



接口

以下主题介绍如何在 威胁防御 设备上配置接口。

- [关于 威胁防御 接口，第 1 页](#)
- [接口的准则和限制，第 4 页](#)
- [配置物理接口，第 5 页](#)
- [配置网桥组，第 10 页](#)
- [配置 EtherChannel，第 14 页](#)
- [配置 VLAN 接口和交换机端口 \(Firepower 1010\)，第 23 页](#)
- [配置 VLAN 子接口和 802.1Q 中继，第 34 页](#)
- [配置被动接口，第 39 页](#)
- [配置高级接口选项，第 42 页](#)
- [扫描接口更改并迁移接口，第 47 页](#)
- [管理 Cisco Secure Firewall 3100 的网络模块，第 51 页](#)
- [对电源故障配置硬件旁路 \(ISA 3000\)，第 60 页](#)
- [监控接口，第 62 页](#)
- [接口示例，第 63 页](#)

关于 威胁防御 接口

威胁防御 包括数据接口和管理/诊断 接口。

将电缆（以物理方式或虚拟方式）连接到接口接头时，您需要配置该接口。至少需要命名并启用该接口，该接口才会传输流量。如果该接口是网桥组的成员，此配置就已足够。对于非网桥组成员，您还需要为该接口指定一个 IP 地址。如果要在特定端口上创建 VLAN 子接口（而非单一物理接口），通常要在该子接口（而不是物理接口）上配置 IP 地址。通过 VLAN 子接口，可以将一个物理接口拆分为多个标记有不同 VLANID 的逻辑接口，这一点在您连接到交换机的中继端口时非常有用。请勿在被动接口上配置 IP 地址。

接口页面包括接口类型的子页面：**接口 (Interfaces)**（适用于物理接口）、**网桥组 (Bridge Groups)**、**虚拟隧道接口 (Virtual Tunnel Interfaces)**、**EtherChannel** 和 **VLAN**（适用于 Firepower 1010）。请注意，Firepower 4100/9300 EtherChannel 列于 **接口 (Interfaces)** 页面上而不是 **EtherChannel** 页面上，因为仅可修改 FXOS 中的 EtherChannel 参数，而不是设备管理器中的参数。各页显示的是可用接

口、接口名称、地址、模式以及状态。您可以直接在接口列表中更改接口的状态，打开接口或将其关闭。列表将基于您的配置显示接口特征。使用网桥组、EtherChannel 或 VLAN 接口上的开/关箭头可查看成员接口，这些成员接口也会显示于相应列表中。还可以查看受支持父接口的子接口。有关如何将接口映射到虚拟接口和网络适配器的信息，请参阅 [VMware 网络适配器和接口如何映射到威胁防御物理接口](#)。

以下主题介绍了通过设备管理器配置接口的局限性及其他接口管理概念。

接口模式

可以为每个接口配置下列其中一种模式：

路由

每个第 3 层路由接口都需要唯一子网上的一个 IP 地址。通常会将这些接口与交换机、另一个路由器上的端口或 ISP/WAN 网关连接。

被动

被动接口使用交换机 SPAN（交换端口分析器）或镜像端口监控在网络中传输的流量。SPAN 或镜像端口允许从交换机的其他端口复制流量。此功能可以提供网络内的系统可视性，而不会影响网络流量。如果在被动部署中配置系统，系统将不能执行某些操作，例如，阻止流量或流量整形。被动接口无条件接收所有流量，这些接口不会重传接收到的流量。

交换机端口 (Firepower 1010)

交换机端口使用硬件中的交换功能在第 2 层转发流量。同一 VLAN 上的交换机端口可使用硬件交换互相通信，且流量不受威胁防御安全策略的限制。接入端口仅接受未标记流量，可以将其分配给单个 VLAN。中继端口接受未标记和已标记流量，且可以属于多个 VLAN。无法将管理接口配置为交换机端口。

BridgeGroupMember

网桥组是威胁防御设备用于桥接而非路由的一组接口。所有接口位于同一网络上。网桥组由在网桥网络上有 IP 地址的桥接虚拟接口 (BVI) 表示。

如果指定 BVI，您可以在路由接口和 BVI 之间路由。在这种情况下，BVI 充当成员接口和路由接口之间的网关。如果不指定 BVI，网桥组成员接口上的流量不能离开网桥组。通常，可以指定该接口，以便将成员接口路由到互联网。

路由模式下网桥组的一种用途是在威胁防御设备上而非外部交换机上使用额外接口。您可以将终端直接连接到网桥组成员接口。您还可以连接交换机，以将更多终端添加到与 BVI 相同的网络。

管理/诊断接口

标记为“管理”的物理端口（对于 threat defense virtual，则为 Management0/0 虚拟接口）实际上有两个与其关联的单独接口。

- 管理虚拟接口 - 此 IP 地址用于系统通信。这是系统用于进行智能许可和检索数据库更新的地址。您可以打开它的管理会话（设备管理器 和 CLI）。您必须配置一个管理地址，该地址在系统设置 > 管理接口上定义。

- 诊断虚拟接口 - 可以使用此接口将系统日志消息发送到外部系统日志服务器。为诊断接口配置 IP 地址是可选项。配置该接口的主要原因是您需要将它用于系统日志消息。此接口显示在**设备 (Device) > 接口 (Interfaces)** 页面上，并可在此页面上进行配置。诊断接口只允许管理流量，而不允许穿越流量。

(硬件设备。) 一种用于配置管理/诊断接口的方法是，不将物理端口连接到网络。而是仅配置管理 IP 地址，并把它配置为将数据接口用作从互联网获取更新的网关。然后，打开 HTTPS/SSH 流量（默认情况下启用 HTTPS）的内部接口，并使用内部 IP 地址打开设备管理器（请参阅[配置管理访问列表](#)）。

对于 threat defense virtual，建议的配置是将 Management0/0 连接到与内部接口相同的网络，并将内部接口用作网关。不要为诊断接口配置单独的地址。

配置单独管理网络的建议

(硬件设备。) 如果要使用单独管理网络，请将物理管理接口连接到交换机或路由器。

对于 threat defense virtual，请将 Management0/0 连接到不同于任何数据接口的独立网络。如果仍然使用默认 IP 地址，则需要更改管理 IP 地址或内部接口 IP 地址（因为它们在同一子网上）。

然后，进行以下配置：

- 依次选择**设备 > 系统设置 > 管理接口**，并配置所连接网络上的 IPv4 或 IPv6 地址（或两者）。如果需要，可以配置 DHCP 服务器以便能向网络上的其他终端提供 IPv4 地址。如果路由器在管理网络上有到互联网的路由，则可将其作为网关来使用。如果没有，请使用数据接口作为网关。
- 仅当您打算通过该接口向系统日志服务器发送系统日志消息时，才需要为诊断接口配置地址（在**设备 > 接口**上）。否则，不要为诊断接口配置地址，因为这不需要。您配置的任何 IP 地址必须与管理 IP 地址在同一子网上，并且不能在 DHCP 服务器池中。例如，如果使用 192.168.45.45 作为管理地址，192.168.45.46 至 192.168.45.254 作为 DHCP 池，则可以使用从 192.168.45.1 到 192.168.45.44 的任何地址配置诊断接口。

安全区

可为每个接口分配一个安全区。然后根据区域应用您的安全策略。例如，您可以将内部接口分配到内部区域，而将外部接口分配到外部区域。例如，可以配置访问控制策略，允许流量从内部传到外部，但不允许从外部传入内部。

每个区域都有一个与接口模式直接相关的模式。您可以仅向同一模式安全区添加接口。

对于网桥组，可将成员接口添加到区域，但不能添加桥接虚拟接口 (BVI)。

不要将管理/诊断接口包括在区域中。区域只适用于数据接口。

可在**对象 (Objects)** 页面创建安全区。

IPv6 寻址

您可以为 IPv6 配置两种类型的单播地址：

- 全局 - 全局地址是可在公用网络上使用的公用地址。对于网桥组，需要在桥接虚拟接口 (BVI) 上而非每个成员接口上配置全局地址。不能将以下任何地址指定为全局地址。
 - 内部保留的 IPv6 地址：fd00:: - 未指定的地址，例如 ::/128
 - 环回地址 ::1/128
 - 组播地址 ff00:: - 链路本地地址 fe80::
- 链路本地 - 链路本地地址是只能在直连网络上使用的专用地址。路由器不使用链路本地地址转发数据包；它们仅用于在特定物理网段上通信。链路本地地址可用于地址配置或网络发现功能，例如地址解析和邻居发现。在网桥组中，对 BVI 启用 IPv6 将为每个网桥组成员接口自动配置链路本地地址。每个接口必须有自己的地址，因为链路本地地址仅在网段中可用，并且会与接口 MAC 地址绑定。

至少需要配置链路本地地址，IPv6 才会起作用。如果配置全局地址，则接口上会自动配置链路本地地址，因此无需另外专门配置链路本地地址。如果不配置全局地址，则需要自动或手动配置链路本地地址。

Auto-MDI/MDIX 功能

对于 RJ-45 接口，默认的自动协商设置还包括 Auto-MDI/MDIX 功能。Auto-MDI/MDIX 在自动协商阶段检测直通电缆时执行内部交叉，从而消除交叉布线的需要。如要启用接口的 Auto-MDI/MDIX，必须将速度或双工设置为自动协商。如果将速度和双工明确设置为固定值，从而禁用了两种设置的自动协商，则 Auto-MDI/MDIX 也将被禁用。对于千兆以太网，当速度和双工被设置为 1000 和全双工时，接口始终会自动协商；因此，Auto-MDI/MDIX 始终会启用，且您无法禁用它。

接口的准则和限制

以下主题介绍接口的局限性。

接口配置的限制条件

使用设备管理器配置设备时，接口配置存在许多局限性。如果您需要以下任意功能，则必须使用管理中心来配置设备。

- 仅支持路由防火墙模式。无法配置透明防火墙模式的接口。
- 可以配置被动接口，但不能配置 ERSPAN 接口。
- 不能将接口配置为内联（在内联集内）或内联分路，用于仅 IPS 的处理。仅 IPS 模式的接口将绕过许多防火墙检查，仅支持 IPS 安全策略。相比之下，防火墙模式接口需要对流量执行防火

墙功能，例如维持流量、跟踪 IP 和 TCP 层的流量状态、IP 分片重组和 TCP 规范化。另外，您还可以根据安全策略，选择配置该防火墙模式接口的 IPS 功能。

- 无法配置冗余接口。
- 您可以在设备管理器中为以下型号配置 EtherChannel：Firepower 1000、Firepower 2100、Secure Firewall 3100、ISA 3000。Firepower 4100/9300 支持 EtherChannel，但必须在机箱上的 FXOS 中执行 EtherChannel 的所有硬件配置。Firepower 4100/9300 EtherChannel 显示在单个物理接口旁的设备管理器 **接口 (Interfaces)** 页面中。
- 仅可添加一个网桥组。
- 威胁防御 仅支持路由接口上的 IPv4 PPPoE。高可用性设备不支持 PPPoE。

各设备型号的最大 VLAN 子接口数量

设备型号限制可配置的最大 VLAN 子接口数量。请注意，仅可在数据接口上而不可在管理接口上配置子接口。

下表介绍各设备型号的限制。

| 型号 | 最大 VLAN 子接口数量 |
|------------------------|---------------|
| Firepower 1010 | 60 |
| Firepower 1120 | 512 |
| Firepower 1140 和 1150 | 1024 |
| Firepower 2100 | 1024 |
| Secure Firewall 3100 | 1024 |
| Firepower 4100 | 1024 |
| Firepower 9300 | 1024 |
| Threat Defense Virtual | 50 |
| ISA 3000 | 100 |

配置物理接口

要启用物理接口，至少必须启用它。通常，您还需要为它命名并配置 IP 寻址。如果要创建 VLAN 子接口，或者配置被动模式接口，或者要将接口添加到网桥组，无需配置 IP 寻址。Firepower 4100/9300 EtherChannel 显示在单个物理接口旁的设备管理器 **接口 (Interfaces)** 页面中，此过程也适用于 EtherChannel。必须在机箱上的 FXOS 中执行 Firepower 4100/9300 EtherChannels 的所有硬件配置。



注释 要将物理接口配置为 Firepower 1010 交换机端口，请参阅[配置 VLAN 接口和交换机端口 \(Firepower 1010\)](#)，第 23 页。

要将物理接口配置为被动接口，请参阅[将物理接口配置为被动模式](#)，第 41 页。

您可以禁用接口，以临时阻止在相连网络中的传输。无需删除该接口的配置。

过程

步骤 1 点击**设备**，然后点击**接口摘要**中的链接。

系统默认选择**接口 (Interfaces)** 页面。接口列表显示可用物理接口、物理接口名称、地址和状态。

步骤 2 点击要编辑的物理接口的编辑图标 (🔗)。

不能编辑在高可用性配置中用作故障转移或状态故障转移链路的接口。

步骤 3 进行以下设置：

Ethernet1/2
Edit Physical Interface

Interface Name: Mode: Status:

Most features work with named interfaces only, although some require unnamed interfaces.

Description:

IPv4 Address | IPv6 Address | Advanced

Type:

IP Address and Subnet Mask: /
e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask: /
e.g. 192.168.5.16

a) 设置接口名称。

设置接口名称，最多 48 个字符。字母字符必须为小写。例如 **inside** 或 **outside**。如果没有名称，将忽略其余的接口配置。除非配置子接口，否则接口应有名称。**注意：**请勿配置要添加至 EtherChannel 的接口的名称。

注释 如果更改名称，更改将自动反映到使用旧名称的所有位置，包括安全区、系统日志服务器对象和 DHCP 服务器定义。但无法删除名称，除非首先删除使用该名称的所有配置，这是因为对于任何策略或设置通常无法使用未命名的接口。


b) 选择模式。

- **路由** - 路由模式接口需要对流量执行所有防火墙功能，例如维持流量、跟踪 IP 和 TCP 层的流量状态、IP 分片重组、TCP 规范化以及防火墙策略。这是正常接口模式。
- **被动** - 被动接口使用交换机 SPAN 或镜像端口监控网络中流经的流量。SPAN 或镜像端口允许从交换机的其他端口复制流量。此功能可以提供网络内的系统可视性，而不会影响网络流量。如果在被动部署中配置系统，系统将不能执行某些操作，例如，阻止流量或流量整形。被动接口无条件接收所有流量，这些接口不会重传接收到的流量。如果您选择此模式，无需

执行此过程的其余部分。请参阅[将物理接口配置为被动模式](#)，第 41 页。请注意，无法在被动接口上配置 IP 地址。

- **交换机端口 - (Firepower 1010)** 交换机端口允许在同一 VLAN 上的端口之间进行硬件切换。交换流量不受安全策略的约束。如果您选择此模式，无需执行此过程的其余部分。相反，请参阅[配置 VLAN 接口和交换机端口 \(Firepower 1010\)](#)，第 23 页

如果稍后将此接口添加至网桥组，则模式将自动更改为 **BridgeGroupMember**。请注意，无法在网桥组成员接口上配置 IP 地址。

- c) 将状态滑块设置为已启用设置 ()。

对于 Firepower 4100/9300 设备上的接口，还必须启用 FXOS 中的接口。

如果要为此物理接口配置子接口，则可能已完成。点击[保存并继续配置 VLAN 子接口和 802.1Q 中继](#)，第 34 页。否则，请继续。

注释 即使在配置子接口时，为接口命名和提供 IP 地址也有效。这不是常规设置，但如果确定符合您的需求，则可以进行配置。

- d) (可选) 设置说明。

一行说明最多可包含 200 个字符（不包括回车符）。

步骤 4 点击 **IPv4 地址** 选项卡，并配置 IPv4 地址。

从**类型**字段中选择以下任一选项：

- **DHCP** - 如果应从网络中的 DHCP 服务器获取地址，请选择此选项。如果您配置高可用性，将不能使用此选项。如有需要，更改以下选项：
 - **路由指标** - 如果从 DHCP 服务器获取默认路由，则此选项是指与获知路由的管理距离，其值介于 1 到 255 之间。默认值为 1。
 - **获取默认路由** - 是否从 DHCP 服务器获取默认路由。您通常会选择此选项，该选项是默认值。
- **静态** - 如果希望分配固定的地址，请选择此选项。对于连接到接口的网络，键入接口的 IP 地址和子网掩码。例如，如果您连接的是 10.100.10.0/24 网络，则可以输入 10.100.10.1/24。确保该地址尚未在网络中使用。

如果您配置了高可用性，并要监控此接口的高可用性，则还要在同一子网上配置一个备用 IP 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

注释 如果为接口配置了 DHCP 服务器，您会看到该配置。您可以编辑或删除 DHCP 地址池。如果将接口 IP 地址更改为不同的子网，必须先删除 DHCP 服务器或在新子网上配置地址池，才能保存接口更改。请参阅[配置 DHCP 服务器](#)。

- **PPPoE** - 如果应使用基于以太网的点对点协议 (PPPoE) 获取地址, 请选择此选项。如果接口连接到 DSL、电缆调制解调器或 ISP 的其他连接, 并且 ISP 使用 PPPoE 来提供 IP 地址, 则可能需要使用 PPPoE。如果您配置高可用性, 将不能使用此选项。设置以下值:

- **组名称** - 指定您选择用于表示此连接的组名称。
- **PPPoE 用户名** - 指定 ISP 提供的用户名。
- **PPPoE 密码** - 指定 ISP 提供的密码。
- **PPP 身份验证** - 选择 **PAP**、**CHAP** 或 **MSCHAP**。

PAP 在身份验证过程中传递明文用户名和密码, 这样并不安全。使用 CHAP 时, 客户端可返回加密的 [challenge plus password] 和明文用户名来响应服务器质询。CHAP 比 PAP 更安全, 但其不会加密数据。MSCHAP 与 CHAP 类似但更安全, 因为服务器只对加密密码进行存储和比较, 而不是像 CHAP 一样存储和比较明文密码。MSCHAP 还可生成密钥, 以便 MPPE 进行数据加密。

- **PPPoE 获知的路由指标** - 向获悉的路由分配管理距离。有效值为从 1 到 255。默认情况下, 获悉的路由的默认管理距离为 1。
- **从 PPPoE 获取默认路由** - 选中此复选框可支持从 PPPoE 服务器获取默认路由。
- **IP 地址类型** - 选择动态可从 PPPoE 服务器获取 IP 地址。如果从 ISP 分配了静态 IP 地址, 也可以选择静态。

步骤 5 (可选。) 点击 **IPv6 地址** 选项卡, 并配置 IPv6 地址。

- **状态** - 在不想配置全局地址时, 要启用 IPv6 处理并自动配置本地链路地址, 请选择 **已启用**。本地链路地址基于接口的 MAC 地址 (修改的 EUI-64 格式) 生成。

注释 禁用 IPv6 不会禁用接口上使用显式 IPv6 地址配置或启用自动配置的 IPv6 处理。

- **地址自动配置** - 选择此选项可自动配置地址。只有设备所在链路中的路由器配置为提供 IPv6 服务 (包括通告 IPv6 全局前缀以用于该链路), IPv6 无状态自动配置才会生成全局 IPv6 地址。如果该链路中的 IPv6 路由服务不可用, 则只能获得本地链路 IPv6 地址, 无法访问设备直接的网络链路之外的服务。本地链路地址以修改的 EUI-64 接口 ID 为基础。

虽然 RFC 4862 规定为无状态自动配置所配置的主机不发送路由器通告消息, 但威胁防御设备在这种情况下确实会发送路由器通告消息。选择 **抑制 RA** 可抑制消息, 遵从 RFC 要求。

- **静态地址/前缀** - 如果不使用无状态自动配置, 请输入完整的静态全局 IPv6 地址和网络前缀。例如, 2001:0DB8::BA98:0:3210/48。有关 IPv6 寻址的详细信息, 请参阅 [IPv6 寻址, 第 3 页](#)。

如果仅使用本地链路地址, 请选择 **本地链路** 选项。本地链路地址在本地网络之外无法访问。在网桥组接口上无法配置本地链路地址。

注释 链路本地地址应以 FE8、FE9、FEA 或 FEB 开头, 例如 fe80::20d:88ff:feec:6a82。请注意, 我们建议根据修改的 EUI-64 格式自动分配链路本地地址。例如, 如果其他设备强制使用修改的 EUI-64 格式, 则手动分配的链路本地地址可能导致丢弃数据包。

- **备用 IP 地址** - 如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IPv6 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。
- **抑制 RA** - 是否抑制路由器通告。威胁防御可以参与路由器通告，以便邻居设备可以动态获悉默认路由器地址。默认情况下，每个配置 IPv6 的接口定期发送路由器通告消息（ICMPv6 类型 134）。

也会发送路由器通告，以响应路由器请求消息（ICMPv6 类型 133）。路由器请求消息由主机在系统启动时发送，以便主机可以立即自动配置，而无需等待下一条预定路由器通告消息。

对于不希望威胁防御设备提供 IPv6 前缀的任何接口（例如外部接口），您可能希望抑制接口上的这些消息。

步骤 6（可选。）[配置高级选项，第 44 页。](#)

高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。

步骤 7 点击确定 (OK)。

下一步做什么

- 将接口添加至相应的安全区。请参阅[配置安全区](#)。
- 向您的动态 DNS 服务提供商注册一个完全限定域名 (FQDN)，并配置 DDNS 以更新 DNS 服务器上的接口地址（IPv4 和 IPv6）。请参阅[配置动态 DNS](#)。

配置网桥组

网桥组是将一个或多个接口分组的虚拟接口。对接口分组的主要原因是创建一组交换接口。如此，就可以将工作站或其他终端设备直接连接到网桥组中所包含的接口。您不需要通过单独的物理交换机来连接这些设备，尽管您也可以将一台交换机连接到某个网桥组成员。

组成员没有 IP 地址。相反，所有成员接口共用桥接虚拟接口 (BVI) 的 IP 地址。如果在 BVI 上启用 IPv6，系统会自动为成员接口分配唯一的链路本地地址。

单独启用和禁用成员接口。这样就可以禁用任何未使用的接口，而无需将其从网桥组删除。网桥组本身始终处于启用状态。

通常会在网桥组接口 (BVI) 上配置 DHCP 服务器，为通过成员接口连接的任何终端提供 IP 地址。不过，如果愿意的话，您也可以在连接到成员接口的终端上配置静态地址。网桥组中的所有终端都必须具有与网桥组 IP 地址位于同一子网的 IP 地址。

准则和限制

- 可以添加一个网桥组。
- 不支持将设备管理器定义的 EtherChannel 作为网桥组成员。Firepower 4100/9300 上的 Etherchannel 可以是网桥组成员。

- 在 Firepower 2100 系列或 threat defense virtual 设备上不能配置网桥组。
- 对于 Firepower 1010，不能将逻辑 VLAN 接口和物理防火墙接口混合在同一个网桥组中。
- ISA 3000 预配置网桥组 BVI1 (未命名，这意味着其不参与路由)。BVI1 包括所有数据接口：GigabitEthernet1/1 (outside1)、GigabitEthernet1/2 (inside1)、GigabitEthernet1/3 (outside2) 和 GigabitEthernet1/4 (inside2)。必须设置 BVI1 IP 地址以匹配您的网络。

开始之前

指定将成为网桥组成员的接口。具体而言，每个成员接口都必须满足以下要求：

- 该接口必须具有名称。
- 该接口不能有任何已定义的 IPv4 或 IPv6 地址，无论是静态分配的还是通过 DHCP 获得的。如果要从当前正在使用的某个接口删除地址，则可能还需要删除该接口的其他配置，例如静态路由、DHCP 服务器或 NAT 规则，具体视具有地址的接口而定。
- 必须将该接口从所属安全区中删除（如果它在某个区域中），并删除该接口的所有 NAT 规则，然后才能将其添加到网桥组。

过程

步骤 1 点击设备 (Device)，然后点击接口 (Interfaces) 摘要中的链接，再点击网桥组 (Bridge Groups)。

网桥组列表显示现有网桥组。点击开/关箭头可查看各网桥组的成员接口。成员接口也会单独显示于接口 (Routing) 或 VLAN 页面上。

步骤 2 执行以下操作之一：

- 点击 BVI1 网桥组的编辑图标 (🔗)。
- 点击创建网桥组 (Create Bridge Group) 或加号图标 (+) 创建新组。

注释 网桥组只能有一个。如果已经定义了一个网桥组，则应编辑该组而非尝试创建新组。如果需要创建新的网桥组，则必须先删除现有网桥组。

- 如果不再需要某个网桥组，点击该网桥组的删除图标 (🗑️)。删除网桥组时，其成员将变成标准路由接口，并且所有 NAT 规则或安全区成员身份保持不变。可以编辑这些接口为其提供 IP 地址。如果要将其添加到新的网桥组，需要先删除 NAT 规则并将接口从所属安全区中删除。

步骤 3 进行以下配置：

a) (可选) 设置接口名称。

设置网桥组的名称，最多 48 个字符。字母字符必须为小写。例如 **inside** 或 **outside**。如果希望此 BVI 参与其与其他命名接口之间的路由，请设置名称。

注释 如果更改名称，更改将自动反映到使用旧名称的所有位置，包括安全区、系统日志服务器对象和 DHCP 服务器定义。但无法删除名称，除非首先删除使用该名称的所有配置，这是因为对于任何策略或设置通常无法使用未命名的接口。

b) (可选) 设置说明。

一行说明最多可包含 200 个字符（不包括回车符）。

c) 编辑网桥组成员列表。

最多可向一个网桥组添加 64 个接口或子接口。

- 添加接口 - 点击加号图标 (+)，点击一个或多个接口，然后点击确定。
- 移除接口 - 将鼠标悬停于接口上方，然后点击右侧的 x。

步骤 4 点击 **IPv4 地址** 选项卡，并配置 IPv4 地址。

从**类型**字段中选择以下任一选项：

- **静态** - 如果希望分配固定的地址，请选择此选项。键入网桥组的 IP 地址和子网掩码。所有连接的终端都将位于此网络中。确保该地址尚未在网络中使用。

如果您配置了高可用性，并要监控此接口的高可用性，则还要在同一子网上配置一个备用 IP 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

注释 如果为接口配置了 DHCP 服务器，您会看到该配置。您可以编辑或删除 DHCP 地址池。如果将接口 IP 地址更改为不同的子网，必须先删除 DHCP 服务器或在新子网上配置地址池，才能保存接口更改。请参阅[配置 DHCP 服务器](#)。

- **动态 (DHCP)** - 如果应从网络中的 DHCP 服务器获取地址，请选择此选项。网桥组通常不会使用此选项，但是您可以根据需要如此配置。如果您配置高可用性，将不能使用此选项。如有需要，更改以下选项：
 - **路由指标** - 如果从 DHCP 服务器获取默认路由，则此选项是指与获知路由的管理距离，其值介于 1 到 255 之间。默认值为 1。
 - **获取默认路由** - 是否从 DHCP 服务器获取默认路由。您通常会选择此选项，该选项是默认值。

步骤 5 (可选。) 点击 **IPv6 地址** 选项卡，并配置 IPv6 地址。

- **状态** - 在不想配置全局地址时，要启用 IPv6 处理并自动配置本地链路地址，请选择 **已启用**。本地链路地址基于接口的 MAC 地址（修改的 EUI-64 格式）生成。

注释 禁用 IPv6 不会禁用接口上使用显式 IPv6 地址配置或启用自动配置的 IPv6 处理。

- **静态地址/前缀** - 如果不使用无状态自动配置，请输入完整的静态全局 IPv6 地址和网络前缀。例如，2001:0DB8::BA98:0:3210/48。有关 IPv6 寻址的详细信息，请参阅[IPv6 寻址](#)，第 3 页。

如果仅使用本地链路地址，请选择 **本地链路** 选项。本地链路地址在本地网络之外无法访问。在网桥组接口上无法配置本地链路地址。

注释 链路本地地址应以 FE8、FE9、FEA 或 FEB 开头，例如 fe80::20d:88ff:feec:6a82。请注意，我们建议根据修改的 EUI-64 格式自动分配链路本地地址。例如，如果其他设备强制使用修改的 EUI-64 格式，则手动分配的链路本地地址可能导致丢弃数据包。

- **备用 IP 地址** - 如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IPv6 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。
- **抑制 RA** - 是否抑制路由器通告。威胁防御设备可以参与路由器通告，以便邻居设备可以动态获悉默认路由器地址。默认情况下，每个配置 IPv6 的接口定期发送路由器通告消息（ICMPv6 类型 134）。

也会发送路由器通告，以响应路由器请求消息（ICMPv6 类型 133）。路由器请求消息由主机在系统启动时发送，以便主机可以立即自动配置，而无需等待下一条预定路由器通告消息。

对于不希望威胁防御设备提供 IPv6 前缀的任何接口（例如外部接口），您可能希望抑制接口上的这些消息。

步骤 6 (可选。) [配置高级选项](#)，第 44 页。

请对网桥组成员接口配置大多数高级选项，不过其中一些选项可用于网桥组接口。
高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。

步骤 7 点击确定。

下一步做什么

- 确保已启用您打算使用的所有成员接口。
- 为网桥组配置 DHCP 服务器。请参阅[配置 DHCP 服务器](#)。
- 将成员接口添加到相应的安全区。请参阅[配置安全区](#)。
- 确保各项策略（例如身份、NAT 和访问策略）可为网桥组和成员接口提供所需的服务。

配置 EtherChannel

本节介绍 EtherChannel 及其配置方式。



注释 您可以将设备管理器中的 EtherChannel 添加到以下型号：

- Firepower 1000
- Firepower 2100
- Secure Firewall 3100
- ISA 3000

Firepower 4100/9300 支持 EtherChannel，但必须在机箱上的 FXOS 中执行 EtherChannel 的所有硬件配置。Firepower 4100/9300 EtherChannel 显示在单个物理接口旁的设备管理器接口页面中。您也无法在其他型号（例如 threat defense virtual）的设备管理器中配置 EtherChannel。

关于 EtherChannel

802.3ad EtherChannel 是逻辑接口（称为端口通道接口），该接口由一组单独的以太网链路（通道组）组成，以便可以提高单个网络的带宽。配置接口相关功能时，可以像使用物理接口一样来使用端口通道接口。

最多可以配置 48 个 Etherchannel，具体取决于型号支持的接口数量。

通道组接口

每个通道组最多可以有 8 个主用接口。

通道组中的所有接口都必须属于同一类型且具有相同速度。添加到通道组的第一个接口确定正确的类型和速度。

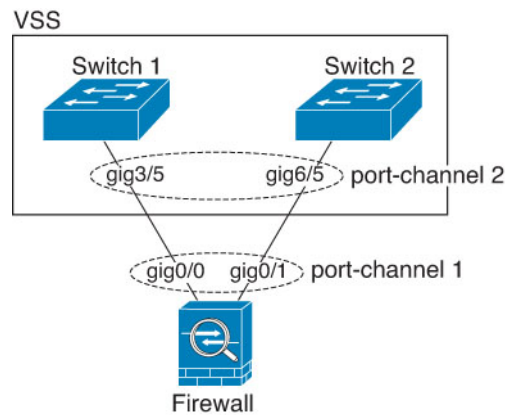
EtherChannel 汇聚通道中所有可用活动接口上的流量。系统根据源或目标 MAC 地址、IP 地址、TCP 端口号、UDP 端口号和 VLAN 编号使用专有散列算法来选择接口。

连接到其他设备上的 EtherChannel

威胁防御 EtherChannel 连接到的设备还必须支持 802.3ad EtherChannel；例如，可以连接到 Catalyst 6500 交换机或 Cisco Nexus 7000。

如果交换机属于虚拟交换系统 (VSS) 或虚拟端口通道 (vPC) 的一部分，则可以将同一 EtherChannel 内的威胁防御接口连接到 VSS/vPC 中的单独交换机。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。

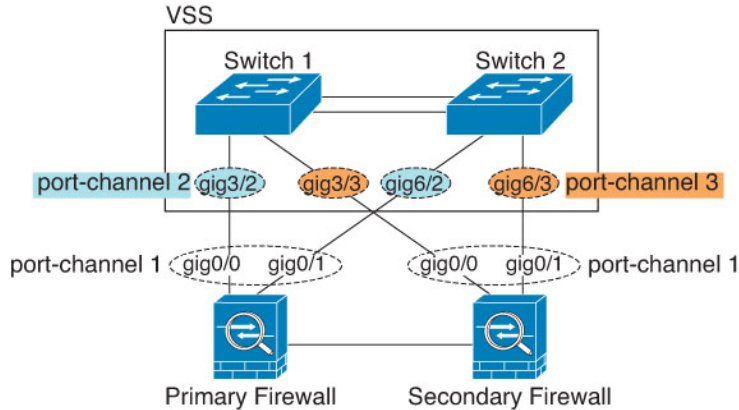
图 1: 连接至 VSS/vPC



注释 如果威胁防御设备处于透明防火墙模式下，并且将威胁防御设备置于两组 VSS/vPC 交换机之间，请确保在使用 EtherChannel 连接到威胁防御设备的所有交换机端口上禁用单向链路检测 (UDLD)。如果启用 UDLD，则交换机端口可能会接收来自另一个 VSS/vPC 对中的两台交换机的 UDLD 数据包。接收交换机会将接收接口置于关闭状态，原因是“UDLD 邻居不匹配”。

如果您在主用/备用故障转移部署中使用威胁防御设备，则需要 VSS/vPC 中的交换机上创建单独的 EtherChannel，为每个威胁防御设备创建一个。在每个威胁防御设备上，单个 EtherChannel 连接至两台交换机。即使您可以将所有的交换机接口分组到连接两个威胁防御设备的一个 EtherChannel 中（在这种情况下，将不会建立 EtherChannel，因为威胁防御系统 ID 是单独的），但单个 EtherChannel 并不可取，因为您不希望将流量发送到备用威胁防御设备。

