IPS 6.X y posterior: Sensores virtuales con el ejemplo de configuración IME

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Productos Relacionados
Convenciones
Antecedentes
Sobre el motor del análisis
Sobre los sensores virtuales
Ventajas y restricciones de la virtualización
Ventajas de la virtualización
Restricciones de la virtualización
Requisitos de la virtualización
Configurar
Agregue los sensores virtuales
Agregue el sensor virtual con IME
Edite los sensores virtuales
Edite el sensor virtual con IME
Borre los sensores virtuales
Borre el sensor virtual con IME
Troubleshooting
El administrador IPS expreso no inicia
Información Relacionada

Introducción

Este documento explica la función del motor del análisis y cómo crear, editar, y borrar los sensores virtuales en el Sistema de prevención de intrusiones (IPS) seguro de Cisco con el administrador del IPS de Cisco exprese (IME). También explica cómo asignar las interfaces a un sensor virtual.

Nota: AIM-IPS y NME-IPS no soportan la virtualización.

prerrequisitos

Requisitos

No hay requisitos previos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dispositivo IPS de las Cisco 4200 Series que funciona con la versión de software 6.0 y posterior
- Versión 6.1.1 y posterior expresa del administrador del IPS de Cisco (IME)**Nota:** Mientras que IME se puede utilizar para monitorear los dispositivos sensores que ejecutan el IPS de Cisco 5.0 y posterior, algo de las nuevas funciones y de las funciones entregadas en IME se soportan solamente en los sensores que ejecutan el IPS de Cisco 6.1 o más adelante.**Nota:** El Sistema de prevención de intrusiones (IPS) seguro 5.x de Cisco soporta solamente el sensor virtual predeterminado vs0. Los sensores virtuales con excepción del valor por defecto vs0 se soportan en IPS 6.x y posterior.

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). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

Esta configuración se puede también utilizar con estos sensores:

- IPS-4240
- IPS-4255
- IPS-4260
- IPS-4270-20
- AIP-SSM

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

Sobre el motor del análisis

El motor del análisis realiza el análisis del paquete y la detección de la alerta. Monitorea el tráfico que atraviesa las interfaces especificadas. Usted crea los sensores virtuales en el motor del análisis. Cada sensor virtual tiene un nombre único con una lista de interfaces, los pares en línea de la interfaz, los pares en línea del VLA N, y los grupos VLAN asociados a él. Para evitar los problemas que ordenan de la definición, no se permite ningunos conflictos o las coincidencias en las asignaciones. Usted asigna las interfaces, los pares en línea de la interfaz, los pares en línea del VLA N, y a los grupos VLAN a un sensor virtual específico de modo que no se procese ningún paquete por más de un sensor virtual. Cada sensor virtual también se asocia a una definición

específicamente Nombrada de la firma, a las reglas de la acción del evento, y a la configuración de la Detección de anomalías. Los paquetes de las interfaces, de los pares en línea de la interfaz, de los pares en línea del VLA N, y de los grupos VLAN que no se asignan a ningún sensor virtual se disponen basaron en la configuración en línea de puente.

Sobre los sensores virtuales

El sensor puede recibir las entradas de datos a partir de una o mucha secuencias de datos monitoreadas. Estas secuencias de datos monitoreadas pueden ser puertos de la interfaz física o puertos de la interfaz virtual. Por ejemplo, un solo sensor puede monitorear el tráfico delante del Firewall, de detrás el Firewall, o de delante y detrás del Firewall de en paralelo. Y un solo sensor puede monitorear una o más secuencias de datos. En esta situación, una sola directiva o configuración del sensor se aplica a todas las secuencias de datos monitoreadas. Un sensor virtual es una obtención de datos que es definida por un conjunto de las directivas de configuración. El sensor virtual se aplica a un conjunto de los paquetes según lo definido por el componente de la interfaz. Un sensor virtual puede monitorear los segmentos múltiples, y usted puede aplicar una diversa directiva o configuración para cada sensor virtual dentro de un solo sensor físico. Usted puede configurar una diversa directiva por el segmento monitoreado bajo análisis. Usted puede también aplicar el mismo caso de la directiva, por ejemplo, sig0, rules0, o ad0, a diversos sensores virtuales. Usted puede asignar las interfaces, los pares en línea de la interfaz, los pares en línea del VLA N, y a los grupos VLAN a un sensor virtual.

Nota: El Sistema de prevención de intrusiones (IPS) seguro de Cisco no soporta más de cuatro sensores virtuales. El sensor virtual predeterminado es vs0. Usted no puede borrar el sensor virtual predeterminado. La lista de interfaz, el modo de operación de la Detección de anomalías, el modo de seguimiento de la sesión TCP en línea, y la descripción virtual del sensor son las únicas características de configuración que usted puede cambiar para el sensor virtual predeterminado. Usted no puede cambiar la definición de la firma, las reglas de la acción del evento, o las directivas de la Detección de anomalías.

Ventajas y restricciones de la virtualización

Ventajas de la virtualización

La virtualización tiene estas ventajas:

- Usted puede aplicar diversas configuraciones a diversos conjuntos de tráfico.
- Usted puede monitorear dos redes con solapar los espacios IP con un sensor.
- Usted puede monitorear tanto en el interior como en el exterior de un Firewall o un dispositivo NAT.

Restricciones de la virtualización

La virtualización tiene estas restricciones:

- Usted debe asignar los ambos lados del tráfico asimétrico al mismo sensor virtual.
- El uso de la captura o del SPAN (supervisión promiscua) VACL es contrario con respecto al VLA N que marca con etiqueta, que causa los problemas con los grupos VLAN.Cuando usted utiliza el Cisco IOS Software, un puerto de la captura VACL o una blanco del SPAN no recibe siempre los paquetes con Tag incluso si se configura para el enlace.Cuando usted utiliza el

MSFC, la transferencia del trayecto rápido de las rutas aprendido cambia el comportamiento de las capturas y del SPAN VACL.
- El almacén persistente es limitado.

