



接口概述

威胁防御 设备包括可在不同模式下配置的数据接口，以及管理 接口。

- [管理接口，第 1 页](#)
- [接口模式和类型，第 2 页](#)
- [安全区域和接口组，第 4 页](#)
- [Auto-MDI/MDIX 功能，第 5 页](#)
- [接口默认设置，第 6 页](#)
- [创建安全区域和接口组对象，第 6 页](#)
- [启用物理接口并配置以太网参数，第 7 页](#)
- [配置 EtherChannel 接口，第 10 页](#)
- [与管理中心同步接口更改，第 17 页](#)
- [管理 Cisco Secure Firewall 3100/4200 的网络模块，第 20 页](#)
- [合并管理和诊断接口，第 34 页](#)
- [接口历史，第 40 页](#)

管理接口

在 7.3 及更早版本中，物理管理接口由诊断逻辑接口和管理逻辑接口共用。在 7.4 及更高版本中，为简化用户体验，诊断接口与管理接口进行了合并。

管理接口

管理接口与设备上的其他接口分离。它用于设置设备并将其注册到管理中心。它使用自己的 IP 地址和静态路由。您可以在 CLI 中使用 **configure network** 命令配置其设置。您还可以在 **设备 (Devices) > 设备管理 (Device Management) > 设备 (Devices) > 接口 (Interfaces)** 页面上查看其状态。如果在将 IP 地址添加到管理中心后在 CLI 中更改该地址，则可以通过 **设备 (Devices) > 设备管理 (Device Management) > 设备 (Devices) > 管理 (Management)** 区域在 Cisco Secure Firewall Management Center 中匹配该 IP 地址。

您也可以使用数据接口而不是管理接口来管理 威胁防御 。

诊断接口

对于使用 7.4 及更高版本的新设备，您不能使用旧诊断接口。仅合并的管理接口可用。

如果已升级到 7.4 或更高版本，并且没有为诊断接口进行任何配置，则接口将自动合并。

如果已升级到 7.4 或更高版本，并且已为诊断接口进行了配置，则可以选择手动合并接口，也可以选择继续使用单独的诊断接口。请注意，在更高版本中将删除对诊断接口的支持，因此您应计划尽快合并接口。要手动合并管理接口和诊断接口，请参阅[合并管理和诊断接口](#)，第 34 页。阻止自动合并的配置包括：

- 名为“management”的数据接口 - 此名称保留用于合并的管理接口。
- 诊断接口中的 IP 地址
- 诊断接口中启用了 DNS
- 系统日志、SNMP、RADIUS 或 AD（对于远程访问 VPN）源接口为诊断接口
- RADIUS 或 AD（对于远程访问 VPN）未指定源接口，并且至少有一个接口配置为管理专用接口（包括诊断接口）- 这些服务的默认路由查找已从管理专用路由表更改为数据路由表，没有回退到管理。因此，除管理外，不能对使用管理专用接口。
- 诊断接口中的静态路由
- 诊断接口中的动态路由
- 诊断接口中的 HTTP 服务器
- 诊断接口中的 ICMP
- 诊断接口的 DDNS
- 使用诊断接口的 FlexConfig

有关旧诊断接口工作方式的详细信息，请参阅本指南的 7.3 版本。

接口模式和类型

您可以在两种模式下部署威胁防御接口：常规防火墙模式和仅 IPS 模式。您可以在同一设备上同时配置防火墙和仅 IPS 接口。

常规防火墙模式

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，选择为此流量配置 IPS 功能。

可以配置的防火墙接口类型取决于为设备设置的防火墙模式：路由或透明模式。有关详细信息，请参阅[透明或路由防火墙模式](#)。

- 路由模式接口（仅路由防火墙模式）- 要在其间路由的每个接口都在不同的子网中。

- 网桥组接口（路由和透明防火墙模式）- 您可以将网络上的多个接口组合在一起，Firepower 威胁防御设备将使用桥接技术在接口之间传递流量。每个桥接组包括一个网桥虚拟接口 (BVI)，供您为其分配一个网络 IP 地址。在路由模式下，Firepower 威胁防御设备在 BVI 和常规路由接口之间路由。在透明模式下，每个网桥组都是独立的，相互之间无法通信。

仅 IPS 模式

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。如果您有单独的防火墙来保护这些接口，并且不希望造成防火墙功能的开销，则可能需要实施仅限 IPS 的接口。



注释 防火墙模式只影响常规的防火墙接口，而不影响仅 IPS 接口，如内联集或被动接口。仅 IPS 接口可以在两种防火墙模式下使用。

仅 IPS 接口可以部署为以下类型：

- 内嵌集，带有可选分路模式 - 内嵌集的作用类似于导线上的凹凸，并将两个接口绑定在一起插入到现有网络中。此功能使 FTD 可以安装在任何网络环境中，而无需配置相邻网络设备。内联接口无条件接收所有流量，但是，除非已明确丢弃，否则这些接口上接收的所有流量将在内嵌集外重传。

在分流模式下，FTD 会进行内联部署，但网络流量不受干扰。相反，FTD 会复制每个数据包，这样它就可以对数据包进行分析。请注意，这些类型的规则在触发时会生成入侵事件，而且入侵事件表视图显示了触发数据包会在内联部署中被丢弃。在已部署内联的 FTD 上使用分流模式有很多优点。例如，您可以设置 FTD 和网络之间的布线，就像 FTD 是内联，并分析 FTD 生成的多种入侵事件。根据结果，您可以修改入侵策略，并添加最好地保护您的网络却不影响有效性的丢弃规则。准备部署 FTD 内联时，您可以禁用分流模式，并开始丢弃可疑流量，而无需重新配置 FTD 和网络之间的走线。



注释 分流模式显著影响 FTD 性能，具体取决于流量。



注释 内嵌集可能是您所熟悉的“透明内联集”，但内联接口类型与透明防火墙模式或防火墙类型接口无关。

- 被动或 ERSPAN 被动 - 被动接口使用交换机 SPAN 或镜像端口监控网络中流动的流量。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 FTD，FTD 将无法执行某些操作，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。封装远程交换端口分析器 (ERSPAN) 接口允许您监控分布于多个交换机的源端口流量，并使用 GRE 来封装流量。仅当 FTD 处于路由防火墙模式时，才允许 ERSPAN 接口。



注释 由于混杂模式限制，某些使用 SR-IOV 驱动程序的 Intel 网络适配器（例如 Intel X710 或 82599）不支持在 NGFWv 上将 SR-IOV 接口用作被动接口。在此情况下，请使用支持此功能的网络适配器。有关英特尔网络适配器的详细信息，请参阅[英特尔以太网产品](#)。

安全区域和接口组

每个接口可以被分配给安全区域和/或接口组。然后，根据区域或组应用您的安全策略。例如，您可以把一个或多个设备上的“内部”接口分配到“内部”区域；而把“外部”接口分配到“外部”区域。然后，您可以配置访问控制策略，以便为使用相同区域的每台设备启用从内部区域到外部区域的流量。

要查看属于每个对象的接口，请选择**对象 (Objects) > 对象管理 (Object Management)**，然后点击**接口 (Interface)**。此页面列出受管设备上配置的区域安全区域和接口组。您可以展开每个接口对象以查看每个接口对象中的接口类型。



注释 适用于任何区域的策略（全局策略）也适用于区域中的接口以及未分配给区域的任何接口。



注释 管理接口不属于区域或接口组。

安全区域 vs. 接口组

有两种类型的接口对象：

- 安全区域 - 接口只能属于一个安全区域。
- 接口组 - 接口可属于多个接口组（和一个安全区域）。

您可以在 NAT 策略、预过滤器策略和 QoS 策略中使用接口组，也可以使用直接指定接口名称的功能，例如系统日志服务器或 DNS 服务器。

某些策略仅支持安全区域，而其他策略则支持区域和组。除非您需要接口组提供的功能，否则应默认使用安全区域，因为所有功能都支持安全区域。

不能将现有安全区域更改为接口组（反之亦然）；而必须创建新接口对象。



注释 尽管隧道区域不是接口对象，但您可以在某些配置中使用它们代替安全区域；请参阅[隧道区域与预过滤](#)。

接口对象类型

请参阅以下接口对象类型：

- 被动 - 适用于仅 IPS 被动或 ERSPAN 接口。
- 内联 - 适用于仅 IPS 内联集接口。
- 已交换 - 适用于常规防火墙网桥组接口。
- 已路由 - 适用于常规防火墙路由接口。
- ASA - （仅安全区域）适用于传统 ASA FirePOWER 设备接口。
- 管理 - （仅接口组）用于管理专用接口。
- 环回 - （仅限接口组）用于环回接口。

接口对象中的所有接口都必须为同一类型。创建接口对象后，不能更改其包含的接口类型。

接口名称

请注意，接口（或区域名称）本身不提供有关安全策略的任何默认行为。我们建议使用自描述的名称，以避免在未来的配置中出错。好的名称能表明逻辑网段或流量规范，例如：

- 内部接口的名称 - InsideV110、InsideV160、InsideV195
- DMZ 接口的名称 - DMZV11、DMZV12、DMZV-TEST
- 外部接口的名称 - Outside-ASN78、Outside-ASN91

接口对象和多租户

在多域部署中，您可以在任何级别创建接口对象。在祖先域中创建的区域接口对象可以包含位于不同域中的设备上的接口。在此情况下，在对象管理器中查看祖先接口对象配置的子域用户只能看到其域中的接口。

除非受角色限制，否则子域用户可以查看和编辑祖先域中创建的接口对象。子域用户可以从这些接口对象添加和删除接口。但是，他们无法删除或重命名接口对象。您既不能查看也不能编辑后代域中创建的接口对象。

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 和全值时，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。

接口默认设置

本部分列出接口的默认设置。

接口的默认状态

接口的默认状态取决于类型。

- 物理接口 - 已禁用。对初始设置启用的管理接口是个例外。
- 冗余接口 - 已启用。但是，要使流量通过冗余接口，还必须启用成员物理接口。
- VLAN 子接口 - 已启用。但是，要使流量通过子接口，还必须启用物理接口。
- EtherChannel port-channel 接口（ISA 3000）- 已启用。但是，要使流量通过 EtherChannel 接口，还必须启用通道组物理接口。
- EtherChannel 端口-通道接口（Firepower 和 Cisco Secure Firewall 型号）- 已禁用。



注释 对于 Firepower 4100/9300，您可以出于管理需要同时启用和禁用机箱和管理中心上的接口。为使接口正常运行，必须同时在两个操作系统中启用该接口。由于接口状态可独立控制，因此机箱与管理中心之间可能出现不匹配的情况。

