IPS 6.X 及更高版本/IDSM2：使用 IDM 的内联接口对模式配置示例

目录

简介

以“内联接口对”模式运行可将入侵防御系统 (IPS) 直接放到数据流中并会影响数据包转发率，在增加延迟时会使转发率变慢。这使得传感器可以停止攻击，在数据流抵达预期目标之前排除恶意数据流，以此提供保护服务。内联设备不只是在第 3 和第 4 层上处理信息，它还会分析数据包的内容和有效载荷以防止更复杂的嵌入式攻击（第 3 至第 7 层）。这种更深层次的分析使得系统能够识别并停止和/或阻止通常会穿越传统防火墙设备的攻击。

在“内联接口对”模式下，数据包通过传感器上接口对的第一个接口传入并通过接口对的第二个接口传出。如果数据包未由某个签名拒绝或修改，则会发送至接口对的第二个接口。

注意： 您可以将 AIM-IPS 和 AIP-SSM 配置为以内联模式运行，即使这些模块只有一个传感器接口。

注意： 如果配对的接口连接至同一交换机，则应在交换机上将其配置为接入端口且两个端口具有不同的接入 VLAN。否则，数据流将不会流过内联接口。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息是基于使用 Command Line Interface 6.0 和 Intrusion Prevention System Device Manager (IDM) 6.0 的 Cisco IPS 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。

内联接口对配置

在服务接口子模式中使用 **inline-interfaces name** 命令以创建内联接口对。

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。

注意： AIP-SSM 的内联接口模式是在 Cisco ASA CLI 中配置的，而不是在 Cisco IPS CLI 中配置。

这些选项适用：

- **inline-interfaces name** — 逻辑内联接口对的名称**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。
- **default** — 将值恢复为系统的默认设置
- **description** — 内联接口对的说明
- **interface1** *interface_name* — 内联接口对的第一个接口
- **interface2** *interface_name* — 内联接口对的第二个接口
- **NO**-取消条目或选择设置
- **admin-state {enabled|disabled}** — 接口的管理链路状态，启用或禁用接口。

CLI 配置

要在传感器上配置内联 VLAN 对设置，请完成以下步骤：

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. 验证是否存在任何内联接口。如果尚未配置任何内联接口，子接口类型应显示 none：`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. 命名内联对：`sensor(config-int)#`**`inline-interfaces PAIR1`**
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. 将两个接口配置为一对：`sensor(config-int)#`**`interface1 GigabitEthernet0/0`** `sensor(config-int-inl)#`**`interface2 GigabitEthernet0/1`** 必须将该接口分配给一个虚拟传感器并启用它，然后它才能监控流量。有关详细信息，请参阅步骤 10。
7. 添加此接口的说明：`sensor(config-int-phy)#`**`description PAIR1 Gig0/0 and Gig0/1`**
8. 为要配置为内联接口对的任何其他接口重复步骤 4 到 7。
9. 验证设置：`sensor(config-int-inl)#`**`show settings`** `name: PAIR1 ---------- description: PAIR1 Gig0/0 & Gig0/1 default: interface1: GigabitEthernet0/0 interface2: GigabitEthernet0/1 ----------`
10. 启用分配给接口对的接口：`sensor(config-int)#`**`exit`** `sensor(config-int)#`**`physical-interfaces GigabitEthernet0/0`** `sensor(config-int-phy)#`**`admin-state enabled`** `sensor(config-int-phy)#`**`exit`**

```
sensor(config-int)#physical-interfaces GigabitEthernet0/1 sensor(config-int-phy)#admin-
state enabled sensor(config-int-phy)#exit sensor(config-int)#
```

11. 验证接口是否已启用：
```
sensor(config-int)#show settings physical-interfaces (min: 0, max:
999999999, current: 5) ---------------------------------------------- <protected entry>
name: GigabitEthernet0/0 ---------------------------------------------- media-type: tx
<protected> description: <defaulted> admin-state: enabled default: disabled duplex: auto
<defaulted> speed: auto <defaulted> default-vlan: 0 <defaulted> alt-tcp-reset-interface --
------------------------------------------- none ------------------------------------
-------- ---------------------------------------------- --------------------------------
------------- subinterface-type ------------------------------------------- none ----
---------------------------------------- ----------------------------------------------
- ---------------------------------------------- ----------------------------------------
------- <protected entry> name: GigabitEthernet0/1 ----------------------------------
-------- media-type: tx <protected> description: <defaulted> admin-state: enabled default:
disabled duplex: auto <defaulted> speed: auto <defaulted> default-vlan: 0 <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> default-vlan: 0 <defaulted> alt-tcp-reset-interface -------------------------
--------------------- none ------------------------------------------------ --------------
---------------------------------- ------------------------------------------------
subinterface-type ------------------------------------------------ none -----------------
---------------------------- ------------------------------------------------ -------------
---------------------------------- ------------------------------------------------
<protected entry> name: GigabitEthernet0/3 <defaulted> ----------------------------------
------------ media-type: tx <protected> --MORE--
```

12. 发出以下命令以删除内联接口对并将接口返回混合模式：`sensor(config-int)#no inline-interfaces PAIR1` 还必须从所分配的虚拟传感器上删除内联接口对。
13. 验证内联接口对是否已删除：
```
sensor(config-int)#show settings ----------------------------
------------------- command-control: Management0/0 <protected> inline-interfaces (min: 0,
max: 999999999, current: 0) ---------------------------------------------- --------------
-------------------------------- bypass-mode: auto <defaulted> interface-notifications --
-------------------------------------------
```

14. 退出接口配置子模式：
```
sensor(config-int)#exit Apply Changes:?[yes]:
```

15. 按 **Enter** 键以应用更改或输入“no”以放弃更改。

IDM 配置

要在使用 IDM 的传感器上配置内联 VLAN 对设置，请完成以下步骤：

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. 转到主页以查看设备信息，如主机名、IP 地址、版本和型号。
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”。此页显示了传感器接口的配置摘要：
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. 转到 **Configuration > Interface Configuration > Interface Pairs** 并单击“Add”以创建内联对。
8. 查看内联对配置的摘要并应用它。

9. 转到 **Configuration > Analysis Engine > Virtual Sensor** 并单击“Edit”以创建新的虚拟传感器。
10. 将内联对 **INLINE** 分配给虚拟传感器 vs0。
11. 查看所分配的虚拟传感器信息的摘要。

为内联模式 IDSM-2 配置交换机

要为内联模式 IDSM-2 配置交换机，请参阅配置 IDSM-2 中的为内联模式 IDSM-2 配置 Catalyst 系列 6500 交换机部分。

故障排除

问题

如果 IPS 失败并且它配置为内联，则接口在失败时是处于打开（继续传输流量）还是关闭（断开流量）状态？

解决方案

可以将 IPS 配置为“fail-open”状态。这样，如果 IPS 失败，它将继续传输流量，但不会监控流量。

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