Firepower 4100 机箱初始配置

本章对您适用吗？

本章介绍如何执行 Cisco Firepower 4100 机箱的初始设置，包括配置与 ASA 和 威胁防御 逻辑设备配合使用的接口。

本指南适用对象

本指南介绍了如何设置 Firepower 4100 机箱，使其与 ASA 和/或 威胁防御 应用程序配合使用。本指南介绍以下部署：

- 使用管理中心的独立威胁防御，用作本地或容器实例（多实例功能）
- 使用设备管理器的独立威胁防御

注释 设备管理器 不支持多实例。

- 使用CDO的独立威胁防御

注释 CDO 不支持多实例。

- 使用 ASDM 的独立式 ASA

本指南不包含以下部署，请参考 FXOS、ASA、FDM、CDO 和 FMC 配置指南了解相关内容：

- 高可用性/故障转移
- 集群（ASA，或仅使用 管理中心 的 威胁防御）
- 多实例（仅使用 管理中心 的 威胁防御）
- Radware DefensePro 修饰器应用程序
- CLI 配置（仅限 ASA 或 FXOS）

本指南还将指导您完成基本安全策略的配置；如果您有更高级的要求，请参阅配置指南。

关于 Firepower 4100 机箱

Firepower 4100 机箱是面向网络和内容安全解决方案的下一代平台。Firepower 4100 包括一个管理引擎和一个安全引擎，您可以在其中安装逻辑设备。还能安装多个高性能网络模块。

逻辑设备如何与以下产品一起使用： Firepower 4100/9300

Firepower 4100/9300 在名为 Firepower 可扩展操作系统 (FXOS) 的管理引擎上运行其操作系统。即用型 机箱管理器 提供简单的基于 GUI 的管理功能。您可以使用 机箱管理器在管理引擎上配置硬件接口设置、智能许可（适用于 ASA）和其他基本运行参数。要使用 FXOS CLI，请参阅 FXOS CLI 配置指南。

逻辑设备允许您运行一个应用实例和一个可选的修饰器应用以形成服务链。部署逻辑设备时，管理引擎将下载您选择的应用映像，并创建默认配置。然后，您可以在应用操作系统中配置安全策略。

逻辑设备不能彼此形成服务链，也不能通过背板彼此通信。所有流量必须在一个接口上退出机箱，并在另一个接口上返回以到达另一个逻辑设备。对于容器实例，可以共享数据接口；只有在这种情况下，多个逻辑设备才能通过背板进行通信。

支持的应用

您可以使用以下应用类型在机箱上部署逻辑设备。

威胁防御

威胁防御 提供各种下一代防火墙服务，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，以及恶意软件防护。

您可以使用以下管理器之一

- 管理中心- 位于单独服务器上的功能齐全的多设备管理器。
- 设备管理器 - 设备上的单设备管理器。
- CDO - 基于云的多设备管理器。

ASA

ASA 在一台设备中提供高级状态防火墙和 VPN 集中器功能。您可以使用以下任一管理器管理 ASA：

- ASDM - 设备上的单设备管理器。本指南介绍使用 *ASDM* 管理 *ASA* 的方法。
- CLI
- CDO - 基于云的多设备管理器。
- CSM - 位于单独服务器上的多设备管理器。

Radware DefensePro （修饰器）

您可以安装 Radware DefensePro (vDP) 以在 ASA 前面运行，或者安装 威胁防御 作为修饰器应用程序。vDP 是基于 KVM 的虚拟平台，可在 Firepower 4100/9300 上提供分布式拒绝服务 (DDoS) 检测和缓解功能。来自网络的流量必须先经过 vDP，然后才能到达 ASA 或 威胁防御。

要部署 vDP，请参阅 FXOS 配置指南。

逻辑设备应用程序实例：容器或本地

逻辑设备应用程序实例在以下部署类型中运行：

- 本地实例 - 本地实例使用安全引擎的所有资源（CPU、RAM 和磁盘空间），因此仅可安装一个本地实例。
- 容器实例 - 容器实例使用安全引擎的部分资源，因此可以安装多个容器实例。**注意**：仅 威胁防御支持多实例功能；ASA 不支持，且其不能与vDP搭配使用。