默认速度和双工

默认情况下，铜缆（RJ-45）接口的速度和双工设置为自动协商。

默认情况下，光纤（SFP）接口的速度和双工会被设为最大速度，同时启用自动协商。

对于 Cisco Secure Firewall 3100/4200，速度设置为检测已安装的 SFP 速度。

创建安全区域和接口组对象

添加您可以为其分配设备接口的安全区域和接口组。



提示 可以创建空的接口对象并随后向其添加接口。要添加接口，该接口必须具有名称。您还可以配置接口时创建安全区域（但不是接口组）。

开始之前

了解每种类型的接口对象的使用要求和限制。请参阅[安全区域和接口组](#)，第 4 页。

过程

- 步骤 1 选择对象 > 对象管理。
- 步骤 2 从对象类型列表中选择接口。
- 步骤 3 点击添加 (Add) > 安全区域 (Security Zone) 或添加 (Add) > 接口组 (Interface Group)。
- 步骤 4 输入 Name。
- 步骤 5 选择接口类型 (Interface Type)。
- 步骤 6 (可选) 从设备 (Device) > 接口 (Interfaces) 下拉列表中，选择包含要添加的接口的设备。
您不需要在此屏幕上分配接口；您可以在配置接口时将接口分配给区域或组。
- 步骤 7 点击保存 (Save)。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅 [部署配置更改](#)。

启用物理接口并配置以太网参数

本节介绍如何执行以下操作：

- 启用物理接口。默认情况下，物理接口处于禁用状态（管理接口除外）。
- 设置特定的速度和复用。默认情况下，速度和复用设置为“自动”。

此过程仅涵盖一小部分接口设置。此时不能设置其他参数。例如，不能命名要用作 EtherChannel 接口一部分的接口。



注释 对于 Firepower 4100/9300，可在 FXOS 中配置基本接口设置。有关详细信息，请参阅 [配置物理接口](#)。



注释 有关 Firepower 1010 交换机端口，请参阅 [配置 Firepower 1010 交换机端口](#)。

开始之前

如果在将设备添加到管理中心后更改了设备上的物理接口，需要点击接口 (Interfaces) 左上角的从设备同步接口 (Sync Interfaces from device) 刷新接口列表。对于支持热插拔的 Cisco Secure Firewall 3100/4200，在更改设备上的接口之前，请参阅 [管理 Cisco Secure Firewall 3100/4200 的网络模块](#)，第 20 页。

过程

- 步骤 1** 依次选择设备 (**Devices**) > 设备管理 (**Device Management**), 并点击 威胁防御 设备的 编辑 (✎)。系统默认选择接口 (**Interfaces**) 页面。
- 步骤 2** 点击要编辑的接口的 编辑 (✎)。
- 步骤 3** 选中启用复选框以启用此接口。
- 步骤 4** (可选) 在说明字段中添加说明。
一行说明最多可包含 200 个字符 (不包括回车符)。

- 步骤 5** (可选) 通过点击 硬件配置 (**Hardware Configuration**) > 速度 (**Speed**), 设置复用和速度。

- 复用-选择全 或 半。SFP 接口仅支持全 复用。
- 速度-选择速度 (因型号而异)。(仅限 Cisco Secure Firewall 3100/4200) 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。
- 自动协商-设置接口以协商速度、链路状态和流量控制。
- 前向纠错模式-(仅限 Cisco Secure Firewall 3100/4200) 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 FEC, 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
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
25/50/100G	Clause 91 RS-FEC	Clause 91 RS-FEC

- 步骤 6** (可选) (Firepower 1100/2100、Cisco Secure Firewall 3100/4200) 通过点击 硬件配置 (**Hardware Configuration**) > 网络连接 (**Network Connectivity**) 启用链路层发现协议 (LLDP)。
- 启用 LLDP 接收-启用防火墙以从其对等体接收 LLDP 数据包。
 - 启用 LLDP 传输-启用防火墙以将 LLDP 数据包发送到其对等体。

步骤 7 (可选) (Cisco Secure Firewall 3100/4200) 通过点击 **硬件配置 (Hardware Configuration) > 网络连接 (Network Connectivity)**, 然后选中 **流量控制发送 (Flow Control Send)** 来为流量控制启用暂停 (XOFF) 帧。

流量控制通过允许拥塞节点在另一端暂停链路操作, 从而让连接的以太网端口能够在拥塞期间控制流量速率。如果威胁防御端口遇到拥塞 (内部交换机上的排队资源耗尽) 并且无法接收更多流量, 则它会通过发送暂停帧来通知另一个端口停止发送, 直到状况恢复正常为止。在收到暂停帧后, 发送设备会停止发送任何数据包, 从而防止在拥塞期间丢失任何数据包。

注释 威胁防御 支持传输暂停帧, 以便远程对等体可以对流量进行速率控制。

但是, 不支持接收暂停帧。

内部交换机有一个包含 8000 个缓冲区的全局池, 而每个缓冲区都有 250 个字节, 并且交换机会为每个端口动态分配缓冲区。当缓冲区使用量超过全局高水位标记 (2 MB [8000 个缓冲区]) 时, 会在每个启用了流量控制的接口上发送暂停帧; 当特定接口的缓冲区超过端口高水位标记 (0.3125 MB [1250 个缓冲区]) 时, 会从该接口发送暂停帧。在发送暂停后, 如果缓冲区使用率降低至低水位标记之下 (全局 1.25 MB [5000 个缓冲区]; 每个端口 0.25 MB [1000 buffers]), 则可发送 XON 帧。链接伙伴可在收到 XON 帧之后恢复流量。

系统仅支持 802.3x 中定义的流量控制帧。系统不支持基于优先级的流量控制。

步骤 8 在 **模式** 下拉列表中, 选择以下选项之一:

- **无** - 为常规防火墙接口和内联集选择此设置。该模式将基于后续配置自动更改为路由、交换或内联。
- **被动** - 为被动仅限 IPS 接口选择此设置。
- **Ersparn** - 为 ERSPAN 被动仅限 IPS 接口选择此设置。

步骤 9 在 **优先级** 字段中, 输入一个介于 0 和 65535 之间的数字。

此值在策略型路由配置中使用。优先级用于确定如何跨多个出口接口分配流量。

步骤 10 点击 **确定 (OK)**。

步骤 11 点击 **保存 (Save)**。

此时, 您可以转至 **部署 > 部署** 并将策略部署到所分配的设备。在部署更改之后, 更改才生效。

步骤 12 继续配置接口。

- [常规防火墙接口](#)
- [内联集和被动接口](#)

配置 EtherChannel 接口

本节介绍如何配置 EtherChannel 接口。



注释 对于 Firepower 4100/9300，可在 FXOS 中配置 EtherChannel。有关详细信息，请参阅[添加 EtherChannel（端口通道）](#)。

关于 EtherChannels

本节介绍 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

各信道组最多可以有 8 个活动接口，但 ISA 3000 除外，支持 16 个活动接口。对于仅支持 8 个主用接口的交换机，您最多可以将 16 个接口分配给一个通道组；但仅有 8 个接口可用作主用接口，其余接口在出现接口故障的情况下用作备用链路。

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。

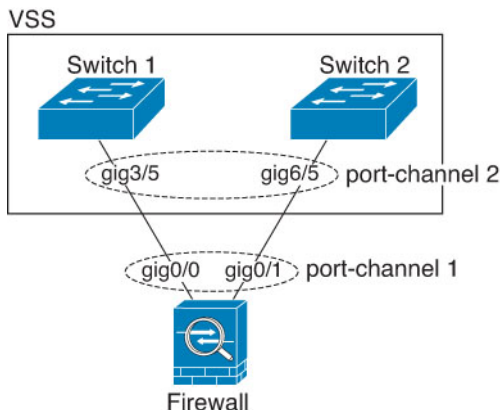
EtherChannel 汇聚通道中所有可用活动接口上的流量。系统根据源或目标 MAC 地址、IP 地址、TCP 端口号、UDP 端口号和 VLAN 编号使用专有散列算法来选择接口。

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。

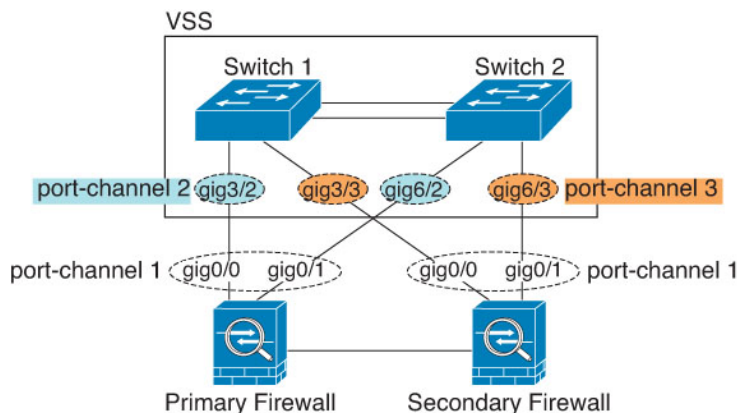
图 1: 连接至 VSS/vPC



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，则需要在 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。
- **被动** - 接收 LACP 更新。备用 EtherChannel 只能与主用 EtherChannel 建立连接。在硬件型号上不受支持。
- **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，因此故障转移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

在路由模式下，不支持将管理中心-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）均需在两台设备上进行预配置。
- 可以使用 **monitor-interface** 命令监控 EtherChannel 成员接口以实现高可用性。如果主用成员接口故障转移到备用接口，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（对于 EtherChannel 接口，可配置允许出现故障的成员接口数量）。
- 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

- 无法在管理中心中添加用于 Firepower 4100/9300 或 threat defense virtual 的 EtherChannel。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。
- 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。
- 各信道组最多可以有 8 个活动接口，但 ISA 3000 除外，支持 16 个活动接口。对于仅支持 8 个主用接口的交换机，您最多可以将 16 个接口分配给一个通道组；但仅有 8 个接口可用作主用接口，其余接口在出现接口故障的情况下用作备用链路。
- 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 3100/4200 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。
- 设备不支持 LACP 快速速率，但 ISA 3000 除外；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。

- 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。

配置 EtherChannel

本节介绍如何创建 EtherChannel 端口通道接口，如何向 EtherChannel 分配接口，以及如何自定义 EtherChannel。

准则

- 最多可以配置 48 个 Etherchannel，具体取决于型号具有的接口数量。
- 各信道组最多可以有 8 个活动接口，但 ISA 3000 除外，支持 16 个活动接口。对于仅支持 8 个主用接口的交换机，您最多可以将 16 个接口分配给一个通道组；但仅有 8 个接口可用作主用接口，其余接口在出现接口故障的情况下用作备用链路。
- 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 3100/4200 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。



注释 对于 Firepower 4100/9300，可在 FXOS 中配置 EtherChannel。有关详细信息，请参阅[添加 EtherChannel（端口通道）](#)。

开始之前

- 如果已为物理接口配置了名称，则不能将该物理接口添加到通道组。您必须先删除该名称。



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

过程

- 步骤 1** 依次选择设备 (**Devices**) > 设备管理 (**Device Management**)，并点击威胁防御设备的编辑 (✎)。系统默认选择接口 (**Interfaces**) 页面。
- 步骤 2** 根据[启用物理接口并配置以太网参数](#)，第 7 页启用成员接口。