Requisitos de la virtualización

La virtualización hace que éstos trafiquen los requisitos de la captura:

- El sensor virtual debe recibir el tráfico que tiene encabezados 802.1q, con excepción del tráfico en el VLAN nativo del puerto de la captura.
- El sensor debe ver a las ambas direcciones del tráfico en el mismo grupo VLAN en el mismo sensor virtual para cualquier sensor dado.

Configurar

En esta sección, le presentan con la información para agregar, para editar, y para borrar los sensores virtuales.

Agregue los sensores virtuales

Publique el comando name del virtual-sensor en el submode del motor del análisis del servicio para crear un sensor virtual. Usted asigna las directivas (Detección de anomalías, reglas de la acción del evento, y definición de la firma) al sensor virtual. Entonces usted asigna los pares de la interfaz de las interfaces (promiscuo, en línea, los pares en línea del VLA N, y a los grupos VLAN) al sensor virtual. Usted debe configurar los pares en línea de la interfaz y los pares del VLA N antes de que usted pueda asignarlos a un sensor virtual. Estas opciones se aplican:

- **Detección de anomalías** — Parámetros de la Detección de anomalías.nombre del anomalía-detección-**nombre** — Nombre de la directiva de la Detección de anomalías**modo de operación** — Modo de la Detección de anomalías (**inactivo, aprenda, detecte**)
- **descripción** — Descripción del sensor virtual
- **evento-acción-reglas** — El nombre de la acción del evento gobierna la directiva
- **en línea-TCP-EVASIÓN-PROTECCIÓN-MODE** — Le deja elegir que el tipo de modo del normalizador usted necesite para el examen del tráfico:**asimétrico** — Puede ver solamente una dirección del flujo del tráfico bidireccional. La protección asimétrica del modo relaja la protección de la evasión en la capa TCP.**Nota:** El modo asimétrico deja el sensor sincronizar el estado con el flujo y mantener el examen para esos motores que no requieran a las ambas direcciones. El modo asimétrico baja la Seguridad porque la protección completa requiere los ambos lados del tráfico ser considerada.**estricto** — Si un paquete se falta por cualquier motivo, todos los paquetes después de que el paquete faltado no se procese. La protección estricta de la evasión proporciona la aplicación completa del estado TCP y del seguimiento de la secuencia.**Nota:** Cualesquiera paquetes defectuosos o paquete faltado pueden producir las despedidas de las firmas 1300 o 1330 del motor del normalizador, que intentan corregir la situación, pero pueden dar lugar a las conexiones negadas.
- **en línea-TCP-SESIÓN-SEGUIR-MODE** — Método avanzado que permite que usted identifique a la sesión TCP duplicado en el tráfico en línea. El valor por defecto es el sensor virtual, que es casi siempre la mejor opción.**virtual-sensor** — Todos los paquetes con la misma clave de la sesión (AaBb) dentro de un sensor virtual pertenecen a la misma

sesión.**interfaz-y-VLAN** — Todos los paquetes con la misma clave de la sesión (AaBb) en el mismo VLA N (o los pares en línea del VLA N) y en la misma interfaz pertenecen a la misma sesión. Los paquetes con la misma clave pero en los diversos VLA N o interfaces se siguen independientemente.**VLAN-solamente** — Todos los paquetes con la misma clave de la sesión (AaBb) en el mismo VLA N (o los pares en línea del VLA N) sin importar la interfaz pertenecen a la misma sesión. Los paquetes con la misma clave pero en diversos VLA N se siguen independientemente.

- **firma-definición** — Nombre de la directiva de la definición de la firma
- **interfaces lógicas** — Nombre de las interfaces lógicas (pares en línea de la interfaz)
- **interfaces físicas** — Nombre de los pares del VLA N de las interfaces físicas (promiscuo, en línea, y de los grupos VLAN)**subinterfaz-número** — El número físico de la subinterfaz. Si el subinterfaz-tipo no es ninguno, el valor de 0 indica que la interfaz entera está asignada en el modo promiscuo.**no** — Quita una entrada o una selección

Para agregar un sensor virtual, complete estos pasos:

1. Inicie sesión al CLI con una cuenta con los privilegios de administrador.
2. Ingrese el modo del análisis del servicio.`sensor# **configure terminal** sensor(config)# **service analysis-engine** sensor(config-ana)#`
3. Agregue un sensor virtual.`sensor(config-ana)# **virtual-sensor vs2** sensor(config-ana-vir)#`
4. Agregue una descripción para este sensor virtual.`sensor(config-ana-vir)# **description virtual sensor 2**`
5. Asigne una directiva y a un modo de operación de la Detección de anomalías a este sensor virtual.`sensor(config-ana-vir)# **anomaly-detection** sensor(config-ana-vir-ano)# **anomaly-detection-name ad1** sensor(config-ana-vir-ano)# **operational-mode learn**`
6. Asigne una directiva de las reglas de la acción del evento a este sensor virtual.`sensor(config-ana-vir-ano)# exit`

   `sensor(config-ana-vir)# **event-action-rules rules1**`
7. Asigne una directiva de la definición de la firma a este sensor virtual.`sensor(config-ana-vir)# **signature-definition sig1**`
8. Asigne el modo de seguimiento de la sesión TCP en línea.`sensor(config-ana-vir)# **inline-TCP-session-tracking-mode virtual-sensor**` El valor por defecto es el modo virtual del sensor, que es casi siempre la mejor opción a elegir.
9. Asigne al Modo de protección en línea de la evasión TCP.`sensor(config-ana-vir)# **inline-TCP-evasion-protection-mode strict**` El valor por defecto es el modo estricto, que es casi siempre la mejor opción a elegir.
10. Visualice la lista de interfaces disponibles.`sensor(config-ana-vir)# **physical-interface ?** GigabitEthernet0/0 GigabitEthernet0/0 physical interface. GigabitEthernet0/1 GigabitEthernet0/1 physical interface. GigabitEthernet2/0 GigabitEthernet0/2 physical interface. GigabitEthernet2/1 GigabitEthernet0/3 physical interface. sensor(config-ana-vir)# physical-interface sensor(config-ana-vir)# logical-interface ?`

