# Ejemplo de Configuración de IPS 6.X y posterior/IDSM2: Pares de Interfaz en Línea con IDM

## Contenido



## Introducción

Al funcionar en modo de par de interfaces en línea, el sistema de prevención de intrusiones (IPS) se introduce directamente en el flujo de tráfico y afecta a las velocidades de reenvío de paquetes, lo que ralentiza su funcionamiento cuando se añade latencia. Esto permite al sensor detener los ataques para que descarte el tráfico malintencionado antes de que llegue al objetivo deseado, por lo que proporciona un servicio de protección. El dispositivo en línea no solo procesa la información de las capas 3 y 4, sino que también analiza el contenido y la carga útil de los paquetes para detectar ataques integrados más sofisticados (capas 3 a 7). Este análisis más profundo permite al sistema identificar y detener o bloquear los ataques que normalmente pasan a través de un dispositivo de firewall tradicional.

En el modo Par de interfaz en línea, un paquete entra a través de la primera interfaz del par en el sensor y sale de la segunda interfaz del par. El paquete se envía a la segunda interfaz del par a menos que una firma lo rechace o modifique.

Nota: Puede configurar AIM-IPS y AIP-SSM para que funcionen en línea aunque estos módulos tengan solamente una interfaz de detección.

Nota: Si las interfaces emparejadas están conectadas al mismo switch, debe configurarlas en el switch como puertos de acceso con VLAN de acceso diferentes para los dos puertos. De lo

contrario, el tráfico no fluye a través de la interfaz en línea.

# Prerequisites

## Requirements

No hay requisitos específicos para este documento.

## Componentes Utilizados

La información de este documento se basa en Cisco IPS Sensor que utiliza la Interfaz de línea de comandos 6.0 y el Administrador de dispositivos del sistema de prevención de intrusiones (IDM) 6.0.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

## Productos Relacionados

La información de este documento también se aplica al módulo de servicios del sistema de detección de intrusiones (IDSM-2).

## Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

# Configuración de Pares de Interfaz en Línea

Utilice el comando inline-interfaces name en el submodo de interfaz de servicio para crear pares de interfaz en línea.

Nota: Use el Command Lookup Tool (únicamente clientes registrados) para obtener más información sobre los comandos que se utilizan en esta sección.

Nota: AIP-SSM está configurado para el modo de interfaz en línea desde la CLI de Cisco ASA y no desde la CLI de Cisco IPS.

Se aplican estas opciones:

- inline-interfaces name: nombre del par de interfaces inline lógicas

  Nota: En todas las interfaces de detección de backplane de todos los módulos (IDSM-2 NM-CIDS y AIP-SSM), admin-state se establece en enabled y está protegido (no puede cambiar la configuración). El estado de administración no tiene ningún efecto (y está protegido) en la

interfaz de comando y control. Sólo afecta a las interfaces de detección. No es necesario habilitar la interfaz de comando y control porque no se puede supervisar.

- default: permite volver a establecer el valor en la configuración predeterminada del sistema
- description: descripción del par de interfaces en línea
- interface1 interface_name: la primera interfaz del par de interfaces en línea
- interface2 interface_name: la segunda interfaz del par de interfaces en línea
- no: elimina una entrada o una configuración de selección
- admin-state {enabled | disabled}: el estado del enlace administrativo de la interfaz, independientemente de si la interfaz está activada o desactivada.

## Configuración de CLI

Complete estos pasos para configurar los parámetros de par VLAN en línea en el sensor:

1. Inicie sesión en la CLI con una cuenta que tenga privilegios de administrador.
2. Ingrese el submodo de interfaz:

```
<#root>

sensor#

configure terminal

sensor(config)#

service interface


sensor(config-int)#
```

3. Verifique si existe alguna interfaz en línea. El tipo de subinterfaz debe ser `none` si no se ha configurado ninguna interfaz en línea:

```
<#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. Asigne un nombre al par en línea:

```
<#root>

sensor(config-int)#
```

```
inline-interfaces PAIR1
```

5. Mostrar la lista de interfaces disponibles:

```
<#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 dos interfaces en un par:

```
<#root>

sensor(config-int)#

interface1 GigabitEthernet0/0
```

```
<#root>

sensor(config-int-inl)#

interface2 GigabitEthernet0/1
```

Debe asignar la interfaz a un sensor virtual y activarla antes de que pueda supervisar el tráfico. Consulte el paso 10 para obtener más información.

7. Agregue una descripción de esta interfaz:

```
<#root>

sensor(config-int-phy)#

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

8. Repita los pasos del 4 al 7 para cualquier otra interfaz que desee configurar en pares de interfaz en línea.

9. Compruebe los parámetros:

```
<#root>

sensor(config-int-inl)#

show settings

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

10. Habilite las interfaces asignadas al 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 que las interfaces estén habilitadas:

```
<#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. Ejecute este comando para eliminar un par de interfaz en línea y devolver las interfaces al modo promiscuo:

<#root>

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

**no inline-interfaces PAIR1**

También debe eliminar el par de interfaz en línea del sensor virtual al que está asignado.

13. Verifique que se haya eliminado el par de interfaz en línea:

<#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. Salir del submodo de configuración de interfaz:

<#root>

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

**exit**

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

15. Presione Enter para aplicar los cambios o ingrese no para descartarlos.

### Configuración de IDM

Complete estos pasos para configurar los parámetros de par VLAN en línea en el sensor mediante IDM:

1. Abra su navegador e ingrese https://<Management_IP_Address_of_IPS> para acceder al IDM en el IPS.
2. Haga clic en Download IDM Launcher e Start IDM para descargar el instalador de la aplicación.
3. Vaya a la página de inicio para ver la información del dispositivo como el nombre de host, la dirección IP, la versión y el modelo.
4. Vaya a Configuration > Sensor Setup y haga clic en Network. Aquí puede especificar el nombre de host, la dirección IP y la ruta predeterminada.
5. Vaya a Configuration > Interface Configuration y haga clic en Summary.

   Esta página muestra el resumen de la configuración de la interfaz de detección:
6. Vaya a Configuration > Interface Configuration > Interfaces y seleccione el nombre de la interfaz. Luego, haga clic en Enable para habilitar la interfaz de detección. Además, configure la información de dúplex, velocidad y VLAN.
7. Vaya a Configuration > Interface Configuration > Interface Pairs y haga clic en Add para crear el Par en Línea.
8. Vea el resumen de la configuración de par en línea y aplíquelo.
9. Vaya a Configuration > Analysis Engine > Virtual Sensor y haga clic en Edit para crear el nuevo sensor virtual.
10. Asigne el par en línea INLINE al sensor virtual vs0.
11. Ver el resumen de la información del sensor virtual asignado.

## Configuración del switch para IDSM-2 en modo en línea

Consulte la sección Configuración del Switch Catalyst de la Serie 6500 para IDSM-2 en Modo en Línea de Configuración de IDSM-2 para configurar el switch para el modo en línea IDSM-2.

## Troubleshoot

### Problema

Si el IPS falla y se configura en línea, haga que las interfaces no se abran (el tráfico continúa pasando) o se cierren (el tráfico se descarta).

### Solución

Puede configurar IPS en estado abierto a fallos. Por lo tanto, si el IPS falla, continuará pasando el tráfico, pero no supervisará el tráfico.

## Información Relacionada

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco Intrusion Prevention System
- Sensores Cisco IPS de la serie 4200
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).