步骤 3 点击添加接口 (**Add Interfaces**) > 以太通道接口 (**Ether Channel Interface**)。

步骤 4 在 **常规** 选项卡上，将 **以太通道 ID** 设置为介于 1 和 48 之间的数字（1-8 针对于 Firepower 1010）。

图 3: 添加以太网通道接口

The screenshot shows the 'Add Ether Channel Interface' configuration window. The 'General' tab is active. The configuration is as follows:

- Name: dmz
- Enabled:
- Management Only:
- Description: (empty)
- Mode: None
- Security Zone: dmz_zone
- MTU: 1500 (range: 64 - 9198)
- Priority: 0 (range: 0 - 65535)
- Propagate Security Group Tag:
- Ether Channel ID *: 1

Buttons: Cancel, OK

步骤 5 在可用接口 (**Available Interfaces**) 区域中，点击某个接口对，然后点击添加 (**Add**)，以将其移动至选定的接口 (**Selected Interfaces**) 区域。对要使其成为成员的所有接口重复此步骤。

确保所有接口的类型和速度相同。

图 4: 可用接口

步骤 6 (可选) 点击高级 (**Advanced**) 选项卡可自定义 EtherChannel。在信息子选项卡上设置下列参数:

图 5: 高级

- (仅限 ISA 3000) **负载均衡**-选择在组通道接口之间对数据包进行负载均衡所用的标准。默认情况下, 威胁防御 根据数据包的源 IP 地址和目标 IP 地址来均衡接口上的数据包负载。如果要更改分类数据包所依据的属性, 请选择另一组条件。例如, 如果流量严重偏向于相同的源 IP 地址和目标 IP 地址, 则分配给 EtherChannel 中的接口的流量将失去平衡。更改为其他算法可使流量分布更均匀。有关负载均衡的详细信息, 请参阅[负载均衡](#), 第 12 页。
- **LACP 模式** - 选择“主动”、“被动”或“启用”。我们建议使用 Active 模式 (默认)。
- (仅限 ISA 3000) **主用物理接口: 范围**-从左侧的下拉列表中, 选择 EtherChannel 要作为主用接口所需的最小主用接口数量 (1 到 16)。默认值为 1。从右侧的下拉列表中, 选择 EtherChannel 中允许的最大主用接口数量 (1 到 16)。默认值为 16。如果交换机不支持 16 个主用接口, 请务必将此命令设置为 8 或更小的值。
- **主用 Mac 地址** - 如果需要, 请设置手动 MAC 地址。mac_address 的格式为 H.H.H, 其中 H 是 16 位十六进制数字。例如, MAC 地址 00-0C-F1-42-4C-DE 以 000C.F142.4CDE 的形式输入。

步骤 7 点击**硬件配置 (Hardware Configuration)** 选项卡，并为所有成员接口设置复用和速度。

步骤 8 点击 **OK**。

步骤 9 点击**保存 (Save)**。

此时，您可以转至**部署 > 部署**并将策略部署到所分配的设备。在部署更改之后，更改才生效。

步骤 10 （可选）添加 VLAN 子接口请参阅[添加子接口](#)。

步骤 11 配置路由或透明模式接口参数。请参阅[配置路由模式接口](#)或[配置网桥组接口](#)。

与管理中心同步接口更改

在设备上进行的接口配置更改可能导致 管理中心 和设备不同步。管理中心 可以通过以下方法之一检测到接口更改：

- 设备发送的事件
- 部署时同步 管理中心
 - 当 管理中心 尝试部署时检测到接口更改，部署将失败。必须先接受接口更改。
- 手动同步

在 管理中心 外部执行的两种类型的接口更改需要同步：

- 添加或删除物理接口-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。删除接口将删除与该接口相关的任何配置。引用安全区域的策略不受影响。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 管理中心 上进行同步。

当 管理中心 检测到更改时，“**接口**”页面会在每个接口左侧显示状态（已删除、已更改或已添加）。

- 管理中心 访问接口更改-如果使用 命令配置用于管理管理中心 FMC 的数据接口，则必须在管理中心 FMC 中手动进行匹配的配置更改，然后确认更改。**configure network management-data-interface** 这些接口更改无法自动进行。

本程序介绍在需要时如何手动同步设备以及如何确认检测到的更改。如果设备更改为临时性的，则不应在 管理中心 中保存更改；而应等待设备稳定后重新同步。

开始之前

- 用户角色：
 - 管理员
 - 访问管理员
 - 网络管理员

过程

步骤 1 依次选择设备 (Devices) > 设备管理 (Device Management)，并点击 威胁防御 设备的 编辑 (✎)。系统默认选择接口 (Interfaces) 页面。

步骤 2 如果需要，请点击 接口左上方的 同步设备。

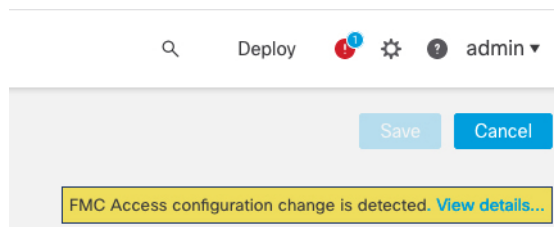
步骤 3 检测到更改后，请参阅以下步骤。

添加或删除物理接口

- 您可以在 接口 上看到红色横幅，表明接口配置已发生更改。点击[了解详情](#)链接以查看接口更改。
- 点击**验证更改 (Validate Changes)** 以确保策略在接口更改后仍有效。
如出现任何错误，则需要更改配置并重新运行验证。
- 点击**保存 (Save)**。
此时，您可以转至**部署 > 部署**并将策略部署到所分配的设备。

FMC 访问接口更改

- 您将在“设备”页面的右上角看到一个黄色横幅，指示 管理中心 访问配置已更改。点击 [查看详情](#) 链接以查看接口更改。



系统将打开 **FMC 访问 - 配置详细信息** 对话框。

- 记下所有突出显示的配置，尤其是粉红色突出显示的配置。您需要通过在 管理中心上手动配置来匹配 威胁防御 上的任何值。

例如，下面的粉红色突出显示 威胁防御 上存在但尚不存在于 管理中心的配置。

FMC Access - Configuration Details ? x

FMC Access configuration on device have been updated outside of FMC. Review the differences and update FMC values accordingly.

Configuration CLI Output Connection Status

Last updated: 2020-06-23 at 23:36:16 UTC [Refresh]

	Configuration on FMC	Configuration on Device
Host Name		
Method Name		
DDNS - Update Methods		
Method Type		
Web URL		
Web Update Type		
▼ 4. GigabitEthernet1/1		
Interface Configuration		
FMC Access Enabled	Disabled	Enabled
FMC Access - Allowed Networks		any
Interface Name		outside
IPv4/IPv6 Address		10.89.5.29 255.255.255.192
Static Route Configuration		
IPv4 Gateway		10.89.5.1
IPv6 Gateway		

Legend: Above configurations will be ■ added, ■ modified or ■ disassociated from FMC Access interface on next deploy to FTD.

Acknowledge Close

以下示例显示在管理中心中配置接口后的此页面；接口设置匹配，并且已删除粉红色突出显示。

FMC Access - Configuration Details ? x

FMC Access configuration on device have been updated outside of FMC. Review the differences and update FMC values accordingly.

Configuration CLI Output Connection Status

Last updated: 2020-06-23 at 23:36:16 UTC [Refresh]

	Configuration on FMC	Configuration on Device
Host Name		
Method Name		
DDNS - Update Methods		
Method Type		
Web URL		
Web Update Type		
▼ 4. GigabitEthernet1/1		
Interface Configuration		
FMC Access Enabled	Enabled	Enabled
FMC Access - Allowed Networks	any	any
Interface Name	outside	outside
IPv4/IPv6 Address	10.89.5.29 255.255.255.192	10.89.5.29 255.255.255.192
Static Route Configuration		
IPv4 Gateway		10.89.5.1
IPv6 Gateway		

Legend: Above configurations will be ■ added, ■ modified or ■ disassociated from FMC Access interface on next deploy to FTD.

Acknowledge Close

c) 点击 **确认**。

我们建议您在完成管理中心配置并准备部署之前，不要点击 **确认**。点击 **确认** 将删除部署阻止。下次部署时，管理中心配置将覆盖威胁防御上任何剩余的冲突设置。在您重新部署之前，您有责任在管理中心中手动修复配置。

d) 此时，您可以转至部署 > 部署并将策略部署到所分配的设备。

管理 Cisco Secure Firewall 3100/4200 的网络模块

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




要查看设备的物理接口详细信息并管理网络模块，请打开机箱操作 (Chassis Operations) 页面。从设备 > 设备管理，点击机箱列中的管理。对于集群或高可用性，此选项仅适用于控制节点/主用设备。系统将打开设备 机箱操作 页面。

图 6: 机箱操作

172.16.0.51 (Chassis Operations)
Network module and interface breakout details for device.

Interfaces

Refresh Sync Modules

 CONSOLE
 MGMT
 USB

Network Module 1

1/11/21/31/41/51/61/71/8

1/91/101/111/121/131/141/151/16

Network Module 2

2/12/32/52/7

2/22/42/62/8

Physical Interfaces

This view lists only the physical interfaces to perform chassis related advanced operations. To view complete list of physical and logical interfaces, navigate to [Interface page in device details](#)

Interface Name	Duplex	Auto Negotiation	Admin FEC	Admin Speed	Media Type
Ethernet1/1	FULL	No	AUTO	1gbps	rj45
Ethernet1/2	FULL	No	AUTO	1gbps	rj45
Ethernet1/3	FULL	No	AUTO	1gbps	rj45
Ethernet1/4	FULL	No	AUTO	1gbps	rj45

点击 **刷新** 以刷新接口状态。如果您在需要检测的设备上进行了硬件更改，请点击 **同步模块**。

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。

更改会立即生效；您不需要部署到设备。在中断或重新加入后，您无法回滚到之前的接口状态。

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。
- 在中断或重新加入之前，接口不能用于以下对象：
 - 故障切换链路
 - 集群控制链路
 - 拥有一个子接口
 - EtherChannel 成员
 - BVI 成员
 - 管理器访问接口
- 中断或重新加入直接用于安全策略中的接口可能会影响配置；但是，操作不会被阻止。

过程

步骤 1 从 **设备 > 设备管理**，点击**机箱**列中的**管理**。对于集群或高可用性，此选项仅适用于控制节点/主用设备；网络模块的更改会被复制到所有的节点。

图 7: 管理机箱

<input type="checkbox"/>	Name	Model	Version	Chassis
<input type="checkbox"/>	Ungrouped (2)			
<input type="checkbox"/>	172.16.0.51 Snort 3 172.16.0.51 - Transparent	Firewall 3120 Threat Defense	7.1.0	Manage