图 2: 主用/备用故障转移和 VSS/vPC



链路聚合控制协议

链路汇聚控制协议 (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。

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。

负载均衡

威胁防御设备通过对数据包的源 IP 地址和目标 IP 地址进行散列处理来将数据包分发给 EtherChannel 中的接口（此条件可配置）。在模数运算中，将得到的散列值除以主用链路数，得到的余数确定哪个接口拥有流量。 $hash_value \bmod active_links$ 结果为 0 的所有数据包都发往 EtherChannel 中的第一个接口，结果为 1 的发往第二个接口，结果为 2 的数据包发往第三个接口，依此类推。例如，如果您有 15 个主用链路，则模数运算的值为 0 到 14。如果有 6 个主用链路，则值为 0 到 5，依此类推。

如果主用接口发生故障且未由备用接口替代，则流量会在剩余的链路之间重新均衡。该故障会在第 2 层的生成树和第 3 层的路由表中被屏蔽，因此故障切换对其他网络设备是透明的。

EtherChannel MAC 地址

属于通道组一部分的所有接口都共享同一 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。

Firepower 和 Cisco Secure Firewall 硬件

端口通道接口使用内部接口 Internal-Data 0/1 的 MAC 地址。或者，您可以为端口通道接口手动配置 MAC 地址。机箱上的所有 EtherChannel 接口都使用相同的 MAC 地址，因此请注意，例如，如果使用 SNMP 轮询，则多个接口将具有相同的 MAC 地址。



注释 成员接口仅在重新启动后使用内部数据 0/1 MAC 地址。在重新启动之前，成员接口使用自己的 MAC 地址。如果在重新启动后添加新的成员接口，则必须再次重新启动以更新其 MAC 地址。

EtherChannel 的准则

桥接组

设备管理器-定义的 EtherChannel 接口作为桥接组成员。Firepower 4100/9300 上的 Etherchannel 可以是网桥组成员。

高可用性

- 如果要将 EtherChannel 接口用作高可用性链路，则必须在高可用性对中的两台设备上预配置要使用的接口；不能在主设备上配置该接口并期望它会复制到辅助设备，因为复制需要高可用性链路本身。
- 如果要将 EtherChannel 接口用于状态链路，则无需特殊配置；可以照常从主设备复制配置。Firepower 4100/9300 机箱的所有接口（包括 EtherChannel）均需在两台设备上预配置。
- 可以使用 **monitor-interface** 命令监控 EtherChannel 余接口以实现高可用性。如果主用成员接口故障切换到备用接口，则此活动不会在监控设备级高可用性时导致 EtherChannel 接口出现故障。仅在所有物理接口都出现故障的情况下，EtherChannel 接口或 EtherChannel 接口才会出现故障。
- 如果将 EtherChannel 接口用于高可用性或状态链路，然后防止无序数据包，则仅会使用 EtherChannel 中的一个接口。如果该接口发生故障，则会使用 EtherChannel 中的下一个接口。您不能在 EtherChannel 配置用作高可用性链路时对其进行修改。要修改配置，您需要暂时禁用高可用性，以防止在此期间发生高可用性。

型号支持

- 您可以将设备管理器中的 EtherChannel 添加到以下型号：
 - Firepower 1000
 - Firepower 2100
 - Cisco Secure Firewall 3100
 - ISA 3000

Firepower 4100/9300 支持 EtherChannel，但必须在机箱上的 FXOS 中执行 EtherChannel 的所有硬件配置。Firepower 4100/9300 EtherChannel 显示在单个物理接口旁的设备管理器接口页面中。您也无法在其他型号（例如 ASA 5500-X 系列）的设备管理器中配置 EtherChannel。

- 无法在 Etherchannel 中使用 Firepower 1010 交换机端口或 VLAN 接口。

《通用 EtherChannel 准则》

- 最多可以配置 48 个 Etherchannel，具体取决于型号可用的接口数量。
- 每个通道组最多可以有 8 个主用接口。
- 通道组中的所有接口都必须具有相同的介质类型和速度能力。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。不能通过在较大容量的接口上将速度设置为较低来混合接口容量（例如 1GB 和 10GB 接口），但 Cisco Secure Firewall 3100 除外，它支持不同的接口容量，只要速度设置为检测 SFP；在此情况下会使用较低的常见速度。
- 威胁防御 EtherChannel 连接到的设备还必须支持 802.3ad EtherChannel。
- 威胁防御设备不支持带有 VLAN 标记的 LACPDU。如果使用 Cisco IOS `vlan dot1Q tag native` 命令在相邻交换机上启用本地 VLAN 标记，则威胁防御设备将会丢弃已标记的 LACPDU。请务必禁用相邻交换机上的本地 VLAN 标记。
- 以下设备模块不支持 LACP 快速速率；LACP 始终使用正常速率。此设置不可配置。请注意，在 FXOS 中配置 EtherChannel 的 Firepower 4100/9300 默认将 LACP 速率设置为快速；在这些平台上，速率是可配置的。
 - Firepower 1000
 - Firepower 2100
 - Cisco Secure Firewall 3100
- 在低于 15.1(1)S2 的 Cisco IOS 软件版本中，威胁防御不支持将 EtherChannel 连接到交换机堆叠。在默认交换机设置下，如果跨堆叠连接威胁防御 EtherChannel，则当主要交换机关闭时，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` 命令设置为足够大的值，以将重载时间计算在内；例如，可将其设置为 8 分钟，或设置为 0 以表示无穷大。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。
- 所有威胁防御配置均引用 EtherChannel 接口，而不是成员物理接口。

添加 EtherChannel

添加 EtherChannel 并为其分配成员接口。



注释 您可以将设备管理器中的 EtherChannel 添加到以下型号：

- Firepower 1000
- Firepower 2100
- Secure Firewall 3100
- ISA 3000

Firepower 4100/9300 支持 EtherChannel，但必须在机箱上的 FXOS 中执行 EtherChannel 的所有硬件配置。Firepower 4100/9300 EtherChannel 显示在单个物理接口旁的设备管理器接口页面中。您也无法在其他型号（例如 ASA 5500-X 系列）的设备管理器中配置 EtherChannel。

开始之前

- 通道组中的所有接口都必须具有相同的介质类型和速度能力。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。不能通过在较大容量的接口上将速度设置为较低来混合接口容量（例如 1GB 和 10GB 接口），但 Cisco Secure Firewall 3100 除外，它支持不同的接口容量，只要速度设置为检测 SFP；在此情况下会使用较低的常见速度。
- 无法命名成员接口。



注意 如果使用的是配置中已有的接口，则删除名称将会清除引用该接口的任何配置。

过程

步骤 1 点击设备，然后点击接口摘要中的链接，再点击 **EtherChannel**。

Etherchannel 列表显示现有 Etherchannel、其名称、地址和状态。点击开/关箭头可查看各 EtherChannel 的成员接口。成员接口也会单独显示于接口 (**Interfaces**) 页面上。

步骤 2 点击创建 **EtherChannel**（如果无当前 EtherChannel）或加号图标 (+)，然后点击 **EtherChannel** 新建 EtherChannel。

步骤 3 进行以下配置：

a) 设置接口名称。


设置 EtherChannel 名称，最多 48 个字符。字母字符必须为小写。例如 **inside** 或 **outside**。

注释 如果更改名称，更改将自动反映到使用旧名称的所有位置，包括安全区、系统日志服务器对象和 DHCP 服务器定义。但无法删除名称，除非首先删除使用该名称的所有配置，这是因为对于任何策略或设置通常无法使用未命名的接口。

b) 设置模式。

- **路由** - 路由模式接口需要对流量执行所有防火墙功能，例如维持流量、跟踪 IP 和 TCP 层的流量状态、IP 分片重组、TCP 规范化以及防火墙策略。如果您希望流量通过接口，请使用此模式。这是正常接口模式。
- **被动** - 被动接口使用交换机 SPAN 或镜像端口监控网络中流经的流量。SPAN 或镜像端口允许从交换机的其他端口复制流量。此功能可以提供网络内的系统可视性，而不会影响网络流量。如果在被动部署中配置系统，系统将不能执行某些操作，例如，阻止流量或流量整形。

被动接口无条件接收所有流量，这些接口不会重传接收到的流量。如果您选择此模式，无需执行此过程的其余部分。请参阅[将物理接口配置为被动模式](#)，第 41 页。

- c) 设置 **EtherChannel ID** (1~48 之间) (1~8 用于 Firepower 1010)。
- d) 将状态滑块设置为已启用设置 ()。
- e) (可选) 设置说明。
一行说明最多可包含 200 个字符 (不包括回车符)。
- f) 选择 **EtherChannel 模式**。
 - **主用** - (推荐) 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。
- g) 添加 **EtherChannel 成员**。
最多可向 EtherChannel 添加 8 个 (未命名) 接口。
 - 添加接口 - 点击加号图标 (+)，点击一个或多个接口，然后点击确定。
 - 移除接口 - 将鼠标悬停于接口上方，然后点击右侧的 **x**。

步骤 4 点击 **IPv4 地址** 选项卡，并配置 IPv4 地址。

从类型字段中选择以下任一选项：

- **DHCP** - 如果应从网络中的 DHCP 服务器获取地址，请选择此选项。如果您配置高可用性，将不能使用此选项。如有需要，更改以下选项：
 - **路由指标** - 如果从 DHCP 服务器获取默认路由，则此选项是指与获知路由的管理距离，其值介于 1 到 255 之间。默认值为 1。
 - **获取默认路由** - 是否从 DHCP 服务器获取默认路由。您通常会选择此选项，该选项是默认值。
- **静态** - 如果希望分配固定的地址，请选择此选项。对于连接到接口的网络，键入接口的 IP 地址和子网掩码。例如，如果您连接的是 10.100.10.0/24 网络，则可以输入 10.100.10.1/24。确保该地址尚未在网络中使用。

如果您配置了高可用性，并要监控此接口的高可用性，则还要在同一子网上配置一个备用 IP 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

注释 如果为接口配置了 DHCP 服务器，您会看到该配置。您可以编辑或删除 DHCP 地址池。如果将接口 IP 地址更改为不同的子网，必须先删除 DHCP 服务器或在新子网上配置地址池，才能保存接口更改。请参阅[配置 DHCP 服务器](#)。

- **PPPoE** - 如果应使用基于以太网的点对点协议 (PPPoE) 获取地址，请选择此选项。如果接口连接到 DSL、电缆调制解调器或 ISP 的其他连接，并且 ISP 使用 PPPoE 来提供 IP 地址，则可能需要使用 PPPoE。如果您配置高可用性，将不能使用此选项。设置以下值：

- **组名称** - 指定您选择用于表示此连接的组名称。
- **PPPoE 用户名** - 指定 ISP 提供的用户名。
- **PPPoE 密码** - 指定 ISP 提供的密码。
- **PPP 身份验证** - 选择 **PAP**、**CHAP** 或 **MSCHAP**。

PAP 在身份验证过程中传递明文用户名和密码，这样并不安全。使用 CHAP 时，客户端可返回加密的 [challenge plus password] 和明文用户名来响应服务器质询。CHAP 比 PAP 更安全，但其不会加密数据。MSCHAP 与 CHAP 类似但更安全，因为服务器只对加密密码进行存储和比较，而不是像 CHAP 一样存储和比较明文密码。MSCHAP 还可生成密钥，以便 MPPE 进行数据加密。

- **PPPoE 获知的路由指标** - 向获悉的路由分配管理距离。有效值为从 1 到 255。默认情况下，获悉的路由的默认管理距离为 1。
- **从 PPPoE 获取默认路由** - 选中此复选框可支持从 PPPoE 服务器获取默认路由。
- **IP 地址类型** - 选择动态可从 PPPoE 服务器获取 IP 地址。如果从 ISP 分配了静态 IP 地址，也可以选择静态。

步骤 5 (可选。) 点击 **IPv6 地址** 选项卡，并配置 IPv6 地址。

- **状态** - 在不想配置全局地址时，要启用 IPv6 处理并自动配置本地链路地址，请选择已启用。本地链路地址基于接口的 MAC 地址（修改的 EUI-64 格式）生成。

注释 禁用 IPv6 不会禁用接口上使用显式 IPv6 地址配置或启用自动配置的 IPv6 处理。

- **地址自动配置** - 选择此选项可自动配置地址。只有设备所在链路中的路由器配置为提供 IPv6 服务（包括通告 IPv6 全局前缀以用于该链路），IPv6 无状态自动配置才会生成全局 IPv6 地址。如果该链路中的 IPv6 路由服务不可用，则只能获得本地链路 IPv6 地址，无法访问设备直接的网络链路之外的服务。本地链路地址以修改的 EUI-64 接口 ID 为基础。

虽然 RFC 4862 规定为无状态自动配置所配置的主机不发送路由器通告消息，但威胁防御设备在这种情况下确实会发送路由器通告消息。选择抑制 **RA** 可抑制消息，遵从 RFC 要求。

- **静态地址/前缀** - 如果不使用无状态自动配置，请输入完整的静态全局 IPv6 地址和网络前缀。例如，2001:0DB8::BA98:0:3210/48。有关 IPv6 寻址的详细信息，请参阅 [IPv6 寻址](#)，第 3 页。

如果仅使用本地链路地址，请选择**本地链路**选项。本地链路地址在本地网络之外无法访问。在网桥组接口上无法配置本地链路地址。

注释 链路本地地址应以 FE8、FE9、FEA 或 FEB 开头，例如 fe80::20d:88ff:feec:6a82。请注意，我们建议根据修改的 EUI-64 格式自动分配链路本地地址。例如，如果其他设备强制使用修改的 EUI-64 格式，则手动分配的链路本地地址可能导致丢弃数据包。

- **备用 IP 地址** - 如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IPv6 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

- **抑制 RA** - 是否抑制路由器通告。威胁防御可以参与路由器通告，以便邻居设备可以动态获悉默认路由器地址。默认情况下，每个配置 IPv6 的接口定期发送路由器通告消息（ICMPv6 类型 134）。

也会发送路由器通告，以响应路由器请求消息（ICMPv6 类型 133）。路由器请求消息由主机在系统启动时发送，以便主机可以立即自动配置，而无需等待下一条预定路由器通告消息。

对于不希望威胁防御设备提供 IPv6 前缀的任何接口（例如外部接口），您可能希望抑制接口上的这些消息。

步骤 6 通过点击 **高级** 并设置速度来设置成员接口的速度。

您还可以配置其他高级选项。请参阅 [配置高级选项](#)，第 44 页。

步骤 7 点击 **确定 (OK)**。

下一步做什么

- 将 Etherchannel 添加至相应的安全区。请参阅 [配置安全区](#)。

配置 VLAN 接口和交换机端口 (Firepower 1010)

可以将各 Firepower 1010 接口配置为作为常规防火墙接口或第 2 层硬件交换机端口运行。本节包括用于启动交换机端口配置的任务，包括启用或禁用交换模式以及创建 VLAN 接口和将交换机端口分配给 VLAN。本节还介绍如何在受支持接口上自定义以太网供电 (PoE)。

了解 Firepower 1010 端口和接口

端口和接口

对于各物理 Firepower 1010 接口，可以将其操作设置为防火墙接口或交换机端口。请参阅以下有关物理接口和端口类型的信息，以及为其分配交换机端口的逻辑 VLAN 接口：

- **物理防火墙接口** - 在路由模式下，这些接口使用已配置的安全策略在第 3 层网络之间转发流量，以应用防火墙和 VPN 服务。在路由模式下，还可以将集成路由和桥接与某些接口一起用作桥接组成员，将其他接口用作第 3 层接口。默认情况下，以太网 1/1 接口配置为防火墙接口。还可以将这些接口配置为仅限 IPS（被动接口）。
- **物理交换机端口** - 交换机端口使用硬件中的交换功能在第 2 层转发流量。同一 VLAN 上的交换机端口可使用硬件交换互相通信，且流量不受威胁防御安全策略的限制。接入端口仅接受未标记流量，可以将其分配给单个 VLAN。中继端口接受未标记和已标记流量，且可以属于多个

VLAN。默认情况下，以太网 1/2 至 1/8 配置为 VLAN 1 上的接入交换机端口。不能将管理接口配置为交换机端口。

- 逻辑 VLAN 接口 - 这些接口的运行方式与物理防火墙接口相同，但不同的是，无法创建子接口仅 IPS 接口（内联集和被动接口）或 EtherChannel 接口。如果交换机端口需要与另一个网络进行通信，则威胁防御设备将安全策略应用至 VLAN 接口，并路由至另一个逻辑 VLAN 接口或防火墙接口。甚至可以将集成路由和桥接与 VLAN 接口一起用作桥接组成员。同一 VLAN 上的交换机端口之间的流量不受安全策略威胁防御的限制，但桥接组中 VLAN 之间的流量会受到安全策略的限制，因此，可以选择将桥接组和交换机端口进行分层，以在某些分段之间实施安全策略。

