思科 FXOS Firepower 机箱管理器配置指南，2.2(2)

首次发布日期: 2017 年 08 月 29 日

上次修改日期: 2017 年 09 月 20 日

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

Firepower 安全设备简介

关于 Firepower 安全设备

思科 Firepower 4100/9300 机箱是网络和内容安全解决方案的下一代平台。Firepower 4100/9300 机箱是思科应用中心基础设施 (ACI) 安全解决方案的一部分，并且提供为实现可扩展性、一致控制和简化管理而构建的灵活、开放、安全的平台。

Firepower 4100/9300 机箱 具有以下特点：

- 基于机箱的模块化安全系统 - 提供高性能、灵活的输入/输出配置和可扩展性。
- Firepower 机箱管理器 - 图形用户界面，简单、直观地显示当前机箱状态并提供简化的机箱功能配置。
- FXOS CLI - 提供基于命令的接口，用于配置功能，监控机箱状态和访问高级故障排除功能。
- FXOS REST API - 允许用户以编程方式配置和管理其机箱。

Firepower 机箱管理器 概况

Firepower 可扩展操作系统提供 Web 界面，让您轻松配置平台设置和接口，调配设备，以及监控系统状态。用户界面顶部的导航栏提供到下列页面的访问：

- 概述 (Overview) - 从“概述 (Overview)”页面，您可以轻松监控 Firepower 机箱的状态。有关详细信息，请参阅监控机箱状态，第 2 页。
- 接口 (Interfaces) - 从“接口 (Interfaces)”页面，您可以查看机箱上安装的接口的状态，编辑接口属性，启用或禁用接口，以及创建端口通道。有关详细信息，请参阅接口管理，第 111 页。

- 逻辑设备 (Logical Devices) - 在“逻辑设备 (Logical Devices)”页面中，您可以创建、编辑和删除逻辑设备。有关详细信息，请参阅逻辑设备，第 117 页。
- 安全模块/安全引擎 (Security Modules/Security Engine) - 从“安全模块/安全引擎 (Security Modules/Security Engine)”页面，您可以查看 安全模块/引擎的状态并执行各种功能，例如电力循环、重新初始化、确认和解除授权。有关详细信息，请参阅安全模块/引擎管理，第 151 页。
- 平台设置 (Platform Settings) - 从“平台设置 (Platform Settings)”页面，您可以配置机箱的下列设置：日期和时间、SSH、SNMP、HTTPS、AAA、系统日志和 DNS。有关详细信息，请参阅平台设置，第 75 页。
- 系统设置 (System Settings) - 从“系统 (System)”菜单，您可以管理下列设置：

  许可 (Licensing) - 从“许可 (Licensing)”页面，您可以配置 Smart Call Home 设置，向许可证颁发机构注册 Firepower 机箱。有关详细信息，请参阅ASA 的许可证管理，第 11 页。

  更新 (Updates) - 从“更新 (Updates)”页面，您可以将平台捆绑包和应用映像上传到 Firepower 机箱。有关详细信息，请参阅映像管理，第 37 页。

  用户管理 (User Management) - 从“用户管理 (User Management)”页面，您可以为 Firepower 4100/9300 机箱配置用户设置和定义用户帐户。有关详细信息，请参阅用户管理，第 21 页。

监控机箱状态

在“概述 (Overview)”页面上，您可以轻松监控 Firepower 4100/9300 机箱的状态。“概述 (Overview)”页面提供下列元素：

- 设备信息 (Device Information) -“概述 (Overview)”页面顶部包含下列有关 Firepower 4100/9300 机箱的信息：

  机箱名称 (Chassis name) - 显示初始配置期间为机箱分配的名称。

  IP 地址 (IP address) - 显示初始配置期间为机箱分配的管理 IP 地址。

  型号 (Model) - 显示 Firepower 4100/9300 机箱型号。

  版本 (Version) - 显示机箱上运行的 FXOS 版本号。

  运行状态 (Operational State) - 显示机箱的可操作状态。

  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。

  “关闭 (Shutdown)”按钮 - 正常关闭 Firepower 4100/9300 机箱（请参阅关闭 Firepower 4100/9300 机箱电源，第 69 页）。

  注释 您可以在“安全模块/安全引擎 (Security Modules/Security Engine)”页面上打开/关闭安全模块/引擎的电源（请参阅打开/关闭安全模块电源，第 154 页）。

“重新启动 (Reboot)”按钮 - 正常关闭 Firepower 4100/9300 机箱（请参阅重新启动 Firepower 4100/9300 机箱，第 69 页）。

注释 您可以在“安全模块/安全引擎 (Security Modules/Security Engine)”页面上重置安全模块/引擎（请参阅重置安全模块/引擎，第 153 页）。

“运行时间信息 (Uptime Information)”图标 - 将光标悬停在该图标上可查看机箱和任何已安装的安全模块/引擎的运行时间。

- 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。对于带有多个安全模块的型号，您可以将光标悬停在“直观状态显示 (Visual Status Display)”中显示的安全模块上，以获取更多信息，例如设备名称、模板类型、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。状态信息分为五个部分：“故障 (Faults)”、“接口 (Interfaces)”、“设备 (Devices)”、“许可证 (License)”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。如果用户正在制定特定故障的解决方法，则他们可以确认故障，以使其他用户知悉当前正在解决故障。

  接口 (Interfaces) - 列出系统中安装的接口。**所有接口 (All Interfaces)** 选项卡和显示接口名称、运行状态、管理状态、接收的字节数和传输的字节数。此**硬件旁路**选项卡仅显示 Firepower 威胁防御应用上支持硬件旁路功能的接口对。对于每个接口对，显示运行状态：被禁用（没有为该对配置硬件旁路）、备用（配置了硬件旁路，但当前未处于活动状态）和旁路（硬件旁路活动）。

  设备 (Devices) - 列出系统中配置的逻辑设备并提供每个逻辑设备的以下详细信息：设备名称、设备状态、应用模板类型、运行状态、管理状态、映像版本、管理 IP 地址和 ASDM URL。

许可证 (License) - 显示是否启用智能许可，提供 Firepower 许可证的当前注册状态，并显示机箱的许可证授权信息。

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

第 2 章

使用入门

任务流

以下程序显示配置 Firepower 4100/9300 机箱时应当完成的基本任务。

过程

步骤 1 配置 Firepower 4100/9300 机箱硬件（请参阅思科 Firepower 安全设备硬件安装指南）。

步骤 2 完成初始配置（请参阅初始配置， 第 6 页）。

步骤 3 登录 Firepower 机箱管理器（请参阅登录或注销 Firepower 机箱管理器， 第 8 页）。

步骤 4 设置日期和时间（请参阅设置日期和时间， 第 75 页）。

步骤 5 配置 DNS 服务器（请参阅配置 DNS 服务器， 第 109 页）。

步骤 6 注册产品许可证（请参阅ASA 的许可证管理， 第 11 页）。

步骤 7 配置用户（请参阅用户管理， 第 21 页）。

步骤 8 按需执行软件更新（请参阅映像管理， 第 37 页）。

步骤 9 配置其他平台设置（请参阅平台设置， 第 75 页）。

步骤 10 配置接口（请参阅接口管理， 第 111 页）。

步骤 11 创建逻辑设备（请参阅逻辑设备， 第 117 页）。

初始配置

在您可以使用 Firepower 机箱管理器或 FXOS CLI 配置和管理您系统之前，必须使用通过控制台端口访问的 FXOS CLI 执行一些初始配置任务。当第一次使用 FXOS CLI 访问 Firepower 4100/9300 机箱时，您将会看到安装向导，您可以用它来配置系统。

您可以选择从现有的备份文件恢复系统配置，或者遍历安装向导手动设置系统。如果选择恢复系统，备份文件必须可从管理网络访问。

您必须为 Firepower 4100/9300 机箱上的单一管理端口指定一个 IPv4 地址、网关和子网掩码，或者一个 IPv6 地址、网关和网络前缀。您可以为管理端口 IP 地址配置 IPv4 或 IPv6 地址。

开始之前

1 在 Firepower 4100/9300 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 安全设备硬件安装指南。

2 验证连接到控制台端口的计算机终端（或控制台服务器）上的控制台端口参数是否如下所示：

- 9600 波特率
- 8 个数据位
- 无奇偶校验
- 1 个停止位

过程

步骤 1 连接到控制台端口。

步骤 2 打开 Firepower 4100/9300 机箱 的电源。
在 Firepower 4100/9300 机箱 启动时，您将看到开机自测消息。

步骤 3 当未配置的系统启动时，安装向导将提示您输入配置系统所需的下列信息：

- 设置模式（从完整系统备份或初始设置中恢复）
- 强密码执行策略（对于强密码准则，请参阅用户帐户，第 21 页）
- 管理员密码
- 系统名称
- 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

- DNS 服务器 IPv4 或 IPv6 地址
- 默认域名

步骤 4 检查安装摘要，输入 **yes**，保存并应用设置，或者输入 **no**，再次遍历安装向导更改某些设置。如果选择再次遍历安装向导，您之前输入的值将显示在括号中。要接受之前输入的值，请按 **Enter** 键。

以下示例使用 IPv4 管理地址设置配置：

```
Enter the setup mode; setup newly or restore from backup. (setup/restore) ? setup
You have chosen to setup a new Fabric interconnect. Continue? (y/n): y
Enforce strong password? (y/n) [y]: n
Enter the password for "admin": adminpassword%958
Confirm the password for "admin": adminpassword%958
Enter the system name: foo
Physical Switch Mgmt0 IP address : 192.168.10.10
Physical Switch Mgmt0 IPv4 netmask: 255.255.255.0
IPv4 address of the default gateway: 192.168.10.1
Configure the DNS Server IP address? (yes/no) [n]: yes
  DNS IP address: 20.10.20.10
Configure the default domain name? (yes/no) [n]: yes
  Default domain name: domainname.com
Following configurations will be applied:
  Switch Fabric=A
  System Name=foo
  Enforce Strong Password=no
  Physical Switch Mgmt0 IP Address=192.168.10.10
  Physical Switch Mgmt0 IP Netmask=255.255.255.0
  Default Gateway=192.168.10.1
  IPv6 value=0
  DNS Server=20.10.20.10
  Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

以下示例使用 IPv6 管理地址设置配置：

```
Enter the setup mode; setup newly or restore from backup. (setup/restore) ? setup
You have chosen to setup a new Fabric interconnect. Continue? (y/n): y
Enforce strong password? (y/n) [y]: n
Enter the password for "admin": adminpassword%652
Confirm the password for "admin": adminpassword%652
Enter the system name: foo
Physical Switch Mgmt0 IP address :  2001::107
Physical Switch Mgmt0 IPv6 prefix: 64
IPv6 address of the default gateway: 2001::1
Configure the DNS Server IPv6 address? (yes/no) [n]: yes
  DNS IP address: 2001::101
Configure the default domain name? (yes/no) [n]: yes
  Default domain name: domainname.com
Following configurations will be applied:
  Switch Fabric=A
  System Name=foo
  Enforced Strong Password=no
  Physical Switch Mgmt0 IPv6 Address=2001::107
  Physical Switch Mgmt0 IPv6 Prefix=64
  Default Gateway=2001::1
  Ipv6 value=1
  DNS Server=2001::101
  Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

登录或注销 Firepower 机箱管理器

您必须先使用有效的用户帐户登录，然后才能使用Firepower机箱管理器配置您的Firepower 4100/9300机箱。有关用户帐户的详细信息，请参阅用户管理，第 21 页。

如果经过一段时间没有任何活动，则您将自动从系统注销。默认情况下，系统将在无活动10分钟后将您注销。要配置此超时设置，请参阅配置会话超时，第 30 页。您还可以配置绝对超时设置，即便会话仍处于活动状态，该设置也可以在一段时间后将用户从系统中注销。要配置绝对超时设置，请参阅配置绝对会话超时，第 30 页。

有关可导致您从 Firepower 机箱管理器自动注销的所有系统更改的列表，请参阅导致 Firepower 机箱管理器会话被关闭的系统更改，第 61 页。

注释 您可以选择将 Firepower 机箱管理器配置为只允许一定数量的不成功登录尝试，然后，用户会被系统锁定一段指定的时间长度。这是为实现系统的通用标准认证合规性提供的众多选项之一。有关详细信息，请参阅安全认证合规性，第 43 页。

过程

步骤 1 要登录 Firepower 机箱管理器，请执行以下操作：

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 4100/9300 机箱的 IP 地址或主机名。

注释 有关受支持的浏览器的信息，请参阅您使用的版本的版本说明（请参阅 http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.html）。

b) 输入您的用户名和密码。

c) 点击 **Login**。

您已登录，Firepower 机箱管理器打开以显示“概述 (Overview)”页面。

步骤 2 要注销Firepower 机箱管理器，请指向导航栏中的用户名，然后选择**注销 (Logout)**。
您已注销 Firepower 机箱管理器，并返回登录屏幕。

访问 FXOS CLI

可以使用插入到控制台端口中的终端来连接到FXOS CLI。验证连接到控制台端口的计算机终端（或控制台服务器）上的控制台端口参数是否如下所示：

- 9600 波特率

- 8 个数据位
- 无奇偶校验
- 1 个停止位

您也可以使用 SSH 和 Telnet 来连接到 FXOS CLI。Firepower 可扩展操作系统最多支持 8 个 SSH 并发连接。要使用 SSH 进行连接，您需要知道 Firepower 4100/9300 机箱的主机名或 IP 地址。

使用以下语法示例之一来通过 SSH、Telnet 或 Putty 进行登录：

注释 SSH 登录区分大小写。

使用 SSH 从 Linux 终端登录：

- **sshucs-***auth-domain\\username@{UCSM-ip-address|UCMS-ipv6-address}*

```
ssh ucs-example\\jsmith@192.0.20.11
ssh ucs-example\\jsmith@2001::1
```

- **ssh -lucs-***auth-domain\\username {UCSM-ip-address| UCSM-ipv6-address| UCSM-host-name}*

```
ssh -l ucs-example\\jsmith 192.0.20.11
ssh -l ucs-example\\jsmith 2001::1
```

- **ssh** *{UCSM-ip-address | UCSM-ipv6-address | UCSM-host-name}* **-lucs-***auth-domain\\username*

```
ssh 192.0.20.11 -l ucs-example\\jsmith
ssh 2001::1 -l ucs-example\\jsmith
```

- **sshucs-***auth-domain\\username@{UCSM-ip-address|UCSM-ipv6-address}*

```
ssh ucs-ldap23\\jsmith@192.0.20.11
ssh ucs-ldap23\\jsmith@2001::1
```

使用 Telnet 从 Linux 终端登录：

注释 默认情况下，会禁用 Telnet。有关启用 Telnet 的说明，请参阅配置 Telnet，第 79 页。

- **telnet ucs-***UCSM-host-name* **ucs-***auth-domain\username*

```
telnet ucs-qa-10
login: ucs-ldap23\blradmin
```

- **telnetucs-***{UCSM-ip-address|UCSM-ipv6-address}ucs-auth-domain\username*

```
telnet 10.106.19.12 2052
ucs-qa-10-A login: ucs-ldap23\blradmin
```

从 Putty 客户端登录：

- 登录方式：**ucs-***auth-domain\username*

```
Login as: ucs-example\jsmith
```

注释 如果默认身份验证设置为本地，并且控制台身份验证设置为LDAP，您可以使用ucs-local\admin从Putty客户端登录交换矩阵互联，其中admin是本地帐户名称。

第 3 章

ASA 的许可证管理

通过思科智能软件许可，您可以集中购买和管理许可证池。您可以轻松部署或停用设备，而不必管理每台设备的许可密钥。通过智能软件许可，您还可以直观地了解许可证使用情况和需求。

注释 本节仅适用于 Firepower 4100/9300 机箱上的 ASA 逻辑设备。有关如何为 Firepower 威胁防御逻辑设备进行许可方面的详细信息，请参阅《Firepower 管理中心配置指南》。

关于智能软件许可

本部分介绍智能软件许可的工作原理。

注释 本节仅适用于 Firepower 4100/9300 机箱上的 ASA 逻辑设备。有关如何为 Firepower 威胁防御逻辑设备进行许可方面的详细信息，请参阅《Firepower 管理中心配置指南》。

适用于 ASA 的智能软件许可

对于 Firepower 4100/9300 机箱上的 ASA 应用，智能软件许可配置在 Firepower 4100/9300 机箱管理引擎和应用之间拆分。

- Firepower 4100/9300 机箱 - 在管理引擎中配置所有智能软件许可基础设施，包括用于与许可证颁发机构进行通信的参数。Firepower 4100/9300 机箱本身无需任何许可证即可运行。

  注释 机箱间集群要求在集群中的每个机箱上启用相同的智能许可方法。

- ASA 应用 - 在应用中配置所有许可证授权。

智能软件管理器和帐户

在为设备购买一个或多个许可证时，可在思科智能软件管理器中对其进行管理：

https://software.cisco.com/#module/SmartLicensing

通过智能软件管理器，您可以为组织创建一个主帐户。

注释 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。

默认情况下，许可证分配给主帐户下的默认虚拟帐户。作为帐户管理员，您可以选择创建其他虚拟帐户；例如，您可以为区域、部门或子公司创建帐户。通过多个虚拟帐户，您可以更轻松地管理大量许可证和设备。

离线管理

如果您的设备没有互联网接入，因此无法向许可证颁发机构注册，则可配置离线许可。

永久许可证预留

如果出于安全原因，设备无法访问互联网，可以选择为每个ASA申请永久许可证。永久许可证不需要定期访问许可证颁发机构。与PAK许可证一样，您将为ASA购买一个许可证并安装许可证密钥。与PAK许可证不同的是，您将通过智能软件管理器获取和管理许可证。您可以在普通的智能许可模式与永久许可证预留模式之间轻松切换。

您可以获取启用所有功能的许可证：标准层，具有最大安全情景和运营商许可证。许可证在Firepower 4100/9300 机箱上进行管理，但您还需要在 ASA 配置中申请授权，以便 ASA 允许其使用。

卫星服务器

如果设备因安全原因无法访问互联网，您可以选择安装一个本地智能软件管理器卫星服务器作为虚拟机(VM)。卫星提供一组智能软件管理器功能，并允许您为所有本地设备提供重要的许可服务。只有卫星需要定期连接到主许可证颁发机构以同步您的许可证使用。您可以按计划同步，也可以手动同步。

一旦下载并部署该卫星应用之后，即可在不使用互联网将数据发送到 Cisco SSM 的情况下执行以下功能：

- 激活或注册许可证
- 查看公司的许可证
- 将公司实体之间传输许可证

有关详细信息，请参阅智能帐户管理器卫星上的智能软件管理器卫星安装和配置指南。

按虚拟帐户管理的许可证和设备

仅当虚拟帐户可以使用分配给该帐户的许可证时，才能按虚拟帐户对许可证和设备进行管理。如果您需要其他许可证，则可以从另一个虚拟帐户传输未使用的许可证。您还可以在虚拟帐户之间迁移设备。

只有 Firepower 4100/9300 机箱作为设备进行注册，而机箱中的 ASA 应用则请求其自己的许可证。例如，对于有 3 个安全模块的 Firepower 9300机箱而言，机箱计为一个设备，但模块使用 3 个单独的许可证。

评估许可证

Firepower 4100/9300 机箱 支持两种类型的评估许可证：

- 机箱级评估模式 - 在 Firepower 4100/9300 机箱向许可证颁发机构注册之前，会在评估模式下运行 90 天（总使用量）。ASA 在此模式下无法请求特定授权；仅会启用默认授权。当此期限结束时，Firepower 4100/9300 机箱 会变为不合规。
- 基于授权的评估模式 - Firepower 4100/9300 机箱 向许可证颁发机构注册后，您可以获取分配给 ASA 的基于时间的评估许可证。在 ASA 中，您可以照常请求授权。当该基于时间的许可证到期时，您需要续订基于时间的许可证或获取永久许可证。

注释 您无法获得针对强密码(3DES/AES)的评估许可证；仅永久许可证支持此授权。

智能软件管理器通信

本部分介绍您的设备如何与智能软件管理器通信。

设备注册和令牌

对于每个虚拟帐户，您可以创建注册令牌。默认情况下，此令牌有效期为30天。当部署每个机箱或注册现有机箱时，请输入此令牌 ID 以及授权级别。如果现有令牌已过期，则可以创建新的令牌。

在部署后或在现有机箱上手动配置这些参数后启动时，机箱会向思科许可证颁发机构注册。当机箱向令牌注册时，许可证颁发机构会颁发ID证书，用于在机箱与许可证颁发机构之间进行通信。此证书有效期为 1 年，但需要每 6 个月续签一次。

与许可证颁发机构的定期通信

设备每30天与许可证颁发机构进行通信。如果您在智能软件管理器中进行更改，则可以刷新设备上的授权，以使更改立即生效。或者，也可以等待设备按计划通信。

您可以随意配置 HTTP 代理。

Firepower 4100/9300 机箱必须能够至少每 90 天直接或通过HTTP代理访问互联网。常规许可证通信每 30 天进行一次，但如果设备具有宽限期，则会最多运行 90 天，而不会进行自动通报。在宽限期后，您必须联系许可证颁发机构，否则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。

不合规状态

设备在以下情况下可能会处于不合规状态：

- 过度使用 - 当设备使用不可用的许可证时。
- 许可证到期 - 当基于时间的许可证到期时。
- 通信不畅 - 当设备无法访问许可证颁发机构以重新获得授权时。

要验证您的帐户是否处于或接近不合规状态，必须将 Firepower 4100/9300 机箱当前正在使用的授权与智能帐户中的授权进行比较。

在不合规状态下，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。例如，针对标准许可证限制的现有情景可以继续运行，并且您可以修改其配置，但您将无法添加新情景。

Smart Call Home 基础设施

默认情况下，Smart Call Home 配置文件存在于用于指定许可颁发机构的 URL 的 FXOS 配置中。您无法删除此配置文件。请注意，许可证配置文件的唯一可配置选项是许可证颁发机构的目标地址 URL。除非获得思科 TAC 的指示，否则不应更改许可证颁发机构 URL。

智能软件许可必备条件

- 请注意，本章仅适用于 Firepower 4100/9300 机箱上的 ASA 逻辑设备。有关如何为 Firepower 威胁防御逻辑设备进行许可方面的详细信息，请参阅《Firepower 管理中心配置指南》。
- 在思科智能软件管理器上创建主帐户：

  https://software.cisco.com/#module/SmartLicensing

  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。
- 从思科商务工作空间购买 1 个或多个许可证。在主页上，在**查找产品和解决方案 (Find Products and Solutions)** 搜索字段中搜索您的平台。有些许可证是免费的，但您仍需将其添加到您的智能软件许可帐户。
- 确保可从机箱接入互联网或访问 HTTP 代理，以使机箱能够访问许可颁发机构。
- 配置 DNS 服务器，以使机箱能够解析许可颁发机构的名称。
- 为机箱设置时间。
- 先在 Firepower 4100/9300 机箱上配置智能软件许可基础设施，再配置 ASA 许可授权。

智能软件许可指南

ASA 故障切换和集群指南

每个 Firepower 4100/9300 机箱都必须在许可证颁发机构或卫星服务器上注册。辅助设备不会产生额外成本。对于预留永久许可证，必须为每个机箱购买单独的许可证。

智能软件许可的默认设置

Firepower 4100/9300 机箱默认配置包括名为“SLProf”的 Smart Call Home 配置文件，该文件用于指定许可颁发机构的 URL。

配置常规智能软件许可

要与思科许可证颁发机构通信，您可以选择配置 HTTP 代理。要向许可证颁发机构注册，必须在 Firepower 4100/9300 机箱上输入您从智能软件许可证帐户获得的注册令牌 ID。

过程

步骤 1 （可选）配置 HTTP 代理，第 16 页.

步骤 2 向许可证颁发机构注册 Firepower 安全设备，第 17 页.

（可选）配置 HTTP 代理

如果您的网络使用 HTTP 代理进行互联网访问，则必须为智能软件许可配置代理地址。此代理一般也用于 Smart Call Home。

注释 不支持认证的HTTP代理。

过程

步骤 1 选择**系统 (System)** > **许可 (Licensing)** > **Call Home**。
Call Home 页面提供用于配置许可证颁发机构的目标地址 URL 以及配置 HTTP 代理的字段。

注释 除非获得思科 TAC 的指示，否则不应更改许可证颁发机构 URL。

步骤 2 在“服务器启用 (Server Enable)”下拉列表中，选择**开 (on)**。

步骤 3 在**服务器 URL (Server URL)** 和 **服务器端口 (Server Port)** 字段中输入代理 IP 地址和端口。例如，为 HTTPS 服务器输入端口 443。

步骤 4 点击**保存 (Save)**。

（可选）删除 Call Home URL

使用以下程序删除先前配置的 Call Home URL。

过程

步骤 1 选择**系统 (System)** > **许可 (Licensing)** > **Call Home**。

步骤 2 在 **Call home 配置 (Call home Configuration)** 区域中，选择删除 (Delete)。

向许可证颁发机构注册 Firepower 安全设备

当注册 Firepower 4100/9300 机箱 时，许可证颁发机构会为 Firepower 4100/9300 机箱 与许可证颁发机构之间的通信颁发 ID 证书。它还会将 Firepower 4100/9300 机箱 分配到相应的虚拟帐户。通常，此程序是一次性实例。但是，如果ID证书由于诸如通信问题等原因而到期，则稍后可能需要重新注册 Firepower 4100/9300 机箱。

过程

步骤 1 在智能软件管理器或智能软件管理器卫星中，为要将此 Firepower 4100/9300 机箱 添加到的虚拟帐户申请并复制注册令牌。
有关如何使用智能软件管理器卫星申请注册令牌的更多信息，请参阅《思科智能软件管理器卫星用户指南》(http://www.cisco.com/web/software/286285517/138897/Smart_Software_Manager_satellite_4.1.0_User_Guide.pdf)。

步骤 2 在 Firepower 机箱管理器中，选择**系统 (System)** > **许可 (Licensing)** > **智能许可证 (Smart License)**。

步骤 3 在**输入产品实例注册令牌 (Enter Product Instance Registration Token)** 字段中输入注册令牌。

步骤 4 点击 **注册**。
Firepower 4100/9300 机箱尝试向许可证颁发机构注册。

要取消注册设备，请点击**取消注册 (Unregister)**。

对Firepower 4100/9300 机箱注销会从帐户中删除设备。系统会删除设备上的所有许可证授权和证书。您可能希望取消注册来为新的 Firepower 4100/9300 机箱 释放许可证。或者，也可以从智能软件管理器删除设备。

配置智能许可证卫星服务器用于 Firepower 4100/9300 机箱

以下程序显示如何配置 Firepower 4100/9300 机箱，以使用智能许可证卫星服务器。

开始之前

- 满足智能软件许可必备条件，第 15 页中列出的所有必要条件。
- 从 Cisco.com 下载智能许可证卫星 OVA 文件，并在 VMwareESXi 服务器上安装和配置此文件。有关详细信息，请参阅《智能软件管理器卫星安装指南》。
- 如果您还没有证书链，请使用下面的程序申请一个：

  创建密钥环（创建密钥环，第 88 页）。

  为该密钥环创建证书请求（使用基本选项创建密钥环的证书请求，第 89 页）。

  将此证书请求发送至可信定位点或证书颁发机构，以便为您的密钥环获得证书链。

有关详细信息，请参阅证书、密钥环和受信任点，第 87 页。

过程

步骤 1 选择**系统 (System)** > **许可 (Licensing)** > **Call Home**。

步骤 2 在 **Call home 配置 (Call home Configuration)** 区域中，将**地址 (Address)** 字段中的默认 URL 替换为卫星 URL：**https://***ip_address*/**Transportgateway/services/DeviceRequestHandler**

步骤 3 使用 CLI 创建新信任点。（请参阅《FXOS CLI 配置指南》中的智能许可证卫星管理器配置步骤，了解更多信息）

步骤 4 向许可证颁发机构注册 Firepower 安全设备，第 17 页。请注意，必须从智能许可证管理器卫星请求和复制注册令牌。

配置永久许可证预留

可以给 Firepower 4100/9300 机箱分配永久许可证。此通用预留允许您在设备上不受计数限制地使用任何授权。

注释 在开始之前，您必须购买永久许可证，才能在智能软件管理器中使用。并非所有帐户都被批准使用永久许可证预留。在您尝试配置此功能之前，请确保已获得思科批准。

安装永久许可证

以下程序显示如何给您的 Firepower 4100/9300 机箱分配永久许可证。

过程

步骤 1 选择**System** > **Licensing** > **Permanent License**。

步骤 2 点击**Generate** 生成预留申请代码。将预留申请代码复制到剪贴板。

步骤 3 转至思科智能软件管理器门户的“智能软件管理器库存 (Smart Software Manager Inventory)”屏幕，点击**Licenses** 选项卡：
https://software.cisco.com/#SmartLicensing-Inventory

Licenses 选项卡显示与您的帐户相关的所有现有许可证（普通和永久）。

步骤 4 点击**License Reservation**，并将生成的预留申请代码粘贴到框中。

步骤 5 点击 **Reserve License**。
智能软件管理器将生成授权码。您可以下载该授权码或将其复制到剪贴板。根据智能软件管理器，许可证现已处于使用状态。

如果您没有看到 **License Reservation** 按钮，则您的帐户未被授权执行永久许可证预留。在这种情况下，您应禁用永久许可证预留并重新输入普通的智能许可证命令。

步骤 6 在 Firepower 机箱管理器中，将生成的授权码输入 **Authorization Code** 文本框。

步骤 7 点击 **Install**。
一旦您的 Firepower 4100/9300 机箱 获得完全的 PLR 许可，“永久许可证 (Permanenet License)”页面将显示您的许可证状态并提供返还永久许可证的选项。

步骤 8 在 ASA 逻辑设备上启用功能授权。请参阅 ASA 许可一章，以启用授权。

（可选）返还永久许可证

如果不再需要永久许可证，您必须使用以下程序将其正式返还给智能软件管理器。如果不遵循所有步骤，许可证将保持使用状态，无法在其他地方使用。

过程

步骤 1 选择**System** > **Licensing** > **Permanent License**。

步骤 2 点击**Return** 生成返还代码。将返还代码复制到剪贴板。
Firepower 4100/9300 机箱将立即变为未许可并进入 Evaluation 状态。

步骤 3 访问“智能软件管理器库存 (Smart Software Manager Inventory)”屏幕，点击**Product Instances** 选项卡：
https://software.cisco.com/#SmartLicensing-Inventory

步骤 4 使用您的 Firepower 4100/9300 机箱的通用设备标识符 (UDI) 搜索该设备。

步骤 5 选择**Actions** > **Remove**，并将生成的返还代码粘贴到框中。

步骤 6 点击 **Remove Product Instance**。
永久许可证被返还到可用池。

智能软件许可历史记录

功能名称	平台版本	说明
面向 Firepower 4100/9300 机箱的思科智能软件许可	1.1(1)	通过智能软件许可，您可以购买和管理许可证池。智能许可证不与特定序列号关联。您可以轻松部署或停用设备，而不必管理每台设备的许可密钥。通过智能软件许可，您还可以直观地了解许可证使用情况和需求。智能软件许可配置在 Firepower 4100/9300 机箱管理引擎和安全模块之间拆分。 引入了以下屏幕： **系统 (System) > 许可 (Licensing) > Call Home** **系统 (System) > 许可 (Licensing) > 智能许可证 (Smart License)**

第 4 章

用户管理

用户帐户

用户帐户用于访问系统。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。

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。管理员帐户没有已分配的默认密码；您必须在初始系统设置中选择密码。

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或AAA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）。

远程身份验证的用户帐户

远程身份验证的用户帐户是指任何通过 LDAP、RADIUS 或 TACACS+ 进行身份验证的用户帐户。

如果用户同时持有本地用户帐户和远程用户帐户，则在本地用户帐户中定义的角色将覆盖在远程用户帐户中持有的角色。

有关远程身份验证指导原则以及如何配置和删除远程身份验证提供程序的详细信息，请参阅以下主题：

- 远程身份验证指导原则，第 23 页
- 配置 LDAP 提供程序，第 99 页
- 配置 RADIUS 提供程序，第 102 页
- 配置 TACACS+ 提供程序，第 104 页

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。

面向用户名的指导原则

用户名还用作 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，请考虑以下指导原则和限制：

- 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。

面向密码的指导原则

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Firepower可扩展操作系统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，请参阅配置最小密码长度检查，第 33 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。

远程身份验证指导原则

如果为支持的远程身份验证服务之一配置系统，则必须创建用于该服务的提供程序，以确保Firepower 4100/9300 机箱 能够与系统进行通信。下列指导原则影响用户授权：

远程身份验证服务中的用户帐户

用户帐户可能存在于 Firepower 4100/9300 机箱 本地或远程身份验证服务器中。

您可以通过Firepower 机箱管理器或 FXOS CLI 查看通过远程身份验证服务登录的用户的临时会话。

远程身份验证服务中的用户角色

如果在远程身份验证服务器中创建用户帐户，则必须确保帐户包括用户在 Firepower 4100/9300 机箱 中工作所需的角色，并且这些角色的名称与FXOS 中使用的名称相匹配。根据角色策略，系统可能会禁止用户登录，或仅向其授予只读权限。

远程身份验证提供程序中的用户属性

对于 RADIUS 和 TACAS+ 配置，您必须为各远程身份验证提供程序中的 Firepower 4100/9300 机箱配置用户属性（用户通过该提供程序登录到 Firepower 机箱管理器或 FXOS CLI）。此用户属性存储分配给各用户的角色和区域设置信息。

用户登录后，FXOS 执行以下操作：

1. 查询远程身份验证服务。
2. 验证用户。
3. 如果用户已通过验证，请检查分配给该用户的角色和区域设置。

下表包含 FXOS 支持的远程身份验证提供程序的用户属性要求比较：

身份验证提供程序	自定义属性	方案扩展	属性 ID 要求
LDAP	可选	您可以选择执行以下操作之一： • 请不要扩展 LDAP 方案，配置符合要求的现有的未使用属性。 • 扩展 LDAP 方案，使用唯一名称（例如，CiscoAVPair）创建自定义属性。	Cisco LDAP 实施需要 unicode 类型属性。 如果选择创建 CiscoAVPair 自定义属性，请使用以下属性 ID：1.3.6.1.4.1.9.287247.1 以下部分提供示例 OID。

身份验证提供程序	自定义属性	方案扩展	属性 ID 要求
RADIUS	可选	您可以选择执行以下操作之一： • 请不要扩展 RADIUS 方案，并使用符合要求的现有未使用属性。 • 扩展 RADIUS 方案，使用唯一名称（例如，cisco-avpair）创建自定义属性。	Cisco RADIUS 实施的供应商 ID 为 009，属性的供应商 ID 为 001。 以下语法示例显示，如果选择创建 cisco-avpair 属性，如何指定多个用户角色和区域：`shell:roles="admin,aaa" shell:locales="L1,abc"`。使用逗号“,”作为分隔多个值的分隔符。
TACAS	必要	必须扩展方案，并使用名称 cisco-av-pair 创建自定义属性。	cisco-av-pair 名称是为 TACACS+ 提供程序提供属性 ID 的字符串。 以下语法示例说明，在创建 cisco-av-pair 属性时，如何指定多个用户角色和区域：`cisco-av-pair=shell:roles="admin aaa" shell:locales*"L1 abc"`。在 cisco-av-pair 属性语法中使用星号 (*) 将区域标记为可选项，以避免使用相同身份验证配置文件的其他思科设备的身份验证失败。使用空格作为分隔符，来分隔多个值。

LDAP 用户属性的示例 OID

以下是自定义 CiscoAVPair 属性的示例 OID：

```
CN=CiscoAVPair,CN=Schema,
CN=Configuration,CN=X
objectClass: top
objectClass: attributeSchema
cn: CiscoAVPair
distinguishedName: CN=CiscoAVPair,CN=Schema,CN=Configuration,CN=X
instanceType: 0x4
uSNCreated: 26318654
```

```
attributeID: 1.3.6.1.4.1.9.287247.1
attributeSyntax: 2.5.5.12
isSingleValued: TRUE
showInAdvancedViewOnly: TRUE
adminDisplayName: CiscoAVPair
adminDescription: UCS User Authorization Field
oMSyntax: 64
lDAPDisplayName: CiscoAVPair
name: CiscoAVPair
objectCategory: CN=Attribute-Schema,CN=Schema,CN=Configuration,CN=X
```

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

对系统配置进行只读访问，但无权修改系统状态。

运营

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。

本地身份验证用户的密码配置文件

密码配置文件包含所有本地身份验证用户的密码历史记录和密码更改时间间隔属性。不能为每个本地身份验证的用户指定其他密码配置文件。

密码历史记录计数

借助密码历史记录计数，您可以阻止本地身份验证的用户反复使用同一密码。配置此属性后，Firepower 机箱最多可以存储本地身份验证的用户先前使用的 15 个密码。密码存储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。

用户必须创建和使用在密码历史记录计数中配置的密码数量，然后才能重新使用密码。例如，如果您将密码历史记录计数设置为 8，本地身份验证用户无法重新使用第一个密码，直至第九个密码过期为止。

默认情况下，密码历史记录设置为0。该值禁用历史记录计数，允许用户随时重新使用以前的密码。

如有必要，可以清除本地身份验证的用户的密码历史记录计数并支持重复使用先前的密码。

密码更改间隔

通过密码更改间隔，可以限制本地身份验证的用户在特定小时数内能够进行的密码更改次数。下表介绍密码更改间隔的两个配置选项。

间隔配置	描述	示例
不允许密码更改 (No password change allowed)	此选项不允许在密码更改后的指定小时数内更改本地身份验证的用户的密码。 可以指定介于 1 和 745 小时之间的无更改间隔。默认情况下，无更改间隔为 24 小时。	例如，要在本地身份验证用户更改其密码后 48 小时内阻止更改密码，请进行以下设置： • 将在间隔期间更改设置为禁用 • 将无更改间隔设置为 48
更改间隔内允许密码更改 (Password changes allowed within change interval)	此选项指定本地身份验证的用户的密码在预定义间隔内可以更改的最大次数。 可以指定介于 1 和 745 小时之间的更改间隔，以及介于 0 和 10 之间的最大密码更改次数。默认情况下，允许本地身份验证的用户在 48 小时间隔内最多更改 2 次密码。	例如，要在本地身份验证用户更改其密码后 24 小时内最多允许一次密码更改，请进行以下设置： • 将在间隔期间更改设置为启用 • 将更改计数设置为 1 • 将更改间隔设置为 24

配置用户设置

过程

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

步骤 2 单击 **Settings**（设置）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。 • **Radius** - 必须在为 Firepower 机箱指定的 RADIUS 服务器上定义用户帐户。 • **TACACS** - 必须在为 Firepower 机箱指定的 TACACS+ 服务器上定义用户帐户。 • **LDAP** - 必须在为 Firepower 机箱指定的 LDAP/MS-AD 服务器上定义用户帐户。 • **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。
控制台身份验证 (Console Authentication) 字段	通过控制台端口连接到 FXOS CLI 时用于用户身份验证的方法。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。 • **Radius** - 必须在为 Firepower 机箱指定的 RADIUS 服务器上定义用户帐户。 • **TACACS** - 必须在为 Firepower 机箱指定的 TACACS+ 服务器上定义用户帐户。 • **LDAP** - 必须在为 Firepower 机箱指定的 LDAP/MS-AD 服务器上定义用户帐户。 • **无 (None)** - 如果用户帐户是 Firepower 机箱的本地帐户，则在用户使用控制台端口连接至 FXOS CLI 时无需密码。
远程用户设置	
远程用户角色策略	控制当用户尝试登录并且远程身份验证提供程序不向用户角色提供身份验证信息时发生的事情： • **分配默认角色 (Assign Default Role)** - 允许用户使用只读用户角色登录。 • **无登录 (No-Login)** - 不允许用户登录系统，即使用户名和密码正确也是如此。
本地用户设置	

