

IPS 5.X和later/IDSM2 : 使用CLI和IDM的内联VLAN对模式配置示例

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[相关产品](#)

[规则](#)

[VACL捕获配置](#)

[轴向VLAN对模式配置](#)

[CLI 配置](#)

[IDM 配置](#)

[故障排除](#)

[相关信息](#)

简介

VLAN的关联在物理接口叫作轴向VLAN对模式。在其中一接收的数据包配对的VLAN被分析并且转发对在另一个VLAN。AIP-SSM-10是与除了NM-CIDS的入侵防御系统(IPS) 5.1兼容，和AIP-SSM-20的所有传感器支持轴向VLAN对。

轴向VLAN对模式是一个感觉的接口作为802.1Q中继端口的一个活动感觉的模式，并且传感器执行在物理接口桥接在中继的VLAN之间。这意味着交换机连接对感觉的接口必须在中继模式。

在每个对的每个VLAN收到的传感器检查流量，并且能转发在另一个VLAN的数据包在对或丢弃数据包，如果入侵尝试检测。您能配置IPS传感器同时桥接在每个感觉的接口的255个VLAN对。传感器用出口替换在每个收到的信息包802.1q报头的VLAN ID字段传感器转发数据包的数据包的VLAN ID。传感器丢弃在没有分配到轴向VLAN对的所有VLAN接收的所有信息包。

注意：对于IPS-4260，轴向VLAN对不支持FAIL开放硬件旁路。参考的[硬件旁路配置限制](#)欲知更多信息。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

使用5.1及以后的本文档中的信息根据思科入侵防御系统传感器。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

[相关产品](#)

本文档中的信息也适用于入侵检测系统服务模块 (IDSM-2)。

[规则](#)

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

[VACL捕获配置](#)

参考[配置IDSM-2的配置的VACL捕获](#)部分为了发送流量到交换机的IDSM。

[轴向VLAN对模式配置](#)

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用[命令查找工具](#)（[仅限注册用户](#)）可获取有关本部分所使用命令的详细信息。

使用CLI，请使用`physical-interfaces interface_name` in命令服务接口从属方式为了配置轴向VLAN配对。接口名称是快速以太网或千兆以太网。

这些选项适用：

- **admin-state {enabled|disabled}** — 接口的管理链路状态，启用或禁用接口。**注意：** 在所有模块（IDSM-2、NM-CIDS 和 AIP-SSM）中的所有背板传感器接口上，**admin-state** 设置为启用并处于保护状态（不能更改该设置）。**admin-state**（处于保护状态）对于命令和控制接口没有影响。它只影响传感器接口。命令和控制接口无需启用，因为无法对其进行监控。
- **默认**—送返回值到系统默认默认设置。
- **说明**—您的轴向接口对的说明。
- **双工**—接口的双工设置。**自动**—设置接口为自动协商双工。**全套**对全双工的接口。**半**设置接口为半双工。**注意：** 双工选项在所有模块保护。
- **NO**-取消条目或选择设置。
- **速度**—接口的速度设置。**自动**—设置接口为自动协商速度。**10** —设置接口为10 MB (仅TX接口)。 **100** —设置接口为100 MB (仅TX接口)。 **1000** —设置接口为1 GB (千兆接口)**注意：** 速度选项在所有模块保护。
- **子接口类型**—指定接口是子接口，并且什么类型的子接口定义。**线型VLAN对**—让您定义子接口作为一个轴向VLAN对。**什么都**—没有定义的子接口。
- **子接口**—定义了子接口作为一个轴向VLAN对。**vlan1** —在轴向VLAN对的第一个VLAN。**vlan2** —在轴向VLAN对的第二个VLAN。

[CLI 配置](#)

使用CLI，完成这些步骤为了配置在传感器的轴向VLAN对设置：

1. 使用具有管理员权限的帐户登录 CLI。

2. 输入接口子模式：`sensor#configure terminal sensor(config)#service interface sensor(config-int)#`

3. 请验证，如果任何轴向接口存在(子接口类型什么都不应该读“”，如果轴向接口未配置)

```
: sensor(config-int)#show settings physical-interfaces (min: 0, max: 999999999, current: 2)
----- <protected entry> name: GigabitEthernet0/0
<defaulted> ----- media-type: tx <protected>
description: <defaulted> admin-state: disabled <protected> duplex: auto <defaulted> speed:
auto <defaulted> alt-tcp-reset-interface -----
none -----
----- subinterface-type -----
----- none -----
----- <protected entry> name: GigabitEthernet0/1
<defaulted> ----- media-type: tx <protected>
description: <defaulted> admin-state: disabled <defaulted> duplex: auto <defaulted> speed:
auto <defaulted> alt-tcp-reset-interface -----
none -----
----- subinterface-type -----
----- none -----
----- <protected entry> name: GigabitEthernet0/2
<defaulted> ----- media-type: tx <protected>
description: <defaulted> admin-state: disabled <defaulted> duplex: auto <defaulted> speed:
auto <defaulted> alt-tcp-reset-interface -----
none -----
----- subinterface-type -----
----- none -----
----- <protected entry> name: GigabitEthernet0/3
<defaulted> ----- media-type: tx <protected>
description: <defaulted> admin-state: disabled <defaulted> duplex: auto <defaulted> speed:
auto <defaulted> alt-tcp-reset-interface -----
none -----
----- subinterface-type -----
----- none -----
----- <protected entry> name: Management0/0
<defaulted> ----- media-type: tx <protected>
description: <defaulted> admin-state: disabled <protected> duplex: auto <defaulted> speed:
auto <defaulted> alt-tcp-reset-interface -----
none -----
----- subinterface-type -----
----- none -----
-----
---- command-control: Management0/0 <protected> inline-interfaces (min: 0, max: 999999999,
current: 0) -----
----- bypass-mode: auto <defaulted> interface-notifications -----
----- missed-percentage-threshold: 0 percent <defaulted>
notification-interval: 30 seconds <defaulted> idle-interface-delay: 30 seconds <defaulted>
----- sensor(config-int)#
```