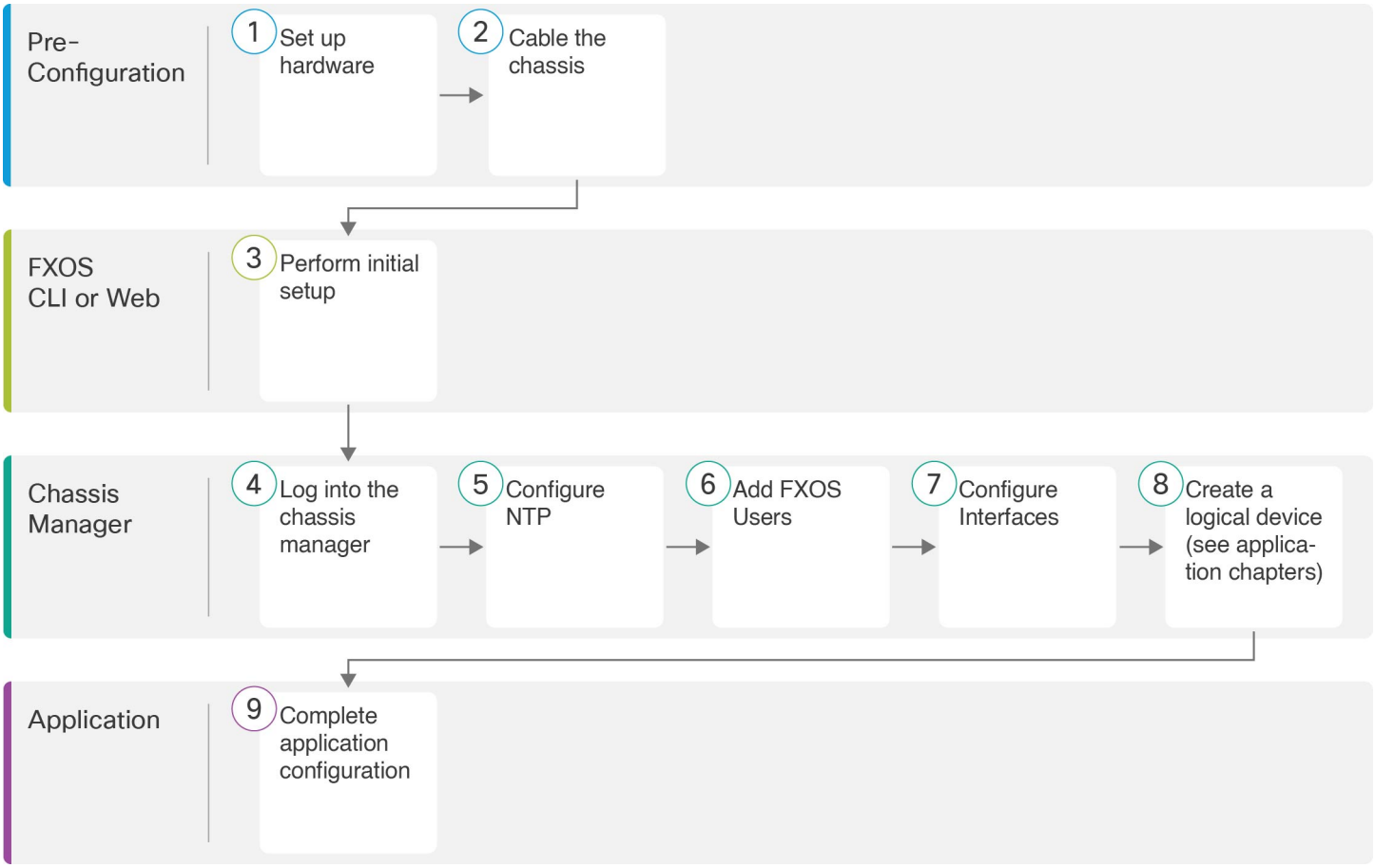
每个型号的最大容器实例数

- Firepower 4110-3
- Firepower 4112-3
- Firepower 4115-7
- Firepower 4120-3
- Firepower 4125-10
- Firepower 4140-7
- Firepower 4145—14

- Firepower 4150-7

端到端程序

请参阅以下任务以设置 Firepower 4100 机箱并在您的机箱上部署逻辑设备。



1	配置前准备工作	设置 Firepower 4100 硬件。请参阅 Firepower 4100 硬件指南。
2	配置前准备工作	连接机箱电缆， 第 5 页。
3	FXOS CLI 或 Web	执行初始机箱设置， 第 8 页。
4	机箱管理器	登录机箱管理器， 第 12 页。
5	机箱管理器	配置 NTP， 第 13 页。

6	机箱管理器	添加 FXOS 用户，第 15 页。
7	机箱管理器	配置接口，第 16 页。
8	机箱管理器	创建逻辑设备： • 具有 管理中心 的 威胁防御 — 请参阅使用管理中心部署威胁防御。 • 具有 设备管理器 的 威胁防御 — 请参阅使用设备管理器部署威胁防御。 • 具有 CDO 的 威胁防御 — 请参阅 使用 CDO 部署威胁防御。 • ASA - 请参阅使用 ASDM 部署 ASA。 注释 FXOS 2.7.1/威胁防御6.5 中，添加了对搭配使用 威胁防御 与 设备管理器 的支持
9	应用	完成应用配置： • 具有 管理中心 的 威胁防御 — 请参阅使用管理中心部署威胁防御。 • 具有 设备管理器 的 威胁防御 — 请参阅使用设备管理器部署威胁防御。 • 具有 CDO 的 威胁防御 — 请参阅 使用 CDO 部署威胁防御。 • ASA - 请参阅使用 ASDM 部署 ASA。

连接机箱电缆

连接以下接口以执行机箱初始设置、持续监控以及使用逻辑设备。

- 控制台端口 -（可选）如果不在机箱管理端口上执行初始设置，请将管理计算机连接到控制台端口以执行机箱的初始设置。Firepower 4100 随附 RS-232 转 RJ-45 串行控制台电缆。可能需要使用第三方串口转 USB 电缆建立连接。
- 机箱管理端口 - 将机箱管理端口连接至您的管理网络，以进行配置和持续的机箱管理。如果从 DHCP 服务器收到 IP 地址，可以在此端口上执行初始设置。
- 逻辑设备管理接口 - 使用一个或多个接口管理逻辑设备。本指南假设您有单独的管理网络，并且有自己的互联网接入。您可以选择机箱上除预留给 FXOS 管理的机箱管理端口以外的任何接口用于此目的。可以在逻辑设备之间共享管理接口，也可以按照逻辑设备使用单独的接口，以获取多实例支持。通常，您与所有逻辑设备共享一个管理接口，或者如果您使用单独的接口，请将其置于单一管理网络中。但是确切的网络要求可能有所不同。对于 威胁防御，管理接口是不同于数据接口的独立接口，具有自己的网络设置。在 6.7 和更高版本中，您可以选择为管理访问配置数据接口，而不使用管理接口。在这种情况下，您仍必须出于内部架构原因为逻辑设

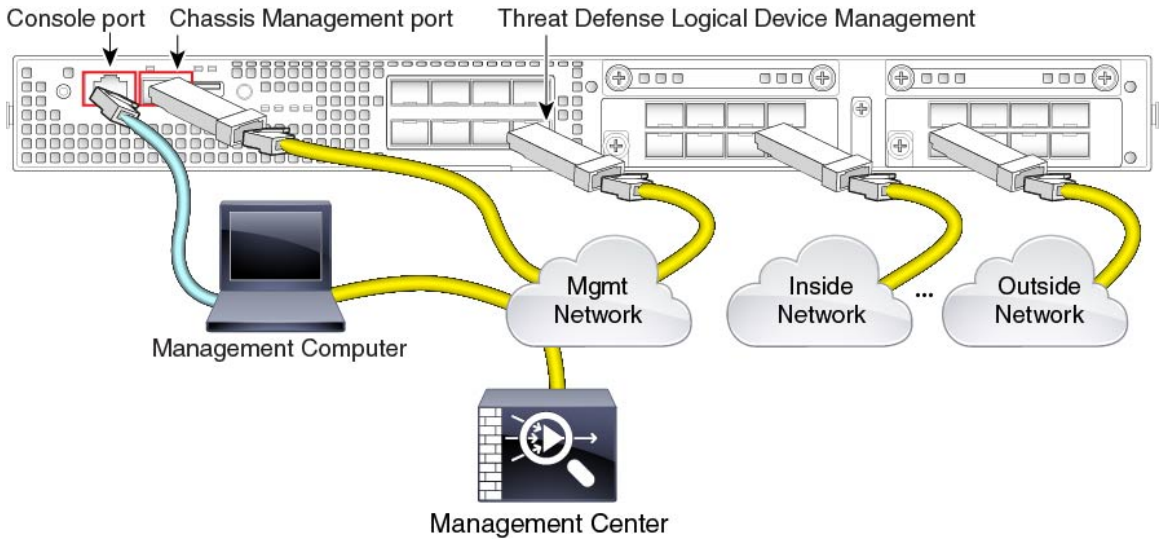
备分配管理接口，但无需用电缆连接它。请注意，对于 管理中心，在高可用性或集群部署中，不支持从数据接口进行管理器访问。有关详细信息，请参阅FTD 命令参考中的**configure network management-data-interface** 命令。

- 数据接口 - 将数据接口连接至您的逻辑设备数据网络。可以配置物理接口、Etherchannel、VLAN 子接口（仅适用于容器实例）和分支端口，以划分高容量接口。可以根据网络要求将多个设备连接至相同网络或不同网络，以获取多实例支持。对于容器实例，可以共享数据接口；只有在这种情况下，多个逻辑设备才能通过背板进行通信。否则，所有流量必须在一个接口上退出机箱，并在另一个接口上返回以到达另一个逻辑设备。有关共享接口限制和指导原则的详细信息，请参阅 FXOS 配置指南。

