内联集和被动接口

您可以配置仅限 IPS 被动接口、被动 ERSPAN 接口和内联集。

- 关于 IPS 接口，第 1 页
- 内联集的要求和前提条件，第 4 页
- 内联集和被动接口的准则，第 6 页
- 配置被动接口，第 8 页
- 配置内联集，第 9 页
- 内联集和被动接口的历史记录，第 12 页

关于 IPS 接口

IPS 接口包括无源接口、无源 ERSPAN 接口和内联集。IPS-only 模式接口可以绕过许多防火墙检查，只支持 IPS 安全策略 (Snort)。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。

IPS-only 模式接口可以绕过许多防火墙检查，只支持 IPS 安全策略 (Snort)。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。

内联集

内联集就像导线上的凸起，用于将一个或多个接口对绑定在一起，以便插入到现有网络中。此功能使 Firewall Threat Defense 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，但除非已明确丢弃，否则这些接口上接收的所有流量都会从内联接口对中的另一个接口重传出去。当当一个内联集中有多个内联对时，流量只能在内联对中的接口间传输，而无法在不同内联对的接口间传输。

在分流模式下，Firewall Threat Defense 会进行内联部署，但网络流量不受干扰。相反，Firewall Threat Defense 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 Firewall Threat Defense 和网络之间的布线，就像 Firewall Threat Defense 是内联，并分析 Firewall Threat Defense 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Firewall Threat Defense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Firewall Threat Defense和网络之间的走线。

注释 分流模式 显著 影响 Firewall Threat Defense 性能，具体取决于流量。

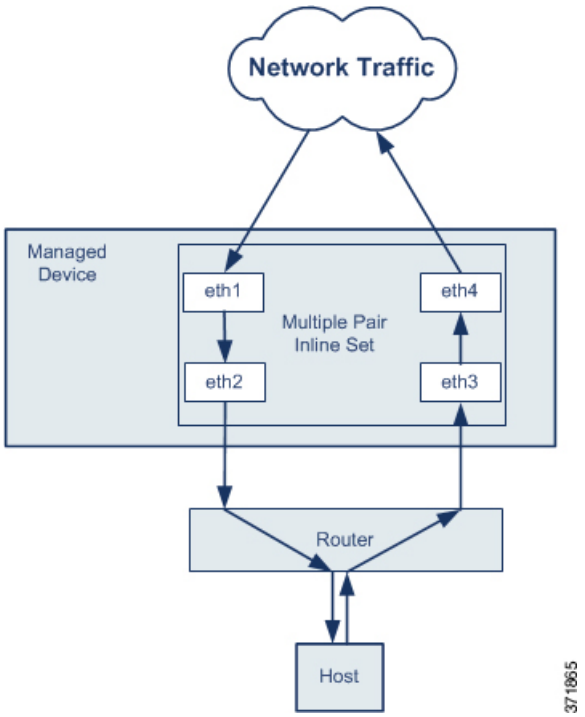
注释 内嵌集可能是您所熟悉的“透明内联集”，但内联接口类型与透明防火墙模式或防火墙类型接口无关。

多个内联对和异步路由

您可以配置接口通过不同的内联对路由网络上的主机和外部主机之间的流量，具体取决于流量是入站还是出站。这是异步路由配置。如果您部署的是异步路由，但一个内联集只包含一个内联对，则设备可能无法正确分析网络流量，因为它可能只会发现一半的流量。

在同一内联集中添加多个内联对，可让系统将入站和出站流量识别为同一流量的一部分。您也可以通过将接口对包括在同一安全区域中来实现此目的，但这种方法仅适用于被动接口。

图 *1:* 异步路由



注释 如果将多个内联对分配给一个内联集，但遇到重复流量问题，则可能需要将内联对重新分配给不同的内联集或修改安全区。

如果在不同的接口对上收到数据包的分片，它们不会重组，而是会被丢弃。确保在同一接口对上接收和发送数据包的所有分片。

被动接口

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 Firewall Threat Defense，Firewall Threat Defense 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 Firewall Threat Defense 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。