系统将打开设备的**机箱操作**页面（在多实例模式下，此页面称为**机箱管理器**）。此页面会显示设备的物理接口详细信息。

步骤 2 从 40GB 或更高的接口分支出 10GB 端口。

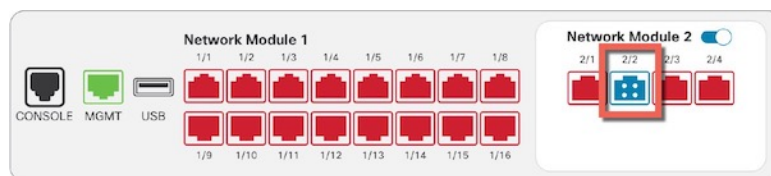
a) 点击接口右侧的**中断**（）。

在确认对话框中点击**是 (Yes)**。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，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：

图 8: 分支端口



- b) 点击屏幕顶部消息中的链接，转至接口 (**Interfaces**) 页面以保存接口更改。

图 9: 转到接口页面

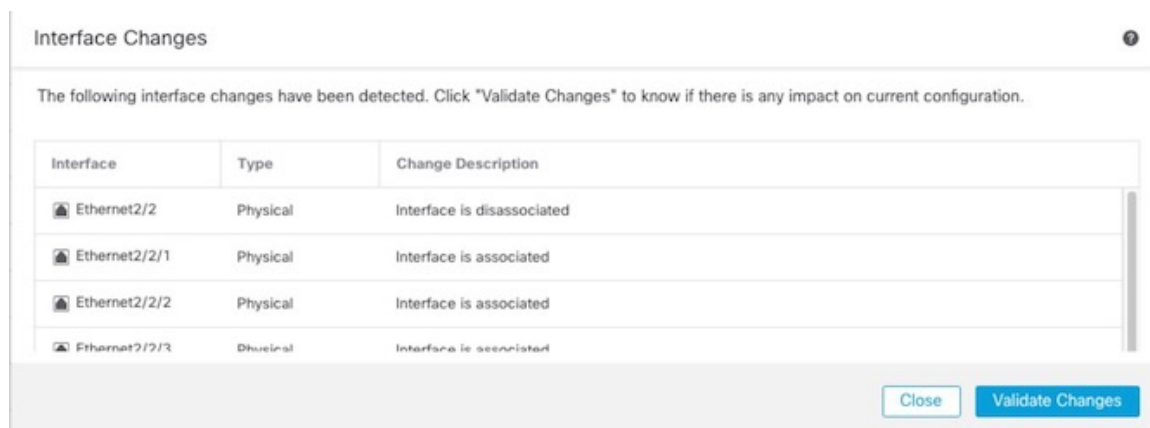
▲ This device has configuration changes that were performed directly on the device. Visit [Interface page in device details](#)

- c) 在接口 (**Interfaces**) 页面顶部，点击点击了解更多信息 (**Click to know more**)。系统将打开接口更改 (**Interface Changes**) 对话框。

图 10: 查看接口更改

Interface configuration has changed on device. [Click to know more.](#)

图 11: 接口更改



- d) 点击验证更改 (**Validate Changes**) 以确保策略在接口更改后仍有效。

如出现任何错误，则需要更改配置并重新运行验证。

但是，删除安全策略中使用的接口会对配置造成影响。可以直接在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。删除接口将删除与该接口相关的任何配置。引用安全区域的策略不受影响。

- e) 点击关闭 (**Close**) 返回接口 (**Interfaces**) 页面。
 f) 点击保存 (**Save**)，以便将接口更改保存到防火墙。
 g) 如果您必须更改任何配置，请转至部署 (**Deploy**) > 部署 (**Deployment**) 并部署策略。

您无需部署即可保存分支端口更改。

步骤 3 重新加入分支端口。

您必须重新加入该接口的所有子端口。

- a) 点击接口右侧的 **加入** (➔)。

在确认对话框中点击**是 (Yes)**。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。

- b) 点击屏幕顶部消息中的链接，转至**接口 (Interfaces)** 页面以保存接口更改。

图 12: 转到接口页面

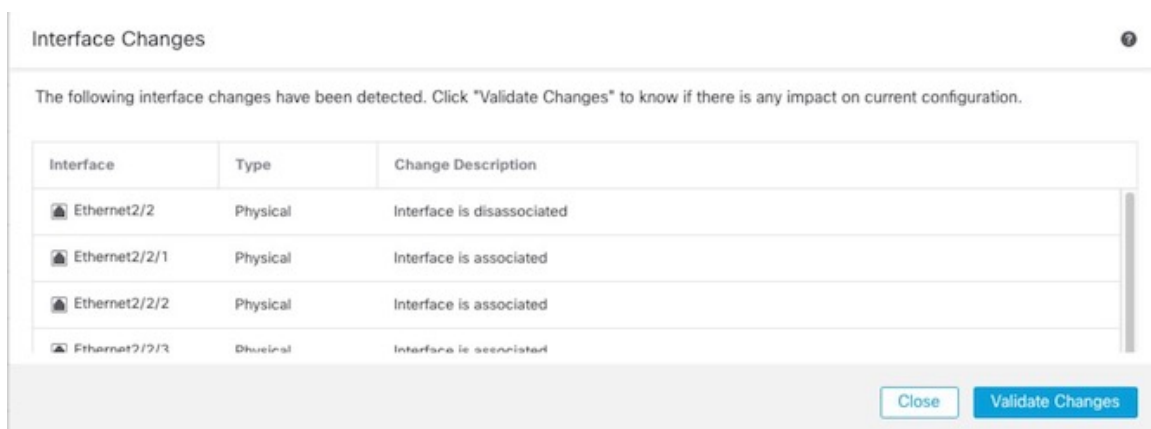
▲ This device has configuration changes that were performed directly on the device. Visit [Interface page in device details](#)

- c) 在**接口 (Interfaces)** 页面顶部，点击**点击了解更多信息 (Click to know more)**。系统将打开**接口更改 (Interface Changes)** 对话框。

图 13: 查看接口更改

Interface configuration has changed on device. [Click to know more.](#)

图 14: 接口更改



- d) 点击**验证更改 (Validate Changes)** 以确保策略在接口更改后仍有效。

如出现任何错误，则需要更改配置并重新运行验证。

替换安全策略中使用的子接口可能会对配置造成影响。可以直接在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。删除接口将删除与该接口相关的任何配置。引用安全区域的策略不受影响。

- e) 点击**关闭 (Close)** 返回**接口 (Interfaces)** 页面。
 f) 点击**保存 (Save)**，以便将接口更改保存到防火墙。
 g) 如果您必须更改任何配置，请转至**部署 (Deploy) > 部署 (Deployment)** 并部署策略。

您无需部署即可保存分支端口更改。

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。

对于集群或高可用性，请在所有节点上安装网络模块。

步骤 2 重新启动防火墙；请参阅[关闭或重新启动设备](#)。

对于集群或高可用性，请首先重新启动数据节点/备用设备，然后等待它们重新启动。然后，您可以更改控制节点（请参阅[更改控制节点](#)）或主用设备（请参阅[在威胁防御高可用性对中切换主用对等体](#)），并重新启动之前的控制节点/主用设备。

步骤 3 从 **设备 > 设备管理**，点击**机箱**列中的**管理**。对于集群或高可用性，此选项仅适用于控制节点/主用设备；网络模块的更改会被复制到所有的节点。

图 15: 管理机箱

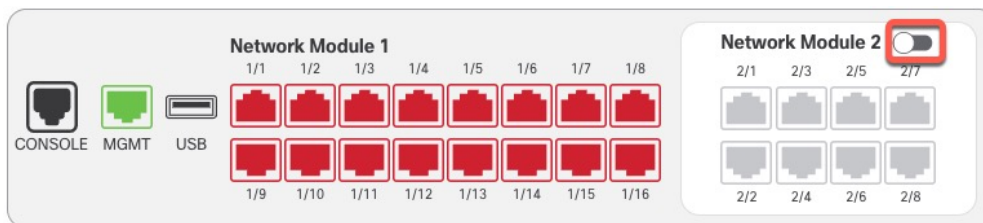
<input type="checkbox"/>	Name	Model	Version	Chassis
<input type="checkbox"/>	Ungrouped (2)			
<input type="checkbox"/>	172.16.0.51 Snort 3 172.16.0.51 - Transparent	Firewall 3120 Threat Defense	7.1.0	Manage

系统将打开设备 **机箱操作** 页面。此页面会显示设备的物理接口详细信息。

步骤 4 点击**同步模块 (Sync Modules)**，使用新的网络模块详细信息更新页面。

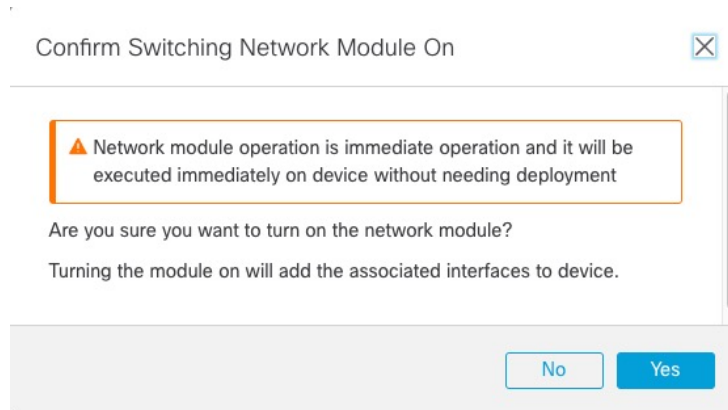
步骤 5 在接口图形上，点击滑块（）以启用网络模块。

图 16: 启用网络模块



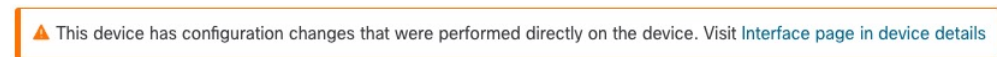
步骤 6 系统将提示您确认是否要开启网络模块。点击 **Yes**。

图 17: 确认启用



步骤 7 您会在屏幕顶部看到一条消息；点击链接可转至**接口 (Interfaces)** 页面以保存接口更改。

图 18: 转到接口页面



步骤 8 (可选) 在**接口 (Interfaces)** 页面顶部，您会看到接口配置已更改的消息。您可以点击**了解更多 (Click to know more)** 打开**接口更改 (Interface Changes)** 对话框以查看更改。