名称	描述
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（请参阅面向密码的指导原则，第 23 页）。
History Count 字段	用户可创建的密码数量。超过此数量后，使用只能使用先前已使用过的旧密码。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。
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。
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。
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。
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 **Change During Interval** 属性设置为 **Disable**，该时间间隔将被忽略。

步骤 4 点击**保存 (Save)**。

配置会话超时

您可以使用 FXOS CLI 来指定在无用户活动的情况下 Firepower 4100/9300 机箱关闭用户会话前可以经过的时间量。您可以为控制台会话以及 HTTPS、SSH 和 Telnet 会话配置不同的设置。

您可以设置最高为 3600 秒（60 分钟）的超时值。默认值为 600 秒。要禁用此设置，请将会话超时值设为 0。

过程

步骤 1 进入安全模式：
Firepower-chassis # **scope security**

步骤 2 进入默认授权安全模式：
Firepower-chassis /security # **scopedefault-auth**

步骤 3 为 HTTPS、SSH 和 Telnet 会话设置空闲超时：
Firepower-chassis /security/default-auth # **set session-timeout** *seconds*

步骤 4 （可选）为控制台会话设置空闲超时：
Firepower-chassis /security/default-auth # **set con-session-timeout** *seconds*

步骤 5 （可选）查看会话和绝对会话超时设置：
Firepower-chassis /security/default-auth # **show detail**

示例：

```
Default authentication:
 Admin Realm: Local
 Operational Realm: Local
 Web session refresh period(in secs): 600
 Session timeout(in secs) for web, ssh, telnet sessions: 600
 Absolute Session timeout(in secs) for web, ssh, telnet sessions: 3600
 Serial Console Session timeout(in secs): 600
 Serial Console Absolute Session timeout(in secs): 3600
 Admin Authentication server group:
 Operational Authentication server group:
 Use of 2nd factor: No
```

配置绝对会话超时

Firepower 4100/9300 机箱具有绝对会话超时设置，即系统会在绝对会话超时期限已过后关闭用户会话，而不考虑会话是否在使用。此绝对超时功能具全局性，适用于所有形式的访问（包括串行控制台、SSH 和 HTTPS）。

您可以为串行控制台会话单独配置绝对会话超时。这允许针对调试需求禁用串行控制台绝对会话超时，同时保持其他访问形式的超时。

绝对超时值默认为3600秒（60分钟），可使用FXOS CLI进行更改。要禁用此设置，请将绝对会话超时值设为0。

过程

步骤1 进入安全模式：
Firepower-chassis # **scope security**

步骤2 进入默认授权安全模式：
Firepower-chassis /security # **scopedefault-auth**

步骤3 设置绝对会话超时：
Firepower-chassis /security/default-auth # **set absolute-session-timeout** *seconds*

步骤4 （可选）设置单独的控制台绝对会话超时：
Firepower-chassis /security/default-auth # **set con-absolute-session-timeout** *seconds*

步骤5 （可选）查看会话和绝对会话超时设置：
Firepower-chassis /security/default-auth # **show detail**

示例：

```
Default authentication:
 Admin Realm: Local
 Operational Realm: Local
 Web session refresh period(in secs): 600
 Session timeout(in secs) for web, ssh, telnet sessions: 600
 Absolute Session timeout(in secs) for web, ssh, telnet sessions: 3600
 Serial Console Session timeout(in secs): 600
 Serial Console Absolute Session timeout(in secs): 3600
 Admin Authentication server group:
 Operational Authentication server group:
 Use of 2nd factor: No
```

设置最大尝试登录次数

您可配置允许用户尝试登录的最大失败次数，如果超过该次数，用户会被Firepower 4100/9300机箱锁定一段指定的时间长度。如果用户超过设置的最大尝试登录次数，用户会被系统锁定。系统不会显示表明用户被锁定的通知。在这种情况下，用户必须等待一段指定的时间长度，然后才能尝试登录。

执行以下步骤，配置最大登录尝试次数。

注释

- 在超过最大尝试登录次数后，所有类型的用户帐户（包括管理员帐户）均被锁定。
- 默认的最大尝试登录失败次数为0。在超过最大尝试登录次数后，用户被系统锁定的默认时间长度为 15 分钟（900 秒）。
- 有关查看用户锁定状态和清除用户锁定状态的步骤，请参阅 查看和清除用户锁定状态，第 32 页。

这是为实现系统的通用标准认证合规性提供的众多选项之一。有关详细信息，请参阅安全认证合规性，第 43 页。

过程

步骤 1 从 FXOS CLI 进入安全模式：
scopesystem

scopesecurity

步骤 2 设置最大尝试登录失败次数。
setmax-login-attempts

max_login
max_login 值可以是 0 到 10 之间的任何整数。

步骤 3 指定在达到最大尝试登录次数后用户应被系统锁定的时间长度（以秒为单位）：
setuser-account-unlock-time

unlock_time

步骤 4 提交配置：
commit-buffer

查看和清除用户锁定状态

对于超过 Maximum Number of Login Attempts CLI 设置中指定的最大失败登录尝试次数之后被 Firepower 4100/9300 机箱锁定的用户，管理员用户可查看和清除其锁定状态。有关详细信息，请参阅设置最大尝试登录次数，第 31 页。

过程

步骤 1 从 FXOS CLI 进入安全模式：
scopesystem

scopesecurity

步骤 2 显示相关用户的用户信息（包括锁定状态）：
Firepower-chassis /security # **show local-user** *user***detail**

示例：

```
Local User user:
 First Name:
 Last Name:
 Email:
 Phone:
 Expiration: Never
 Password:
 User lock status: Locked
 Account status: Active
 User Roles:
 Name: read-only
 User SSH public key:
```

步骤 3 （可选）清除用户锁定状态：
Firepower-chassis /security # **scope local-user** *user*

Firepower-chassis /security/local-user # **clear lock-status**

配置最小密码长度检查

如果启用最小密码长度检查，则必须最少使用指定数目的字符创建密码。例如，如果将 *min_length* 选项设为 15，则用户必须使用 15 个或更多字符创建密码。此选项是在系统上用于实施通用标准认证合规性的众多选项之一。有关详细信息，请参阅安全认证合规性，第 43 页。

执行以下步骤以配置最小密码长度检查。

过程

步骤 1 从 FXOS CLI 进入安全模式：

步骤 2 **scopesystem**
scopesecurity

步骤 3 进入密码配置文件安全模式：
scopepassword-profile

步骤 4 指定最小密码长度：
setmin-password-length *min_length*

步骤 5 提交配置：
commit-buffer

创建本地用户帐户

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（请参阅面向用户名的指导原则，第 22 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。
名字字段	用户的名字。该字段最多包含 32 个字符。
姓氏字段	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。
密码字段	与此帐户关联的密码。如果启用密码强度检查，则用户的密码必须为强密码，Firepower 可扩展操作系统会拒绝任何不满足强度检查要求的密码（请参阅面向密码的指导原则，第 23 页）。
确认密码字段	第二次用于确认目的的密码。
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 26 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。

名称	描述
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 **Add**。

删除本地用户帐户

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 在与您想要删除的用户帐户对应的行中，点击**删除 (Delete)**。

步骤 4 在**确认 (Confirm)** 对话框中，点击**是 (Yes)**。

激活或停用本地用户帐户

您必须是拥有管理员或 AAA 权限的用户，才能激活或停用本地用户帐户。

过程

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

步骤 2 点击**本地用户 (Local Users)** 选项卡。

步骤 3 在您要激活或停用的用户帐户所在的行中，点击**编辑 (Edit)**（铅笔图标）。

步骤 4 在**编辑用户 (Edit User)** 对话框中，执行以下操作之一：

- 要激活用户帐户，请点击**帐户状态 (Account Status)** 字段中的**活动 (Active)** 单选按钮。

- 要停用用户帐户，请点击**帐户状态 (Account Status)** 字段中的**非活动 (Inactive)** 单选按钮。

管理员用户帐户始终设置为活动。不能修改。

步骤 5 点击**保存 (Save)**。

清除本地身份验证的用户的密码历史记录

过程

步骤 1 进入安全模式：
Firepower-chassis # **scopesecurity**

步骤 2 进入已指定用户帐户的本地用户安全模式：
Firepower-chassis /security # **scope local-user** *user-name*

步骤 3 清除已指定用户帐户的密码历史记录：
Firepower-chassis /security/local-user # **clear password-history**

步骤 4 将任务提交到系统配置：
Firepower-chassis /security/local-user # **commit-buffer**

以下示例将清除密码历史记录并提交任务：

```
Firepower-chassis # scope security
Firepower-chassis /security # scope local-user admin
Firepower-chassis /security/local-user # clear password-history
Firepower-chassis /security/local-user* # commit-buffer
Firepower-chassis /security/local-user #
```

第 5 章

映像管理

关于映像管理

Firepower 4100/9300 机箱使用的映像分为两个基本类型：

注释 所有映像都可通过安全启动进行数字签名和验证。请勿以任何方式修改映像，否则系统会报告验证错误。

- 平台捆绑包 (Platform Bundle) - Firepower 平台捆绑包是一系列运行在 Firepower 管理引擎和 Firepower 安全模块/引擎上的多个独立映像。平台捆绑包是 Firepower 可扩展操作系统软件包。
- 应用 (Application) - 应用是您想在 安全模块/引擎的Firepower 4100/9300 机箱上部署的软件映像。应用映像作为思科安全数据包文件 (CSP) 进行交付，在部署到安全模块/引擎之前，存储在管理引擎上，参与逻辑设备创建，或者为稍后的逻辑设备创建做准备。您可以在 Firepower 管理引擎上存储相同应用映像类型的多个不同版本。

注释 如果您正在升级平台捆绑包映像和一个或多个应用映像，必须首先升级平台捆绑包。

从 Cisco.com 下载映像

开始之前

您必须有 Cisco.com 帐户。

过程

步骤 1 选择**系统 (System)** > **更新 (Updates)**。
“可用更新 (Available Updates)”页面显示机箱上可用的 FXOS 平台捆绑包映像和应用映像列表。

步骤 2 点击页面底部的**从 CCO 下载最新更新 (Download latest updates from CCO)** 链接。
Firepower 4100/9300 机箱的软件下载页面可在浏览器中的新标签中打开。

步骤 3 查找适当的软件映像，然后将其下载到本地计算机。

将映像上传到 Firepower 安全设备

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 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 可扩展操作系统 平台捆绑包映像和应用映像列表。

步骤 2 点击**上传映像 (Upload Image)**，可打开“上传映像 (Upload Image)”对话框。

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**。
已选中的映像被上传到 Firepower 4100/9300 机箱。

步骤 5 对于某些软件映像，上传映像后，系统将显示一份最终用户许可协议。请按照系统提示接受这份最终用户许可协议。

验证映像的完整性

将新的映像添加至 Firepower 4100/9300 机箱 后，系统自动验证映像的完整性。如果需要，您可以使用以下过程手动验证映像的完整性。

过程

步骤 1 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 可扩展操作系统 平台捆绑包映像和应用映像列表。

步骤 2 点击与您要验证映像相对应的**验证 (Verify)**（复选标记图标）。
系统将验证映像的完整性并在“映像完整性 (Image Integrity)”字段中显示状态。

升级Firepower 可扩展操作系统平台捆绑包

开始之前

从 Cisco.com 下载平台捆绑包软件映像（请参阅从 Cisco.com 下载映像，第 38 页），然后将此映像上传到 Firepower 4100/9300 机箱（请参阅将映像上传到 Firepower 安全设备，第 38 页）。

注释 升级过程通常需要 20 到 30 分钟。

如果要升级运行独立逻辑设备的 Firepower 9300 或 Firepower 4100 系列安全设备，或者如果要升级运行机箱内集群的 Firepower 9300 安全设备，则升级期间流量不会通过该设备。

如果要升级属于某机箱间集群的 Firepower 9300 或 Firepower 4100 系列安全设备，则升级期间流量不会通过正在升级的设备。但是，该集群中的其他设备将继续传输流量。

过程

步骤 1 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 可扩展操作系统 平台捆绑包映像和应用映像列表。

步骤 2 点击想要升级到的 FXOS 平台捆绑包所对应的**升级 (Upgrade)**。
系统将首先验证想要安装的软件包。它会告知您当前已安装的应用与指定的 FXOS 平台软件包之间的所有不兼容。此外，它还会警告您，在升级过程中，任何现有会话都将终止，系统将需要重启。

步骤 3 点击**是 (Yes)**，确认您想要继续安装，或者点击**否 (No)** 取消安装。
Firepower 可扩展操作系统打开捆绑包，升级/重新加载组件。

更新逻辑设备的映像版本

开始之前

注释 在初始创建 Firepower 威胁防御逻辑设备后，您将无法使用 Firepower 机箱管理器或 FXOS CLI升级 Firepower 威胁防御逻辑设备。要升级 Firepower 威胁防御逻辑设备，您必须使用 Firepower 管理中心。有关详细信息，请参阅《Firepower 系统版本说明》:http://www.cisco.com/c/en/us/support/security/defense-center/products-release-notes-list.html。

另请注意，Firepower 威胁防御逻辑设备的任何更新都不会反映在 Firepower 机箱管理器的 **Logical Devices** > **Edit** 和 **System** > **Updates** 页面上。在这些页面上，显示的版本表示用于创建 Firepower 威胁防御逻辑设备的软件版本（CSP 映像）。

从 Cisco.com 下载要用于逻辑设备的应用映像（请参阅从 Cisco.com 下载映像，第 38 页），然后将映像上传到 Firepower 4100/9300 机箱（请参阅将映像上传到 Firepower 安全设备，第 38 页）。

如果您正在升级平台捆绑包映像和一个或多个应用映像，必须首先升级平台捆绑包。

过程

步骤 1 选择**逻辑设备 (Logical Devices)** 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。

步骤 2 点击想要更新的逻辑设备对应的**更新版本 (Update Version)**，可打开**更新映像版本 (Update Image Version)** 对话框。

步骤 3 对于**新版本 (New Version)**，选择想要更新的软件版本。

步骤 4 点击 **OK**。

固件升级

使用以下操作步骤升级 Firepower 4100/9300 机箱上的固件。

过程

步骤 1 使用网络浏览器导航至 http://www.cisco.com/go/firepower9300-software 或 http://www.cisco.com/go/firepower4100-software。
系统将在浏览器中打开 Firepower 4100/9300 机箱的软件下载页面：

步骤 2 从 Cisco.com 查找，然后将合适的固件包下载到您可从 Firepower 4100/9300 机箱访问的服务器。

步骤 3 在 Firepower 4100/9300 机箱上，进入固件模式：

Firepower-chassis # **scopefirmware**

步骤 4 将 FXOS 固件映像下载到 Firepower 4100/9300 机箱：
Firepower-chassis /firmware # **download image** *URL*

使用以下语法之一，为正在导入的文件指定 URL：

- **ftp**:// *username@hostname* / *path*
- **scp**:// *username@hostname* / *path*
- **sftp**:// *username@hostname* / *path*
- **tftp**:// *hostname* : *port-num* / *path*

步骤 5 要监控下载过程，请执行以下操作：
Firepower-chassis /firmware # **show download task** *image_name* **detail**

步骤 6 下载完成后，可输入以下命令查看固件包的内容：
Firepower-chassis /firmware # **show package** *image_name* **expand**

步骤 7 可输入以下命令查看固件包的版本号：
Firepower-chassis /firmware # **show package**

当安装固件包时，在以下步骤中使用此版本号：

步骤 8 要安装固件包：

a) 进入固件安装模式：
Firepower-chassis /firmware # **scope firmware-install**

b) 安装固件包：
Firepower-chassis /firmware/firmware-install # **install firmware pack-version** *version_number*

系统将验证固件包，并通知您验证过程可能需要几分钟才能完成。

c) 点击**yes** 继续验证。
固件包验证完成后，系统将通知您安装过程可能需要几分钟才能完成，并且系统在更新过程中将重启。

d) 点击**yes** 继续安装。升级流程中请勿重启 Firepower 4100/9300 机箱。

步骤 9 要监控升级流程，请执行以下操作：
Firepower-chassis /firmware/firmware-install # **show detail**

步骤 10 安装完成后，可输入以下命令查看当前固件版本：
Firepower-chassis /firmware/firmware-install # **top**

Firepower-chassis # **scope chassis 1**

Firepower-chassis /firmware # **show sup version**

下面的示例将固件升级到了版本 1.0.10：

```
Firepower-chassis# scope firmware
Firepower-chassis /firmware # download image
tftp://10.10.10.1/fxos-k9-fpr9k-firmware.1.0.10.SPA
Firepower-chassis /firmware # show download-task fxos-k9-fpr9k-firmware.1.0.10.SPA detail
```

```
Download task:
    File Name: fxos-k9-fpr9k-firmware.1.0.10.SPA
    Protocol: Tftp
    Server: 10.10.10.1
    Port: 0
    Userid:
    Path:
    Downloaded Image Size (KB): 2104
    Time stamp: 2015-12-04T23:51:57.846
    State: Downloading
    Transfer Rate (KB/s): 263.000000
    Current Task: unpacking image fxos-k9-fpr9k-firmware.1.0.10.SPA on primary(
FSM-STAGE:sam:dme:FirmwareDownloaderDownload:UnpackLocal)

Firepower-chassis /firmware # show package fxos-k9-fpr9k-firmware.1.0.10.SPA expand

Package fxos-k9-fpr9k-firmware.1.0.10.SPA:
    Images:
        fxos-k9-fpr9k-fpga.1.0.5.bin
        fxos-k9-fpr9k-rommon.1.0.10.bin

Firepower-chassis /firmware # show package

Name                                       Version
------------------------------------------ -------
fxos-k9-fpr9k-firmware.1.0.10.SPA          1.0.10

Firepower-chassis /firmware # scope firmware-install
Firepower-chassis /firmware/firmware-install # install firmware pack-version 1.0.10

Verifying FXOS firmware package 1.0.10. Verification could take several minutes.
Do you want to proceed? (yes/no):yes

FXOS SUP ROMMON: Upgrade from 1.0.10 to 1.0.10
FXOS SUP FPGA  : Upgrade from 1.04 to 1.05

This operation upgrades SUP firmware on Security Platform.
Here is the checklist of things that are recommended before starting the install operation
(1) Review current critical/major faults
(2) Initiate a configuration backup

Attention:
   The system will be reboot to upgrade the SUP firmware.
   The upgrade operation will take several minutes to complete.
   PLEASE DO NOT POWER RECYCLE DURING THE UPGRADE.
Do you want to proceed? (yes/no):yes

Upgrading FXOS SUP firmware software package version 1.0.10

command executed
```

第 6 章

安全认证合规性

安全认证合规性

美国联邦政府机构有时需要仅使用符合由美国国防部和全球认证组织建立的安全标准的设备和软件。Firepower 4100/9300 机箱支持符合其中若干安全认证标准。

请参阅以下主题，了解支持符合这些标准的功能的启用步骤：

- 关于证书吊销列表检查，第 51 页
- 配置 CRL 定期下载，第 55 页
- 启用 NTP 服务器身份验证，第 57 页
- 设置 LDAP 密钥环证书，第 58 页
- 配置 IP 访问列表，第 59 页
- 启用客户端证书身份验证，第 59 页
- 配置最小密码长度检查，第 33 页
- 设置最大尝试登录次数，第 31 页
- 用户角色，第 26 页

注释 请注意，这些主题只讨论在 Firepower 4100/9300 机箱上启用认证合规性。在 Firepower 4100/9300 机箱上启用认证合规性不会导致合规性自动传播到与之连接的任何逻辑设备。

启用 FIPS 模式

执行以下步骤以在 Firepower 4100/9300 机箱 上启用 FIPS 模式。

过程

步骤 1 以管理员用户身份登录 Firepower 4100/9300 机箱。

步骤 2 选择 **Platform Settings** 以打开“平台设置 (Platform Settings)”页面。

步骤 3 选择 **FIPS/CC mode**以打开“FIPS 和常用标准 (FIPS and Common Criteria)”窗口。

步骤 4 选中 FIPS 所对应的**Enable** 复选框。

步骤 5 点击**Save** 保存配置。

步骤 6 按照提示重新启动系统。

接下来的操作

在 FXOS 版本 2.0.1 之前，首次设置设备时创建的现有 SSH 主机密钥被硬编码为 1024 位。要符合 FIPS 和通用标准认证需求，您必须销毁此旧主机密钥，并使用生成 SSH 主机密钥，第 45 页中的详细操作步骤生成新的主机密钥。如果不执行这些附加步骤，则在FIPS模式启用的情况下，设备重新启动后，将无法使用 SSH 连接到管理引擎。如果您使用 FXOS 2.0.1 或更高版本执行初始设置，则无需生成新的主机密钥。

启用通用标准模式

执行以下步骤，在 Firepower 4100/9300 机箱 上启用通用标准模式。

过程

步骤 1 以管理员用户身份登录 Firepower 4100/9300 机箱。

步骤 2 选择 **Platform Settings** 以打开“平台设置 (Platform Settings)”页面。

步骤 3 选择 **FIPS/CC mode**以打开“FIPS 和常用标准 (FIPS and Common Criteria)”窗口。

步骤 4 选中“通用标准”(Common Criteria) 所对应的**Enable** 复选框。

步骤 5 点击**Save** 保存配置。

步骤 6 按照提示重新启动系统。

接下来的操作

在 FXOS 版本 2.0.1 之前，首次设置设备时创建的现有 SSH 主机密钥被硬编码为 1024 位。要符合 FIPS 和通用标准认证需求，您必须销毁此旧主机密钥，并使用生成 SSH 主机密钥，第 45 页中的详细操作步骤生成新的主机密钥。如果不执行这些附加步骤，则在“通用标准 (Common Criteria)”模式启用的情况下，设备重新启动后，将无法使用 SSH 连接到管理引擎。如果您使用 FXOS 2.0.1 或更高版本执行初始设置，则无需生成新的主机密钥。

生成 SSH 主机密钥

在 FXOS 版本 2.0.1 之前，设备初始设置期间创建的现有 SSH 主机密钥被硬编码为 1024 位。要符合 FIPS 和通用标准认证需求，您必须销毁此旧主机密钥并生成新的主机密钥。有关详细信息，请参阅启用 FIPS 模式，第 44 页或启用通用标准模式，第 45 页。

执行以下步骤，以销毁旧的 SSH 主机密钥并生成新的符合认证证书要求的主机密钥。

过程

步骤 1 从 FXOS CLI 进入服务模式：
scopesystem

scopeservices

步骤 2 删除 SSH 主机密钥：
deletessh-serverhost-key

步骤 3 提交配置：
commit-buffer

步骤 4 将 SSH 主机密钥长度设置为 2048 位：

setssh-serverhost-keyrsa 2048

步骤 5 提交配置：
commit-buffer

步骤 6 创建新的 SSH 主机密钥：
createssh-serverhost-key

commit-buffer

步骤 7 确认新的主机密钥长度：
showssh-serverhost-key

主机密钥长度：2048

配置 IPSec 安全通道

您可以在 Firepower 4100/9300 机箱上配置 IPSec，对通过公用网络的数据包提供端到端数据加密和身份验证服务。这是为实现系统的通用标准认证合规性提供的众多选项之一。有关详细信息，请参阅安全认证合规性，第 43 页。

注释 如果选择配置执行 IKE 和 SA 连接间加密密钥强度的匹配（在以下步骤中将 sa-strength-enforcement 设为 yes）：

启用 SA 执行后：	在 IKE 协商的密钥大小小于 ESP 协商的密钥大小时，连接失败。 IKE 协商的密钥大小大于或等于 ESP 协商的密钥大小时，SA 执行检查通过并且连接成功。
禁用 SA 执行后：	SA 执行检查通过且连接成功。

执行这些步骤，以配置 IPSec 安全通道。

过程

步骤 1 从 FXOS CLI 进入安全模式：
scopesystem

scopesecurity

步骤 2 创建密钥环：
enterkeyringssp

!createcertreqsubject-name *subject-name***ip** *ip*

步骤 3 输入关联的证书请求信息：
entercertreq

步骤 4 设置国家/地区：
setcountry 国家/地区

步骤 5 设置 DNS：
setdns *dns*

步骤 6 设置邮件：
sete-mail 电子邮件

步骤 7 设置 IP 信息：
setfi-a-ip *fi-a-ip*

setfi-a-ipv6 *fi-a-ipv6*

setfi-b-ip *fi-b-ip*

setfi-b-ipv6 *fi-b-ipv6*

setipv6 *ipv6*

步骤 8 设置位置：
setlocality *locality*

步骤 9 设置组织名称：
setorg-name *org-name*

步骤 10 设置组织单位名称：
setorg-unit-name *org-unit-name*

步骤 11 设置密码：
!setpassword

步骤 12 设置状态：
setstate *state*

步骤 13 设置 certreq 的主题名称：
setsubject-name *subject-name*

步骤 14 退出：
exit

步骤 15 设置模数：
setmodulus *modulus*

步骤 16 设置证书请求的重新生成：
setregenerate *{ yes | no }*

步骤 17 设置信任点：
settrustpointinterca

步骤 18 退出：
exit

步骤 19 输入新创建的信任点：
entertrustpointinterca

步骤 20 生成证书签名请求：
setcertchain

示例：

```
-----BEGIN CERTIFICATE-----
MIIF3TCCA8WgAwIBAgIBADANBgkqhkiG9w0BAQsFADBwMQswCQYDVQQGEwJVUzEL
MAkGA1UECAwCQ0ExDDAKBgNVBAcMA1NKQzEOMAwGA1UECgwFQ2lzY28xDTALBgNV
BAsMBFNUQlUxCzAJBgNVBAMMAkNBMRowGAYJKoZIhvcNAQkBFgtzc3BAc3NwLm5l
dDAeFw0xNjEyMDgxOTMzNTJaFw0yNjEyMDYxOTMzNTJaMHAxCzAJBgNVBAYTAlVT
MQswCQYDVQQIDAJDQTEMMAoGA1UEBwwDU0pDMQ4wDAYDVQQKDAVDaXNjbzENMAsG
A1UECwwEU1RCVTELMAkGA1UEAwwCQ0ExGjAYBgkqhkiG9w0BCQEWC3NzcEBzc3Au
bmV0MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA2ukWyMLQuLqTvhq7
zFb3Oz/iyDG/ui6mrLIYn8wE3E39XcXA1/x9IHCmxFKNJdD7EbsggfOuy0Bj+Y4s
+uZ1VapBXV/JrAie7bNn3ZYrI29yuyOrIqoi9k9gL/oRBzH18BwBwGHBOz3hGrSK
Yc2yhsq9y/6yI3nSuLZm6ybmUKjTa+B4YuhDTz4hl/I9x/J5nbGiab3vLDKss1nO
xP9+1+Lc690Vl8/mNPWdjCjDI+U/L9keYs/rbZdRSeXy9kMae42+4FlRHDJjPcSN
Yw1g/gcR2F7QUKRygKckJKXDX2QIiGYSctlSHj18O87o5s/pmQAWWRGkKpfDv3oH
cMPgI2T9rC0D8NNcgPXj9PFKfexoGNGwNTO85fK3kjgMOdWbdeMG3EihxEEOUPD0
Fdu0HrTM5lvwb+vr5wE9HsAiMJ8UuujmHqH5mlwyy3Me+cEDHo0hLeNs+AFrqEXQ
e9S+KZC/dq/9zOLpRsVqSfJsAuVl/QdPDbWShjflE/fP2Wj01PqXywQydzymVvgE
wEZaoFg+mlGJm0+q4RDvnpzEviOYNSAGmOkILh5HQ/eYDcxvd0qbORWb31H32ySl
Ila6UTT9+vnND1f838fxvNvr8nyGD2S/LVaxnZlO4jcSIvtdizbbT8u5B4VcLKIC
x0vkqjo6RvNZJ52sUaD9C3UodTUCAwEAAaOBgTB/MC8GA1UdHwQoMCYwJKAioCCG
Hmh0dHA6Ly8xOTIuMTY4LjQuMjkvcm9vdGNhLmNybDAdBgNVHQ4EFgQU7Jg01A74
jpx8U0APk76pVfYQQ5AwHwYDVR0jBBgwFoAU7Jg01A74jpx8U0APk76pVfYQQ5Aw
DAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAgEAvI8ky2jiXc4wPiMuxIfY
W7DRmszPUWQ7edor7yxuCqzHLVFFOwYRudsyXbv7INR3rJ/X1cRQj9+KidWWVxpo
pFahRhzYxVZ10DHKIzGTQS3jiHgrF3Z8ohWbL15L7PEDlrxMBoJvabPeQRgTmY/n
XZJ7qRYbypO3gUMCaCZ12raJc3/DIpBQ29yweCbUkc9qiHKA0IbnvAxoroHWmBld
94LrJCggfMQTuNJQszJiVVsYJfZ+utlDp2QwfdDv7B0JkwTBjdwRSfotEbc5R18n
BNXYHqxuoNMmqbS3KjCLXcH6xIN8t+UkfP89hvJt/fluJ+s/VJSVZWK4tAWvR7wl
QngCKRJW6FYpzeyNBctiJ07wO+Wt4e3KhIjJDYvA9hFixWcVGDf2r6QW5BYbgGOK
DkHb/gdr/bcdLBKN/PtSJ+prSrpBSaA6rJX8D9UmfhqqN/3f+sS1fM4qWORJc6G2
gAcg7AjEQ/0do512vAI8p8idOg/Wv1O17mavzLpcue05cwMCX9fKxKZZ/+7Pk19Y
ZrXS6uMn/CGnViptn0w+uJ1IRj1oulk+/ZyPtBvFHUkFRnhoWj5SMFyds2IaatyI
47N2ViaZBxhU3GICaH+3O+8rs9Kkz9tBZDSnEJVZA6yxaNCVP1bRUO20G3oRTmSx
8iLBjN+BXggxMmG8ssHisgw=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFqDCCA5CgAwIBAgIBBDANBgkqhkiG9w0BAQsFADBwMQswCQYDVQQGEwJVUzEL
MAkGA1UECAwCQ0ExDDAKBgNVBAcMA1NKQzEOMAwGA1UECgwFQ2lzY28xDTALBgNV
BAsMBFNUQlUxCzAJBgNVBAMMAkNBMRowGAYJKoZIhvcNAQkBFgtzc3BAc3NwLm5l
dDAeFw0xNjEyMTUyMTM0NTRaFw0yNjEyMTMyMTM0NTRaMHwxCzAJBgNVBAYTAlVT
MQswCQYDVQQIDAJDQTEPMA0GA1UECgwGbmV3c3RnMRAwDgYDVQQLDAduZXdzdGJ1
MRMwEQYDVQQDDApbnRlcm0xLWNhMSgwJgYJKoZIhvcNAQkBFhlpbnRlcm0xLWNh
QGludGVybTEtY2EubmV0MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA
wLpNnyEx5I4P8uDoWKWF3IZsegjhLANsodxuAUmhmwKekd0OpZZxHMw1wSO4IBX5
4itJS0xyXFzPmeptG3OXvNqCcsT+4BXl3DoGgPMULccc4NesHeg2z8+q3SPA6uZh
iseWNvKfnUjixbQEBtcrWBiSKnZuOz1cpuBn34gtgeFFoCEXN+EZVpPESiancDVh
8pCPlipc/08ZJ3o9GW2j0eHJN84sguIEDL812ROejQvpmfqGUq11stkIIuh+wB+V
VRhUBVG7pV57I6DHeeRp6cDMLXaM3iMTelhdShyo5YUaRJMak/t8kCqhtGXfuLlI
E2AkxKXeeveR9n6cpQd5JiNzCT/t9IQL/T/CCqMICRXLFpLCS9o5S5O2B6QFgcTZ
```

```
yKR6hsmwe22wpK8QI7/5oWNXlolb96hHJ7RPbG7RXYqmcLiXY/d2j9/RuNoPJawI
hLkfhoIdPA28xlnfIB1azCmMmdPcBO6cbUQfCj5hSmk3StVQKgJCjaujz55TGGd1
GjnxDMX9twwz7Ee51895Xmtr24qqaCXJoW/dPhcIIXRdJPMsTJ4yPG0BieuRwd0p
i8w/rFwbHzv4C9Fthw1JrRxH1yeHJHrLlZgJ5txSaVUIgrgVCJaf6/jrRRWoRJwt
AzvnzYql2dZPCcEAYgP7JcaQpvdpuDgq++NgBtygiqECAwEAAaNBMD8wDAYDVR0T
BAUwAwEB/zAvBgNVHR8EKDAmMCSgIqAghh5odHRwOi8vMTkyLjE2OC40LjI5L2lu
dGVybS5jcmwwDQYJKoZIhvcNAQELBQADggIBAG/XujJh5G5UWo+cwTSitAezWbJA
h1dAiXZ/OYWZSxkFRliErKdupLqL0ThjnX/wRFfEXbrBQwm5kWAUUDr97D1Uz+2A
8LC5I8SWKXmyf0jUtsnEQbDZb33oVL7yXJk/A0SF0jihpPheMA+YRazalT9xj9KH
PE7nHCJMbb2ptrHUyvBrKSYrSeEqOpQU2+otnFyV3rS9aelgVjuaWyaWOc3lZ1Oi
CC2tJvY3NnM56j5iesxUCeY/SZ2/ECXN7RRBViLHmA3gFKmWf3xeNiKkxmJCxOaa
UWPC1x2V66I8DG9uUzlWyd79O2dy52aAphAHC6hqlzb6v+gw1Tld7UxaqVd8CD5W
ATjNs+ifkJS1h5ERxHjgcurZXOpR+NWpwF+UDzbMXxx+KAAXCI6ltCd8Pb3wOUC3
PKvwEXaIcCcxGx71eRLpWPZFyEoi4N2NGE9OXRjz0K/KERZgNhsIW3bQMjcw3aX6
OXskEuKgsayctnWyxVqNnqvpuz06kqyubh4+ZgGKZ5LNEXYmGNz3oED1rUN636Tw
SjGAPHgeROzyTFDixCei6aROlGdP/Hwvb0/+uThIe89g8WZ0djTKFUM8uBO3f+II
/cbuyBO1+JrDMq8NkAjxKlJlp1c3WbfCue/qcwtcfUBYZ4i53a56UNF5Ef0rpy/8
B/+07Me/p2y9Luqa
-----END CERTIFICATE-----
ENDOFBUF
```

步骤 21 显示证书签名请求：

showcertreq

示例：

```
Firepower-chassis# /security/keyring # show certreq
Certificate request subject name: SSP
Certificate request ip address: 192.168.0.111
Certificate request FI A ip address: 0.0.0.0
Certificate request FI B ip address: 0.0.0.0
Certificate request e-mail name:
Certificate request ipv6 address: ::
Certificate request FI A ipv6 address: ::
Certificate request FI B ipv6 address: ::
Certificate request country name: US
State, province or county (full name): CA
Locality name (eg, city): SJC
Organisation name (eg, company): Cisco
Organisational Unit Name (eg, section): Sec
DNS name (subject alternative name):
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIICwTCCAakCAQAwVTELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAkNBMQwwCgYDVQQH
DANTSkMxDjAMBgNVBAoMBUNpc2NvMQ0wCwYDVQQLDARTVEJVMQwwCgYDVQQDDANT
U1AwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDq292Rq3t0laoxPbfE
p/lTKr6rxFhPqSSbtm6sXer//VZFiDTWODockDItuf4Kja215mIS0RyvEYVeRgAs
wbN459wm0BASd8xCjIhsuHDV7yHu539BnvRW6Q2o+gHeSRwckqjClK/tsIxsPkV0
6OduZYXk2bnsLWs6tNk3uzOIT2Q0FcZ1ET66C8fyyKWTrmvcZjDjkMm2nDFsPlX9
39TYPItDkJE3PocqyaCqmT4uobOuvQeLJh/efkBvwhb4BF8vwzRpHWTdjjU5YnR1
qiR4q7j1RmzVFxCDY3IVP/KDBoa5NyCLEUZECP5QCQFDzIRETZwVOKtxUVG0Nljd
K5TxAgMBAAGgJzAlBgkqhkiG9w0BCQ4xGDAWMBQGA1UdEQQNMAuCA1NTUIcEwKgA
rjANBgkqhkiG9w0BAQsFAAOCAQEARtRBoInxXkBYNlVeEoFCqKttu3+Hc7UdyoRM
2L2pjx5OHbQICC+8NRVRMYujTnp67BWuUZZl03dGP4/lbN6bC9P3CvkZdKUsJkN0
m1Ye9dgz7MO/KEcosarmoMl9WB8LlweVdt6ycSdJzs9shOxwT6TAZPwL7gq/1ShF
RJh6sq5W9p6E0SjYefK62E7MatRjDjS8DXoxj6gfn9DqK15iVpkK2QqT5rneSGj+
```

```
R+20TcUnT0h/S5K/bySEM/3U1gFxQCOzbzPuHkj28kXAVczmTxXEkJBFLVduWNo6
DT3u0xImiPR1sqW1jpMwbhC+ZGDtvgKjKHToagup9+8R9IMcBQ==
-----END CERTIFICATE REQUEST-----
```

步骤 22 进入 IPSec 模式：
scopeipsec

步骤 23 设置日志冗长级别：
setlog-level *log_level*

步骤 24 创建并输入一个 IPSec 连接：
enterconnection *connection_name*

步骤 25 将 IPSec 模式设置为隧道或传输：
setmode *tunnel_or_transport*

步骤 26 设置本地 IP 地址：
setlocal-addr *ip_address*

步骤 27 设置远程 IP 地址：
setremote-addr *ip_address*

步骤 28 如果使用隧道模式，则设置远程子网：
setremote-subnet *ip/mask*

步骤 29 （可选）设置远程身份：
setremote-ike-ident *remote_identity_name*

步骤 30 设置密钥环名称：
setkeyring-name *name*

步骤 31 （可选）设置密钥环密码：
setkeyring-passwd 口令

步骤 32 （可选）设置 IKE-SA 生命周期（分钟）：
setike-rekey-time *minutes*

minutes 值可以是 60-1440（包含在内）之间的任何整数。

步骤 33 （可选）设置子 SA 生命周期（分钟）(30-480)：
setesp-rekey-time *minutes*

minutes 值可以是 30-480（包含在内）之间的任何整数。

步骤 34 （可选）设置初次连接期间重新传输序列的执行次数：
setkeyringtries *retry_number*

retry_number 值可以是 1-5（包含在内）之间的任何整数。

步骤 35 （可选）启用或禁用证书吊销列表检查：
setrevoke-policy *{ relaxed | strict }*

步骤 36 启用连接：
setadmin-stateenable

步骤 37 重新加载所有连接：

reload-conns

步骤 38 （可选）将现有信任点名称添加至 IPsec：
createauthority *trustpoint_name*

步骤 39 配置执行 IKE 和 SA 连接间加密密钥强度的匹配：
setsa-strength-enforcement *yes_or_no*

配置信任点静态 CRL

已吊销证书保留在证书吊销列表 (CRL) 中。客户端应用使用 CRL 检查服务器的身份验证。服务器应用利用 CRL 授予或拒绝来自不再受信任的客户端应用的访问请求。
您可配置 Firepower 4100/9300 机箱 以使用证书吊销列表 (CRL) 信息验证对等证书。这是为实现系统的通用标准认证合规性提供的众多选项之一。有关详细信息，请参阅安全认证合规性，第 43 页。

执行这些步骤以使用 CRL 信息验证对等证书。

过程

步骤 1 从 FXOS CLI 进入安全模式：
scopesecurity

步骤 2 进入信任点模式：
scopetrustpoint *trustname*

步骤 3 进入吊销模式：
scoperevoke

步骤 4 下载 CRL 文件：
importcrl *protocol://user_id@CA_or_CRL_issuer_IP*/tmp/*DoDCA1CRL1.crl*

