



Firepower 4100/9300 上的逻辑设备

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。

必须配置机箱接口、添加逻辑设备，并使用防火墙机箱管理器或 FXOS CLI 将接口分配给 Firepower 4100/9300 机箱上的设备。您无法在防火墙设备管理器中执行这些任务。

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，第 1 页](#)
- [Firepower 9300 硬件和软件组合的要求与前提条件，第 3 页](#)
- [逻辑设备的准则和限制，第 3 页](#)
- [配置接口，第 4 页](#)
- [配置逻辑设备，第 8 页](#)
- [逻辑设备的历史记录，第 18 页](#)

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。此接口在接口 (Interfaces) 选项卡顶部显示为 **MGMT**，您只可在接口 (Interfaces) 选项卡上启用或禁用此接口。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 `Firewall Threat Defense`-使用-）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 `Firewall Threat Defense`-using- 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。防火墙设备管理器 和 Security Cloud Control 不支持群集技术。

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。

Firepower 9300 硬件和软件组合的要求与前提条件

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。
- 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 Firewall Threat Defense 应用类型-您可以在机箱中的独立模块上安装不同类型的應用。例如，您可以在模块 1 和模块 2 上安装 ASA，在模块 3 上安装 Firewall Threat Defense。
- ASA 或 Firewall Threat Defense 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 Firewall Threat Defense 6.3，在模块 2 上安装 Firewall Threat Defense 6.4，在模块 3 上安装 Firewall Threat Defense 6.5。

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

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。
- 高可用性故障转移配置中的两个设备必须：
 - 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。
- 有关详细信息，请参阅[高可用性的系统要求](#)。

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。

启用或禁用接口

可以将每个接口的管理状态更改为启用或禁用。默认情况下，物理接口处于禁用状态。

过程

步骤 1 选择接口 (**Interfaces**) 打开接口页面。

“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 要启用接口，请点击已禁用滑块已禁用（），使其更改为已启用滑块已启用（）。

点击是，确认更改。以直观展示图表现的对应接口从灰色变为绿色。

步骤 3 要禁用接口，请点击已启用滑块已启用（），使其更改为已禁用滑块已禁用（）。

点击是，确认更改。以直观展示图表现的对应接口从绿色变为灰色。

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 QSFP40G-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 选择接口 (**Interfaces**) 打开“接口” (**Interfaces**) 页面。

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

步骤 2 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，请选中启用复选框。要禁用接口，请取消选中启用复选框。

步骤 4 选择接口类型：

有关接口类型使用的详细信息，请参阅[接口类型](#)，第 2 页。

- 数据
- 管理
- 集群 - 请勿选择集群类型；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（可选）从**速度 (Speed)** 下拉列表中选择接口的速度。

步骤 6（可选）如果您的接口支持**自动协商**，请点击**是 (Yes)** 或**否 (No)** 单选按钮。

如果通过 50G 电缆连接到端口的对等交换机不支持自动协商，请确保同时在交换机和平台接口上禁用自动协商。例如，N9K-C93400LD-H1 不支持在 50G 电缆上进行自动协商。因此，要连接端口，必须在平台和交换机上禁用默认自动协商。

步骤 7（可选）从**双工 (Duplex)** 下拉列表中选择接口双工。

步骤 8（可选）明确配置**防反跳时间 (ms)**。输入 0-15000 毫秒之间的值。

注释

不支持在 1G 接口上配置防反跳时间。

步骤 9 点击**确定**。

添加 EtherChannel（端口通道）

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

Firepower 4100/9300 仅支持主用 LACP 模式下的 Etherchannel，以便每个成员接口发送和接收 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。

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 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 选择接口 (**Interfaces**) 打开“接口” (**Interfaces**) 页面。

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

步骤 2 点击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，可以将其删除并为集群类型 EtherChannel 配置不同的 ID。对于机箱内集群，请不要将任何接口分配给集群 EtherChannel。

