逻辑设备 Firepower 4100/9300

Firepower 4100/9300 是具有灵活性的安全平台，可在其中安装一个或多个逻辑设备。本章介绍基本的接口配置以及如何使用 防火墙机箱管理器添加独立或高可用性逻辑设备。要添加集群逻辑设备，请参阅Firepower 4100/9300 的 ASA 集群。要使用 FXOS CLI，请参阅 FXOS CLI 配置指南。有关更多高级 FXOS 程序和故障排除，请参阅 FXOS 配置指南。

关于接口

Firepower 4100/9300 机箱支持物理接口和 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。

机箱管理接口

机箱管理接口用于通过 SSH 或 防火墙机箱管理器来管理 FXOS 机箱。此接口独立于分配给应用管理用逻辑设备的 MGMT 型接口。

要配置此接口参数，必须从 CLI 进行配置。要在 FXOS CLI 中查看此接口，请连接到本地管理并显示管理端口：

Firepower # **connect local-mgmt**

Firepower(local-mgmt) # **show mgmt-port**

请注意，即使将物理电缆或小型封装热插拔模块拔下，或者执行了 **mgmt-port shut** 命令，或者逻辑设备已离线，机箱管理接口仍会保持正常运行状态。

注释 机箱管理接口不支持巨型帧。

接口类型

物理接口 和 EtherChannel（端口通道）接口可以是下列类型之一：

- 数据 - 用于常规数据。不能在逻辑设备之间共享数据接口，且逻辑设备无法通过背板与其他逻辑设备通信。对于数据接口上的流量，所有流量必须在一个接口上退出机箱，并在另一个接口上返回以到达另一个逻辑设备。
- 数据共享 - 用于常规数据。仅容器实例支持这些数据接口，可由一个或多个逻辑设备/容器实例（仅限防火墙威胁防御-使用-防火墙管理中心 ）共享。
- 管理 - 用于管理应用实例。这些接口可以由一个或多个逻辑设备共享，以访问外部主机；逻辑设备无法通过此接口与共享接口的其他逻辑设备通信。只能为每个逻辑设备分配一个管理接口。根据您的应用和管理器，您可以稍后从数据接口启用管理；但必须将管理接口分配给逻辑设备，即使您不打算在启用数据管理后使用该接口。有关独立机箱管理接口的信息，请参阅机箱管理接口 ，第 1 页。

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

- 事件 - 用作 防火墙威胁防御-using-防火墙管理中心 设备的辅助管理接口。

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

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

- 集群 - 用作集群逻辑设备的集群控制链路。默认情况下，系统会在端口通道 48 上自动创建集群控制链路。“集群”类型仅在 EtherChannel 接口上受支持。

有关独立部署和集群部署中和 ASA 应用的接口类型支持，请参阅下表。

表 *1:* 接口类型支持

应用		数据	数据：子接口	数据共享	数据共享：子接口	管理	事件	集群（仅 EtherChannel）	集群：子接口
防火墙威胁防御	独立本地实例	是	—	—	—	是	是	—	—
	独立容器实例	是	是	是	是	是	是	—	—
	集群本地实例	是（EtherChannel 仅用于机箱间集群）	—	—	—	是	是	是	—
	集群容器实例	是（EtherChannel 仅用于机箱间集群）	—	—	—	是	是	是	是
ASA	独立本地实例	是	—	—	—	是	—	是	—
	集群本地实例	是（EtherChannel 仅用于机箱间集群）	—	—	—	是	—	是	—

FXOS 接口与应用接口

Firepower 4100/9300 管理物理接口和 EtherChannel（端口通道）接口的基本以太网设置。在应用中，您可以配置更高级别的设置。例如，您只能在 FXOS 中创建 EtherChannel；但是，您可以为应用中的 EtherChannel 分配 IP 地址。