4. 消除使用此物理接口的所有轴向接口：`sensor(config-int)#no inline-interfaces interface_name`

5. 显示可用接口列表：`sensor(config-int)#physical-interfaces ?` GigabitEthernet0/0
GigabitEthernet0/0 physical interface. GigabitEthernet0/1 GigabitEthernet0/1 physical
interface. GigabitEthernet0/2 GigabitEthernet0/2 physical interface. GigabitEthernet0/3
GigabitEthernet0/3 physical interface. Management0/0 Management0/0 physical interface.
`sensor(config-int)#physical-interfaces`

6. 指定接口：`sensor(config-int)#physical-interfaces GigabitEthernet0/2`

7. 启用接口的管理员状态：`sensor(config-int-phy)#admin-state enabled` 必须分配到虚拟传感器

和启用接口为了监控流量。

8. 添加此接口的说明：`sensor(config-int-phy)#description INT1`
9. 配置双工设置：`sensor(config-int-phy)#duplex full` 此选项不是可用的在模块。
10. 配置速度：`sensor(config-int-phy)#speed 1000` 此选项不是可用的在模块。
11. 设置轴向VLAN对：`sensor(config-int-phy)#subinterface-type inline-vlan-pair`
`sensor(config-int-phy-inl)#subinterface 1` `sensor(config-int-phy-inl-sub)#vlan1 52`
`sensor(config-int-phy-inl-sub)#vlan2 53`
12. 添加轴向VLAN对的一说明：`sensor(config-int-phy-inl-sub)#description pairs vlans 52 and 53`
13. 验证轴向VLAN对设置：`sensor(config-int-phy-inl-sub)#show settings subinterface-number: 1`
----- description: VLANpair1 default: vlan1:
52 vlan2: 53 ----- sensor(config-int-phy-inl-sub)#
14. 退出接口从属方式：`sensor(config-int-phy-inl-sub)#exit` `sensor(config-int-phy-inl)#exit`
`sensor(config-int-phy)#exit` `sensor(config-int)#exit` Apply Changes:[yes]:
15. 按回车为了应用更改或者输入不丢弃他们。
16. 输入虚拟传感器配置模式：`sensor(config)#service analysis-engine` `sensor(config-ana)#virtual-sensor vs0`
17. 添加接口到虚拟传感器：`sensor(config-ana-vir)#physical-interface GigabitEthernet0/2`
`subinterface-number 1`
18. 退出虚拟传感器从属方式：`sensor(config-ana-vir)#exit` `sensor(config-ana)#exit` Apply Changes:[yes]:
19. 按回车为了应用更改或者输入不丢弃他们。

[IDM 配置](#)

使用IDS服务管理器(IDM)，完成这些步骤配置在传感器的轴向VLAN对设置：

1. 打开浏览器并输入 https://<Management_IP_Address_of_IPS> 以访问 IPS 上的 IDM。
2. 单击 **Download IDM Launcher** 和“Start IDM”以下载应用程序的安装程序。
3. 去主页为了查看设备信息例如主机名、IP地址、版本和型号。等等。
4. 转到 **Configuration > Sensor Setup** 并单击“Network”。在这里可以指定“Hostname”、“IP Address”和“Default Route”。
5. 转到 **Configuration > Interface Configuration** 并单击“Summary”。此页显示感觉的接口的配置汇总。
6. 转到 **Configuration > Interface Configuration > Interfaces** 并选择接口名称。然后，单击 **Enable** 以启用传感器接口。此外还要配置 Duplex、Speed 和 VLAN 信息。
7. 去**Configuration>接口配置> VLAN对**并且单击**添加**为了创建轴向VLAN对。
8. 输入感觉的接口的(GigabitEthernet0/0)子接口号、VLAN A和VLAN B。您能查看轴向VLAN对配置的摘要。
9. 转到 **Configuration > Analysis Engine > Virtual Sensor** 并单击“Edit”以创建新的虚拟传感器。
10. 分配对虚拟传感器vs0的轴向VLAN对52和53。查看所分配的虚拟传感器信息的摘要。

[故障排除](#)

目前没有针对此配置的故障排除信息。

[相关信息](#)

- [Cisco ASA 5500 系列自适应安全设备](#)
- [Cisco Intrusion Prevention System](#)
- [Cisco IPS 4200 系列传感器](#)
- [技术支持和文档 - Cisco Systems](#)