以太网供电

以太网 1/7 和以太网 1/8 支持以太网供电+ (PoE+)。

Firepower 1010 交换机端口准则和限制

高可用性

- 使用高可用性时，不应使用交换机端口功能。由于交换机端口在硬件中运行，因此会继续在主用设备和备用设备上传输流量。高可用性旨在防止流量通过备用设备，但此功能不会扩展至交换机端口。在正常高可用性网络设置中，两台设备上的活动交换机端口将导致网络环路。建议将外部交换机用于任何交换功能。请注意，VLAN 接口可通过故障转移监控，而交换机端口无法通过故障转移监控。理论上，您可以将单个交换机端口置于 VLAN 上并成功使用高可用性，但更简单的设置是改用物理防火墙接口。
- 仅可使用防火墙接口作为故障转移链路。

逻辑 VLAN 接口

- 您可以创建多达 60 个 VLAN 接口。
- 如果还在防火墙接口上使用 VLAN 子接口，则无法使用与逻辑 VLAN 接口相同的 VLAN ID。
- MAC 地址：
 - - 所有 VLAN 接口共享一个 MAC 地址。确保所有连接的交换机均可支持此方案。如果连接的交换机需要唯一 MAC 地址，可手动分配 MAC 地址。请参阅[配置高级选项](#)，第 44 页。

网桥组

您不能将逻辑 VLAN 接口和物理防火墙接口混合在同一个网桥组中。

VLAN 接口和交换机端口不支持的功能

VLAN 接口和交换机端口不支持：

- 动态路由

- 组播路由
- 等价多路径路由 (ECMP)
- 被动接口
- EtherChannel
- 故障转移和状态链路

其他准则和限制

- 您最多可以在 Firepower 1010 上配置 60 个命名接口。
- 不能将 管理接口配置为交换机端口。

默认设置

- 以太网 1/1 是一个防火墙接口。
- 以太网 1/2 至以太网 1/8 是分配给 VLAN 1 的交换机端口。
- 默认速度和复用 - 默认情况下，速度和复用设置为自动协商。

配置 VLAN 接口

本节介绍如何配置 VLAN 接口以用于关联交换机端口。您必须先为要分配至交换机端口的各 VLAN 配置 VLAN 接口。



注释 如果只希望在特定 VLAN 上的交换机端口之间启用切换，且不希望 VLAN 和其他 VLAN 或防火墙接口之间进行路由，则将 VLAN 接口名称留空。在这种情况下，您无需配置 IP 地址；任何 IP 配置都将被忽略。

过程

步骤 1 点击**设备**，然后点击**接口摘要**中的链接，再点击**VLAN**。

VLAN 列表显示现有 VLAN 接口。点击打开/关闭箭头，查看与各 VLAN 关联的交换机端口。交换机端口也会单独出现在**接口 (Interfaces)**页面上。

步骤 2 点击**创建 VLAN 接口**（如果无当前 VLAN）或加号图标 (+) 以创建新的 VLAN 接口。

步骤 3 进行以下配置：

a) 设置接口名称。

设置 VLAN 名称，最多 48 个字符。字母字符必须为小写。例如 **inside** 或 **outside**。

如果不希望在 VLAN 和其他 VLAN 或防火墙接口之间进行路由，则将 VLAN 接口名称留空。

注释 如果更改名称，更改将自动反映到使用旧名称的所有位置，包括安全区、系统日志服务器对象和 DHCP 服务器定义。但无法删除名称，除非首先删除使用该名称的所有配置，这是因为对于任何策略或设置通常无法使用未命名的接口。

b) 将模式保持为路由。

如果稍后将此 VLAN 接口添加至网桥组，则模式将自动更改为 **BridgeGroupMember**。无法在网桥组成员接口上配置 IP 地址。

c) 将状态滑块设置为已启用设置 ()。

d) 设置介于 1 和 4070 之间的 **VLAN ID**。

保存接口后，无法更改 VLAN ID；VLAN ID 既是使用的 VLAN 标记，也是您的配置中的接口 ID。

- e) (可选) 在不转发至此 VLAN 字段中，输入此 VLAN 接口无法向其发起流量的 VLAN ID。

例如，您有一个 VLAN 分配给外部以供互联网访问，另一个 VLAN 分配给内部企业网络，第三个 VLAN 分配给您的家庭网络。家庭网络无需访问企业网络，因此，您可以使用此接口上的阻止流量来选择家庭 VLAN；企业网络可以访问家庭网络，但家庭网络不能访问企业网络。

- f) (可选) 设置说明。

一行说明最多可包含 200 个字符（不包括回车符）。

步骤 4 点击 IPv4 地址选项卡，并配置 IPv4 地址。

从类型字段中选择以下任一选项：

- **DHCP** - 如果应从网络中的 DHCP 服务器获取地址，请选择此选项。如果您配置高可用性，将不能使用此选项。如有需要，更改以下选项：
 - **路由指标** - 如果从 DHCP 服务器获取默认路由，则此选项是指与获知路由的管理距离，其值介于 1 到 255 之间。默认值为 1。
 - **获取默认路由** - 是否从 DHCP 服务器获取默认路由。您通常会选择此选项，该选项是默认值。
- **静态** - 如果希望分配固定的地址，请选择此选项。对于连接到接口的网络，键入接口的 IP 地址和子网掩码。例如，如果您连接的是 10.100.10.0/24 网络，则可以输入 10.100.10.1/24。确保该地址尚未在网络中使用。

如果您配置了高可用性，并要监控此接口的高可用性，则还要在同一子网上配置一个备用 IP 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

注释 如果为接口配置了 DHCP 服务器，您会看到该配置。您可以编辑或删除 DHCP 地址池。如果将接口 IP 地址更改为不同的子网，必须先删除 DHCP 服务器或在新子网上配置地址池，才能保存接口更改。请参阅[配置 DHCP 服务器](#)。
- **PPPoE** - 如果应使用基于以太网的点对点协议 (PPPoE) 获取地址，请选择此选项。如果接口连接到 DSL、电缆调制解调器或 ISP 的其他连接，并且 ISP 使用 PPPoE 来提供 IP 地址，则可能需要使用 PPPoE。如果您配置高可用性，将不能使用此选项。设置以下值：
 - **组名称** - 指定您选择用于表示此连接的组名称。
 - **PPPoE 用户名** - 指定 ISP 提供的用户名。
 - **PPPoE 密码** - 指定 ISP 提供的密码。
 - **PPP 身份验证** - 选择 **PAP**、**CHAP** 或 **MSCHAP**。

PAP 在身份验证过程中传递明文用户名和密码，这样并不安全。使用 CHAP 时，客户端可返回加密的 [challenge plus password] 和明文用户名来响应服务器质询。CHAP 比 PAP 更安全，但其不会加密数据。MSCHAP 与 CHAP 类似但更安全，因为服务器只对加密密码进行

存储和比较，而不是像 CHAP 一样存储和比较明文密码。MSCHAP 还可生成密钥，以便 MPPE 进行数据加密。

- **PPPoE 获知的路由指标** - 向获悉的路由分配管理距离。有效值为从 1 到 255。默认情况下，获悉的路由的默认管理距离为 1。
- **从 PPPoE 获取默认路由** - 选中此复选框可支持从 PPPoE 服务器获取默认路由。
- **IP 地址类型** - 选择动态可从 PPPoE 服务器获取 IP 地址。如果从 ISP 分配了静态 IP 地址，也可以选择静态。

步骤 5（可选。）点击 **IPv6 地址** 选项卡，并配置 IPv6 地址。

- **状态** - 在不想配置全局地址时，要启用 IPv6 处理并自动配置本地链路地址，请选择 **已启用**。本地链路地址基于接口的 MAC 地址（修改的 EUI-64 格式）生成。

注释 禁用 IPv6 不会禁用接口上使用显式 IPv6 地址配置或启用自动配置的 IPv6 处理。

- **地址自动配置** - 选择此选项可自动配置地址。只有设备所在链路中的路由器配置为提供 IPv6 服务（包括通告 IPv6 全局前缀以用于该链路），IPv6 无状态自动配置才会生成全局 IPv6 地址。如果该链路中的 IPv6 路由服务不可用，则只能获得本地链路 IPv6 地址，无法访问设备直接的网络链路之外的服务。本地链路地址以修改的 EUI-64 接口 ID 为基础。

虽然 RFC 4862 规定为无状态自动配置所配置的主机不发送路由器通告消息，但威胁防御设备在这种情况下确实会发送路由器通告消息。选择 **抑制 RA** 可抑制消息，遵从 RFC 要求。

- **静态地址/前缀** - 如果不使用无状态自动配置，请输入完整的静态全局 IPv6 地址和网络前缀。例如，2001:0DB8::BA98:0:3210/48。有关 IPv6 寻址的详细信息，请参阅 [IPv6 寻址](#)，第 3 页。

如果仅使用本地链路地址，请选择 **本地链路** 选项。本地链路地址在本地网络之外无法访问。在网桥组接口上无法配置本地链路地址。

注释 链路本地地址应以 FE8、FE9、FEA 或 FEB 开头，例如 fe80::20d:88ff:feec:6a82。请注意，我们建议根据修改的 EUI-64 格式自动分配链路本地地址。例如，如果其他设备强制使用修改的 EUI-64 格式，则手动分配的链路本地地址可能导致丢弃数据包。

- **备用 IP 地址** - 如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IPv6 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。
- **抑制 RA** - 是否抑制路由器通告。威胁防御可以参与路由器通告，以便邻居设备可以动态获悉默认路由器地址。默认情况下，每个配置 IPv6 的接口定期发送路由器通告消息（ICMPv6 类型 134）。

也会发送路由器通告，以响应路由器请求消息（ICMPv6 类型 133）。路由器请求消息由主机在系统启动时发送，以便主机可以立即自动配置，而无需等待下一条预定路由器通告消息。

对于不希望威胁防御设备提供 IPv6 前缀的任何接口（例如外部接口），您可能希望抑制接口上的这些消息。

步骤 6（可选。）[配置高级选项](#)，第 44 页。

高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。

步骤 7 点击确定。

下一步做什么

- 将 VLAN 添加至相应的安全区。请参阅[配置安全区](#)。

将交换机端口配置为接入端口

要将交换机端口分配给单个 VLAN，请将其配置为接入端口。默认情况下，以太网 1/2 至以太网 1/8 交换机端口已启用并分配给 VLAN 1。



注释 Firepower 1010 不支持在网络中进行环路检测的生成树协议。因此，您必须确保与威胁防御设备的任何连接均不会在网络环路中结束。

开始之前

将 VLAN 接口添加用于要为其分配接入端口的 VLAN ID。接入端口仅接受未标记流量。请参阅[配置 VLAN 接口](#)，第 25 页。


过程

步骤 1 点击设备，然后点击接口摘要中的链接。

系统默认选择接口 (**Interfaces**) 页面。接口列表显示可用物理接口、物理接口名称、地址和状态。

步骤 2 点击要编辑的物理接口的编辑图标 (🔗)。

步骤 3 进行以下设置：

- 请勿设置交换机端口的接口名称；仅关联 VLAN 接口是命名接口。
- 将模式设置为交换机端口。
- 将状态滑块设置为已启用设置 ()。
- (可选) 设置说明。

一行说明最多可包含 200 个字符 (不包括回车符)。

步骤 4 点击 VLAN 设置以下内容：

- (可选) 选中受保护端口复选框以将此交换机端口设置为受保护端口，因此您可以阻止交换机端口与同一 VLAN 上的其他受保护交换机端口进行通信。

在以下情况下，您可能想要防止交换机端口相互之间进行通信：主要从其他 VLAN 访问这些交换机端口上的设备；您不需要允许 VLAN 间访问；由于病毒感染或其他安全漏洞，您想要将设备相互隔离开。例如，如果具有托管 3 台 Web 服务器的 DMZ，则在您将此选项应用于各交换机端口后，则可以将 Web 服务器相互隔离。内部网络和外部网络均可以与这 3 台网络服务器进行通信，反之亦然，但这些网络服务器相互之间无法进行通信。

- 对于使用类型，请点击接入。
- 对于接入 VLAN，点击向下箭头以选择现有 VLAN 接口之一。

您可以通过点击新建 VLAN 添加新的 VLAN 接口。请参阅[配置 VLAN 接口，第 25 页](#)。

步骤 5 点击确定 (OK)。

将交换机端口配置为中继端口

此程序介绍如何创建可以使用 802.1 Q 标记传输多个 VLAN 的中继端口。中继端口接受未标记和标记流量。允许的 VLAN 上的流量通过中继端口保持不变。

中继端口接收未标记流量后将其标记为本地 VLAN ID，以便 ASA 可以将流量转发至正确交换机端口，或可以将流量路由至另一个防火墙接口。如果 ASA 从中继端口发送本地 VLAN ID 流量，则会删除 VLAN 标记。请务必在另一台交换机上的中继端口上设置相同的本地 VLAN，以便将未标记流量标记至同一 VLAN。

开始之前

将 VLAN 接口添加用于要为其分配中继端口的各 VLAN ID。请参阅[配置 VLAN 接口](#)，第 25 页。

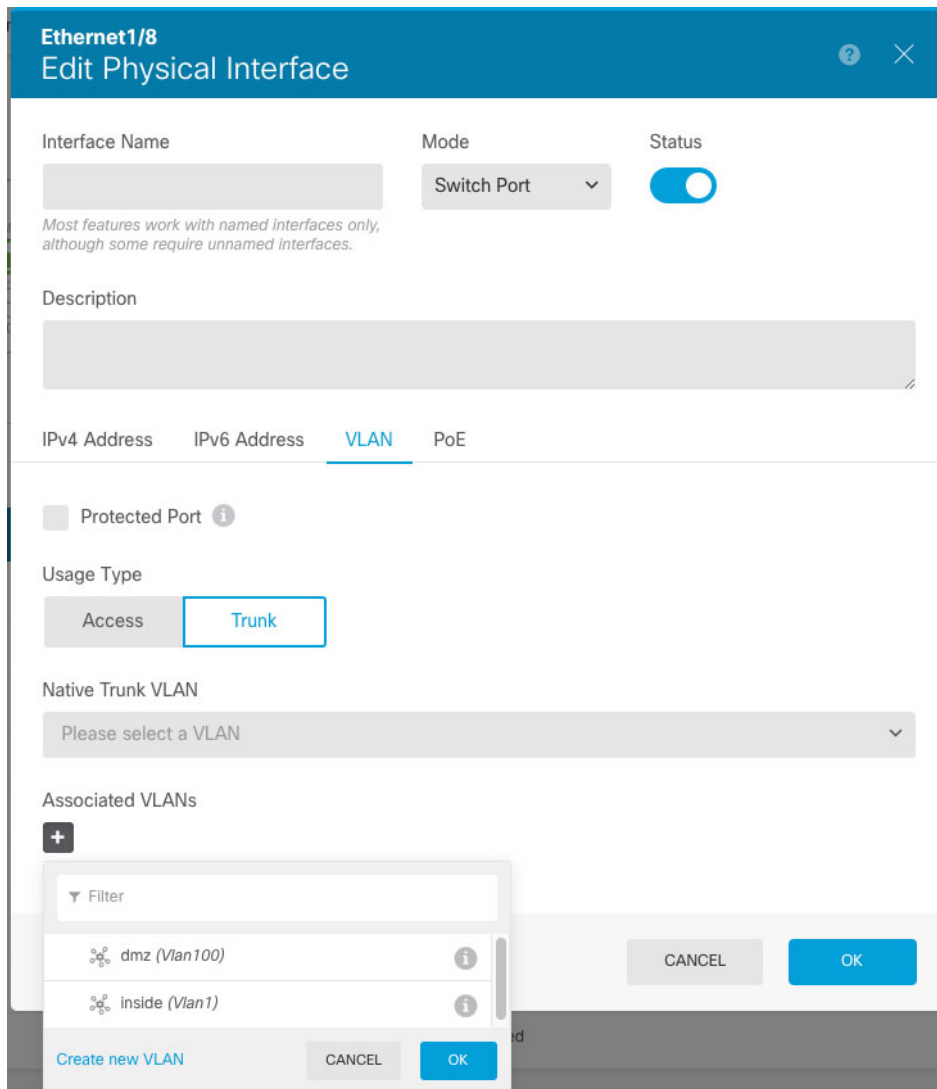
过程


步骤 1 点击**设备**，然后点击**接口摘要**中的链接。

系统默认选择**接口 (Interfaces)** 页面。接口列表显示可用物理接口、物理接口名称、地址和状态。

步骤 2 点击要编辑的物理接口的编辑图标 (🔗)。

步骤 3 进行以下设置：



- 请勿设置交换机端口的接口名称；仅关联 VLAN 接口是命名接口。
- 将模式设置为交换机端口。
- 将状态滑块设置为已启用设置 ()。
- (可选) 设置说明。

一行说明最多可包含 200 个字符 (不包括回车符)。

步骤 4 点击 VLAN 设置以下内容：

- (可选) 选中受保护端口复选框以将此交换机端口设置为受保护端口，因此您可以阻止交换机端口与同一 VLAN 上的其他受保护交换机端口进行通信。

在以下情况下，您可能想要防止交换机端口相互之间进行通信：主要从其他 VLAN 访问这些交换机端口上的设备；您不需要允许 VLAN 间访问；由于病毒感染或其他安全漏洞，您想要将设备相互隔离开。例如，如果具有托管 3 台 Web 服务器的 DMZ，则在您将此选项应用于各交换机