注释 除控制台端口之外的所有接口均需要 SFP/SFP+/QSFP 收发器。请参阅受支持收发器的硬件安装指南。

注释 虽然本指南中没有涉及到，但对于高可用性，请将数据接口用于故障转移/状态链路。对于机箱间集群，请将机箱上定义的 EtherChannel 用作集群类型接口。

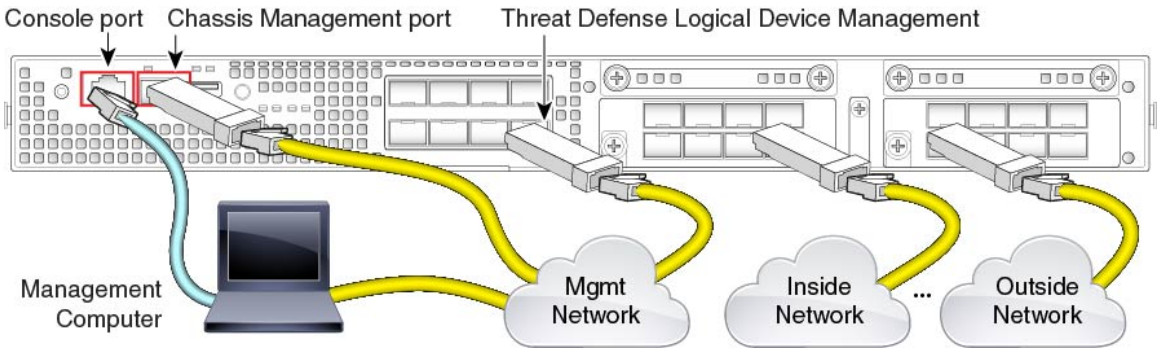
带有 管理中心 的 威胁防御 布线



本指南假设您有单独的管理网络，并且有自己的互联网接入。默认情况下，管理接口在部署时已预配置，但稍后还必须配置数据接口。

将 管理中心 置于逻辑设备管理网络，或者从逻辑设备管理网络进行访问。威胁防御 和 管理中心 必须通过管理网络访问互联网，才能进行更新和许可。在 6.7 和更高版本中，可以选择为 管理中心 管理配置数据接口，而非管理接口。请注意，在高可用性或集群部署中，不支持从数据接口进行 管理中心 访问。有关为 管理中心 访问配置数据接口的详细信息，请参阅 FTD 命令参考中的 **configure network management-data-interface** 命令。

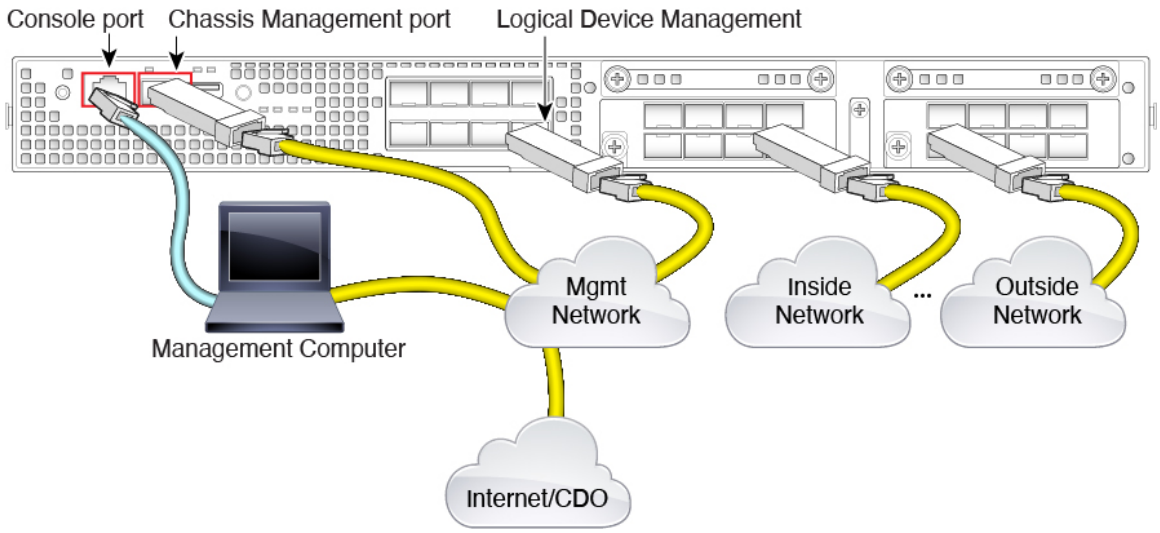
带有 设备管理器 的 威胁防御 布线



本指南假设您有单独的管理网络，并且有自己的互联网接入。默认情况下，管理接口在部署时已预配置，但稍后还必须配置数据接口。

在逻辑设备管理接口上执行初始威胁防御配置。威胁防御需连接互联网才可访问许可、更新和CDO管理，且默认行为是将管理流量路由至部署 威胁防御 时指定的网关 IP 地址。您可以稍后从任何数据接口启用 设备管理器 管理。

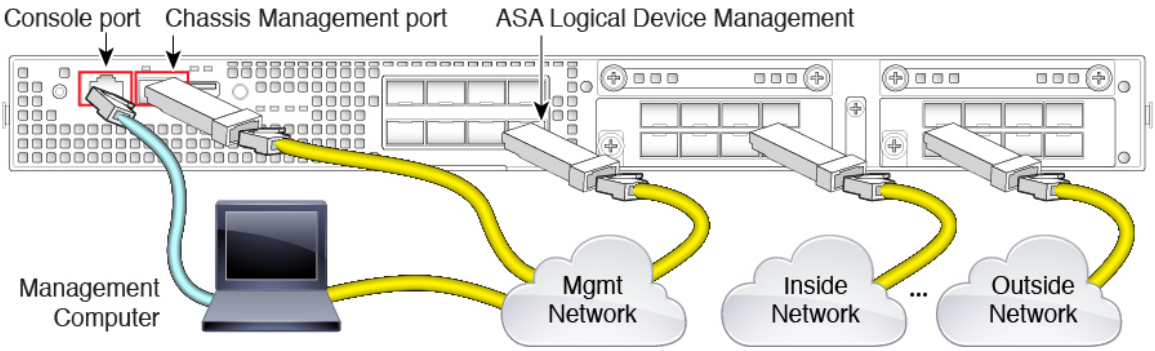
带有 CDO 的 威胁防御 布线



本指南假设您有单独的管理网络，并且有自己的互联网接入。默认情况下，管理接口在部署时已预配置，但稍后还必须配置数据接口。

确保可以从逻辑设备管理网络访问互联网。威胁防御 需要通过管理网络访问互联网，以进行 CDO 管理、更新和许可。您可以选择为CDO管理配置数据接口，而非管理接口。有关为管理器访问配置数据接口的详细信息，请参阅 FTD 命令参考中的 **configure network management-data-interface** 命令。

