IPS 6.X e posterior/IDSM2: Exemplo de Configuração de Modo de Pares de Interface em Linha Usando o IDM

Contents

Introdução

Operar no modo Par de interface em linha coloca o Sistema de prevenção de intrusão (IPS) diretamente no fluxo de tráfego e afeta as taxas de encaminhamento de pacotes, o que os torna mais lentos quando a latência é adicionada. Isso permite que o sensor interrompa os ataques para que ele descarte o tráfego mal-intencionado antes de atingir o destino pretendido, fornecendo, assim, um serviço de proteção. O dispositivo em linha não apenas processa informações nas camadas 3 e 4, mas também analisa o conteúdo e o payload dos pacotes para ataques incorporados mais sofisticados (camadas 3 a 7). Essa análise mais profunda permite que o sistema identifique e pare e/ou bloqueie ataques que normalmente passam por um dispositivo de firewall tradicional.

No modo de Par de Interface em Linha, um pacote entra pela primeira interface do par no sensor e sai pela segunda interface do par. O pacote é enviado para a segunda interface do par, a menos que o pacote esteja sendo negado ou modificado por uma assinatura.

Observação: você pode configurar o AIM-IPS e o AIP-SSM para operar em linha, mesmo que esses módulos tenham apenas uma interface de detecção.

Observação: se as interfaces emparelhadas estiverem conectadas ao mesmo switch, você deverá configurá-las no switch como portas de acesso com VLANs de acesso diferentes para as duas

portas. Caso contrário, o tráfego não flui pela interface em linha.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco IPS Sensor que usa a Interface de linha de comando 6.0 e o Intrusion Prevention System Device Manager (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

As informações neste documento também se aplicam ao módulo de serviços do Sistema de detecção de intrusão (IDSM-2).

Conventions

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

Configuração de pares de interface em linha

Use o comando inline-interfaces name no submodo da interface de serviço para criar pares de interface em linha.

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

Observação: o AIP-SSM é configurado para o modo de interface em linha a partir da CLI do Cisco ASA e não a partir da CLI do Cisco IPS.

As seguintes opções se aplicam:

- inline-interfaces name — Nome do par lógico de interfaces em linha

  Observação: em todas as interfaces de detecção de backplane em todos os módulos (IDSM-2 NM-CIDS e AIP-SSM), admin-state está definido como habilitado e protegido (não é possível alterar a configuração). O estado admin não tem efeito (e está protegido) na interface de comando e controle. Ele afeta apenas interfaces de detecção. A interface de

comando e controle não precisa ser habilitada porque não pode ser monitorada.

- default — Define o valor de volta para a configuração padrão do sistema
- description — Sua descrição do par de interfaces em linha
- interface1 interface_name — A primeira interface no par de interface em linha
- interface2 interface_name — A segunda interface no par de interface em linha
- no — Remove uma entrada ou configuração de seleção
- admin-state {enabled | disabled} — O estado do link administrativo da interface, independentemente de ela estar ativada ou desativada.

Configuração de CLI

Conclua estes passos para definir as configurações do par VLAN em linha no sensor:

1. Faça login na CLI com uma conta que tenha privilégios de administrador.
2. Entre no submodo da interface:

```
<#root>

sensor#

configure terminal

sensor(config)#

service interface


sensor(config-int)#
```

3. Verifique se existe alguma interface em linha. O tipo de subinterface deverá ler `none` se nenhuma interface em linha tiver sido configurada:

```
<#root>

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 o par em linha:

<#root>

```
sensor(config-int)#
```

inline-interfaces PAIR1

5. Exiba a lista de interfaces disponíveis:

```
<#root>

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. Configure duas interfaces em um par:

```
<#root>

sensor(config-int)#

interface1 GigabitEthernet0/0
```

```
<#root>

sensor(config-int-inl)#

interface2 GigabitEthernet0/1
```

Você deve atribuir a interface a um sensor virtual e ativá-lo antes que ele possa monitorar o tráfego. Consulte a etapa 10 para obter mais informações.

7. Adicione uma descrição para esta interface:

```
<#root>

sensor(config-int-phy)#

description PAIR1 Gig0/0 and Gig0/1
```

8. Repita as etapas de 4 a 7 para todas as outras interfaces que você deseja configurar para pares de interface embutidos.

9. Verifique as configurações:

```
<#root>

sensor(config-int-inl)#

show settings

   name: PAIR1
   ----------------------------------------------
      description: PAIR1 Gig0/0 & Gig0/1 default:
      interface1: GigabitEthernet0/0
      interface2: GigabitEthernet0/1
   ----------------------------------------------
```

10. Ative as interfaces atribuídas ao par de interfaces:

```
<#root>

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 se as interfaces estão ativadas:

```
<#root>

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. Execute este comando para excluir um par de interfaces em linha e retornar as interfaces ao modo promíscuo:

<#root>

```
sensor(config-int)#
```

no inline-interfaces PAIR1

Você também deve excluir o par de interface embutida do sensor virtual ao qual ele está atribuído.

13. Verifique se o par de interfaces em linha foi excluído:

<#root>

```
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. Sair do submodo de configuração de interface:

<#root>

```
sensor(config-int)#
```

exit

```
Apply Changes:?[yes]:
```

15. Pressione Enter para aplicar as alterações ou insira no para descartá-las.

Configuração do IDM

Conclua estes passos para configurar as definições do par VLAN em linha no sensor usando o IDM:

1. Abra o navegador e digite https://<Management_IP_Address_of_IPS> para acessar o IDM no IPS.
2. Clique em Download IDM Launcher e em Start IDM para fazer o download do instalador do aplicativo.
3. Vá para a página inicial para exibir as informações do dispositivo, como Nome do host, Endereço IP, versão e modelo.
4. Vá para Configuration > Sensor Setup e clique em Network. Aqui você pode especificar o nome de host, o endereço IP e a rota padrão.
5. Vá para Configuration > Interface Configuration e clique em Summary.

   Esta página mostra o resumo da configuração da interface de detecção:
6. Vá para Configuration > Interface Configuration > Interfaces e selecione o nome da interface. Em seguida, clique em Enable para habilitar a interface de detecção. Além disso, configure as informações de Duplex, Velocidade e VLAN.
7. Vá para Configuration > Interface Configuration > Interface Pairs e clique em Add para criar o par em linha.
8. Exiba o resumo da Configuração de Par em Linha e aplique-o.
9. Vá para Configuration > Analysis Engine > Virtual Sensor e clique em Edit para criar o novo sensor virtual.
10. Atribua o par em linha INLINE ao Virtual Sensor vs0.
11. Exiba o resumo das informações do sensor virtual atribuído.

Configurar o switch para IDSM-2 no modo em linha

Consulte a seção Configuração do Catalyst Series 6500 Switch para IDSM-2 em Modo Inline de Configuração do IDSM-2 para configurar o switch para o modo inline IDSM-2.

Troubleshooting

Problema

Se o IPS falhar e estiver configurado em linha, as interfaces falharão ao abrir (o tráfego continua a passar) ou fechar (o tráfego é descartado).

Solução

Você pode configurar o IPS no estado de fail-open. Assim, se o IPS falhar, ele continuará a passar o tráfego, mas não monitorará o tráfego.

Informações Relacionadas

- Dispositivos de segurança adaptáveis Cisco ASA 5500 Series
- Cisco Intrusion Prevention System
- Cisco IPS 4200 Series Sensors
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.