关于内联集的硬件旁路

对于支持的型号上的某些接口模块（请参阅内联集的要求和前提条件，第 4 页），您可以启用 硬件旁路 功能。硬件旁路可确保流量在停电期间继续在内联接口对之间流动。在软件或硬件发生故障时，此功能可用于维持网络连接性。

硬件旁路触发器

硬件旁路可以在以下情况下触发：

- Firewall Threat Defense崩溃
- Firewall Threat Defense 重新启动
- 安全模块重新启动
- 机箱崩溃
- 重新引导机箱
- 手动触发
- 机箱断电
- 安全模块断电

注释 硬件旁路适用于计划外/意外故障情况，并且在计划的软件升级期间不会自动触发。硬件旁路仅在计划的升级过程结束时，当 Firewall Threat Defense 应用重新启动时才会启用。

硬件旁路切换

当从正常操作切换到硬件旁路或从硬件旁路切换回正常操作时，流量可能会中断几秒钟。中断时长可能受许多因素影响；例如，铜缆端口自动协商、光纤链路合作伙伴的行为（比如如何处理链路故障和去抖时间）、生成树协议汇聚、动态路由协议汇聚等等。在此期间，您可能会遇到连接中断。

还有可能在恢复正常运行后分析连接中游时由于应用识别错误而遇到连接中断。

Snort 故障开启与硬件旁路

对于不是分路模式下的内联集的内联集，您可以使用“Snort 故障开启”选项，在不检查 Snort 进程何时繁忙或关闭的情况下丢弃流量或允许流量通过。除了分路模式下的内联集，其他所有内联集上都支持“Snort 故障开启”，而不仅仅是支持硬件旁路的接口。

硬件旁路功能允许流量在硬件故障（包括完全断电以及有限的一些软件故障）期间流动。触发 Snort 故障开启的软件故障不会触发硬件旁路。

硬件旁路 状态

如果系统通电，则旁路 LED 指示灯指示硬件旁路状态。请参阅 Firepower 机箱硬件安装指南中有关 LED 的说明。

内联集的要求和前提条件

用户角色

- 管理员
- 访问管理员
- 网络管理员

硬件旁路 支持

对于以下型号上特定网络模块的接口对，Firewall Threat Defense 支持 硬件旁路：

- Cisco Secure Firewall 3100
- Firepower 4100
- Cisco Secure Firewall 4200
- Firepower 9300