端口后，则可以将 Web 服务器相互隔离。内部网络和外部网络均可以与这 3 台网络服务器进行通信，反之亦然，但这些网络服务器相互之间无法进行通信。

- b) 对于**使用类型**，请点击**中继**。
- c) （可选）对于**本地中继 VLAN**，点击向下箭头以选择本地 VLAN 的现有 VLAN 接口之一。

默认的本地 VLAN ID 为 1。

每个端口只能有一个本地 VLAN，但各端口的本地 VLAN 可以相同也可以不同。

您可以通过点击**新建 VLAN**添加新的 VLAN 接口。请参阅[配置 VLAN 接口](#)，第 25 页。

- d) 对于**关联 VLAN**，点击加号图标 (+) 以选择一个或多个现有 VLAN 接口。

如果在此字段中包含本地 VLAN，则将忽略该本地 VLAN；从端口发送本地 VLAN 流量时，中继端口始终会删除 VLAN 标记。此外，不会接收仍具有 VLAN 标记的流量。

您可以通过点击**新建 VLAN**添加新的 VLAN 接口。请参阅[配置 VLAN 接口](#)，第 25 页。

步骤 5 点击**确定 (OK)**。

配置以太网供电

以太网 1/7 和以太网 1/8 支持 IP 电话或无线接入点等设备的以太网供电 (PoE)。Firepower 1010 支持 IEEE 802.3af (PoE) 和 802.3at (PoE+)。PoE+ 使用链路层发现协议 (LLDP) 来协商功率级别。PoE+ 可以为受电设备提供 30 瓦的功率。仅在需要时提供功率。

如果关闭接口，则会禁用设备电源。

默认情况下，在以太网 1/7 和以太网 1/8 上启用 PoE。此过程介绍如何禁用和启用 PoE 以及如何设置可选参数。


过程

步骤 1 点击**设备**，然后点击**接口摘要**中的链接。

系统默认选择**接口 (Interfaces)** 页面。接口列表显示可用物理接口、物理接口名称、地址和状态。

步骤 2 点击以太网 1/7 或 1/8 的编辑图标 (🔗)。

步骤 3 点击**PoE**，并设置以下内容：

a) 要启用以太网供电，请点击滑块 () 以便使其处于启用状态。
默认情况下，PoE 处于启用状态。

b) (可选) 如果您知道所需的确切功率，请输入**功耗瓦数**。

默认情况下，PoE 使用适合受电设备类别的瓦数将电源自动传送至受电设备。Firepower 1010 使用 LLDP 进一步协商正确的瓦数。如果知道特定瓦数并想要禁用 LLDP 协商，请输入介于 4000 和 30000 毫瓦的值。

步骤 4 点击确定 (OK)。

配置 VLAN 子接口和 802.1Q 中继

通过 VLAN 子接口，可将一个物理接口划分成多个标记有不同 VLAN ID 的逻辑接口。带有一个或多个 VLAN 子接口的接口将自动配置为 802.1Q 中继。由于 VLAN 允许您在特定物理接口上将流量分开，所以您可以增加网络中可用的接口数量，而无需增加物理接口或设备。

如果您将物理接口连接到交换机的中继端口，请创建子接口。为交换机中继端口上显示的每个 VLAN 创建子接口。如果您将物理接口连接到交换机的接入端口，创建子接口将没有意义。

准则和限制

- 防止物理接口上的未标记数据包 - 如果使用子接口，则通常表明也不希望物理接口传递流量，因为物理接口会传递未标记的数据包。由于必须启用物理接口，才能允许子接口传递流量，所以请确保物理接口不会通过未命名接口传递流量。如果要允许物理接口传递未标记数据包，可以照常命名接口。
- Firepower 1010 - 交换机端口或 VLAN 接口上不支持子接口。
- 您不能在网桥组成员接口上配置 IP 地址，但是可以根据需要修改高级设置。
- 同一父接口上的所有子接口必须为网桥组成员或路由接口；您无法混合搭配。
- 威胁防御不支持动态中继协议 (DTP)，因此您必须无条件地将连接的交换机端口配置到中继上。
- 您可能想要为威胁防御设备上定义的子接口分配唯一 MAC 地址，因为它们使用父接口上相同的固化 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。此外，由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一 MAC 地址分配给子接口会允许使用唯一 IPv6 链路本地地址，这能够避免威胁防御上特定实例内发生流量中断。

过程

步骤 1 点击**设备**，然后点击**接口摘要**中的链接。

系统默认选择**接口 (Interfaces)** 页面。要将子接口添加至 EtherChannel，请点击**EtherChannel**。接口列表显示可用物理接口、物理接口名称、地址和状态。

步骤 2 执行以下操作之一：

- 在**接口 (Interfaces)** 页面上，点击加号图标 (+) 以创建新的子接口。
- 在**EtherChannel** 页面上，点击加号和向下箭头图标 (+v)，然后选择子接口 (Subinterface)。
- 点击要编辑的子接口的编辑图标 (🔗)。

如果不再需要某个子接口，请点击该子接口对应的删除图标 (🗑️) 将其删除。

步骤 3 将状态滑块设置为已启用设置 (🔘)。

步骤 4 配置父接口、名称和说明：

Add Subinterface ? ×

Parent Interface

Subinterface Name

Mode

Status

Most features work with named interfaces only, although some require unnamed interfaces.

Description

VLAN ID

1 - 4094

Subinterface ID

IPv4 Address

IPv6 Address

Advanced

Type

IP Address and Subnet Mask

 /

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask

 /

e.g. 192.168.5.16

a) 选择父接口。

父接口是将子接口添加至其中的物理接口。创建子接口后，父接口则无法更改。

b) 设置子接口名称，最多 48 个字符。

字母字符必须为小写。例如 **inside** 或 **outside**。如果没有名称，将忽略其余的接口配置。

注释 如果更改名称，更改将自动反映到使用旧名称的所有位置，包括安全区、系统日志服务器对象和 DHCP 服务器定义。但无法删除名称，除非首先删除使用该名称的所有配置，这是因为对于任何策略或设置通常无法使用未命名的接口。

c) 将模式设置为路由。

如果稍后将此接口添加到网桥组，则该模式将自动更改为 **BridgeGroupMember**。请注意，无法在网桥组成员接口上配置 IP 地址。

d) （可选）设置说明。

一行说明最多可包含 200 个字符（不包括回车符）。

e) 设置 **VLAN ID**。

输入 VLAN ID，介于 1 和 4094 之间，用于标记该子接口上的数据包。

f) 设置子接口 **ID**。

以整数形式输入介于 1 和 4294967295 之间的子接口 ID。此 ID 附加至接口 ID；例如 Ethernet1/1.100。方便起见，您可以匹配 VLAN ID，但这不是必需的。创建子接口后，则无法更改该 ID。

步骤 5 点击 **IPv4 地址** 选项卡，并配置 IPv4 地址。

从**类型**字段中选择以下任一选项：

- **DHCP** - 如果应从网络中的 DHCP 服务器获取地址，请选择此选项。如果您配置高可用性，将不能使用此选项。如有需要，更改以下选项：
 - **路由指标** - 如果从 DHCP 服务器获取默认路由，则此选项是指与获知路由的管理距离，其值介于 1 到 255 之间。默认值为 1。
 - **获取默认路由** - 是否从 DHCP 服务器获取默认路由。您通常会选择此选项，该选项是默认值。

- **静态** - 如果希望分配固定的地址，请选择此选项。对于连接到接口的网络，键入接口的 IP 地址和子网掩码。例如，如果您连接的是 10.100.10.0/24 网络，则可以输入 10.100.10.1/24。确保该地址尚未在网络中使用。

如果您配置了高可用性，并要监控此接口的高可用性，则还要在同一子网上配置一个备用 IP 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

注释 如果为接口配置了 DHCP 服务器，您会看到该配置。您可以编辑或删除 DHCP 地址池。如果将接口 IP 地址更改为不同的子网，必须先删除 DHCP 服务器或在新子网上配置地址池，才能保存接口更改。请参阅[配置 DHCP 服务器](#)。

- **PPPoE** - 如果应使用基于以太网的点对点协议 (PPPoE) 获取地址，请选择此选项。如果接口连接到 DSL、电缆调制解调器或 ISP 的其他连接，并且 ISP 使用 PPPoE 来提供 IP 地址，则可能需要使用 PPPoE。如果您配置高可用性，将不能使用此选项。设置以下值：

- **组名称** - 指定您选择用于表示此连接的组名称。
- **PPPoE 用户名** - 指定 ISP 提供的用户名。
- **PPPoE 密码** - 指定 ISP 提供的密码。
- **PPP 身份验证** - 选择 **PAP**、**CHAP** 或 **MSCHAP**。

PAP 在身份验证过程中传递明文用户名和密码，这样并不安全。使用 CHAP 时，客户端可返回加密的 [challenge plus password] 和明文用户名来响应服务器质询。CHAP 比 PAP 更安全，但其不会加密数据。MSCHAP 与 CHAP 类似但更安全，因为服务器只对加密密码进行

存储和比较，而不是像 CHAP 一样存储和比较明文密码。MSCHAP 还可生成密钥，以便 MPPE 进行数据加密。

- **PPPoE 获知的路由指标** - 向获悉的路由分配管理距离。有效值为从 1 到 255。默认情况下，获悉的路由的默认管理距离为 1。
- **从 PPPoE 获取默认路由** - 选中此复选框可支持从 PPPoE 服务器获取默认路由。
- **IP 地址类型** - 选择动态可从 PPPoE 服务器获取 IP 地址。如果从 ISP 分配了静态 IP 地址，也可以选择静态。

步骤 6（可选。）点击 **IPv6 地址** 选项卡，并配置 IPv6 地址。

- **状态** - 在不想配置全局地址时，要启用 IPv6 处理并自动配置本地链路地址，请选择 **已启用**。本地链路地址基于接口的 MAC 地址（修改的 EUI-64 格式）生成。

注释 禁用 IPv6 不会禁用接口上使用显式 IPv6 地址配置或启用自动配置的 IPv6 处理。

- **地址自动配置** - 选择此选项可自动配置地址。只有设备所在链路中的路由器配置为提供 IPv6 服务（包括通告 IPv6 全局前缀以用于该链路），IPv6 无状态自动配置才会生成全局 IPv6 地址。如果该链路中的 IPv6 路由服务不可用，则只能获得本地链路 IPv6 地址，无法访问设备直接的网络链路之外的服务。本地链路地址以修改的 EUI-64 接口 ID 为基础。

虽然 RFC 4862 规定为无状态自动配置所配置的主机不发送路由器通告消息，但威胁防御设备在这种情况下确实会发送路由器通告消息。选择 **抑制 RA** 可抑制消息，遵从 RFC 要求。

- **静态地址/前缀** - 如果不使用无状态自动配置，请输入完整的静态全局 IPv6 地址和网络前缀。例如，2001:0DB8::BA98:0:3210/48。有关 IPv6 寻址的详细信息，请参阅 [IPv6 寻址，第 3 页](#)。

如果仅使用本地链路地址，请选择 **本地链路** 选项。本地链路地址在本地网络之外无法访问。在网桥组接口上无法配置本地链路地址。

注释 链路本地地址应以 FE8、FE9、FEA 或 FEB 开头，例如 fe80::20d:88ff:feec:6a82。请注意，我们建议根据修改的 EUI-64 格式自动分配链路本地地址。例如，如果其他设备强制使用修改的 EUI-64 格式，则手动分配的链路本地地址可能导致丢弃数据包。

- **备用 IP 地址** - 如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IPv6 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。
- **抑制 RA** - 是否抑制路由器通告。威胁防御可以参与路由器通告，以便邻居设备可以动态获悉默认路由器地址。默认情况下，每个配置 IPv6 的接口定期发送路由器通告消息（ICMPv6 类型 134）。

也会发送路由器通告，以响应路由器请求消息（ICMPv6 类型 133）。路由器请求消息由主机在系统启动时发送，以便主机可以立即自动配置，而无需等待下一条预定路由器通告消息。

对于不希望威胁防御设备提供 IPv6 前缀的任何接口（例如外部接口），您可能希望抑制接口上的这些消息。

步骤 7（可选。）[配置高级选项，第 44 页](#)。

高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。

步骤 8 点击确定 (OK)。

下一步做什么

- 将子接口添加至相应的安全区。请参阅[配置安全区](#)。
- 向您的动态 DNS 服务提供商注册一个完全限定域名 (FQDN)，并配置 DDNS 以更新 DNS 服务器上的接口地址 (IPv4 和 IPv6)。请参阅[配置动态 DNS](#)。

配置被动接口

被动接口使用交换机 SPAN（交换端口分析器）或镜像端口监控在网络中传输的流量。SPAN 或镜像端口允许从交换机的其他端口复制流量。此功能可以提供网络内的系统可视性，而不会影响网络流量。

如果系统是在被动部署中配置的，则无法执行某些操作，例如阻止流量。被动接口无条件接收所有流量，这些接口不会重传接收到的流量。

使用被动接口监控网络上的流量，以收集流量相关的信息。例如，您可以应用入侵策略来识别攻击网络的威胁类型，或了解用户正在发出的 Web 请求的 URL 类别。您可以实施各种安全策略和规则，了解系统在主动部署的情况下会执行哪些操作，以便可以根据访问控制和其他规则丢弃流量。

但是，由于被动接口无法影响流量，因此存在很多配置限制。这些接口只是让系统知悉有流量通过：进入被动接口的数据包不会从设备流出。

以下主题更加详细地介绍了被动接口及其配置方法。

为什么使用被动接口？

被动接口的主要目的是提供一种简单的演示模式。您可以设置交换机监控单个源端口，然后使用工作站发送通过被动接口监控的测试流量。由此，可以了解威胁防御系统如何评估连接、识别威胁等。系统性能满足要求后，可以将其主动部署在网络中，并删除被动接口配置。

不过，您也可以在生产环境中使用被动接口，以提供以下服务：

- 纯 ID 部署 - 如果您不想使用系统作为防火墙或 IPS（入侵防御系统），可以将其被动部署为 IDS（入侵检测系统）。在此部署方法中，您将使用访问控制规则将入侵策略应用于所有流量。您还必须设置系统监控交换机上的多个源端口。然后，您将可以使用控制面板监控网络上发现的威胁。但是，在此模式下，系统不会执行任何操作来阻止这些威胁。
- 混合部署 - 您可以在同一系统上搭配使用主动路由接口和被动接口。因此，在某些网络中，您可以将威胁防御设备部署为防火墙，同时配置一个或多个被动接口监控其他网络中的流量。

被动接口的限制

定义为被动模式接口的任何物理接口具有以下限制：

- 无法为被动接口配置子接口。
- 不能将被动接口添加到网桥组。
- 不能在被动接口上配置 IPv4 或 IPv6 地址。
- 不能对被动接口选择“仅管理”选项。
- 只能将接口添加到被动模式安全区，不能将其添加到路由安全区。
- 可以将被动安全区添加到访问控制或身份规则的源条件中。不能在目标条件中使用被动区域。同时，也不能在同一规则中搭配使用被动和路由区域。
- 不能为被动接口配置管理访问规则（HTTPS 或 SSH）。
- 不能在 NAT 规则中使用被动接口。
- 不能为被动接口配置静态路由。也不能在路由协议配置中使用被动接口。
- 不能在被动接口上配置 DHCP 服务器。也不能使用被动接口通过自动配置获取 DHCP 设置。
- 不能在系统日志服务器配置中使用被动接口。
- 不能在被动接口上配置任何类型的 VPN。

为硬件威胁防御被动接口配置交换机

只有当网络交换机配置正确时，硬件威胁防御设备上的被动接口才可以正常工作。以下过程基于 Cisco Nexus 5000 系列交换机。如果您有不同类型的交换机，所用的命令可能会有所不同。

其基本思路是，配置 SPAN（交换端口分析器）或镜像端口，将被动接口连接到该端口，在交换机上配置监控会话以将流量副本从一个或多个源端口发送到 SPAN 或镜像端口。

过程

步骤 1 将交换机上的端口配置为监控（SPAN 或镜像）端口。

```
switch(config)# interface Ethernet1/48
switch(config-if)# switchport monitor
switch(config-if)#
```

步骤 2 定义监控会话以识别要监控的端口。

确保您将 SPAN 或镜像端口定义为目标端口。在以下示例中，监控两个源端口。

```
switch(config)# monitor session 1
switch(config-monitor)# source interface ethernet 1/7
```



```
switch(config-monitor)# source interface ethernet 1/8
switch(config-monitor)# destination interface ethernet 1/48
switch(config-monitor)# no shut
```

步骤 3 (可选。)使用 **show monitor session** 命令验证配置。

以下示例显示会话 1 的简要输出。

```
switch# show monitor session 1 brief
  session 1
-----
type           : local
state          : up
source intf    :
  rx           : Eth1/7      Eth1/8
  tx           : Eth1/7      Eth1/8
  both        : Eth1/7      Eth1/8
source VSANs   :
destination ports : Eth1/48

Legend: f = forwarding enabled, l = learning enabled
```

