点击所需角色。 **注释** 用户角色和权限的更改在用户下一次登录之后才会生效。如果在向用户帐户分配新角色或从中删除现有角色时用户已登录，则活动会话将继续使用上一个角色和权限。
帐户到期 (Account Expires) 复选框	如果选中，在**到期日期 (Expiration Date)** 字段中指定的日期过后，此帐户将到期且无法使用。 **注释** 在为用户帐户配置过期日期后，无法将帐户重新配置为不过期。然而，您可以为帐户配置可用的最新过期日期。
到期日期 (Expiry Date) 字段	帐户到期日期。日期格式应为 yyyy-mm-dd。 点击此字段末尾的日历图标，查看您可以用来选择到期日期的日历。

步骤 5 点击**添加 (Add)**。

步骤 6 要停用某一用户，请执行以下操作：

a) 对于要停用的用户，请点击**编辑 (Edit)**（**铅笔图标**）
管理员用户帐户始终设置为活动。不能修改。

b) 点击**帐户状态 (Account Status)** 字段中的**非活动状态 (Inactive)** 单选按钮。

c) 点击**保存 (Save)**。

配置用户设置

您可以为所有用户配置全局设置。

过程

步骤 1 依次选择**系统 (System)** > **用户管理 (User Management)**。

步骤 2 点击**设置** (Settings) 选项卡。

步骤 3 使用必填信息填写下列字段：

名称	描述
默认身份验证 (Default Authentication) 字段	在远程登录期间，对用户进行身份验证的默认方式。这可以是以下其中一项： • **本地 (Local)** - 必须在 Firepower 机箱本地定义用户帐户。 • **无 (None)** - 如果用户帐户是 Firepower 机箱的本地帐户，当用户在远程登录时，不需要密码。
本地用户设置 (Local User Settings)	
密码强度检查 (Password Strength Check) 复选框	如果选中，所有本地用户密码都必须符合强密码准则（请参阅用户帐户的准则，第 41 页）。
历史记录计数 (History Count) 字段	用户在重新使用先前使用的密码之前必须创建的唯一密码的数量。历史记录计数的顺序与时间顺序正好相反，最近的密码在前，这样可确保当达到历史记录计数阈值后仅重复使用最旧的密码。 该值可以是从 0 至 15 的任意值。 您可以将**历史记录计数 (History Count)** 字段设置为 0，这表示禁用历史记录计数，使用户随时都能够重复使用之前已使用的密码。
间隔期间更改 (Change During Interval) 字段	控制本地验证用户何时能够更改其密码。该字段可以是： • **启用 (Enable)** - 本地身份验证用户可以根据“更改间隔 (Change Interval)”和“更改计数 (Change Count)”设置更改其密码。 • **禁用 (Disable)** - 本地身份验证用户不能在为“无更改间隔 (No Change Interval)”指定的期限内更改其密码。
更改间隔 (Change Interval) 字段	在其期间执行在**更改计数 (Change Count)** 字段中指定的密码更改次数的小时数。 该值可以是 1 至 745（小时）的任意值。 例如，如果该字段设置为 48，**更改计数 (Change Count)** 字段设置为 2，那么本地身份验证用户在 48 小时内执行的密码更改不能超过 2 次。
更改计数 (Change Count) 字段	本地身份验证用户能够在“更改间隔 (Change Interval)”内更改其密码的最大次数。 该值可以是从 0 到 10 的任意值。

名称	描述
无更改间隔 (No Change Interval) 字段	本地身份验证用户在更改新建密码之前必须等待的最少小时数。 该值可以是 1 至 745（小时）的任意值。 如果未将**间隔期间更改 (Change During Interval)** 属性设置为**禁用 (Disable)**，该时间间隔将被忽略。

步骤 4 点击**保存 (Save)**。