步骤 5 （可选）显示 CRL 信息的导入过程状态：
showimport-taskdetail

步骤 6 将证书撤销方法设置为仅限于 CRL：
setcertrevokemethod{crl}

关于证书吊销列表检查

您可以在 IPSec、HTTPS 和安全 LDAP 连接中将证书吊销列表 (CRL) 检查模式配置为“严格”或“宽松”。

动态（非静态）CRL 信息从 X.509 证书的 CDP 信息中获取，并指示动态 CRL 信息。静态 CRL 信息由系统管理人员手动下载，并指示 FXOS 系统中的本地 CRL 信息。动态 CRL 信息的处理仅特定于证书链中当前正在处理的证书；静态 CRL 信息则应用于整个对等证书链。

有关启用或禁用对安全 IPSec、LDAP 和 HTTPS 连接的证书吊销检查的具体步骤，请参阅配置 IPSec 安全通道，第 46 页、创建 LDAP 提供程序，第 100 页和配置 HTTPS，第 94 页。

注释

- 如果“证书撤销检查模式 (Certificate Revocation Check Mode)”设置为“严格 (Strict)”，则仅当对等证书链具有级别 1 或更高级别时，静态 CRL 才适用。（例如，当对等证书链仅包含根 CA 证书和根 CA 证书签名的对等证书时。）
- 为 IPSec 配置静态 CRL 时，导入的 CRL 文件中必须具有“授权密钥标识符 (authkey) (Authority Key Identifier [authkey])”字段。否则，IPSec 会将其视为无效。
- 静态 CRL 优先于来自同一颁发者的动态 CRL。验证对等证书时，如果存在同一颁发者的有效（已确定）静态 CRL，则对等证书中的 CDP 会被忽略。

下表说明了连接结果，具体取决于证书吊销列表检查设置和证书验证。

表 *1*：无本地静态 *CRL* 时将“证书撤销检查模式 *(Certificate Revocation Check Mode)*”设置为“严格 *(Strict)*”

无本地静态 CRL	LDAP 连接	IPSec 连接	客户端证书身份验证
检查对等证书链	需要完整的证书链	需要完整的证书链	需要完整的证书链
检查对等证书链中的 CDP	需要完整的证书链	需要完整的证书链	需要完整的证书链
针对对等证书链的根 CA 证书执行 CDP 检查	是	不适用	是
对等证书链中的任何证书验证失败	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
在对等证书链中撤销了任何证书	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
某个 CDP 缺少对等证书链	连接失败，系统显示系统日志消息	对等证书：连接失败，系统显示系统日志消息 中间 CA：连接失败	连接失败，系统显示系统日志消息
某个 CDP CRL 在具有有效签名的对等证书链中为空	连接成功	连接成功	连接失败，系统显示系统日志消息

无本地静态 CRL	LDAP 连接	IPSec 连接	客户端证书身份验证
无法下载对等证书链中的任何 CDP	连接失败，系统显示系统日志消息	对等证书：连接失败，系统显示系统日志消息 中间 CA：连接失败	连接失败，系统显示系统日志消息
证书具有 CDP，但 CDP 服务器已关闭	连接失败，系统显示系统日志消息	对等证书：连接失败，系统显示系统日志消息 中间 CA：连接失败	连接失败，系统显示系统日志消息
证书具有 CDP，服务器已启动且 CDP 上具有 CRL，但 CRL 具有无效签名	连接失败，系统显示系统日志消息	对等证书：连接失败，系统显示系统日志消息 中间 CA：连接失败	连接失败，系统显示系统日志消息

表 *2*：具有本地静态 *CRL* 时将“证书撤销检查模式 *(Certificate Revocation Check Mode)*”设置为“严格 *(Strict)*”

具有本地静态 CRL	LDAP 连接	IPSec 连接
检查对等证书链	需要完整的证书链	需要完整的证书链
检查对等证书链中的 CDP	需要完整的证书链	需要完整的证书链
针对对等证书链的根 CA 证书执行 CDP 检查	是	不适用
对等证书链中的任何证书验证失败	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
在对等证书链中撤销了任何证书	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
一个 CDP 缺少对等证书链（证书链级别为 1）	连接成功	连接成功
对等证书链中的一个 CDP CRL 为空（证书链级别为 1）	连接成功	连接成功
无法下载对等证书链中的任何 CDP（证书链级别为 1）	连接成功	连接成功
证书具有 CDP，但 CDP 服务器已关闭（证书链级别为 1）	连接成功	连接成功

具有本地静态 CRL	LDAP 连接	IPSec 连接
证书具有 CDP，服务器已启动且 CRL 在 CDP 上，但 CRL 具有无效签名（证书链级别为 1）	连接成功	连接成功
对等证书链级别高于 1	连接失败，系统显示系统日志消息	如果与 CDP 结合，连接会成功 如果没有 CDP，连接会失败并生成系统日志消息

表 *3*：无本地静态 *CRL* 时将“证书撤销检查模式 *(Certificate Revocation Check Mode)*”设置为“释放 *(Relaxed)*”

无本地静态 CRL	LDAP 连接	IPSec 连接	客户端证书身份验证
检查对等证书链	完整的证书链	完整的证书链	完整的证书链
检查对等证书链中的 CDP	完整的证书链	完整的证书链	完整的证书链
针对对等证书链的根 CA 证书执行 CDP 检查	是	不适用	是
对等证书链中的任何证书验证失败	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
在对等证书链中撤销了任何证书	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
某个 CDP 缺少对等证书链	连接成功	连接成功	连接失败，系统显示系统日志消息
某个 CDP CRL 在具有有效签名的对等证书链中为空	连接成功	连接成功	连接成功
无法下载对等证书链中的任何 CDP	连接成功	连接成功	连接成功
证书具有 CDP，但 CDP 服务器已关闭	连接成功	连接成功	连接成功
证书具有 CDP，服务器已启动且 CRL 在 CDP 上，但 CRL 具有无效签名	连接成功	连接成功	连接成功

表 4：具有本地静态 *CRL* 时将“证书撤销检查模式 *(Certificate Revocation Check Mode)*”设置为“释放 *(Relaxed)*”

具有本地静态 CRL	LDAP 连接	IPSec 连接
检查对等证书链	完整的证书链	完整的证书链
检查对等证书链中的 CDP	完整的证书链	完整的证书链
针对对等证书链的根 CA 证书执行 CDP 检查	是	不适用
对等证书链中的任何证书验证失败	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
在对等证书链中撤销了任何证书	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
一个 CDP 缺少对等证书链（证书链级别为 1）	连接成功	连接成功
对等证书链中的一个 CDP CRL 为空（证书链级别为 1）	连接成功	连接成功
无法下载对等证书链中的任何 CDP（证书链级别为 1）	连接成功	连接成功
证书具有 CDP，但 CDP 服务器已关闭（证书链级别为 1）	连接成功	连接成功
证书具有 CDP，服务器已启动且 CRL 在 CDP 上，但 CRL 具有无效签名（证书链级别为 1）	连接成功	连接成功
对等证书链级别高于 1	连接失败，系统显示系统日志消息	如果与 CDP 结合，连接会成功 如果没有 CDP，连接会失败并生成系统日志消息

配置 CRL 定期下载

您可将系统配置为定期下载 (CRL)，以便每隔 1 至 24 小时使用新的 CRL 验证证书。

您可将以下协议和接口用于该功能：

- FTP
- SCP
- SFTP
- TFTP
- USB

注释

- 不支持 SCEP 和 OCSP。
- 每个 CRL 仅可配置一个定期下载。
- 每个信任点支持一个 CRL。

注释 您只能以一小时为间隔配置周期。

执行以下步骤，配置 CRL 定期下载。

开始之前

确保您已配置 Firepower 4100/9300 机箱 以使用 (CRL) 信息验证对等证书。有关详细信息，请参阅配置信任点静态 CRL，第 51 页。

过程

步骤 1 从 FXOS CLI 进入安全模式：
scopesecurity

步骤 2 进入信任点模式：
scopetrustpoint

步骤 3 进入吊销模式：
scoperevoke

步骤 4 编辑吊销配置：
shconfig

步骤 5 设置首选配置：

示例：

```
set certrevokemethod crl
set crl-poll-filename rootCA.crl
set crl-poll-path /users/myname
set crl-poll-period 1
set crl-poll-port 0
set crl-poll-protocol scp
```

```
! set crl-poll-pwd
set crl-poll-server 182.23.33.113
set crl-poll-user myname
```

步骤 6 退出配置文件：
exit

步骤 7 （可选）通过下载新 CRL 测试新配置：

示例：

```
Firepower-chassis /security/trustpoint/revoke # sh import-task

Import task:
File Name Protocol Server          Port      Userid        State
--------- -------- --------------- ---------- -------------- -----
rootCA.crl Scp     182.23.33.113   0         myname        Downloading
```

启用 NTP 服务器身份验证

执行以下步骤以在 Firepower 4100/9300 机箱 上启用 NTP 服务器身份验证。

注释

- 启用时，NTP 身份验证功能全局应用于所有已配置的服务器。
- 仅支持使用 SHA1 进行 NTP 服务器身份验证。
- 您需要密钥 ID 和密钥值，才能进行服务器身份验证。密钥 ID 用于告知客户端和服务器在计算消息摘要时要使用哪个密钥值。密钥值是使用 ntp-keygen 得出的固定值。

过程

步骤 1 下载 ntp 4.2.8p8。

步骤 2 在 **ntpd openssl** 启用时安装 NTP 服务器。

步骤 3 生成 NTP 密钥 ID 和密钥值：
ntp-keygen-M

使用这些生成的密钥执行以下步骤。

步骤 4 以管理员用户身份登录 Firepower 4100/9300 机箱。

步骤 5 选择 **Platform Settings** 以打开“平台设置 (Platform Settings)”页面。

步骤 6 在“设置时间来源 (Set Time Source)”区域，点击 **Use NTP server** 单选按钮。

步骤 7 使用生成的 SHA1 字符串和密钥添加 NTP 服务器。

步骤 8 点击**Save** 保存 NTP 服务器配置。

步骤 9 选中**Enable ntp-authentication** 复选框。

步骤 10 点击**Save**。

设置 LDAP 密钥环证书

您可配置安全的 LDAP 客户端密钥环证书，以便支持 Firepower 4100/9300 机箱 上的 TLS 连接。这是为实现系统的通用标准认证合规性提供的众多选项之一。有关详细信息，请参阅安全认证合规性，第 43 页。

注释 如果启用“通用标准 (Common Criteria)”模式，则必须启用 SSL，且必须使用服务器 DNS 信息创建密钥环证书。

如果为进入 LDAP 服务器启用 SSL，则系统在建立连接时会参考并检查密钥环信息。

LDAP 服务器信息必须是 CC 模式下用于安全 LDAP 连接（启用 SSL）的 DNS 信息。

执行以下步骤，配置安全的 LDAP 客户端密钥环证书：

过程

步骤 1 从 FXOS CLI 进入安全模式：
scopesecurity

步骤 2 进入 LDAP 模式：
scopeldap

步骤 3 进入 LDAP 服务器模式：
enterserver *{server_ip|server_dns}*

步骤 4 设置 LDAP 密钥环：
setkeyring *keyring_name*

步骤 5 提交配置：
commit-buffer

配置 IP 访问列表

默认情况下，Firepower 4100/9300 机箱 拒绝对本地 Web 服务器的所有访问。您必须使用每个 IP 块的允许服务列表配置 IP 访问列表。

IP 访问列表支持以下协议：

- HTTPS
- SNMP
- SSH

对于各 IP 地址块（v4 或 v6），可为各服务配置最多 25 个不同子网。子网 0 和前缀 0 允许无限访问服务。

过程

步骤 1 以管理员用户身份登录 Firepower 4100/9300 机箱。

步骤 2 选择 **Platform Settings**，以打开“平台设置 (Platform Settings)”页面。

步骤 3 选择 **Access List**，以打开“访问列表 (Access List)”区域。

步骤 4 在此区域中，您可以查看、添加和删除 IP 访问列表中列出的 IPv4 和 IPv6 地址。
要添加 IPv4 块，必须输入有效的 IPv4 IP 地址（前缀 [0-32] 长度）并选择协议。

要添加 IPv6 块，必须输入有效的 IPv6 IP 地址（前缀 [0-128] 长度）并选择协议。

启用客户端证书身份验证

您可使系统将客户端证书与 LDAP 结合使用，对 HTTPS 访问用户进行身份验证。Firepower 4100/9300 机箱 上的默认身份验证配置基于凭据。

注释 启用证书身份验证后，这是允许用于 HTTPS 的唯一一种身份验证形式。

客户端证书身份验证功能的 FXOS 2.1.1 版本不支持证书吊销检查。

客户端证书必须满足以下要求，才能使用此功能：

- 用户名必须包含在 X509 属性“证书持有者备用名称 - 邮件 (Subject Alternative Name - Email)”中。
- 客户端证书必须由已将其证书导入到管理引擎上的信任点的根 CA 签名。

过程

步骤 1 从 FXOS CLI 进入服务模式：
scopesystem

scopesecurity

步骤 2 （可选）查看 HTTPS 身份验证选项：
sethttpsauth-type

示例：

```
Firepower-chassis /system/services # set https auth-type
cert-auth Client certificate based authentication
cred-auth Credential based authentication
```

步骤 3 将 HTTPS 身份验证设为基于客户端：
sethttpsauth-typecert-auth

步骤 4 提交配置：
commit-buffer

第 7 章

系统管理

导致 Firepower 机箱管理器会话被关闭的系统更改

以下系统更改可能会导致系统自动将您从 Firepower 机箱管理器 注销：

- 如果您修改系统时间，使其改变超过 10 分钟
- 如果使用 Firepower 机箱管理器或 FXOS CLI 重新引导或关闭系统
- 如果您升级 Firepower 4100/9300 机箱上的 FXOS 版本
- 如果您启用或禁用 FIPS 或“通用标准”(Common Criteria) 模式。

注释

除了上述更改以外，如果一段时间没有任何活动的话，您会自动从系统注销。默认情况下，系统会在无活动 10 分钟后将您注销。要配置此超时设置，请参阅配置会话超时， 第 30 页。您还可以配置绝对超时设置，即便会话仍处于活动状态，该设置也可以在一段时间后将用户从系统中注销。要配置绝对超时设置，请参阅配置绝对会话超时， 第 30 页。

更改管理 IP 地址

开始之前

您可以从 FXOS CLI 更改 Firepower 4100/9300 机箱上的管理 IP 地址。

注释 更改管理 IP 地址后，您需要使用新地址重新建立到 Firepower 机箱管理器或 FXOS CLI的任何连接。

过程

步骤 1 连接到 FXOS CLI（请参阅访问 FXOS CLI，第 8 页）。

步骤 2 要配置 IPv4 管理 IP 地址，请执行以下操作：

a) 设置交换矩阵互联 a 的范围：
Firepower-chassis# **scopefabric-interconnecta**

b) 要查看当前管理 IP 地址，请输入以下命令：
Firepower-chassis /fabric-interconnect # **show**

c) 输入以下命令，配置新的管理 IP 地址和网关：
Firepower-chassis /fabric-interconnect # **setout-of-band staticip** *ip_address***netmask** *network_mask***gw** *gateway_ip_address*

d) 将任务提交到系统配置：
Firepower-chassis /fabric-interconnect* # **commit-buffer**

步骤 3 要配置 IPv6 管理 IP 地址，请执行以下操作：

a) 设置交换矩阵互联 a 的范围：
Firepower-chassis# **scopefabric-interconnecta**

b) 设置管理 IPv6 配置的范围：
Firepower-chassis /fabric-interconnect # **scopeipv6-config**

c) 要查看当前管理 IPv6 地址，请输入以下命令：
Firepower-chassis /fabric-interconnect/ipv6-config # **show ipv6-if**

d) 输入以下命令，配置新的管理 IP 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*

e) 将任务提交到系统配置：
Firepower-chassis /fabric-interconnect/ipv6-config* # **commit-buffer**

以下示例配置 IPv4 管理接口和网关：

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # show

Fabric Interconnect:
    ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
 Prefix Operability
    ---- --------------- --------------- --------------- ---------------- ----------------
 ------ -----------
    A    192.0.2.112     192.0.2.1       255.255.255.0   ::               ::
 64     Operable
Firepower-chassis /fabric-interconnect # set out-of-band static ip 192.0.2.111 netmask
255.255.255.0 gw 192.0.2.1
Warning: When committed, this change may disconnect the current CLI session
Firepower-chassis /fabric-interconnect* #commit-buffer
Firepower-chassis /fabric-interconnect #
```

以下示例配置 IPv6 管理接口和网关：

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # scope ipv6-config
Firepower-chassis /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
    IPv6 Address                            Prefix     IPv6 Gateway
    --------------------------------------- ---------- ------------
    2001::8998                              64         2001::1
Firepower-chassis /fabric-interconnect/ipv6-config # set out-of-band static ipv6 2001::8999
 ipv6-prefix 64 ipv6-gw 2001::1
Firepower-chassis /fabric-interconnect/ipv6-config* # commit-buffer
Firepower-chassis /fabric-interconnect/ipv6-config #
```

更改应用管理 IP

您可以从 FXOS CLI 更改连接到 Firepower 4100/9300 机箱的应用上的管理 IP 地址。为此，您必须首先在 FXOS 平台级别更改 IP 信息，然后在应用级别更改 IP 信息。

注释 尝试使用 Firepower 机箱管理器进行这些更改可能会导致服务中断。为了避免任何可能的服务中断，您必须使用 FXOS CLI 执行这些更改。

过程

步骤 1 连接到 FXOS CLI。（请参阅访问 FXOS CLI，第 8 页）。

步骤 2 将范围设置为逻辑设备：

scopessa

scopelogical-device *logical_device_name*

步骤 3 将范围设置为管理引导程序，并配置新的管理引导程序参数。请注意，配置之间存在差异：对于 ASA 逻辑设备的独立配置：

a) 输入逻辑设备管理引导程序：

scopemgmt-bootstrap *asa*

b) 输入插槽的 IP 模式：
scope *ipv4_or_6 slot_number* default

c) （仅限 IPv4）设置新的 IP 地址：
setip *ipv4_address***mask** *network_mask*

d) （仅限 IPv6）设置新的 IP 地址：
setip *ipv6_address***prefix-length** *prefix_length_number*

e) 设置网关地址：
setgateway *gateway_ip_address*

f) 提交配置：
commit-buffer

对于 ASA 逻辑设备的集群配置：

a) 输入集群管理引导程序：
scopecluster-bootstrap *asa*

b) （仅限 IPv4）设置新的虚拟 IP：
setvirtualipv4 *ip_address***mask** *network_mask*

c) （仅限 IPv6）设置新的虚拟 IP：
setvirtualipv6 *ipv6_address***prefix-length** *prefix_length_number*

d) 设置新的 IP 池：
setippool *start_ip end_ip*

e) 设置网关地址：
setgateway *gateway_ip_address*

f) 提交配置：
commit-buffer

对于 Firepower 威胁防御的独立和集群配置：

a) 输入逻辑设备管理引导程序：
scopemgmt-bootstrap *ftd*

b) 输入插槽的 IP 模式：
scope *ipv4_or_6 slot_number* firepower

c) （仅限 IPv4）设置新的 IP 地址：
setip *ipv4_address***mask** *network_mask*

d) （仅限 IPv6）设置新的 IP 地址：
setip *ipv6_address***prefix-length** *prefix_length_number*

e) 设置网关地址：
setgateway *gateway_ip_address*

f) 提交配置：
commit-buffer

注释 对于集群配置，必须为连接到 Firepower 4100/9300 机箱的每个应用设置新的 IP 地址。如果您有机箱间集群或 HA 配置，则必须对两个机箱上的每个应用重复这些步骤。

步骤 4 为每个应用清除管理引导程序信息：

a) 将范围设置为 ssa 模式：
scopessa

b) 将范围设置为插槽：
scopeslot *slot_number*

c) 将范围设置为应用实例：
scopeapp-instance *asa_or_ftd*

d) 清除管理引导程序信息：
clearmgmt-bootstrap

e) 提交配置：
commit-buffer

步骤 5 禁用应用：
disable

commit-buffer

注释 对于集群配置，必须对连接到 Firepower 4100/9300 机箱 的每个应用清除并禁用管理引导程序信息。如果您有机箱间集群或HA配置，则必须对两个机箱上的每个应用重复这些步骤。

步骤 6 当应用离线且插槽恢复在线时，重新启用应用。

a) 将范围重置为 ssa 模式：
scopessa

b) 将范围设置为插槽：
scopeslot *slot_number*

c) 将范围设置为应用实例：
scopeapp-instance *asa_or_ftd*

d) 启用应用：
enable

e) 提交配置：
commit-buffer

注释 对于集群配置，必须重复执行这些步骤以重新启用连接到Firepower 4100/9300 机箱的每个应用。如果您有机箱间集群或 HA 配置，则必须对两个机箱上的每个应用重复这些步骤。

更改 Firepower 4100/9300 机箱 名称

开始之前

您可以通过 FXOS CLI 更改用于 Firepower 4100/9300 机箱的名称。

过程

步骤 1 连接到 FXOS CLI（请参阅访问 FXOS CLI，第 8 页）。

步骤 2 进入系统模式：
Firepower-chassis-A# **scopesystem**

步骤 3 要查看当前名称：
Firepower-chassis-A /system # **show**

步骤 4 要配置新名称：
Firepower-chassis-A /system # **setname** *device_name*

步骤 5 将任务提交到系统配置：
Firepower-chassis-A /fabric-interconnect* # **commit-buffer**

以下示例更改了设备名称：

```
Firepower-chassis-A# scope system
Firepower-chassis-A /system # set name New-name
Warning: System name modification changes FC zone name and redeploys them non-disruptively
Firepower-chassis-A /system* # commit-buffer
Firepower-chassis-A /system # show

Systems:
    Name       Mode         System IP Address System IPv6 Address
    ---------- ------------ ----------------- -------------------
    New-name   Stand Alone 192.168.100.10    ::
New-name-A /system #
```

登录前横幅

如果配置了登录前横幅，当用户登录到Firepower机箱管理器时，系统将显示横幅文本，用户必须在消息屏幕上点击**确定(OK)**，然后系统才会提示输入用户名和密码。如果未配置登录前横幅，系统会直接进入用户名和密码输入提示屏幕。

当用户登录到 FXOS CLI 时，系统显示横幅文本（如已配置），然后提示输入密码。

创建登录前横幅

过程

步骤 1 连接到 FXOS CLI（请参阅访问 FXOS CLI，第 8 页）。

步骤 2 进入安全模式：
Firepower-chassis# **scopesecurity**

步骤 3 进入横幅安全模式：
Firepower-chassis /security # **scopebanner**

步骤 4 输入以下命令创建登录前横幅：
Firepower-chassis /security/banner # **create pre-login-banner**

步骤 5 指定在用户登录 Firepower 机箱管理器或 FXOS CLI 前 FXOS 应向用户显示的消息：
Firepower-chassis /security/banner/pre-login-banner* # **set message**

启动一个对话框，用于输入登录前横幅消息文本。

步骤 6 在提示符处，键入登录前横幅消息。您可以在此字段中输入任何标准 ASCII 字符。您可以输入多行文本，每行最多 192 个字符。按 **Enter** 键换行。
在您输入信息的下一行，键入 ENDOFBUF 并按 **Enter** 键以完成操作。

按 Ctrl 和 C 键取消设置消息对话框。

步骤 7 将任务提交到系统配置：
Firepower-chassis /security/banner/pre-login-banner* # **commit-buffer**

以下示例创建登录前横幅：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # create pre-login-banner
Firepower-chassis /security/banner/pre-login-banner* # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>Welcome to the Firepower Security Appliance
>**Unauthorized use is prohibited**
>ENDOFBUF
Firepower-chassis /security/banner/pre-login-banner* # commit-buffer
Firepower-chassis /security/banner/pre-login-banner #
```

修改登录前横幅

过程

步骤 1 连接到 FXOS CLI（请参阅访问 FXOS CLI，第 8 页）。

步骤 2 进入安全模式：
Firepower-chassis# **scopesecurity**

步骤 3 进入横幅安全模式：
Firepower-chassis /security # **scopebanner**

步骤 4 进入登录前横幅安全模式：
Firepower-chassis /security/banner # **scope pre-login-banner**

步骤 5 指定在用户登录 Firepower 机箱管理器或 FXOS CLI 前 FXOS 应向用户显示的消息：
Firepower-chassis /security/banner/pre-login-banner # **set message**

启动一个对话框，用于输入登录前横幅消息文本。

步骤 6 在提示符处，键入登录前横幅消息。您可以在此字段中输入任何标准 ASCII 字符。您可以输入多行文本，每行最多 192 个字符。按 **Enter** 键换行。
在您输入信息的下一行，键入 ENDOFBUF 并按 **Enter** 键以完成操作。

按 Ctrl 和 C 键取消设置消息对话框。

步骤 7 将任务提交到系统配置：
Firepower-chassis /security/banner/pre-login-banner* # **commit-buffer**

以下示例修改登录前横幅：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # scope pre-login-banner
Firepower-chassis /security/banner/pre-login-banner # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>Welcome to the Firepower Security Appliance
>**Unauthorized use is prohibited**
>ENDOFBUF
Firepower-chassis /security/banner/pre-login-banner* # commit-buffer
Firepower-chassis /security/banner/pre-login-banner #
```

删除登录前横幅

过程

步骤 1 连接到 FXOS CLI（请参阅访问 FXOS CLI，第 8 页）。

步骤 2 进入安全模式：
Firepower-chassis# **scopesecurity**

步骤 3 进入横幅安全模式：
Firepower-chassis /security # **scopebanner**

步骤 4 从系统中删除登录前横幅：
Firepower-chassis /security/banner # **delete pre-login-banner**

步骤 5 将任务提交到系统配置：
Firepower-chassis /security/banner* # **commit-buffer**

以下示例删除登录前横幅：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # delete pre-login-banner
Firepower-chassis /security/banner* # commit-buffer
Firepower-chassis /security/banner #
```

重新启动 Firepower 4100/9300 机箱

过程

步骤 1 选择**概览 (Overview)** 打开“概览 (Overview)”页面。

步骤 2 点击“概览 (Overview)”页面右上角“机箱运行时间 (Chassis Uptime)”旁边的**重新启动 (Reboot)**。

步骤 3 点击**是 (Yes)** 确认您要关闭 Firepower 4100/9300 机箱。
系统将正常关闭系统上配置的任何逻辑设备，然后关闭每个安全模块/引擎，最后关闭并重新启动 Firepower 4100/9300 机箱。此过程大约需要 15-20 分钟。

关闭 Firepower 4100/9300 机箱电源

过程

步骤 1 选择**概览 (Overview)** 打开“概览 (Overview)”页面。

步骤 2 点击“概览 (Overview)”页面右上角“机箱运行时间 (Chassis Uptime)”旁边的**关闭 (Shutdown)**。

步骤 3 点击**是 (Yes)** 确认您要关闭 Firepower 4100/9300 机箱。
系统将正常关闭系统上配置的任何逻辑设备，然后关闭每个安全模块/引擎，最后关闭 Firepower 4100/9300 机箱。

安装受信任身份证书

在完成初始配置后，将生成自签名 SSL 证书以供 Firepower 4100/9300 机箱 Web 应用使用。由于该证书是自签名证书，客户端浏览器不会自动信任它。新的客户端浏览器首次访问 Firepower 4100/9300 机箱 Web 界面时，浏览器会抛出 SSL 警告，要求用户在访问 Firepower 4100/9300 机箱之前接受证书。您可以使用以下程序，使用 FXOS CLI 生成证书签名请求 (CSR)，并安装得到的身份证书以供 Firepower 4100/9300 机箱使用。此身份证书允许客户端浏览器信任连接，并直接启动 Web 界面而无警告。

过程

步骤 1 连接到 FXOS CLI。（请参阅访问 FXOS CLI，第 8 页）。

步骤 2 输入安全模块：
scopesecurity

步骤 3 创建密钥环：
createkeyring *keyring_name*

步骤 4 设置私钥的模数大小：
setmodulus *size*

步骤 5 提交配置：
commit-buffer

步骤 6 配置CSR字段。可以使用基本选项（例如，主题名称）生成证书，也可以选择允许将信息（例如，区域和组织）嵌入证书的更高级选项。请注意，在您配置CSR字段时，系统会提示输入证书密码。
createcertreqcertreq *subject_name*

password

setcountry 国家/地区

setstate *state*

setlocality *locality*

setorg-name *organization_name*

setorg-unit-name *organization_unit_name*

setsubject-name *subject_name*

步骤 7 提交配置：
commit-buffer

步骤 8 导出 CSR，将其提供给您的证书颁发机构。

a) 显示完整 CSR：
showcertreq

b) 复制从（并包含）“-----BEGIN CERTIFICATE REQUEST-----”到（并包含）“-----END CERTIFICATE REQUEST-----”的输出：

示例：

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC6zCCAdMCAQAwdzELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3JuaWEx
ETAPBgNVBAcMCFNhbiBKb3NlMRYwFAYDVQQKDA1DaXNjbyBTeXN0ZW1zMQwwCgYD
VQQLDANUQUMxGjAYBgNVBAMMEWZwNDEyMC50ZXN0LmxvY2FsMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs0ON5gagkfZ2fi4JVEANG+7YGgcHbnUt7LpV
yMChnKOPJjBwkUMNQA1mQsRQDcbJ232/sK0fMSnyqOL8JzC7itxeVEZRyz7/ax7W
GNveg/XP+zd03nt4GXM63FsrPcPmA7EwgqDSLoShtBEV10hhf4+Nw4pKCZ+eSSkS
JkTB1ZHaKV9bttYg3kf/UEUUgk/EyrVq3B+u2DsooPVq76mTm8BwYMqHbJEv4Pmu
RjWE88yEvVwH7JTEij9OvxbatjDjVSJHZBURtCanvyBvGuLP/Q/Nmv3Lo3G9ITbL
L5gIYZVatTxp6HTUezH2MIIzOavU6d1tB9rnyxgGth5dPV0dhQIDAQABoC8wLQYJ
KoZIhvcNAQkOMSAwHjAcBgNVHREEFTATghFmcDQxMjAudGVzdC5sb2NhbDANBgkq
hkiG9w0BAQsFAAOCAQEAZUfCbwx9vt5aVDcL+tATu5xFE3LA310ck6GjlNv6W/6r
jBNLxusYi1rZZcW+CgnvNs4ArqYGyNVBySOavJO/VvQ1KfyxxJ1OIkyx3RzEjgK0
zzyoyrG+EZXC5ShiraS8HuWvE2wFM2wwWNtHWtvcQy55+/hDPD2Bv8pQOC2Zng3I
kLfG1dxWf1xAxLzf5J+AuIQ0CM5HzM9Zm8zREoWT+xHtLSqAqg/aCuomN9/vEwyU
OYfoJMvAqC6AZyUnMfUfCoyuLpLwgkxB0gyaRdnea5RhiGjYQ2lDXYDjEXp7rCx9
+6bvDl1n70JCegHdCWtP75SaNyaBEPkO0365rTckbw==
-----END CERTIFICATE REQUEST-----
```

步骤 9 退出证书请求模式：
exit

步骤 10 退出密钥环模式：
exit

步骤 11 注释　所有证书必须采用 Base64 格式才能导入到 FXOS。如果从证书颁发机构接收到的证书或链采用的是其他格式，您必须先使用 SSL 工具（例如，OpenSSL）进行转换。
创建新的信任点保存证书链。
createtrustpoint *trustpoint_name*

步骤 12 在信任点设置生成的 CSR：
setcertchain

步骤 13 注释　对于使用中间证书的证书颁发机构，必须对根证书和中间证书进行组合。在文本文件中，将根证书粘贴在顶部，然后是链中的每一个中间证书，包括所有 BEGIN CERTIFICATE 和 END CERTIFICATE 标记。将整个文本块复制并粘贴到信任点。
输入您在第 8 步中复制的 CSR 输出，按照屏幕上的说明操作。

示例：

```
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
>-----BEGIN CERTIFICATE-----
>MIICDTCCAbOgAwIBAgIQYIutxPDPw6BOp3uKNgJHZDAKBggqhkjOPQQDAjBTMRUw
>EwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3RpbjEg
>MB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTUwNzI4MTc1NjU2
>WhcNMjAwNzI4MTgwNjU2WjBTMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJ
>kiaJk/IsZAEZFghuYWF1c3RpbjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4t
>UEMtQ0EwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASvEA27V1Enq1gMtLkvJ6rx
>GXRpXWIEyuiBM4eQRoqZKnkeJUkm1xmqlubaDHPJ5TMGfJQYszLBRJPq+mdrKcDl
>o2kwZzATBgkrBgEEAYI3FAIEBh4EAEMAQTAOBgNVHQ8BAf8EBAMCAYYwDwYDVR0T
>AQH/BAUwAwEB/zAdBgNVHQ4EFgQUyInbDHPrFwEEBcbxGSgQW7pOVIkwEAYJKwYB
>BAGCNxUBBAMCAQAwCgYIKoZIzj0EAwIDSAAwRQIhAP++QJTUmniB/AxPDDN63Lqy
>18odMDoFTkG4p3Tb/2yMAiAtMYhlsv1gCxsQVOw0xZVRugSdoOak6n7wCjTFX9jr
>RA==
>-----END CERTIFICATE-----
>ENDOFBUF
```

步骤 14 提交配置：
commit-buffer

步骤 15 退出信任点模式：
exit

步骤 16 进入密钥环模式：
scopekeyring *keyring_name*

步骤 17 将在第 13 步中创建的信任点与为 CSR 创建的密钥环关联：
settrustpoint *trustpoint_name*

步骤 18 导入服务器的签名身份证书。
setcert

步骤 19 粘贴证书颁发机构提供的身份证书的内容：

示例：

```
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
>-----BEGIN CERTIFICATE-----
>MIIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAACjAKBggqhkjOPQQDAjBT
>MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3Rp
```

```
>bjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTYwNDI4MTMw
>OTU0WhcNMTgwNDI4MTMwOTU0WjB3MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2Fs
>aWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxFjAUBgNVBAoTDUNpc2NvIFN5c3Rl
>bXMxDDAKBgNVBAsTA1RBQzEaMBgGA1UEAxMRZnA0MTIwLnRlc3QubG9jYWwwggEi
>MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+LglUQA0b7tga
>BwdudS3sulXIwKGco48mMHCRQw1ADWZCxFANxsnbfb+wrR8xKfKo4vwnMLuK3F5U
>RlHLPv9rHtYY296D9c/7N3Tee3gZczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
>ikoJn55JKRImRMHVkdopX1u21iDeR/9QRRSCT8TKtWrcH67YOyig9WrvqZObwHBg
>yodskS/g+a5GNYTzzIS9XAfslMSKP06/Ftq2MONVIkdkFRG0Jqe/IG8a4s/9D82a
>/cujcb0hNssvmAhhlVq1PGnodNR7MfYwgjM5q9Tp3W0H2ufLGAa2Hl09XR2FAgMB
>AAGjggJYMIICVDAcBgNVHREEFTATghFmcDQxMjAudGVzdC5sb2NhbDAdBgNVHQ4E
>FgQU/1WpstiEYExs8DlZWcuHZwPtu5QwHwYDVR0jBBgwFoAUyInbDHPrFwEEBcbx
>GSgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBy6CByIaBxWxkYXA6Ly8vQ049bmFh
>dXN0aW4tTkFBVVNUSU4tUEMtQ0EsQ049bmFhdXN0aW4tcGMsQ049Q0RQLENOPVB1
>YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRp
>b24sREM9bmFhdXN0aW4sREM9bG9jYWw/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlz
>dD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHMBggrBgEF
>BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGgaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B
>QVVTVElOLVBDLUNBLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxD
>Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2Fs
>P2NBQ2VydGlmaWNhdGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0
>aG9yaXR5MCEGCSsGAQQBgjcUAgQUHhIAVwBlAGIAUwBlAHIAdgBlAHIwDgYDVR0P
>AQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0gAMEUC
>IFew7NcJirEtFRvyxjkQ4/dVo2oI6CRB308WQbYHNUu/AiEA7UdObiSJBG/PBZjm
>sgoIK60akbjotOTvUdUd9b6K1Uw=
>-----END CERTIFICATE-----
>ENDOFBUF
```

步骤 20 退出密钥环模式：
exit

步骤 21 退出安全模式：
exit

步骤 22 进入系统模式：
scopesystem

步骤 23 进入服务模式：
scopeservices

步骤 24 配置 FXOS Web 服务以使用新证书：
sethttpskeyring *keyring_name*

步骤 25 提交配置：
commit-buffer

步骤 26 显示与 HTTPS 服务器关联的密钥环。它应显示在本程序的第 3 步中创建的密钥环名称。如果屏幕输出显示默认的密钥环名称，则 HTTPS 服务器尚未更新，不能使用新证书：
showhttps

示例：

```
fp4120 /system/services # show https
Name: https
    Admin State: Enabled
    Port: 443
    Operational port: 443
    Key Ring: firepower_cert
    Cipher suite mode: Medium Strength
   Cipher suite: ALL:!ADH:!EXPORT40:!EXPORT56:!LOW:!RC4:!MD5:!IDEA:+HIGH:+MEDIUM:+EXP:+eNULL
```