    `<none available>`
11. Asigne al modo promiscuo le interconecta quieren agregar a este sensor virtual.`sensor(config-ana-vir)# **physical-interface GigabitEthernet0/2**` Relance este paso para todas las interfaces promiscuas que usted quiere asignar a este sensor virtual.
12. Asigne la interfaz en línea le empareja quieren agregar a este sensor virtual.`sensor(config-ana-vir)# **logical-interface inline_interface_pair_name**` Usted debe haber emparejado ya las interfaces.
13. Asigne las subinterfaces de los pares en línea del VLA N o le agrupa quieren agregar a

este sensor virtual como se muestra abajo:`sensor(config-ana-vir)# **physical-interface GigabitEthernet2/0 subinterface-number subinterface_number**` Usted debe haber subdividido ya cualquier interfaz en los pares o los grupos del VLA N.

14. Verifique las configuraciones virtuales del sensor.`sensor(config-ana-vir)# **show settings**`
```
name: vs2 ----------------------------------------------- description: virtual sensor 1
default: signature-definition: sig1 default: sig0 event-action-rules: rules1 default:
rules0 anomaly-detection ------------------------------------------------ anomaly-
detection-name: ad1 default: ad0 operational-mode: learn default: detect -----------------
------------------------------ physical-interface (min: 0, max: 999999999, current: 2) ---
------------------------------------------- name: GigabitEthernet0/2 subinterface-number:
0 <defaulted> ------------------------------------------------ inline-TCP-session-tracking-
mode: virtual-sensor default: virtual-sensor ----------------------------------------------
-- logical-interface (min: 0, max: 999999999, current: 0) -------------------------------
-------------- ------------------------------------------------ -------------------------
--------------------- sensor(config-ana-vir)#
```
15. Dé salida al modo del motor del análisis.`sensor(config-ana-vir)# **exit** sensor(config-ana)# exit sensor(config)# Apply Changes:?[yes]:`
16. Presione ENTER para aplicar los cambios o ingresar **no** para desecharlos.

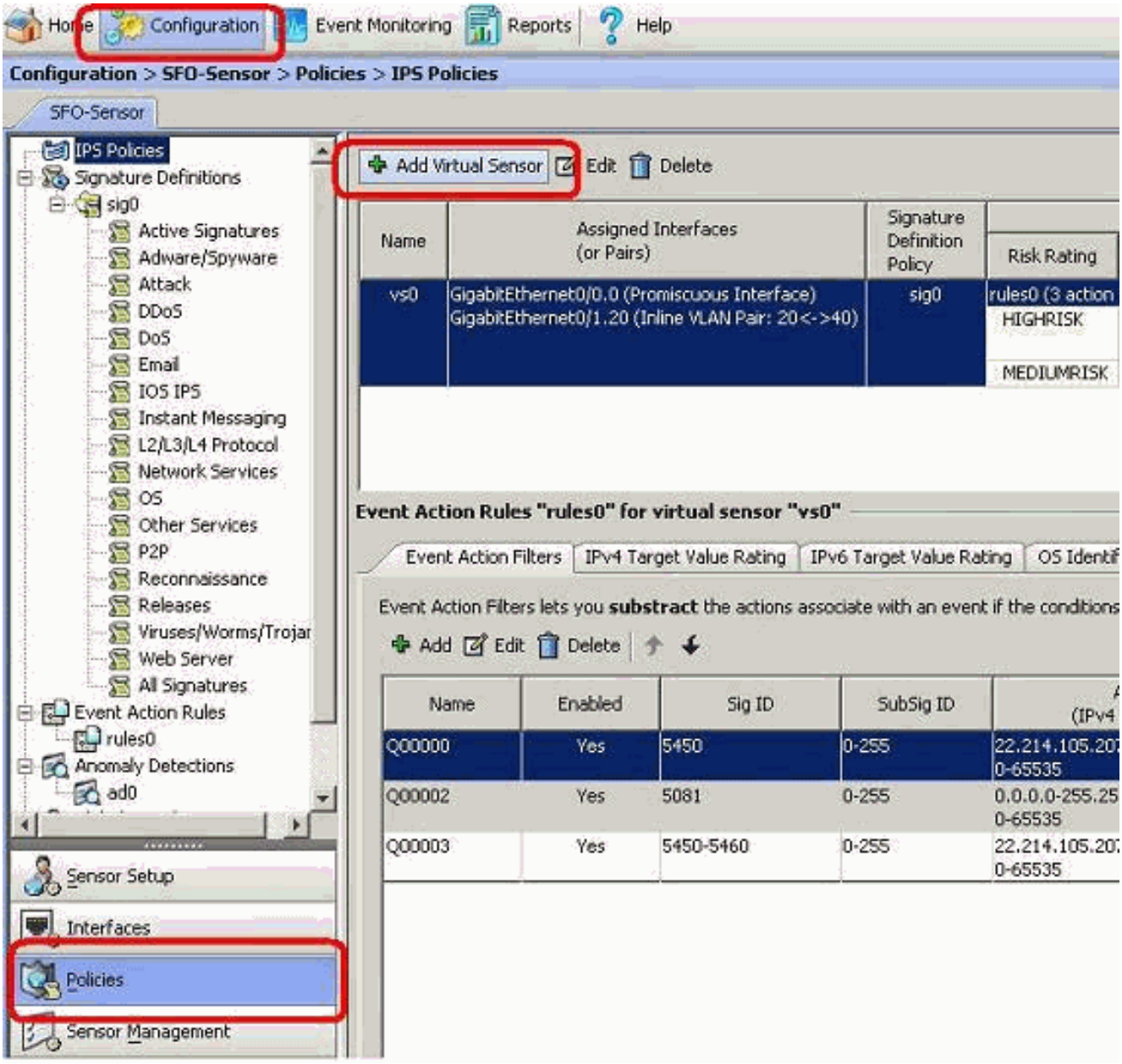
Esto completa el proceso para agregar un sensor virtual al Sistema de prevención de intrusiones (IPS) seguro de Cisco. Complete el mismo procedimiento para agregar sensores más virtuales.

