IPS 6.X e later/IDSM2: A relação Inline emparelha o modo usando o exemplo de configuração IDM

Índice

Introdução

Operar-se no modo Inline dos pares da relação põe o Intrusion Prevention System (IPS) diretamente no fluxo de tráfego e afeta taxas do encaminhamento de pacote, que as faz mais lentas quando a latência é adicionada. Isto permite que o sensor pare ataques assim que deixa cair o tráfego malicioso antes que alcance o alvo pretendido, assim proporciona um serviço protetor. É não somente a informação de processamento inline do dispositivo nas camadas 3 e 4, mas igualmente analisa os índices e o payload dos pacotes para uns ataques encaixados mais sofisticados (camadas 3 a 7). Esta análise mais profunda deixa o sistema identificar e parar e/ou obstruir os ataques que passam normalmente através de um dispositivo de firewall tradicional.

No modo Inline dos pares da relação, um pacote entra através da primeira relação dos pares no sensor e para fora da segunda relação dos pares. O pacote é enviado à segunda relação dos pares a menos que esse pacote estiver sendo negado ou alterado por uma assinatura.

Note: Você pode configurar AIM-IPS e AIP-SSM para operar-se inline mesmo que estes módulos tenham somente uma relação de detecção.

Note: Se as relações emparelhadas são conectadas ao mesmo interruptor, você deve configurar-las no interruptor como portas de acesso com acesso diferente VLAN para as duas portas. Se não, o tráfego não corre através da relação inline.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada no sensor do ips Cisco que usa a interface da linha de comando 6.0 e o gerente de dispositivo de sistema da prevenção de intrusão (IDM) 6.0.

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.

A relação Inline emparelha a configuração

Use o *comando name das inline-**relações no*** submode da relação do serviço a fim criar pares inline da relação.

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

Note: AIP-SSM é configurado para o modo inline da relação de Cisco ASA CLI e não do ips Cisco CLI.

As seguintes opções se aplicam:

- *nome das inline-**relações*** — Nome dos pares inline lógicos da relação**Note**: 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.
- **padrão** — Ajusta o valor de volta ao ajuste de padrão de sistema
- **descrição** — Sua descrição dos pares inline da relação
- *interface_name* **interface1** — A primeira relação nos pares inline da relação

- *interface_name* **interface2** — A segunda relação nos pares inline da relação
- **não** — Remove um ajuste da entrada ou da seleção
- **estado administrativo {permitido | deficiente}** — o estado administrativo do link da relação, se a relação está permitida ou desabilitada.

Configuração de CLI

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

1. Entre ao CLI com uma conta que tenha privilégios do administrado.
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. Nomeie os pares inline:

```
sensor(config-int)#inline-interfaces PAIR1
```

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. Configurar duas relações em um par:

```
sensor(config-int)#interface1 GigabitEthernet0/0



sensor(config-int-inl)#interface2 GigabitEthernet0/1
```

   Você deve atribuir a relação a um sensor virtual e permiti-la antes que possa monitorar o tráfego. Veja a etapa 10 para mais informação.

7. Adicionar uma descrição desta relação:

```
sensor(config-int-phy)#description PAIR1 Gig0/0 and Gig0/1
```

8. Repita etapas 4 com 7 para todas as outras relações que você quiser configurar aos pares inline da relação.
9. Verifique as configurações:

```
sensor(config-int-inl)#show settings
   name: PAIR1
   ------------------------------------------
      description: PAIR1 Gig0/0 & Gig0/1 default:
      interface1: GigabitEthernet0/0
      interface2: GigabitEthernet0/1
   ------------------------------------------
```

10. Permita as relações atribuídas aos pares da relação:

```
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. Verifique que as relações estão permitidas:

```
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. Emita este comando a fim suprimir de um par inline da relação e retornar as relações ao modo misturado:
    ```
    sensor(config-int)#no inline-interfaces PAIR1
    ```

    Você deve igualmente suprimir dos pares inline da relação do sensor virtual a que é atribuído.
13. Verifique que o par inline da relação esteve suprimido:
    ```
    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. Retire o submode da configuração da interface:
    ```
    sensor(config-int)#exit
    Apply Changes:?[yes]:
    ```
15. A imprensa **entra** a fim aplicar as mudanças ou entrá-las **nenhum** a fim rejeitá-las.

Configuração IDM

Termine estas etapas a fim configurar os ajustes inline dos pares VLAN no sensor usando o 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. Vá 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.
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 aos **pares da configuração > da configuração da interface > da relação** e o clique **adiciona** a fim criar os pares Inline.
8. Veja o sumário da configuração Inline dos pares e aplique-o.
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 **INLINE ao** sensor virtual vs0.

11. Veja o sumário da informação virtual atribuída do sensor.

Configurar o interruptor para o IDSM-2 no modo Inline

Refira configurar o 6500 Switch do Catalyst Series para o IDSM-2 na seção de modo Inline de configurar o IDSM-2 a fim configurar o interruptor para o modo IDSM-2 inline.

Troubleshooting

Problema

Se o IPS falha e está configurado inline, faça as relações falham aberto (o tráfego continua a passar) ou fechado (o tráfego é deixado cair).

Solução

Você pode configurar o IPS no estado falha-aberto. Assim, se o IPS falha continuará a passar o tráfego, mas não monitora o tráfego.

Informações Relacionadas

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