下文将介绍 FXOS 接口与应用接口之间的交互。

VLAN 子接口

对于所有逻辑设备，您可以在应用内创建 VLAN 子接口。

机箱和应用中的独立接口状态

您可以从管理上启用和禁用机箱和应用中的接口。必须在两个操作系统中都启用能够正常运行的接口。由于接口状态可独立控制，因此机箱与应用之间可能出现不匹配的情况。

关于逻辑设备

逻辑设备允许您运行一个应用实例（ASA 或 防火墙威胁防御）和一个可选修饰器应用 (Radware DefensePro) 以形成服务链。

当您添加逻辑设备时，还应定义应用实例类型和版本，分配接口，并配置推送至应用配置的引导程序设置。

注释 对于Firepower 9300，可以在机箱中的独立模块上安装不同类型的应用（ASA 和 防火墙威胁防御）。还可以在独立模块上运行一种应用实例的不同版本。

独立和集群逻辑设备

您可以添加以下类型的逻辑设备：

- 独立 - 独立逻辑设备作为独立单元或高可用性对中的单元运行。
- 集群 - 集群逻辑设备允许您将多个单元集合在一起，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。对于 Firepower 9300，所有三个模块必须参与集群，同时适用于本地实例和容器实例。

硬件和软件组合的要求与前提条件

Firepower 4100/9300支持多种型号、安全模块、应用类型以及高可用性和可扩展性功能。请参阅以下要求，了解允许的组合。

Firepower 9300 的要求

Firepower 9300 包括 3 个安全模块插槽和多种类型的安全模块。请参阅以下要求：

- 安全模块类型 - 您可以在 Firepower 9300 中安装不同类型的模块。例如，您可以将 SM-48 作为模块 1、SM-40 作为模块 2、SM-56 作为模块 3 安装。
- 本地和容器实例 - 在安全模块上安装容器实例时，该模块只能支持其他容器实例。本地实例将使用模块的所有资源，因此只能在模块上安装一个本地实例。可以在某些模块上使用本地实例，在其他模块上使用容器实例。例如，您可以在模块 1 和模块 2 上安装本地实例，但在模块 3 上安装容器实例。

- 集群 - 集群中的所有安全模块（无论是机箱内还是机箱间）都必须为同一类型。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。例如，您可以在机箱 1 中安装 2 个 SM-40，在机箱 2 中安装 3 个 SM-40。 如果在同一机箱中安装了 1 个 SM-48 和 2 个 SM-40，则无法使用集群。
- 高可用性 - 仅在 Firepower 9300 上的同类模块间支持高可用性。 但是，这两个机箱可以包含混合模块。例如，每个机箱都设有 SM-40、SM-48 和 SM-56。可以在 SM-40 模块之间、SM-48 模块之间和 SM-56 模块之间创建高可用性对。
- ASA 和 应用类型-您可以在机箱中的独立模块上安装不同类型的应用。例如，您可以在模块 1 和模块 2 上安装 ASA，在模块 3 上安装 。
- ASA 或 版本 - 您可以在单独的模块上运行不同版本的应用实例类型，或在同一模块上运行单独的容器实例。例如，您可以在模块 1 上安装 6.3，在模块 2 上安装 6.4，在模块 3 上安装 6.5。

Firepower 4100 的要求

Firepower 4100 有多个型号。请参阅以下要求：

- 本地和容器实例 - 在 Firepower 4100 上安装容器实例时，该设备只能支持其他容器实例。本地实例将使用设备的所有资源，因此只能在设备上安装一个本地实例。
- 集群 - 集群内的所有机箱都必须为同一型号。
- 高可用性 - 仅在同类模块间支持高可用性。
- ASA 和 应用类型 - Firepower 4100 只能运行一种应用类型。

逻辑设备的准则和限制

有关准则和限制，请参阅以下章节。

接口的准则和限制

默认 MAC 地址

默认 MAC 地址分配取决于接口类型。

- 物理接口 - 物理接口使用已刻录的 MAC 地址。
- EtherChannel - 对于 EtherChannel，属于通道组的所有接口共用同一个 MAC 地址。此功能使 EtherChannel 对网络应用和用户透明，因为他们只看到一个逻辑连接；而不知道各个链路。端口通道接口使用来自池中的唯一 MAC 地址；接口成员身份不影响 MAC 地址。