ASA 连接



本指南假设您有一个单独的管理网络，并且有自己的互联网接入。默认情况下，管理接口在部署时已预配置，但稍后还必须配置数据接口。

在逻辑设备管理接口上执行初始 ASA 配置。可以稍后从任何数据接口启用管理。

执行初始机箱设置

在可以使用机箱管理器配置和管理系统之前，必须执行一些初始配置任务。您可以使用控制台端口上的 FXOS CLI 或与机箱管理端口的 SSH 会话，或者使用机箱管理端口上的 HTTPS，执行初始配置。

使用浏览器执行初始机箱设置

机箱管理端口使用 DHCP 获取 IP 地址。对于初始配置，您可以使用网络浏览器配置机箱的基本设置。如果没有 DHCP 服务器，则需要使用控制台端口进行初始设置。

注释 要重复初始设置，您需要在 CLI 中使用以下命令清除任何现有配置：

```
Firepower-chassis# connect local-mgmt
firepower-chassis(local-mgmt)# erase configuration
```

开始之前

收集以下信息以与设置脚本一起使用：

- 新管理员密码
- 管理 IP 地址和子网掩码
- 网关 IP 地址
- 要允许 HTTPS 和 SSH 访问的子网

- 主机名和域名
- DNS 服务器 IP 地址

过程

步骤 1 配置您的 DHCP 服务器以将 IP 地址分配到机箱管理端口。

来自机箱的 DHCP 客户端请求包含以下信息：

- 管理接口的 MAC 地址。
- DHCP 选项 60 (vendor-class-identifier) - 设置为“FPR4100”。
- DHCP 选项 61 (dhcp-client-identifier) - 设置为机箱序列号。此序列号可在机箱的拉出卡舌上找到。

步骤 2 接通机箱电源。

步骤 3 在浏览器中输入以下 URL：

https://*ip_address***/api**

指定由 DHCP 服务器分配给机箱管理端口的 IP 地址。

步骤 4 系统提示时，使用用户名 **install** 和密码 *chassis_serial_number* 登录。

chassis_serial_number 可在机箱的拉出卡舌上找到。

步骤 5 根据提示完成系统配置。

- 强密码实施策略。
- 管理员帐户的密码。
- 系统名称
- 监控程序管理端口 IPv4 地址和子网掩码，或者 IPv6 地址和前缀。
- 默认网关 IPv4 或 IPv6 地址。
- 允许使用 SSH 访问的主机/网络地址和网络掩码/前缀。
- 允许使用 HTTPS 访问的主机/网络地址和网络掩码/前缀。
- DNS 服务器 IPv4 或 IPv6 地址。
- 默认域名。

步骤 6 点击**提交**。

在 CLI 中执行初始机箱设置

当您第一次在控制台上或使用与机箱管理端口的 SSH 会话访问 FXOS CLI 时，安装向导将提示您输入基本网络配置，以便您可以从机箱管理端口访问 机箱管理器（使用 HTTPS）或 FXOS CLI（使用 SSH）。

机箱管理端口使用 DHCP 获取 IP 地址。如果没有 DHCP 服务器，则需要使用控制台端口进行初始设置。

注释 要重复初始设置，您需要使用以下命令清除任何现有配置：

```
Firepower-chassis# connect local-mgmt
firepower-chassis(local-mgmt)# erase configuration
```

开始之前

收集以下信息以与设置脚本一起使用：

- 新管理员密码
- 管理 IP 地址和子网掩码
- 网关 IP 地址
- 要从中允许 HTTPS 和 SSH 访问的子网
- 主机名和域名
- DNS 服务器 IP 地址

过程

步骤 1 接通机箱电源。

步骤 2 使用终端仿真器连接至串行控制台端口或使用 SSH 连接机箱管理端口。

Firepower 4100 随附 RS-232 转 RJ-45 串行控制台电缆。可能需要使用第三方串口转 USB 电缆建立连接。使用以下串行参数：

- 9600 波特率
- 8 个数据位
- 无奇偶校验
- 1 个停止位

步骤 3 系统提示时，使用用户名 **admin** 和密码 **cisco123** 登录。

步骤 4 根据提示完成系统配置。

示例：

```
          ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Only minimal configuration including IP connectivity to
the FXOS Supervisor is performed through these steps.

Type Ctrl-C at any time for more options or to abort configuration
and reboot system.
To back track or make modifications to already entered values,
complete input till end of section and answer no when prompted
to apply configuration.


You have chosen to setup a new Security Appliance.
      Continue? (yes/no): y

Enforce strong password? (yes/no) [y]: n

Enter the password for "admin": Farscape&32
Confirm the password for "admin": Farscape&32
Enter the system name:  firepower-4125

Supervisor Mgmt IP address : 10.80.6.12

Supervisor Mgmt IPv4 netmask : 255.255.255.0

IPv4 address of the default gateway : 10.80.6.1

The system cannot be accessed via SSH if SSH Mgmt Access is not configured.

Do you want to configure SSH Mgmt Access? (yes/no) [y]: y

SSH Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0

SSH Mgmt Access IPv4 netmask: 255.0.0.0

Firepower Chassis Manager cannot be accessed if HTTPS Mgmt Access is not configured.

Do you want to configure HTTPS Mgmt Access? (yes/no) [y]: y

HTTPS Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0

HTTPS Mgmt Access IPv4 netmask: 255.0.0.0

Configure the DNS Server IP address? (yes/no) [n]: y

  DNS IP address : 10.164.47.13

Configure the default domain name? (yes/no) [n]: y

  Default domain name : cisco.com

Following configurations will be applied:

  Switch Fabric=A
  System Name=firepower-4125
  Enforced Strong Password=no
  Supervisor Mgmt IP Address=10.89.5.14
  Supervisor Mgmt IP Netmask=255.255.255.192
```

```
    Default Gateway=10.89.5.1
    SSH Access Configured=yes
        SSH IP Address=10.0.0.0
        SSH IP Netmask=255.0.0.0
    HTTPS Access Configured=yes
        HTTPS IP Address=10.0.0.0
        HTTPS IP Netmask=255.0.0.0
    DNS Server=72.163.47.11
    Domain Name=cisco.com

  Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): y
  Applying configuration. Please wait...  Configuration file - Ok
.....

Cisco FPR Series Security Appliance
firepower-9300 login:  admin
Password: Farscape&32
Successful login attempts for user 'admin' : 1
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2019, Cisco Systems, Inc. All rights reserved.

[...]

firepower-chassis#
```

步骤 5 您可以从控制台端口断开连接（如果已使用）或结束 SSH 会话。

登录机箱管理器

使用 机箱管理器 配置机箱设置，包括启用接口和部署逻辑设备。

开始之前

- 有关受支持的浏览器的信息，请参阅您使用的版本的发行说明（请参阅 http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.html）。
- 您只能从 IP 地址在初始机箱设置期间指定的范围内的管理计算机访问机箱管理器。