- Cisco Secure Firewall 6100

注释 您可以将 硬件旁路 接口用作常规接口，而无需启用 硬件旁路 功能。

这些型号的受支持 硬件旁路 网络包括：

- Cisco Secure Firewall 3100：
  - 6-端口 1G SFP 故障时自动旁路网络模块，SX（多模）(FPR3K-XNM-6X1SXF)
  - 6-端口 10G SFP 故障时自动旁路网络模块，SR（多模）(FPR3K-XNM-6X10SRF)
  - 6-端口 10G SFP 故障时自动旁路网络模块，LR（单模式）(FPR3K-XNM-6X10LRF)
  - 6-端口 25G SFP 故障时自动旁路网络模块，SR（多模）(FPR3K-XNM-X25SRF)
  - 6-端口 25G 故障时自动旁路网络模块，LR（单模式）(FPR3K-XNM-6X25LRF)
  - 8-端口 1G 铜缆故障时自动旁路网络模块，RJ45（铜）(FPR3K-XNM-8X1GF)
- Cisco Secure Firewall 4200：
  - 6-端口 1G SFP 故障时自动旁路网络模块，SX（多模）(FPR4K-XNM-6X1SXF)
  - 6-端口 10G SFP 故障时自动旁路网络模块，SR（多模）(FPR4K-XNM-6X10SRF)
  - 6-端口 10G SFP 故障时自动旁路网络模块，LR（单模式）(FPR4K-XNM-6X10LRF)
  - 6-端口 25G SFP 故障时自动旁路网络模块，SR（多模）(FPR4K-XNM-X25SRF)
  - 6-端口 25G 故障时自动旁路网络模块，LR（单模式）(FPR4K-XNM-6X25LRF)
  - 8-端口 1G 铜缆故障时自动旁路网络模块，RJ45（铜）(FPR4K-XNM-8X1GF)
- Firepower 4100：
  - Firepower 6-端口 1G SX FTW 单位宽网络模块 (FPR4K-NM-6X1SX-F)
  - Firepower 6-端口 10G SR FTW 单位宽网络模块 (FPR4K-NM-6X10SR-F)
  - Firepower 6-端口 10G LR FTW 单位宽网络模块 (FPR4K-NM-6X10LR-F)
  - Firepower 2-端口 40G SR FTW 单位宽网络模块 (FPR4K-NM-2X40G-F)
  - Firepower 8-端口 1G 铜 FTW 单位宽网络模块 (FPR-NM-8X1G-F)
- Cisco Secure Firewall 6100：
  - 6-端口 1G SFP 故障时自动旁路网络模块，SX（多模）(FPR4K-XNM-6X1SXF)
  - 6-端口 10G SFP 故障时自动旁路网络模块，SR（多模）(FPR4K-XNM-6X10SRF)
  - 6-端口 10G SFP 故障时自动旁路网络模块，LR（单模式）(FPR4K-XNM-6X10LRF)

- 6-端口 25G SFP 故障时自动旁路网络模块，SR（多模）(FPR4K-XNM-X25SRF)
- 6-端口 25G 故障时自动旁路网络模块，LR（单模式）(FPR4K-XNM-6X25LRF)
- 8-端口 1G 铜缆故障时自动旁路网络模块，RJ45（铜）(FPR4K-XNM-8X1GF)

- Firepower 9300：
  - Firepower 6-端口 10G SR FTW 单位宽网络模块 (FPR9K-NM-6X10SR-F)
  - Firepower 6-端口 10G LR FTW 单位宽网络模块 (FPR9K-NM-6X10LR-F)
  - Firepower 2-端口 40G SR FTW 单位宽网络模块 (FPR9K-NM-2X40G-F)

硬件旁路 仅可使用以下端口对：

- 1、2
- 3、4
- 5、6
- 7、8

内联集和被动接口的准则

防火墙模式

- 仅当设备处于路由防火墙模式时，才允许 ERSPAN 接口。

集群

- 集群不支持内联集的链路状态传播。
- 单个接口模式不支持仅 IPS 接口。

多实例模式

- 不支持多实例共享接口。您必须使用非共享接口。
- 不支持多实例机箱定义的子接口。必须使用物理接口或 EtherChannel 接口。

一般准则

- 内联集和被动接口仅支持物理接口和 EtherChannel，并且不能使用 VLAN 或其他虚拟接口，包括多实例机箱定义的子接口。
- 由于 IPS 接口不支持常规防火墙保护，因此 IPS 安全策略 (Snort) 要求流量通过同一个 Firewall Threat Defense ，以便检测所有流量。

- 使用内联集时，不允许双向转发检测 (BFD) 回应数据包通过 Firewall Threat Defense。如果 Firewall Threat Defense 的一端有两个邻居运行 BFD，则 Firewall Threat Defense 会因二者具有相同的源 IP 地址和目标 IP 地址且疑似属于 LAND 攻击而丢弃 BFD 回应数据包。
- 对于内联集和被动接口， Firewall Threat Defense 在数据包中最多支持两个 802.1Q 报头（也称为 Q-in-Q 支持），但 Firepower 4100/9300 仅支持一个 802.1Q 报头。**注意**：防火墙类型的接口不支持 Q-in-Q，并且仅支持一个 802.1Q 报头。