步骤 4 要启用端口通道，请选中启用复选框。要禁用端口通道，请取消选中启用复选框。

步骤 5 选择接口类型：

有关接口类型使用的详细信息，请参阅[接口类型](#)，第 2 页。

- 数据
- 管理
- 集群

步骤 6 从下拉列表设置成员接口要求的**管理速度**。

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。

步骤 7 对于数据接口，选择 LACP 端口通道模式、主用或保持。

对于非数据接口，模式始终是主用模式。

步骤 8 为成员接口、全双工或半双工设置所需的**管理双工**。

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。

步骤 9 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”列表。

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）。

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 10 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 11 点击确定。

配置逻辑设备

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

为 防火墙设备管理器 添加独立的 Firewall Threat Defense

可以将防火墙设备管理器与本地实例结合使用。不支持容器实例。独立逻辑设备可单独使用，也可在高可用性对中使用。

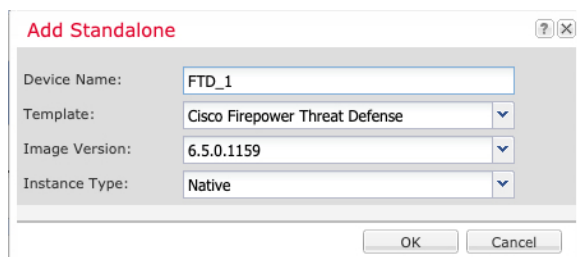
开始之前

- 从 Cisco.com 下载要用于逻辑设备的应用映像，然后将映像上传到 Firepower 4100/9300。
- 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（并且在接口选项卡的顶部显示为 **MGMT**）。
- 您还必须至少配置一个数据类型的接口。
- 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
 - DNS 服务器 IP 地址
 - Firewall Threat Defense 主机名和域名

过程

步骤 1 选择逻辑设备。

步骤 2 点击添加 > 独立设备，并设置以下参数：



The screenshot shows a dialog box titled "Add Standalone" with the following fields and values:

Field	Value
Device Name	FTD_1
Template	Cisco Firepower Threat Defense
Image Version	6.5.0.1159
Instance Type	Native