过程

步骤 1 使用支持的浏览器输入以下 URL。

https://*chassis_mgmt_ip_address*

- *chassis_mgmt_ip_address* - 标识在初始配置期间输入的机箱管理端口的 IP 地址或主机名。

步骤 2 输入用户名 **admin** 和新密码。

您可以在以后根据添加 FXOS 用户，第 15 页添加更多用户。

步骤 3 点击 **Login**。

您将登录，机箱管理器将打开以显示**概述**页面。

配置 NTP

尽管可以手动设置时间，但我们建议使用 NTP 服务器。对于 ASA 以及采用 设备管理器 的 威胁防御来说，需要正确的智能软件许可时间。对于采用 管理中心 的 威胁防御，机箱与 管理中心 之间的时间必须匹配。这种情况下，我们建议您在机箱上使用与 管理中心 相同的 NTP 服务器。请勿将 管理中心 自身用作 NTP 服务器；此方法不受支持。

开始之前

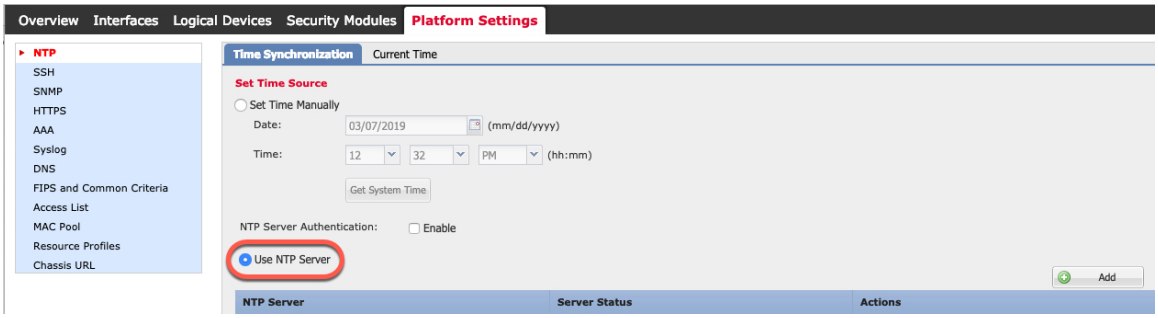
如果您要将主机名用于 NTP 服务器，则必须配置 DNS 服务器（如果尚未在初始设置中执行此操作）。请参阅**平台设置** > **DNS**。

过程

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

默认情况下，系统会选择**时间同步**选项卡。

步骤 2 点击**使用 NTP 服务器 (Use NTP Server)** 单选按钮。

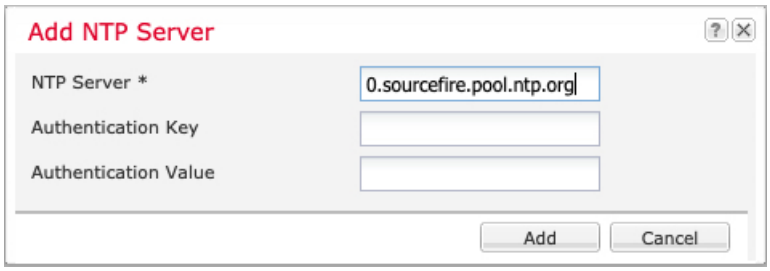


步骤 3 （可选） 如果需要对 NTP 服务器进行身份验证，请选中 **NTP 服务器身份验证: 启用**复选框。

系统将提示您启用 NTP 验证。点击**是**将要求所有 NTP 服务器条目的验证密钥 ID 和值。

仅支持使用 SHA1 进行 NTP 服务器身份验证。

步骤 4 点击**添加**，然后设置以下参数：



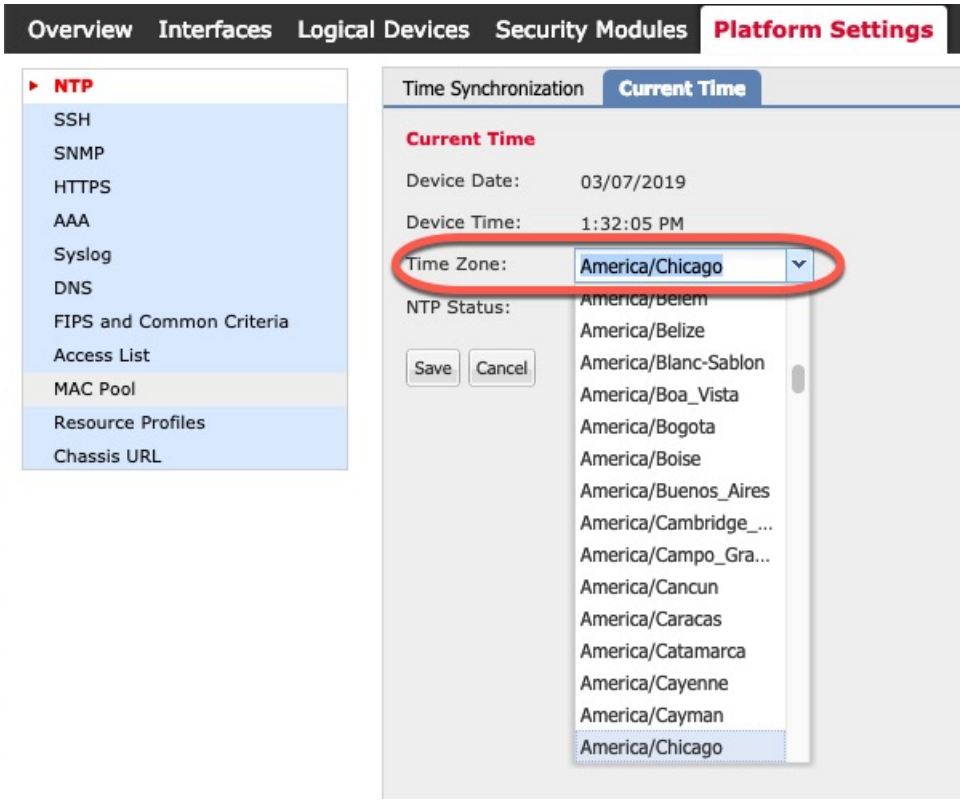
- **NTP 服务器** - NTP 服务的 IP 地址或主机名。
- **验证密钥**和**验证值** - 从 NTP 服务器获取密钥 ID 和值。例如，要在安装了 OpenSSL 的 NTP 服务器 4.2.8p8 版或更高版本上生成 SHA1 密钥，请输入 **ntp-keygen -M** 命令，然后在 ntp.keys 文件中查看密钥 ID 和值。密钥用于告知客户端和服务器在计算消息摘要时要使用哪个值。