步骤 27 显示导入的证书的内容，确认**Certificate Status** 值显示为**Valid**：
scopesecurity

showkeyring *keyring_name***detail**

示例：

```
fp4120 /security #  scope security
fp4120 /security #  show keyring firepower_cert detail
Keyring firepower_cert:
    RSA key modulus: Mod2048
    Trustpoint CA: firepower_chain
    Certificate status: Valid
    Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            45:00:00:00:0a:de:86:55:16:82:24:f3:be:00:00:00:00:0a
    Signature Algorithm: ecdsa-with-SHA256
        Issuer: DC=local, DC=naaustin, CN=naaustin-NAAUSTIN-PC-CA
        Validity
            Not Before: Apr 28 13:09:54 2016 GMT
            Not After : Apr 28 13:09:54 2018 GMT
        Subject: C=US, ST=California, L=San Jose, O=Cisco Systems, OU=TAC,
CN=fp4120.test.local
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b3:43:8d:e6:06:a0:91:f6:76:7e:2e:09:54:40:
                    0d:1b:ee:d8:1a:07:07:6e:75:2d:ec:ba:55:c8:c0:
                    a1:9c:a3:8f:26:30:70:91:43:0d:40:0d:66:42:c4:
                    50:0d:c6:c9:db:7d:bf:b0:ad:1f:31:29:f2:a8:e2:
                    fc:27:30:bb:8a:dc:5e:54:46:51:cb:3e:ff:6b:1e:
                    d6:18:db:de:83:f5:cf:fb:37:74:de:7b:78:19:73:
                    3a:dc:5b:2b:3d:c3:e6:03:b1:30:82:a0:d2:2e:84:
                    a1:b4:11:15:d7:48:61:7f:8f:8d:c3:8a:4a:09:9f:
                    9e:49:29:12:26:44:c1:d5:91:da:29:5f:5b:b6:d6:
                    20:de:47:ff:50:45:14:82:4f:c4:ca:b5:6a:dc:1f:
                    ae:d8:3b:28:a0:f5:6a:ef:a9:93:9b:c0:70:60:ca:
                    87:6c:91:2f:e0:f9:ae:46:35:84:f3:cc:84:bd:5c:
                    07:ec:94:c4:8a:3f:4e:bf:16:da:b6:30:e3:55:22:
                    47:64:15:11:b4:26:a7:bf:20:6f:1a:e2:cf:fd:0f:
                    cd:9a:fd:cb:a3:71:bd:21:36:cb:2f:98:08:61:95:
                    5a:b5:3c:69:e8:74:d4:7b:31:f6:30:82:33:39:ab:
                    d4:e9:dd:6d:07:da:e7:cb:18:06:b6:1e:5d:3d:5d:
                    1d:85
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                DNS:fp4120.test.local
            X509v3 Subject Key Identifier:
                FF:55:A9:B2:D8:84:60:4C:6C:F0:39:59:59:CB:87:67:03:ED:BB:94
            X509v3 Authority Key Identifier:
                keyid:C8:89:DB:0C:73:EB:17:01:04:05:C6:F1:19:28:10:5B:BA:4E:54:89
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:ldap:///CN=naaustin-NAAUSTIN-PC-CA,CN=naaustin-pc,CN=CDP,
                    CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=naaustin,
                  DC=local?certificateRevocationList?base?objectClass=cRLDistributionPoint

            Authority Information Access:
                CA Issuers - URI:ldap:///CN=naaustin-NAAUSTIN-PC-CA,CN=AIA,
                  CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=naaustin,
                  DC=local?cACertificate?base?objectClass=certificationAuthority
            1.3.6.1.4.1.311.20.2:
                ...W.e.b.S.e.r.v.e.r
            X509v3 Key Usage: critical
```

```
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
    Signature Algorithm: ecdsa-with-SHA256
         30:45:02:20:57:b0:ec:d7:09:8a:b1:2d:15:1b:f2:c6:39:10:
         e3:f7:55:a3:6a:08:e8:24:41:df:4f:16:41:b6:07:35:4b:bf:
         02:21:00:ed:47:4e:6e:24:89:04:6f:cf:05:98:e6:b2:0a:08:
         2b:ad:1a:91:b8:e8:b4:e4:ef:51:d5:1d:f5:be:8a:d5:4c
-----BEGIN CERTIFICATE-----
MIIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAACjAKBggqhkjOPQQDAjBT
MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3Rp
bjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTYwNDI4MTMw
OTU0WhcNMTgwNDI4MTMwOTU0WjB3MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2Fs
aWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxFjAUBgNVBAoTDUNpc2NvIFN5c3Rl
bXMxDDAKBgNVBAsTA1RBQzEaMBgGA1UEAxMRZnA0MTIwLnRlc3QubG9jYWwwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+LglUQA0b7tga
BwdudS3sulXIwKGco48mMHCRQw1ADWZCxFANxsnbfb+wrR8xKfKo4vwnMLuK3F5U
RlHLPv9rHtYY296D9c/7N3Tee3gZczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
ikoJn55JKRImRMHVkdopX1u21iDeR/9QRRSCT8TKtWrcH67YOyig9WrvqZObwHBg
yodskS/g+a5GNYTzzIS9XAfslMSKP06/Ftq2MONVIkdkFRG0Jqe/IG8a4s/9D82a
/cujcb0hNssvmAhhlVq1PGnodNR7MfYwgjM5q9Tp3W0H2ufLGAa2Hl09XR2FAgMB
AAGjggJYMIICVDAcBgNVHREEFTATghFmcDQxMjAudGVzdC5sb2NhbDAdBgNVHQ4E
FgQU/1WpstiEYExs8DlZWcuHZwPtu5QwHwYDVR0jBBgwFoAUyInbDHPrFwEEBcbx
GSgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBy6CByIaBxWxkYXA6Ly8vQ049bmFh
dXN0aW4tTkFBVVNUSU4tUEMtQ0EsQ049bmFhdXN0aW4tcGMsQ049Q0RQLENOPVB1
YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRp
b24sREM9bmFhdXN0aW4sREM9bG9jYWw/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlz
dD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHMBggrBgEF
BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGgaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B
QVVTVElOLVBDLUNBLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxD
Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2Fs
P2NBQ2VydGlmaWNhdGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0
aG9yaXR5MCEGCSsGAQQBgjcUAgQUHhIAVwBlAGIAUwBlAHIAdgBlAHIwDgYDVR0P
AQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0gAMEUC
IFew7NcJirEtFRvyxjkQ4/dVo2oI6CRB308WQbYHNUu/AiEA7UdObiSJBG/PBZjm
sgoIK60akbjotOTvUdUd9b6K1Uw=
-----END CERTIFICATE-----

    Zeroized: No
```

接下来的操作

要验证显示的证书是新的受信任证书，请通过在 Web 浏览器的地址栏输入 *https://<FQDN_or_IP>/* 转至 Firepower 机箱管理器。

注释 浏览器还根据地址栏中的输入验证证书的主题名称。如果证书颁发给完全限定域名，则必须在浏览器中以相应方式访问它。如果通过 IP 地址访问，将引发其他 SSL 错误（公用名无效 [Common Name Invalid]），即使使用的是受信任证书。

第 8 章

平台设置

设置日期和时间

使用 NTP 页面在系统上配置网络时间协议 (NTP)，手动设置日期和时间，或者查看当前系统时间。

NTP 设置在 Firepower 4100/9300 机箱与机箱上安装的任何逻辑设备之间自动同步。

注释 如果您在 Firepower 4100/9300 机箱上部署 Firepower 威胁防御，则必须在 Firepower 4100/9300 机箱上配置 NTP，使智能许可正常工作并确保设备注册的时间戳正确。应对 Firepower 4100/9300 机箱和 Firepower 管理中心使用相同 NTP 服务器。

如果您使用的是 NTP，则可以在**当前时间 (Current Time)** 选项卡上查看整体同步状态，或者也可以通过**时间同步 (Time Synchronization)** 选项卡上 **NTP 服务器 (NTP Server)** 表中的“服务器状态 (Server Status)”字段查看每个已配置的 NTP 服务器的同步状态。如果系统无法与特定 NTP 服务器同步，您可以将光标悬停在“服务器状态 (Server Status)”旁边的信息图标上获取更多信息。

查看配置的日期和时间

过程

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

步骤 2 点击**当前时间 (Current Time)** 选项卡。
系统显示设备上配置的日期、时间和时区。

如果您使用 NTP，您还可以在**当前时间 (Current Time)** 选项卡上查看整体同步状态。您可以通过**时间同步 (Time Synchronization)** 选项卡上的 **NTP 服务器 (NTP Server)** 表中的“服务器状态 (Server Status)”字段查看每台已配置的 NTP 服务器的同步状态。如果系统无法与特定 NTP 服务器同步，您可以将光标悬停在“服务器状态 (Server Status)”旁边的信息图标上获取更多信息。

设置时区

过程

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

步骤 2 点击**当前时间 (Current Time)** 选项卡。

步骤 3 从**时区 (Time Zone)** 下拉列表中为 Firepower 机箱选择适当的时区。

使用 NTP 设置日期和时间

NTP 用于实施分层服务器系统，可在网络系统中提供精确的同步时间。时间敏感性操作需要这种精确度，例如验证 CRL，其包括精确时间戳。您最多可以配置 4 个 NTP 服务器。

注释 FXOS 2.2(2) 和更高版本使用 NTP 版本 3。

过程

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

步骤 2 点击**时间同步 (Time Synchronization)** 选项卡。

步骤 3 在**设置时间来源 (Set Time Source)** 下面，点击**使用 NTP 服务器 (Use NTP Server)**。

步骤 4 对于您要使用的每个 NTP 服务器（最多 4 个），请在 **NTP 服务器 (NTP Server)** 字段中输入 NTP 服务器的 IP 地址或主机名，点击**添加 (Add)**。

步骤 5 点击**保存**。
使用指定的 NTP 服务器信息配置 Firepower 机箱。

您可以通过 **NTP 服务器 (NTP Server)** 表中的“服务器状态 (Server Status)”字段查看每台服务器的同步状态。如果系统无法与特定NTP服务器同步，您可以将光标悬停在“服务器状态(Server Status)”旁边的信息图标上获取更多信息。

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。

删除 NTP 服务器

过程

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

步骤 2 点击**时间同步 (Time Synchronization)** 选项卡。

步骤 3 对于您要删除的每台 NTP 服务器，请在 **NTP 服务器 (NTP Server)** 表中点击该服务器所对应的**删除 (Delete)** 图标。

步骤 4 点击**保存 (Save)**。

手动设置日期和时间

本部分介绍如何在 Firepower 机箱上手动设置日期和时间。

过程

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

步骤 2 点击**时间同步 (Time Synchronization)** 选项卡。

步骤 3 在**设置时间来源 (Set Time Source)** 下面，点击**手动设置时间 (Set Time Manually)**。

步骤 4 点击**日期 (Date)** 下拉列表，显示日历，然后使用日历中的可用控件设置日期。

步骤 5 使用对应的下拉列表将时间指定为小时、分钟和 AM/PM。

提示 您可以点击**获取系统时间 (Get System Time)**，设置日期和时间，以匹配您正在用来连接到 Firepower 机箱管理器的系统上所配置的日期和时间。

步骤 6 点击**保存 (Save)**。
使用指定的日期和时间配置 Firepower 机箱。

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。

配置 SSH

以下程序介绍了如何启用或禁用对 Firepower 机箱的 SSH 访问，以及如何将 FXOS 机箱作为 SSH 客户端启用。默认情况下，SSH 处于启用状态。

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 要启用到 Firepower 机箱的 SSH 访问，请选中**启用 SSH (Enable SSH)** 复选框。要禁用 SSH 访问，请取消选中**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。

注释 “通用标准”(Common Criteria) 不支持 3des-cbc。如果在 FXOS 机箱上启用了“通用标准”(Common Criteria) 模式，则您无法将 3des-cbc 用作加密算法。

步骤 4 对于服务器**密钥交换算法 (Key Exchange Algorithm)**，请选中与每种允许的 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**卷重新生成密钥限制 (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**时间重新生成密钥限制 (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)** - 如果主机密钥尚未处于 FXOS 已知主机文件中，则系统将拒绝该连接。您必须在系统/服务范围内使用 **enter ssh-host** 命令在 FXOS CLI 手动添加主机。
- **提示 (prompt)** - 如果主机密钥尚未存储在机箱中，则系统会提示您接受或拒绝该主机密钥。
- **禁用 (disable)** -（默认值）如果以前未存储主机密钥，则机箱会自动接受该主机密钥。

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。

注释 “通用标准”(Common Criteria) 不支持 3des-cbc。如果在 FXOS 机箱上启用了“通用标准”(Common Criteria) 模式，则您无法将 3des-cbc 用作加密算法。

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**卷重新生成密钥限制 (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**时间重新生成密钥限制 (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)**。

配置 Telnet

以下程序介绍如何启用或禁用对 Firepower 机箱的 Telnet 访问。默认情况下，会禁用 Telnet。

注释 目前，Telnet 配置只有在使用 CLI 时才可使用。

过程

步骤 1 进入系统模式：

Firepower-chassis #**scope system**

步骤 2 进入系统服务模式：
Firepower-chassis /system #**scope services**

步骤 3 要配置对 Firepower 机箱的 Telnet 访问，请执行以下操作之一：

- 要允许对 Firepower 机箱进行 Telnet 访问，请输入以下命令：

  Firepower-chassis /system/services # **enable telnet-server**

- 要禁止对 Firepower 机箱进行 Telnet 访问，请输入以下命令：

  Firepower-chassis /system/services # **disable telnet-server**

步骤 4 将任务提交到系统配置：
Firepower /system/services # **commit-buffer**

以下示例启用 Telnet 并且提交任务：

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /services # enable telnet-server
Firepower-chassis /services* # commit-buffer
Firepower-chassis /services #
```

配置 SNMP

使用 SNMP 页面，在 Firepower 机箱上配置简单网络管理协议 (SNMP)。有关详细信息，请参阅以下主题：

关于 SNMP

简单网络管理协议 (SNMP) 是一个应用层协议，用于为 SNMP 管理器和代理之间的通信提供消息格式。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。要启用 SNMP 代理并创建管理器和代理之间的关系，请在 Firepower 机箱管理器或 FXOS CLI 中启用并配置 SNMP。
- 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。有关 SNMP 的定义，请参阅以下标准：

- RFC 3410 (http://tools.ietf.org/html/rfc3410)

- RFC 3411 (http://tools.ietf.org/html/rfc3411)
- RFC 3412 (http://tools.ietf.org/html/rfc3412)
- RFC 3413 (http://tools.ietf.org/html/rfc3413)
- RFC 3414 (http://tools.ietf.org/html/rfc3414)
- RFC 3415 (http://tools.ietf.org/html/rfc3415)
- RFC 3416 (http://tools.ietf.org/html/rfc3416)
- RFC 3417 (http://tools.ietf.org/html/rfc3417)
- RFC 3418 (http://tools.ietf.org/html/rfc3418)
- RFC 3584 (http://tools.ietf.org/html/rfc3584)

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 安全等级和权限

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等级。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。安全等级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 *5*: *SNMP* 安全模型和级别

型号	Level	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。
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

Firepower 机箱使用高级加密标准 (AES) 作为用于 SNMPv3 消息加密的隐私协议之一并符合 RFC 3826。

隐私密码或 priv 选项提供对 DES 或 128 位 AES 加密的选择，以进行 SNMP 安全加密。如果启用 AES-128 配置并包含 SNMPv3 用户的隐私密码，则 Firepower 机箱使用该隐私密码来生成 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 64 个字符。

启用 SNMP 并配置 SNMP 属性

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。

名称	描述
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 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，例如电邮地址或姓名和电话号码。
位置字段	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 点击**保存 (Save)**。

接下来的操作

创建 SNMP 陷阱和用户。

创建 SNMP 陷阱

过程

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

步骤 2 在 **SNMP 陷阱 (SNMP Traps)** 区域中，点击**添加 (Add)**。

步骤 3 在**添加 SNMP 陷阱 (Add SNMP Trap)** 对话框中，填写以下字段：

名称	描述
主机名称字段	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 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。
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 • 告知
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 4 点击**确定 (OK)**，可关闭**添加 SNMP 陷阱 (Add SNMP Trap)** 对话框。

步骤 5 点击**保存 (Save)**。

删除 SNMP 陷阱

过程

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

步骤 2 在 **SNMP 陷阱 (SNMP Traps)** 区域中，在与您想要删除的陷阱对应的表的行中点击**删除 (Delete)** 图标。

创建 SNMPv3 用户

过程

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

步骤 2 在 **SNMP 用户 (SNMP Users)** 区域中，点击**添加 (Add)**。

步骤 3 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**。
使用 AES-128 (Use AES-128) 复选框	如果选中，该用户将使用 AES-128 加密。
密码字段	该用户的密码：
确认密码字段	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 4 点击**确定 (OK)**，可关闭**添加 SNMP 用户 (Add SNMP User)** 对话框。

步骤 5 点击**保存 (Save)**。

删除 SNMPv3 用户

过程

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

步骤 2 在 **SNMP 用户 (SNMP Users)** 区域中，在与您想要删除的用户对应的表的行中点击**删除 (Delete)** 图标。

配置 HTTPS

本节介绍如何在 Firepower 4100/9300 机箱 上配置 HTTPS。

注释 您可以使用 Firepower 机箱管理器或 FXOS CLI 更改 HTTPS 端口。所有其他 HTTPS 配置仅可使用 FXOS CLI 完成。

证书、密钥环和受信任点

HTTPS 使用公钥基础设施 (PKI) 的组件在两个设备（例如客户端浏览器和 Firepower 4100/9300 机箱）之间建立安全通信。

加密密钥和密钥环

每个 PKI 设备具有一对非对称 Rivest-Shamir-Adleman (RSA) 加密密钥（其中一个保持为私有，另一个公开），存储在内部密钥环中。用任一密钥加密的消息均可用另一密钥解密。要发送加密消息，发送方使用接收方的公钥加密消息，接收方使用自己的私钥解密消息。发送方也可以通过使用其自有私钥加密（也称为“签名”）已知消息来证明其对公钥的所有权。如果接收方可使用上述公钥成功解密消息，则发送方对相应私钥的所有权得以证明。加密密钥长度可以不同，典型的长度为 512 位至 2048 位。一般来说，秘钥长度越长，安全性就越高。FXOS 提供一个默认密钥环，带有 2048 位的初始密钥对，并允许创建更多密钥环。

如果群集名称更改或证书过期，则必须手动重新生成默认密钥环证书。

证书

作为安全通信前的准备，两台设备首先会交换数字证书。证书是包含设备公钥以及设备身份相关签名信息的文件。要仅支持加密通信，设备可生成自己的密钥对和自签名证书。远程用户连接至呈现自签名证书的设备时，用户无法轻易验证设备身份，且用户浏览器最初显示身份验证警告。默认情况下，FXOS 包含内置的自签名证书，其中包含来自默认密钥环的公共密钥。

受信任点

要为 FXOS提供更强的身份验证，您可从受信任来源或信任点获取并安装确认设备身份的第三方证书。第三方证书由颁发证书的受信任点签署，该受信任点可以是根证书颁发机构 (CA)，也可以是中间 CA 或信任锚（通向根 CA 的信任链一部分）。要获取新证书，您必须通过 FXOS 生成证书请求，并将请求提交至受信任点。

重要事项 证书必须采用 Base64 编码 X.509 (CER) 格式。

创建密钥环

FXOS 最多支持 8 个密钥环，包括默认密钥环。

过程

步骤 1 进入安全模式：
Firepower-chassis #**scope security**

步骤 2 创建并命名密钥环：
Firepower-chassis # **createkeyring** *keyring-name*

步骤 3 设置 SSL 密钥长度（以位为单位）：
Firepower-chassis # **setmodulus** {**mod1024** | **mod1536** | **mod2048** | **mod512**}

步骤 4 提交任务：
Firepower-chassis # **commit-buffer**

以下示例创建密钥大小为 1024 位的密钥环：

```
Firepower-chassis# scope security
Firepower-chassis /security # create keyring kr220
Firepower-chassis /security/keyring* # set modulus mod1024
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring #
```

接下来的操作

为该密钥环创建证书请求。

重新生成默认密钥环

如果群集名称更改或证书过期，则必须手动重新生成默认密钥环证书。

过程

步骤 1 进入安全模式：
Firepower-chassis #**scope security**

步骤 2 进入默认密钥环的密钥环安全模式：
Firepower-chassis /security # **scopekeyring default**

步骤 3 重新生成默认密钥环：
Firepower-chassis /security/keyring # **setregenerate yes**

步骤 4 提交任务：
Firepower-chassis # **commit-buffer**

以下示例重新生成默认密钥环：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring default
Firepower-chassis /security/keyring* # set regenerate yes
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring #
```

创建密钥环的证书请求

使用基本选项创建密钥环的证书请求

过程

步骤 1 进入安全模式：
Firepower-chassis #**scope security**

步骤 2 进入密钥环配置模式：
Firepower-chassis /security # **scope keyring** *keyring-name*

步骤 3 使用指定 IPv4 或 IPv6 地址或交换矩阵互联的名称创建证书请求。系统将提示您输入证书请求的密码。
Firepower-chassis /security/keyring # **create certreq** {**ip** [*ipv4-addr* | *ipv6-v6*] |**subject-name** *name*}

步骤 4 提交任务：
Firepower-chassis /security/keyring/certreq # **commit-buffer**

步骤 5 显示您可以复制并发送至信任锚或证书颁发机构的证书请求：

Firepower-chassis /security/keyring # **show certreq**

以下示例使用基本选项为密钥环创建并显示具有 IPv4 地址的证书请求：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq ip 192.168.200.123 subject-name sjc04
Certificate request password:
Confirm certificate request password:
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name:
Certificate request country name:
State, province or county (full name):
Locality (eg, city):
Organization name (eg, company):
Organization Unit name (eg, section):
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
BA==
-----END CERTIFICATE REQUEST-----

Firepower-chassis /security/keyring #
```

接下来的操作

- 复制证书请求文本（包括开始[BEGIN]和结束[END]行），并将其保存到文件中。将带有证书请求的文件发送至信任锚或证书颁发机构，以获取密钥环证书。
- 创建受信任点并为从信任锚接收的信任证书设置证书链。

使用高级选项创建密钥环的证书请求

过程

步骤 1 进入安全模式：
Firepower-chassis #**scope security**

步骤 2 进入密钥环配置模式：
Firepower-chassis /security # **scope keyring** *keyring-name*

步骤 3 创建证书请求：
Firepower-chassis /security/keyring # **createcertreq**

步骤 4 指定公司所在国家/地区的国家/地区代码：
Firepower-chassis /security/keyring/certreq* # **set country** *country name*

步骤 5 指定与请求相关联的域名服务器 (DNS) 地址：
Firepower-chassis /security/keyring/certreq* # **set dns** *DNS Name*

步骤 6 指定与证书请求相关联的邮件地址：
Firepower-chassis /security/keyring/certreq* # **set e-mail** *E-mail name*

步骤 7 指定 Firepower 4100/9300 机箱 的 IP 地址：
Firepower-chassis /security/keyring/certreq* # **set ip** {*certificate request ip-address*|*certificate request ip6-address* }

步骤 8 指定请求此证书的公司总部所在的城市或城镇：
Firepower-chassis /security/keyring/certreq* # **set locality** *locality name (eg, city)*

步骤 9 指定请求证书的组织：
Firepower-chassis /security/keyring/certreq* # **set org-name** *organization name*

步骤 10 指定组织单位：
Firepower-chassis /security/keyring/certreq* # **set org-unit-name** *organizational unit name*

步骤 11 为证书请求指定可选密码：
Firepower-chassis /security/keyring/certreq* # **set password** *certificate request password*

步骤 12 指定请求此证书的公司总部所在的省、市或自治区：
Firepower-chassis /security/keyring/certreq* # **set state** *state, province or county*

步骤 13 指定 Firepower 4100/9300 机箱 的完全限定域名：
Firepower-chassis /security/keyring/certreq* # **set subject-name** *certificate request name*

步骤 14 提交任务：
Firepower-chassis /security/keyring/certreq # **commit-buffer**

步骤 15 显示您可以复制并发送至信任锚或证书颁发机构的证书请求：
Firepower-chassis /security/keyring # **show certreq**

以下示例使用高级选项为密钥环创建并显示具有 IPv4 地址的证书请求：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq
Firepower-chassis /security/keyring/certreq* # set ip 192.168.200.123
Firepower-chassis /security/keyring/certreq* #  set subject-name sjc04
Firepower-chassis /security/keyring/certreq* # set country US
Firepower-chassis /security/keyring/certreq* # set dns bgl-samc-15A
Firepower-chassis /security/keyring/certreq* # set email test@cisco.com
Firepower-chassis /security/keyring/certreq* # set locality new york city
Firepower-chassis /security/keyring/certreq* # set org-name "Cisco Systems"
Firepower-chassis /security/keyring/certreq* # set org-unit-name Testing
Firepower-chassis /security/keyring/certreq* # set state new york
Firepower-chassis /security/keyring/certreq* # commit-buffer
Firepower-chassis /security/keyring/certreq # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name: test@cisco.com
Certificate request country name: US
State, province or county (full name): New York
Locality name (eg, city): new york city
Organization name (eg, company): Cisco
Organization Unit name (eg, section): Testing
```

```
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
BA==
-----END CERTIFICATE REQUEST-----

Firepower-chassis /security/keyring/certreq #
```

接下来的操作

- 复制证书请求文本（包括开始[BEGIN]和结束[END]行），并将其保存到文件中。将带有证书请求的文件发送至信任锚或证书颁发机构，以获取密钥环证书。
- 创建受信任点并为从信任锚接收的信任证书设置证书链。

创建受信任点

过程

步骤 1 进入安全模式：
Firepower-chassis #**scope security**

步骤 2 创建受信任点：
Firepower-chassis /security # **createtrustpoint** *name*

步骤 3 为此受信任点指定证书信息：
Firepower-chassis /security/trustpoint # **setcertchain** [*certchain*]

如果不在命令中指定证书信息，系统将提示您输入证书或信任点列表，定义到根证书授权(CA)的证书路径。在您输入信息的下一行，键入 ENDOFBUF 以完成操作。

重要事项 证书必须采用 Base64 编码 X.509 (CER) 格式。

步骤 4 提交任务：
Firepower-chassis /security/trustpoint # **commit-buffer**

以下示例创建受信任点并提供受信任点证书：

```
Firepower-chassis# scope security
Firepower-chassis /security # create trustpoint tPoint10
Firepower-chassis /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMDCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
```

```
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3nO4MIGeBgNVHSMEgZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3nO4oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> C1NhbnRhIENsYXJhMRswGQYDVQQKExJOdW92YSBTeXN0ZW1zIEluYy4xFDASBgNV
> BAsTC0VuZ2luZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GCAQAwDAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copP1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/trustpoint* # commit-buffer
Firepower-chassis /security/trustpoint #
```

接下来的操作

从信任锚或证书颁发机构获取密钥环证书并将其导入密钥环。

将证书导入密钥环

开始之前

- 配置包含密钥环证书的证书链的信任点。
- 从信任锚或证书颁发机构获取密钥环证书。

过程

步骤 1 进入安全模式：
Firepower-chassis #**scope security**

步骤 2 进入将接收证书的密钥环的配置模式：
Firepower-chassis /security # **scopekeyring** *keyring-name*

步骤 3 为从其中获取密钥环证书的信任锚或证书颁发机构指定受信任点：
Firepower-chassis /security/keyring # **settrustpoint** *name*

步骤 4 启动用于输入和上传密钥环证书的对话框：
Firepower-chassis /security/keyring # **setcert**

在提示符后，粘贴从信任锚或证书颁发机构接收的证书文本。在证书后的下一行，键入ENDOFBUF完成证书输入。

重要事项 证书必须采用 Base64 编码 X.509 (CER) 格式。

步骤 5 提交任务：
Firepower-chassis /security/keyring # **commit-buffer**

以下示例指定信任点并将证书导入密钥环：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # set trustpoint tPoint10
Firepower-chassis /security/keyring* # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
> -----BEGIN CERTIFICATE-----
> MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring #
```

接下来的操作

使用密钥环配置 HTTPS 服务。

配置 HTTPS

> **注意** 完成HTTPS配置（包括更改将由HTTPS使用的端口和密钥环）后，一旦保存或提交事务，所有当前 HTTP 和 HTTPS 会话都将关闭，而不显示警告。

过程

步骤 1 进入系统模式：
Firepower-chassis# **scope system**

步骤 2 进入系统服务模式：
Firepower-chassis /system # **scope services**

步骤 3 启用 HTTPS 服务：
Firepower-chassis /system/services # **enable https**

步骤 4 （可选） 指定要用于 HTTPS 连接的端口：
Firepower-chassis /system/services # **set https port** *port-num*

步骤 5 （可选） 指定创建用于 HTTPS 的密钥环名称：
Firepower-chassis /system/services # **set https keyring** *keyring-name*

步骤 6 （可选） 指定域使用的 Cipher Suite 安全级别：
Firepower-chassis /system/services # **set https cipher-suite-mode** *cipher-suite-mode*

cipher-suite-mode 可以是以下关键字之一：

- **high-strength**
- **medium-strength**
- **low-strength**
- **custom**- 允许您指定用户定义的 Cipher Suite 规格规范字符串。

步骤 7 （可选） 如果将 **cipher-suite-mode** 设为 **custom**，请指定域的 Cipher Suite 安全性自定义级别：
Firepower-chassis /system/services # **set https cipher-suite** *cipher-suite-spec-string*

cipher-suite-spec-string 可以包含最多 256 个字符，并且必须符合 OpenSSL Cipher Suite 规范。不得使用任何空格或特殊字符，！（感叹号）、+（加号）、-（连字符）和:（冒号）除外。有关详细信息，请参阅 http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite。

例如，默认情况下，FXOS 使用的中强度规范字符串为：
ALL:!ADH:!EXPORT56:!LOW:RC4+RSA:+HIGH:+MEDIUM:+EXP:+eNULL

注释 如果将 **cipher-suite-mode** 设置为除 **custom** 之外的任何其他值，则忽略此选项。

步骤 8 （可选） 启用或禁用证书吊销列表检查：
setrevoke-policy *{ relaxed | strict }*

步骤 9 将任务提交到系统配置：
Firepower-chassis /system/services # **commit-buffer**

以下示例启用 HTTPS，将端口号设置为 443，将密钥环名称设为 kring7984，将 Cipher Suite 安全级别设置为高，并提交任务：

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # enable https
Firepower-chassis /system/services* # set https port 443
Warning: When committed, this closes all the web sessions.
Firepower-chassis /system/services* # set https keyring kring7984
Firepower-chassis /system/services* # set https cipher-suite-mode high
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

更改 HTTPS 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。

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。

删除密钥环

过程

步骤 1 进入安全模式：
Firepower-chassis #**scope security**

步骤 2 删除指定密钥环：
Firepower-chassis /security # **deletekeyring** *name*

步骤 3 提交任务：
Firepower-chassis /security # **commit-buffer**

以下示例删除密钥环：

```
Firepower-chassis# scope security
Firepower-chassis /security # delete keyring key10
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