步骤 4 以物理方式将电缆从 威胁防御被动接口连接到交换机的目标端口。

可以在进行物理连接前后，将接口配置为被动模式。请参阅[将物理接口配置为被动模式，第 41 页](#)。

为 Threat Defense Virtual 被动接口配置 VLAN

只有在虚拟网络上正确配置了 VLAN 时，threat defense virtual 设备的被动接口才可以正常工作。请确保执行以下操作：

- 将 threat defense virtual 接口连接到已在混杂模式下配置的 VLAN。然后，按照[将物理接口配置为被动模式，第 41 页](#)中的说明配置接口。被动接口会看到混合 VLAN 上所有流量的副本。
- 将一个或多个终端设备（例如虚拟 Windows 系统）连接到同一 VLAN。如果 VLAN 已连接到互联网，可以使用单台设备。否则，需要至少两台设备，才可以在两者之间传递流量。要想获取 URL 类别数据，需要建立互联网连接。

将物理接口配置为被动模式

您可以将接口配置为被动模式。在被动模式下工作时，接口仅监控交换机自身（针对硬件设备）或混合 VLAN（针对 threat defense virtual）配置的监控会话中来自源端口的流量。有关需要在交换机或虚拟网络中配置哪些对象的详细信息，请参阅以下主题：

- [为硬件 威胁防御 被动接口配置交换机，第 40 页](#)
- [为 Threat Defense Virtual 被动接口配置 VLAN，第 41 页](#)

当您想要分析通过受监控交换机端口传入的流量，而不影响这些流量时，可使用被动模式。有关使用被动模式的端到端示例，请参阅[如何被动监控网络上的流量](#)。

过程

步骤 1 点击设备，然后点击接口摘要中的链接，再点击接口或 **EtherChannel**。

步骤 2 点击要编辑的物理接口或 EtherChannel 的编辑图标 (🔗)。

选择当前未使用的接口。如果您要将使用中的接口转换为被动接口，需先从任何安全区中删除该接口，并删除使用该接口的所有其他配置。

步骤 3 将状态滑块设置为已启用设置 (🔘)。

步骤 4 进行以下配置：

- **接口名称** - 接口名称，最多 48 个字符。字母字符必须为小写。例如，monitor。
- **模式** - 选择被动。
- (可选。) **说明** - 说明最多为 200 个字符，单行，不能使用回车。

注释 无法配置 IPv4 或 IPv6 地址。在“高级”选项卡中，仅可以更改 MTU、复用和速度设置。

步骤 5 点击确定 (OK)。

下一步做什么

创建被动接口并不会在控制面板上填充接口上所发现流量的相关信息。您还必须执行以下操作：使用案例会介绍这些步骤。请参阅[如何被动监控网络上的流量](#)。

- 创建被动安全区并向其添加接口。请参阅[配置安全区](#)。
- 创建将被动安全区用作源区域的访问控制规则。通常，您将在这些规则中应用入侵策略以实施 IDS（入侵检测系统）监控。请参阅[配置访问控制策略](#)。
- 或者，为被动安全区创建 SSL 解密和身份规则，并启用安全智能策略。

配置高级接口选项

高级选项包括设置 MTU、硬件设置、仅管理、MAC 地址和其他设置。

关于 MAC 地址

您可以手动配置介质访问控制 (MAC) 地址来覆盖默认地址。

对于高可用性配置，您可以同时配置接口的主用和备用 MAC 地址。如果主用设备进行故障切换，并且备用设备成为主用设备，则新的主用设备会开始使用主用 MAC 地址，以最大限度地减少网络中断。

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。
- VLAN 接口 (Firepower 1010) - 所有 VLAN 接口均共享一个 MAC 地址。确保所有连接的交换机均可支持此方案。如果连接的交换机需要唯一 MAC 地址，可手动分配 MAC 地址。请参阅[配置高级选项，第 44 页](#)。
- EtherChannels - 对于 EtherChannel，属于通道组的所有接口均共享同一 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。
- 子接口 - 物理接口的所有子接口都使用同一个烧录 MAC 地址。您可能想为子接口分配唯一的 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。此外，由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一 MAC 地址分配给子接口会允许使用唯一 IPv6 链路本地地址，这能够避免威胁防御上特定实例内发生流量中断。

关于 MTU

MTU 指定威胁防御设备在给定以太网接口上传输的最大帧负载大小。MTU 值是没有以太网报头、VLAN 标记或其他系统开销情况下的帧大小。例如，将 MTU 设置为 1500 时，预期帧大小为 1518 字节（含报头）或 1522 字节（使用 VLAN）。请勿为容纳这些报头而将 MTU 的值设得过高。

路径 MTU 发现

威胁防御设备支持路径 MTU 发现（如 RFC 1191 中所定义），从而使两个主机之间的网络路径中的所有设备均可协调 MTU，以便它们可以标准化路径中的最低 MTU。

MTU 和分段

对于 IPv4，如果传出 IP 数据包大于指定 MTU，则该数据包将分为 2 帧或更多帧。片段在目标处（有时在中间跃点处）重组，而分片可能会导致性能下降。对于 IPv6，通常不允许对数据包进行分段。因此，IP 数据包大小应在 MTU 大小范围内，以避免分片。

对于 UDP 或 ICMP，应用应将 MTU 考虑在内，以避免分段。



注释 只要有内存空间，威胁防御设备就可接收大于所配置的 MTU 的帧。

MTU 和巨型帧

MTU 越大，您能发送的数据包越大。加大数据包可能有利于提高网络效率。请参阅以下准则：

- 与流量路径上的 MTU 相匹配 - 我们建议将所有威胁防御接口以及流量路径的其他设备接口上的 MTU 设为相同。匹配 MTU 可防止中间设备对数据包进行分片。
- 容纳巨型帧 - 巨型帧是指大于标准最大值 1522 字节（包括第 2 层报头和 VLAN 报头）的以太网数据包，最大为 9216 字节。MTU 可设置为 9000 字节或更高，以容纳巨型帧。最大值取决于型号。



注释 加大 MTU 会为巨型帧分配更多内存，这样可能会限制其他功能（例如访问规则）的最大使用量。如果在 `threat defense virtual` 上将 MTU 增加到默认值 1500 以上，则必须重新启动系统。如果设备已为高可用性，还须重新启动备用设备。无需重新启动其他型号，因为巨型帧支持在该型号上始终启用。

配置高级选项

高级接口选项的默认设置适用于大多数网络。只有当您解决网络问题或配置高可用性时，才需要进行配置。

以下步骤程序假定已定义接口。另外，您还可以在初始编辑或创建接口时编辑这些设置。

限制

- 对于网桥组，您可以在成员接口上配置大多数这些选项。除用于 DAD 尝试和高可用性监控之外，这些选项不适用于桥接虚拟接口 (BVI)。
- 您无法在 Firepower 1000 或 2100 设备的 MTU、复用或速度。
- 高级选项不适用于 Firepower 1010 交换机端口。
- 在 Firepower 4100/9300 上，您无法设置接口复用或速度。请使用 FXOS 为接口设置这些功能。
- 对于被动接口，您只能设置 MTU、复用以及速度。不能将接口仅用于管理。

过程

- 步骤 1** 点击设备，点击接口摘要中的链接，然后点击接口类型以查看接口列表。
- 步骤 2** 点击要编辑的接口的编辑图标 (🔗)。
- 步骤 3** 点击高级选项 (**Advanced Options**)。
- 步骤 4** 如果您想让系统在决定是否故障转移到高可用性配置中的对等体设备时考虑接口的运行状况，请选择对高可用性监控启用 (**Enable for HA Monitoring**)。

如果不配置高可用性，可忽略此选项。如果不配置接口的名称，也可以忽略此选项。

步骤 5 要将数据接口仅用于管理，请选择**仅管理**。

仅管理接口不允许直通流量，所以将数据接口设置为仅管理的价值微乎其微。不能更改管理/诊断接口的此项设置，它们始终为仅管理。

步骤 6 要启用思科 Trustsec，请选择**传播安全组标记 (Propagate Security Group Tag)**。

您可以在物理接口、子接口、EtherChannel、VLAN、管理接口或 BVI 接口（无论是命名还是未命名）上启用或禁用 Cisco Trustsec。默认情况下，当您为接口命名时，Cisco Trustsec 会自动启用。

步骤 7 将 **MTU**（最大传输单位）更改为所需的值。

默认 MTU 为 1500 字节。最小值和最大值取决于您的平台。如果通常在网络中使用巨型帧，请设置一个较大的值。

注释 如果在 ISA 3000 系列设备，**threat defense virtual**上将 MTU 提高到 1500 以上。如果设备已为高可用性，还须重新启动备用设备。无需重新启动其他型号，因为巨型帧支持在该型号上始终启用。

步骤 8 （仅限物理接口）。修改速度和复用设置。

默认设置为该接口与线路另一端的接口协商最佳复用和速度，但如有必要，您可以强制实施特定的复用或速度。所列的选项仅为接口支持的设置。在网络模块上设置这些选项之前，请阅读[接口配置的限制条件，第 4 页](#)。

- **复用-选择半或全**。SFP 接口仅支持**全**复用。
- **速度**-具体选项取决于型号和接口类型。选择**速度**、**自动**、**无协商**或**检测 SFP**。对于 Firepower 1000 和 2100 光纤端口，**无协商**将速度设置为 1000 Mbps，并禁用流量控制参数和远程故障信息的链路协商。（仅限 Cisco Secure Firewall 3100）选择**检测 SFP**以检测已安装的 SFP 模块的速度并使用适当的速度。复用始终为全复用，并且始终启用自动协商。如果您稍后将网络模块更改为其他型号，并希望速度自动更新，则此选项非常有用。
- （仅限安全防火墙 3100）**自动协商**-根据接口类型，设置接口以协商流量控制参数和远程故障信息的链路状态。
- **前向纠错模式**-（仅限 Cisco Secure Firewall 3100）对于 25 Gbps 及更高的接口，请启用前向纠错 (FEC)。对于 EtherChannel 成员接口，必须先配置前向纠错，然后才能将其添加到 EtherChannel。使用**自动 (Auto)**时选择的设置取决于收发器类型，以及接口是固定接口（内置）还是在网络模块上。

表 1: 用于自动设置的默认 **FEC**

| 收发器类型 | 固定端口默认 FEC （以太网 1/9 至 1/16） | 网络模块默认 FEC |
|--------|------------------------------------|-------------------|
| 25G-SR | Clause 108 RS-FEC | Clause 108 RS-FEC |
| 25G-LR | Clause 108 RS-FEC | Clause 108 RS-FEC |

| 收发器类型 | 固定端口默认 FEC（以太网 1/9 至 1/16） | 网络模块默认 FEC |
|--------------|----------------------------|------------------|
| 10/25G-CSR | Clause 108 RS-FEC | Clause 74 FC-FEC |
| 25G-AOCxM | Clause 74 FC-FEC | Clause 74 FC-FEC |
| 25G-CU2.5/3M | 自动协商 | 自动协商 |
| 25G-CU4/5M | 自动协商 | 自动协商 |

步骤 9 修改 IPv6 配置设置。

- 启用 **DHCP 客户端 (Enable DHCP Client)** — 使用 DHCPv6 获取地址。
选中使用 **DHCP 获取默认路由 (Obtain default route using DHCP)**，从路由器通告中获取默认路由。
- 启用 **DHCP 以获取 IPv6 地址配置** - 是否在 IPv6 路由器通告数据包中设置“托管地址配置”标志。此标志通知 IPv6 自动配置客户端应使用 DHCPv6 来获取相关地址以及派生的无状态自动配置地址。
- 启用 **DHCP 以获取 IPv6 非地址配置** - 是否在 IPv6 路由器通告数据包中设置“其他地址配置”标志。此标志通知 IPv6 自动配置客户端应使用 DHCPv6 从 DHCPv6 获取其他信息，如 DNS 服务器地址。
- **DAD 尝试** - 接口执行重复地址检测 (DAD) 的频率，介于 0 - 600 之间。默认值为 1。在无状态自动配置过程中，DAD 会验证新单播 IPv6 地址的唯一性，再将地址分配给接口。如果重复地址是接口的链路本地地址，则在接口上禁用 IPv6 数据包处理。如果重复地址是全局地址，则将不使用该地址。接口将使用邻居的询求消息来执行重复地址检测。将该值设置为 0 可禁用重复地址检测 (DAD) 流程。

步骤 10 （可选，建议为子接口和高可用性设备配置。）配置 MAC 地址。

默认情况下，系统对接口使用预烧到网络接口卡 (NIC) 的 MAC 地址。因此，该接口上的所有子接口都使用相同的 MAC 地址，也因此您可能想要为每个子接口创建唯一地址。如果您配置高可用性，建议手动配置主用/备用 MAC 地址。定义 MAC 地址有助于在故障转移时保持网络中的一致性。

- **MAC 地址** - 采用 H.H.H 格式的介质访问控制，其中 H 是 16 位十六进制数字。例如，您可以将 MAC 地址 00-0C-F1-42-4C-DE 输入为 000C.F142.4CDE。MAC 地址不能设置组播位，即左起第二个十六进制数字不能是奇数。
- **备用 MAC 地址** - 用于高可用性。如果主用设备发生故障切换，备用设备变为主用设备，则新的主用设备开始使用主用 MAC 地址，以最大限度地减少网络中断，而原来的主用设备使用备用地址。

步骤 11 点击确定 (OK)。

扫描接口更改并迁移接口

更改设备上的接口时，设备会通知设备管理器已发生更改。在执行接口扫描之前，您将无法部署配置。设备管理器支持通过其他接口迁移安全策略中的接口，因此几乎可以无缝删除接口。

关于接口扫描和迁移

扫描

更改设备上的接口时，设备会通知设备管理器已发生更改。执行接口扫描前，您将无法部署配置。在检测到任何已添加、已删除或已恢复接口的扫描后，您可以部署您的配置；但是，将不会部署引用已删除接口的配置部分。

需要扫描的接口更改包括添加或删除接口。例如：网络模块更改；Firepower 4100/9300 机箱上的已分配接口更改；threat defense virtual上的接口更改。

以下更改在扫描后不阻止部署：

- 安全区成员身份
- EtherChannel 接口成员身份
- Firepower 1010 VLAN 接口交换机端口成员身份
- 网桥组接口成员身份，适用于引用 BVI 的策略



注释 虽然您应手动或使用接口替换功能来修复系统日志服务器配置，但系统日志服务器出口接口更改不会阻止部署。

正在迁移

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，包括安全区、NAT、VPN、路由、DHCP 服务器等。

设备管理器支持通过其他接口迁移安全策略中的接口，因此几乎可以无缝删除接口。



注释 迁移功能不会将名称、IP 地址和其他配置从一个接口复制到另一个接口；相反，此功能会将安全策略更改为引用新接口，而不是旧接口。需要在迁移之前手动配置新接口设置。

如果需要删除接口，我们建议您添加新接口并迁移旧接口，然后再将其删除。如果同时添加和删除接口，迁移过程仍将正常工作；但是，您无法手动编辑已删除接口或引用这些接口的策略，因此您可能会发现分阶段执行迁移更容易。

如果替换同一类型的接口（例如，需要对网络模块执行 RMA 操作），则可以：1. 从旧机箱中移除模块；2. 执行扫描；3. 部署与已删除接口无关的更改；4. 更换模块；5. 执行新扫描；6. 部署配置，包括与接口相关的任何更改。如果新接口具有与旧接口相同的接口 ID 和特征，则无需执行迁移。

接口扫描和迁移准则和限制

不受支持的接口迁移

- BVI 物理接口
- 防火墙接口的被动接口
- 网桥组成员
- EtherChannel 接口成员
- ISA 3000 硬件旁路成员
- Firepower 1010 VLAN 接口或交换机端口
- 诊断接口
- HA 故障转移和状态链路
- 迁移不同类型的接口，例如将网桥组接口迁移至需要物理接口的功能

其他准则

- 如果需要删除接口，我们建议您添加新接口并迁移旧接口，然后再将其删除。
- 对于 **threat defense virtual**，仅在接口列表结尾添加和删除接口。如果在任何其他位置添加或删除接口，则虚拟机监控程序将对接口重新编号，从而致使配置中的接口 ID 与错误接口相符。
- 如果扫描/迁移出现故障，请恢复机箱上的原始接口，然后重新扫描以恢复原始状态。
- 对于备份，请务必使用新接口创建新备份。使用旧配置还原将恢复旧的接口信息，您必须再次执行扫描/替换。
- 对于 **HA**，在主用设备上执行接口扫描前，请对两台设备进行相同的接口更改。您只需在主用设备上执行扫描/迁移。配置更改会复制到备用设备。

扫描和迁移接口

扫描设备管理器中的接口更改，并从已删除接口迁移接口配置。如果您仅想迁移接口配置（且无需扫描），请忽略与扫描相关的以下过程中的步骤。



注释 迁移功能不会将名称、IP 地址和其他配置从一个接口复制到另一个接口；相反，此功能会将安全策略更改为引用新接口，而不是旧接口。需要在迁移之前手动配置新接口设置。