一般准则和限制

防火墙模式

您可以在 防火墙威胁防御和 ASA 的引导程序配置中将防火墙模式设置为路由或透明模式。

高可用性

- 在应用配置中配置高可用性。
- 可以将任何数据接口用作故障转移和状态链路。 不支持数据共享接口。

情景模式

- 部署后，请在 ASA 中启用多情景模式。

高可用性的要求和前提条件

- 高可用性故障转移配置中的两个设备必须：
  - 位于单独的机箱上；不支持 Firepower 9300 的机箱内高可用性。
  - 型号相同。
  - 将同一接口分配至高可用性逻辑设备。
  - 拥有相同数量和类型的接口。启用高可用性之前，所有接口必须在 FXOS 中进行相同的预配置。
- 仅 Firepower 9300 上同种类型模块之间支持高可用性；但是两个机箱可以包含混合模块。例如，每个机箱都设有 SM-56、SM-48 和 SM-40。可以在 SM-56 模块之间、SM-48 模块之间和 SM-40 模块之间创建高可用性对。
- 有关其他高可用性系统要求，请参阅 故障转移系统要求一章。

配置接口

默认情况下，物理接口处于禁用状态。可以启用接口，添加 Etherchannel，编辑接口属性。

注释 如果在 FXOS 中删除一个接口（例如，如果您移除网络模块，移除 EtherChannel，或将某个接口重新分配到 EtherChannel），则 ASA 配置会保留原始命令，以便您可以进行任何必要的调整；从配置中删除接口会产生广泛的影响。您可以在 ASA OS 中手动移除旧的接口配置。

配置物理接口

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

注释

- 对于 QSFPH40G-CUxM，默认情况下自动协商会始终处于启用状态，并且您无法将其禁用。
- 如果使用其他 SFP 模块替换端口上的 SFP，则该接口的速度、双工和自动协商不会自动更新。您必须手动重新配置该接口。

开始之前

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

过程

步骤 1 进入接口模式。

scope eth-uplink

scope fabric a

步骤 2 启用接口。

enter interface *interface_id*

enable

示例：

```
Firepower /eth-uplink/fabric # enter interface Ethernet1/8
Firepower /eth-uplink/fabric/interface # enable
```

注释

不能单独修改作为端口通道成员的接口。如果您在作为端口通道成员的接口上使用 **enter interface** 或 **scope interface** 命令，将会收到一条错误消息，说明对象不存在。应先使用 **enter interface** 命令编辑接口，然后在将接口添加到端口通道。

步骤 3 （可选）设置防反跳时间。

set debounce-time 5000 {Enter a value between 0-15000 milli-seconds}

示例：

```
Firepower /eth-uplink/fabric/interface # set debounce-time 5000
```

示例：

注释
不支持在 1G 接口上配置防反跳时间。

步骤 4 （可选）设置接口类型。

set port-type {**data** | **mgmt** | **cluster**}

示例：

```
Firepower /eth-uplink/fabric/interface # set port-type mgmt
```

data 关键字为默认类型。请勿选择 **cluster** 关键字；默认情况下，系统会自动在端口通道 48 上创建集群控制链路。

步骤 5 启用或禁用自动协商（如果您的接口支持）。

set auto-negotiation {**on** | **off**}

示例：

```
Firepower /eth-uplink/fabric/interface* # set auto-negotiation off
```

步骤 6 设置接口速度。

set admin-speed {**1gbps** | **10gbps** | **40gbps** | **100gbps**}

示例：

```
Firepower /eth-uplink/fabric/interface* # set admin-speed 1gbps
```

步骤 7 设置接口双工模式。

set admin-duplex {**fullduplex** |**halfduplex**}

示例：

```
Firepower /eth-uplink/fabric/interface* # set admin-duplex halfduplex
```

步骤 8 如果您编辑了默认流量控制策略，则它已应用于接口。如果您创建了新策略，请将其应用于接口。

set flow-control-policy *name*

示例：

```
Firepower /eth-uplink/fabric/interface* # set flow-control-policy flow1
```

步骤 9 保存配置。

commit-buffer

示例：

```
Firepower /eth-uplink/fabric/interface* # commit-buffer
Firepower /eth-uplink/fabric/interface #
```

添加 EtherChannel（端口通道）

EtherChannel（也称为端口通道）最多可以包含 16 个同一介质类型和容量的成员接口，并且必须设置为相同的速度和双工模式。介质类型可以是RJ-45或SFP；可以混合使用不同类型（铜缆和光纤）的SFP。不能通过在大容量接口上将速度设置为较低值来混合接口容量（例如1GB和10GB接口）。链路聚合控制协议(LACP)将在两个网络设备之间交换链路汇聚控制协议数据单元(LACPDU)，进而汇聚接口。