a) 提供设备名称。

此名称由机箱管理引擎用于配置管理设置和分配接口；它不是在应用配置中使用的设备名称。

注释

添加逻辑设备后，无法更改此名称。

b) 对于模板，请选择 **Cisco Firepower Threat Defense**。

c) 选择映像版本。

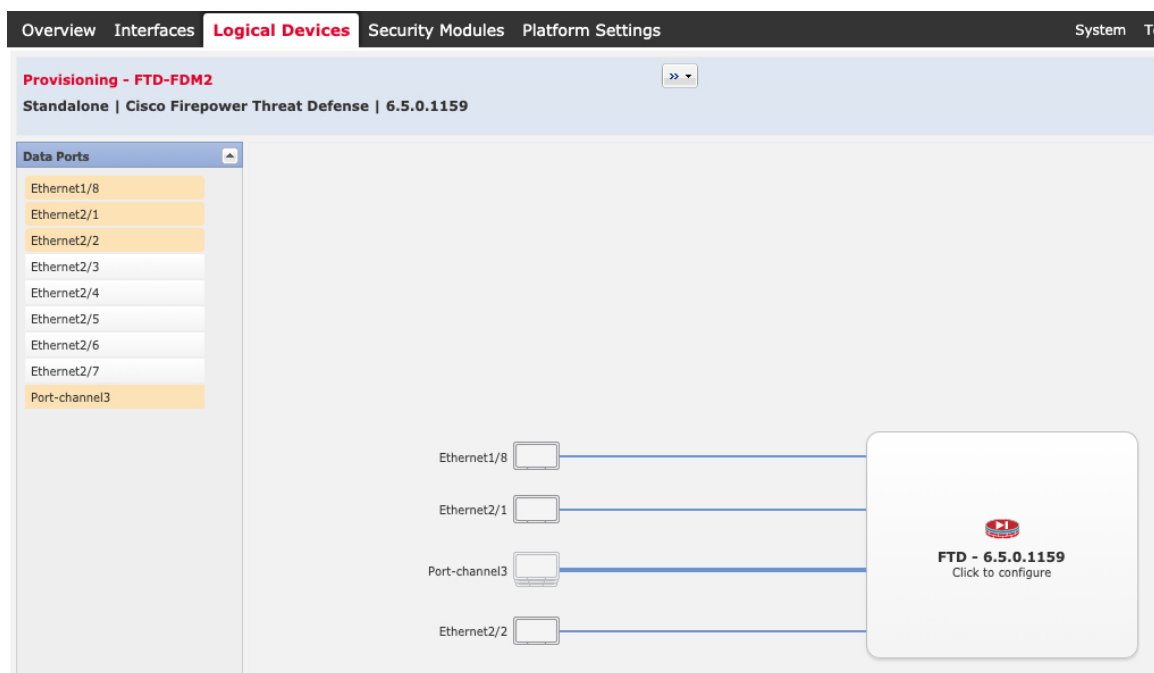
d) 选择实例类型：本地。

防火墙设备管理器不支持容器实例。

e) 点击确定。

屏幕会显示调配 - 设备名称窗口。

步骤 3 展开数据端口 (**Data Ports**) 区域，然后点击要分配给设备的每个接口。

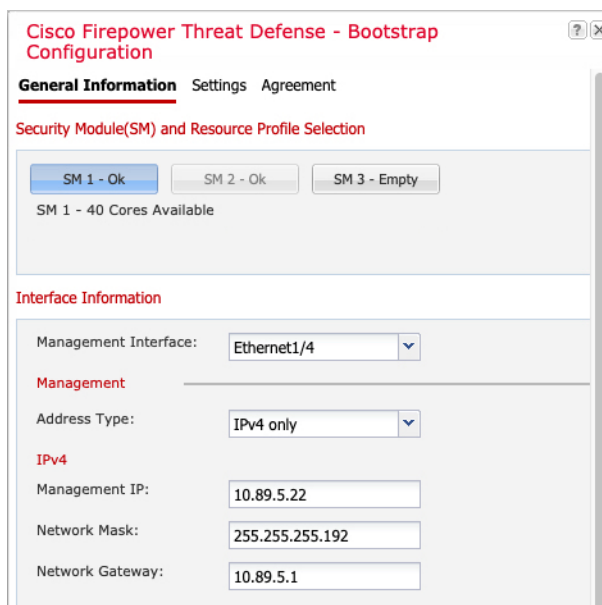


仅可分配先前在接口 (**Interfaces**) 页面上启用的数据接口。稍后您需要在 防火墙设备管理器 中启用和配置这些接口，包括设置 IP 地址。

步骤 4 点击屏幕中心的设备图标。

系统将显示对话框，可以在该对话框中配置初始引导程序设置。这些设置仅用于仅初始部署或灾难恢复。为了实现正常运行，稍后可以更改应用 CLI 配置中的大多数值。

步骤 5 在一般信息 (**General Information**) 页面上，完成下列操作：



a) (对于 Firepower 9300) 在安全模块选择下，点击您想用于此逻辑设备的安全模块。

- b) 选择**管理接口**。
此接口用于管理逻辑设备。此接口独立于机箱管理端口。
- c) 选择**管理接口地址类型**：仅 IPv4、仅 IPv6 或 IPv4 和 IPv6。
- d) 配置**管理 IP** 地址。
设置用于此接口的唯一 IP 地址。
- e) 输入**网络掩码或前缀长度**。
- f) 输入**网络网关地址**。

步骤 6 在设置选项卡上，完成下列操作：

The screenshot shows the 'Cisco Firepower Threat Defense - Bootstrap Configuration' dialog box with the 'Settings' tab selected. The fields are as follows:

- Management type of application instance: **LOCALLY_MANAGED** (dropdown)
- Firepower Management Center IP: (empty text box)
- Search domains: **cisco.com** (text box)
- Firewall Mode: **Routed** (dropdown)
- DNS Servers: **10.8.9.6** (text box)
- Firepower Management Center NAT ID: (empty text box)
- Fully Qualified Hostname: **ftd.example.cisco.com** (text box)
- Registration Key: (empty text box)
- Confirm Registration Key: (empty text box)
- Password: ********* (password field)
- Confirm Password: ********* (password field)
- Eventing Interface: (empty dropdown)

Buttons at the bottom: OK, Cancel.