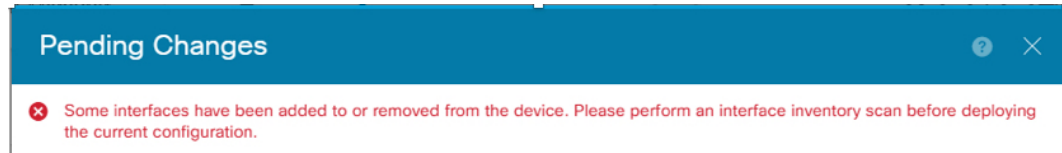
过程

步骤 1 在机箱上添加或删除接口。

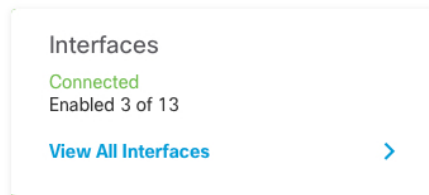
如果需要删除接口，我们建议您添加新接口并替换旧接口，然后再将其删除。

步骤 2 接口更改扫描。

执行接口扫描前，您将无法部署配置。如果尝试在扫描之前进行部署，您会看到以下错误：

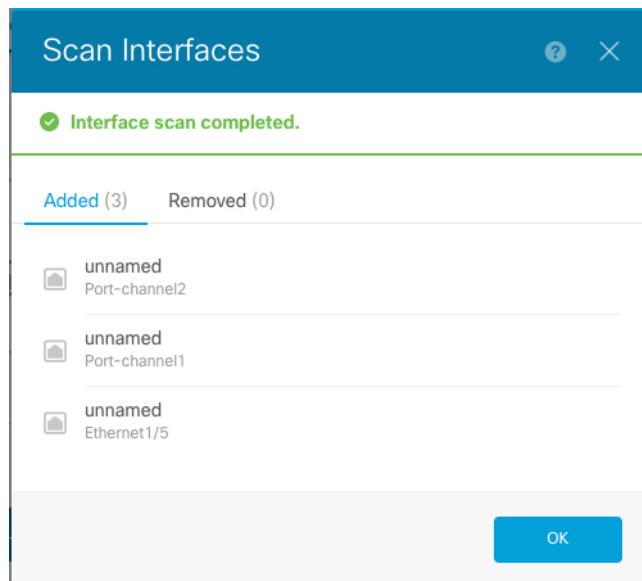


a) 点击**设备**，然后点击**接口摘要**中的**查看所有接口**链接。

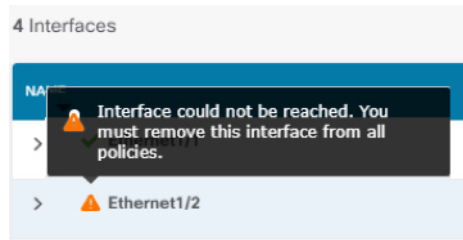


b) 点击扫描接口图标 ()。

c) 等待接口扫描，然后点击**确定**。



扫描后，已删除接口显示在 **接口** 页面上，并带有警告符号：



步骤 3 要将现有接口迁移至新接口：

- a) 使用名称、IP 地址等配置新接口。

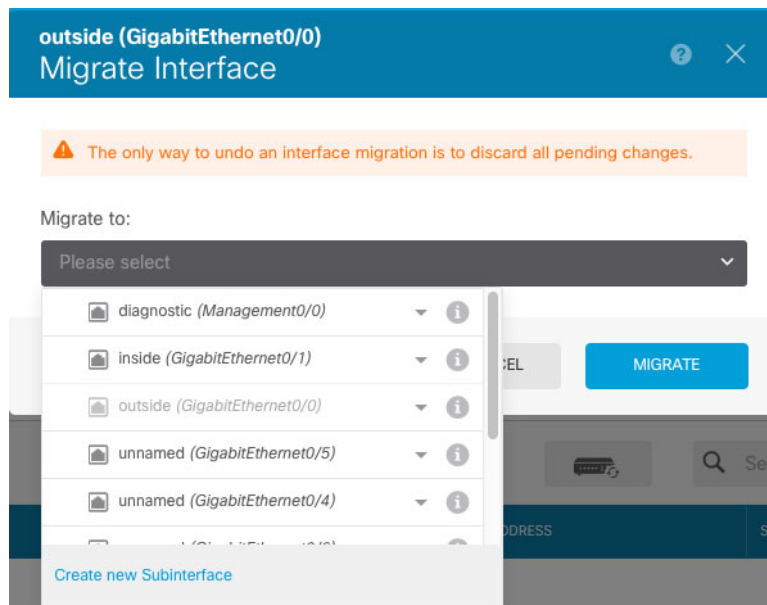
如果要使用待删除接口的现有 IP 地址和名称，则首先需要使用虚拟名称和 IP 地址重新配置旧接口，以便可以在新接口上使用这些设置。

- b) 点击旧接口的“迁移”图标。

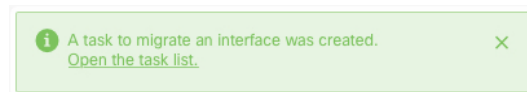


此过程会将旧接口迁移至引用该接口的所有配置设置中的新接口。

- c) 从**迁移至**：下拉列表中选择新接口。



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



- e) 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 status 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. One task is listed: 'Config migration from source interface outside to destination interface outside_2' with a start time of '06 Jun 2019 12:37 PM', an end time of '06 Jun 2019 12:37 PM', and a status of 'Migration is successful' with a green checkmark icon.

| 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 | |

f) 如果迁移失败，您可以在 API Explorer 中查看原因。

要打开 API Explorer，点击更多选项按钮 (☰) 并选择 **API Explorer**。选择接口 > **GET /jobs/interfacemigrations**，然后点击**尝试!**。

步骤 4 部署配置。

将不会部署引用已删除接口的配置部分，在这种情况下，您将看到以下消息：

The screenshot shows a 'Pending Changes' window with a blue header. Below the header is a warning icon (triangle with exclamation mark) and the text: 'The current configuration has warnings:'. A bullet point follows: 'The configuration includes references to a missing interface. Any elements that are dependent on the missing interface will not be deployed. Please re-evaluate the configuration, and if necessary, re-create the undeployable parts of the configuration for a valid interface. For more details, go to [Interfaces](#).'

步骤 5 删除机箱上的旧接口，然后执行其他扫描。

系统将从接口 (**Interfaces**) 页面中删除您的策略中不再使用的已删除接口。

步骤 6 重新部署配置，以从配置中删除未使用接口。

管理 Cisco Secure Firewall 3100 的网络模块

如果在首次打开防火墙之前安装网络模块，则无需执行任何操作；网络模块已启用并可供使用。

如果您需要在初始启动后更改网络模块安装，请参阅以下程序。

配置分支端口

您可以为每个 40GB 或更高的接口配置 10GB 分支端口。此程序介绍如何断开和重新加入端口。分支端口可以像任何其他物理以太网端口一样使用，包括添加到 EtherChannel。

要获得高可用性，请在主用设备上执行此程序；接口更改将复制到另一台设备。

开始之前

- 您必须使用受支持的分支电缆。有关详细信息，请参阅硬件安装指南。
- 该接口不能在您的配置中使用。它不能有子接口或属于 EtherChannel。
- 为实现高可用性，无法命名、启用或监控接口的高可用性。

过程

步骤 1 点击设备，然后点击接口摘要中的链接。


系统默认选择接口 (**Interfaces**) 页面。接口列表显示可用物理接口、物理接口名称、地址和状态。

步骤 2 要从 40GB 或更高接口拆分出 10GB 端口，请点击接口右侧的 **拆分** 图标 ()。

点击确认对话框中的 **确定 (OK)**。如果接口正在使用，您将看到一条错误消息。您必须先解决任何使用案例，然后才能重试分支。例如，您可以迁移配置以使用不同的接口。

例如，要拆分出 Ethernet2/1 40GB 接口，生成的子接口将被标识为 Ethernet2/1/1、Ethernet2/1/2、Ethernet2/1/3 和 Ethernet2/1/4。

在接口图形上，断开的端口具有以下外观： 您可以点击左右箭头滚动浏览详细介绍分支端口状态的页面。

步骤 3 要重新加入分支端口，请点击接口右侧的 **加入** 图标 ()。

点击确认对话框中的 **确定 (OK)**。如果有任何子端口正在使用，您将看到一条错误消息。您必须先解决任何使用案例，然后才能重试重新加入。例如，您可以迁移配置以使用不同的接口。

您必须重新加入该接口的所有子端口。

步骤 4 部署配置。

增加网络模块

要在初始启动后将网络模块添加到防火墙，请执行以下步骤。添加新模块需要重新启动。

过程

步骤 1 根据硬件安装指南安装网络模块。

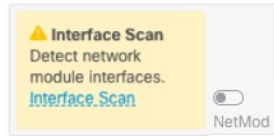
对于高可用性，请在两台设备上安装网络模块。

步骤 2 重新启动防火墙；请参阅 [重启或关闭系统](#)。对于高可用性，请重新启动备用设备，然后在备用设备上执行此程序的其余部分。

步骤 3 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。

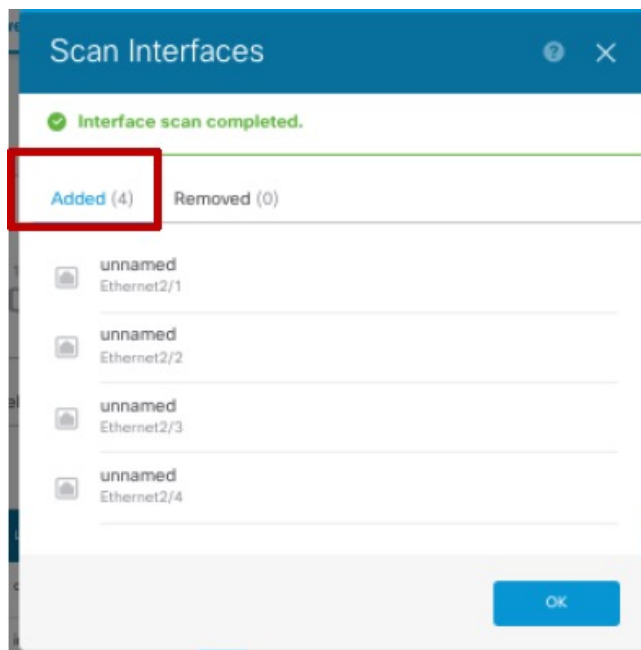
该图显示需要进行接口扫描。

图 3: 需要进行接口扫描



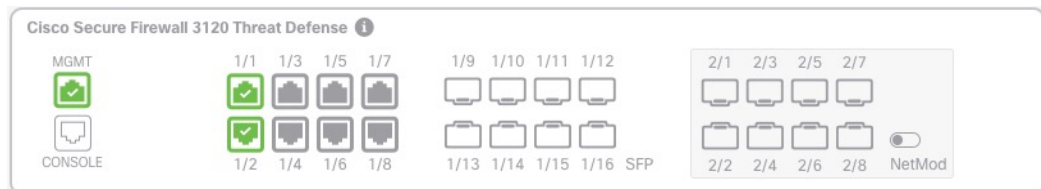
步骤 4 点击 **接口扫描 (Interface Scan)**，使用新的网络模块详细信息更新页面。
等待接口扫描，然后点击**确定**。

图 4: 扫描接口



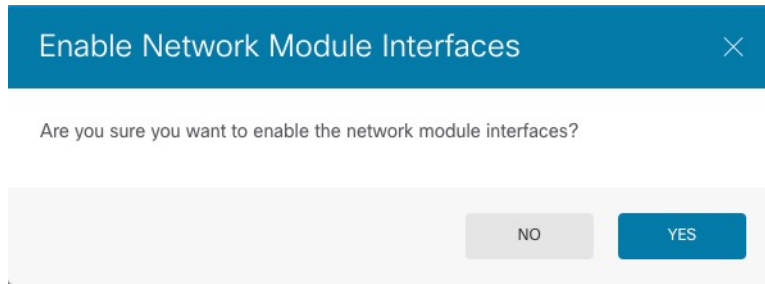
步骤 5 在接口图形上，点击滑块 () 以启用网络模块。

图 5: 启用网络模块



步骤 6 系统将提示您确认是否要启用网络模块。点击 **Yes**。

图 6: 确认启用



步骤 7 对于高可用性，请更改主用设备（请参阅 [切换主用和备用对等体（强制故障转移）](#)），然后对新的备用设备执行上述步骤。

热插拔网络模块

您可以将网络模块热插拔为相同类型的新模块，而无需重新启动。但是，您必须关闭当前模块才能安全地将其删除。此程序介绍如何关闭旧模块、安装新模块以及如何启用它。

开始之前

对于高可用性，如果故障转移链路在模块上，则不能禁用该网络模块。您必须中断高可用性（请参阅 [中断高可用性](#)）。热插拔模块后，您可以重新设置高可用性。

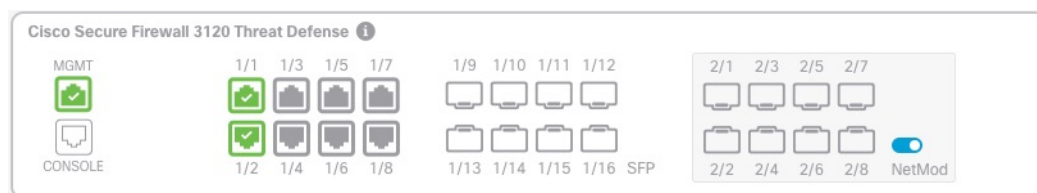
过程

步骤 1 对于高可用性，请确保要执行热插拔的设备是备用节点。请参阅 [切换主用和备用对等体（强制故障转移）](#)。

步骤 2 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。

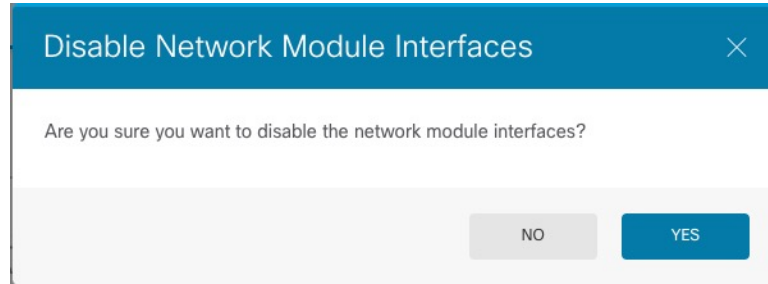
步骤 3 在接口图形上，点击滑块 () 以禁用网络模块。

图 7: 禁用网络模块



步骤 4 系统将提示您是否确认要禁用网络模块。点击 **Yes**。

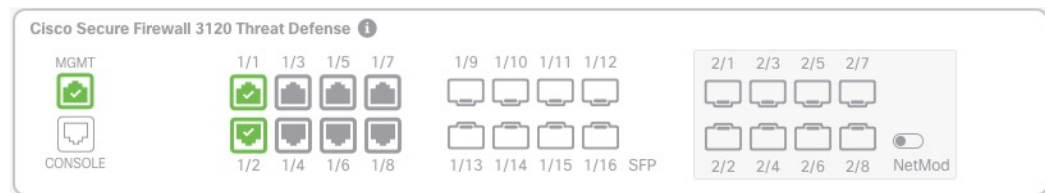
图 8: 确认禁用



步骤 5 根据硬件安装指南安装网络模块。

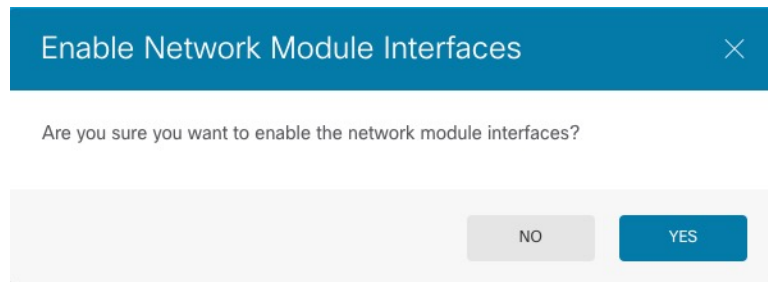
步骤 6 在接口图形上，点击滑块 (☐) 以启用网络模块。

图 9: 启用网络模块



步骤 7 系统将提示您确认是否要启用网络模块。点击 **Yes**。

图 10: 确认启用



将网络模块更换为其他类型

如果您更换了其他类型的网络模块，则需要重新启动。如果新模块的接口少于旧模块，则必须手动删除与不再存在的接口相关的任何配置。

开始之前

为实现高可用性，如果故障转移链路在模块上，则不能禁用该网络模块。您将不得不中断高可用性（请参阅 [中断高可用性](#)），这意味着您将在重新启动主用设备时停机。设备完成重新启动后，您可以重新设置高可用性。