Nota: El Sistema de prevención de intrusiones (IPS) seguro de Cisco no soporta más de cuatro sensores virtuales. El sensor virtual predeterminado es vs0.

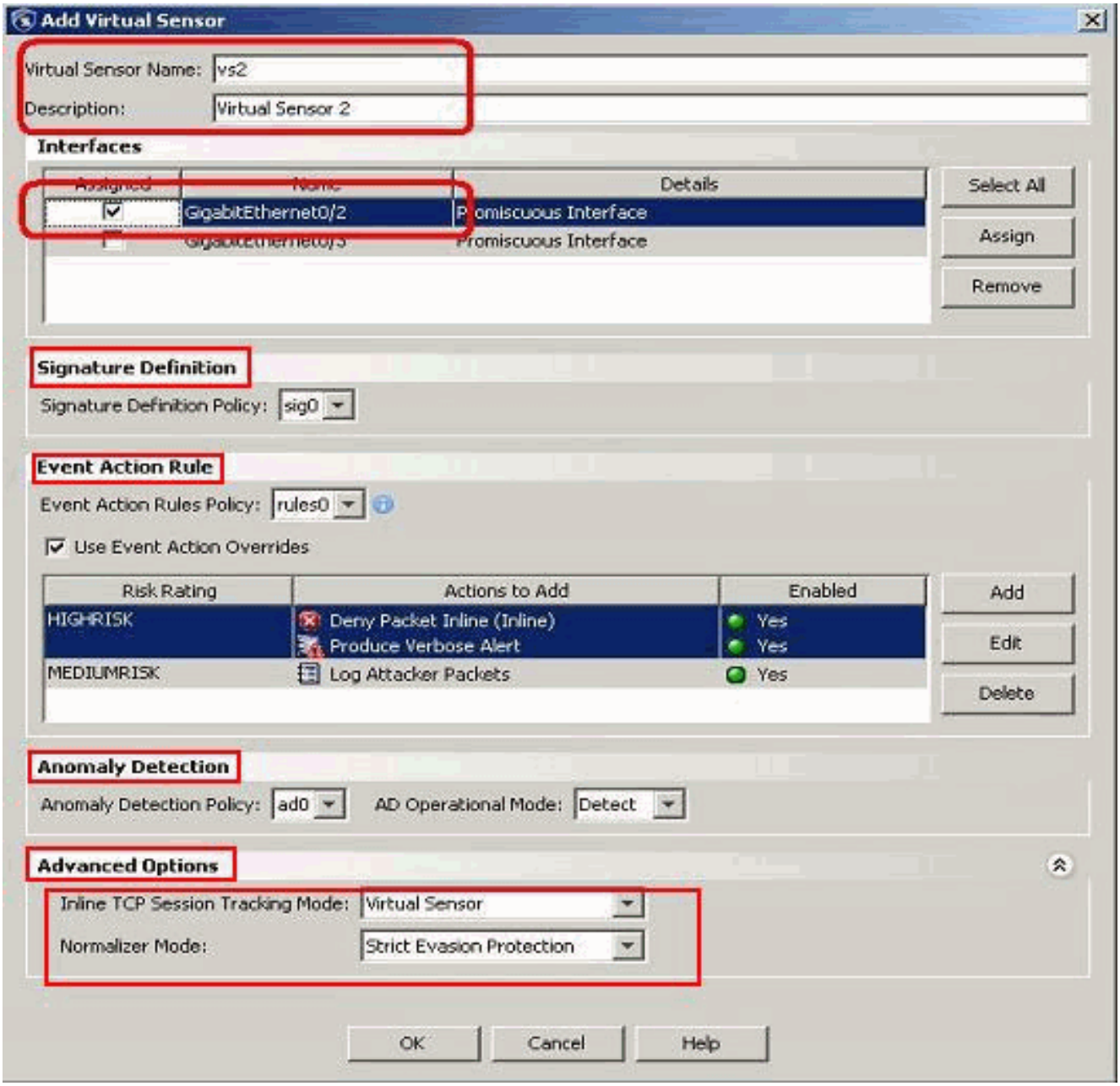
Agregue el sensor virtual con IME

Complete estos pasos para configurar un sensor virtual en el Sistema de prevención de intrusiones (IPS) seguro de Cisco con el administrador del IPS de Cisco expreso:

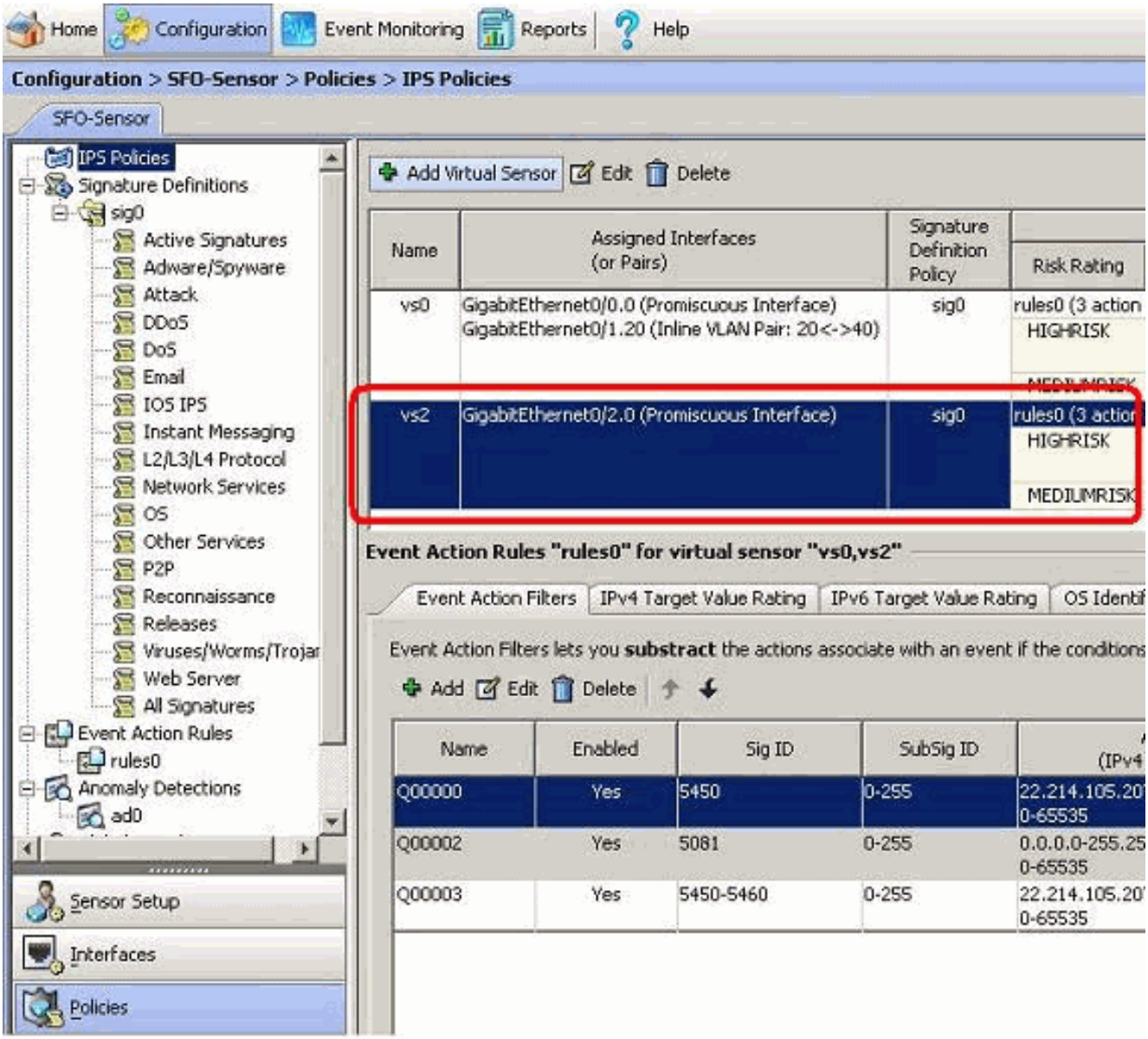
1. Elija la **configuración > las directivas de SFO-Sensor> Policies> IPS**. Entonces, haga clic en **agregan el sensor virtual** tal y como se muestra en del tiro de pantalla.



2. Nombre el sensor virtual (vs2 en este ejemplo) y agregue una descripción al sensor virtual en el espacio proporcionado. También asigne al modo promiscuo le interconecta quieren agregar a este sensor virtual. Gigabit Ethernet 0/2 se elige aquí. Ahora proporcione los detalles en la **definición de la firma**, la **regla de la acción del evento**, la **Detección de anomalías** y las secciones **avanzadas de las opciones** tal y como se muestra en de la captura de pantalla.Bajo **opciones avanzadas** proporcione los detalles sobre el modo de seguimiento de la sesión TCP y el modo del normalizador. Aquí el **modo de seguimiento de la sesión TCP** es **sensor virtual** y el **modo del normalizador** es **Modo de protección estricto de la**
evasión.



3. Haga clic en OK.
4. El sensor virtual nuevamente agregado vs2 se muestra en la lista de sensores virtuales. El tecleo **solicita la** nueva Configuración del sensor virtual que se enviará al Sistema de prevención de intrusiones (IPS) seguro de
Cisco.



Esto completa la configuración para agregar un sensor virtual.

Edite los sensores virtuales

Estos parámetros de un sensor virtual pueden ser editados:

- Directiva de la definición de la firma
- La acción del evento gobierna la directiva
- Directiva de la Detección de anomalías
- Modo de operación de la Detección de anomalías
- Modo de seguimiento de la sesión TCP en línea
- Descripción
- Interfaces asignadas

Para editar un sensor virtual, complete estos pasos:

1. Inicie sesión al CLI con una cuenta con los privilegios de administrador.
2. Ingrese el modo del análisis del servicio.`sensor# configure terminal sensor(config)# service analysis-engine sensor(config-ana)#`
3. Edite el sensor virtual, vs1.`sensor(config-ana)# virtual-sensor vs2 sensor(config-ana-vir)#`
4. Edite la descripción de este sensor virtual.`sensor(config-ana-vir)# description virtual sensor`

A

5. Cambie la directiva y al modo de operación de la Detección de anomalías asignados a este sensor virtual.`sensor(config-ana-vir)# anomaly-detection`

   `sensor(config-ana-vir-ano)# **anomaly-detection-name ad0** sensor(config-ana-vir-ano)# **operational-mode learn**`
6. Cambie la directiva de las reglas de la acción del evento asignada a este sensor virtual.`sensor(config-ana-vir-ano)# exit`