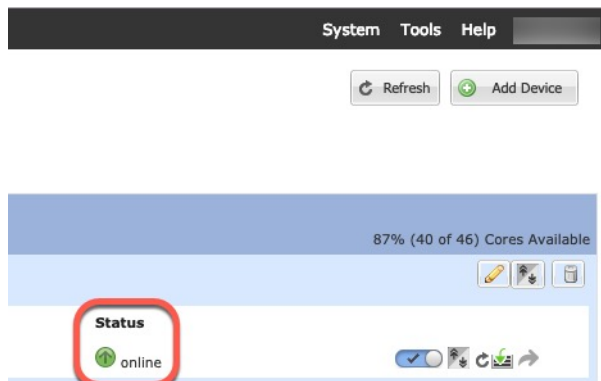
- a) 在**应用实例的管理类型**下拉列表中，选择 **LOCALLY_MANAGED**。
本地实例还支持 作为管理器。如果在部署逻辑设备后更改管理器，则系统会清除您的配置，并重新初始化设备。
- b) 输入逗号分隔列表形式的**搜索域**。
- c) 防火墙模式仅支持路由式。
- d) 输入逗号分隔列表形式的**DNS 服务器**。
- e) 输入Firewall Threat Defense的**完全限定主机名**。
- f) 输入供Firewall Threat Defense管理员用户用于 CLI 访问的**密码**。

步骤 7 在协议选项卡上，阅读并接受最终用户许可协议 (EULA)。

步骤 8 点击**确定**关闭配置对话框。

步骤 9 点击保存 (Save)。

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。在**逻辑设备 (Logical Devices)** 页面中，查看新逻辑设备的状态。当逻辑设备将其状态显示为**在线**时，可以开始在应用中配置安全策略。



步骤 10 请参阅《[防火墙设备管理器 配置指南](#)》，以开始配置安全策略。

添加高可用性对

Firewall Threat Defense 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[高可用性的系统要求](#)。

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[高可用性（故障转移）](#)。

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。

更改Firewall Threat Defense逻辑设备上的接口

可以在 Firewall Threat Defense 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 或 防火墙设备管理器 中同步接口配置。

添加新接口或删除未使用接口对 Firewall Threat Defense 配置的影响最小。但是，删除安全策略中使用的接口会影响配置。可以直接在 Firewall Threat Defense 配置中的很多位置引用接口，包括访问规则、NAT、SSL、身份规则、VPN、DHCP 服务器等。引用安全区的策略不受影响。还可以编辑已分配的 EtherChannel 的成员关系，而不影响逻辑设备或要求在 或 防火墙设备管理器 上进行同步。

对于 防火墙设备管理器：可以在删除旧接口前，将配置从一个接口迁移至另一个接口。

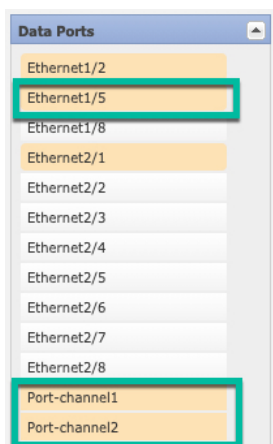
开始之前

- 根据 [配置物理接口](#)，第 5 页和 [添加 EtherChannel（端口通道）](#)，第 6 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。
- 如果要将管理或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。Firewall Threat Defense 重新启动（管理接口更改导致重新启动），并且在 或 防火墙设备管理器 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。
- 对于高可用性，请确保在所有设备上添加或删除该接口，然后在 或 防火墙设备管理器 中同步配置。我们建议先在备用设备上更改接口，然后再在主用设备上更改接口。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。
- 在多实例模式下，要更改具有相同 vlan 标记的另一个子接口的子接口，必须先删除该接口的所有配置（包括 `nameif config`），然后从 防火墙机箱管理器取消分配该接口。取消分配后，添加新接口，然后使用 中的同步接口。