图 19: 查看接口更改

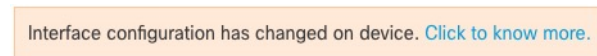
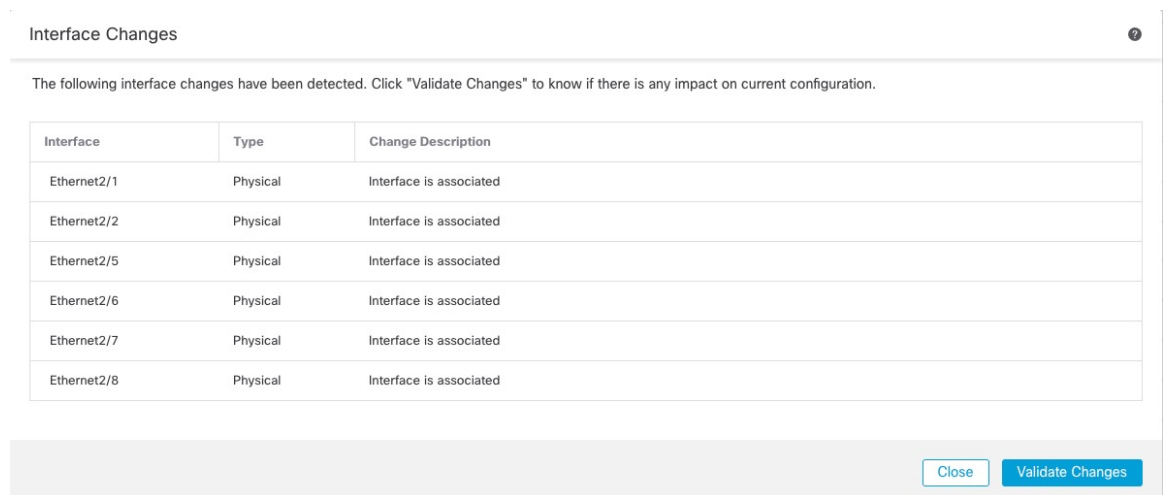


图 20: 接口更改



点击**关闭 (Close)** 返回**接口 (Interfaces)** 页面。(由于您要添加新模块，因此不应有任何配置影响，所以您无需点击**验证更改 (Validate Changes)**。)

步骤 9 点击**保存 (Save)**，以便将接口更改保存到防火墙。

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。

对于群集或高可用性，您只能在控制节点/主用设备上执行机箱操作。如果群集控制链路/故障转移链路在模块上，则不能禁用该模块。

开始之前

过程

步骤 1 对于群集或高可用性，请执行以下步骤。

- **群集 (Clustering)** - 确保要执行热插拔的设备是数据节点（请参阅[更改控制节点](#)）；然后中断节点，使其不再位于群集中。请参阅[中断节点](#)。

在执行热插拔后，您需要将节点添加回群集。或者，您可以在控制节点上执行所有操作，然后网络模块更改将同步到所有数据节点。但在热插拔期间，您将无法在所有节点上使用这些接口。

- **高可用性 (High Availability)** - 要在禁用网络模块时避免故障切换，请执行以下操作：
 - 如果故障切换链路位于网络模块上，则必须中断高可用性。请参阅[中断高可用性对](#)。不允许禁用具有主动故障转移链路的网络模块。
 - 对网络模块上的接口禁用接口监控。请参阅[配置备用 IP 地址和接口监控](#)。

步骤 2 从 **设备 > 设备管理**，点击**机箱** 列中的 **管理**。对于群集或高可用性，此选项仅适用于控制节点/主用设备；网络模块的更改会被复制到所有的节点。

图 21: 管理机箱

<input type="checkbox"/>	Name	Model	Version	Chassis
<input type="checkbox"/>	▼ Ungrouped (2)			
<input type="checkbox"/>	172.16.0.51 Snort 3 172.16.0.51 - Transparent	Firewall 3120 Threat Defense	7.1.0	Manage

系统将打开设备 **机箱操作** 页面。此页面会显示设备的物理接口详细信息。


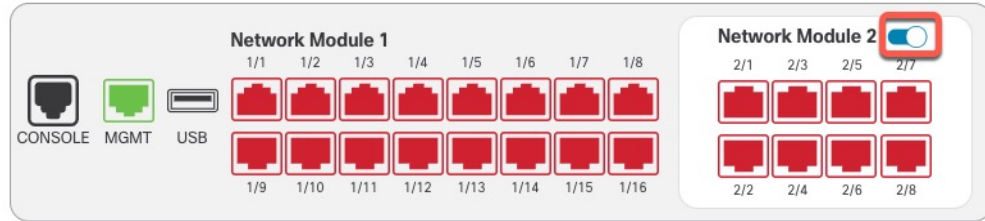
步骤 3 在接口图形上，点击滑块（）以禁用网络模块。

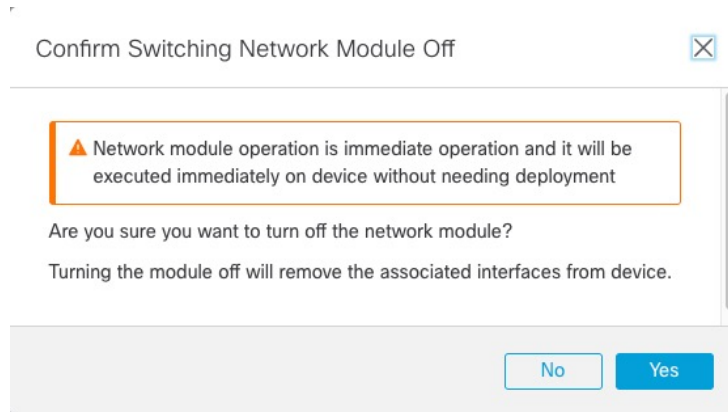
图 22: 禁用网络模块



不要在接口 (**Interfaces**) 页面上保存任何更改。由于您要更换网络模块，因此您不会希望中断任何现有配置。

步骤 4 系统将提示您确认是否要关闭网络模块。点击 **Yes**。

图 23: 确认禁用



步骤 5 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。


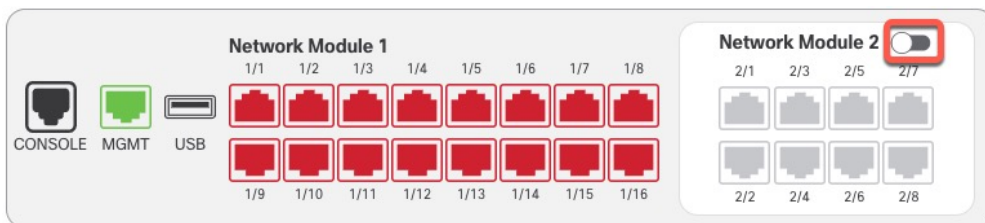
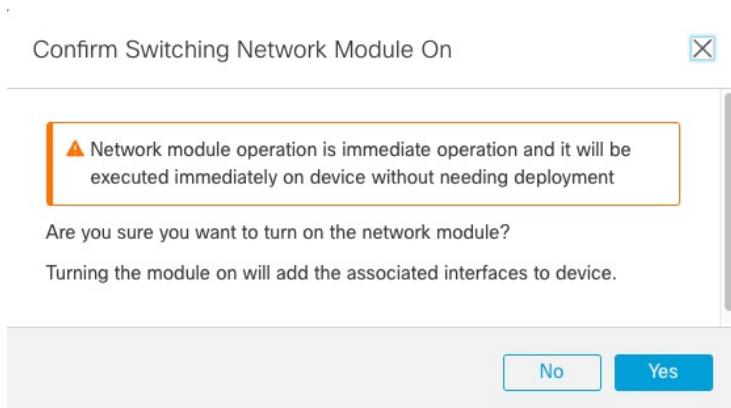
步骤 6 在管理中心中，通过点击滑块 () 来启用新模块。

图 24: 启用网络模块



步骤 7 系统将提示您确认是否要开启网络模块。点击 **Yes**。

图 25: 确认启用



步骤 8 对于集群或高可用性，请执行以下步骤。

- **集群 (Clustering)** - 将节点添加回集群。请参阅[添加新的集群节点](#)。
- **高可用性 (High Availability)** -
 - 如果您中断了高可用性，则要重新构建高可用性。请参阅[添加高可用性对](#)。
 - 为网络模块上的接口重新启用接口监控。请参阅[配置备用 IP 地址和接口监控](#)。

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。

对于集群或高可用性，您只能在控制节点/主用设备上执行机箱操作。

开始之前

对于高可用性，如果故障切换链路在模块上，则不能禁用该网络模块。您必须中断高可用性（请参阅[中断高可用性对](#)），这意味着您会在重新启动主用设备时遇到停机。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 对于集群或高可用性，请执行以下步骤。

- **集群** - 为避免停机，您可以一次中断每个节点，使其在执行网络模块更换时不再位于集群中。请参阅[中断节点](#)。

执行替换后，您需要将节点添加回集群。

- **高可用性** - 要在更换网络模块时避免故障转移，请对网络模块上的接口禁用接口监控。请参阅 [配置备用 IP 地址和接口监控](#)。

步骤 2 从 **设备 > 设备管理**，点击**机箱** 列中的 **管理**。对于集群或高可用性，此选项仅适用于控制节点/主用设备；网络模块的更改会被复制到所有的节点。

图 26: 管理机箱

<input type="checkbox"/>	Name	Model	Version	Chassis
<input type="checkbox"/>	Ungrouped (2)			
<input type="checkbox"/>	172.16.0.51 Snort 3 172.16.0.51 - Transparent	Firewall 3120 Threat Defense	7.1.0	Manage

系统将打开设备 **机箱操作** 页面。此页面会显示设备的物理接口详细信息。


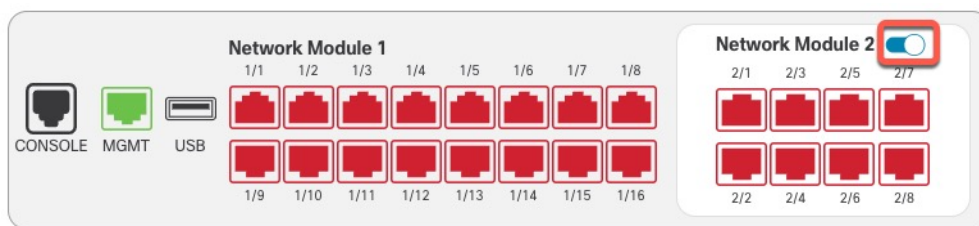
步骤 3 在接口图形上，点击滑块 () 以禁用网络模块。

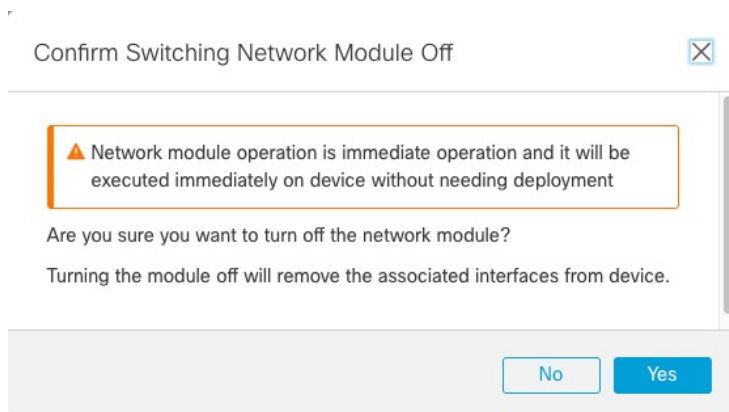
图 27: 禁用网络模块



不要在**接口 (Interfaces)** 页面上保存任何更改。由于您要更换网络模块，因此您不会希望中断任何现有配置。

步骤 4 系统将提示您确认是否要关闭网络模块。点击 **Yes**。

图 28: 确认禁用



步骤 5 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 6 重新启动防火墙；请参阅 [关闭或重新启动设备](#)。