过程


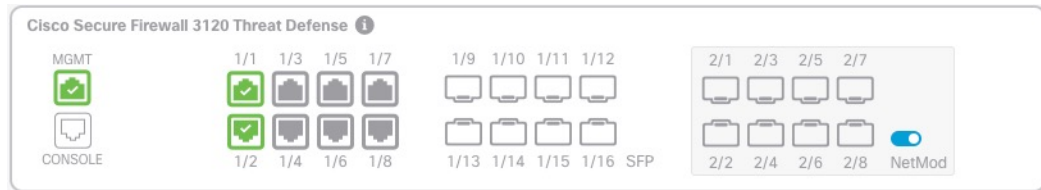
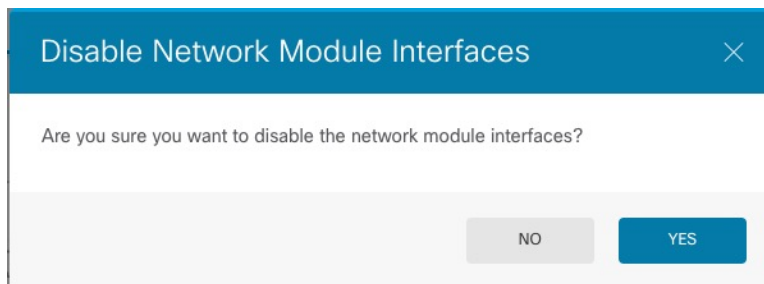
- 步骤 1** 点击设备 (**Device**)，然后点击接口 (**Interfaces**) 摘要中的查看所有接口 (**View All Interfaces**) 链路。要实现高可用性，请先在备用设备上执行此程序。
- 步骤 2** 在接口图形上，点击滑块 () 以禁用网络模块。

图 11: 禁用网络模块



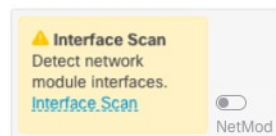
- 步骤 3** 系统将提示您是否确认要禁用网络模块。点击 **Yes**。

图 12: 确认禁用



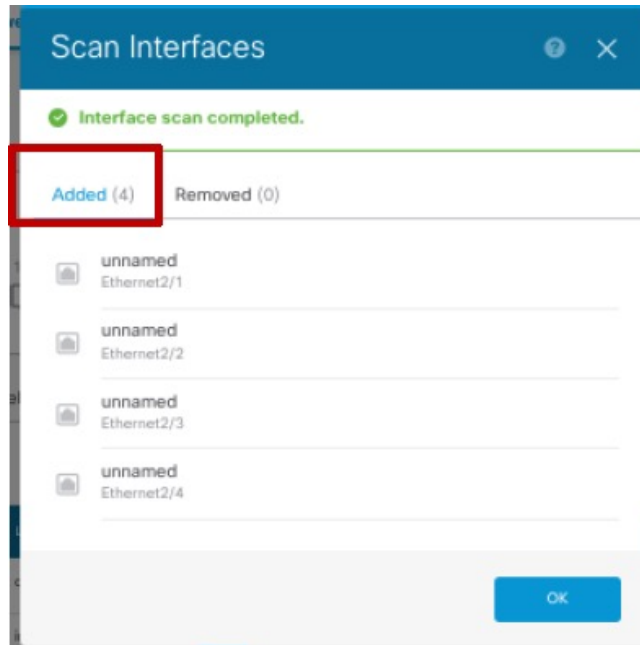
- 步骤 4** 在设备上，根据硬件安装指南，取下旧的网络模块并更换为新的网络模块。
- 步骤 5** 重新启动防火墙；请参阅 [重启或关闭系统](#)。
- 步骤 6** 在 **接口 (Interfaces)** 页面上，该图显示需要进行接口扫描。点击 **接口扫描 (Interface Scan)**，使用新的网络模块详细信息更新页面。

图 13: 需要进行接口扫描



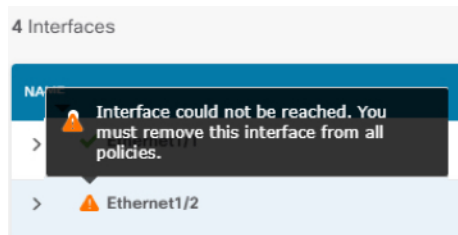
- 步骤 7** 等待接口扫描，然后点击确定。

图 14: 扫描接口



扫描后，已删除接口显示在 **接口 (Interfaces)** 页面上，并带有警告符号：

图 15: 删除的接口

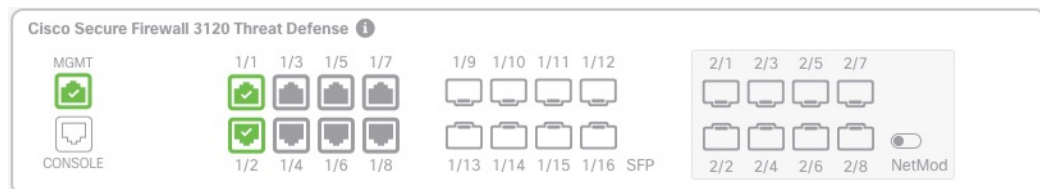


步骤 8 如果网络模块有较少接口，则需要删除直接引用已删除接口的任何配置。

引用安全区的策略不受影响。您可以选择将配置迁移到其他接口。请参阅[扫描和迁移接口](#)，第 48 页。

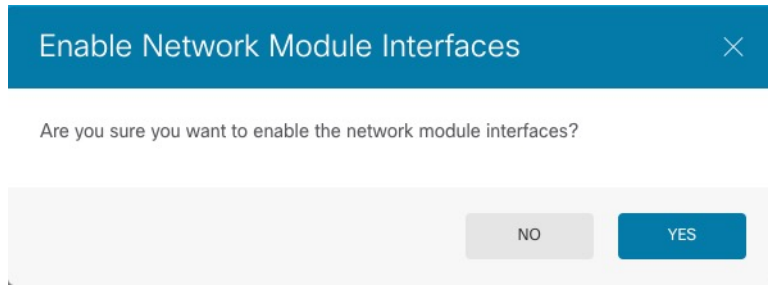
步骤 9 在接口图形上，点击滑块 () 以启用网络模块。

图 16: 启用网络模块



步骤 10 系统将提示您确认是否要启用网络模块。点击 **Yes**。

图 17: 确认启用



步骤 11 要更改接口速度，请参阅 [配置高级选项](#)，第 44 页。

默认速度设置为“检测 SFP”，用于检测已安装的 SFP 的正确速度。仅当您手动将速度设置为特定值并且现在需要新的速度时，才需要修复速度。

步骤 12 如果必须更改任何配置，请点击 **部署** 图标。

无需部署即可保存网络模块更改。

步骤 13 对于高可用性，请更改主用设备（请参阅 [切换主用和备用对等体（强制故障转移）](#)），然后对新的备用设备执行上述步骤。

拆卸网络模块

如果要永久删除网络模块，请执行以下步骤。拆卸网络模块需要重新启动。

开始之前

对于高可用性，请确保故障转移链路不在网络模块上。

过程

步骤 1 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。对于高可用性，请先在备用设备上执行此程序。


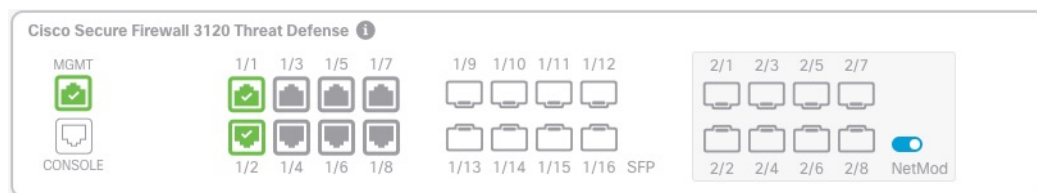
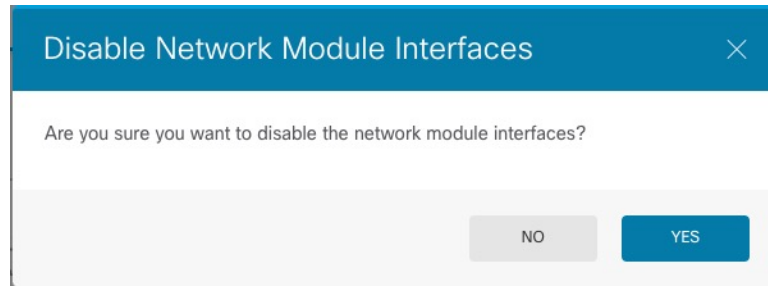
步骤 2 在接口图形上，点击滑块 () 以禁用网络模块。

图 18: 禁用网络模块



步骤 3 系统将提示您是否确认要禁用网络模块。点击 **Yes**。

图 19: 确认禁用

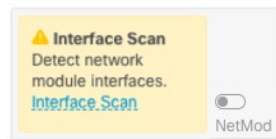


步骤 4 在防火墙上，拆卸网络模块。

步骤 5 重新启动防火墙；请参阅 [重启或关闭系统](#)。

步骤 6 在 **接口 (Interfaces)** 页面上，该图显示需要进行接口扫描。点击 **接口扫描 (Interface Scan)**，使用正确的网络模块详细信息更新页面。

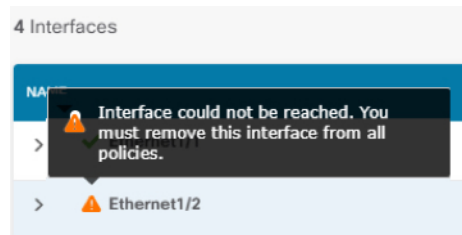
图 20: 需要进行接口扫描



步骤 7 等待接口扫描，然后点击**确定**。

扫描后，已删除接口显示在 **接口 (Interfaces)** 页面上，并带有警告符号：

图 21: 删除的接口



步骤 8 您需要删除直接引用已删除接口的任何配置。

引用安全区的策略不受影响。您可以选择将配置迁移到其他接口。请参阅[扫描和迁移接口](#)，第 48 页。

步骤 9 如果必须更改任何配置，请点击 **部署** 图标。

无需部署即可保存网络模块更改。

步骤 10 对于高可用性，请更改主用设备（请参阅 [切换主用和备用对等体（强制故障转移）](#)），然后对新的备用设备执行上述步骤。

对电源故障配置硬件旁路 (ISA 3000)

您可以启用硬件旁路，使流量在断电期间继续在接口对之间流动。支持的接口对为铜缆接口 GigabitEthernet 1/1 和 1/2 以及 GigabitEthernet 1/3 和 1/4。如果您使用的是光纤以太网型号，则只有铜缆以太网对（GigabitEthernet 1/1 和 1/2）支持硬件旁路。默认情况下，如果支持，两个接口对均启用硬件旁路。

启用硬件旁路时，流量将在这些接口对之间的第 1 层传递。在设备管理器和威胁防御 CLI 中都可以看到接口处于关闭状态。不使用防火墙功能，因此请确保您了解允许流量通过设备的风险。

我们建议您禁用 TCP 序列号随机化（如本过程中所述）。默认情况下，ISA 3000 会将通过其的 TCP 连接的初始序列号 (ISN) 重写为随机编号。硬件旁路激活后，ISA 3000 不再位于数据路径中，也不再转换序列号。接收客户端会收到意外序列号，并丢弃连接，因此需要重新建立 TCP 会话。即便禁用 TCP 序列号随机化后，某些 TCP 连接将也需要重新建立，因为链路在切换期间会临时关闭。

在 CLI 控制台或 SSH 会话中，使用 `show hardware-bypass` 命令以监控运行状态。

开始之前

要使用硬件旁路：

- 必须将接口对放置在同一网桥组内。
- 必须将接口连接到交换机的接入端口。不能将它们连接到中继端口。

过程

步骤 1 点击设备，然后点击接口摘要中的链接。

在页面顶部的**硬件旁路 (Hardware Bypass)**部分显示设备允许的接口对的当前配置。

但是，在启用硬件旁路之前，必须确保在同一网桥组中配置接口对。

步骤 2 点击编辑以配置硬件旁路。

系统将显示**硬件旁路配置**对话框。

步骤 3 要配置自动硬件旁路行为，请为每个接口对在**断电期间硬件旁路**区域中选择以下一个选项。

- **禁用** - 禁用硬件旁路。断电期间流量不会流过设备。
- **启用** - 在断电期间激活硬件旁路。硬件旁路可确保在断电期间流量不会中断。请注意，系统不会检查绕过的流量，并且不会应用安全策略。恢复电源后，硬件旁路会自动禁用，以便流量可以经过检测正常通行。请注意，禁用硬件旁路时可能会出现短暂的流量中断。
- **持久性启用** - 在断电期间激活硬件旁路，并在恢复供电后继续启用硬件旁路。恢复供电后，您必须使用**手动硬件旁路**滑块禁用硬件旁路。此选项允许您控制何时短暂中断流量。

步骤 4（可选）要手动启用或禁用硬件旁路，请点击**手动硬件旁路**滑块。

例如，您可能想要测试系统，或出于某些原因需要暂时绕过设备。请注意，您必须部署配置来更改硬件旁路的状态；只更改设置是不够的。

手动启用/禁用硬件旁路时，您将看到以下系统日志消息，其中对为 1/1-1/2 或 1/3-1/4。

- %FTD-6-803002: 系统不对通过 GigabitEthernet 对的流量提供保护
- %FTD-6-803003: 用户已手动在 GigabitEthernet 对上禁用旁路

步骤 5 点击**确定**。

更改不会立即生效。您必须部署配置。

步骤 6 (可选。) 创建禁用 TCP 序列号随机化所需的 FlexConfig 对象和策略。

- 在**设备 > 高级配置**中点击**查看配置**。
- 在“高级配置”目录中依次点击 **FlexConfig > FlexConfig** 对象。
- 点击 **+** 按钮以创建新的对象。
- 为对象输入名称。例如，**Disable_TCP_Randomization**。
- 在**模板编辑器**中，输入命令禁用 TCP 序列号随机化。

命令是 **set connection random-sequence-number disable**，但您必须为策略映射中的特定类配置此命令。到目前为止，最简单的方法是全局禁用随机序列号，这需要使用以下命令：

```
policy-map global_policy
class default_class
set connection random-sequence-number disable
```

- 在**取消模板编辑器**中，输入撤消此配置所需的命令。

例如，如果您全局禁用 TCP 序列号随机化，取消模板将为：

```
policy-map global_policy
class default_class
set connection random-sequence-number enable
```

- 点击**确定**保存对象。

现在需要将此对象添加到 FlexConfig 策略。并非创建好对象就可以了。

- 点击目录中的 **FlexConfig** 策略。
- 在组列表中点击 **+**。
- 选择 **Disable_TCP_Randomization** 对象，然后点击**确定**。

系统应随使用模板中的命令更新预览。验证您是否看到预期的命令。

- 点击**保存**。

您现在可以部署策略。

监控接口

可在以下区域查看有关接口的一些基本信息：

- **设备。**使用端口图可监控接口的当前状态。将鼠标悬停在端口上方可查看其 IP 地址、EtherChannel 成员身份、启用状态和链路状态。IP 地址可静态分配，也可以使用 DHCP 获取。

接口端口使用以下颜色代码：

- 绿色 - 接口已配置和启用，链路为运行状态。
 - 灰色 - 接口未启用。
 - 橙色/红色 - 接口已配置和启用，但链路中断。如果该接口已连接电缆，则此状态表示有错误需要更正。如果该接口未连接电缆，则此状态为预期状态。
- **监控 > 系统。**吞吐量控制面板显示有关流经系统的流量的信息。您可以查看所有接口的信息，也可以选择特定接口查看其信息。
 - **监控 > 区域。**该控制面板显示基于安全区的统计信息，这些安全区由接口组成。您可以深入分析此信息以了解更多详情。

在 CLI 中监控接口

您还可以打开 CLI 控制台或登录设备 CLI，使用以下命令获取有关接口相关行为与统计信息的更详细信息。

- **show interface** 显示接口统计信息和配置信息。此命令有许多关键字，可用于获取所需的信息。使用 ? 作为关键字可查看可用选项。
- **show ipv6 interface** 显示有关接口的 IPv6 配置信息。
- **show bridge-group** 显示网桥虚拟接口 (BVI) 的相关信息，包括成员信息和 IP 地址。
- **show conn** 显示当前通过接口建立的连接的相关信息。
- **show traffic** 显示流过每个接口的流量的相关统计信息。
- **show ipv6 traffic** 显示流过设备的 IPv6 流量的相关统计信息。
- **show dhcpd** 显示接口上的 DHCP 使用统计信息及其他信息，特别是接口上配置的 DHCP 服务器的相关信息。
- **show switch vlan** 显示 VLAN 到交换机端口的关联。
- **show switch mac-address-table** 显示静态和动态 MAC 地址条目。
- **show arp** 显示动态、静态和代理 ARP 条目。
- **show power inline** 显示 PoE 状态。
- **show vpdn group** 显示 PPPoE 组以及已配置的用户名和身份验证。

- **show vpdn username** 显示 PPPoE 用户名和密码。
- **show vpdn session pppoe state** 显示 PPPoE 会话的状态。

接口示例

使用案例章节涵盖以下与接口相关的示例：

- [如何在设备管理器上配置设备](#)
- [如何添加子网](#)
- [如何被动监控网络上的流量](#)

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。