过程

- 步骤 1** 在 防火墙机箱管理器 中，选择 **逻辑设备**。
- 步骤 2** 点击右上角的 **编辑** 图标以编辑逻辑设备。
- 步骤 3** 通过在 **数据端口** 区域中选择新的数据接口来分配该接口。

请勿删除任何接口。

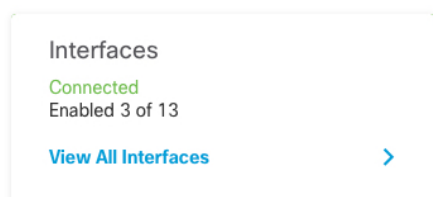
**步骤 4** 替换管理接口：

对于这些类型的接口，在您保存更改后，设备会重新启动。

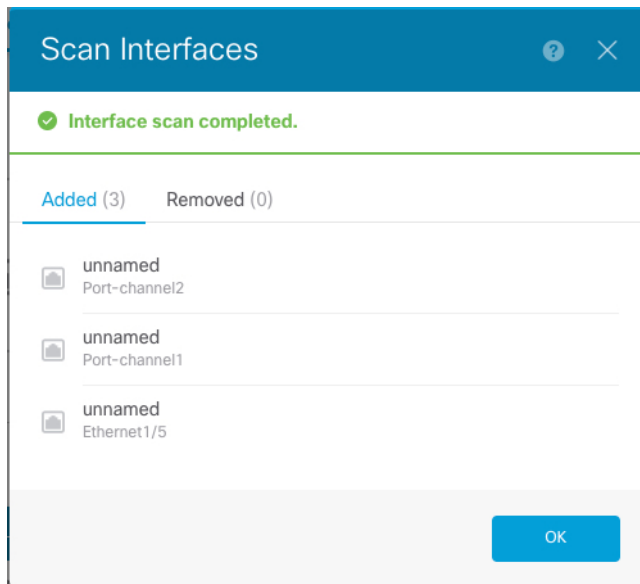
- a) 点击页面中心的设备图标。
- b) 在常规选项卡上，从下拉列表中选择新的管理接口。
- c) 点击确定。