   `sensor(config-ana-vir)# **event-action-rules rules0**`
7. Cambie la directiva de la definición de la firma asignada a este sensor virtual.`sensor(config-ana-vir)# **signature-definition sig0**`
8. Cambie el modo de seguimiento de la sesión TCP en línea.`sensor(config-ana-vir)# **inline-TCP-session-tracking-mode interface-and-vlan**` El valor por defecto es el modo virtual del sensor, que es casi siempre la mejor opción a elegir.
9. Visualice la lista de interfaces disponibles.`sensor(config-ana-vir)# **physical-interface ?**`
   `GigabitEthernet0/0 GigabitEthernet0/0 physical interface. GigabitEthernet0/1 GigabitEthernet0/1 physical interface. GigabitEthernet2/0 GigabitEthernet0/2 physical interface. GigabitEthernet2/1 GigabitEthernet0/3 physical interface. sensor(config-ana-vir)# physical-interface sensor(config-ana-vir)# logical-interface ?`

   `<none available>`
10. Cambie las interfaces del modo promiscuo asignadas a este sensor virtual.`sensor(config-ana-vir)# physical-interface GigabitEthernet0/2`
11. Cambie los pares en línea de la interfaz asignados a este sensor virtual.`sensor(config-ana-vir)# **logical-interface inline_interface_pair_name**` Usted debe haber emparejado ya las interfaces.
12. Cambie la subinterfaz con los pares o los grupos en línea del VLA N asignados a este sensor virtual.`sensor(config-ana-vir)# physical-interface GigabitEthernet2/0 subinterface-number`
    `subinterface_number`Usted debe haber subdividido ya cualquier interfaz en los pares o los grupos del VLA N.
13. Verifique las configuraciones virtuales editadas del sensor.`sensor(config-ana-vir)# **show settings** name: vs2 ---------- description: virtual sensor 1 default: signature-definition: sig1 default: sig0 event-action-rules: rules1 default: rules0 anomaly-detection ---------- anomaly-detection-name: ad1 default: ad0 operational-mode: learn default: detect ---------- ---------- physical-interface (min: 0, max: 999999999, current: 2) ---------- name: GigabitEthernet0/2 subinterface-number: 0 <defaulted> ---------- inline-TCP-session-tracking-mode: interface-and-vlan default: virtual-sensor ---------- ------ logical-interface (min: 0, max: 999999999, current: 0) ---------- ---------- ---------- sensor(config-ana-vir)#`
14. Dé salida al modo del motor del análisis.`sensor(config-ana)# exit`

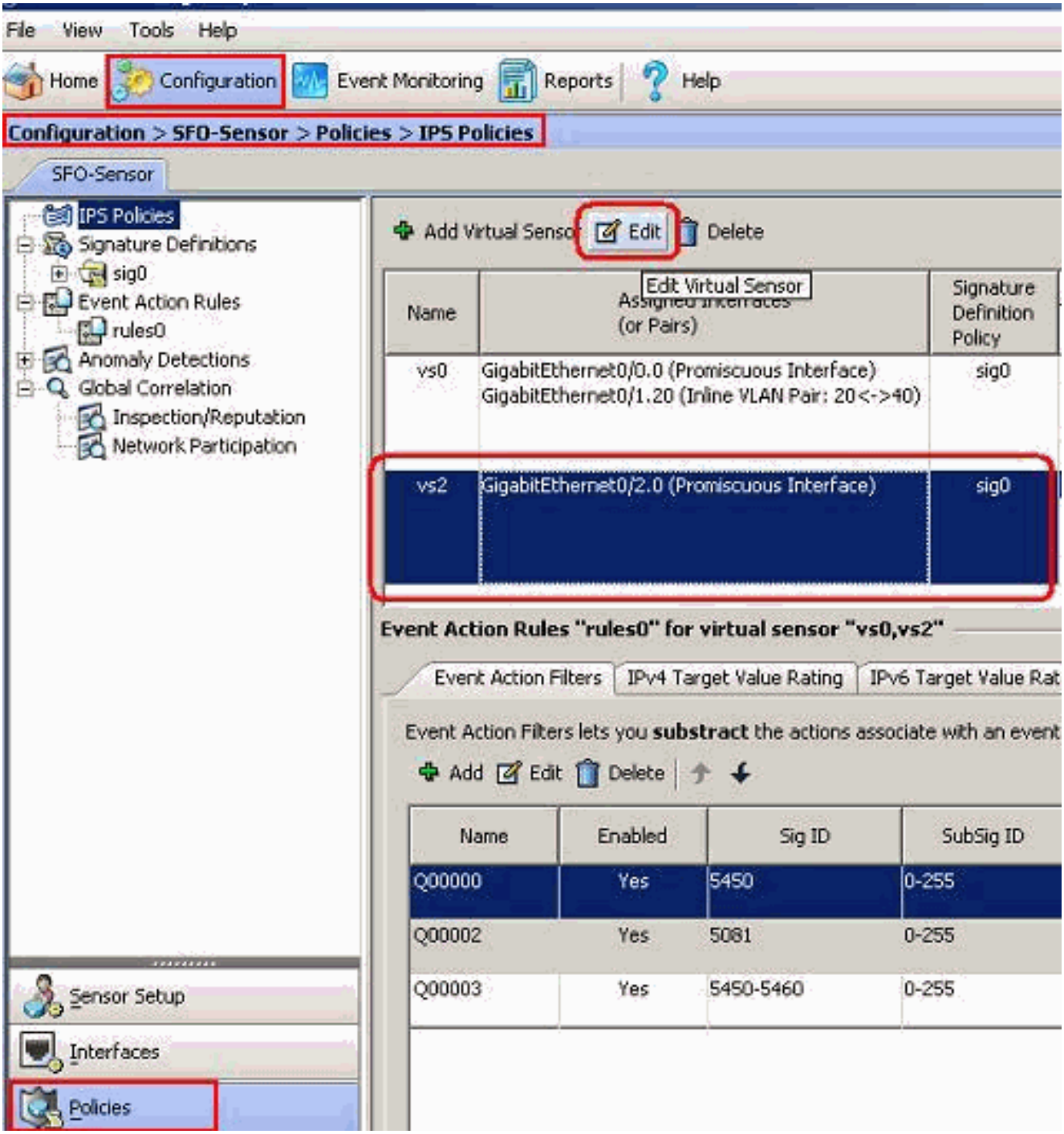
    `sensor(config)#`

    `Apply Changes:?[yes]:`
15. Presione ENTER para aplicar los cambios o ingresar **no** para desecharlos.