硬件旁路 准则

- 硬件旁路 端口仅对内联集支持。
- 硬件旁路 端口不能是 EtherChannel 的一部分。
- 硬件旁路 在高可用性模式下不受支持。
- Firepower 9300 支持使用机箱内集群的硬件旁路 端口。当机箱中的最后一个设备出现故障时，将端口置于硬件旁路模式。不支持机箱间集群，因为机箱间集群仅支持跨网络 EtherChannel；硬件旁路 端口不能是 EtherChannel 的一部分。
- 如果 Firepower 9300 上机箱内群集中的所有模块都发生故障，则在最后一个设备上触发硬件旁路，使流量继续通过。当设备重新恢复时，硬件旁路将恢复为备用模式。但是，当您使用匹配应用流量的规则时，这些连接可能会被丢弃，且需要重新建立。由于在集群设备上未保留状态信息，并且设备无法将流量标识为属于允许的应用，连接会被丢弃。若要避免流量被丢弃，请使用基于端口的规则，而不是基于应用的规则（如果适合您的部署）。
- 您可以将 硬件旁路 接口用作常规接口，而无需启用 硬件旁路 功能。

IPS 接口上不支持的防火墙功能

- DHCP 服务器
- DHCP 中继
- DHCP 客户端
- TCP 拦截
- 路由
- NAT
- VPN
- 应用检测
- QoS
- NetFlow
- VXLAN

配置被动接口

本节介绍如何执行以下操作：

- 启用接口。默认情况下，接口处于禁用状态。
- 将接口模式设为被动或 ERSPAN。对于 ERSPAN 接口，需要设置 ERSPAN 参数和 IP 地址。
- 更改 MTU。默认情况下，MTU 设置为 1500 字节。有关 MTU 的详细信息，请参阅关于 MTU。
- 设置特定的速度和双工（如有）。默认情况下，速度和双工均设置为“自动”。

注释 对于 FXOS 机箱上的 Cisco Secure Firewall Threat Defense，可在 Firepower 4100/9300上配置基本接口设置。有关详细信息，请参阅配置物理接口。

开始之前

- 如果您使用的是 EtherChannel，请根据 配置 EtherChannel添加它们。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 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 在**模式**下拉列表中，选择**被动**或 **Erspan**。

步骤 4 选中**启用**复选框以启用此接口。

步骤 5 在**名称**字段中，输入长度最大为 48 个字符的名称。

步骤 6 从**安全区域**下拉列表中选择一个安全区域，或者点击**新建**添加一个新的安全区域。

步骤 7 （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 8 （可选） 在**常规 (General)** 中，将 **MTU** 设置为介于 64 和 9198 字节之间；对于 Secure Firewall Threat Defense Virtual 和 FXOS 机箱上的 Cisco Secure Firewall Threat Defense，最大值为 9000 字节。

默认值为 1500 字节。

步骤 9 对于 ERSPAN 接口，请设置以下参数：

- **流 ID** - 配置源和目标会话使用的 ID 来标识 ERSPAN 流量，介于 1 和 1023 之间。在 ERSPAN 目标会话配置中也必须输入此 ID。
- **源 IP** - 配置用作 ERSPAN 流量的源的 IP 地址。

步骤 10 对于 ERSPAN 接口，请在 **IPv4** 上设置 IPv4 地址和掩码。

步骤 11 （可选） 点击**硬件配置 (Hardware Configuration)**，设置双工和速度。

确切的速度和复用选项取决于您的硬件。

- **复用 (Duplex)** - 选择**全 (Full)**、**半 (Half)**或**自动 (Auto)**。默认值为“自动”。
- **速度 (Speed)** - 选择 **10**、**100**、**1000** 或**自动 (Auto)**。默认值为“自动”。

步骤 12 点击**确定**。

步骤 13 点击**保存**。

此时，您可以转至**部署** > **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。

配置内联集

本节启用并命名可以添加到内联集的每个内联对的两个物理接口或 EtherChannels。您可以为每个内联集添加多个内联对。您也可以选择为支持的内联对启用 硬件旁路 。

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。

开始之前

- 如果您使用的是 EtherChannel，请根据 配置 EtherChannel 添加它们。
- 我们建议您为连接到 Firewall Threat Defense 内联接口对且启用 STP 的交换机设置 STP PortFast。此设置对硬件旁路配置尤其有用，可以减少绕行时间。