删除受信任点

开始之前

确保密钥环未使用受信任点。

过程

步骤 1 进入安全模式：
Firepower-chassis# **scopesecurity**

步骤 2 删除指定受信任点：
Firepower-chassis /security # **deletetrustpoint** *name*

步骤 3 提交任务：
Firepower-chassis /security # **commit-buffer**

以下示例删除受信任点：

```
Firepower-chassis# scope security
Firepower-chassis /security # delete trustpoint tPoint10
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

禁用 HTTPS

过程

步骤 1 进入系统模式：
Firepower-chassis# **scope system**

步骤 2 进入系统服务模式：
Firepower-chassis /system # **scope services**

步骤 3 禁用 HTTPS 服务：
Firepower-chassis /system/services # **disable https**

步骤 4 将任务提交到系统配置：
Firepower-chassis /system/services # **commit-buffer**

以下示例禁用 HTTPS 并提交任务：

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # disable https
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

配置 AAA

本部分介绍身份验证、授权和记帐。有关详细信息，请参阅以下主题：

关于 AAA

AAA 是一组服务，用于控制对计算机资源的访问、实施策略、评估使用情况并提供对服务进行计费所需的信息。这些过程对于高效进行网络管理和安全性而言至关重要。

身份验证

身份验证提供了一种识别用户的方法，这种方法通常先请用户输入有效用户名和有效密码，然后再授予访问权限。AAA 服务器将用户的身份验证凭证与数据库中存储的其他用户凭证进行比较。如果凭证匹配，则允许用户访问网络。如果凭证不匹配，则身份验证失败，并拒绝网络访问。

您可以将 Firepower 4100/9300 机箱配置对机箱的管理连接进行身份验证，包括以下会话：

- HTTPS
- SSH
- 串行控制台

授权

授权是执行策略的过程：确定允许用户访问哪些类型的活动、资源或服务。对用户进行身份验证后，可能会授权该用户执行各种类型的访问或活动。

会计

记帐用于测量用户在访问期间使用的资源量，这可以包括系统时间长度或者用户在会话期间发送或接收的数据量。记帐是通过记录会话统计信息和使用量信息来执行的，这些信息用于进行授权控制、计费、趋势分析、资源利用和容量规划活动。

身份验证、授权和记帐之间的交互

您可以单独使用身份验证功能，也可以将其与授权和记帐功能配合使用。授权始终要求先对用户进行身份验证。您可以单独使用记帐功能，也可以将其与身份验证和授权功能配合使用。

AAA 服务器

AAA 服务器是用于进行访问控制的网络服务器。身份验证用于识别用户。授权用于实施策略，这些策略确定经过身份验证的用户能够访问哪些资源和服务。记帐对时间和数据资源进行追踪，这些资源用于计费和分析。

本地数据库支持

Firepower 机箱维护可用用户配置文件填充的本地数据库。您可以使用本地数据库代替 AAA 服务器来提供用户身份验证、授权和记帐。

配置 LDAP 提供程序

配置 LDAP 提供程序的属性

在此任务中配置的属性对于此类型的所有提供程序连接而言是默认设置。如果单个提供程序包括任何这些属性的设置，Firepower 可扩展操作系统将使用该设置并忽略默认设置。

如果使用 Active Directory 作为 LDAP 服务器，请在 Active Directory 服务器中创建用户帐户以绑定 Firepower 可扩展操作系统。此帐户应具有非到期的密码。

过程

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

步骤 2 点击 **LDAP** 选项卡。

步骤 3 在**属性 (Properties)** 区域中，填写以下字段：

名称	描述
超时 (Timeout) 字段	在系统超时之前，系统尝试连接 LDAP 数据库时应花费的时间（以秒为单位）。 请输入一个介于 1 到 60 秒的整数。默认值为 30 秒。该属性为必填项。
属性 (Attribute) 字段	LDAP 属性，存储用户角色值和区域设置值。此属性始终是一个名称值对。系统在用户记录中查询匹配此属性名称的值。
基础 DN (Base DN) 字段	LDAP 层级结构中的特定区别名，在此层次结构中，当远程用户登录并且系统尝试根据其用户名获取用户的 DN 时，服务器应当开始搜索。基础 DN 的长度可以设置为最大 255 个字符减去 CN=$userid 的长度，其中，$userid 标识尝试使用 LDAP 身份验证访问 Firepower 机箱的远程用户。 该属性为必填项。如果您没有在此选项卡上指定基础 DN，则必须为自己定义的每个 LDAP 提供程序指定一个基础 DN。
过滤器 (Filter) 字段	LDAP 搜索仅限于那些匹配已定义过滤器的用户名。 该属性为必填项。如果您没有在此选项卡上指定过滤器，则必须为自己定义的每个 LDAP 提供程序指定一个过滤器。

步骤 4 点击**保存 (Save)**。

接下来的操作

创建 LDAP 提供程序。

创建 LDAP 提供程序

Firepower 可扩展操作系统最多支持 16 个 LDAP 提供程序。

开始之前

如果使用 Active Directory 作为 LDAP 服务器，请在 Active Directory 服务器中创建用户帐户以绑定 Firepower 可扩展操作系统。此帐户应具有非到期的密码。

过程

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

步骤 2 点击 **LDAP** 选项卡。

步骤 3 对于要添加的每个 LDAP 提供程序：

a) 在 **LDAP 提供程序 (LDAP Providers)** 区域中，点击**添加 (Add)**。

b) 在**添加 LDAP 提供程序 (Add LDAP Provider)** 对话框中，填写以下字段：

名称	描述
主机名/FDQN (Hostname/FDQN)（或 **IP 地址 [IP Address]**）字段	LDAP 提供程序所驻留的主机名或 IP 地址。如果启用了 SSL，此字段必须精确匹配 LDAP 数据库安全认证中的通用名称 (CN)。
顺序字段	Firepower 可扩展操作系统使用此提供程序对用户进行身份验证的顺序。 输入一个介于 1 和 16 之间的整数，或者输入最低可用值或 0（零），前提是您想让 Firepower 可扩展操作系统根据在 Firepower 机箱管理器或 FXOS CLI 定义的其他提供程序分配下一个可用顺序。
绑定 DN (Bind DN) 字段	LDAP 数据库帐户的区别名 (DN)，对基础 DN 下的所有对象拥有读取和搜索权限。 支持的最大字符串长度为 255 个 ASCII 字符。
基础 DN (Base DN) 字段	LDAP 层级结构中的特定区别名，在此层次结构中，当远程用户登录并且系统尝试根据其用户名获取用户的 DN 时，服务器应当开始搜索。基础 DN 的长度可以设置为最大长度 255 个字符减去 CN=$userid 的长度，其中 $userid 标识尝试使用 LDAP 身份验证访问 Firepower 机箱管理器或 FXOS CLI 的远程用户。 该值为必填项，除非已在 **LDAP** 选项卡上设置了默认基础 DN。

名称	描述
端口字段	Firepower 机箱管理器或 FXOS CLI 与 LDAP 数据库进行通信所使用的端口。标准端口号为 389。
启用 SSL 复选框	如果选中，需要对与 LDAP 数据库之间的通信进行加密。如果取消选中，身份验证信息将以明文发送。 LDAP 使用 STARTTLS。这允许使用端口 389 进行加密通信。
过滤器 (Filter) 字段	LDAP 搜索仅限于那些匹配已定义过滤器的用户名。 该值为必填项，除非已在 **LDAP** 选项卡上设置了默认过滤器。
属性 (Attribute) 字段	LDAP 属性，存储用户角色值和区域设置值。此属性始终是一个名称值对。系统在用户记录中查询匹配此属性名称的值。 该值为必填项，除非已在 **LDAP** 选项卡上设置了默认属性。
密钥 (Key) 字段	在**绑定 DN (Bind DN)** 字段中指定的 LDAP 数据库帐户的密码。您可以输入任意标准 ASCII 字符，但空格、§（分节号）、？（问号）或 =（等号）除外。
确认密钥 (Confirm Key) 字段	重复用于确认目的的 LDAP 数据库密码。
超时 (Timeout) 字段	在系统超时之前，系统尝试连接 LDAP 数据库时应花费的时间（以秒为单位）。 输入一个介于 1 和 60 秒之间的整数，或者输入 0（零），以使用在 **LDAP** 选项卡上指定的全局超时值。默认值为 30 秒。
Vendor 字段	此选择标识提供 LDAP 提供程序或服务器详细信息的供应商： • 如果 LDAP 提供程序是 Microsoft Active Directory，请选择 **MS AD**。 • 如果 LDAP 提供程序不是 Microsoft Active Directory，请选择**打开 LDAP (Open LDAP)**。 默认值为**打开 LDAP (Open LDAP)**。

c) 点击**确定 (OK)** 以关闭**添加 LDAP 提供程序 (Add LDAP Provider)** 对话框。

步骤 4 点击**保存 (Save)**。

步骤 5 （可选）启用证书吊销列表检查：

Firepower-chassis /security/ldap/server # **set revoke-policy** *{strict | relaxed}*

注释 此配置仅在启用 SSL 连接后才生效。

删除 LDAP 提供程序

过程

步骤 1 选择平台设置 **(Platform Settings)** > **AAA**.

步骤 2 点击 **LDAP** 选项卡。

步骤 3 在 **LDAP 提供程序 (LDAP Providers)** 区域中，在与您想要删除的 LDAP 提供程序对应的表的行中点击删除 **(Delete)** 图标。

配置 RADIUS 提供程序

配置 RADIUS 提供程序的属性

在此任务中配置的属性对于此类型的所有提供程序连接而言是默认设置。如果单个提供程序包括任何这些属性的设置，Firepower 可扩展操作系统将使用该设置并忽略默认设置。

过程

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

步骤 2 点击 **RADIUS** 选项卡。

步骤 3 在属性 **(Properties)** 区域中，填写以下字段：

名称	描述
超时 (Timeout) 字段	在系统超时之前，系统尝试连接 RADIUS 数据库时应花费的时间（以秒为单位）。 请输入一个介于 1 到 60 秒的整数。默认值为 5 秒。 该属性为必填项。
重试次数 (Retries) 字段	请求被视为失败之前的连接重试次数。

步骤 4 点击保存 **(Save)**。

接下来的操作

创建 RADIUS 提供程序。

创建 RADIUS 提供程序

Firepower 可扩展操作系统最多支持 16 个 RADIUS 提供程序。

过程

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

步骤 2 点击 **RADIUS** 选项卡。

步骤 3 对于要添加的每个 RADIUS 提供程序：

a) 在 **RADIUS 提供程序 (RADIUS Providers)** 区域中，点击**添加 (Add)**。

b) 在**添加 RADIUS 提供程序 (Add RADIUS Provider)** 对话框中，填写以下字段：

名称	描述
主机名/FDQN (Hostname/FDQN)（或 **IP 地址 [IP Address]**）字段	RADIUS 提供程序所驻留的主机名或 IP 地址。
顺序字段	Firepower 可扩展操作系统使用此提供程序对用户进行身份验证的顺序。 输入一个介于 1 和 16 之间的整数，或者输入最低可用值或 0（零），前提是您想让 Firepower 可扩展操作系统根据在 Firepower 机箱管理器或 FXOS CLI 定义的其他提供程序分配下一个可用顺序。
密钥 (Key) 字段	数据库 SSL 加密密钥。
确认密钥 (Confirm Key)字段	反复用于确认目的的 SSL 加密密钥。
授权端口 (Authorization Port) 字段	Firepower 机箱管理器或 FXOS CLI 与 RADIUS 数据库进行通信时使用的端口。有效范围为 1 至 65535。标准端口号为 1700。
超时 (Timeout) 字段	在系统超时之前，系统尝试连接 RADIUS 数据库时应花费的时间（以秒为单位）。 输入一个介于 1 和 60 秒之间的整数，或者输入 0（零），使用在 **RADIUS** 选项卡上指定的全局超时值。默认值为 5 秒。

名称	描述
重试次数 (Retries) 字段	请求被视为失败之前的连接重试次数。 如果需要，请输入一个介于 0 和 5 之间的整数。如果不指定该值，Firepower 机箱管理器将使用在 **RADIUS** 选项卡上指定的值。

c）点击**确定 (OK)**，可关闭**添加 RADIUS 提供程序 (Add RADIUS Provider)** 对话框。

步骤 4 点击**保存 (Save)**。

删除 RADIUS 提供程序

过程

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

步骤 2 点击 **RADIUS** 选项卡。

步骤 3 在 **RADIUS 提供程序 (RADIUS Providers)** 区域中，在与您想要删除的 RADIUS 提供程序对应的表的行中点击**删除 (Delete)** 图标。

配置 TACACS+ 提供程序

配置 TACACS+ 提供程序的属性

在此任务中配置的属性对于此类型的所有提供程序连接而言是默认设置。如果单个提供程序包括任何这些属性的设置，Firepower 可扩展操作系统将使用该设置并忽略默认设置。

过程

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

步骤 2 点击 **TACACS** 选项卡。

步骤 3 在**属性 (Properties)** 区域中，填写以下字段：

名称	描述
超时 (Timeout) 字段	在系统超时之前，系统尝试连接 TACACS+ 数据库时应花费的时间（以秒为单位）。 请输入一个介于 1 到 60 秒的整数。默认值为 5 秒。 该属性为必填项。

步骤 4 点击**保存 (Save)**。

接下来的操作

创建 TACACS+ 提供程序。

创建 TACACS+ 提供程序

Firepower 可扩展操作系统最多支持 16 个 TACACS+ 提供程序。

过程

步骤 1 选择**平台设置 (Platform Settings)** > **AAA**.

步骤 2 点击 **TACACS** 选项卡。

步骤 3 对于您要添加的每个 TACACS+ 提供程序：

a) 在 **TACACS 提供程序 (TACACS Providers)** 区域中，点击**添加 (Add)**。

b) 在**添加 TACACS 提供程序 (Add TACACS Provider)** 对话框中，填写以下字段：

名称	描述
主机名/FDQN (Hostname/FDQN)（或 **IP 地址 [IP Address]**）字段	TACACS+ 提供程序所驻留的主机名或 IP 地址。
顺序字段	Firepower 可扩展操作系统使用此提供程序对用户进行身份验证的顺序。 输入一个介于 1 和 16 之间的整数，或者输入最低可用值或 0（零），前提是您想让 Firepower 可扩展操作系统根据在 Firepower 机箱管理器或 FXOS CLI 定义的其他提供程序分配下一个可用顺序。
密钥 (Key) 字段	数据库 SSL 加密密钥。
确认密钥 (Confirm Key)字段	反复用于确认目的的 SSL 加密密钥。

名称	描述
端口字段	Firepower 机箱管理器或 FXOS CLI与 TACACS+ 数据库进行通信时使用的端口。 输入 1 和 65535 之间的整数。默认端口为 49。
Timeout 字段	在系统超时之前，系统尝试连接 TACACS+ 数据库时应花费的时间（以秒为单位）。 输入一个介于 1 和 60 秒之间的整数，或者输入 0（零），以使用在 **TACACS+** 选项卡上指定的全局超时值。默认值为 5 秒。

c) 点击**确定 (OK)**，可关闭**添加 TACACS 提供程序 (Add TACACS Provider)** 对话框。

步骤 4 点击**保存 (Save)**。

删除 TACACS+ 提供程序

过程

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

步骤 2 点击 **TACACS** 选项卡。

步骤 3 在 **TACACS 提供程序 (TACACS Providers)** 区域中，在与您想要删除的 TACACS+ 提供程序对应的表的行中点击**删除 (Delete)** 图标。

配置系统日志

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。系统日志服务接受消息并将其存储在文件中，或者根据简单配置文件打印消息。以这种形式记录日志可为日志提供受保护的长期存储。日志对常规故障排除及事件处理均有帮助。

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) 在**本地目标 (Local Destinations)** 选项卡上，填写以下字段：

名称	描述
控制台 (Console) 部分	
Admin State 字段	Firepower 机箱是否在控制台上显示系统日志消息。 如果您想在控制台上显示系统日志消息并将这些日志消息添加到日志中，请选中**启用 (Enable)** 复选框。如果取消选中**启用 (Enable)** 复选框，系统日志消息将会添加到日志中，但不会显示在控制台上。
Level 字段	如果选中了**控制台 - 管理状态 (Console - Admin State)** 的**启用 (Enable)** 复选框，请选择您想在控制台上显示的最低消息级别。Firepower 机箱在控制台上显示此级别及以上消息。这可以是以下其中一项： • **紧急联系方式** • **风险通告** • **严重**
监控 (Monitor) 部分	
Admin State 字段	Firepower 机箱是否在监视器上显示系统日志消息。 如果您想在监视器上显示系统日志消息并将这些日志消息添加到日志中，请选中**启用 (Enable)** 复选框。如果取消选中**启用 (Enable)** 复选框，系统日志消息将会添加到日志中，但不会显示在监视器上。
级别 (Level) 下拉列表	如果选中了**监视器 - 管理状态 (Monitor - Admin State)** 的**启用 (Enable)** 复选框，请选择您想在监视器上显示的最低消息级别。系统在监视器上显示此级别及以上消息。这可以是以下其中一项： • **紧急联系方式** • **风险通告** • **严重** • **错误** • **警告** • **通知** • **信息** • **调试**

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
Admin State 字段	如果您想在远程日志文件中存储系统日志消息，请选中**启用 (Enable)** 复选框。
级别 (Level) 下拉列表	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。这可以是以下其中一项： • **紧急联系方式** • **风险通告** • **严重** • **错误** • **警告** • **通知** • **信息** • **调试**
主机名/IP 地址 (Hostname/IP Address) 字段	远程日志文件所驻留的主机名或 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。

名称	描述
设备 (Facility) 下拉列表	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。这可以是以下其中一项： • **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) 在**本地源 (Local Sources)** 选项卡上，填写以下字段：

名称	描述
故障管理状态 (Faults Admin State) 字段	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。
审核管理状态 (Audits Admin State) 字段	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) 字段	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)**。

配置 DNS 服务器

如果系统要求将主机名解析为 IP 地址，您需要指定 DNS 服务器。例如，如果不配置 DNS 服务器，当您在 Firepower 机箱上配置设置时，不能使用 www.cisco.com 等名称。您可能需要使用服务器的 IP 地址，其可以是 IPv4 或 IPv6 地址。您最多可以配置 4 个 DNS 服务器。

注释 配置多个 DNS 服务器时，系统仅以任意随机顺序搜索服务器。如果本地管理命令要求 DNS 服务器查询，它只能以随机顺序搜索 3 个 DNS 服务器。

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)**。

第 9 章

接口管理

关于 Firepower 安全设备接口

Firepower 4100/9300 机箱支持单一接口以及 EtherChannel（端口通道）接口。EtherChannel 接口最多可以包含同一类型的 16 个成员接口。

“接口 (Interfaces)”页面

从 Firepower 机箱管理器的“接口 (Interfaces)”页面，您可以查看机箱上已安装的接口的状态，编辑接口属性，启用或禁用接口，以及创建端口通道。

“接口 (Interfaces)”页面由两部分组成：

- 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 - 已安装并启用接口。

  深灰色 - 已安装但禁用接口。

  红色 - 接口的运行状态有问题。

  浅灰色 - 未安装接口。

注释 充当端口通道中的端口的接口不会显示在此列表中。

- 下半部分包含两个选项卡：**所有接口 (All Interfaces)** 和**硬件旁路**。在**所有接口 (All Interfaces)** 选项卡上：对于每个接口，您可以启用或禁用接口。您也可以点击**编辑 (Edit)** 编辑接口属性，例如速度和接口类型。有关**硬件旁路**，请参阅硬件旁路对 ，第 113 页。

注释 如果端口通道 48 集群类型接口不包括任何成员接口，则该接口的**运行状态 (Operation State)** 将显示为**失败 (failed)**。对于机箱内集群，此 EtherChannel 无需任何成员接口，您可忽略此“运行状态 (Operational State)”。

接口类型

每个接口可以是以下类型之一：

- 数据 (Data)（默认设置）- 不能在逻辑设备之间共享数据接口。
- 管理 (Management) - 可以在逻辑设备之间共享管理接口。只能为每个逻辑设备分配一个管理接口。

  在 Firepower 威胁防御 应用内，物理管理接口在诊断逻辑接口和管理逻辑接口之间进行共享。管理逻辑接口与设备上的其他接口分离。它用于设置设备并将其注册到 Firepower 管理中心。它运行单独的SSH服务器并使用其自己的本地身份验证、IP地址和静态路由。可以使用**configure network** 命令在 CLI 上配置其设置，也可以从管理中心**设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Devices)** > **管理 (Management)** 区域更改 IP 地址。

  诊断逻辑接口可以连同管理中心**设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** 屏幕上的其余数据接口一起进行配置。使用诊断接口是可选的。诊断接口和数据接口允许进行 LDAP 或 RADIUS 外部身份验证。例如，如果您不想允许数据接口上的 SSH 访问，您可以选择为 SSH 访问配置诊断接口。诊断接口只允许管理流量，而不允许通过流量。
- Firepower 事件 (Firepower-eventing) - 此接口是 Firepower 威胁防御设备的二级管理接口。要使用此接口，您必须在 Firepower 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 Firepower 管理中心命令参考中的 **configure network** 命令。
- 集群 (Cluster) - 用于集群式逻辑设备的特定接口类型。此类型自动分配到集群控制链路以进行设备间集群通信。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。

注释 您可以使用 Firepower 管理中心或 Firepower 威胁防御 CLI 将两个上行链路、分支或数据端口接口配置为内联对。一旦将两个端口配置为内联对，它们将相当于一个接口。然后，此配置被传播到 FXOS 机箱。

请注意内联对的以下限制：

- 两个端口接口必须是唯一的。端口一旦加入一个内联对，将无法加入其他内联对。
- 只有上行链路端口、数据端口或分支端口才可以配置为内联对。

有关详细信息，请参阅《Firepower 管理中心配置指南》中的“配置 IPS 专用接口的内联集”主题。

硬件旁路对

对于 Firepower 威胁防御，Firepower 9300 和 4100 系列上的某些接口模块允许您启用硬件旁路功能。硬件旁路可在停电时确保流量在内联接口对之间继续流动。在软件或硬件发生故障时，此功能可用于维持网络连接性。

硬件旁路功能在 硬件旁路应用中进行配置。您不需要将这些接口用作 硬件旁路对；它们可用作 ASA 和 Firepower 威胁防御应用的常规接口。请注意，不可为分支端口配置具有 硬件旁路功能的接口。如果您想使用 硬件旁路 功能，请勿将端口配置为 EtherChannel；否则，您可将这些接口作为常规接口模式下的 EtherChannel 成员。

对于以下型号上特定网络模块的接口对，Firepower 威胁防御支持硬件旁路：

- Firepower 9300
- Firepower 4100 系列

这些型号的受支持硬件旁路网络模块包括：

- Firepower 6 端口 1G SX FTW 单位宽网络模块 (FPR-NM-6X1SX-F)
- Firepower 6 端口 10G SR FTW 单位宽网络模块 (FPR-NM-6X10SR-F)
- Firepower 6 端口 10G LR FTW 单位宽网络模块 (FPR-NM-6X10LR-F)
- Firepower 2 端口 40G SR FTW 单位宽网络模块 (FPR-NM-2X40G-F)
- Firepower 8 端口 1G 铜缆 FTW 单位宽网络模块 (FPR-NM-8X1G-F)

硬件旁路只能使用以下端口对：

- 1、2
- 3、4
- 5、6
- 7、8

巨帧支持

Firepower 4100/9300 机箱默认启用巨帧支持。要在 Firepower 4100/9300 机箱上安装的特定逻辑设备上启用巨帧支持，您将需要为逻辑设备上的接口配置合适的 MTU 设置。

Firepower 4100/9300 机箱 上应用支持的最大 MTU 为 9184。

编辑接口属性

过程

步骤 1 选择**接口 (Interfaces)** 打开 Interfaces 页面。
“接口 (Interfaces)”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 在您要编辑的接口所对应的行中点击**编辑 (Edit)**，可打开**编辑接口 (Edit Interface)** 对话框。

步骤 3 要启用接口，请选中**启用 (Enable)** 复选框。要禁用接口，请取消选中**启用 (Enable)** 复选框。

步骤 4 （可选）从 **类型 (Type)** 下拉列表中选择**数据 (data)**，将此接口配置为数据接口，选择 **firepower 事件 (firepower-eventing)**，以将接口配置为 Firepower 事件接口，或者选择**管理 (mgmt)**，以将接口配置为管理接口。

注释 请勿选择**集群 (Cluster)** 类型。

步骤 5 （可选）从**速度 (Speed)** 下拉列表中选择接口速度。

步骤 6 点击 **OK**。

更改接口的管理状态

过程

步骤 1 选择**接口 (Interfaces)** 打开 Interfaces 页面。
“接口 (Interfaces)”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 对于您想更改其管理状态的每个接口，请执行以下操作之一：

- 要将接口的管理状态设置为启用，请点击您想启用的接口的“状态 (State)”栏中的**已禁用 (Disabled)** 开关，将设置更改为**已启用 (Enabled)**。点击**是 (Yes)**，确认更改。

  接口的管理状态更改为已启用。以直观展示图表现的对应接口从灰色变为绿色。

- 要将接口的管理状态更改为已禁用，请点击您想禁用的接口的“状态 (State)”栏中的**已启用 (Enabled)** 开关，将设置更改为**已禁用 (Disabled)**。点击**是 (Yes)**，确认更改。

接口的管理状态更改为已禁用。以直观展示图表现的对应接口从绿色变为灰色。

创建端口通道

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

当 Firepower 4100/9300 机箱创建 EtherChannel 时，EtherChannel 将处于**挂起 (Suspended)** 状态，直到您将其分配给逻辑设备，即使物理链路是连通的。EtherChannel 在以下情况下将退出**挂起 (Suspended)** 状态：

- EtherChannel 添加为独立逻辑设备的数据或管理端口
- EtherChannell 添加为作为集群一部分的逻辑设备的管理或 CCL 端口
- EtherChannell 添加为作为集群一部分，且至少有一个安全模块加入了集群的逻辑设备的数据端口

请注意，EtherChannel 在您将它分配到逻辑设备前不会正常工作。如果从逻辑设备移除 EtherChannel 或删除逻辑设备，EtherChannel 将恢复为**挂起 (Suspended)** 状态。

开始之前

Firepower 4100/9300 机箱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。

过程

步骤 1 选择**接口 (Interfaces)** 打开 Interfaces 页面。
“接口 (Interfaces)”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 点击接口表上方的**添加端口通道 (Add Port Channel)**，可打开**添加端口通道 (Add Port Channel)** 对话框。

步骤 3 在**端口通道 ID (Port Channel ID)** 字段中输入端口通道 ID。有效值介于 1 与 47 之间。
部署集群逻辑设备时，端口通道 48 为集群控制链路预留。如果不想将端口通道 48 用于集群控制链路，您可以为 EtherChannel 配置不同的 ID，为接口选择“集群 (Cluster)”类型。不要将任何接口分配给集群 EtherChannel。

步骤 4 要启用端口通道，请选中**启用 (Enable)** 复选框。要禁用端口通道，请取消选中**启用 (Enable)** 复选框。

步骤 5 从**类型 (Type)** 下拉列表中选择端口通道类型：**数据 (Data)**、**管理 (Mgmt)** 或**集群 (Cluster)**。

步骤 6 如果未选中，请点击**接口 (Interfaces)** 选项卡。

步骤 7 要将接口添加到端口通道，请在**可用接口 (Available Interface)** 列表中选择该接口，点击**添加接口 (Add Interface)**，将接口移动至“成员 ID (Member ID)”列表。您最多可以添加 16 个同一类型和速度的接口。

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 8　要从端口通道删除接口，请点击“成员 ID (Member ID)”列表中接口右侧的**删除 (Delete)** 按钮。

步骤 9　单击 **Settings**（设置）选项卡。

步骤 10　从**速度 (Speed)** 下拉列表中选择端口通道的速度。

步骤 11　点击 **OK**。

配置分支电缆

以下操作步骤介绍如何配置分支电缆以用于 Firepower 4100/9300 机箱。您可以使用分支线缆提供 4 个 10 Gbps 端口，代替单个 40 Gbps 端口。

开始之前

具有 硬件旁路功能的接口不可为分支端口配置。

过程

步骤 1　选择**接口 (Interfaces)** 打开 Interfaces 页面。
“接口 (Interfaces)”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。

接口对应的行中的“分支端口 (Breakout Port)”图标表示能够支持分支线缆但当前未配置为支持的接口。对于已配置为使用分支线缆的接口，分别列出各个分支接口（例如，以太网 2/1/1、2/1/2、2/1/3 和 2/1/4）。

步骤 2　要将 40 Gbps 接口转换为 4 个 10 Gbps 接口，请执行以下操作：

a) 点击您想转换的接口所对应的**分支端口 (Breakout Port)** 图标。
“创建分支端口 (Breakout Port Creation)”对话框打开，要求您确认是否想要继续，并警告您机箱将被重启。

b) 点击**是**进行确认。
Firepower 机箱重启，指定接口转换为 4 个 10 Gbps 接口。

步骤 3　要将 4 个 10 Gbps 分支接口转换回单个 40 Gbps 接口，请执行以下操作：

a) 点击任意分支接口所对应的 **删除 (Delete)**。
确认对话框打开，要求您确认是否想要继续，并警告您全部 4 个分支接口都将被删除，机箱将重启。

b) 点击**是**进行确认。
Firepower 机箱重启，指定的接口转换为单个 40 Gbps 接口。

第 10 章

逻辑设备

关于逻辑设备

创建逻辑设备时，Firepower 4100/9300 机箱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指定的安全模块/引擎，或在使用机箱内集群的情况下推送到 Firepower 机箱中安装的所有安全模块来部署逻辑设备。

您可以创建以下两类逻辑设备之一：

- 独立 (Standalone) - 您可以为安装在 Firepower 机箱中的每个安全模块/引擎创建独立逻辑设备。
- 集群 (Cluster) - 通过集群，您可以将多个安全模块组合成一个逻辑设备。集群具有单个设备的全部便捷性（管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。Firepower 9300 等多模块设备支持机箱内集群。

注释 在支持多个安全模块的 Firepower 4100/9300 机箱上，只能创建独立或集群一种类型的逻辑设备。换句话说，如果您已安装三个安全模块，则不能在一个安全模块上创建独立逻辑设备，使用剩余的两个逻辑设备创建集群。

注释 如果您正在配置独立逻辑设备，必须在机箱中的所有模块上安装同一类型软件；此时不支持不同的软件类型。请注意，模块可以运行特定设备类型的不同版本，但所有模块必须配置为同一类型的逻辑设备。

“逻辑设备 (Logical Devices)”页面

使用 Firepower 机箱管理器的“逻辑设备 (Logical Devices)”页面创建、编辑和删除逻辑设备。“逻辑设备 (Logical Devices)”页面包含每个 Firepower 4100/9300 机箱安全模块/引擎上安装的逻辑设备的信息区域。

每个逻辑设备区域的标头均提供以下信息：

- 逻辑设备的唯一名称。
- 安全模块/引擎上安装的主要应用的名称，即 ASA 或 FTD。
- 逻辑设备模式，即“独立 (Standalone)”或“集群 (Clustered)”。
- 状态 (Status) - 显示逻辑设备的状态：

  ok - 逻辑设备配置完成。

  incomplete-configuration - 逻辑设备配置未完成。

每个逻辑设备区域均提供以下信息：

- 安全模块 (Security Module) - 显示安全模块。
- 端口 (Ports) - 显示分配给应用实例的端口。
- 应用 (Application) - 显示安全模块上运行的应用。
- 版本 (Version) - 显示安全模块上运行的应用的软件版本号。

注释 对逻辑设备Firepower威胁防御进行的更新是通过Firepower管理中心完成的，而且所做的更新并未反映在Firepower机箱管理器中的**逻辑设备编辑 (Logical Devices > Edit)** 和**系统更新 (System > Updates)** 页面上。这些页面中显示的版本是指创建 Firepower 威胁防御逻辑设备所用的软件版本（CSP 映像）。

- 管理 IP (Management IP) - 显示分配作为逻辑设备管理 IP 的本地 IP 地址。
- 管理 URL (Management URL) - 显示分配给应用实例的管理 URL。
- 网关 (Gateway) - 显示分配给应用实例的网络网关地址。
- 管理端口 (Management Port) - 显示分配给应用实例的管理端口。
- 状态 (Status) - 显示应用实例的状态：

在线 (Online) - 应用正在运行和工作。

离线 (Offline) - 应用已停止并且不可操作。

正在安装 (Installing) - 应用安装正在进行。

未安装 (Not Installed) - 应用未安装。

安装失败 (Install Failed) - 应用安装失败。

正在启动 (Starting) - 应用正在启动。

启动失败 (Start Failed) - 应用启动失败。

已启动 (Started) - 应用成功启动，正在等待应用代理心跳。

正在停止 (Stopping) - 应用正在停止。

停止失败 (Stop Failed) - 应用无法进入离线状态。

未响应 (Not Responding) - 应用未响应。

正在更新 (Updating) - 应用软件正在升级。

更新失败 (Update Failed) - 应用软件升级失败。

更新成功 (Update Succeeded) - 应用软件升级成功。

创建独立的逻辑设备

您可以为安装在 Firepower 机箱中的每个安全模块/引擎创建独立的逻辑设备。

创建独立的 ASA 逻辑设备

您可以为 Firepower 4100/9300 机箱中安装的每个 安全模块/引擎 创建独立逻辑设备。在 Firepower 9300 等多模块设备上，如果您已配置了集群，则无法创建独立逻辑设备。您需要删除集群，然后才能配置独立设备。

注释 或者，您可以安装第三方 Radware DefensePro 虚拟平台，作为位于安全模块上 ASA 防火墙前面的 DDoS 检测和迁移服务（请参阅关于服务链，第 140 页）。

注释 您必须在机箱中的所有模块上安装同一类型软件；目前不支持使用其他类型的软件。请注意，模块可以运行特定设备类型的不同版本，但所有模块必须配置为同一类型的逻辑设备。

开始之前

- 如果您想用于逻辑设备的安全模块/引擎上已配置了逻辑设备，则必须首先删除现有的逻辑设备（请参阅删除逻辑设备，第 145 页）。
- 从 Cisco.com 下载要用于逻辑设备的应用映像（请参阅从 Cisco.com 下载映像，第 38 页），然后将映像上传到 Firepower 4100/9300 机箱（请参阅将映像上传到 Firepower 安全设备，第 38 页）。
- 配置逻辑设备要使用的管理接口。
- 您只能在 Firepower 4100/9300 机箱中部署路由防火墙模式 ASA。要将 ASA 更改为透明防火墙模式，请完成该程序，然后参阅将 ASA 更改为透明防火墙模式，第 146 页。

过程

步骤 1 选择**逻辑设备 (Logical Devices)** 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。

步骤 2 点击**添加设备 (Add Device)**，可打开**添加设备 (Add Device)** 对话框。

步骤 3 对于**设备名称 (Device Name)**，请为逻辑设备提供一个名称。

步骤 4 对于**模板 (Template)**，请选择**思科自适应安全设备 (Cisco Adaptive Security Appliance)**。

步骤 5 对于**映像版本 (Image Version)**，请选择 ASA 软件版本。

步骤 6 在**设备模式 (Device Mode)** 中，点击**独立 (Standalone)** 单选按钮。

步骤 7 点击**确定 (OK)**。
屏幕将显示调配 - 设备名称 *(Provisioning - device name)* 窗口。

步骤 8 展开**数据端口 (Data Ports)** 区域，然后点击要分配给设备的每个端口。

步骤 9 点击屏幕中心的设备图标。
系统将显示“ASA 配置 (ASA Configuration)”对话框。

步骤 10 在**常规信息 (General Information)** 选项卡上，完成以下操作：

a) 在 Firepower 9300 等多模块设备上，在“安全模块选择 (Security Module Selection)”下面，点击您想用于此逻辑设备的安全模块，将其选中。

b) 从**管理接口 (Management Interface)** 下拉列表中选择逻辑设备要使用的管理接口。

c) 在默认情况下，配置管理接口：
此信息用于配置安全模块/引擎配置中的管理接口。此管理 IP 地址也是将用于连接 ASDM 的 IP 地址。

1. 从**地址类型 (Address Type)** 下拉列表中选择地址类型。
2. 在**管理 IP (Management IP)** 字段中，配置本地 IP 地址。
3. 输入**网络掩码 (Network Mask)** 或**前缀长度 (Prefix Length)**。
4. 输入**网络网关 (Network Gateway)** 地址。

步骤 11 在**设置 (Settings)** 选项卡中，在**密码 (Password)** 字段中输入“管理员 (admin)”用户的密码。

步骤 12 点击**确定 (OK)** 关闭“ASA 配置”(ASA Configuration) 对话框。

步骤 13 点击**保存 (Save)**。
Firepower 可扩展操作系统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指定的安全模块/引擎来部署逻辑设备。

创建独立威胁防御逻辑设备

您可以为 Firepower 4100/9300 机箱中安装的每个 安全模块/引擎 创建独立逻辑设备。在 Firepower 9300 等多模块设备上，如果您已配置了集群，则无法创建独立逻辑设备。您需要删除集群，然后才能配置独立设备。

注释 或者，您可以安装第三方 Radware DefensePro 虚拟平台，作为位于安全模块上 Firepower 威胁防御逻辑设备前面的 DDoS 检测和迁移服务（请参阅关于服务链，第 140 页）。

注释 您必须在机箱中的所有模块上安装同一类型软件；目前不支持使用其他类型的软件。请注意，模块可以运行特定设备类型的不同版本，但所有模块必须配置为同一类型的逻辑设备。

开始之前

- 如果您想用于逻辑设备的安全模块/引擎上已配置了逻辑设备，必须首先删除现有的逻辑设备（请参阅删除逻辑设备，第 145 页）。
- 从 Cisco.com 下载要用于逻辑设备的应用映像（请参阅从 Cisco.com 下载映像，第 38 页），然后将映像上传到 Firepower 4100/9300 机箱（请参阅将映像上传到 Firepower 安全设备，第 38 页）。
- 配置逻辑设备要使用的管理接口。您还必须至少配置一个数据类型的接口。或者，您也可以创建 Firepower 事件接口，传输所有事件流量（例如 Web 事件）。

过程

步骤 1 选择**逻辑设备 (Logical Devices)** 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。

步骤 2 点击**添加设备 (Add Device)**，可打开**添加设备 (Add Device)** 对话框。

步骤 3 对于**设备名称 (Device Name)**，请为逻辑设备提供一个名称。

此名称由 Firepower 4100/9300 机箱 管理引擎用于配置管理设置以及分配接口；它不是在 安全模块/引擎 配置中使用的设备名称。

步骤 4 对于**模板 (Template)**，请选择 **Cisco Firepower 威胁防御 (Cisco Firepower Threat Defense)**。

步骤 5 对于**映像版本 (Image Version)**，请选择威胁防御软件版本。

步骤 6 在**设备模式 (Device Mode)** 中，点击**独立 (Standalone)** 单选按钮。

步骤 7 点击**确定 (OK)**。
屏幕将显示调配 - 设备名称 *(Provisioning - device name)* 窗口。

步骤 8 展开**数据端口 (Data Ports)** 区域，然后点击要分配给设备的每个端口。
具有硬件旁路功能的端口使用以下图标显示：。如果您未同时分配一个硬件旁路对中的两个接口，则会收到一条警告消息，确认您是故意这样分配。您不需要使用硬件旁路功能，因此如果您愿意，可以分配单个接口。

步骤 9 点击屏幕中心的设备图标。
系统将显示配置对话框。

步骤 10 在**常规信息 (General Information)** 选项卡上，完成以下操作：

a) 在 Firepower 9300 等多模块设备上，在“安全模块选择 (Security Module Selection)”下面，点击您想用于此逻辑设备的安全模块，将其选中。

b) 从**管理接口 (Management Interface)** 下拉列表中选择逻辑设备要使用的管理接口。
如果您分配一个支持硬件旁路功能的接口作为“管理(Management)”接口，则会收到一条警告消息，确认您是故意这样分配。

c) 在“管理 (Management)”下，配置管理接口：

1. 从**地址类型 (Address Type)** 下拉列表中选择地址类型。
2. 在**管理 IP (Management IP)** 字段中，配置本地 IP 地址。
3. 输入**网络掩码 (Network Mask)** 或**前缀长度 (Prefix Length)**。
4. 输入**网络网关 (Network Gateway)** 地址。

步骤 11 在**设置 (Settings)** 选项卡上，完成下列操作：

a) 在**注册密钥 (Registration Key)** 字段中，输入注册期间要在 Firepower 管理中心和设备之间共享的密钥。

b) 在**密码 (Password)** 字段中，输入设备密码。

c) 在 **Firepower 管理中心 IP (Firepower Management Center IP)** 字段中，输入执行管理的 Firepower 管理中心的 IP 地址。

d) 在**搜索域 (Search Domains)** 字段中，输入设备的搜索域列表（用逗号隔开）。

e) 选择防火墙模式：“透明 (Transparent)”或“路由 (Routed)”。

f) 在 **DNS 服务器 (DNS Servers)** 字段中，输入设备使用的 DNS 服务器列表，用逗号隔开。

g) 在**完全限定主机名 (Fully Qualified Hostname)** 字段中，输入威胁防御设备的完全限定名称。

h) 选择发送 Firepower 事件应当使用的接口。如果未指定，将使用管理接口。
要指定发送 Firepower 事件所用的接口，必须将接口配置为 *firepower-eventing* 接口。有关详细信息，请参阅关于 Firepower 安全设备接口，第 111 页。

步骤 12 在**协议 (Agreement)** 选项卡上，阅读并接受最终用户许可协议 (EULA)。

步骤 13 点击**确定 (OK)** 关闭配置对话框。

步骤 14 点击**保存 (Save)**。

Firepower可扩展操作系统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指定的安全模块/引擎来部署逻辑设备。

部署集群

通过集群，您可以将多台设备组合成单个逻辑设备。集群具有单个设备的全部便捷性（管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。包含多个模块的 Firepower 9300 支持机箱内集群，您可以将单个机箱中的所有模块组合到一个集群中。您还可使用将多个机箱分组在一起的机箱间集群；机箱间集群是单模块设备（例如 Firepower 4100 系列）的唯一选择。

关于 Firepower 4100/9300 机箱上的集群

集群由充当单一逻辑单元的多个设备组成。在 Firepower 4100/9300 机箱 上部署集群时，它执行以下操作：

- 为设备间通信创建集群控制链路（默认情况下，使用端口通道 48）。对于机箱内集群（仅限 Firepower 9300），此链路利用 Firepower 9300背板进行集群通信。对于机箱间集群，需要手动将物理接口分配到此 EtherChannel 以进行机箱间通信。
- 在应用中创建集群引导程序配置。

  在部署集群时，Firepower 4100/9300 机箱 管理引擎将最低引导程序配置推送到包含集群名称、集群控制链路接口及其他集群设置的每个设备。如果您需要自定义集群环境，可以在应用内对引导程序配置的某些用户可配置部分进行配置。
- 将数据接口作为跨网络接口分配给集群。

  对于机箱内集群，跨网络接口不仅限于EtherChannel，与机箱间集群类似。Firepower 9300 管理引擎在内部利用 EtherChannel 技术，将流量负载均衡到共享接口上的多个模块，使任何数据接口类型都可用于跨网络模式。对于机箱间集群，必须对所有数据接口使用跨网络EtherChannel。

  注释 除管理接口以外，不支持单个接口。
- 向集群中的所有设备分配管理接口。

以下部分提供有关集群概念和实施的更多详细信息。

主设备角色和辅助设备角色

集群的一个成员是主设备。系统自动确定主设备。所有其他成员都是辅助设备。

您必须仅在主设备上执行所有配置；然后，配置将复制到辅助设备。

群集控制链接

集群控制链路使用端口通道48接口自动进行创建。对于机箱内集群，此接口没有成员接口。对于机箱间集群，必须将一个或多个接口添加到 EtherChannel。此集群类型 EtherChannel 利用 Firepower 9300 背板进行机箱内集群的集群通信。

对于包含 2 个成员的机箱间集群，请勿直接将集群控制链路从一个机箱连接到另一个机箱。如果直接连接两个接口，则当一台设备发生故障时，集群控制链路失效，会导致剩下的那台正常设备也发生故障。而如果通过交换机连接集群控制链路，则集群控制链路仍会对正常设备打开。

集群控制链路流量包括控制流量和数据流量。

设定机箱间集群的集群控制链路大小

如果可能，应将集群控制链路的大小设定为与每个机箱的预期吞吐量匹配，以使集群控制链路可以处理最坏情况。

集群控制链路流量主要由状态更新和转发的数据包组成。集群控制链路在任一给定时间的流量大小不尽相同。转发流量的大小取决于负载均衡的效率或是否存在大量用于集中功能的流量。例如：

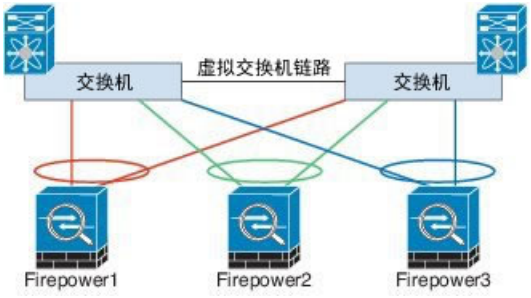
- NAT 会使连接的负载均衡不佳，需要对所有返回流量进行再均衡，将其转发到正确的设备。
- 当成员身份更改时，集群需要对大量连接进行再均衡，因此会暂时耗用大量集群控制链路带宽。

带宽较高的集群控制链路可以帮助集群在发生成员身份更改时更快地收敛，并防止出现吞吐量瓶颈。

注释 如果集群中存在大量非对称（再均衡）流量，应增加集群控制链路的吞吐量大小。

机箱间集群的集群控制链路冗余

下图显示了如何在虚拟交换系统 (VSS) 或虚拟端口通道 (vPC) 环境中使用 EtherChannel 作为集群控制链路。EtherChannel 中的所有链路都是活动链路。当交换机是 VSS 或 vPC 的一部分时，您可以将同一 EtherChannel 中的 Firepower 4100/9300 机箱接口连接到 VSS 或 vPC 中不同的交换机。交换机接口是同一个 EtherChannel 端口通道接口的成员，因为两台单独的交换机的行为就像一台交换机一样。请注意，此 EtherChannel 是设备本地的，而非跨网络 EtherChannel。



机箱间集群的集群控制链路可靠性

为了确保集群控制链路的功能，设备之间的往返时间 (RTT) 务必要小于 20 毫秒。此最大延迟能够增强与不同地理位置安装的集群成员的兼容性。要检查延迟，请在设备之间的集群控制链路上执行 ping 操作。

集群控制链路必须可靠，没有数据包无序或丢弃数据包的情况；例如，站点间部署应使用专用链路。

集群控制链路网络

Firepower 4100/9300 机箱会根据机箱 ID 和插槽 ID 自动生成每台设备的集群控制链路接口 IP 地址：127.2.*chassis_id*.*slot_id*。无论在 FXOS 中还是在应用中，您都无法手动设置此 IP 地址。集群控制链路网络不能包含设备之间的任何路由器；仅允许第 2 层交换。对于站点间流量，思科建议使用重叠传输虚拟化 (OTV)。

管理网络

我们建议将所有设备都连接到一个管理网络。此网络与集群控制链路分隔开来。

管理界面

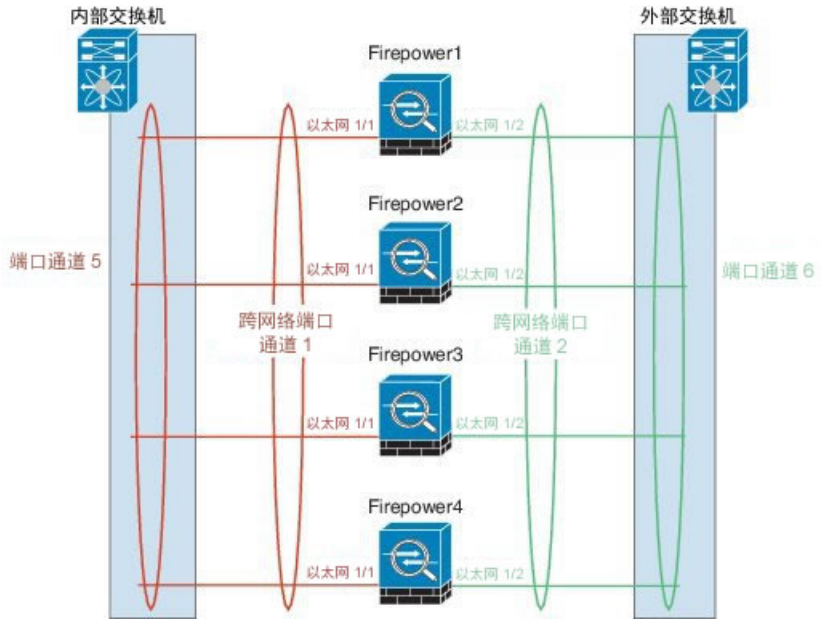
您可以向集群分配管理 (Management) 类型接口。此接口是相对于跨网络 (Spanned) 接口的特殊单独接口。通过管理接口，可以直接连接到每个设备。

对于 ASA，主集群 IP 地址是始终属于当前主设备的集群的固定地址。您也可以配置一个地址范围，使每个设备（包括当前主设备在内）都能使用该范围内的本地地址。主集群 IP 地址提供对地址的统一管理访问权限；当主设备更改时，主集群 IP 地址将转移给新的主设备，使集群管理可以无缝衔接。本地 IP 地址用于路由，在排除故障时也非常有用。例如，可以通过连接到主集群 IP 地址来管理集群，该地址始终连接到当前主设备。要管理单个成员，您可以连接到本地 IP 地址。对于 TFTP 或系统日志等出站管理流量，包括主设备在内的每个设备都使用本地 IP 地址来连接到服务器。

对于 Firepower 威胁防御，请向同一网络上的每个设备分配管理 IP 地址。将每个设备连接到 管理中心时，请使用这些 IP 地址。

跨网络 EtherChannel

您可以将每个机箱的一个或多个接口组成跨集群中所有机箱的 EtherChannel。EtherChannel 汇聚通道中所有可用活动接口上的流量。在路由模式和透明防火墙模式下都可以配置跨网络 EtherChannel。在路由模式下，EtherChannel 被配置为只有一个 IP 地址的路由接口。在透明模式下，IP 地址分配到 BVI 而非网桥组成员接口。负载均衡属于 EtherChannel 固有的基本操作。



站点间集群

对于站点间安装，您只要遵循建议的准则即可充分发挥集群的作用。

您可以将每个集群机箱配置为属于单独的站点 ID。

站点 ID 与站点特定的 MAC 地址和 IP 地址配合使用。集群发送的数据包使用站点特定的 MAC 地址和 IP 地址，而集群接收的数据包使用全局 MAC 地址和 IP 地址。此功能可防止交换机从两个不同端口上的两个站点获知相同全局 MAC 地址，导致 MAC 地址摆动；相反，它们仅获知站点 MAC 地址。只有使用跨网络 EtherChannel 的路由模式支持站点特定的 MAC 地址和 IP 地址。

站点 ID 还用于启用流移动性，从而使用 LISP 检测和导向器本地化为数据中心的站点间集群提高性能并缩短往返时间延迟。

有关站点间集群的详细信息，请参阅以下各节：

- 确定数据中心互联的规格 -集群必备条件，第 127 页
- 站点间准则 -面向集群的指导原则，第 128 页
- 站点间示例 -站点间集群示例，第 137 页

集群必备条件

机箱间硬件和软件要求

集群中的所有机箱：

- 对于 Firepower 4100 系列：所有机箱必须为同一型号。对于 Firepower 9300：所有安全模块必须为同一类型。您可以在各机箱中安装不同数量的安全模块，但机箱中存在的所有模块（包括任何空插槽）必须属于集群。
- 除进行映像升级外，必须运行完全相同的 FXOS 软件。
- 对于分配给集群的接口，必须采用相同的接口配置，例如：相同的管理接口、EtherChannel、主用接口、速度和复用等。您可在机箱中使用不同的网络模块类型，但必须满足以下条件：对于相同接口 ID，容量必须匹配，且接口可成功捆绑于同一跨网络 EtherChannel 中。请注意，所有数据接口必须是机箱间集群中的 EtherChannel。
- 必须使用同一台 NTP 服务器。对于 Firepower 威胁防御，Firepower 管理中心也必须使用同一 NTP 服务器。请勿手动设置时间。
- ASA：每个 FXOS 机箱都必须注册到许可证颁发机构或卫星服务器。辅助设备不会产生额外成本。对于预留永久许可证，必须为每个机箱购买单独的许可证。对于 Firepower 威胁防御，所有许可由 Firepower 管理中心处理。

机箱间集群交换机必备条件

- 请务必先完成交换机配置并将机箱中的所有 EtherChannel 成功连接至交换机后，再在 Firepower 4100/9300 机箱 上配置集群。
- 有关受支持的交换机列表，请参阅《思科 FXOS 兼容性》。

调整站点间集群的数据中心互联

您应在数据中心互联 (DCI) 上为集群控制链路流量保留等同于以下计算结果的带宽：

$$\frac{\text{每个站点的集群成员数量}}{2} \times \text{每个成员的集群控制链路大小}$$

如果各站点的成员数不同，请使用较大的数量进行计算。DCI 的最低带宽不得低于一个成员的集群控制链路的流量大小。

例如：

- 位于 4 个站点的 2 个成员：

  总共 4 个集群成员

  每个站点 2 个成员

  每个成员 5 Gbps 集群控制链路

保留的 DCI 带宽 = 5 Gbps (2/2 x 5 Gbps)。

- 对位于 3 个站点的 6 个成员而言，规格加大：

  总共 6 个集群成员

  站点 1 有 3 个成员，站点 2 有 2 个成员，站点 3 有 1 个成员

  每个成员 10 Gbps 集群控制链路

  保留的 DCI 带宽 = 15 Gbps (3/2 x 10 Gbps)。

- 位于 2 个站点的 2 个成员：

  总共 2 个集群成员

  每个站点 1 个成员

  每个成员 10 Gbps 集群控制链路

  保留的 DCI 带宽 = 10 Gbps（1/2 x 10 Gbps = 5 Gbps；但最低带宽不得低于集群控制链路的流量大小 (10 Gbps)）。

面向集群的指导原则

模式

- Firepower 9300 上的 ASA - 支持机箱内、机箱间和站点间集群。
- Firepower 4100 系列 上的 ASA - 支持机箱间和站点间集群。
- Firepower 9300 上的 Firepower 威胁防御 - 支持机箱内和机箱间集群。
- Firepower 4100 系列 上的 Firepower 威胁防御 - 支持机箱间集群。
- Radware DefensePro - 对于包含 ASA 的机箱内集群受支持。
- Radware DefensePro - 对于包含 Firepower 威胁防御的机箱内集群受支持。

机箱间集群的交换机

- 对于 ASR 9006，如果要设置非默认 MTU，请将 ASR 接口 MTU 设置为高于集群设备 MTU 14 个字节。除非使用 **mtu-ignore** 选项，否则 OSPF 邻近对等尝试可能会失败。请注意，集群设备 MTU 应与 ASR *IPv4* MTU 匹配。
- 在用于集群控制链路接口的交换机上，您可以选择在连接到集群设备的交换机端口上启用生成树 PortFast 来加快新设备加入集群的过程。
- 当发现交换机上跨网络 EtherChannel 的绑定速度缓慢时，可以对交换机上的单个接口启用快速 LACP 速率。请注意，在执行运行中软件升级 (ISSU) 时，某些交换机（如 Nexus 系列）不支持快速 LACP 速率，因此我们不建议将 ISSU 用于集群。

- 在交换机上，我们建议使用以下其中一种 EtherChannel 负载均衡算法：**source-dest-ip** 或 **source-dest-ip-port**（请参阅思科 Nexus OS 和思科 IOS **port-channel load-balance** 命令）。请勿在负载均衡算法中使用关键字 **vlan**，否则会导致传输到集群中的设备的流量分摊不均。
- 如果在交换机上更改 EtherChannel 的负载均衡算法，则交换机上的 EtherChannel 接口将暂时停止转发流量，生成树协议重新启动。在流量再次开始传输之前会存在延迟。
- 集群控制链路路径上的交换机不应验证第 4 层校验和。集群控制链路上的重定向流量没有正确的第 4 层校验和。交换机验证第 4 层校验和可能导致流量被丢弃。
- 端口通道绑定中断时间不得超过配置的 keepalive 间隔。
- 在 Supervisor 2T EtherChannel 上，默认的散列值分配算法是自适应算法。为了避免 VSS 设计中的非对称流量，请将连接到集群设备的端口通道上的散列算法更改为固定：

  router(config)# **port-channel** *id***hash-distributionfixed**

  请勿全局更改算法；您可能需要对 VSS 对等链路使用自适应算法。

机箱间集群的 EtherChannel

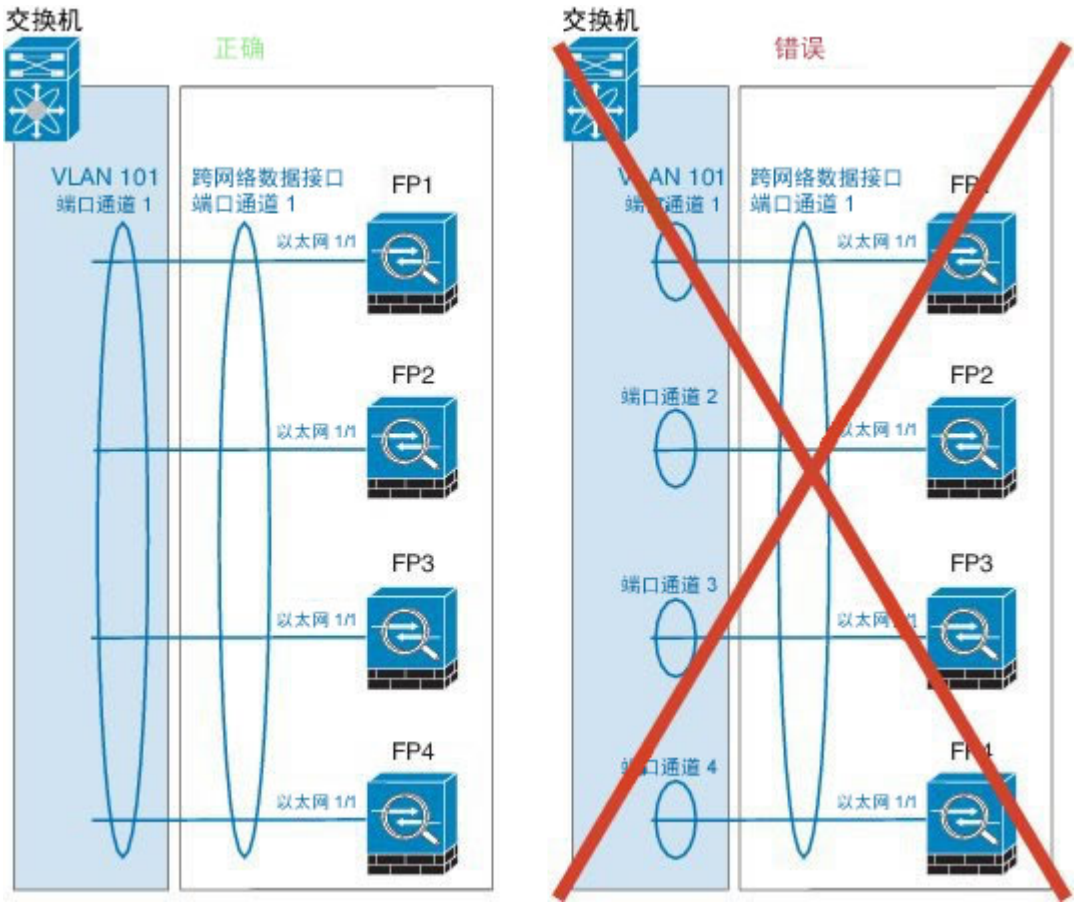
- 为了连接交换机，请将 EtherChannel 模式设置为 Active；Firepower 4100/9300 机箱 不支持 ON 模式，甚至对于集群控制链路也是如此。
- 默认情况下系统将 FXOS EtherChannel 的 LACP 速率设为正常。此设置可能使端口通道成员的捆绑时间超过 30 秒，从而导致集群接口运行状况检查失败，这会让设备从集群中删除。我们建议您将 LACP 速率更改为快速。以下示例修改了“默认”lacp 策略：