您可以将 EtherChannel 中的每个物理数据接口配置为：

- Active - 发送和接收 LACP 更新。主用 EtherChannel 可以与主用或备用 EtherChannel 建立连接。除非您需要最大限度地减少 LACP 流量，否则应使用主用模式。
- 开启 - EtherChannel 始终开启，并且不使用 LACP。“开启”的 EtherChannel 只能与另一个“开启”的 EtherChannel 建立连接。

注释 如果将其模式从打开更改为主用或从主用更改为打开状态，则可能需要多达三分钟的时间才能使 EtherChannel 进入运行状态。

非数据接口仅支持主用模式。

LACP 将协调自动添加和删除指向 EtherChannel 的链接，而无需用户干预。LACP 还会处理配置错误，并检查成员接口的两端是否连接到正确的通道组。 如果接口发生故障且未检查连接和配置，“开启”模式将不能使用通道组中的备用接口。

Firepower 4100/9300 机箱 创建 EtherChannel 时，EtherChannel 将处于**挂起**状态（对于主动 LACP 模式）或**关闭**状态（对于打开 LACP 模式），直到将其分配给逻辑设备，即使物理链路是连通的。EtherChannel 在以下情况下将退出**挂起**状态：

- 将 EtherChannel 添加为独立逻辑设备的数据或管理端口
- 将 EtherChannel 添加为属于集群一部分的逻辑设备的管理接口或集群控制链路
- 将 EtherChannel 添加为属于集群一部分的逻辑设备的数据端口，并且至少有一个单元已加入该集群

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**或**关闭**状态。

过程

步骤 1 进入接口模式：

scope eth-uplink

scope fabric a

步骤 2 创建端口通道：

create port-channel *id*

enable

步骤 3 分配成员接口：

create member-port *interface_id*

您最多可以添加相同介质类型和容量的16个成员接口。成员接口必须设置为相同的速度和双工，并且必须与您为此端口通道配置的速度和双工相匹配。介质类型可以是 RJ-45 或 SFP；可以混合使用不同类型（铜缆和光纤）的SFP。不能通过在大容量接口上将速度设置为较低值来混合接口容量（例如 1GB 和 10GB 接口）。

示例：

```
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
```

步骤 4 （可选） 设置接口类型。

set port-type {**data** | **mgmt** | **cluster**}

示例：

```
Firepower /eth-uplink/fabric/port-channel # set port-type data
```

data 关键字为默认类型。请勿选择 **cluster** 关键字，除非要将此端口通道用作集群控制链路，而不是默认设置。

步骤 5 为端口通道的成员设置所需的接口速度。

set speed {**10mbps** | **100mbps** | **1gbps** | **10gbps** | **40gbps** | **100gbps**}

如果添加未达到指定速度的成员接口，接口将无法成功加入端口通道。默认值为 **10gbps**。

示例：

```
Firepower /eth-uplink/fabric/port-channel* # set speed 1gbps
```

步骤 6 （可选）为端口通道的成员设置所需的双工。

set duplex {**fullduplex** | **halfduplex**}

如果添加以指定双工配置的成员接口，接口将无法成功加入端口通道。默认值为 **fullduplex**。

示例：

```
Firepower /eth-uplink/fabric/port-channel* # set duplex fullduplex
```

步骤 7 启用或禁用自动协商（如果您的接口支持）。

set auto-negotiation {**on** | **off**}

示例：

```
Firepower /eth-uplink/fabric/interface* # set auto-negotiation off
```

步骤 8 设置数据接口的 LACP 端口通道模式。

对于非数据接口，模式始终是主用模式。

set port-channel-mode {**active** | **on**}

示例：

```
Firepower /eth-uplink/fabric/port-channel* # set port-channel-mode on
```

步骤 9 如果您编辑了默认流量控制策略，则它已应用于接口。如果您创建了新策略，请将其应用于接口。

set flow-control-policy *name*

示例：

```
Firepower /eth-uplink/fabric/interface* # set flow-control-policy flow1
```

步骤 10 提交配置：

commit-buffer

配置逻辑设备

在 Firepower 4100/9300 机箱上添加独立逻辑设备或高可用性对。

有关集群，请参阅#unique_225。

添加独立 ASA

独立逻辑设备可单独使用，也可在高可用性对中使用。在具有多个安全模块的 Firepower 9300 上，可以配置集群或独立设备。集群必须使用所有模块，因此无法将双模块集群和独立设备进行混用和搭配。