过程

步骤 1 选择 **设备** > **设备管理** 并点击您的 Firewall Threat Defense 设备的 **编辑** (✎)。系统默认选择**接口 (Interfaces)** 页面。

步骤 2 为该内联对中的每个接口命名并启用该接口。您还可以配置其他硬件设置。对于内联对中的每个接口，请务必使其硬件设置相匹配。可以配置多对接口。

a) 点击要编辑的接口的 **编辑** (✎)。

b) 在**名称**字段中，输入长度最大为 48 个字符的名称。

c) 选中**启用**复选框以启用此接口。

d) （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）。

e) 将 **模式** 保留为 **无**。

在将此接口添加到内联集后，此字段将显示的模式为“内联”。

f) 暂时不要设置安全区域；此过程中，必须在稍后创建好内联集后，再设置它。

g) （可选） 点击**硬件配置 (Hardware Configuration)**，设置双工和速度。

确切的速度和复用选项取决于您的硬件。

- **复用 (Duplex)** - 选择**全 (Full)**、**半 (Half)**或**自动 (Auto)**。默认值为“自动”。
- **速度 (Speed)** - 选择 **10**、**100**、**1000** 或**自动 (Auto)**。默认值为“自动”。

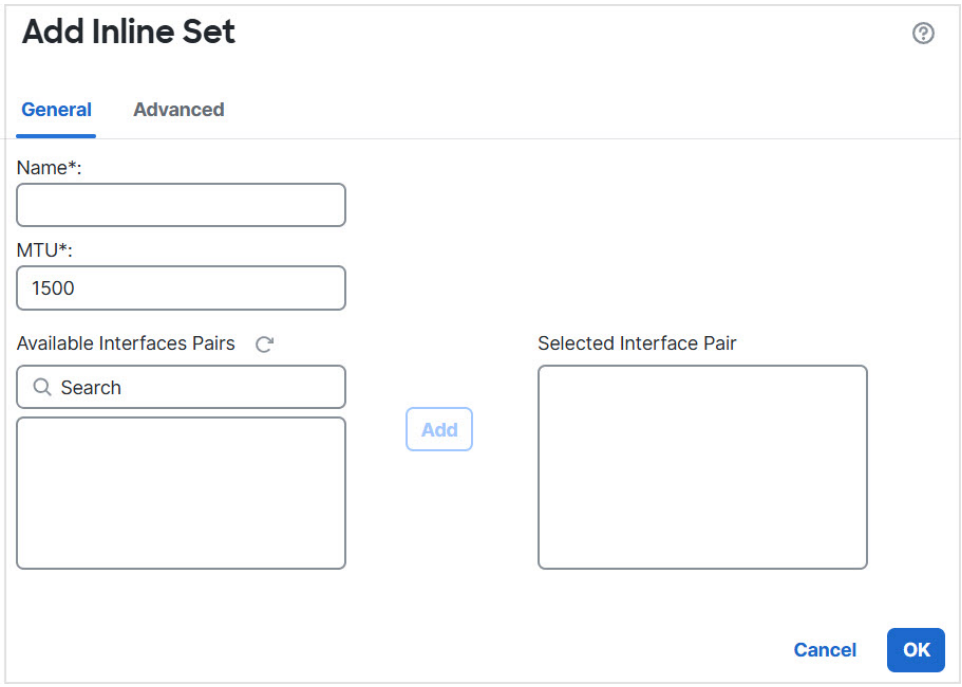
h) 点击**确定**。

请勿为此接口设置任何其他设置。

步骤 3 点击**内联集 (Inline Sets)**。

步骤 4 点击**添加内联集 (Add Inline Set)**。

图 *2:* 添加内联集



此时将显示**添加内联集 (Add Inline Set)** 对话框，其中**常规 (General)** 处于选中状态。

步骤 5 在**名称**字段中，输入内联集的名称。

步骤 6 （可选） 更改 **MTU** 以启用巨帧。

对于内联集，不使用 MTU 设置。但是，巨型帧设置与内联集相关；巨型帧使内嵌接口能够接收多达 9000 字节的数据包。要启用巨型帧，必须将设备上的任意接口的 MTU 设置为 1500 字节以上。