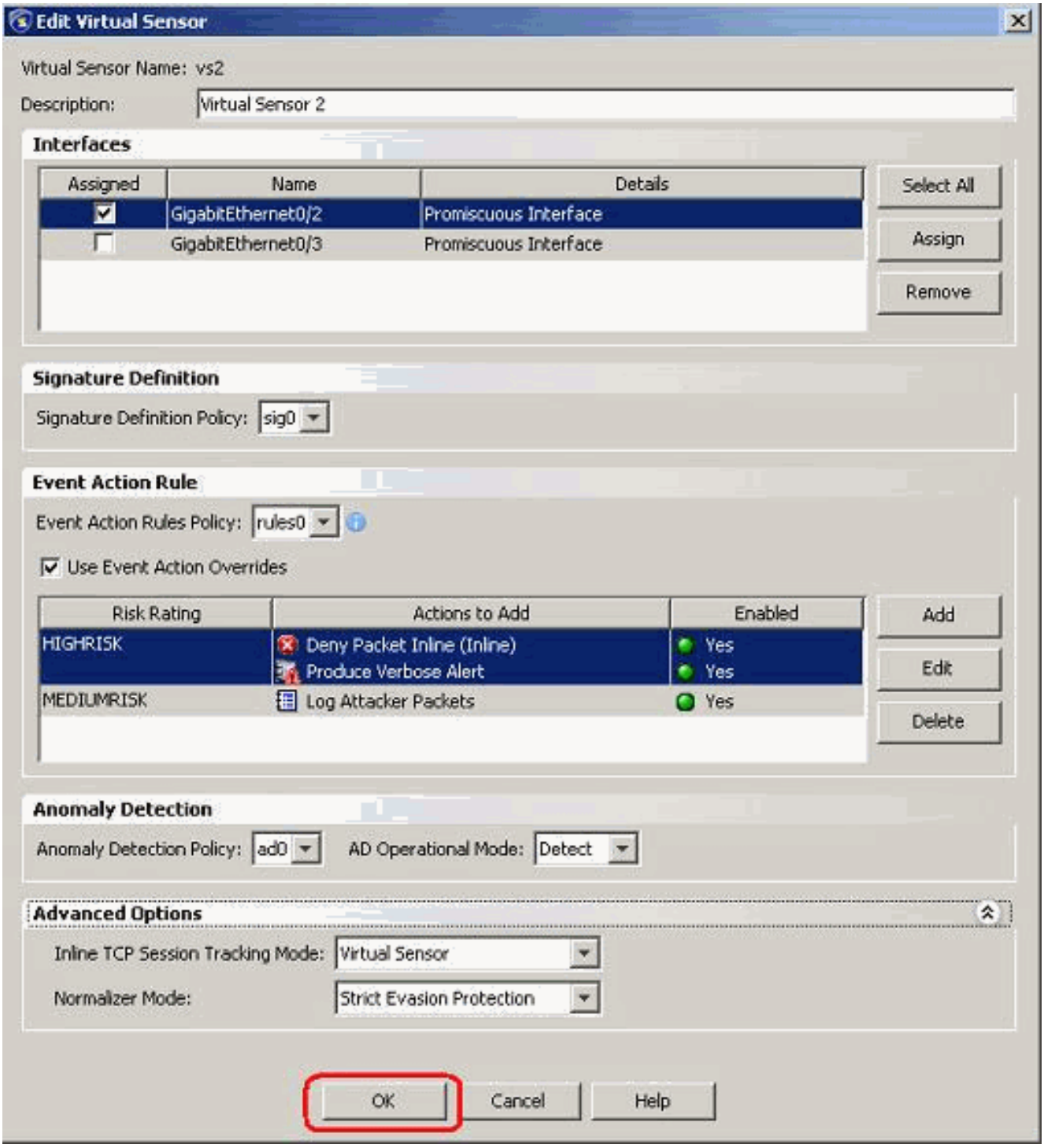
Edite el sensor virtual con IME

Complete estos pasos para editar un sensor virtual en el Sistema de prevención de intrusiones (IPS) seguro de Cisco con el administrador del IPS de Cisco expreso:

1. Elija la **configuración > las directivas de SFO-Sensor> Policies> IPS**.
2. Elija el sensor virtual que se editará, y después haga clic **editan** tal y como se muestra en del tiro de pantalla. En este ejemplo vs2 es el sensor virtual que se editará.



3. En la ventana **virtual del sensor del editar**, realice los cambios a los parámetros para el sensor virtual presente bajo la **definición de la firma de las** secciones, la **regla de la acción del evento**, la **Detección de anomalías** y **opciones avanzadas**. El Haga Click en OK, y entonces hace clic **se aplica**.



Esto completa el proceso para editar un sensor virtual.

Sensores virtuales de la cancelación

Para borrar un sensor virtual, complete estos pasos:

1. Para borrar un sensor virtual, no publique el **ningún** comando del virtual-**sensor**.`sensor(config-ana)# virtual-sensor vs2 sensor(config-ana-vir)# sensor(config-ana-vir)# exit sensor(config-ana)# no virtual-sensor vs2`
2. Verifique el sensor virtual borrado.`sensor(config-ana)# show settings`

```
global-parameters

-----------------------------------------------
```

```
   ip-logging
   ------------------------------------------------
      max-open-iplog-files: 20 <defaulted>
   ------------------------------------------------
------------------------------------------------
virtual-sensor (min: 1, max: 255, current: 2)
------------------------------------------------
   <protected entry>
   name: vs0 <defaulted>
   ------------------------------------------------
      description: default virtual sensor <defaulted>
      signature-definition: sig0 <protected>
      event-action-rules: rules0 <protected>
      anomaly-detection
      ------------------------------------------------
         anomaly-detection-name: ad0 <protected>
         operational-mode: detect <defaulted>
      ------------------------------------------------
      physical-interface (min: 0, max: 999999999, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      logical-interface (min: 0, max: 999999999, current: 0)
      ------------------------------------------------
      ------------------------------------------------
```

`sensor(config-ana)#` Solamente el sensor virtual predeterminado, **vs0**, está presente.