步骤 5 点击**添加**以添加服务器。

最多可以添加 4 个 NTP 服务器。

步骤 6 点击**保存**以保存服务器。

步骤 7 从**时区**下拉列表中选择**当前时间**，然后为机箱选择适当的时区。



步骤 8 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，您需要再次登录机箱管理器。

添加 FXOS 用户

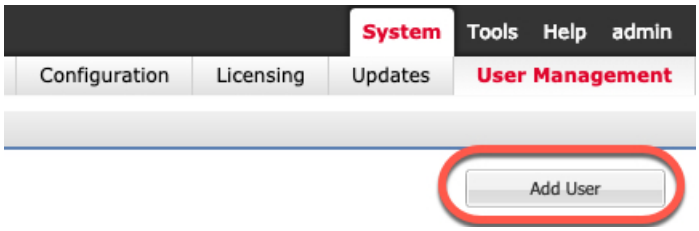
为机箱管理器和 FXOS CLI 登录添加本地用户。

过程

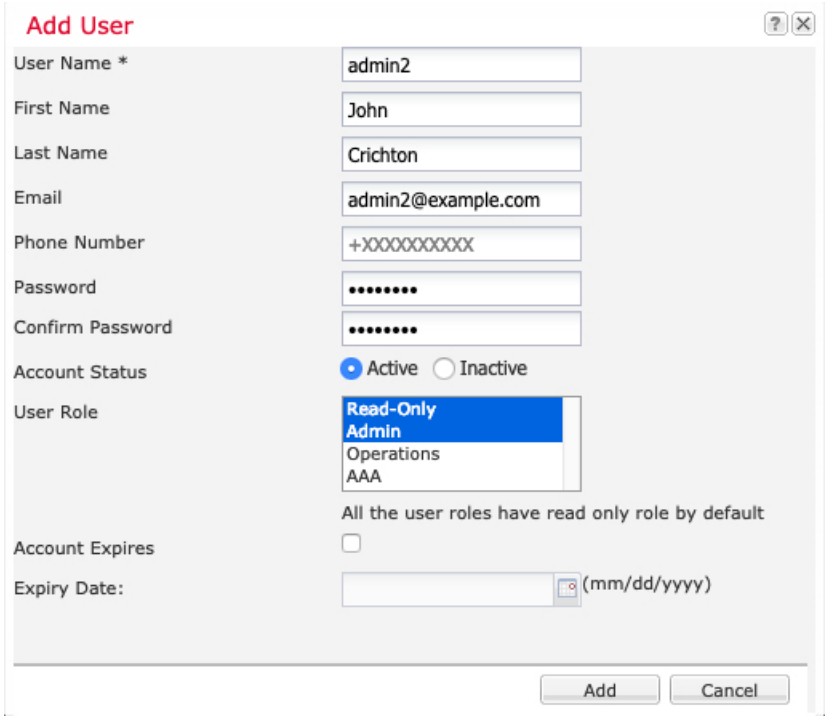
步骤 1 依次选择 **System** > **User Management**。

步骤 2 点击**本地用户**。

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：



- **用户名** - 设置用户名，最多 32 个字符。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。
- （可选）**名字** - 设置用户的名字，最多 32 个字符。
- （可选）**姓氏** - 设置用户的姓氏，最多 32 个字符。
- （可选）**电子邮箱** - 设置用户的电子邮件地址。
- （可选）**电话号码** - 设置用户的电话号码。
- **密码**和**确认密码** - 设置与此帐户关联的密码。如果启用了密码强度检查，则密码必须为强密码，FXOS 会拒绝任何不满足强度检查要求的密码。有关强密码指导原则，请参阅 FXOS 配置指南。
- **帐户状态** - 将状态设置为**活动**或**非活动**。
- **用户角色** - 设置表示要分配给用户帐户的权限的角色。系统会默认为所有用户分配**只读**角色，并且此角色无法取消选择。要分配不同的角色，请在窗口中点击角色名称以使其突出显示。您可以使用以下用户角色之一：
  - **管理员** - 完成对整个系统的读写访问。
  - **只读** - 对系统配置进行只读访问，但无权修改系统状态。
  - **操作** - 对 NTP 配置、用于智能许可的 Smart Call Home 配置和系统日志（包括系统日志服务器和故障）进行读写访问。对系统其余部分的读取访问。
  - **AAA 管理员** - 对用户、角色和 AAA 配置的读写访问。对系统其余部分的读取访问。
- （可选）**帐户到期** - 设置帐户到期。在**到期日期**字段中指定的日期过后，无法使用帐户。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。默认情况下，用户帐户不会到期。
- （可选）**到期日期** - 帐户到期的日期。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**。

配置接口

默认情况下，物理接口处于禁用状态。在 FXOS 中，您可以启用接口、添加以太网通道、添加 VLAN 子接口和编辑接口属性。要使用某一接口，必须在 FXOS 中以物理方式启用它，并在应用中以逻辑方式启用它。

要配置分支端口，请参阅 FXOS 配置指南。

接口类型

每个接口为以下类型之一：

- 数据 - 用于常规数据。不能在逻辑设备之间共享数据接口，且逻辑设备无法通过背板与其他逻辑设备通信。对于数据接口上的流量，所有流量必须在一个接口上退出机箱，并在另一个接口上返回以到达另一个逻辑设备。
- 数据共享 - 用于常规数据。仅容器实例支持这些数据接口，可由一个或多个逻辑设备/容器实例（仅限威胁防御-使用-管理中心 ）共享。 每个容器实例都可通过背板与共享此接口的所有其他实例通信。共享的接口可能会影响您可以部署容器实例的数量。共享接口不支持用于网桥组成员接口（在透明模式或路由模式下）、内联集、被动接口、集群或故障切换链路。
- 管理 - 用于管理应用程序实例。这些接口可以由一个或多个逻辑设备共享，以访问外部主机；逻辑设备无法通过此接口与共享接口的其他逻辑设备通信。只能为每个逻辑设备分配一个管理接口。根据您的应用和管理器，您可以稍后从数据接口启用管理；但必须将管理接口分配给逻辑设备，即使您不打算在启用数据管理后使用该接口。

注释 管理接口更改会导致逻辑设备重新启动，例如将管理接口从 e1/1 更改为 e1/2 会导致逻辑设备重新启动以应用新的管理接口。

- 事件 - 用作 威胁防御-using-管理中心 设备的辅助管理接口。 要使用此接口，您必须在 威胁防御 CLI 上配置其 IP 地址和其他参数。例如，您可以将管理流量从活动（例如网络活动）中分隔出来。有关详细信息，请参阅《管理中心配置指南》。事件接口可以由一个或多个逻辑设备共享，以访问外部主机；逻辑设备无法通过此接口与共享接口的其他逻辑设备通信。 如果稍后为管理配置数据接口，则无法使用单独的事件接口。

注释 安装每个应用实例时，会分配一个虚拟以太网接口。如果应用不使用事件接口，则虚拟接口将处于管理员关闭状态。

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- 集群 - 用作集群逻辑设备的集群控制链路。默认情况下，系统会在端口通道 48 上自动创建集群控制链路。“集群”类型仅在 EtherChannel 接口上受支持。 对于多实例集群，无法在设备之间共享集群类型接口。您可以将 VLAN 子接口添加到集群 EtherChannel，以便为每个集群提供单独的集群控制链路。如果向某个集群接口添加子接口，则不能将该接口用于本地集群。设备管理器 和 CDO 不支持集群。