您可以通过 Firepower 4100/9300 机箱部署一个路由或透明防火墙模式的 ASA。

对于多情景模式，您必须先部署逻辑设备，然后在 ASA 应用中启用多情景模式。

开始之前

- 从 Cisco.com 下载要用于逻辑设备的应用映像，然后将映像下载到 Firepower 4100/9300 机箱。

注释 对于 Firepower 9300，可以在机箱中的独立模块上安装不同类型的应用（ASA 和 ）。还可以在独立模块上运行一种应用实例的不同版本。

- 配置逻辑设备要使用的管理接口。管理接口是必需的。请注意，此管理接口不同于仅用于机箱管理的机箱管理端口（在 FXOS 中，可能会看到该接口显示为 MGMT、management0 或其他类似名称）。
- 收集以下信息：
  - 此设备的接口 ID
  - 管理接口 IP 地址和网络掩码
  - 网关 IP 地址

过程

步骤 1 进入安全服务模式。

scope ssa

示例：

```
Firepower# scope ssa
Firepower /ssa #
```

步骤 2 设置应用实例映像版本。

a) 查看可用映像。请注意您想要使用的版本号。

show app

示例：

```
Firepower /ssa # show app
```

```
   Name       Version         Author     Supported Deploy Types CSP Type    Is Default
App
   ---------- --------------- ---------- ---------------------- -----------
--------------
   asa        9.9.1           cisco      Native                 Application No
   asa        9.10.1          cisco      Native                 Application Yes
   ftd        6.2.3           cisco      Native                 Application Yes
```

b) 将范围设置为安全模块/引擎插槽。

scope slot *slot_id*

对于 Firepower 4100，*slot_id*始终为 1；对于 Firepower 9300，则始终为 1、2 或 3。

示例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot #
```

c) 创建应用实例。

enter app-instance asa *device_name*

device_name 可介于 1 至 64 个字符之间。在对此实例创建逻辑设备时，您将使用此设备名称。

示例：

```
Firepower /ssa/slot # enter app-instance asa ASA1
Firepower /ssa/slot/app-instance* #
```

d) 设置 ASA 映像版本。

set startup-version *version*

示例：

```
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
```

e) 退出到插槽模式。

exit

示例：

```
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* #
```

f) 退出到 ssa 模式。

exit

示例：

```
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

示例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa ASA1
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

步骤 3 创建逻辑设备。

enter logical-device *device_name* **asa** *slot_id* **standalone**

使用与您之前添加的应用实例相同的 *device_name*。

示例：

```
Firepower /ssa # enter logical-device ASA1 asa 1 standalone
Firepower /ssa/logical-device* #
```

步骤 4 向逻辑设备分配管理和数据接口。对各个接口重复此步骤。

create external-port-link *name interface_id* **asa**

set description *description*

exit

- *name* - 由 Firepower 4100/9300 机箱管理引擎使用；它不是在 ASA 配置中使用的接口名称。
- *description* - 在含有空格的短语两侧使用引号 (")。

