IPS 5.X e later/IDSM2: Modo Inline dos pares VLAN usando o exemplo de configuração CLI e IDM

Índice

Introdução

A associação dos VLAN em uma interface física é sabida em pares como o modo inline dos pares VLAN. Os pacotes recebidos em um dos VLAN emparelhados são analisados e enviados ao outro VLAN nos pares. Os pares Inline VLAN são apoiados em todos os sensores que são compatíveis com Intrusion Prevention System (IPS) 5.1, exceto NM-CIDS, AIP-SSM-10, e AIP-SSM-20.

O modo Inline dos pares VLAN é um modo de detecção ativo onde uma relação de detecção atue como uma porta de tronco 802.1Q, e o sensor executa o VLAN Bridging entre pares de VLAN no tronco. Isto significa que o interruptor conectado à relação de detecção deve reagir do modo de tronco.

O sensor inspeciona o tráfego que recebe em cada VLAN em cada par, e pode para a frente os pacotes no outro VLAN nos pares ou para deixar cair o pacote se uma tentativa da intrusão é detectada. Você pode configurar um sensor IPS para construir uma ponte sobre simultaneamente até 255 pares VLAN em cada relação de detecção. O sensor substitui o campo do ID de VLAN no encabeçamento 802.1q de cada pacote recebido com o ID da saída VLAN em que o sensor para a frente o pacote. O sensor deixa cair todos os pacotes recebidos em todos os VLAN que não forem atribuídos aos pares inline VLAN.

Nota: Para o IPS-4260, o desvio falha-aberto do hardware não é apoiado em pares inline VLAN. Refira restrições de configuração do desvio do hardware para mais informação.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada no sensor de Sistema de prevenção de intrusões da Cisco que usa os 5.1 e mais atrasado.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Produtos Relacionados

A informação neste documento é igualmente aplicável ao Módulo de serviços do sistema de detecção de intrusões (IDSM-2).

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

O VACL captura a configuração

Refira a seção configurando da captação VACL de configurar o IDSM-2 a fim enviar o tráfego ao IDSM no interruptor.

Configuração de modo Inline dos pares VLAN

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Use o comando do **interface_name das interfaces física no** submode da relação do serviço a fim configurar pares inline VLAN usando o CLI. O nome da relação é FastEthernet ou gigabitethernet.

As seguintes opções se aplicam:

- **estado administrativo {permitido | deficiente}** — o estado administrativo do link da relação, se a relação está permitida ou desabilitada.**Nota:** Em todo o backplane que detecta relações em todos os módulos (IDSM-2 NM-CIDS, e em AIP-SSM), o estado administrativo é ajustado ao permitido e protegido (você não pode mudar o ajuste). O estado administrativo não tem

nenhum efeito (e é protegido) no comando e na interface de controle. Afeta somente a detecção de relações. O comando e a interface de controle não precisam de ser permitidos porque não pode ser monitorada.
- **default** — Define o valor de volta para a configuração padrão do sistema.
- **descrição** — Sua descrição dos pares inline da relação.
- **duplex** — A configuração bidirecional da relação.**auto** — Ajusta a relação ao automóvel negociam o duplex.**definições completas a** relação completamente - ao duplex.**meio** — Ajusta a relação à metade - duplex.**Nota:** A opção frente e verso é protegida em todos os módulos.
- **no** — Remove uma entrada ou configuração de seleção.
- **velocidade** — O ajuste da velocidade da relação.**auto** — Ajusta a relação ao automóvel negociam a velocidade.**10** — Ajusta a relação ao 10 MB (para relações TX somente).**100** — Ajusta a relação ao 100 MB (para relações TX somente).**1000** — Ajusta a relação a 1 GB (para interfaces de gigabit)**Nota:** A opção da velocidade é protegida em todos os módulos.
- **subinterface-tipo** — Especifica que a relação é uma subinterface e que tipo de subinterface é definido.**inline-VLAN-pares** — Deixa-o definir a subinterface como um par inline VLAN.**nenhuns** — Nenhumas subinterfaces definidas.
- **subinterface** — Define a subinterface como um par inline VLAN.**vlan1** — O primeiro VLAN nos pares inline VLAN.**vlan2** — O segundo VLAN nos pares inline VLAN.