步骤 5 点击保存。**步骤 6** 同步和迁移 防火墙设备管理器 中的接口。

- a) 登录至防火墙设备管理器。
- b) 点击设备，然后点击接口摘要中的查看所有接口链接。



- c) 点击扫描接口图标。
- d) 等待接口扫描，然后点击确定。



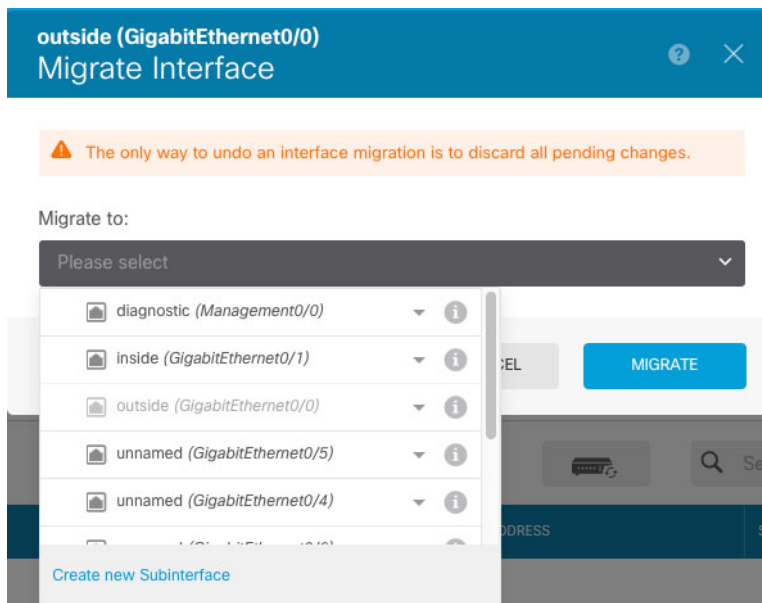
- e) 使用名称、IP 地址等配置新接口。

如果要使用待删除接口的现有 IP 地址和名称，则需要使用虚拟名称和 IP 地址重新配置旧接口，以便可以在新接口上使用这些设置。

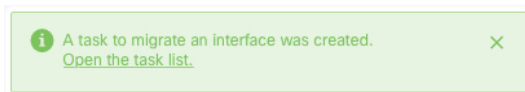
- f) 要将旧接口替换为新接口，请点击旧接口的“替换”图标。

此过程会将旧接口替换为引用该接口的所有配置设置中的新接口。

- g) 从替换接口下拉列表中选择新接口。



- h) 一则消息将显示在接口 (Interfaces) 页面上。点击消息中的链接。

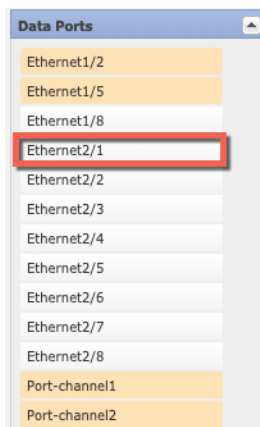


i) 检查任务列表，以确保迁移成功。

The screenshot shows a 'Task List' window with a blue header. Below the header, there are four summary boxes: '8 total', '0 running', '7 completed' (highlighted with a blue border), and '1 failures'. To the right is a link 'Delete all finished tasks'. Below this is a table with columns: Name, Start Time, End Time, Status, and Actions.

Name	Start Time	End Time	Status	Actions
Config migration from source interface outside to destination interface outside_2	06 Jun 2019 12:37 PM	06 Jun 2019 12:37 PM	✓ Migration is successful	

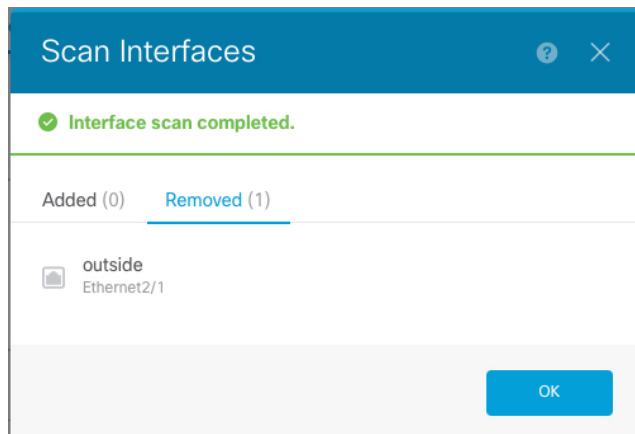
步骤 7 在 防火墙机箱管理器 中，通过在 **数据端口 (Data Ports)** 区域中取消选择数据接口来取消分配该接口。



步骤 8 点击保存。

步骤 9 再次在 或 防火墙设备管理器 中同步接口。

图 1: 防火墙设备管理器扫描接口



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 ftd name

要查看实例名称，请输入不含名称的命令。

示例：

```
Firepower-module1> connect ftd ftd1
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
[...]
>
```

步骤 3 退出应用控制台到 FXOS 模块 CLI。

- Firewall Threat Defense - 输入 **exit**

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-]**。

逻辑设备的历史记录

特性	版本	详细信息
支持 Firepower 4100/9300 上的防火墙设备管理器。	6.5.0	您现在可将 防火墙设备管理器 与 Firepower 4100/9300 上的 Firewall Threat Defense 逻辑设备结合使用。防火墙设备管理器 不支持多实例功能；仅支持本地实例。 注释 需要 FXOS 2.7.1。

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。

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。

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。

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。