```
firepower# scope org
firepower /org # scope lacppolicy default
firepower /org/lacppolicy# set lacp-rate fast
firepower /org* # commit-buffer
```

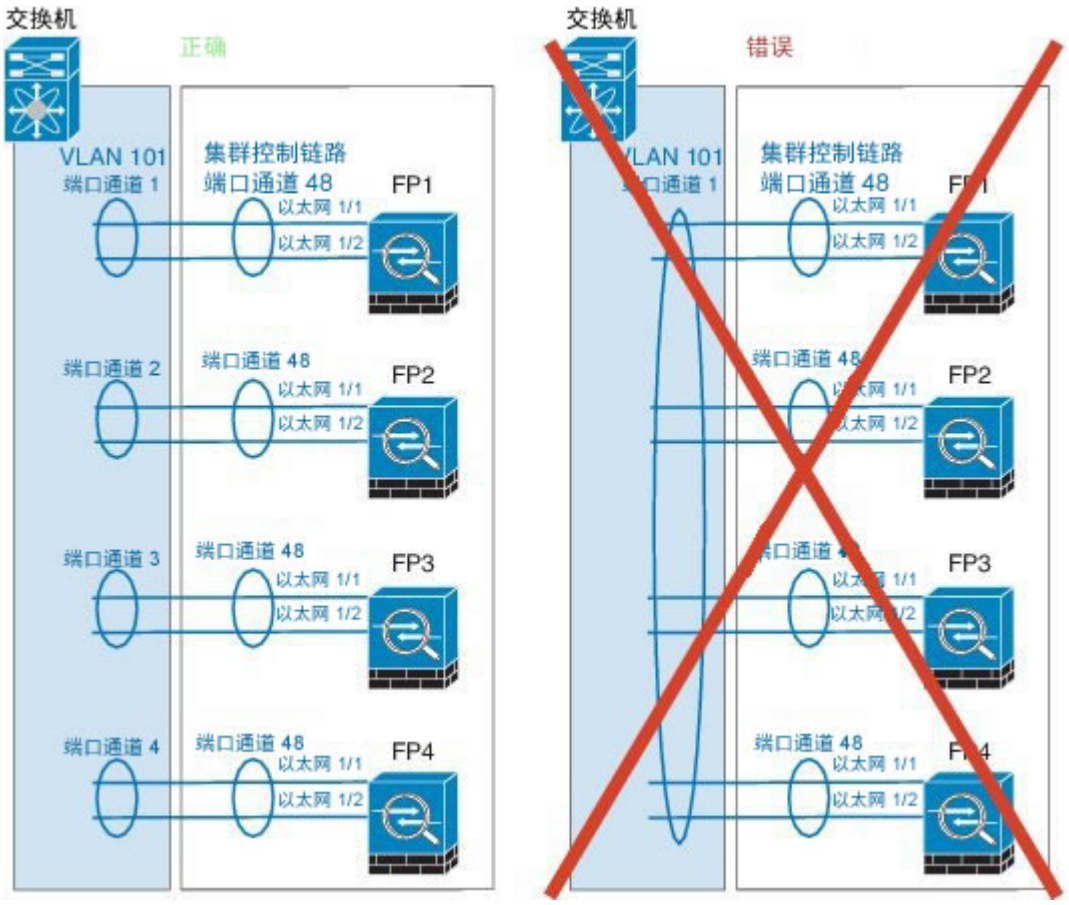
注释 在执行运行中软件升级 (ISSU) 时，某些交换机（如 Nexus 系列）不支持快速 LACP 速率，因此我们不建议将 ISSU 用于集群。

- 在低于 15.1(1)S2 的 Catalyst 3750-X 思科 IOS 软件版本中，此集群设备不支持将 EtherChannel 连接到交换机堆叠。在默认交换机设置下，如果跨堆叠连接集群设备 EtherChannel，则当主交换机关闭时，连接到其余交换机的 EtherChannel 不会正常工作。要提高兼容性，请将 **stack-mac persistent timer** 命令设置为一个足够大的值，以考虑重新加载时间；例如，8 分钟或无限接近 0。或者，您可以升级到更加稳定的交换机软件版本，例如 15.1(1)S2。
- 跨网络与设备本地 EtherChannel 配置 - 请务必为跨网络 EtherChannel 和设备本地 EtherChannel 适当地配置交换机。

  跨网络 EtherChannel - 对于跨越所有集群成员的集群设备跨网络 EtherChannel，所有接口在交换机上合并为一个 EtherChannel。请确保每个接口都属于交换机上的同一个通道组。



设备本地 EtherChannel - 对于集群设备本地 EtherChannels，包括为集群控制链路配置的任何 EtherChannel，请务必在交换机上配置分散的 EtherChannel；请勿在交换机上将多个集群设备 EtherChannel 合并为一个 EtherChannel。



其他规定

- 我们建议将 EtherChannel 连接到 VSS 或 vPC，以实现冗余。
- 在机箱内，您不能对某些安全模块进行集群，也不能在单机模式下运行其他安全模块；必须在集群内包含所有安全模块。

集群默认设置

集群控制链路使用端口通道 48。

配置 ASA 集群

您可以从 Firepower 4100/9300 机箱管理引擎轻松部署集群。自动为每台设备生成所有初始配置。对于机箱间集群，您必须单独配置每个机箱。在一个机箱上部署集群；然后，您可以将引导程序配置从第一个机箱复制到下一个机箱，实现轻松部署。

开始之前

- 您必须对 Firepower 9300 机箱中全部 3 个模块插槽启用集群，即使您没有安装模块。如果不配置全部 3 个模块，集群将不会正常工作。
- 在**接口 (Interfaces)** 选项卡上，如果不包括任何成员接口，则端口通道 48 集群类型接口的**运行状态 (Operation State)**将显示为**失败 (failed)**。对于机箱内集群，此 EtherChannel 无需任何成员接口，您可忽略此“运行状态 (Operational State)”。
- 您只能在 Firepower 4100/9300 机箱中部署路由防火墙模式 ASA 集群。要将 ASA 集群更改为透明防火墙模式，请完成该程序，然后参阅将 ASA 更改为透明防火墙模式，第 146 页。

过程

步骤 1 部署集群之前，至少添加一个“数据 (Data)”类型接口或 EtherChannel（也称为端口通道）。请参阅创建端口通道，第 115 页或编辑接口属性，第 114 页。
部署之后，您也可以将数据接口添加到集群。

对于机箱间集群，所有数据接口必须为至少带有一个成员接口的 EtherChannel。在每个机箱上添加同一 EtherChannel。

步骤 2 添加“管理 (Management)”类型接口或 EtherChannel。请参阅创建端口通道，第 115 页或编辑接口属性，第 114 页。
对于机箱间集群，在各机箱上添加相同的“管理 (Management)”接口。

步骤 3 对于机箱间集群，向端口通道 48 添加成员接口，用作集群控制链路。
如果不包含成员接口，那么当您部署逻辑设备时，Firepower 机箱管理器 会认为此集群为机箱内集群，并且不显示**机箱 ID (Chassis ID)** 字段。在各机箱上添加相同的成员接口。

步骤 4 选择**逻辑设备 (Logical Devices)** 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。

步骤 5 点击**添加设备 (Add Device)**，可打开**添加设备 (Add Device)** 对话框。
如果您目前有一个集群，系统将提示您删除该集群并添加新集群。安全模块上的所有集群相关配置将被新信息代替。

步骤 6 对于**设备名称 (Device Name)**，请为逻辑设备提供一个名称。Firepower 4100/9300 机箱管理引擎使用该名称配置集群设置以及分配接口；该名称不是在安全模块配置中使用的集群名称。

步骤 7 对于**模板 (Template)**，请选择**思科自适应安全设备 (Cisco Adaptive Security Appliance)**。

步骤 8 对于**映像版本 (Image Version)**，请选择 ASA 软件版本。

步骤 9 在**设备模式 (Device Mode)** 中，点击**集群 (Cluster)** 单选按钮。

步骤 10 点击**创建新集群 (Create New Cluster)** 单选按钮。

步骤 11 点击 **OK**。
如果您配置了任何独立设备，系统将提示您用新集群替代它们。屏幕将显示调配 - 设备名称 *(Provisioning - device name)* 窗口。

默认情况下，所有接口都会分配给集群。

步骤 12 点击屏幕中心的设备图标。
系统将显示“ASA 配置 (ASA Configuration)”对话框，其中**集群信息 (Cluster Information)** 选项卡已选定。

步骤 13 在**机箱 ID (Chassis ID)** 字段中，输入机箱 ID。集群中的每个机箱都必须使用唯一 ID。

步骤 14 对于站点间集群，在**站点 ID (Site ID)** 字段中输入此机箱的站点 ID（1 和 8 之间的整数）。

步骤 15 在**集群密钥 (Cluster Key)** 字段中，为集群控制链路上的控制流量配置身份验证密钥。
共享密钥是长度为 1 到 63 个字符的 ASCII 字符串。共享密钥用于生成密钥。此选项不影响数据路径流量，包括连接状态更新和转发的数据包，它们始终以明文发送。

步骤 16 设置**集群组名称 (Cluster Group Name)**，这是安全模块配置中的集群组名称。
名称必须是长度为 1 到 38 个字符的 ASCII 字符串。

步骤 17 点击**管理接口 (Management Interface)**，选择您之前创建的管理接口。

步骤 18 选择管理接口的**地址类型 (Address Type)**。
此信息用于配置安全模块配置中的管理接口。

a) 在**管理 IP 池 (Management IP Pool)** 字段中，配置本地 IP 地址池，其中一个地址将分配给接口的每个集群设备，方法是输入以连字符分隔的起始地址和结束地址。
至少包含与集群中的设备数量相同的地址。请注意，对于 Firepower 9300，每台机箱必须包括 3 个地址，即使未填满所有模块插槽。如果计划扩展集群，则应包含更多地址。属于当前主设备的虚拟 IP 地址（称作“主集群 IP 地址”）不在此地址池中；请务必在同一个网络中为主集群 IP 地址保留一个 IP 地址。您可以使用 IPv4 和/或 IPv6 地址。

b) 输入**网络掩码 (Network Mask)** 或**前缀长度 (Prefix Length)**。

c) 输入**网络网关 (Network Gateway)**。

d) 输入**虚拟 IP 地址 (Virtual IP address)**。
此 IP 地址必须与集群池地址属于同一个网络，但不在地址池中。

步骤 19 在**设置 (Settings)** 选项卡中，对于**密码 (Password)**，输入“管理员 (admin)”用户的密码。

步骤 20 点击**确定 (OK)** 关闭“ASA 配置”(ASA Configuration) 对话框。

步骤 21 点击**保存 (Save)**。
Firepower 4100/9300 机箱管理引擎通过下载指定的软件版本并向每个安全模块推送集群引导程序配置和管理接口设置来部署集群。

步骤 22 对于机箱间集群，将下一个机箱添加到集群中：

a) 在第一个机箱 Firepower 机箱管理器上，点击右上角的**显示集群详细信息 (Show Cluster Details)** 图标；复制显示的集群配置。

b) 连接到下一机箱上的 Firepower 机箱管理器，并按照此程序添加逻辑设备。

c) 选择**加入现有集群 (Join an Existing Cluster)**。

d) 点击**复制配置 (Copy config)** 复选框，然后点击**确定 (OK)**。如果取消选中此复选框，必须手动输入设置，以匹配第一个机箱配置。

e) 在**复制集群详细信息 (Copy Cluster Details)** 对话框中，粘贴第一个机箱的集群配置，然后点击**确定 (OK)**。

f) 点击屏幕中心的设备图标。集群信息通常已预填充，但您必须更改以下设置：

- **机箱 ID (Chassis ID)** - 输入唯一的机箱 ID。
- **站点 ID (Site ID)** - 输入正确的站点 ID。
- **集群密钥 (Cluster Key)** -（未预填充）输入相同的集群密钥。

点击 **OK**。

g) 点击 **Save**。

步骤 23 连接到主设备安全模块以自定义集群配置。

配置 Firepower 威胁防御集群

您可以从 Firepower 4100/9300 机箱管理引擎轻松部署集群。自动为每台设备生成所有初始配置。 对于机箱间集群，您必须单独配置每个机箱。在一个机箱上部署集群；然后，您可以将引导程序配置从第一个机箱复制到下一个机箱，实现轻松部署。

开始之前

- 您必须对 Firepower 9300 机箱中全部 3 个模块插槽启用集群，即使您没有安装模块。如果不配置全部 3 个模块，集群将不会正常工作。
- 在**接口 (Interfaces)** 选项卡上，如果不包括任何成员接口，则端口通道 48 集群类型接口的**运行状态 (Operation State)**将显示为**失败 (failed)**。对于机箱内集群，此 EtherChannel 无需任何成员接口，您可忽略此“运行状态 (Operational State)”。

过程

步骤 1 部署集群之前，至少添加一个“数据 (Data)”类型接口或 EtherChannel（也称为端口通道）。
部署之后，您也可以将数据接口添加到集群。

对于机箱间集群，所有数据接口必须为至少带有一个成员接口的 EtherChannel。在每个机箱上添加同一 EtherChannel。

步骤 2 添加“管理 (Management)”类型接口或 EtherChannel。
对于机箱间集群，在各机箱上添加相同的“管理 (Management)”接口。

步骤 3 对于机箱间集群，向端口通道 48 添加成员接口，用作集群控制链路。
如果不包含成员接口，那么当您部署逻辑设备时，Firepower 机箱管理器 会认为此集群为机箱内集群，并且不显示**机箱 ID (Chassis ID)** 字段。在各机箱上添加相同的成员接口。

步骤 4 （可选） 添加 Firepower 事件接口。

此接口是 Firepower 威胁防御设备的二级管理接口。要使用此接口，您必须在 Firepower 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 Firepower 威胁防御命令参考中的 **configure network** 命令。

对于机箱间集群，在各机箱上添加相同的事件接口。

步骤 5 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。

步骤 6 点击**添加设备 (Add Device)**，可打开**添加设备 (Add Device)** 对话框。
如果存在现有逻辑设备，系统会提示您删除该设备并添加新的逻辑设备。设备上的所有配置都将替换为新的信息。

步骤 7 对于**设备名称 (Device Name)**，请为逻辑设备提供一个名称。Firepower 4100/9300 机箱管理引擎使用此名称来配置集群/管理设置以及分配接口；该名称不是逻辑设备配置中使用的集群名称。

步骤 8 对于**模板 (Template)**，请选择**思科 Firepower 威胁防御 (Cisco Firepower Threat Defense)**。

步骤 9 对于**映像版本 (Image Version)**，请选择 Firepower 威胁防御软件版本。确保此版本与您的 FXOS 版本及 Firepower 管理中心版本兼容。

步骤 10 在**设备模式 (Device Mode)** 中，点击**集群 (Cluster)** 单选按钮。

步骤 11 点击**创建新集群 (Create New Cluster)** 单选按钮。

步骤 12 点击 **OK**。
如果您配置了任何独立设备，系统将提示您用新集群替代它们。您会看到**调配-设备名称 (Provisioning - *device name)*** 窗口。

默认情况下，所有接口都会分配给集群。具有硬件旁路功能的端口使用以下图标显示：  。如果您未同时分配一个硬件旁路对中的两个接口，则会收到一条警告消息，确认您是故意这样分配。您不需要使用硬件旁路功能，因此如果您愿意，可以分配单个接口。 机箱间集群不支持硬件旁路端口，因为不支持将其作为 EtherChannel 成员。

步骤 13 点击屏幕中心的设备图标。
此时将显示**思科 Firepower 威胁防御配置 (Cisco Firepower Threat Defense Configuration)** 对话框。

步骤 14 在**集群信息 (Cluster Information)** 选项卡上，填写以下字段：

a) 在**机箱 ID (Chassis ID)** 字段中，输入机箱 ID。集群中的每个机箱都必须使用唯一 ID。

b) 在**集群密钥 (Cluster Key)** 字段中，为集群控制链路上的控制流量配置身份验证密钥。
共享密钥是长度为 1 到 63 个字符的 ASCII 字符串。共享密钥用于生成密钥。此选项不影响数据路径流量，包括连接状态更新和转发的数据包，它们始终以明文发送。

c) 设置**集群组名称 (Cluster Group Name)**，即逻辑设备配置中的集群组名称。
名称必须是长度为 1 到 38 个字符的 ASCII 字符串。

d) 从**管理接口 (Management Interface)** 下拉列表中选择逻辑设备要使用的管理接口。
如果您分配一个支持硬件旁路功能的接口作为管理接口，则会收到一条警告消息，确认您是故意这样分配。

步骤 15 在**设置 (Settings)** 选项卡上，完成下列操作：

a) 在**注册密钥 (Registration Key)** 字段中，输入注册期间 Firepower 管理中心与集群成员之间要共享的密钥。
b) 在**密码 (Password)** 字段中，输入集群中管理员用户的密码。
c) 在 **Firepower 管理中心 IP (Firepower Management Center IP)** 字段中，输入执行管理的 Firepower 管理中心的 IP 地址。
d) 在**搜索域 (Search Domains)** 字段中，输入管理网络的搜索域逗号分隔列表。
e) 从**防火墙模式 (Firewall Mode)** 下拉列表中选择**透明 (Transparent)** 或**路由 (Routed)**。
f) 在 **DNS 服务器 (DNS Servers)** 字段中，输入 Firepower 威胁防御设备应在管理网络中使用的 DNS 服务器逗号分隔列表。
g) 在**完全限定主机名 (Fully Qualified Hostname)** 字段中，输入 Firepower 威胁防御设备的完全限定名称。
h) 从**事件接口 (Eventing Interface)** 下拉列表中，选择发送 Firepower 事件时应当使用的接口。如果未指定，系统将使用管理接口。
要指定发送 Firepower 事件所用的独立接口，必须将接口配置为 *firepower-eventing* 接口。如果您分配一个支持硬件旁路功能的接口作为事件接口，则会收到一条警告消息，确认您是故意这样分配的。

步骤 16 在**接口信息 (Interface Information)** 选项卡中，为集群中的每个安全模块配置一个管理 IP 地址。从**地址类型 (Address Type)** 下拉列表中选择地址类型，然后为每个安全模块填写以下字段。
注释 您必须为机箱中全部 3 个模块插槽设置 IP 地址，即使您没有安装模块。如果不配置全部 3 个模块，集群将不会正常工作。
a) 在**管理 IP (Management IP)** 字段中，配置 IP 地址。
在同一网络上为每个模块指定 IP 地址。
b) 输入**网络掩码 (Network Mask)** 或**前缀长度 (Prefix Length)**。
c) 输入**网络网关 (Network Gateway)** 地址。

步骤 17 在**协议 (Agreement)** 选项卡上，阅读并接受最终用户许可协议 (EULA)。

步骤 18 点击**确定 (OK)** 以关闭**思科 Firepower 威胁防御配置 (Cisco Firepower Threat Defense Configuration)** 对话框。

步骤 19 点击**保存 (Save)**。
Firepower 4100/9300 机箱管理引擎通过下载指定的软件版本并向每个安全模块推送集群引导程序配置和管理接口设置来部署集群。

步骤 20 对于机箱间集群，将下一个机箱添加到集群中：
a) 在第一个机箱 Firepower 机箱管理器上，点击右上角的**显示集群详细信息 (Show Cluster Details)** 图标；复制显示的集群配置。
b) 连接到下一机箱上的 Firepower 机箱管理器，并按照此程序添加逻辑设备。
c) 选择**加入现有集群 (Join an Existing Cluster)**。
d) 点击**复制配置 (Copy config)** 复选框，然后点击**确定 (OK)**。如果取消选中此复选框，必须手动输入设置，以匹配第一个机箱配置。
e) 在**复制集群详细信息 (Copy Cluster Details)** 对话框中，粘贴第一个机箱的集群配置，然后点击**确定 (OK)**。
f) 点击屏幕中心的设备图标。集群信息通常已预填充，但您必须更改以下设置：

- **机箱 ID (Chassis ID)** - 输入唯一的机箱 ID。
- **集群密钥 (Cluster Key)** -（未预填充）输入相同的集群密钥。
- **管理 IP (Management IP)** - 将每个模块的管理地址更改为与其他集群成员位于同一网络中的唯一 IP 地址。

点击 **OK**。

g）点击 **Save**。

步骤 21 使用管理 IP 地址将每台设备单独添加到 Firepower 管理中心，然后在 Web 界面上将它们组成集群。所有集群设备必须在 FXOS 上已成功建立的集群中，然后才可将其添加到 Firepower 管理中心 中。

站点间集群示例

以下示例显示支持的集群部署。

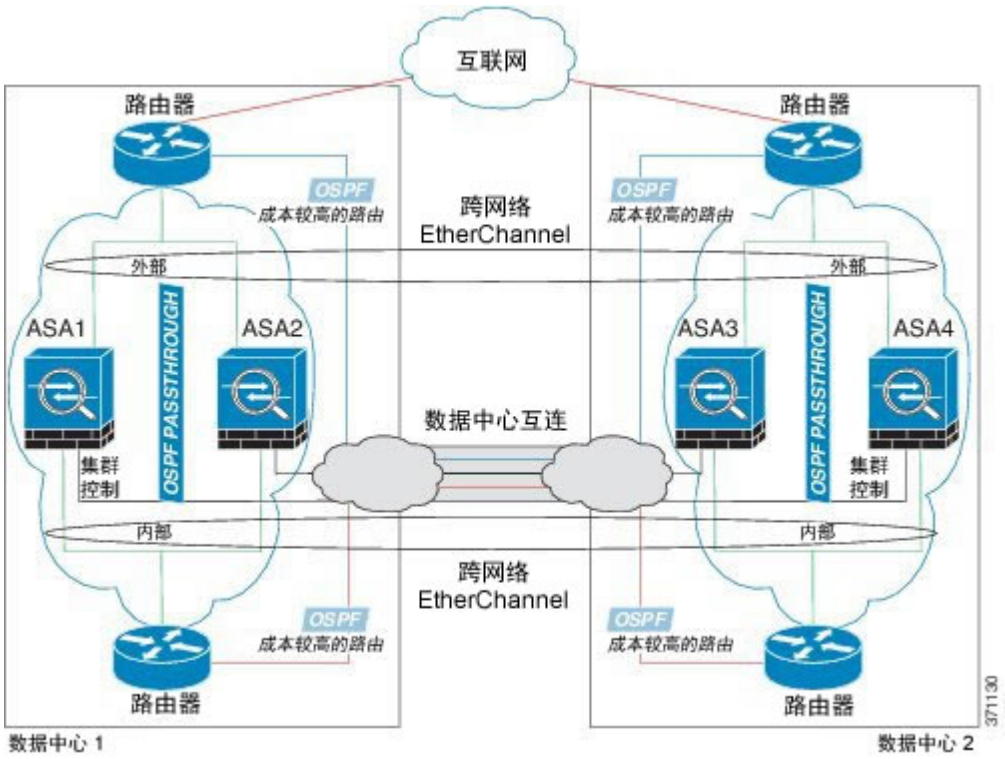
跨网络 EtherChannel 透明模式南北站点间集群示例

以下示例显示了 2 个集群成员，这两个集群成员分别位于 2 个部署在内部和外部路由器之间（南北插入）的数据中心。集群成员由集群控制链路通过 DCI 连接。位于每个站点的集群成员使用面向内部和外部的跨网络 EtherChannel 连接到本地交换机。每个 EtherChannel 跨越集群中的所有机箱。

位于每个数据中心的内部和外部路由器均使用 OSPF（可通过透明的 ASA）。与 MAC 地址不同，路由器 IP 地址在所有路由器上都是唯一的。通过指定 DCI 中开销较高的路由，可将流量保持在每个数据中心内，除非给定站点上的所有集群成员都中断连接。通过 ASA 的开销较低的路由必须经过位于每个站点的同一网桥组才能使集群维持非对称连接。如果位于一个站点的所有集群成员都发生故障，流量将从每台路由器通过 DCI 发往位于另一个站点的集群成员。

位于每个站点的交换机的实施可包括：

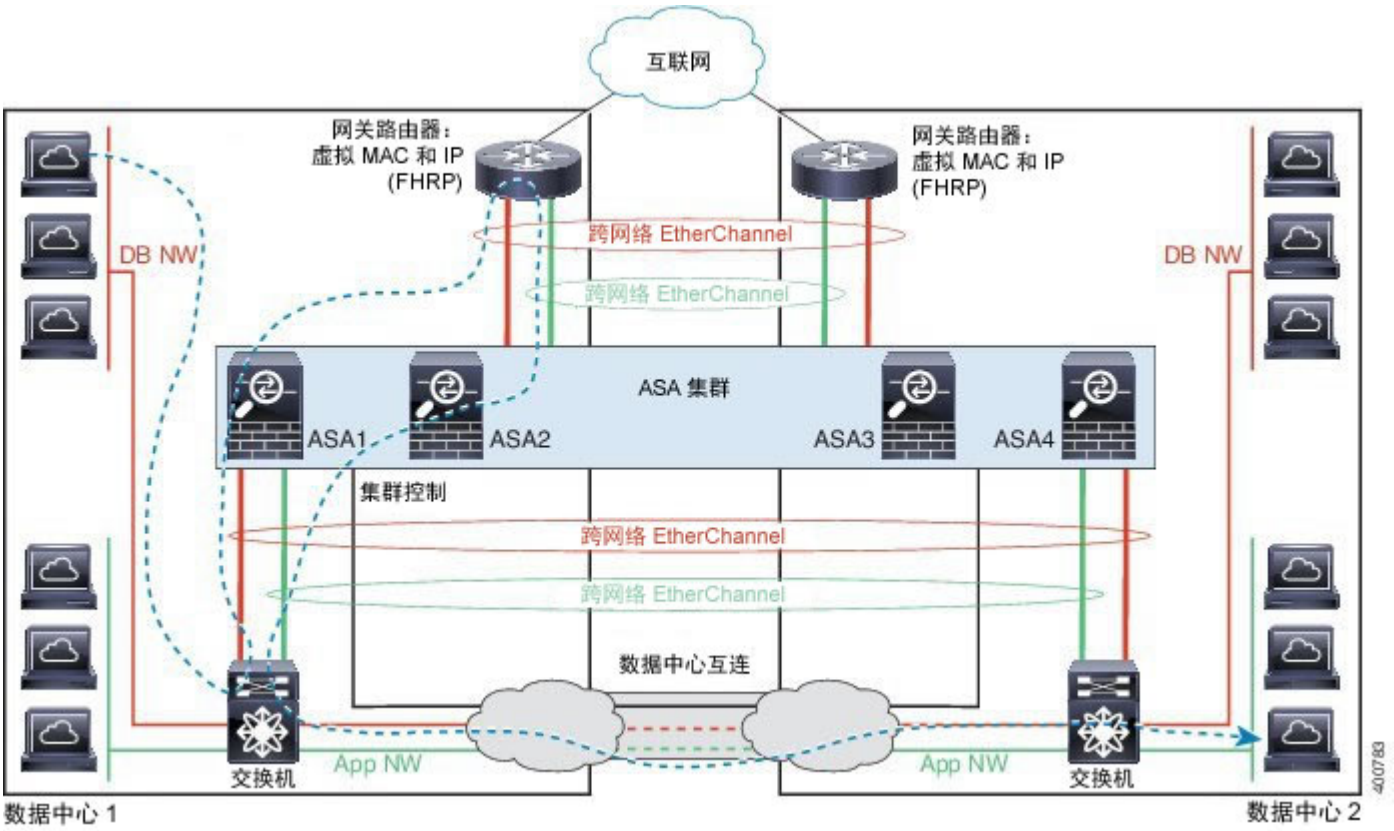
- 站点间 VSS/vPC - 在此情景中，一台交换机安装在数据中心 1，另一台交换机安装在数据中心 2。一个方案是将位于每个数据中心的集群设备只连接到本地交换机，而 VSS/vPC 流量通过 DCI 传输。在此情况下，连接多半会保持在每个数据中心本地。如果 DCI 可以处理额外的流量，您也可以选择将每台设备通过 DCI 连接到两台交换机。在此情况下，流量跨数据中心分摊，因此 DCI 必须非常强健稳定。
- 位于每个站点的本地 VSS/vPC - 为了获得更高的交换机冗余能力，您可以在每个站点安装 2 对单独的 VSS/vPC。在此情况下，尽管集群设备仍然有一个跨网络 EtherChannel 将数据中心 1 的机箱仅连接到两台本地交换机，将数据中心 2 的机箱连接到本地交换机，但跨网络 EtherChannel 本质上是“分离的”。每个本地 VSS/vPC 都会将跨网络 EtherChannel 视作站点本地的 EtherChannel。



跨网络 EtherChannel 透明模式东西站点间集群示例

以下示例显示了 2 个集群成员，这两个集群成员分别位于 2 个部署在每个站点上的网关路由器和两个内部网络（应用网络和数据库网络）之间（东西插入）的数据中心。集群成员由集群控制链路通过DCI连接。每个站点上的集群成员使用面向内部与外部应用网络和数据库网络的跨网络EtherChannel连接到本地交换机。每个 EtherChannel 跨越集群中的所有机箱。

每个站点上的网关路由器使用 FHRP（例如 HSRP）在每个站点上提供相同的目标虚拟 MAC 和 IP 地址。要避免 MAC 地址意外摆动，最好将网关路由器实际 MAC 地址静态添加到 ASA MAC 地址表。如果没有这些条目，当位于站点 1 的网关与位于站点 2 的网关通信时，流量可能通过 ASA 并尝试从内部接口到达站点 2，从而导致出现问题。数据 VLAN 使用重叠传输虚拟化 (OTV) 或类似技术在站点之间扩展。您必须添加过滤器，阻止发往网关路由器的流量通过 DCI 发送到另一站点。如果无法访问一个站点上的网关路由器，则您必须删除过滤器，使流量能够发送到另一站点的网关路由器。



有关 vPC/VSS 选项的详细信息，请参阅跨网络 EtherChannel 透明模式南北站点间集群示例，第 137 页。

集群历史记录

功能名称	平台版本	功能信息
对 Cisco ASA 进行机箱内集群	1.1.1	您可以对 Firepower 9300 机箱内的所有 ASA 安全模块创建集群。 我们引入了以下屏幕：**逻辑设备 (Logical Devices)** > **配置 (Configuration)**
对 6 个 ASA 模块进行机箱间集群	1.1.3	现在，您可以对 ASA 启用机箱间集群。您最多可以在 6 个机箱中包含 6 个模块。 我们修改了以下屏幕：**逻辑设备 (Logical Devices)** > **配置 (Configuration)**
支持在 Firepower 9300 上的 Firepower 威胁防御 上执行机箱内集群	1.1.4	Firepower 9300 支持使用 Firepower 威胁防御 应用执行机箱内集群。 我们修改了以下屏幕：**逻辑设备 (Logical Devices)** > **配置 (Configuration)**

功能名称	平台版本	功能信息
Firepower 4100/9300 机箱上的 ASA 的站点间集群改进	2.1.1	现在，您可以在部署 ASA 集群时为每个 Firepower 4100/9300 机箱配置站点 ID。以前，您必须在 ASA 应用中配置站点 ID；此新功能简化了最初的部署。请注意，您不能再在 ASA 配置中设置站点 ID。此外，为了实现与站点间集群的最佳兼容性，我们建议您升级到 ASA 9.7(1) 和 FXOS 2.1.1，升级版包含对稳定性和性能的多项改进。 我们修改了以下屏幕：**逻辑设备 (Logical Devices)** > **配置 (Configuration)**
对 6 个 Firepower 威胁防御 模块进行机箱间集群	2.1.1	现在，您可以对 Firepower 威胁防御启用机箱间集群。您最多可以在 6 个机箱中包含 6 个模块。 我们修改了以下屏幕：**逻辑设备 (Logical Devices)** > **配置 (Configuration)**

配置服务链

Cisco Firepower 4100/9300 机箱可在单个刀片上支持多个服务（例如防火墙和第三方 DDoS 应用）。这些应用和服务可以链接在一起形成服务链。

关于服务链

在当前支持的服务链配置中，可以安装第三方 Radware DefensePro 虚拟平台以在 ASA 防火墙前面或在 Firepower 威胁防御前面运行。Radware DefensePro 是基于 KVM 的虚拟平台，可在 Firepower 4100/9300 机箱上提供分布式拒绝服务 (DDoS) 检测和缓解功能。当在 Firepower 4100/9300 机箱上启用服务链时，来自网络的流量必须先通过 DefensePro 虚拟平台，然后再到达主要 ASA 或 Firepower 威胁防御。

Radware DefensePro 虚拟平台可以称为 *Radware vDP*（虚拟 DefensePro），或者简称为 *vDP*。Radware DefensePro 虚拟平台有时可能是指链路修饰器。

服务链的先决条件

在 Firepower 4100/9300 机箱上部署 Radware DefensePro 之前，必须将 Firepower 4100/9300 机箱配置为使用 **etc/UTC** 时区的 NTP 服务器。有关设置 Firepower 4100/9300 机箱日期与时间的详细信息，请参阅设置日期和时间，第 75 页。

服务链准则

模式

- Radware DefensePro 平台仅在 Firepower 9300 安全设备上受支持。

- 在以下安全设备上支持 Radware DefensePro 平台使用 Firepower 威胁防御：

  Firepower 9300

  Firepower 4110 - 请注意，还必须将修饰器与逻辑设备同时部署。在设备上配置了逻辑设备后，无法安装修饰器。

  Firepower 4120 - 请注意，还必须将修饰器与逻辑设备同时部署。在设备上配置了逻辑设备后，无法安装修饰器。

  Firepower 4140

  Firepower 4150

其他规定

- 服务链在机箱间集群配置中不受支持。但是，Radware DefensePro 应用可在机箱间集群情景的独立配置中进行部署。
- DefensePro 应用可以作为单独实例在最多三个安全模块上运行。

在独立逻辑设备上配置 Radware DefensePro 服务链

以下程序显示如何在独立 ASA 或 Firepower 威胁防御逻辑设备前面的单个服务链中安装 Radware DefensePro。

注释 如果您是在 Firepower 4120 或 4140 安全设备上在 ASA 前面安装 Radware vDP，则必须使用 FXOS CLI 部署修饰器。有关如何在 Firepower 4100 设备上在 ASA 前面的服务链中安装和配置 Radware DefensePro 的完整 CLI 说明，请参阅 FXOS CLI 配置指南。

开始之前

- 从 Cisco.com 下载 vDP 映像（请参阅从 Cisco.com 下载映像，第 38 页），然后将此映像上传到 Firepower 4100/9300 机箱（请参阅将映像上传到 Firepower 安全设备，第 38 页）。
- 您可以在机箱内集群的独立配置中部署 Radware DefensePro 应用；对于机箱内集群，请参阅在机箱内集群上配置 Radware DefensePro 服务链，第 142 页。

过程

步骤 1 如果要将单独的管理接口用于 vDP，请启用该接口并根据编辑接口属性，第 114 页将其设置为管理类型。否则，您可以共享应用管理接口。

步骤 2 选择**逻辑设备 (Logical Devices)** 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。如果尚未配置逻辑设备，系统将显示一条消息，要求您配置逻辑设备。

步骤 3 创建独立 ASA 或 Firepower 威胁防御逻辑设备（请参阅创建独立的 ASA 逻辑设备，第 119 页或创建独立威胁防御逻辑设备，第 121 页）。

步骤 4 在**修饰器 (Decorators)** 区域中，选择 vDP。系统将显示“Radware：虚拟 DefensePro - 配置 (Radware: Virtual DefensePro - Configuration)”窗口。配置**常规信息 (General Information)** 选项卡下的以下字段。

步骤 5 如果您已将多个 vDP 版本上传到 Firepower 4100/9300 机箱，请在**版本 (Version)** 下拉列表中选择要使用的版本。

步骤 6 在**管理接口 (Management Interface)** 下拉列表下，选择在此操作步骤的步骤 1 中创建的管理接口。

步骤 7 选择默认**地址类型 (Address Type)**：仅 IPv4、仅 IPv6，或者 IPv4 和 IPv6。

步骤 8 根据在上一步中选择的**地址类型 (Address Type)**，配置以下字段。

a) 在**管理 IP (Management IP)** 字段中，配置本地 IP 地址。

b) 仅 IPv4：输入**网络掩码 (Network Mask)**。
仅 IPv6：输入**前缀长度 (Prefix Length)**。

c) 输入**网络网关 (Network Gateway)** 地址。

步骤 9 点击您想要分配给设备的每个数据端口旁边的复选框。

步骤 10 点击 **OK**。

步骤 11 点击 **Save**。
Firepower 可扩展操作系统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指定的安全模块来部署逻辑设备。

在机箱内集群上配置 Radware DefensePro 服务链

以下程序显示如何安装 Radware DefensePro 映像，以及在 ASA 或 Firepower 威胁防御机箱内集群前面的服务链中配置此映像。

开始之前

- 从 Cisco.com 下载 vDP 映像（请参阅从 Cisco.com 下载映像，第 38 页），然后将此映像上传到 Firepower 4100/9300 机箱（请参阅将映像上传到 Firepower 安全设备，第 38 页）。

过程

步骤 1 如果要将单独的管理接口用于 vDP，请启用该接口并根据编辑接口属性，第 114 页将其设置为管理类型。否则，您可以共享应用管理接口。

步骤 2 配置 ASA 或 Firepower 威胁防御机箱内集群（请参阅配置 ASA 集群，第 131 页或配置 Firepower 威胁防御集群，第 134 页）。
请注意，在配置机箱内集群的程序结束时点击 **Save** 之前，必须首先按照以下步骤将 vDP 修饰器添加到集群。

步骤 3 在**修饰器 (Decorators)** 区域中，选择 vDP。系统将显示 **Radware：虚拟 DefensePro - 配置 (Radware: Virtual DefensePro - Configuration)** 对话框。配置**常规信息 (General Information)** 选项卡下的以下字段。

步骤 4 如果已将多个 vDP 版本上传到 Firepower 4100/9300 机箱，请在**版本 (Version)** 下拉列表中选择要使用的 vDP 版本。

步骤 5 在**管理接口 (Management Interface)** 下拉列表下，选择管理接口。

步骤 6 点击您想分配给 vDP 修饰程序的每个数据端口旁边的复选框。

步骤 7 点击**接口信息 (Interface Information)** 选项卡。

步骤 8 选择要使用的**地址类型 (Address Type)**，仅 IPv4、仅 IPv6 或 IPv4 和 IPv6。

步骤 9 为每个安全模块配置以下字段。请注意，显示的字段取决于您在上一步中选择的**地址类型 (Address Type)**。

a) 在**管理 IP (Management IP)** 字段中，配置本地 IP 地址。

b) 仅 IPv4：输入**网络掩码 (Network Mask)**。
仅 IPv6：输入**前缀长度 (Prefix Length)**。

c) 输入**网络网关 (Network Gateway)** 地址。

步骤 10 点击 **OK**。

步骤 11 点击 **Save**。
Firepower可扩展操作系统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指定的安全模块来部署逻辑设备。

步骤 12 选择**逻辑设备 (Logical Devices)** 打开“逻辑设备”(Logical Devices) 页面。

步骤 13 滚动已配置的逻辑设备列表至 vDP 条目。验证**管理 IP (Management IP)** 列中列出的属性。

- 如果 **CLUSTER-ROLE** 元素针对 DefensePro 实例显示为 *unknown*，必须进入 DefensePro 应用，配置主 IP 地址，完成 vDP 集群创建。
- 如果 **CLUSTER-ROLE** 元素针对 DefensePro 实例显示为 *primary* 或 *secondary*，说明应用在线，并且已在集群中形成。

开放 UDP/TCP 端口和启用 vDP Web 服务

Radware APSolute Vision 管理器接口可使用各种 UDP/TCP 端口与 Radware vDP 应用进行通信。为使 vDP 应用与 APSolute Vision 管理器进行通信，您必须确保这些端口可访问及未被防火墙阻止。有关哪些特定接口可开放的详细信息，请参阅《APSolute Vision 用户指南》中的以下表格：

- **APSolute Vision 服务器端口 - WBM 通信和操作系统**
- **带 Radware 设备的 APSolute Vision 服务器的通信端口**

为使 Radware APSolute Vision 管理部署在 FXOS 机箱上的虚拟 DefensePro 应用，您必须使用 FXOS CLI 启用 vDP Web 服务。

过程

步骤 1 从 FXOS CLI 连接到 vDP 应用实例。
connect module *slot***console**

connect vdp

步骤 2 启用 vDP Web 服务。
manage secure-web status set enable

步骤 3 退出 vDP 应用控制台并返回 FXOS 模块 CLI。
Ctrl]

管理逻辑设备

您可以删除逻辑设备，将 ASA 转换为透明模式，更改接口配置，以及对现有逻辑设备执行其他任务。

连接到应用或修饰器的控制台

使用以下程序连接至应用或修饰程序的控制台。

注释 如果您在访问控制台时遇到任何问题，我们建议您尝试不同的 SSH 客户端，或者将 SSH 客户端升级到较新的版本。

过程

步骤 1 要连接至应用或修饰程序的控制台，请执行以下操作：

a) 从 FXOS CLI，连接至安全模块/引擎：
Firepower-chassis # **connectmodule** *slot_number***console**

注释 要连接至不支持多个安全模块的设备的安全引擎，请使用 1 作为 *slot_number*。

首次连接到安全模块时，您会进入 FXOS 模块 CLI。

b) 要连接到应用或修饰程序，请输入适用于您的设备的命令：
Firepower-module1>**connect asa**

Firepower-module1>**connect ftd**

Firepower-module1>**connect vdp**

从 FXOS CLI 的管理引擎层到安全模块/引擎的后续连接直接访问安全模块/引擎操作系统。

步骤 2 （可选） 键入 **Ctrl-A-D**，使应用控制台返回到 FXOS 模块 CLI。
键入 **Ctrl-]-**，使修饰程序控制台返回到 FXOS 模块 CLI。

出于故障排除目的，您可能想访问 FXOS 模块 CLI。

步骤 3 返回 FXOS CLI 的管理引擎层。

a) 要退出安全模块/引擎控制台，请输入 ~。
您将退出至 Telnet 应用。

b) 要退出 Telnet 应用，请输入：
telnet>**quit**

示例

以下示例连接至安全模块 1 上的 ASA，然后返回到 FXOS CLI 的管理引擎层。

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect asa
asa> ~
telnet> quit
Connection closed.
Firepower#
```