Configuração de CLI

Termine estas etapas a fim configurar os ajustes inline dos pares VLAN no sensor usando o CLI:

1. Faça logon na CLI usando uma conta com privilégios de administrador.
2. Incorpore o submode da relação:`sensor#configure terminal sensor(config)#service interface sensor(config-int)#`
3. Verifique se alguma relação inline existe (o tipo da subinterface deve não ler “nenhuns” se nenhuma relação inline foi configurada):`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. Remova todas as relações inline que usarem esta interface física:`sensor(config-int)#` **`no inline-interfaces interface_name`**
5. Indique a lista de relações disponíveis:`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. Especifique uma relação:`sensor(config-int)#` **`physical-interfaces GigabitEthernet0/2`**
7. Permita o estado administrativo da relação:`sensor(config-int-phy)#` **`admin-state enabled`** A relação deve ser atribuída ao sensor virtual e ser permitida a fim monitorar o tráfego.
8. Adicionar uma descrição desta relação:`sensor(config-int-phy)#` **`description INT1`**
9. Configurar as configurações bidirecional:`sensor(config-int-phy)#` **`duplex full`** Esta opção não está disponível nos módulos.
10. Configurar a velocidade:`sensor(config-int-phy)#` **`speed 1000`** Esta opção não está disponível nos módulos.
11. Estabelecer os pares inline VLAN:`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. Adicionar uma descrição para os pares inline VLAN:`sensor(config-int-phy-inl-sub)#` **`description pairs vlans 52 and 53`**
13. Verifique os ajustes inline dos pares VLAN:`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. Retire o submode da relação:`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. A imprensa **entra** a fim aplicar as mudanças, ou entra **não** para rejeitá-las.
16. Entre no modo virtual da configuração de sensor:`sensor(config)#` **`service analysis-engine`**
    `sensor(config-ana)#` **`virtual-sensor vs0`**
17. Adicionar a relação ao virtual-sensor:`sensor(config-ana-vir)#` **`physical-interface GigabitEthernet0/2 subinterface-number 1`**
18. Retire o submode do virtual-sensor:`sensor(config-ana-vir)#` **`exit`** `sensor(config-ana)#` **`exit`**
    `Apply Changes:?[yes]:`
19. A imprensa **entra** a fim aplicar as mudanças, ou entra **não** para rejeitá-las.

Configuração IDM

Termine estas etapas para configurar os ajustes inline dos pares VLAN no sensor usando o gerenciador de dispositivo ids (IDM):

1. Abra seu navegador e incorpore o **<Management_IP_Address_of_IPS> de https://** para alcançar o IDM no IPS.
2. Clique o **lançador da transferência IDM e comece o IDM** transferir o instalador para o aplicativo.
3. Vão ao Home Page a fim ver a informação do dispositivo tal como o nome de host, o endereço IP de Um ou Mais Servidores Cisco ICM NT, a versão, e o modelo., etc.
4. Vá à **configuração > à instalação do sensor** e clique a **rede**. Aqui você pode especificar o hostname, o endereço IP de Um ou Mais Servidores Cisco ICM NT e a rota padrão.
5. Vá à **configuração > à configuração da interface** e clique o **sumário**.Esta página mostra o sumário de configuração da relação de detecção.
6. Vá à **configuração > à configuração da interface > às relações** e selecione o nome da relação. Então, o clique **permite** a fim permitir a relação de detecção. Também, configurar o duplex, a velocidade e a informação de VLAN.
7. Vá à **configuração > à configuração da interface > aos pares VLAN** e o clique **adiciona** a fim criar os pares Inline VLAN.
8. Incorpore o número da subinterface, o VLAN A e o VLAN B para a relação de detecção (GigabitEthernet0/0).Você pode ver o sumário da configuração Inline dos pares VLAN.
9. Vai ao **motor da configuração > da análise > o sensor virtual** e o clique **edita** a fim criar o sensor virtual novo.
10. Atribua os pares Inline 52 e 53 VLAN ao sensor virtual vs0.Veja o sumário da informação virtual atribuída do sensor.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco Intrusion Prevention System
- Cisco IPS 4200 Series Sensors
- Suporte Técnico e Documentação - Cisco Systems