



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 Cisco Secure Firewall 机箱管理器或 FXOS CLI 将接口分配到 Firepower 4100/9300 机箱上的设备。您无法在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 6 页](#)
- [Firepower 4100/9300 逻辑设备的历史记录，第 11 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，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（仅限威胁防御-使用-管理中心）共享。
- 管理 - 用于管理应用程序实例。这些接口可以由一个或多个逻辑设备共享，以访问外部主机；逻辑设备无法通过此接口与共享接口的其他逻辑设备通信。只能为每个逻辑设备分配一个管理接口。根据您的应用和管理器，您可以稍后从数据接口启用管理；但必须将管理接口分配给逻辑设备，即使您不打算在启用数据管理后使用该接口。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 威胁防御-using-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。设备管理器 和 CDO 不支持集群。

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 威胁防御 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 威胁防御。
- ASA 或 威胁防御 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 威胁防御 6.3，在模块 2 上安装 威胁防御 6.4，在模块 3 上安装 威胁防御 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。

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。

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 机箱仅支持主用 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 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。

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。

为设备管理器添加独立的威胁防御

可以将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，然后将映像到 Firepower 4100/9300 机箱。
- 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。
- 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
 - 威胁防御 主机名和域名

过程

请参阅《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

威胁防御 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。

更改威胁防御逻辑设备上的接口

可以在威胁防御 逻辑设备上分配或取消分配接口。然后，您可以在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威胁防御配置的影响最小。但是，删除安全策略中使用的接口会影响配置。可以直接在威胁防御 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设备管理器上进行同步。

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

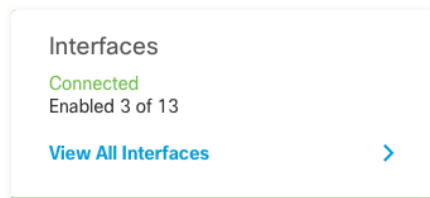
- 根据[配置物理接口](#)，第 5 页和[添加 EtherChannel（端口通道）](#)，第 5 页配置您的接口，并添加任何 EtherChannel。

- 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。
- 对于高可用性，请确保在所有设备上添加或删除该接口，然后在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。

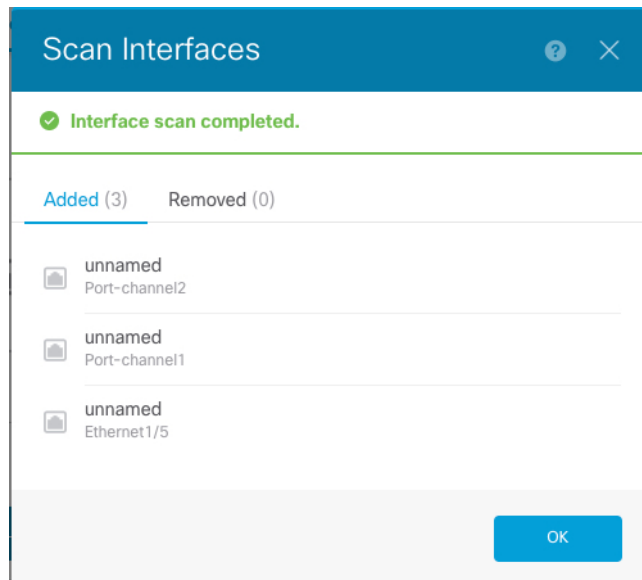
过程

步骤 1 同步和迁移 设备管理器 中的接口。

- 登录至设备管理器。
- 点击**设备 (Device)**，然后点击**接口 (Interfaces)**摘要中的**查看所有接口 (View All Interfaces)**链路。