删除逻辑设备

过程

步骤 1 选择**逻辑设备 (Logical Devices)** 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。如果尚未配置逻辑设备，系统将显示一条消息，要求您进行相关配置。

步骤 2 点击想要删除的逻辑设备所对应的**删除 (Delete)**。

步骤 3 点击**是 (Yes)** 确认想要删除此逻辑设备。

步骤 4 点击**是 (Yes)** 确认想要删除应用配置。

删除与逻辑设备不关联的应用实例

删除逻辑设备后，系统将提示您是否要删除逻辑设备的应用配置。如果不删除应用配置，则在删除该应用实例之前，将无法使用其他应用创建逻辑设备。当应用实例不再与逻辑设备关联时，可使用以下程序步骤从 安全模块/引擎中删除应用实例。

过程

步骤 1 选择**逻辑设备 (Logical Devices)** 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。在逻辑设备列表下方，您可以看到与逻辑设备不关联的应用实例列表。

步骤 2 点击想要删除的应用实例所对应的**删除 (Delete)**。

步骤 3 点击**是 (Yes)** 确认想要删除应用实例。

将 ASA 更改为透明防火墙模式

您只能在 Firepower 4100/9300 机箱中部署路由防火墙模式 ASA。要将 ASA 更改为透明防火墙模式，请完成初始部署，然后更改 ASA CLI 中的防火墙模式。由于更改防火墙模式会擦除配置，因此必须在 Firepower 4100/9300 机箱中重新部署配置才能重新获取引导程序配置。然后，ASA 会保持在透明模式，并且具有正常工作的引导程序配置。

过程

步骤 1 根据连接到应用或修饰器的控制台，第 144 页，连接到 ASA 控制台。对于集群，连接到主设备。对于故障切换对，连接到主用设备。

步骤 2 进入配置模式：
enable

configure terminal

默认情况下，启用密码为空。

步骤 3 将防火墙模式设置为透明：
firewall transparent

步骤 4 保存配置：
write memory

对于集群或故障切换对，此配置会复制到辅助设备：

```
asa(config)# firewall transparent
asa(config)# write memory
```

```
Building configuration...
Cryptochecksum: 9f831dfb 60dffa8c 1d939884 74735b69

3791 bytes copied in 0.160 secs
[OK]
asa(config)#
Beginning configuration replication to Slave unit-1-2
 End Configuration Replication to slave.

asa(config)#
```

步骤 5 在Firepower 机箱管理器**逻辑设备 (Logical Devices)** 页面上，点击**编辑 (Edit)** 图标以编辑 ASA。系统将显示**调配 (Provisioning)** 页面。

步骤 6 点击设备图标可编辑引导程序配置。更改配置中的任何值，然后点击**确定 (OK)**。
您必须更改至少一个字段的值。思科建议将**密码 (Password)** 更改为新密码，因为此设置不重要。

您会看到有关更改引导程序配置的一条警告；请点击**是 (Yes)**。

步骤 7 点击**保存 (Save)** 将配置重新部署到 ASA。对于机箱间集群或故障切换对，请重复执行步骤 5 到 7 以在每个机箱上重新部署引导程序配置。
等待几分钟以便机箱/安全模块重新加载，以及 ASA 恢复可运行状态。现在，ASA 已具有可运行的引导程序配置，但是保持在透明模式。

更改 Firepower 威胁防御逻辑设备上的接口

可以在 Firepower 威胁防御逻辑设备上分配或取消分配接口，或者替换管理接口。然后，您可以在 Firepower 管理中心中同步接口配置。

开始之前

- 根据编辑接口属性，第 114 页和创建端口通道，第 115 页配置您的接口，并添加任何 EtherChannel。
- 您可以编辑已分配的 EtherChannel 的成员，而不影响逻辑设备或要求在 Firepower 管理中心上进行同步。
- 如果您要将已分配的接口添加到 EtherChannel（例如，默认情况下将所有接口分配给集群），则需要先从逻辑设备取消分配接口，然后再将该接口添加到 EtherChannel。对于新的 EtherChannel，您可以随后将 EtherChannel 分配到设备。
- 如果要将管理或 Firepower 事件接口替换为管理 EtherChannel，则需要创建至少具有 1 个取消分配数据成员接口的 EtherChannel，然后将当前管理接口替换为 EtherChannel。在 Firepower 威胁防御设备重新启动（管理接口更改导致重新启动），并且您在 Firepower 管理中心中同步配置后，还可以将（目前取消分配的）管理接口添加到 EtherChannel。
- 对于集群或高可用性，请确保在所有设备上添加或删除该接口，然后在 Firepower 管理中心中同步配置。请注意，新的接口在管理权限关闭的状态下添加，因此，它们不会影响接口监控。

过程

步骤 1 在 Firepower 机箱管理器中，选择**逻辑设备 (Logical Devices)**。

步骤 2 点击右上角的**编辑 (Edit)** 图标以编辑逻辑设备。

步骤 3 通过在**数据端口 (Data Ports)** 区域中取消选择数据接口来取消分配该接口。

步骤 4 通过在**数据端口 (Data Ports)** 区域中选择新的数据接口来分配该接口。

步骤 5 替换管理或事件接口：
对于这些类型的接口，在您保存更改后，设备会重新启动。

a) 点击页面中心的设备图标。
b) 在**常规/集群信息 (General/Cluster Information)** 选项卡上，从下拉列表中选择新的**管理接口 (Management Interface)**。
c) 在**设置 (Settings)** 选项卡上，从下拉列表中选择新的**事件接口 (Eventing Interface)**。
d) 点击 **OK**。

如果更改管理接口的 IP 地址，则还必须更改 Firepower 管理中心中设备的 IP 地址：转到**设备 (Devices)** > **设备管理 (Device Management)** > **设备/集群 (Device/Cluster)**。在**管理 (Management)** 区域中，设置 IP 地址以匹配引导程序配置地址。

步骤 6 点击**保存 (Save)**。

步骤 7 登录至Firepower 管理中心。

步骤 8 依次选择**设备 (Devices)** > **设备管理 (Device Management)** 并点击 Firepower 威胁防御 设备的编辑图标 ( )。系统会默认选择**接口 (Interfaces)** 选项卡。

步骤 9 点击**接口 (Interfaces)** 选项卡左上方的**从设备同步接口 (Sync Interfaces from device)** 按钮。

步骤 10 点击**保存 (Save)**。
此时，可以点击**部署 (Deploy)** 并将策略部署到所分配的设备。在部署更改之后，更改才生效。

更改 ASA 逻辑设备上的接口

可以在 ASA 逻辑设备上分配、取消分配或替换管理接口。ASDM 会自动发现新接口。

开始之前

- 根据编辑接口属性，第 114 页和创建端口通道，第 115 页配置您的接口，并添加任何 EtherChannel。
- 您可以编辑已分配的 EtherChannel 的成员，而不影响逻辑设备。
- 如果您要将已分配的接口添加到 EtherChannel（例如，默认情况下将所有接口分配给集群），则需要先从逻辑设备取消分配接口，然后再将该接口添加到 EtherChannel。对于新的 EtherChannel，您可以随后将 EtherChannel 分配到设备。

- 如果要将管理接口替换为管理 EtherChannel，则需要创建至少具有 1 个取消分配数据成员接口的 EtherChannel，然后将当前管理接口替换为 EtherChannel。在 ASA 重新加载（管理接口更改导致重新加载）后，您还可以将（当前取消分配的）管理接口添加到 EtherChannel。
- 对于集群或故障切换，新的接口在管理权限关闭的状态下添加，因此，它们不会影响接口监控。

过程

步骤 1 在 Firepower 机箱管理器中，选择**逻辑设备 (Logical Devices)**。

步骤 2 点击右上角的**编辑 (Edit)** 图标以编辑逻辑设备。

步骤 3 通过在**数据端口 (Data Ports)** 区域中取消选择数据接口来取消分配该接口。

步骤 4 通过在**数据端口 (Data Ports)** 区域中选择新的数据接口来分配该接口。

步骤 5 替换管理接口：
对于此类型的接口，在您保存更改后，设备会重新加载。

a) 点击页面中心的设备图标。
b) 在**常规/集群信息 (General/Cluster Information)** 选项卡上，从下拉列表中选择新的**管理接口 (Management Interface)**。
c) 点击 **OK**。

步骤 6 点击 **Save**。

第 11 章

安全模块/引擎管理

关于 FXOS 安全模块/安全引擎

在 Firepower 机箱管理器的“安全模块/安全引擎 (Security Modules/Security Engine)”页面上，您可以查看安全模块/引擎的状态并执行以下功能：

- 停用/重新启用 (Decommission/Recommission)（仅限安全模块）- 停用安全模块后，安全模块将进入维护模式。您还可以先停用安全模块，然后重新启用安全模块，从而纠正某些故障状态。请参阅停用/重新启用安全模块， 第 152 页。
- 确认 (Acknowledge) - 让新安装的安全模块上线。请参阅确认安全模块/引擎， 第 153 页。
- 重启 (Power Cycle) - 重新启动安全模块/引擎。请参阅重置安全模块/引擎， 第 153 页。
- 重新初始化 (Reinitialize) - 重新格式化安全模块/引擎硬盘，从安全模块/引擎上删除所有部署的应用和配置，然后重新启动系统。在重新初始化完成后，如果为安全模块/引擎配置了逻辑设备，Firepower 可扩展操作系统将重新安装应用软件，重新部署逻辑设备，并自动启动应用。请参阅重新初始化安全模块/引擎， 第 154 页。

警告 在重新初始化期间，安全模块/引擎上的所有应用数据将被删除。在重新初始化安全模块/引擎之前，请备份所有应用数据。

- 电源关/开 (Power off/on) - 切换安全模块/引擎的电源状态。请参阅打开/关闭安全模块电源，第 154 页。

安全模块/安全引擎 (Security Modules/Security Engine) 页面提供以下信息：

- 硬件状态 (Hardware State) - 显示安全模块/引擎硬件的状态。

  启动 (Up) - 安全模块/引擎已成功启动，未显示任何硬件故障。

  正在启动 (Booting Up) - 安全模块/引擎正在启动过程中。

  关闭 (Down) - 安全模块/引擎的电源未打开或硬件故障阻止安全模块/引擎成功启动。

  未关联 (Unassociated) - 安全模块/引擎没有与之关联的逻辑设备。

  不匹配 (Mismatch) - 安全模块已停用或插槽中安装了新的安全模块。使用“重新启用 (Recommission)”或“确认 (Acknowledge)”功能，使安全模块恢复正常运行状态。

- 服务状态 (Service State) - 显示安全模块/引擎上软件的状态：

  不可用 (Not-available) - 安全模块已从插槽中移除。重新安装安全模块，使之回到正常运行状态。

  离线 (Offline) - 安全模块/引擎已安装但已被停用、已关闭电源或仍在启动过程中。

  在线 (Online) - 安全模块/引擎已安装并处于正常运行模式。

  未响应 (Not Responding) - 安全模块/引擎未响应。

  故障 (Fault) - 安全模块/引擎处于故障状态。查看系统故障列表，了解有关故障状态可能原因的详细信息。

  令牌不匹配 (Token Mismatch) - 表示已安装到机箱插槽中的安全模块不是之前配置的安全模块。这也可能是软件安装错误引起的。使用“重新初始化 (Reinitialize)”功能使安全模块恢复正常运行状态。

- 电源 (Power) - 显示安全模块/引擎的电源状态：

  开 (On) - 使用“电源关/开 (Power off/on)”功能切换安全模块/引擎的电源状态。

  关 (Off) - 使用“电源关/开 (Power off/on)”功能切换安全模块/引擎的电源状态。

- 应用 (Application) - 显示安全模块/引擎上安装的逻辑设备类型。

停用/重新启用安全模块

当您停用安全模块时，安全模块对象将从配置中删除，安全模块将变为非托管状态。安全模块上运行的任何逻辑设备或软件都将变为非活动状态。

如果要暂时停止使用安全模块，您可以停用安全模块。此外，如果重新启动安全模块无法纠正错误状态，您可以尝试停用然后重新启用安全模块，以查看是否能够纠正错误状态而不必重新初始化安全模块。

过程

步骤 1 选择**安全模块 (Security Modules)** 打开“安全模块 (Security Modules)”页面。

步骤 2 要停用安全模块，点击该安全模块所对应的**下线 (Decommission)**。
要重新启用安全模块，点击该安全模块所对应的**重新上线 (Recommission)**。

步骤 3 点击**是 (Yes)** 确认要停用或重新启用指定的安全模块。

确认安全模块/引擎

当新的安全模块安装到机箱中时，您必须确认该安全模块，然后才能开始使用它。

如果安全模块显示“mismatch”或“token mismatch”状态，这表示安装在插槽中的安全模块上的数据与之前安装在该插槽中的模块不匹配。如果安全模块上已有数据并且您确定要在新的插槽中使用它（换句话说，安全模块并非无意中安装到错误插槽），您必须重新初始化该安全模块，然后才可以向它部署逻辑设备。

过程

步骤 1 选择**安全模块/安全引擎 (Security Modules/Security Engine)** 打开“安全模块/安全引擎 (Security Modules/Security Engine”页面。

步骤 2 点击您想要确认的安全模块/引擎所对应的**确认 (Acknowledge)**。

步骤 3 点击**是 (Yes)** 确定您要确认指定的安全模块/引擎。

重置安全模块/引擎

过程

步骤 1 选择**安全模块/安全引擎 (Security Modules/Security Engine)** 打开“安全模块/安全引擎 (Security Modules/Security Engine”页面。

步骤 2 点击您想要重置的安全模块/引擎所对应的**重启 (Power Cycle)**。

步骤 3 执行以下操作之一：

- 点击**安全重启 (Safe Power Cycle)** 让系统等待最多五分钟，以便在系统重置指定的安全模块/引擎之前关闭安全模块/引擎上运行的应用。
- 点击**立即重启 (Power Cycle Immediately)** 让系统立即重置指定的安全模块/引擎。

重新初始化安全模块/引擎

在重新初始化安全模块/引擎时，安全模块/引擎硬盘将被格式化，所有安装的应用实例和配置均会被删除。在重新初始化完成后，如果为安全模块/引擎配置了逻辑设备，Firepower可扩展操作系统将重新安装应用软件，重新部署逻辑设备，并自动启动应用。

警告 在重新初始化期间，安全模块/引擎上的所有应用数据将被删除。在重新初始化安全模块/引擎之前，请备份所有应用数据。

过程

步骤 1 选择**安全模块/安全引擎 (Security Modules/Security Engine)** 打开“安全模块/安全引擎 (Security Modules/Security Engine”页面。

步骤 2 点击您想要重新初始化的安全模块/引擎所对应的**重新初始化 (Reinitialize)**。

步骤 3 点击**是 (Yes)** 确认您要重新初始化指定的安全模块/引擎。
安全模块/引擎重新启动，安全模块上的所有数据均被删除。此过程可能需要数分钟。

打开/关闭安全模块电源

过程

步骤 1 选择**安全模块/安全引擎 (Security Modules/Security Engine)** 打开“安全模块/安全引擎 (Security Modules/Security Engine”页面。

步骤 2 要关闭安全模块/引擎电源，请执行以下操作：

a) 点击该安全模块/引擎所对应的**关机 (Power Off)**。

b) 执行以下操作之一：

- 点击**安全关机 (Safe Power Off)** 让系统等待最多五分钟，以便在系统关闭指定的安全模块/引擎之前关闭安全模块/引擎上运行的应用。
- 点击**立即关机 (Power Off Immediately)** 让系统立即关闭指定的安全模块/引擎。

步骤 3 要打开安全模块/引擎电源，请执行以下操作：

a) 点击该安全模块/引擎所对应的**开机 (Power on)**。

b) 点击**是 (Yes)** 确认您要打开指定的安全模块/引擎的电源。

第 12 章

配置导入/导出

关于配置导入/导出

您可以使用配置导出功能将包含 Firepower 4100/9300 机箱逻辑设备和平台配置设置的 XML 文件导出到远程服务器或本地计算机。之后，您便可以导入此配置文件，快速将配置设置应用于 Firepower 4100/9300 机箱，以返回到已知的正确配置，或从系统故障中恢复。

准则和限制

- 请勿修改配置文件的内容。如果配置文件被修改，使用该文件进行配置导入可能会失败。
- 特定应用的配置设置不包含在配置文件内。您必须使用应用提供的配置备份工具来管理特定应用的设置和配置。
- 将配置导入到 Firepower 4100/9300 机箱时，Firepower 4100/9300 机箱上的所有现有配置（包括任何逻辑设备）将被删除并完全替换为导入文件中包含的配置。
- 我们建议您只将配置文件导入当初从中导出配置的同一个 Firepower 4100/9300 机箱。
- 进行导入的 Firepower 4100/9300 机箱的平台软件版本应与执行导出时的版本相同。否则，导入操作将无法确保会成功。我们建议您在升级或降级 Firepower 4100/9300 机箱时导出备份配置。
- 进行导入的 Firepower 4100/9300 机箱必须在与执行导出时所用的相同插槽中安装相同的网络模块。
- 进行导入的 Firepower 4100/9300 机箱必须为您正在导入的导出文件中定义的任意逻辑设备安装了正确的软件应用映像。

- 如果导入的配置文件包含其应用具有最终用户许可协议 (EULA) 的逻辑设备，则在导入配置之前，必须在 Firepower 4100/9300 机箱上接受该应用的 EULA，否则操作将失败。
- 要避免覆盖现有的备份文件，请务必更改备份操作中的文件名或将现有文件复制到其他位置。

导出配置文件

使用配置导出功能将包含 Firepower 4100/9300 机箱逻辑设备和平台配置设置的 XML 文件导出到远程服务器或本地计算机。

请查看关于配置导入/导出，了解有关使用配置导出功能的重要信息。

过程

步骤 1 依次选择**系统 (System)** > **配置 (Configuration)** > **导出 (Export)**。

步骤 2 要将配置文件导出到本地计算机，请点击**本地导出 (Export Locally)**。
配置文件已创建，然后根据您的浏览器，该文件可能会自动下载到默认下载位置，或者系统会提示您保存文件。

步骤 3 要将配置文件导出到之前配置的远程服务器，请点击您要使用的远程配置的**导出 (Export)** 按钮。
配置文件已创建，并已被导出到指定位置。

步骤 4 要将配置文件导出到新的远程服务器：

a) 在“按需导出 (On-Demand Export)”下面，点击**添加按需配置 (Add On-Demand Configuration)**。

b) 选择与远程服务器通信时要使用的协议。它可以是以下协议之一：FTP、TFTP、SCP 或 SFTP。

c) 输入备份文件应存储位置的主机名或IP地址。它可以是服务器、存储阵列、本地驱动器或Firepower 4100/9300 机箱可通过网络访问的任何读/写媒体。
如果使用主机名而不使用 IP 地址，则必须配置 DNS 服务器。

d) 如果您使用非默认端口，请在**端口 (Port)** 字段中输入端口号。

e) 输入系统在登录远程服务器时应使用的用户名。如果协议是 TFTP，将无法应用该字段。

f) 输入远程服务器用户名的密码。如果协议是 TFTP，将无法应用该字段。

g) 在**位置 (Location)** 字段中，输入配置文件导出位置的完整路径，包括文件名。如果您省略了文件名，导出操作步骤将为该文件分配一个名称。

h) 点击 **OK**。
“远程配置 (Remote Configuration)”将添加到按需导出 (On-Demand Export) 表。

i) 点击您想使用的远程配置的**导出 (Export)** 按钮。
配置文件已创建，并已被导出到指定位置。

计划自动配置导出

使用计划的导出功能将包含 Firepower 4100/9300 机箱逻辑设备和平台配置设置的 XML 文件自动导出到远程服务器或本地计算机。您可以计划每日、每周或每两周运行一次导出。配置导出将按计划执行，计划基于计划的导出功能的启用时间。例如，如果您在星期三的晚上 10:00 启用每周一次的计划的导出，系统将在每个星期三的晚上 10:00 触发新的导出。

请查看关于配置导入/导出，了解有关使用配置导出功能的重要信息。

过程

步骤 1 依次选择**系统 (System)** > **配置 (Configuration)** > **导出 (Export)**。

步骤 2 点击**计划导出 (Schedule Export)**。
您将看到**配置计划的导出 (Configure Scheduled Export)** 对话框。

步骤 3 选择与远程服务器通信时要使用的协议。它可以是以下协议之一：FTP、TFTP、SCP 或 SFTP。

步骤 4 要启用计划的导出，请选中**启用 (Enable)** 复选框。

注释 之后，您可以使用此复选框启用或禁用计划的导出；但是，在启用或禁用计划的导出时，您将需要重新指定密码。

步骤 5 输入备份文件应存储位置的主机名或IP地址。它可以是服务器、存储阵列、本地驱动器或Firepower 4100/9300 机箱可通过网络访问的任何读/写媒体。
如果使用主机名而不使用 IP 地址，则必须配置 DNS 服务器。

步骤 6 如果您使用非默认端口，请在**端口 (Port)** 字段中输入端口号。

步骤 7 输入系统在登录远程服务器时应使用的用户名。如果协议是 TFTP，将无法应用该字段。

步骤 8 输入远程服务器用户名的密码。如果协议是 TFTP，将无法应用该字段。

步骤 9 在**位置 (Location)** 字段中，输入配置文件导出位置的完整路径，包括文件名。如果您省略了文件名，导出操作步骤将为该文件分配一个名称。

步骤 10 选择您想要根据它自动导出配置的计划。它可以是以下计划之一：“每天(Daily)”、“每周(Weekly)”或“每两周 (BiWeekly)”。

步骤 11 点击 **OK**。
计划的导出已创建。如果启用了计划的导出，系统将按照您选择的计划自动将配置文件导出到指定位置。

设置配置导出提醒

使用导出提醒功能，让系统在一定天数内没有执行配置导出时报告错误。

过程

步骤 1 依次选择**系统 (System)** > **配置 (Configuration)** > **导出 (Export)**。

步骤 2 要启用配置导出提醒，请选中**导出触发提醒 (Reminder to trigger an export)** 下的复选框。

步骤 3 输入在两次配置导出之间，系统在生成提醒错误前应等待的天数（1 和 365 之间的整数）。

步骤 4 点击**保存提醒 (Save Reminder)**。

导入配置文件

您可以使用配置导入功能应用之前已从 Firepower 4100/9300 机箱导出的配置设置。此功能允许您返回已知的良好配置或从系统故障中进行恢复。请查看关于配置导入/导出，了解有关使用配置导入功能的重要信息。

过程

步骤 1 依次选择**系统 (System)** > **配置 (Configuration)** > **导入 (Import)**。

步骤 2 要从本地配置文件导入：

a) 点击**选择文件 (Choose File)** 以导航到要导入的配置文件并将其选定。

b) 点击 **Import**。
系统将打开确认对话框，请求您确认是否要继续，并警告您可能需要重新启动机箱。

c) 点击**是 (Yes)** 以确认要导入指定的配置文件。
现有配置被删除，导入文件中指定的配置应用到Firepower 4100/9300机箱。在导入过程中，如果有分支端口配置更改，Firepower 4100/9300 机箱将需要重新启动。

步骤 3 要从之前配置的远程服务器导入配置文件：

a) 在“Remote Import (远程导入)”表中，点击您想要使用的远程配置的**导入 (Import)** 按钮。
系统将打开确认对话框，请求您确认是否要继续，并警告您可能需要重新启动机箱。

b) 点击**是 (Yes)** 以确认要导入指定的配置文件。
现有配置被删除，导入文件中指定的配置应用到Firepower 4100/9300机箱。在导入过程中，如果有分支端口配置更改，Firepower 4100/9300 机箱将需要重新启动。

步骤 4 要从新的远程服务器上的配置文件导入：

a) 在“远程导入 (Remote Import)”下，点击**添加远程配置 (Add Remote Configuration)**。

b) 选择与远程服务器通信时要使用的协议。它可以是以下协议之一：FTP、TFTP、SCP 或 SFTP。

c) 如果您使用非默认端口，请在**端口 (Port)** 字段中输入端口号。

d) 输入备份文件存储位置的主机名或IP地址。它可以是服务器、存储阵列、本地驱动器或Firepower 4100/9300 机箱可通过网络访问的任何读/写媒体。
如果使用主机名而不使用 IP 地址，则必须配置 DNS 服务器。

e) 输入系统在登录远程服务器时应使用的用户名。如果协议是 TFTP，将无法应用该字段。

f) 输入远程服务器用户名的密码。如果协议是 TFTP，将无法应用该字段。
g) 在**文件路径 (File Path)** 字段中，输入配置文件的完整路径，包括文件名。
h) 点击**保存 (Save)**。
远程配置将添加到“远程导入 (Remote Import)”表。
i) 点击您想使用的远程配置的**导入 (Import)** 按钮。
系统将打开确认对话框，请求您确认是否要继续，并警告您可能需要重新启动机箱。
j) 点击**是 (Yes)** 以确认要导入指定的配置文件。
现有配置被删除，导入文件中指定的配置应用到Firepower 4100/9300 机箱。在导入过程中，如果有分支端口配置更改，Firepower 4100/9300 机箱将需要重新启动。

第 13 章

故障排除

数据包抓包

数据包捕获工具是一项宝贵资产，可用于调试连接和配置问题，了解通过 Firepower 4100/9300 机箱的流量。您可以使用数据包捕获工具记录通过 Firepower 4100/9300 机箱上面向特定客户的端口或应用端口的流量。

您还可以创建多个数据包捕获会话，每个会话都可以捕获多个端口上的流量。对于包含在数据包捕获会话中的每个端口，将创建单独的数据包捕获 (PCAP) 文件。

背板端口映射

Firepower 4100/9300 机箱对内部背板端口使用以下映射：

安全模块	端口映射	说明
安全模块 1/安全引擎	Ethernet1/9	内部数据 0/0
安全模块 1/安全引擎	Ethernet1/10	内部数据 0/1
安全模块 2	Ethernet1/11	内部数据 0/0
安全模块 2	Ethernet1/12	内部数据 0/1
安全模块 3	Ethernet1/13	内部数据 0/0

安全模块	端口映射	说明
安全模块 3	Ethernet1/14	内部数据 0/1

规定和限制

数据包捕获工具存在以下限制：

- 捕获速度最多达到 100 Mbps。
- 即使没有足够的存储空间来运行数据包捕获会话，依然可以创建数据包捕获会话。在开始数据包捕获会话之前，您应验证您有足够的存储空间。
- 不支持多个活动数据包捕获会话。
- 仅在内部交换机的入口阶段进行捕获。
- 对于内部交换机无法理解的数据包（例如，安全组标记和网络服务报头数据包），过滤器不起作用。
- 不支持抽象（例如，端口通道和服务链）。

注释 尽管不支持在端口通道上捕获流量，但您可以包含在数据包捕获会话中组成端口通道的单个成员端口，数据包捕获工具将为每个成员端口创建单独的数据包捕获文件。

- 当捕获会话仍处于活动状态时，您无法复制或导出 PCAP 文件。
- 删除数据包捕获会话时，与此会话相关的所有数据包捕获文件也将被删除。

创建或编辑数据包捕获会话

过程

步骤 1 依次选择**工具 (Tools)** > **数据包捕获 (Packet Capture)**。
捕获会话 (Capture Session) 选项卡将会显示当前已配置的数据包捕获会话列表。如果当前未配置数据包捕获会话，将会显示说明此情况的消息。

步骤 2 执行以下操作之一：

- 要创建数据包捕获会话，请点击**捕获会话 (Capture Session)** 按钮。
- 要编辑现有的数据包捕获会话，请点击该会话的**编辑 (Edit)** 按钮。

您会看到**配置数据包捕获会话 (Configure Packet Capture Session)** 窗口。**配置数据包捕获会话 (Configure Packet Capture Session)** 窗口的左侧允许您选择在 Firepower 4100/9300 机箱上配置的特定

逻辑设备，然后显示该逻辑设备的表示。此表示用于选择您希望捕获数据包的接口。**配置数据包捕获会话 (Configure Packet Capture Session)** 窗口的右侧包含用于定义数据包捕获会话的字段。

步骤 3 请在**会话名称 (Session Name)** 字段中输入数据包捕获会话的名称。

步骤 4 可以通过以下两种方式指定要用于此数据包捕获会话的缓冲区大小：从**缓冲区大小 (Buffer Size)** 列表中选择预定义的值之一，或选择**自定义 (MB) (Custom in MB)**，然后输入所需的缓冲区大小。指定的缓冲区大小必须介于 1 和 2048 MB 之间。