在部署逻辑设备之前，必须配置管理接口和至少一个数据（或数据共享）接口。

配置物理接口

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，并在应用中以逻辑方式启用它。

开始之前

不能单独修改已经是 EtherChannel 成员的接口。务必在将接口添加到 EtherChannel 之前为其配置设置。

过程

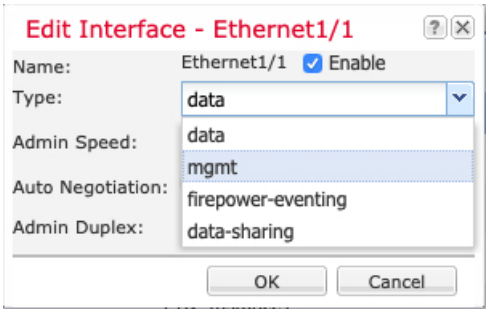
步骤 1 点击 **Interfaces**。

所有接口页面顶部显示当前已安装的接口的直观展示图，在下表中提供已安装接口列表。

步骤 2 点击要编辑的接口的 **编辑**（ ） 以打开**编辑接口**对话框。

步骤 3 选中**启用**复选框。

步骤 4 选择接口**类型**：**数据**、**数据共享**、**管理**或 **Firepower 事件**



注释 使用数据共享型接口时有一些限制；有关详细信息，请参阅 FXOS 配置指南。

对于 Firepower 事件，请参阅《Firepower 管理中心配置指南》。

步骤 5 （可选） 选择接口的**速度**。

步骤 6 （可选） 如果您的接口支持**自动协商**，请点击**是**或**否**单选按钮。

步骤 7 （可选） 选择接口的**双工**。

步骤 8 点击**确定**。

添加 EtherChannel（端口通道）

EtherChannel（也称为端口通道）最多可以包含 16 个同一介质类型和容量的成员接口，并且必须设置为相同的速度和双工模式。介质类型可以是 RJ-45 或 SFP；可以混合使用不同类型（铜缆和光纤）的 SFP。不能通过在大容量接口上将速度设置为较低值来混合接口容量（例如 1GB 和 10GB 接口）。

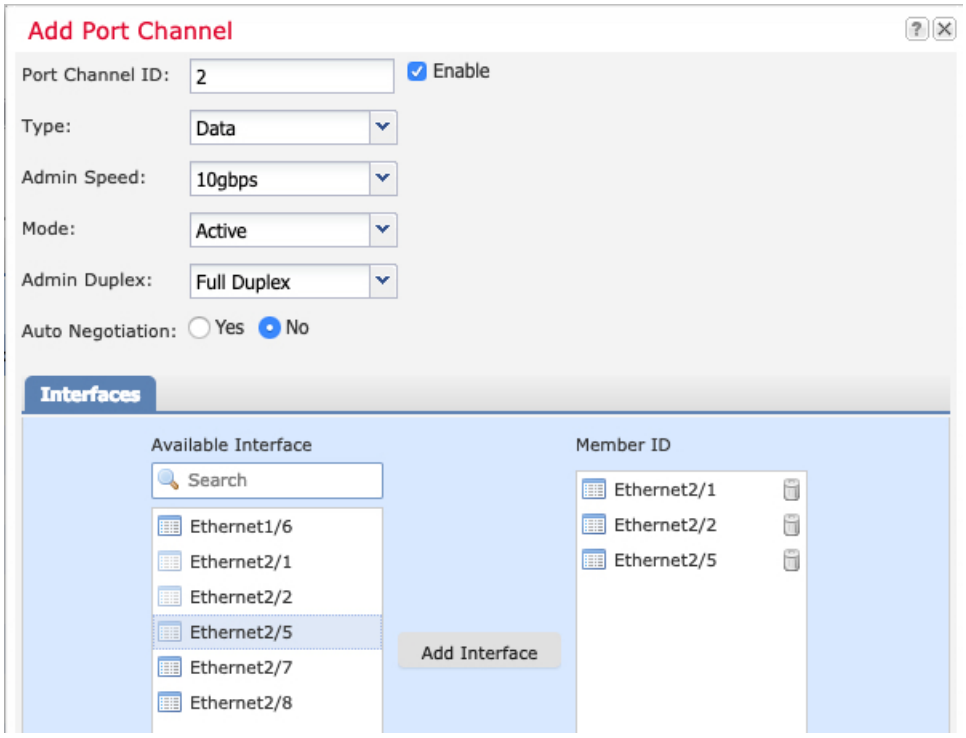
注释 机箱创建 EtherChannel 时，EtherChannel 将处于**挂起**状态（对于主动 LACP 模式）或**关闭**状态（对于打开 LACP 模式），直到将其分配给逻辑设备，即使物理链路是连通的。

过程

步骤 1 点击 **Interfaces**。

所有接口页面顶部显示当前已安装的接口的直观展示图，在下表中提供已安装接口列表。

步骤 2 点击**新增** > **端口通道**。



步骤 3 输入一个介于 1 和 47 之间的**端口通道 ID**。

步骤 4 选中**启用**复选框。

步骤 5 选择**接口类型**：

- **数据**
- **数据共享** - 仅用于容器实例。
- **管理**
- **Firepower 事件** - 仅用于 威胁防御 。
- **Cluster** - 仅用于集群。

注释 使用数据共享型接口时有一些限制；有关详细信息，请参阅 FXOS 配置指南。

对于 Firepower 事件，请参阅《Firepower 管理中心配置指南》。

步骤 6 从下拉列表设置成员接口的**管理速度**。

步骤 7 对于数据或数据共享接口，选择 LACP 端口通道**模式**：**主用**或**保持**。

对于非数据或数据共享接口，模式始终是主用模式。除非您需要最大限度地减少 LACP 流量，否则应使用主用模式。

步骤 8 从下拉列表中选择**管理双工**。

步骤 9 要将某个接口添加到端口通道，请在**可用接口**列表中选择接口，然后点击**添加接口**以将其移至**成员 ID** 列表。

最多可以添加 16 个接口。

提示 一次可添加多个接口。在按住 **Ctrl** 键的同时点击所需接口。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 10 要从端口通道删除接口，请点击**成员 ID** 列表中接口右侧的 **删除**（ ）。

步骤 11 点击**确定**。

为容器实例添加 VLAN 子接口

您最多可以将 500 个子接口连接到您的机箱。仅容器实例支持子接口；有关详细信息，请参阅逻辑设备应用程序实例：容器或本地，第 3 页。

对于多实例集群，只能将子接口添加到集群类型接口；不支持数据接口上的子接口。

每个接口的 VLAN ID 都必须具有唯一性，并且在容器实例内，VLAN ID 在所有已分配接口上也必须具有唯一性。只要系统将 VLAN ID 分配至不同的容器实例，您就可以在单独接口上重新使用它们。然而，即使每个子接口使用相同的 ID，这些子接口仍将计入限值。