对于集群或高可用性，请首先重新启动数据节点/备用设备，然后等待它们重新启动。然后，您可以更改控制节点（请参阅[更改控制节点](#)）或主用设备（请参阅[在威胁防御高可用性对中切换主用对等体](#)），并重新启动之前的控制节点/主用设备。

步骤 7 在管理中心中，点击同步模块 (Sync Modules) 以便使用新的网络模块详细信息来更新页面。


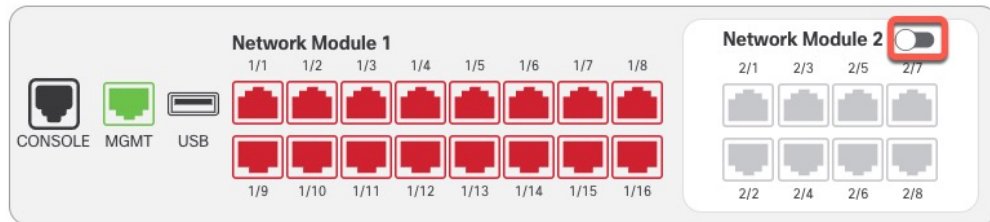
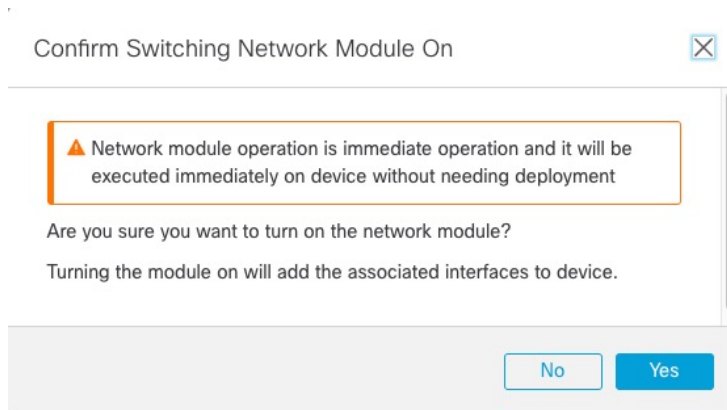
步骤 8 通过点击滑块启用新模块（）。

图 29: 启用网络模块



步骤 9 系统将提示您确认是否要开启网络模块。点击 **Yes**。

图 30: 确认启用



步骤 10 点击屏幕顶部消息中的链接，转至接口 (Interfaces) 页面以保存接口更改。

图 31: 转到接口页面

 This device has configuration changes that were performed directly on the device. Visit [Interface page in device details](#)

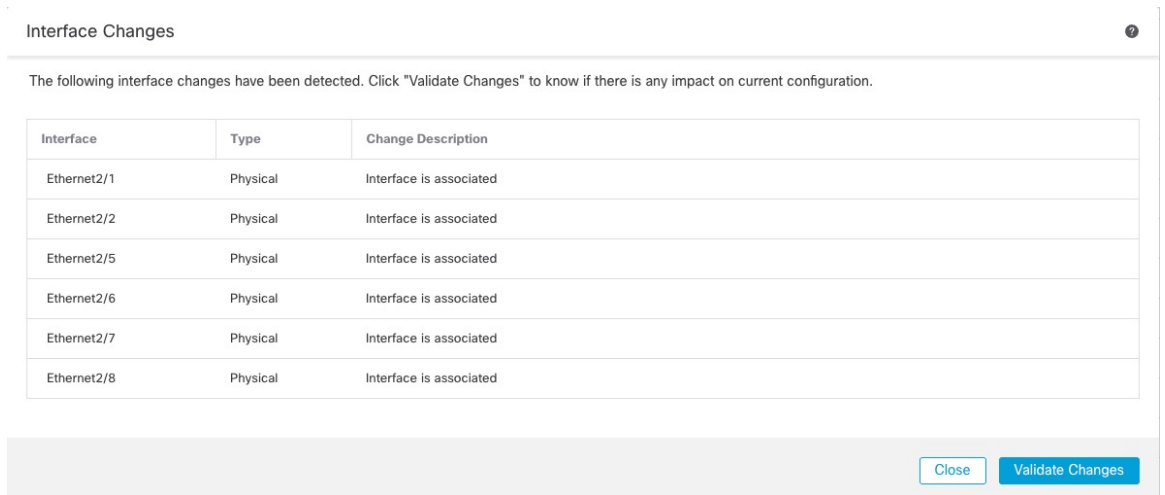
步骤 11 如果网络模块的接口较少：

a) 在接口 (Interfaces) 页面顶部，点击[点击了解更多信息 \(Click to know more\)](#)。系统将打开接口更改 (Interface Changes) 对话框。

图 32: 查看接口更改

Interface configuration has changed on device. [Click to know more.](#)

图 33: 接口更改



b) 点击**验证更改 (Validate Changes)** 以确保策略在接口更改后仍有效。

如出现任何错误，则需要更改配置并重新运行验证。

删除安全策略中使用的接口会影响配置。可以直接在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。删除接口将删除与该接口相关的任何配置。引用安全区域的策略不受影响。

c) 点击**关闭 (Close)** 返回**接口 (Interfaces)** 页面。

步骤 12 要更改接口速度，请参阅 [启用物理接口并配置以太网参数](#)，第 7 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 13 点击**保存 (Save)**，以便将接口更改保存到防火墙。

步骤 14 如果您必须更改任何配置，请转至**部署 (Deploy) > 部署 (Deployment)** 并部署策略。

无需部署即可保存网络模块更改。

步骤 15 对于集群或高可用性，请执行以下步骤。

- **群集 (Clustering)** - 将节点添加回集群。请参阅[添加新的集群节点](#)。
- **高可用性 (High Availability)** - 对网络模块上的接口重新启用接口监控。请参阅[配置备用 IP 地址和接口监控](#)。

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。

对于群集或高可用性，您只能在控制节点/主用设备上执行机箱操作。

开始之前

对于集群或高可用性，请确保集群/故障转移链路不在网络模块上。

过程

步骤 1 从 **设备 > 设备管理**，点击**机箱** 列中的 **管理**。对于集群或高可用性，此选项仅适用于控制节点/主用设备；网络模块的更改会被复制到所有的节点。

图 34: 管理机箱

<input type="checkbox"/>	Name	Model	Version	Chassis
<input type="checkbox"/>	Ungrouped (2)			
<input type="checkbox"/>	172.16.0.51 Snort 3 172.16.0.51 - Transparent	Firewall 3120 Threat Defense	7.1.0	Manage

系统将打开设备 **机箱操作** 页面。此页面会显示设备的物理接口详细信息。


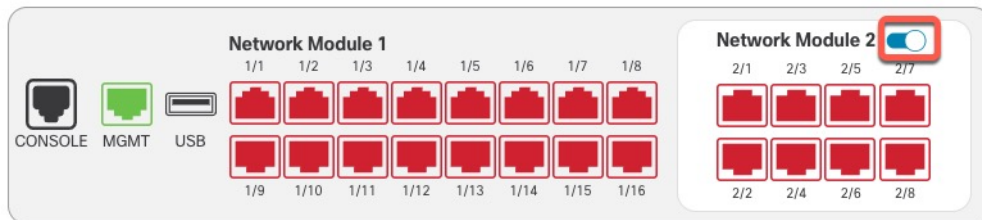
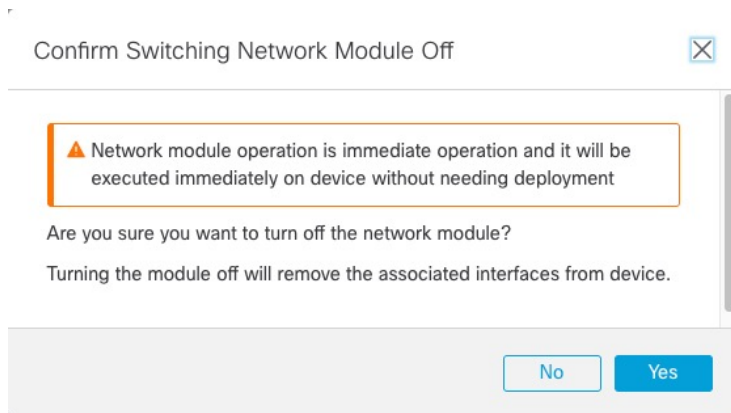
步骤 2 在接口图形上，点击滑块（）以禁用网络模块。

图 35: 禁用网络模块



步骤 3 系统将提示您确认是否要关闭网络模块。点击 **Yes**。

图 36: 确认禁用



步骤 4 您会在屏幕顶部看到一条消息；点击链接可转至**接口 (Interfaces)** 页面以保存接口更改。

图 37: 转到接口页面

▲ This device has configuration changes that were performed directly on the device. Visit [Interface page in device details](#)

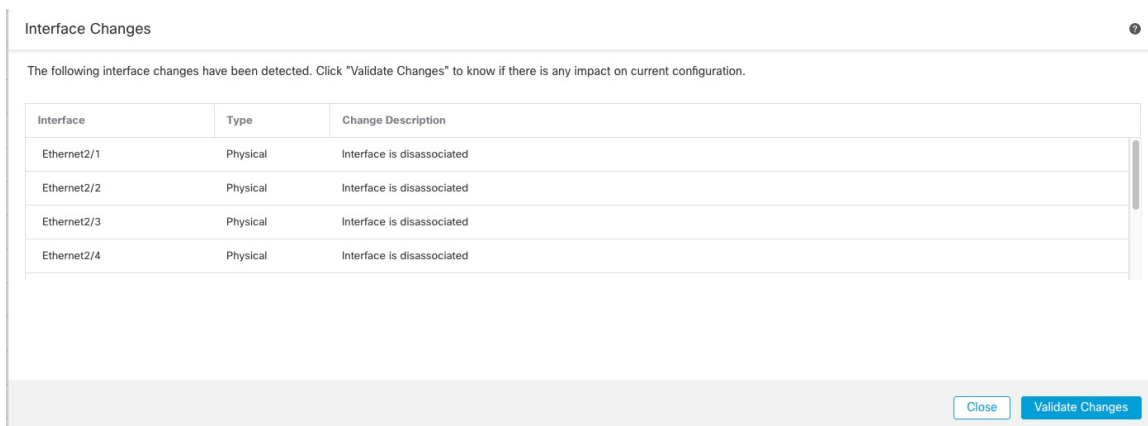
步骤 5 在接口 (**Interfaces**) 页面顶部，您会看到接口配置已更改的消息。