管理接口与机箱管理端口不同。稍后您需要在 ASA 上启用和配置数据接口，包括设置 IP 地址。

示例：

```
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
```

步骤 5 配置管理引导程序信息。

a) 创建引导程序对象。

create mgmt-bootstrap asa

示例：

```
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

b) 指定防火墙模式：路由或透明。

create bootstrap-key FIREWALL_MODE

set value {**routed** |**transparent**}

exit

在路由模式中，设备被视为网络中的路由器跃点。要在其间路由的每个接口都位于不同的子网上。另一方面，透明防火墙是一个第2层防火墙，充当“线缆中的块”或“隐蔽的防火墙”，不被视为是到所连接设备的路由器跃点。

系统仅在初始部署时设置防火墙模式。如果您重新应用引导程序设置，则不会使用此设置。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

c) 指定管理员并启用密码。

create bootstrap-key-secret PASSWORD

set value

输入值： 密码

确认值： 密码

exit

示例：

预配置的 ASA 管理员用户和启用密码在进行密码恢复时非常有用；如果您有 FXOS 访问权限，在您忘记了管理员用户密码时，可以将其重置。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

d) 配置 IPv4 管理接口设置。

create ipv4 *slot_id* **default**

set ip *ip_address* **mask** *network_mask*

set gateway *gateway_address*

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
```

```
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.34 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

e) 配置 IPv6 管理接口设置。

create ipv6 *slot_id* **default**

set ip *ip_address* **prefix-length** *prefix*

set gateway *gateway_address*

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

f) 退出管理引导程序模式。

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

步骤 6 保存配置。

commit-buffer

机箱通过下载指定软件版本，并将引导程序配置和管理接口设置推送至应用实例来部署逻辑设备。使用 **show app-instance** 命令检查部署状态。当**管理状态**为**已启用**且**运行状态**为**在线**时，应用实例正在运行且可供使用。

示例：

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup Version
 Deploy Type Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- --------------- ---------------
 ----------- ------------ --------------- -------------
asa        asa1       2          Disabled    Not Installed                    9.12.1
    Native                    Not Applicable  None
ftd        ftd1       1          Enabled     Online           6.4.0.49        6.4.0.49
    Container   Default-Small Not Applicable  None
```

步骤 7 请参阅 ASA 配置指南，以开始配置安全策略。

示例

```
Firepower# scope ssa
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa MyDevice1
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* # create logical-device MyDevice1 asa 1 standalone
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value transparent
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: secretglassine
Confirm the value: secretglassine
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # commit-buffer
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key #
```

添加高可用性对

ASA 高可用性（也称为故障转移）是在应用中配置，而不是在 FXOS 中配置。但为了让您的机箱做好配置高可用性的准备，请参阅以下步骤。

开始之前

请参阅故障转移系统要求。

过程

步骤 1 将相同的接口分配给各个逻辑设备。

步骤 2 为故障转移和状态链路分配 1 个或 2 个数据接口。

这些接口用于交换 2 个机箱之间的高可用性流量。我们建议您将一个 10 GB 数据接口用于组合的故障转移和状态链路。如果您有可用的接口，可以使用单独的故障转移和状态链路；状态链路需要的带宽最多。不能将管理类型的接口用于故障转移或状态链路。我们建议您在机箱之间使用一个交换机，并且不将同一网段中的其他任何设备作为故障转移接口。

步骤 3 在逻辑设备上启用高可用性。请参阅通过故障转移实现高可用性。

步骤 4 如果您在启用高可用性后需要更改接口，请先在备用设备上执行更改，然后再在主用设备上执行更改。

注释
对于 ASA，如果在 FXOS 中移除一个接口（例如，如果您移除网络模块，移除 EtherChannel，或将某个接口重新分配到 EtherChannel），则 ASA 配置会保留原始命令，以便您可以进行任何必要的调整；从配置中移除接口会产生广泛的影响。您可以在 ASA OS 中手动移除旧的接口配置。

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。

添加新接口或删除未使用的接口对 ASA 配置的影响很小。但是，如果在 FXOS 中删除已分配的接口（例如，如果删除网络模块、删除 EtherChannel，或将分配的接口重新分配给 EtherChannel），并且在安全策略中使用该接口，则删除操作会影响 ASA 配置。在这种情况下，ASA 配置会保留原始命令，以便您可以进行任何必要的调整。您可以在 ASA OS 中手动移除旧的接口配置。

注释 您可以编辑已分配的 EtherChannel 的成员，而不影响逻辑设备。

开始之前

- 根据配置物理接口，第 7 页和添加 EtherChannel（端口通道），第 9 页配置您的接口，并添加任何 EtherChannel。
- 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。
- 对于集群或故障转移，请确保添加或移除所有设备上的接口。我们建议先在数据/备用设备上更改接口，然后再在控制/主用设备上更改接口。新的接口在管理性关闭的状态下添加，因此，它们不会影响接口监控。

过程

步骤 1 进入安全服务模式：

Firepower# **scope ssa**

步骤 2 编辑逻辑设备：

Firepower /ssa # **scope logical-device** *device_name*

步骤 3 从逻辑设备取消分配接口：

Firepower /ssa/logical-device # **delete external-port-link** *name*

输入 **show external-port-link** 命令以查看接口名称。

对于管理接口，请删除当前接口，然后在添加新的管理接口之前，使用 **commit-buffer** 命令确认更改。

步骤 4 将新的接口分配到逻辑设备：

Firepower /ssa/logical-device* # **create external-port-link** *name interface_id* **asa**