您还可以在应用内添加子接口。有关何时使用 FXOS 子接口与应用子接口的详细信息，请参阅 FXOS 配置指南。

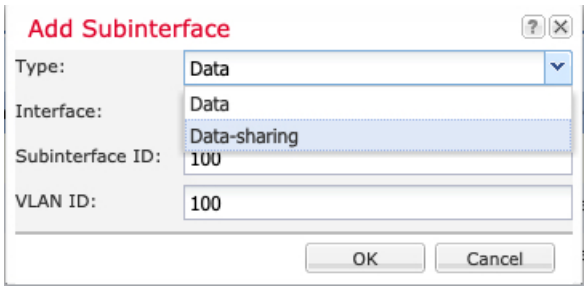
过程

步骤 1 点击 **Interfaces**。

所有接口页面顶部显示当前已安装的接口的直观展示图，在下表中提供已安装接口列表。

步骤 2 点击**添加新** > **子接口**打开**添加子接口**对话框。

步骤 3 选择接口**类型**：



- 数据
- 数据共享
- 集群 - 如果向某个集群接口添加子接口，则不能将此接口用于本地集群。

对于数据和数据共享接口：此类型独立于父接口类型；例如，您可以设数据共享父接口和数据子接口。

使用数据共享型接口时有一些限制；有关详细信息，请参阅 FXOS 配置指南。

步骤 4 从下拉列表选择父**接口**。

不得将子接口添加到当前已分配至逻辑设备的物理接口。如果系统已分配父接口的其他子接口，只要未分配此父接口，您就可以添加新的子接口。

步骤 5 输入一个介于 1 和 4294967295 之间的**子接口 ID**。

此 ID 将附加到父接口 ID，作为 *interface_id.subinterface_id*。例如，如果您将子接口添加到 ID 为 100 的以太网接口 1/1，则子接口 ID 将为：以太网接口 1/1.100。尽管可以出于方便目的将此 ID 和 VLAN ID 设置为相互匹配，但两者始终不同。

步骤 6 设置介于 1 和 4095 之间的 **VLAN ID** 。

步骤 7 点击**确定 (OK)**。

展开父接口查看其项下所有子接口。

将软件映像上传到机箱

此程序介绍如何上传新的 FXOS 和应用程序映像，以及如何升级 FXOS 映像。如果预先安装的映像不是所需的版本，可能需要上传新的映像。

开始之前

- 查看 FXOS 兼容性指南，了解 FXOS、ASA 和 威胁防御 版本之间的兼容性。
- 确保您要上传的映像在本地计算机上可用。要获取 Firepower 4100 的 FXOS 和应用程序软件，请参阅：

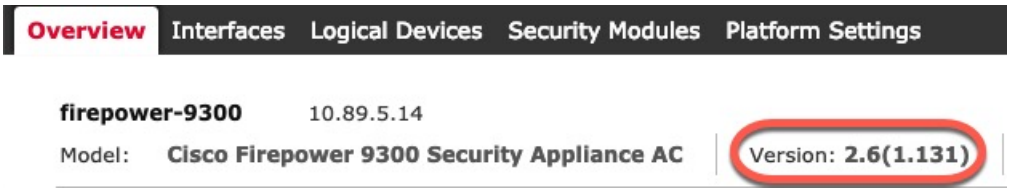
http://www.cisco.com/go/firepower4100-software

- 要确保在 HTTPS 会话期间上传成功，您可能需要在 FXOS CLI 上更改绝对超时。绝对超时为 60 分钟（最大值）；如果上传的内容较大，可能需要超过 60 分钟的时间。要禁用绝对超时，请输入：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope default-auth
Firepower-chassis /security/default-auth # set absolute-session-timeout 0
Firepower-chassis /security/default-auth* # commit-buffer
```

过程

步骤 1 查看**概述**页面，检查您当前的 FXOS 版本。



您可以在下一步中查看机箱上当前可用的应用程序映像。

步骤 2 依次选择**系统 (System)** > **更新 (Updates)**。

可用更新页面显示 FXOS 平台捆绑包映像和应用映像列表。

步骤 3 点击**上传映像**以打开**上传映像**对话框。

步骤 4 点击**浏览 (Browse)**，可导航到并选择想要上传的映像。

步骤 5 点击**上传**。所选映像将上传到机箱。

上传映像对话框会显示一个进度条，映像上传完成时会显示**成功**对话框。

步骤 6 要升级 FXOS 映像：

a) 点击想要升级到的 FXOS 平台捆绑包所对应的 升级图标（）。

b) 点击**是**以确认要继续安装。

机箱会重新加载。升级过程通常需要 20 到 30 分钟。

FXOS 的历史记录

功能名称	版本	功能信息
用于容器实例的VLAN子接口	2.4.1	要确保灵活使用物理接口，可以在FXOS中创建VLAN子接口，还可以在多个实例之间共享接口。 **注释** 要求使用 6.3 或更高版本的 威胁防御。 新增/修改的菜单项： **接口 (Interfaces)** > **所有接口 (All Interfaces)** > **新增 (Add New)**下拉菜单 > **子接口 (Subinterface)** 新增/修改的 管理中心菜单项： **设备** > **设备管理** > **编辑** 图标> **接口**
用于容器实例的数据共享接口	2.4.1	要确保灵活使用物理接口，可以在多个实例之间共享接口。 **注释** 要求使用 6.3 或更高版本的 威胁防御。 新增/修改的菜单项： **接口** > **所有接口** > **类型**
支持保存模式下的数据Etherchannel	2.4.1	现在可以将数据和数据共享 Etherchannel 设置为“主用”LACP 模式或“保持”模式。其他类型 Etherchannel 仅支持“主用”模式。 新增/修改的菜单项： **接口** > **所有接口** > **编辑端口通道** > **模式**
支持 威胁防御 内联集中的 Etherchannel	2.1.1	现在可以使用 威胁防御 内联集中的 EtherChannel。
威胁防御 支持的内联集链路状态传播	2.0.1	当您在 威胁防御 应用中配置内联集并启用链路状态传播时，威胁防御 会向 FXOS 机箱发送内联集成员身份。链路状态传播意味着，当内联集的一个接口断开时，机箱将自动关闭内联接口对的第二个接口。 新增/修改的命令：**show fault |grep link-down**, **show interface detail**
威胁防御 支持的硬件绕行网络模块	2.0.1	硬件绕行确保流量在断电期间继续在接口对之间流动。在软件或硬件发生故障时，此功能可用于维持网络连接性。 新增/修改的 管理中心菜单项： **设备** > **设备管理** > **接口** > **编辑物理接口**

功能名称	版本	功能信息
用于 威胁防御 的 Firepower事件类型接口	1.1.4	可以将接口指定为用于 威胁防御 的 Firepower 事件接口。此接口是 威胁防御 设备的辅助管理接口。要使用此接口，您必须在 威胁防御 CLI 上配置其 IP 地址和其他参数。例如，您可以将管理流量从活动（例如网络活动）中分隔出来。请参阅《管理中心配置指南》“系统配置”一章中的“管理接口”部分。 新增/修改的 机箱管理器菜单项： **接口 > 所有接口 > 类型**

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。