图 38: 查看接口更改

Interface configuration has changed on device. [Click to know more.](#)

a) 点击[点击了解更多 \(Click to know more\)](#) 打开接口更改 (**Interface Changes**) 对话框以查看更改。

图 39: 接口更改



b) 点击[验证更改 \(Validate Changes\)](#) 以确保策略在接口更改后仍有效。

如出现任何错误，则需要更改配置并重新运行验证。

删除安全策略中使用的接口会影响配置。可以直接在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。删除接口将删除与该接口相关的任何配置。引用安全区域的策略不受影响。

c) 点击[关闭 \(Close\)](#) 返回接口 (**Interfaces**) 页面。

步骤 6 点击[保存 \(Save\)](#)，以便将接口更改保存到防火墙。

步骤 7 如果您必须更改任何配置，请转至[部署 \(Deploy\) > 部署 \(Deployment\)](#) 并部署策略。

步骤 8 重新启动防火墙；请参阅[关闭或重新启动设备](#)。

对于集群或高可用性，请首先重新启动数据节点/备用设备，然后等待它们重新启动。然后，您可以更改控制节点（请参阅[更改控制节点](#)）或主用设备（请参阅[在威胁防御高可用性对中切换主用对等体](#)），并重新启动之前的控制节点/主用设备。

合并管理和诊断接口

威胁防御 7.4 及更高版本支持合并的管理和诊断接口。如果有任何使用诊断接口的配置，则不会自动合并接口，您需要执行以下程序。此程序要求您确认配置更改，在某些情况下，需要手动修复配置。

备份/恢复和管理中心配置回滚功能可保存和恢复合并状态（非合并或合并）。例如，如果合并接口，然后恢复之前的非合并配置，则恢复的配置将处于非合并状态。

下表显示了旧诊断接口上的可用配置，以及完成合并的方式。

表 2: 管理中心 合并管理接口支持

旧诊断接口配置	合并行为	在管理接口上受支持?
接口		“管理”接口现在在接口页面上以只读模式显示。
• IP 地址	需要手动删除。	<p>改为使用当前的管理 IP 地址。</p> <p>对于高可用性和集群，管理接口不支持备用 IP 地址或 IP 地址池；每台设备有自己的 IP 地址，故障转移期间将保持这些地址。因此，不能使用单个管理 IP 地址与当前主用/控制设备通信。</p> <p>使用 configure network ipv4 或 configure network ipv6 命令在 CLI 中设置。</p>
• 名称“诊断”	<p>自动更改为“管理”。</p> <p>注释 任何其他接口都不能命名为“管理”。您必须更改名称才能继续合并。</p>	更改为“管理”。
静态路由	需要手动删除。	<p>不支持。</p> <p>管理接口具有与数据接口不同的 Linux 路由表。威胁防御实际上有两个“数据”路由表：一个用于数据接口，另一个用于管理专用接口（过去包括“诊断”接口，但也包括设置为管理专用的任何接口）。根据流量类型，威胁防御会检查一个路由表，然后回退到另一个路由表。此路由查找不再包括诊断接口，也不包括管理接口的 Linux 路由表。有关详细信息，请参阅管理流量的路由表。</p> <p>您可以使用 configure network static-routes 命令在 CLI 中为 Linux 路由表添加静态路由</p> <p>注释 使用 configure network ipv4 或 configure network ipv6 命令设置默认路由。</p>

旧诊断接口配置	合并行为	在管理接口上受支持?
动态路由	需要手动删除。	不支持。
HTTP 服务器	无更改。	不支持。 此设置在合并后的设备上不再有效，但不会从平台设置中删除。平台设置可用于多台设备，其中有一些可能尚未合并。
ICMP	无更改。	不支持。 此设置在合并后的设备上不再有效，但不会从平台设置中删除。平台设置可用于多台设备，其中有一些可能尚未合并。
系统日志服务器	自动改为管理接口。	是。 系统日志服务器配置已具有从管理接口发送系统日志的选项（从 6.3 开始）。如果您特意系统日志选择了诊断接口，系统会将其改为使用管理接口。 注释 如果系统日志服务器或 SNMP 主机的平台设置按名称指定诊断接口，则必须为合并设备和非合并设备使用单独的平台设置策略。 注释 合并的管理接口不支持安全系统日志。
SMTP	无更改。	不支持。 威胁防御仅检查 SMTP 服务器的数据路由表，因此不能使用管理接口或任何其他仅管理接口。有关详细信息，请参阅 管理流量的路由表 。
SNMP	自动改为管理接口。	是。 SNMP 主机配置已具有允许在管理接口上使用 SNMP 主机的选项（从 6.3 开始）。如果您特意 SNMP 选择了诊断接口，系统会将其改为使用管理接口。 注释 如果系统日志服务器或 SNMP 主机的平台设置按名称指定诊断接口，则必须为合并设备和非合并设备使用单独的平台设置策略。
RADIUS 服务器	自动改为管理接口。	是。 如果您特意选择了诊断接口，系统会将其改为使用管理接口。 注释 如果您指定了路由查找来查找源接口，则威胁防御将无法再从管理专用接口发送流量；您必须明确选择“管理”接口作为源接口。不能使用其他管理专用接口。

旧诊断接口配置	合并行为	在管理接口上受支持？
AD 服务器	自动改为管理接口。	是。 如果您特意选择了诊断接口，系统会将其改为使用管理接口。 注释 如果您指定了路由查找来查找源接口，则 威胁防御 将无法再从管理专用接口发送流量；您必须明确选择“管理”接口作为源接口。不能使用其他管理专用接口。
DDNS	需要手动删除。	不支持。
DHCP 服务器	需要手动删除。	不支持。
DNS 服务器	自动改为管理接口。	是。 如果选中同时通过诊断接口启用 DNS 查找复选框，系统会将其改为使用管理接口。不选择任何接口或选中同时通过诊断/管理接口启用 DNS 查找复选框时，路由查找会发生变化：威胁防御 仅使用数据路由表，不会回退到使用管理专用路由表。因此，除管理接口外，不能对 DNS 使用管理专用接口。 注释 管理接口还具有仅用于其管理流量的单独 DNS 查找设置。使用 configure network dns 命令在 CLI 中设置。
FlexConfig	需要手动删除。	不支持。

开始之前

- 要查看设备的当前模式，请在 威胁防御 CLI 上输入 **show management-interface convergence** 命令。以下输出显示管理接口已合并：

```
> show management-interface convergence
management-interface convergence
>
```

以下输出显示管理接口未合并：

```
> show management-interface convergence
no management-interface convergence
>
```

- 对于高可用性对和集群，请在主用/控制设备中执行此任务。合并的配置将自动复制到备用/数据设备。

过程

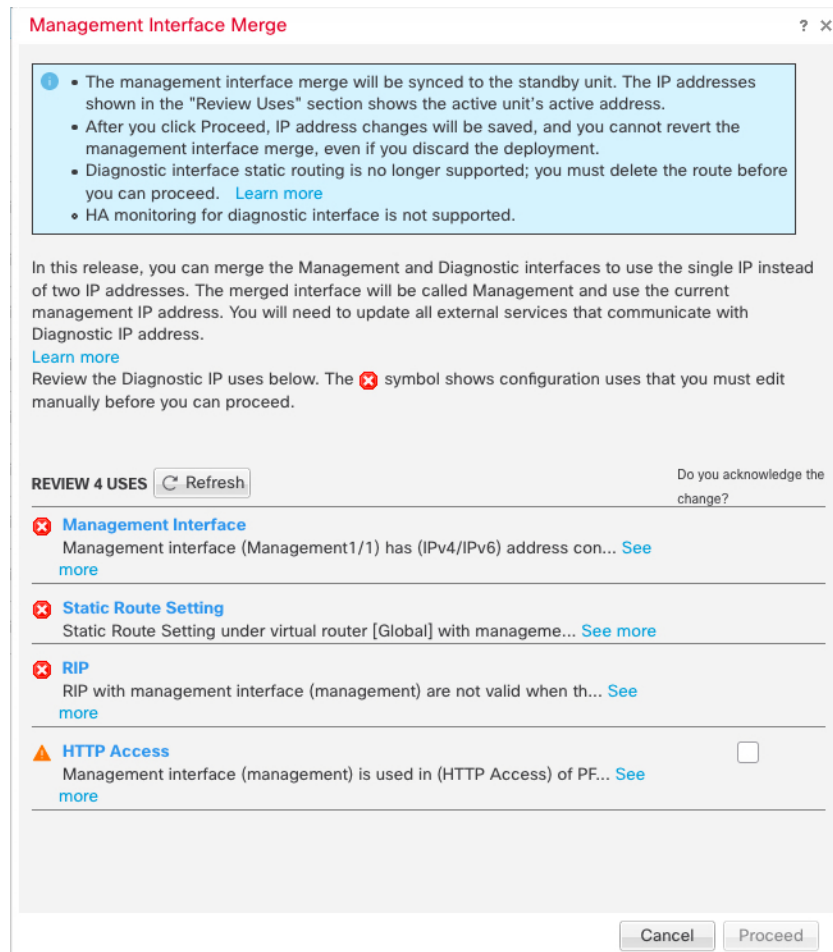
步骤 1 选择 **设备 > 设备管理**，然后点击 威胁防御的 **编辑** (✎)。系统默认选择接口 (**Interfaces**) 页面。。

步骤 2 编辑诊断接口，并删除 IP 地址。

在删除诊断 IP 地址之前，您无法完成合并。

步骤 3 点击所需管理接口操作区域中的**管理接口合并**。

管理接口合并 (Management Interface Merge) 对话框显示配置中所有使用诊断接口的情况。任何需要您手动删除或更改配置的情况将显示警告图标。在您的设备上不再有效的平台设置标有警告图标，需要您确认。