步骤 7 配置 硬件旁路。

a) 对于**绕行 (Bypass)** 模式，请选择以下其中一个选项：

- **禁用** - 对支持硬件旁路的接口，将硬件旁路设置为禁用，或使用不支持硬件旁路的接口。
- **备用** - 在支持硬件旁路的接口上，将硬件绕行设为备用状态。只有成对的硬件旁路接口才会显示出来。在“备用”状态下，接口可以保持正常运行，直至发生触发事件。
- **强制绕行** - 手动强制接口对进入绕行状态。对于处于“强制绕行”模式的任何接口对，**内联集**均显示**是**。

b) 在**可用接口对 (Available Interfaces Pairs)** 区域中，点击某个接口对，然后点击**添加 (Add)**，以将其移动至**选定的接口对 (Selected Interface Pair)** 区域。

此区域中会显示模式设置为“无”的已命名接口和已启用接口之间所有可能的配对。

步骤 8 （可选） 点击**高级 (Advanced)** 设置以下可选参数：

- **分流模式** - 设置为内联分流模式。

  请注意，您不能在同一内联集中启用此选项和严格 TCP 执行选项。

  注释
  如果需要启用或禁用分流模式，应在维护窗口期间执行此操作。在设备传递流量时更改模式可能会导致流量中断。

  注释
  分流模式 显著 影响 Firewall Threat Defense 性能，具体取决于流量。

- **传播链路状态** - 配置链路状态传播。

  当内联集的一个接口断开时，链路状态传播自动关闭内联接口对的第二个接口。当被关闭的接口恢复运行时，第二个接口也将自动恢复运行。换句话说，如果一个接口的链路状态更改，设备会感知该更改并更新其他接口的链路状态以与其匹配。请注意，设备最多需要 4 秒即可传播链路状态更改。在将路由器配置为在处于故障状态的网络设备上自动重新路由流量的弹性网络环境中，链路状态传播特别有用。

  注释
  使用集群时，请勿启用**传播链路状态 (Propagate Link State)**。

- **Snort 故障时自动打开** - 如果您希望在 Snort 进程繁忙或关闭时，新流量和现有流量不检查直接通过（启用）或丢弃（禁用），请启用或禁用**繁忙 (Busy)** 和**关闭 (Down)** 选项之一或两项都启用。

  默认情况下，当Snort进程关闭时，流量会不进行检查就通过，而当进程繁忙时，流量会丢弃。

  当 Snort 进程处于以下状态时：

  - “繁忙” - 由于流量缓冲区已满，进程无法足够快速地处理流量，这表明流量超过设备的处理能力，或者存在其他软件资源问题。
  - “关闭” - 由于您部署了要求进程重启的配置，因此它会重启。请参阅部署或激活时重启 Snort 进程的配置。

当 Snort 进程关闭并重新启动后，它会检查新的连接。为了防止误报和漏报，此进程不检查内联、路由或透明接口上的现有连接，因为最初的会话信息可能已经在它关闭时丢失。

注释
如果 Snort 无法打开，则依赖 Snort 进程的功能会停止运行，这些功能包括应用控制和深度检查。借助简单、易于确定的传输层和网络层特征，系统仅执行基本访问控制。

注释
不支持**严格 TCP 执行 (Strict TCP Enforcement)** 选项。

步骤 9 设置每个接口的安全区域。

a) 点击**接口 (Interfaces)**。
b) 点击成员接口的 **编辑** (✎)。
c) 从**安全区域 (Security Zone)** 下拉列表中选择一个安全区域，或者点击**新建 (New)** 添加一个新的安全区域。