- 点击**扫描接口图标**。
- 等待接口扫描，然后点击**确定**。



- 使用名称、IP 地址等配置新接口。

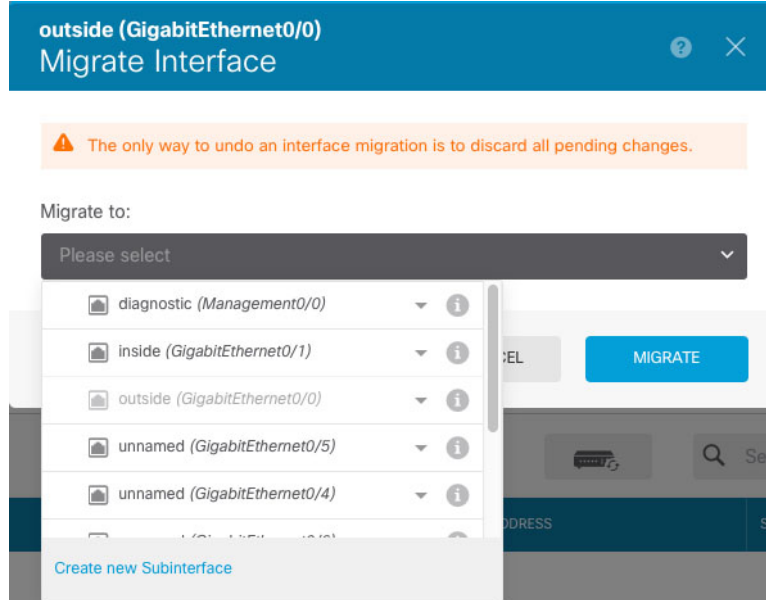
如果要使用待删除接口的现有 IP 地址和名称，则需要使用虚拟名称和 IP 地址重新配置旧接口，以便可以在新接口上使用这些设置。

- 要将旧接口替换为新接口，请点击旧接口的“替换”图标。

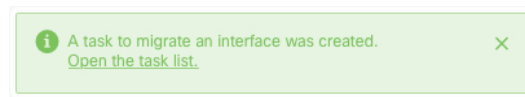
替换图标

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。

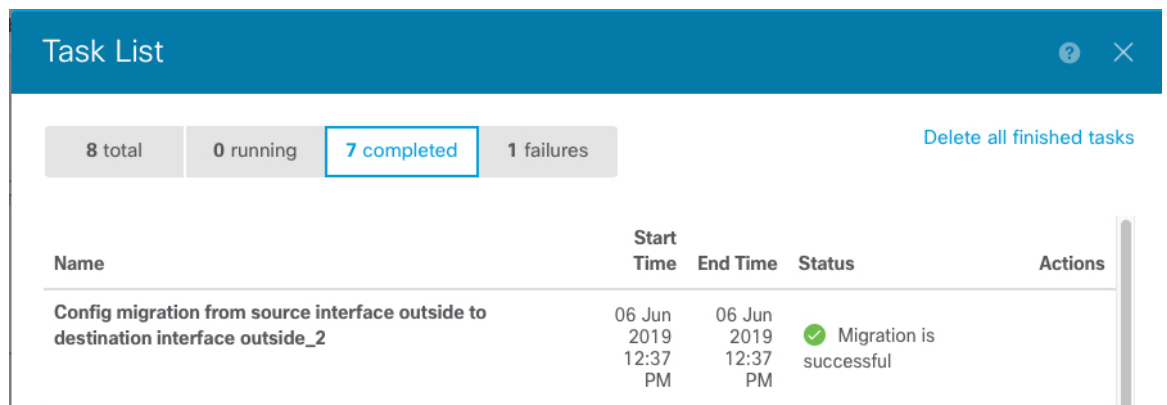
- g) 从替换接口下拉列表中选择新接口。



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

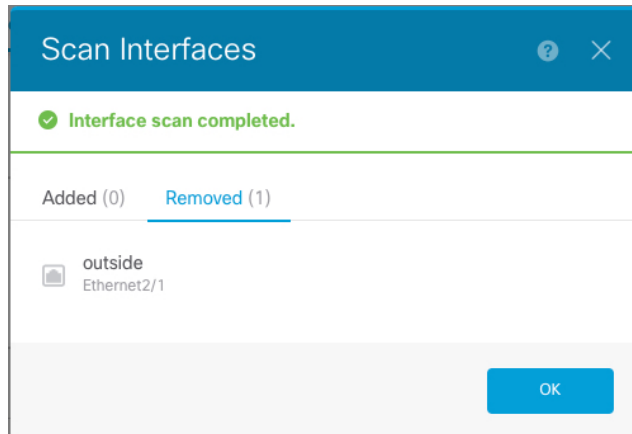


- i) 检查任务列表，以确保迁移成功。



步骤 2 再次在设备管理器中同步接口。

图 1: 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。

- 威胁防御 - 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-]**。

Firepower 4100/9300 逻辑设备的历史记录

特性	版本	详细信息
支持 Firepower 4100/9300 上的设备管理器	6.5.0	现在，您可以将设备管理器与 Firepower 4100/9300 上的威胁防御逻辑设备配合使用。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。