步骤 5 提交配置：

commit-buffer

提交系统配置任务。

连接到应用控制台

使用以下程序连接至应用的控制台。

过程

步骤 1 使用控制台连接或 Telnet 连接来连接至模块 CLI。

connect module *slot_number* {**console** | **telnet**}

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*。

使用 Telnet 连接的优点在于，您可以同时对模块开展多个会话，并且连接速度更快。

示例：

```
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>
```

步骤 2 连接到应用控制台。

connect asa *name*

要查看实例名称，请输入不含名称的命令。

示例：

```
Firepower-module1> connect asa asa1
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

步骤 3 退出应用控制台到 FXOS 模块 CLI。

- ASA - 输入 **Ctrl-a, d**

步骤 4 返回 FXOS CLI 的管理引擎层。

退出控制台：

a) 输入 **~**

您将退出至 Telnet 应用。

b) 要退出 Telnet 应用，请输入：

telnet>**quit**

退出 Telnet 会话：

a) 输入 **Ctrl-],**。

示例

以下示例连接至安全模块 1 上的 ASA，然后退回到 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 asa1
asa> ~
telnet> quit
Connection closed.
Firepower#
```

逻辑设备的历史记录

特性	Version	详细信息
用于 Firepower 4112 的 ASA	9.14(1)	我们推出了 Firepower 4112。 **注释** 需要 FXOS 2.8.1。
Firepower 9300 SM-56 支持	9.12.2	我们推出了 SM-56 安全模块。 **注释** 需要 FXOS 2.6.1.157。
适用于 Firepower 4115、4125 和 4145 的 ASA	9.12(1)	我们推出了 Firepower 4115、4125 和 4145。 **注释** 需要 FXOS 2.6.1。
Firepower 9300 SM-40 和 SM-48 支持	9.12.1	我们引入了 SM-40 和 SM-48 安全模块。 **注释** 需要 FXOS 2.6.1。
支持在同一个 Firepower 9300 上使用独立的 ASA 和 防火墙威胁防御 模块	9.12.1	您现在可以在同一个 Firepower 9300 上同时部署 ASA 和 防火墙威胁防御 逻辑设备。 **注释** 需要 FXOS 2.6.1。
Firepower 4100/9300 的集群控制链路可自定义 IP 地址	9.10.1	默认情况下， 集群控制链路使用 127.2.0.0/16 网络。现在，可以在 FXOS 中部署集群时设置网络。机箱根据机箱 ID 和插槽 ID 自动生成每个设备的集群控制链路接口 IP 地址：127.2.*chassis_id*.*slot_id*。但是，某些网络部署不允许 127.2.0.0/16 流量通过。因此，您现在可以为 FXOS 中的集群控制链路设置一个自定义的 /16 子网（环回 (127.0.0.0/8) 和组播 (224.0.0.0/4 地址除外）。 **注释** 需要 FXOS 2.4.1。 新增/修改的 FXOS 命令：**set cluster-control-link network**
支持保存模式下的数据 Etherchannel	9.10.1	现在可以将数据和数据共享 Etherchannel 设置为“主用”LACP 模式或“保持”模式。其他类型 Etherchannel 仅支持“主用”模式。 **注释** 需要 FXOS 2.4.1。 新增/修改的 FXOS 命令：**set port-channel-mode**

特性	Version	详细信息
Firepower 4100/9300 机箱上的 ASA 的站点间集群改进	9.7(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。 修改了以下命令：**site-id**
支持 Firepower 4100 系列	9.6(1)	使用 FXOS 1.1.4，ASA 在 Firepower 4100 系列上支持机箱间集群。 未修改任何命令。
6 个模块的机箱间集群，以及 Firepower 9300 ASA 应用的站点间集群	9.5(2.1)	现在您可利用 FXOS 1.1.3 启用机箱内集群，并扩展至站点间集群。在最多 6 个机箱中最多可以包含 6 个模块。 未修改任何命令。
Firepower 9300 的机箱内 ASA 集群	9.4(1.150)	最多可对 Firepower 9300 机箱内的 3 个安全模块建立集群。机箱中的所有模块都必须属于该集群。 引入了以下命令：**cluster replication delay**、**debug service-module**、**management-only individual**、**show cluster chassis**

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。