只有在将接口添加到内联集之后，才能设置安全区域；将接口添加到内联集可将模式配置为“内联”(Inline)，并且可让您选择内联类型的安全区域。

d) 点击**确定**。

步骤 10 点击**保存**。

此时，您可以转至**部署** > **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。

内联集和被动接口的历史记录

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
Cisco Secure Firewall 6100 上对所支持网络模块的硬件绕行支持	10.0.0	10.0.0	Cisco Secure Firewall 6100 支持在使用硬件绕行网络模块时使用硬件绕行功能。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **编辑物理接口 (Edit Physical Interface)** 支持的平台：Cisco Secure Firewall 6100

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
Cisco Secure Firewall 4200上对所支持网络模块的硬件绕行支持	7.4.0	7.4.0	Cisco Secure Firewall 4200 支持在使用硬件绕行网络模块时使用硬件绕行功能。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **编辑物理接口 (Edit Physical Interface)** 支持的平台：Cisco Secure Firewall 4200
Cisco Secure Firewall 3100上对所支持网络模块的硬件绕行支持	7.2	任意	Cisco Secure Firewall 3100 现在支持在使用硬件绕行网络模块时使用硬件绕行功能。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **编辑物理接口 (Edit Physical Interface)** 支持的平台：Cisco Secure Firewall 3100
Firepower 4100/9300 的 Firewall Threat Defense 运行链路状态与物理链路状态之间的同步	6.7	任意	Firepower 4100/9300 机箱现在可以将 Firewall Threat Defense 运行链路状态与数据接口的物理链路状态同步。目前，只要 FXOS 管理状态为“运行”且物理链路状态为“运行”，接口将处于“运行”状态，而不考虑 Firewall Threat Defense 应用接口管理状态。如果没有从 Firewall Threat Defense同步，数据接口可能在 Firewall Threat Defense 应用完全上线之前处于“Up”物理状态，或者在您启动关闭后的一段时间内保持“Up”状态。对于内联集，此状态不匹配可能会导致数据包丢失，因为外部路由器可能会在 Firewall Threat Defense 可以处理流量之前开始向 Firewall Threat Defense 发送流量。该功能默认为禁用状态并可在 FXOS 中按逻辑设备逐一启用。 **注释** 集群、容器实例或具有 Radware vDP 修饰器的 Firewall Threat Defense 不支持此功能。ASA 也不支持此功能。 新增/修改的 Firepower 机箱管理器屏幕：**逻辑设备** > **启用链路状态** 新增/修改的 FXOS 命令：**set link-state-sync enabled**、**show interface expand detail** 支持的平台：Firepower 4100/9300

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
Firepower 2130 和 2140 上对所支持网络模块的硬件绕行支持	6.3.0	任意	Firepower 2130 和 2140 现在支持在使用硬件绕行网络模块时使用硬件绕行功能。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **编辑物理接口 (Edit Physical Interface)** 支持的平台：Firepower 2130 和 2140
支持 Firewall Threat Defense 内联集中的 Etherchannel 或被动接口	6.2.0	任意	现在，您可以在 Firewall Threat Defense 内联集或被动接口中使用 EtherChannel。
Firepower 4100/9300 上对所支持网络模块的硬件旁路支持	6.1.0	任意	硬件绕行确保流量在断电期间继续在接口对之间流动。在软件或硬件发生故障时，此功能可用于维持网络连接性。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** > **编辑物理接口 (Edit Physical Interface)** 支持的平台：Firepower 4100/9300
内联集链路状态传播支持 Firewall Threat Defense	6.1.0	任意	当您在 Firewall Threat Defense 应用中配置内联集并启用链路状态传播时，Firewall Threat Defense 会向 FXOS 机箱发送内联集成员身份。链路状态传播意味着，当内联集的一个接口断开时，机箱将自动关闭内联接口对的第二个接口。 新增/修改的 FXOS 命令：**show fault |grep link-down**、**show interface detail**

当地语言翻译版本说明

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

当地语言翻译版本说明

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

当地语言翻译版本说明

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