步骤 5 在 **Snap 长度 (Snap Length)** 字段中指定要捕获的数据包的长度。有效值范围为 64 至 9006 个字节。默认的 Snap 长度为 1518 个字节。

步骤 6 指定当执行此数据包捕获会话时，您是希望覆盖现有的 PCAP 文件还是将数据附加到 PCAP 文件。

步骤 7 在**配置数据包捕获会话 (Configure Packet Capture Session)** 窗口的左侧，请点击要捕获数据包的逻辑设备的名称。
您将会看到所选的逻辑设备的表示，包括为该设备分配的所有接口。

步骤 8 要捕获分配给该设备的面向客户的任意端口的流量，请点击所需接口进行选定。

步骤 9 要捕获从背板端口传出的逻辑设备的流量：

a) 点击表示该逻辑设备的框。
捕获位置 (Capture On)、**应用端口 (Application Port)** 和**应用捕获方向 (Application Capture Direction)** 字段位于**配置数据包捕获会话 (Configure Packet Capture Session)** 窗口的右侧。

b) 选择您想要在其上捕捉流量的背板端口或从**捕捉端口 (Capture On)** 下拉列表中选择**所有背板端口 (All Backplane Ports)**。

步骤 10 要捕获逻辑设备和特定接口之间的流量：

a) 点击表示该逻辑设备的框。
捕获位置 (Capture On)、**应用端口 (Application Port)** 和**应用捕获方向 (Application Capture Direction)** 字段位于**配置数据包捕获会话 (Configure Packet Capture Session)** 窗口的右侧。

b) 确定在**捕捉位置 (Capture On)** 下拉列表中选择了逻辑设备（例如，asa）。

c) 在**应用端口 (Application Port)** 下拉列表中选择您想要捕捉流出或流入流量的接口。

d) 要仅捕获从逻辑设备流向指定接口的流量，请点击**应用捕获方向 (Application Capture Direction)** 旁边的**出口数据包 (Egress Packets)** 选项。

e) 要捕捉流出或流入指定接口的流量，请点击**应用捕捉方向 (Application Capture Direction)** 旁边的**所有数据包 (All Packets)** 选项。

步骤 11 要过滤捕获的流量：

a) 点击**捕获过滤器 (Capture Filter)** 字段的**应用过滤器 (Apply Filter)** 选项。
您将看到一组用于配置过滤器的字段。

b) 如果您需要创建过滤器，请点击**创建过滤器 (Create Filter)**。
您将看到**创建数据包过滤器 (Create Packet Filter)** 对话框。有关详细信息，请参阅配置数据包捕获的过滤器，第 166 页。

c) 从**应用 (Apply)** 下拉列表中选择要使用的过滤器。

d) 从**应用目标 (To)** 下拉列表中选择要应用过滤器的接口。

e) 要应用其他过滤器，请点击**应用其他过滤器 (Apply Another Filter)**，然后重复以上步骤应用其他过滤器。

步骤 12 执行以下操作之一：

- 要保存此数据包捕获会话并立刻运行该会话，请点击**保存并运行 (Save and Run)** 按钮。仅在当前未运行其他数据包捕获会话时，此选项才可用。
- 要保存此数据包捕获会话，以便在稍后运行，请点击**保存 (Save)** 按钮。

在**捕获会话 (Capture Session)** 选项卡中，您将看到列出了您的会话及之前创建的任何其他会话。如果选择**保存并运行 (Save and Run)**，数据包捕获会话将捕获数据包。要从会话下载 PCAP 文件，您需要先停止捕获。

配置数据包捕获的过滤器

您可以创建过滤器来限制数据包捕获会话中包含的流量。在创建数据包捕获会话时，您可以选择哪些接口应使用特定过滤器。

注释 如果您修改或删除已应用于当前正在运行的数据包捕获会话的过滤器，那么在您禁用并重新启用该会话后，更改才会生效。

过程

步骤 1 依次选择**工具 (Tools)** > **数据包捕获 (Packet Capture)**。
捕获会话 (Capture Session) 选项卡将会显示当前已配置的数据包捕获会话列表。如果当前未配置数据包捕获会话，将会显示说明此情况的消息。

步骤 2 执行以下操作之一：

- 要创建过滤器，请点击**添加过滤器 (Add Filter)** 按钮。
- 要编辑现有过滤器，请点击该过滤器的**编辑 (Edit)** 按钮。

您将看到**创建或编辑数据包过滤器 (Create or Edit Packet Filter)** 对话框。

步骤 3 请在**会话名称 (Session Name)** 字段中输入数据包捕获过滤器的名称。

步骤 4 要对特定协议进行过滤，请从**协议 (Protocol)** 列表中选择该协议，或选择**自定义 (Custom)**，然后输入所需的协议。自定义协议必须为 IANA 定义的协议，并采用十进制格式 (0 - 255)。

步骤 5 要对特定以太网类型进行过滤，请从**以太网类型 (EtherType)** 列表中选择该以太网类型，或选择**自定义 (Custom)**，然后输入所需的以太网类型。自定义以太网类型必须是 IANA 定义的以太网类型，并采用十进制格式（例如，IPv4 = 2048，IPv6 = 34525，ARP = 2054 和 SGT = 35081）。

步骤 6 要基于内部 VLAN（进入端口时的 VLAN ID）或外部 VLAN（Firepower 4100/9300 机箱添加的 VLAN ID）过滤流量，请在指定字段中输入 VLAN ID。

步骤 7 要过滤特定来源或目标的流量，请在指定的来源或目标字段中输入 IP 地址和端口或输入 MAC 地址。

注释 您可以使用 IPv4 或 IPv6 地址过滤，但无法在同一数据包捕获会话中同时过滤这两类地址。

步骤 8 点击**保存 (Save)** 保存过滤器，
在**过滤器列表 (Filter List)** 选项卡中，您将看到列出了您的过滤器和已创建的任何其他过滤器。

启动和停止数据包捕获会话

过程

步骤 1 依次选择**工具 (Tools)** > **数据包捕获 (Packet Capture)**。
捕获会话 (Capture Session) 选项卡将会显示当前已配置的数据包捕获会话列表。如果当前未配置数据包捕获会话，将会显示说明此情况的消息。

步骤 2 要启动数据包捕获会话，请点击该会话的**启用会话 (Enable Session)** 按钮，然后点击**是 (Yes)** 进行确认。

注释 您无法在另一个会话运行时启动数据包捕获会话。

会话中所包含接口的 PCAP 文件将开始收集流量。如果会话配置为覆盖会话数据，现有的 PCAP 数据将会擦除。如果不这样配置，数据将被附加到现有文件（如有）。

在数据包捕获会话运行时，单个 PCAP 文件的文件大小将随流量捕获而增加。一旦达到缓冲区大小限制，系统将开始丢弃数据包，您将会看到“丢弃计数 (Drop Count)”字段数值增加。

步骤 3 要停止数据包捕获会话，请点击该会话的**禁用会话 (Disable Session)** 按钮，然后点击**是 (Yes)** 进行确认。
在禁用会话后，您便可以下载 PCAP 文件（请参阅 下载数据包捕获文件，第 168 页）。

下载数据包捕获文件

您可将数据包捕获 (PCAP) 文件从会话下载到本地计算机，以便使用网络数据包分析器分析这些文件。

过程

步骤 1 依次选择**工具 (Tools)** > **数据包捕获 (Packet Capture)**。
捕获会话 (Capture Session) 选项卡将会显示当前已配置的数据包捕获会话列表。如果当前未配置数据包捕获会话，将会显示说明此情况的消息。

步骤 2 要从数据包捕获会话下载特定接口的 PCAP 文件，请点击对应此接口的**下载 (Download)** 按钮。
注释 在数据包捕获会话运行时，无法下载 PCAP 文件。
根据您的浏览器，指定的PCAP文件要么会自动下载到默认下载位置，要么系统会提示您保存文件。

删除数据包捕获会话

如果单个数据包捕获会话当前未运行，则可将其删除，或者可以删除所有不活动的数据包捕获会话。

过程

步骤 1 依次选择**工具 (Tools)** > **数据包捕获 (Packet Capture)**。
捕获会话 (Capture Session) 选项卡将会显示当前已配置的数据包捕获会话列表。如果当前未配置数据包捕获会话，将会显示说明此情况的消息。

步骤 2 要删除特定数据包捕获会话，请点击对应于该会话的**删除 (Delete)** 按钮。

步骤 3 要删除所有不活动的数据包捕获会话，请点击数据包捕获会话列表上方的**删除所有会话 (Delete All Sessions)** 按钮。

测试网络连接

开始之前

要使用网络上另一台设备的主机名或 IPv4 地址来 ping 该设备以测试基本网络连接性，请使用 **ping** 命令。要使用网络上另一台设备的主机名或 IPv6 地址来 ping 该设备，请使用 **ping6** 命令。

要使用网络上另一台设备的主机名或 IPv4 地址来跟踪通向该设备的路由，请使用 **traceroute** 命令。要使用网络上另一台设备的主机名或IPv6地址来跟踪通向该设备的路由，请使用**traceroute6**命令。

- **ping** 和 **ping6** 命令可在 `local-mgmt` 模式下使用。
- **ping** 命令还可在 `module` 模式下使用。
- **traceroute** 和 **traceroute6** 命令可在 `local-mgmt` 模式下使用。
- **traceroute** 命令还可在 `module` 模式下使用。

过程

步骤 1 通过输入以下命令之一连接到 `local-mgmt` 或 `module` 模式：

- **connect local-mgmt**
- **connect module** *module-ID* {**console** | **telnet**}

示例：

```
FP9300-A# connect local-mgmt
FP9300-A(local-mgmt)#
```

步骤 2 要使用网络上另一台设备的主机名或 IPv4 地址来 ping 该设备以测试基本网络连接性：
ping {*hostname* | *IPv4_address*} [**count** *number_packets*] | [**deadline** *seconds*] | [**interval** *seconds*] | [**packet-size** *bytes*]

示例：
此示例显示了如何连接以便对网络上的另一台设备 ping 12 次：

```
FP9300-A(local-mgmt)# ping 198.51.100.10 count 12
PING 198.51.100.10 (198.51.100.10) from 203.0.113.5 eth0: 56(84) bytes of data.
64 bytes from 198.51.100.10: icmp_seq=1 ttl=61 time=0.264 ms
64 bytes from 198.51.100.10: icmp_seq=2 ttl=61 time=0.219 ms
64 bytes from 198.51.100.10: icmp_seq=3 ttl=61 time=0.234 ms
64 bytes from 198.51.100.10: icmp_seq=4 ttl=61 time=0.205 ms
64 bytes from 198.51.100.10: icmp_seq=5 ttl=61 time=0.216 ms
64 bytes from 198.51.100.10: icmp_seq=6 ttl=61 time=0.251 ms
64 bytes from 198.51.100.10: icmp_seq=7 ttl=61 time=0.223 ms
64 bytes from 198.51.100.10: icmp_seq=8 ttl=61 time=0.221 ms
64 bytes from 198.51.100.10: icmp_seq=9 ttl=61 time=0.227 ms
64 bytes from 198.51.100.10: icmp_seq=10 ttl=61 time=0.224 ms
64 bytes from 198.51.100.10: icmp_seq=11 ttl=61 time=0.261 ms
64 bytes from 198.51.100.10: icmp_seq=12 ttl=61 time=0.261 ms

--- 198.51.100.10 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11104ms
rtt min/avg/max/mdev = 51.005/51.062/51.164/0.064 ms

FP9300-A(local-mgmt)#
```

步骤 3 要使用网络上另一台设备的主机名或 IPv4 地址来跟踪通向该设备的路由：
traceroute {*hostname* | *IPv4_address*}

示例：

```
FP9300-A(local-mgmt)# traceroute 198.51.100.10
traceroute to 198.51.100.10 (198.51.100.10), 30 hops max, 40 byte packets
```

```
 1  198.51.100.57 (198.51.100.57)  0.640 ms  0.737 ms  0.686 ms
 2  net1-gw1-13.cisco.com (198.51.100.101)  2.050 ms  2.038 ms  2.028 ms
 3  net1-sec-gw2.cisco.com (198.51.100.201)  0.540 ms  0.591 ms  0.577 ms
 4  net1-fp9300-19.cisco.com (198.51.100.108)  0.336 ms  0.267 ms  0.289 ms

FP9300-A(local-mgmt)#
```

步骤 4 （可选）输入 **exit** 退出 `local-mgmt` 模式并返回到顶级模式。

确定端口通道状态

您可以按照以下步骤来确定当前定义的端口通道的状态。

过程

步骤 1 通过输入以下命令，进入 `/eth-uplink/fabric` 模式：

- **connect eth-uplink**
- **scope fabric** {**a** | **b**}

示例：

```
FP9300-A# connect eth-uplink
FP9300-A /eth-uplink # scope fabric a
FP9300-A /eth-uplink/fabric #
```

步骤 2 输入 **show port-channel** 命令以显示当前端口通道的列表，其中包括每个端口通道的管理状态和运行状态。

示例：

```
FP9300-A /eth-uplink/fabric # show port-channel

Port Channel:
    Port Channel Id Name             Port Type          Admin
 State Oper State       State Reason
    --------------- ---------------- ------------------ -----
------ ---------------- ------------
    10              Port-channel10   Data               Enabl
ed     Failed           No operational members
    11              Port-channel11   Data               Enabl
ed     Failed           No operational members
    12              Port-channel12   Data               Disab
led    Admin Down       Administratively down
    48              Port-channel48   Cluster            Enabl
ed     Up

FP9300-A /eth-uplink/fabric #
```

步骤 3 进入 `/port-channel` 模式，通过输入以下命令来显示单个端口通道和端口信息：

- **scope port-channel** *ID*

示例：

```
FP9300-A /eth-uplink/fabric/port-channel # top
FP9300-A# connect fxos
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2017, Cisco Systems, Inc. All rights reserved.

The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license.

    <--- remaining lines removed for brevity --->

FP9300-A(fxos)#
```

步骤 4 输入 **show** 命令，以显示指定端口通道的状态信息。

示例：

```
FP9300-A /eth-uplink/fabric/port-channel # show

Port Channel:
    Port Channel Id Name             Port Type          Admin
 State Oper State       State Reason
    ---------------- ---------------- ------------------ -----
------ ---------------- ------------
    10               Port-channel10   Data               Enabl
ed     Failed           No operational members

FP9300-A /eth-uplink/fabric/port-channel #
```

步骤 5 输入 **show member-port** 命令，以显示端口通道的成员端口的状态信息。

示例：

```
FP9300-A /eth-uplink/fabric/port-channel # show member-port

Member Port:
    Port Name       Membership         Oper State       State Reas
on
    --------------- ------------------ ---------------- ----------
--
    Ethernet2/3     Suspended          Failed           Suspended
    Ethernet2/4     Suspended          Failed           Suspended

FP9300-A /eth-uplink/fabric/port-channel #
```

端口通道在您将其分配给逻辑设备前不会正常工作。如果从逻辑设备移除端口通道，或删除逻辑设备，则端口通道将恢复为“挂起”(Suspended) 状态。

步骤 6 要查看其他端口通道和 LACP 信息，请退出 `/eth-uplink/fabric/port-channel` 模式，然后通过输入以下命令进入 `fxos` 模式：

- **top**
- **connect fxos**

示例：

步骤 7 输入 **show port-channel summary** 命令，以显示当前端口通道的摘要信息。

示例：

```
FP9300-A(fxos)# show port-channel summary
Flags:  D - Down         P - Up in port-channel (members)
        I - Individual   H - Hot-standby (LACP only)
        s - Suspended    r - Module-removed
        S - Switched     R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
------------------------------------------------------------
------------------
Group Port-       Type     Protocol  Member Ports
      Channel
------------------------------------------------------------
------------------
10    Po10(SD)    Eth      LACP      Eth2/3(s)    Eth2/4(s)

11    Po11(SD)    Eth      LACP      Eth2/1(s)    Eth2/2(s)

12    Po12(SD)    Eth      LACP      Eth1/4(D)    Eth1/5(D)

48    Po48(SU)    Eth      LACP      Eth1/1(P)    Eth1/2(P)
```

其他 **show port-channel** 和 **show lacp** 命令可在 `fxos` 模式下使用。您可以用这些命令来显示各种端口通道和 LACP 信息，如容量、流量、计数器和使用情况。

接下来的操作

有关创建端口通道的信息，请参阅创建端口通道，第 115 页。

从软件故障中恢复

开始之前

在阻止系统成功引导的软件故障情况下，您可以使用以下程序引导新的软件版本。要完成该过程，您需要 TFTP 来引导 kickstart 映像，下载新的系统和管理器映像，然后使用新映像进行引导。

特定 FXOS 版本的恢复映像可以从 Cisco.com 上的以下任一位置获取：

- Firepower 9300 -https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286287252&flowid=77282&softwareid=286287263
- Firepower 4100 系列 -https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286305187&flowid=79423&softwareid=286287263

恢复映像包含三个单独的文件。例如，以下是 FXOS 2.1.1.64 的当前恢复映像。

```
Recovery image (kickstart) for FX-OS 2.1.1.64.
fxos-k9-kickstart.5.0.3.N2.4.11.63.SPA

Recovery image (manager) for FX-OS 2.1.1.64.
fxos-k9-manager.4.1.1.63.SPA

Recovery image (system) for FX-OS 2.1.1.64.
fxos-k9-system.5.0.3.N2.4.11.63.SPA
```

过程

步骤 1 访问 ROMMON：

a) 连接到控制台端口。

b) 重启系统。
系统将开始加载，并且在该过程中会显示一个倒计时计时器。

c) 在倒计时期间按 **Escape** 键可进入 ROMMON 模式。

示例：

```
Cisco System ROMMON, version 1.0.09, RELEASE SOFTWARE
Copyright (c) 1994-2015 by Cisco Systems, Inc.
Compiled Sun 01/01/1999 23:59:59.99 by user

Current image running: Boot ROM0
Last reset cause: LocalSoft
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!

Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address aa:aa:aa:aa:aa:aa

find the string ! boot bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.0.00.00.SPA

  bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.0.00.00.SPA

Use BREAK, ESC or CTRL+L to interrupt boot.
use SPACE to begin boot immediately.
Boot interrupted.

rommon 1  >
```

步骤 2 TFTP 引导 kickstart 映像：

a) 确认已正确设置管理 IP 地址、管理网络掩码和网关 IP 地址。您可以使用 **set** 命令查看其值。您可以使用 **ping** 命令测试与 TFTP 服务器的连接性。

```
rommon 1 > set
    ADDRESS=
    NETMASK=
    GATEWAY=
    SERVER=
    IMAGE=
    PS1="ROMMON ! > "
rommon > address <ip-address>
rommon > netmask <network-mask>
rommon > gateway <default-gateway>
```

b) 将 kickstart 映像复制到可从 Firepower 4100/9300 机箱访问的 TFTP 目录。

注释 该 kickstart 映像的版本号将与捆绑包版本号不匹配。显示 FXOS 版本与 kickstart 映像之间映射的信息可在 Cisco.com 软件下载页面找到。

c) 使用引导命令从 ROMMON 引导映像：

```
boot tftp://<IP address>/<path to image>
```

注释　您还可以使用插入 Firepower 4100/9300 机箱前面板的 USB 插槽中的 USB 介质设备，从 ROMMON 引导 kickstart。如果 USB 设备是在系统运行期间插入的，则您需要先重新引导系统，然后系统才会识别该 USB 设备。

系统将显示一系列 # 指示正在接收映像并且随后会加载 kickstart 映像。

示例：

```
rommon 1 > set
    ADDRESS=
    NETMASK=
    GATEWAY=
    SERVER=
    IMAGE=
    PS1="ROMMON ! > "

rommon 2 > address 10.0.0.2
rommon 3 > netmask 255.255.255.0
rommon 4 > gateway 10.0.0.1
rommon 5 > ping 10.0.0.2
..!!!!!!!!!!
Success rate is 100 percent (10/10)
rommon 6 > ping 192.168.1.2
..!!!!!!!!!!
Success rate is 100 percent (10/10)

rommon 7 > boot tftp://192.168.1.2/fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA
             ADDRESS: 10.0.0.2
             NETMASK: 255.255.255.0
             GATEWAY: 10.0.0.1
              SERVER: 192.168.1.2
               IMAGE: fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA

        TFTP_MACADDR: aa:aa:aa:aa:aa:aa
.....................................................................

Receiving fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA from 192.168.1.2

############################################################################
############################################################################
############################################################################

File reception completed.
```

步骤 3　下载与您刚刚加载到 Firepower 4100/9300 机箱的 kickstart 映像相匹配的恢复系统和管理器映像：

a) 要下载恢复系统和管理器映像，您需要设置管理 IP 地址和网关。您无法通过 USB 下载这些映像。

```
switch(boot)# config terminal
switch(boot)(config)# interface mgmt 0
switch(boot)(config-if)# ip address <ip address> <netmask>
switch(boot)(config-if)# no shutdown
switch(boot)(config-if)# exit
switch(boot)(config)# ip default-gateway <gateway>
switch(boot)(config)# exit
```

b) 将恢复系统和管理器映像从远程服务器复制到 bootflash：
switch(boot)# **copy** *URL* **bootflash:**

使用以下语法之一，为正在导入的文件指定 URL：

- **ftp**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*

- **sftp**://*username@hostname/path/image_name*
- **tftp**://*hostname/path/image_name*

示例：

```
switch(boot)# copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
  bootflash:

switch(boot)# copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
  bootflash:
```

c) 将映像成功复制到 Firepower 4100/9300 机箱后，创建一个自 nuova-sim-mgmt-nsg.0.1.0.001.bin 的管理器映像系统链接。此链接可向加载机制指明要加载的管理器映像。该系统链接的名称应始终为 nuova-sim-mgmt-nsg.0.1.0.001.bin，无论您尝试加载什么映像都是如此。

```
switch(boot)# copy bootflash:<manager-image>
  bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin
```

示例：

```
switch(boot)# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.

switch(boot)(config)# interface mgmt 0
switch(boot)(config-if)# ip address 10.0.0.2 255.255.255.0
switch(boot)(config-if)# no shutdown
switch(boot)(config-if)# exit
switch(boot)(config)# ip default-gateway 10.0.0.1
switch(boot)(config)# exit
switch(boot)# copy
  tftp://192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
  bootflash:
Trying to connect to tftp server......
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy
  tftp://192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
  bootflash:
Trying to connect to tftp server......
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy bootflash:fxos-k9-manager.4.1.1.69.SPA
  bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin

Copy complete, now saving to disk (please wait)...

switch(boot)#
```

步骤 4 加载您刚刚下载的系统映像：

```
switch(boot)# load bootflash:<system-image>
```

示例：

```
switch(boot)# load bootflash:fxos-k9-system.5.0.3.N2.4.11.69.SPA
Uncompressing system image: bootflash:/fxos-k9-system.5.0.3.N2.4.11.69.SPA


Manager image digital signature verification successful
...
System is coming up ... Please wait ...


Cisco FPR Series Security Appliance
FP9300-A login:
```

步骤 5 加载恢复映像后，输入以下命令以避免系统尝试加载旧映像：

注释 在加载恢复映像后应立即执行此步骤。

```
FP9300-A# scope org
FP9300-A /org # scope fw-platform-pack default
FP9300-A /org/fw-platform-pack # set platform-bundle-version ""
Warning: Set platform version to empty will result software/firmware incompatibility issue.
FP9300-A /org/fw-platform-pack* # commit-buffer
```

步骤 6 下载并安装您要在 Firepower 4100/9300 机箱上使用的平台捆绑包映像。有关详细信息，请参阅映像管理，第 37 页。

示例：

```
FP9300-A# scope firmware
FP9300-A /firmware # show download-task

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    fxos-k9.2.1.1.73.SPA
              Tftp     192.168.1.2            0                  Downloaded
FP9300-A /firmware # show package fxos-k9.2.1.1.73.SPA detail
Firmware Package fxos-k9.2.1.1.73.SPA:
    Version: 2.1(1.73)
    Type: Platform Bundle
    State: Active
Time Stamp: 2012-01-01T07:40:28.000
Build Date: 2017-02-28 13:51:08 UTC
FP9300-A /firmware #
```

恢复损坏的文件系统

开始之前

如果管理引擎的板载闪存损坏，并且系统无法再成功启动，您可以使用以下程序恢复系统。要完成该过程，您需要 TFTP 来引导 kickstart 映像，重新格式化闪存，下载新的系统和管理器映像，然后使用新映像进行引导。

注释 此程序包括重新格式化系统闪存。因此，您需要在系统恢复后对其进行完全重新配置。

特定 FXOS 版本的恢复映像可以从 Cisco.com 上的以下任一位置获取：

- Firepower 9300 -https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286287252&flowid=77282&softwareid=286287263
- Firepower 4100 系列 -https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286305187&flowid=79423&softwareid=286287263

恢复映像包含三个单独的文件。例如，以下是 FXOS 2.1.1.64 的恢复映像。

```
Recovery image (kickstart) for FX-OS 2.1.1.64.
fxos-k9-kickstart.5.0.3.N2.4.11.63.SPA

Recovery image (manager) for FX-OS 2.1.1.64.
fxos-k9-manager.4.1.1.63.SPA

Recovery image (system) for FX-OS 2.1.1.64.
fxos-k9-system.5.0.3.N2.4.11.63.SPA
```

过程

步骤 1 访问 ROMMON：

a) 连接到控制台端口。

b) 重启系统。

系统将开始加载，并且在该过程中会显示一个倒计时计时器。

c) 在倒计时期间按 **Escape** 键可进入 ROMMON 模式。

示例：

```
Cisco System ROMMON, version 1.0.09, RELEASE SOFTWARE
Copyright (c) 1994-2015 by Cisco Systems, Inc.
Compiled Sun 01/01/1999 23:59:59:59.99 by user

Current image running: Boot ROM0
Last reset cause: LocalSoft
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!

Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address aa:aa:aa:aa:aa:aa

find the string ! boot bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.0.00.00.SPA

  bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.0.00.00.SPA

Use BREAK, ESC or CTRL+L to interrupt boot.
use SPACE to begin boot immediately.
Boot interrupted.

rommon 1  >
```

步骤 2 TFTP 引导 kickstart 映像：

a) 确认已正确设置管理 IP 地址、管理网络掩码和网关 IP 地址。您可以使用 **set** 命令查看其值。您可以使用 **ping** 命令测试与 TFTP 服务器的连接性。

```
rommon 1 > set
    ADDRESS=
    NETMASK=
    GATEWAY=
    SERVER=
    IMAGE=
    PS1="ROMMON ! > "
rommon > address <ip-address>
rommon > netmask <network-mask>
rommon > gateway <default-gateway>
```

b) 将 kickstart 映像复制到可从 Firepower 4100/9300 机箱访问的 TFTP 目录。

注释 该 kickstart 映像的版本号将与捆绑包版本号不匹配。显示 FXOS 版本与 kickstart 映像之间映射的信息可在 Cisco.com 软件下载页面找到。

c) 使用引导命令从 ROMMON 引导映像：

```
boot tftp://<IP address>/<path to image>
```

注释 您还可以使用插入 Firepower 4100/9300 机箱前面板的 USB 插槽中的 USB 介质设备，从 ROMMON 引导 kickstart。如果 USB 设备是在系统运行期间插入的，则您需要先重新引导系统，然后系统才会识别该 USB 设备。

系统将显示一系列 #，指示正在接收映像并且随后会加载启动映像。

示例：

```
rommon 1 > set
    ADDRESS=
    NETMASK=
    GATEWAY=
    SERVER=
    IMAGE=
    PS1="ROMMON ! > "

rommon 2 > address 10.0.0.2
rommon 3 > netmask 255.255.255.0
rommon 4 > gateway 10.0.0.1
rommon 5 > ping 10.0.0.2
..!!!!!!!!!!
Success rate is 100 percent (10/10)
rommon 6 > ping 192.168.1.2
..!!!!!!!!!!
Success rate is 100 percent (10/10)

rommon 7 > boot tftp://192.168.1.2/fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA
             ADDRESS: 10.0.0.2
             NETMASK: 255.255.255.0
             GATEWAY: 10.0.0.1
              SERVER: 192.168.1.2
               IMAGE: fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA

        TFTP_MACADDR: aa:aa:aa:aa:aa:aa
.....................................................................

Receiving fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA from 192.168.1.2

################################################################################
################################################################################
################################################################################
```

```
File reception completed.
```

步骤 3 加载 kickstart 映像后，使用 **init system** 命令重新格式化闪存。
init system 命令会擦除闪存内容，包括下载到系统的所有软件映像以及系统上的所有配置。完成该命令大概需要 20-30 分钟。

示例：

```
switch(boot)# init system

This command is going to erase your startup-config, licenses as well as the contents of
your bootflash:.

Do you want to continue? (y/n)  [n] y

Detected 32GB flash...
Initializing the system
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):        done
Initializing startup-config and licenses
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):        done
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):        done
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):        done
Formatting bootflash:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):        done
Formatting SAM partition:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):        done
Formatting Workspace partition:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):        done
Formatting Sysdebug  partition:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):        done
```

步骤 4 将恢复映像下载到 Firepower 4100/9300 机箱：

a) 要下载恢复映像，您需要设置管理 IP 地址和网关。您无法通过 USB 下载这些映像。

```
switch(boot)# config terminal
switch(boot)(config)# interface mgmt 0
switch(boot)(config-if)# ip address <ip address> <netmask>
switch(boot)(config-if)# no shutdown
switch(boot)(config-if)# exit
switch(boot)(config)# ip default-gateway <gateway>
switch(boot)(config)# exit
```

b) 将三个恢复映像从远程服务器复制到 bootflash：
switch(boot)# **copy** *URL* **bootflash:**

使用以下语法之一，为正在导入的文件指定 URL：

- **ftp**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*
- **sftp**://*username@hostname*/*path*/*image_name*
- **tftp**://*hostname*/*path*/*image_name*

示例：

```
switch(boot)# copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA
  bootflash:

switch(boot)# copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
  bootflash:

switch(boot)# copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
  bootflash:
```

c) 将映像成功复制到 Firepower 4100/9300 机箱后，创建一个自 nuova-sim-mgmt-nsg.0.1.0.001.bin 的管理器映像系统链接。此链接可向加载机制指明要加载的管理器映像。该系统链接的名称应始终为 nuova-sim-mgmt-nsg.0.1.0.001.bin，无论您尝试加载什么映像都是如此。

```
switch(boot)# copy bootflash:<manager-image>
  bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin
```

示例：

```
switch(boot)# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.

switch(boot)(config)# interface mgmt 0
switch(boot)(config-if)# ip address 10.0.0.2 255.255.255.0
switch(boot)(config-if)# no shutdown
switch(boot)(config-if)# exit
switch(boot)(config)# ip default-gateway 10.0.0.1
switch(boot)(config)# exit
switch(boot)# copy
  tftp://192.168.1.2/recovery_images/fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA
  bootflash:
Trying to connect to tftp server......
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy
  tftp://192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
  bootflash:
Trying to connect to tftp server......
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy
  tftp://192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
  bootflash:
Trying to connect to tftp server......
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy bootflash:fxos-k9-manager.4.1.1.69.SPA
  bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin

Copy complete, now saving to disk (please wait)...
```

```
switch(boot)#
```

步骤 5 重新加载交换机：

```
switch(boot)# reload
```

示例：

```
switch(boot)# reload
This command will reboot this supervisor module. (y/n) ? y
[ 1866.310313] Restarting system.

!!  Rommon image verified successfully  !!


Cisco System ROMMON, Version 1.0.11, RELEASE SOFTWARE
Copyright (c) 1994-2016  by Cisco Systems, Inc.
Compiled Wed 11/23/2016 11:23:23.47 by builder
Current image running: Boot ROM1
Last reset cause: ResetRequest
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!
BIOS has been locked !!

Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address: bb:aa:77:aa:aa:bb

autoboot: Can not find autoboot file 'menu.lst.local'
          Or can not find correct boot string !!
rommon 1 >
```

步骤 6 从 kickstart 和系统映像引导：

```
rommon 1 > boot <kickstart-image> <system-image>
```

注释 在加载系统映像期间，您很可能会看到许可证管理器失败消息。可以安全忽略这些消息。

示例：

```
rommon 1 > dir
Directory of: bootflash:\

  01/01/12  12:33a <DIR>          4,096  .
  01/01/12  12:33a <DIR>          4,096  ..
  01/01/12  12:16a <DIR>         16,384  lost+found
  01/01/12  12:27a           34,333,696  fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA
  01/01/12  12:29a          330,646,465  fxos-k9-manager.4.1.1.69.SPA
  01/01/12  12:31a          250,643,172  fxos-k9-system.5.0.3.N2.4.11.69.SPA
  01/01/12  12:34a          330,646,465  nuova-sim-mgmt-nsg.0.1.0.001.bin
          4 File(s) 946,269,798 bytes
          3 Dir(s)

rommon 2 > boot fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA fxos-k9-system.5.0.3.N2.4.11.69.SPA
  !!   Kickstart Image verified successfully   !!

Linux version: 2.6.27.47 (security@cisco.com) #1 SMP Thu Nov 17 18:22:00 PST 2016
[    0.000000] Fastboot Memory at 0c100000 of size 201326592
Usage: init 0123456SsQqAaBbCcUu

INIT: version 2.86 booting

POST INIT Starts at Sun Jan  1 00:27:32 UTC 2012
S10mount-ramfs.supnuovaca Mounting /isan 3000m
Mounted /isan
Creating /callhome..
Mounting /callhome..
```

```
Creating /callhome done.
Callhome spool file system init done.
Platform is BS or QP MIO: 30
FPGA Version 0x00010500 FPGA Min Version 0x00000600
Checking all filesystems..r.r..r done.
Warning: switch is starting up with default configuration
Checking NVRAM block device ... done
.
FIPS power-on self-test passed
Unpack CMC Application software
Loading system software
Uncompressing system image: bootflash:/fxos-k9-system.5.0.3.N2.4.11.69.SPA


Manager image digital signature verification successful

...

System is coming up ... Please wait ...
nohup: appending output to `nohup.out'

           ---- 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 Fabric interconnect and its clustering mode is performed through these steps.

  Type Ctrl-C at any time 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? (y/n):
```

步骤 7 加载映像后，系统将提示您进入初始配置设置。有关详细信息，请参阅初始配置，第 6 页。

步骤 8 下载您要在 Firepower 4100/9300 机箱上使用的平台捆绑包映像。平台捆绑包映像版本应与您用于恢复系统的映像一致。有关详细信息，请参阅映像管理，第 37 页。

示例：

```
FP9300-A# scope firmware
FP9300-A /firmware # show download-task

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    fxos-k9.2.1.1.73.SPA
              Tftp     192.168.1.2            0                 Downloaded
FP9300-A /firmware # show package fxos-k9.2.1.1.73.SPA detail
Firmware Package fxos-k9.2.1.1.73.SPA:
    Version: 2.1(1.73)
    Type: Platform Bundle
    State: Active
Time Stamp: 2012-01-01T07:40:28.000
Build Date: 2017-02-28 13:51:08 UTC
FP9300-A /firmware #
```

步骤 9 在成功下载平台捆绑包后，您必须手动激活 kickstart 和系统映像，以便在将来加载系统时使用它们。使用此程序从损坏的文件系统进行恢复时不会发生自动激活，因为正在运行的版本与建议的启动版本相匹配。

a) 设置交换矩阵互联 a 的范围：

```
FP9300-A# scope fabric-interconnect a
```

b) 使用 **show version** 命令查看正在运行的内核版本和系统版本。您将使用这些字符串激活映像。

```
FP9300-A /fabric-interconnect # show version
```

c) 输入以下命令以激活映像：

```
FP9300-A /fabric-interconnect # activate firmware
  kernel-version <running_kernel_version> system-version <running_system_version>
commit-buffer
```

注释 服务器状态可能更改为“Disk Failed”。您无需担心此消息，并可继续执行此程序。

d) 使用 **show version** 命令确认已正确设置启动版本并监控映像的激活状态。

重要事项 在状态从“Activating”更改为“Ready”之前，请勿继续进行下一步。

```
FP9300-A /fabric-interconnect # show version
```

示例：

```
FP9300-A /firmware # top
FP9300-A# scope fabric-interconnect a
FP9300-A /fabric-interconnect # show version
Fabric Interconnect A:
    Running-Kern-Vers: 5.0(3)N2(4.11.69)
    Running-Sys-Vers: 5.0(3)N2(4.11.69)
    Package-Vers: 2.1(1.73)
    Startup-Kern-Vers:
    Startup-Sys-Vers:
    Act-Kern-Status: Ready
    Act-Sys-Status: Ready
    Bootloader-Vers:

FP9300-A /fabric-interconnect # activate firmware kernel-version
  5.0(3)N2(4.11.69) system-version 5.0(3)N2(4.11.69)
Warning: When committed this command will reset the end-point
FP9300-A /fabric-interconnect* # commit-buffer
FP9300-A /fabric-interconnect # show version
Fabric Interconnect A:
    Running-Kern-Vers: 5.0(3)N2(4.11.69)
    Running-Sys-Vers: 5.0(3)N2(4.11.69)
    Package-Vers: 2.1(1.73)
    Startup-Kern-Vers: 5.0(3)N2(4.11.69)
    Startup-Sys-Vers: 5.0(3)N2(4.11.69)
    Act-Kern-Status: Activating
    Act-Sys-Status: Activating
    Bootloader-Vers:

FP9300-A /fabric-interconnect # show version
Fabric Interconnect A:
    Running-Kern-Vers: 5.0(3)N2(4.11.69)
    Running-Sys-Vers: 5.0(3)N2(4.11.69)
    Package-Vers: 2.1(1.73)
    Startup-Kern-Vers: 5.0(3)N2(4.11.69)
    Startup-Sys-Vers: 5.0(3)N2(4.11.69)
    Act-Kern-Status: Ready
    Act-Sys-Status: Ready
    Bootloader-Vers:
```

步骤 10 重新启动系统：

示例：

```
FP9300-A /fabric-interconnect # top
FP9300-A# scope chassis 1
```

```
FP9300-A /chassis # reboot no-prompt
Starting chassis reboot. Monitor progress with the command "show fsm status"
FP9300-A /chassis #
```

在最终关闭之前，系统会先关闭每个安全模块/引擎，然后重新启动 Firepower 4100/9300 机箱。此过程大约需要 5-10 分钟。

步骤 11 监控系统状态。服务器状态应从“Discovery”转为“Config”，最后转为“Ok”。

示例：

```
FP9300-A# show server status
Server  Slot Status                        Overall Status        Discovery
------- --------------------------------- --------------------- ---------
1/1     Equipped                          Discovery             In Progress
1/2     Equipped                          Discovery             In Progress
1/3     Empty

FP9300-A# show server status
Server  Slot Status                        Overall Status        Discovery
------- --------------------------------- --------------------- ---------
1/1     Equipped                          Config                Complete
1/2     Equipped                          Config                Complete
1/3     Empty

FP9300-A# show server status
Server  Slot Status                        Overall Status        Discovery
------- --------------------------------- --------------------- ---------
1/1     Equipped                          Ok                    Complete
1/2     Equipped                          Ok                    Complete
1/3     Empty
```

当整体状态为“Ok”时，您的系统即已恢复。您仍必须重新配置安全设备（包括许可证配置），并重新创建所有逻辑设备。更多详情：

- Firepower 9300 快速入门指南 -http://www.cisco.com/go/firepower9300-quick
- Firepower 9300 配置指南 -http://www.cisco.com/go/firepower9300-config
- Firepower 4100 系列快速入门指南 -http://www.cisco.com/go/firepower4100-quick
- Firepower 4100 系列配置指南 -http://www.cisco.com/go/firepower4100-config

索 引

字母

A

B

C

D

F

G

H

J

K

L

M

P

Q

R

S

T

W

X

Y

Z