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。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。

关于 IPS 接口

本节介绍了 IPS 接口。

IPS 接口类型

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联集外重传。

  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。

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必备条件，第3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：

- 威胁防御崩溃
- 威胁防御 重新启动
- 安全模块重新启动
- 机箱崩溃
- 机箱重新启动或升级

- 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 威胁防御 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。

内联集的要求和必备条件

型号支持

威胁防御

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，威胁防御 支持 硬件旁路：

- Firepower 9300
- Firepower 4100
- Secure Firewall 3100
- Firepower 2130 和 2140

注释 ISA 3000 会对硬件旁路进行单独实施，你可以只用 FlexConfig 来启用它（请参阅 FlexConfig 策略）。不要按照本章来配置 ISA 3000 硬件旁路。

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：

- 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 (FPR4K-NM-8X1G-F)
- 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)
- 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)

- Firepower 2130 和 2140：
  - Firepower 6 端口 1G SX FTW 单位宽网络模块 (FPR2K-NM-6X1SX-F)
  - Firepower 6 端口 10G SR FTW 单位宽网络模块 (FPR2K-NM-6X10SR-F)
  - Firepower 6 端口 10G LR FTW 单位宽网络模块 (FPR2K-NM-6X10LR-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。

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。
- 使用内联集时，不允许双向转发检测 (BFD) 回应数据包通过 威胁防御。如果 威胁防御 的一端有两个邻居运行 BFD，则 威胁防御 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， 威胁防御 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 指南

- 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区以太网通道； 硬件旁路 端口不能是 EtherChannel 的一部分。
- 如果 Firepower 9300 上机箱内集群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，当您使用匹配应用程序流量的规则时，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程序，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，而不是基于应用程序的规则（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。

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 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 Cisco 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 (OK)**。

步骤 13 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。

配置内联集

此部分启用并命名可以添加到内联集的两个物理接口。您也可以选择为支持的接口对启用硬件旁路。

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

- 我们建议您为连接到 威胁防御 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 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 在**模式 (Mode)** 下拉列表中，选择**无 (None)**。

在将此接口添加到内联集后，此字段将显示的模式为“内联”。

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。

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。

步骤 6 （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 7 （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 8 点击**确定 (OK)**。

请勿为此接口设置任何其他设置。

步骤 9 对于要添加到内联集的第二个接口，请点击**编辑**（）。

步骤 10 同第一个接口一样配置相应设置。

步骤 11 点击**内联集 (Inline Sets)**。

步骤 12 点击**添加内联集 (Add Inline Set)**。
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 13 在**名称**字段中，输入内联集的名称。

步骤 14 （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 15 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 16 （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 分流模式 显著 影响 威胁防御 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。

- **严格 TCP 执行** - 为最大程度地提高 TCP 安全性，您可以启用严格执行，从而阻止未完成三次握手的连接。

  严格执行功能也阻止：

  - 三次握手尚未完成的连接的非 SYN TCP 数据包
  - TCP 连接上由发起方发出的、响应方尚未发送 SYN-ACK 数据包的非 SYN/RST 数据包
  - TCP 连接上由响应方在 SYN 数据包之后、但在会话建立前发出的非 SYN-ACK/RST 数据包
  - 来自发起方或响应方的已建立 TCP 连接上的 SYN 数据包

- **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。

步骤 17 点击**接口 (Interfaces)**。

步骤 18 对一个成员接口点击**编辑**（ ）。

步骤 19 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。

步骤 20 点击**确定 (OK)**。

步骤 21 设置第二个接口的安全区域。

步骤 22 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。

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。