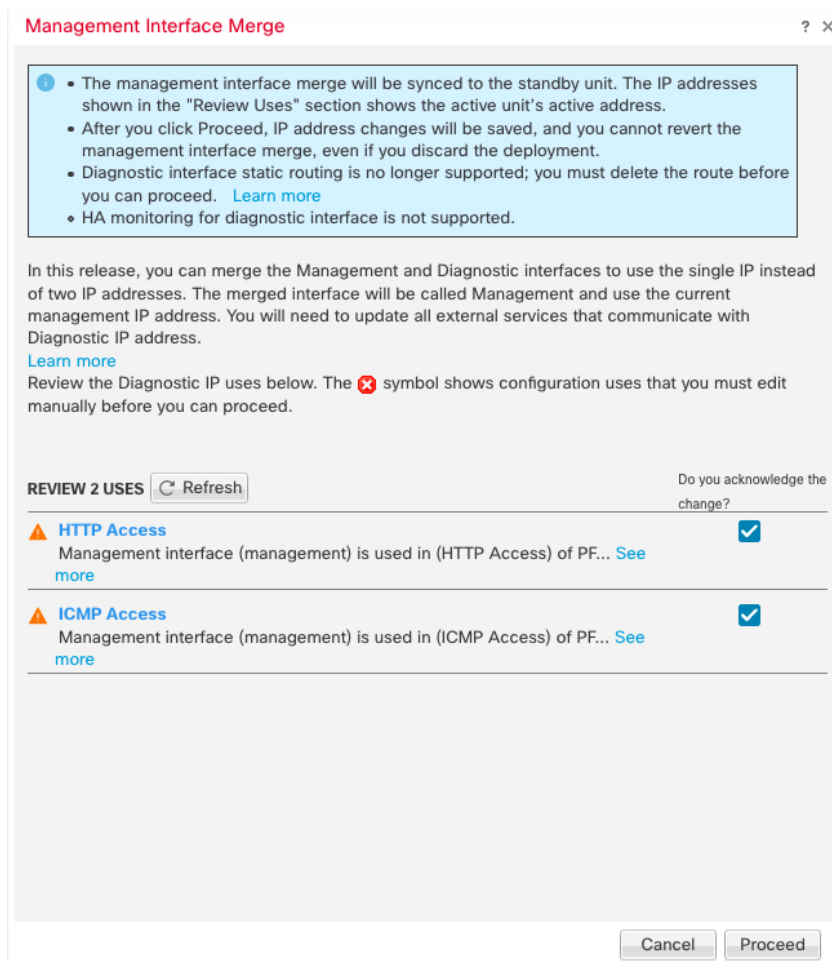


步骤 4 如果需要手动删除或更改任何列出的配置，请执行以下操作。

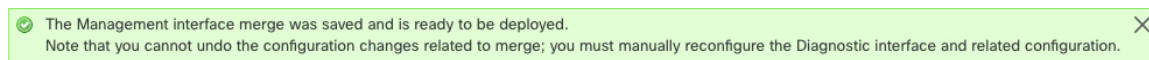
- 点击**取消**以关闭**管理接口合并**对话框。
- 导航至功能区域。然后，您可以删除项目，或者改为选择数据接口。
- 重新打开**管理接口合并**对话框。

此时不应再显示任何警告。

步骤 5 对于每个配置警告，请点击**您是否确认更改？**列中的框，然后点击**继续**。



合并配置后，您会看到成功横幅：



步骤 6 部署新的合并配置。

注意 部署合并的配置后，可以从管理中心中取消合并接口；但是，诊断接口必须手动重新配置。请参阅[取消合并管理接口](#)，第 39 页。此外，如果恢复未合并配置，或回退到未合并配置，设备将恢复为该未合并配置。

合并后，管理接口显示在[接口](#)页面上，但它是只读状态。

步骤 7 合并后，如果有任何与诊断接口通信的外部服务，您需要将其配置更改为使用管理接口 IP 地址。

例如：

- SNMP 客户端

- RADIUS 服务器 - RADIUS 服务器通常会验证传入流量的 IP 地址，因此您需要将该 IP 地址更改为管理地址。此外，对于高可用性对，您需要允许可同时使用主管理 IP 地址和辅助管理 IP 地址；诊断接口用于支持与主用设备一起使用的单个“浮动”IP地址，但管理接口不支持该功能。

取消合并管理接口

威胁防御 7.4 及更高版本支持合并的管理和诊断接口。如果您需要取消合并您的接口，请执行此程序。建议您在将网络迁移到合并模式部署时暂时使用未合并模式。可能并非所有未来版本都支持单独的管理接口和诊断接口。

取消合并接口不会恢复原始诊断配置（如果您是先升级然后再合并接口）。您需要手动重新配置诊断接口。此外，管理接口现在命名为“management”；不能将其重命名为“diagnostic”。

或者，如果您使用备份功能保存旧的未合并配置，则可以恢复该配置，或者您可以使用或者管理中心配置回滚功能，设备将处于未合并状态，诊断配置保持不变。

开始之前

- 要查看设备的当前模式，请在威胁防御 CLI 上输入 **show management-interface convergence** 命令。以下输出显示管理接口已合并：

```
> show management-interface convergence
management-interface convergence
>
```

以下输出显示管理接口未合并：

```
> show management-interface convergence
no management-interface convergence
>
```

- 对于高可用性对和集群，请在主用/控制设备中执行此任务。合并的配置将自动复制到备用/数据设备。

过程

步骤 1 选择 **设备 > 设备管理**，然后点击威胁防御的 **编辑** (✎)。系统默认选择接口 (**Interfaces**) 页面。。

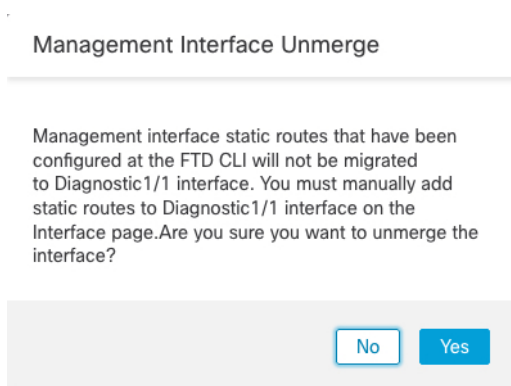
步骤 2 对于管理接口，请点击 **取消合并管理接口** (↶)。

图 40: 管理接口选择



步骤 3 点击是 (**Yes**) 确认要取消合并接口。

图 41: 取消合并确认



步骤 4 部署新的未合并配置。

注释 如果恢复合并配置，或回退到合并配置，设备将恢复为该合并配置。

合并后，管理接口将显示在 **接口** 页面上，并且不再在该页面上配置。

接口历史

特性	最低 管理中心	最低 威胁 防御	详细信息
环回和管理类型接口组对象	任意	7.4	<p>现在，您可以创建仅包含管理专用接口或仅包含环回接口的接口组对象。然后，您可以将这些组用于管理功能，例如 DNS 服务器、HTTP 访问或 SSH。支持环回接口的任何功能都支持环回组。请注意，DNS 不支持管理接口。</p> <p>新增/修改的屏幕：对象 > 对象管理 > 接口 > 添加 > 接口组</p>
合并的管理接口和诊断接口	任意	7.4	<p>对于使用 7.4 及更高版本的新设备，您不能使用旧诊断接口。仅合并的管理接口可用。如果已升级到 7.4 或更高版本，并且没有为诊断接口进行任何配置，则接口将自动合并。</p> <p>如果已升级到 7.4 或更高版本，并且已为诊断接口进行了配置，则可以选择手动合并接口，也可以使用单独的诊断接口。请注意，在更高版本中将删除对诊断接口的支持，因此您应计划尽快合并接口。</p> <p>合并模式还会将 AAA 流量的行为更改为默认使用数据路由表。现在，只有在配置中指定管理专用接口（包括管理接口）时，才可以使用管理专用路由表。</p> <p>新增/修改的屏幕：设备 > 设备管理 > 接口</p> <p>新增/修改的命令：show management-interface convergence</p>

特性	最低管理中心	最低威胁防御	详细信息
Cisco Secure Firewall 3100 固定端口上的默认前向纠错 (FEC) 从第 74 条 FC-FEC 更改为第 108 条 RS-FEC，适用于 25 GB+ SR、CSR 和 LR 收发器	任意	7.2.4/7.3	当您在 Cisco Secure Firewall 3100 固定端口上将 FEC 设置为自动时，对于 25 GB+ SR、CSR 和 LR 收发器，默认类型现在设置为 Clause 108 RS-FEC，而不是 Clause 74 FC-FEC。 支持的平台：Cisco Secure Firewall 3100
对 Firepower 2100，Cisco Secure Firewall 3100 的 LLDP 支持	任意	7.2	您可以为 Firepower 2100 和 Cisco Secure Firewall 3100 接口启用链路层发现协议 (LLDP)。 新增/修改的屏幕： 设备 (Devices) > 设备管理 (Device Management) > 接口 (Interfaces) > 硬件配置 (Hardware Configuration) > 网络连接 (Network Connectivity) 新增/修改的命令： show lldp status, show lldp neighbors, show lldp statistics 支持的平台：Firepower 2100、Cisco Secure Firewall 3100
为 Cisco Secure Firewall 3100 暂停流量控制的帧	任意	7.2	如果流量激增，数据包会在激增量超过 NIC 上的 FIFO 缓冲区的缓冲容量且接收环缓冲的情况下发生中断。启用暂停帧来进行流量控制可缓解此问题。 新增/修改的屏幕： 设备 (Devices) > 设备管理 (Device Management) > 接口 (Interfaces) > 硬件配置 (Hardware Configuration) > 网络连接 (Network Connectivity) 支持的平台：Cisco Secure Firewall 3100
支持 Cisco Secure Firewall 3100 的前向纠错	任意	7.1	Cisco Secure Firewall 3100 25 Gbps 接口支持前向纠错 (FEC)。FEC 默认为启用并会设为“自动” (Auto)。 新增/修改的屏幕： 设备 > 设备管理 > 接口 > 编辑物理接口 > 硬件配置
支持基于 SFP 为 Cisco Secure Firewall 3100 设置速度	任意	7.1	Cisco Secure Firewall 3100 支持基于安装的 SFP 的接口速度检测。检测 SFP 默认为启用。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。 新增/修改的屏幕： 设备 > 设备管理 > 接口 > 编辑物理接口 > 硬件配置
对 Firepower 1100 的 LLDP 支持	任意	7.1	您可以为 Firepower 1100 接口启用链路层发现协议 (LLDP)。 新增/修改的屏幕： 设备 > 设备管理 > 接口 > 硬件配置 > LLDP 新增/修改的命令： show lldp status, show lldp neighbors, show lldp statistics 支持的平台：Firepower 1100

特性	最低管理中心	最低威胁防御	详细信息
接口自动协商现在独立于速度和双工设置，改进了接口同步	任意	7.1	<p>接口自动协商现在独立于速度和双工设置此外，当您在管理中心中同步接口时，可以更有效地检测硬件更改。</p> <p>新增/修改的屏幕：设备 > 设备管理 > 接口 > 硬件配置 > 速度</p> <p>支持的平台：Firepower 1000、2100、Cisco Secure Firewall 3100</p>
Firepower 1100 / 2100 系列光纤接口现在支持禁用自动协商	任意	6.7	<p>现在，您可以配置 Firepower 1100/2100 系列光纤接口以禁用流量控制和链路状态协商。</p> <p>以前，在这些设备上设置光纤接口速度（1000 或 10000 Mbps）时，会自动启用流量控制和链路状态协商。您无法禁用它。</p> <p>现在，您可以取消选择自动协商 (Auto-negotiation) 并将速度设置为 1000，以禁用流量控制和链路状态协商。您无法在 10000 Mbps 时禁用协商。</p> <p>新增/修改的屏幕：设备 > 设备管理 > 接口 > 硬件配置 > 速度</p> <p>支持的平台：Firepower 1100、2100</p>

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。