3. Dé salida al modo del motor del análisis.`sensor(config-ana)# exit`

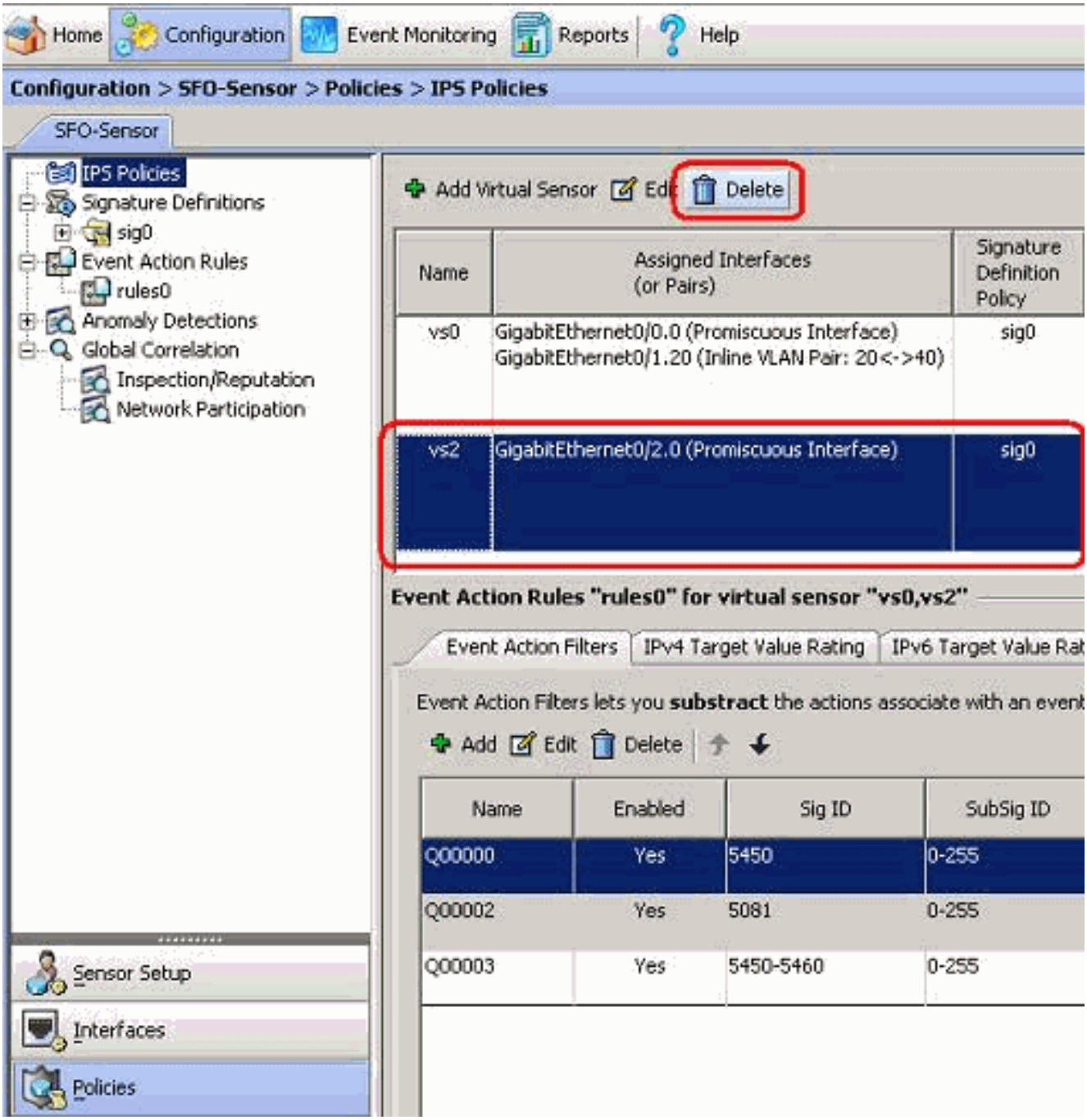
```
sensor(config)#
Apply Changes:?[yes]:
```

Borre el sensor virtual con IME

Complete esto camina para borrar un sensor virtual en el Sistema de prevención de intrusiones (IPS) seguro de Cisco con el administrador del IPS de Cisco expreso:

1. Elija la **configuración > las directivas de SFO-Sensor> Policies> IPS**.

2. Elija el sensor virtual que se borrará, y después haga clic la **cancelación**, tal y como se muestra en del tiro de pantalla. En este ejemplo vs2 es el sensor virtual que se borrará.



Esto completa el proceso para borrar un sensor virtual. Se borra el sensor virtual vs2.

Troubleshooting

El administrador IPS expreso no inicia

Problema

Cuando una tentativa se hace para acceder el IPS con el IME, el administrador IPS expreso no comienza y se recibe este mensaje de error:

```
"Cannot start IME client. Please check if it is already started.
Exception: Address already in use: Cannot bind"
```

Solución

Para resolver esto, recargue el puesto de trabajo PC IME.

Información Relacionada

- Página de soporte del Cisco Intrusion Prevention System
- Página de soporte expresa del administrador del IPS de Cisco
- Network Time Protocol (NTP)
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems