IPS 6.X e mais tarde: Sensores virtuais com exemplo de configuração IME

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Produtos Relacionados
Convenções
Informações de Apoio
Sobre o motor da análise
Sobre sensores virtuais
Vantagens e limitações da virtualização
Vantagens da virtualização
Limitações da virtualização
Exigências da virtualização
Configurar
Adicionar sensores virtuais
Adicionar o sensor virtual com IME
Edite sensores virtuais
Edite o sensor virtual com IME
Suprima de sensores virtuais
Suprima do sensor virtual com IME
Troubleshooting
O gerente IPS expresso não se lança
Informações Relacionadas

Introdução

Este documento explica a função do motor da análise e como criar, para editar, e suprimir de sensores virtuais no Intrusion Prevention System (IPS) seguro de Cisco com o gerente do ips Cisco expresse (IME). Igualmente explica como atribuir relações a um sensor virtual.

Nota: AIM-IPS e NME-IPS não apoiam a virtualização.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Dispositivo IPS do Cisco 4200 Series que executa a versão de software 6.0 e mais atrasado
- Versão 6.1.1 e mais recente expressa do gerente do ips Cisco (IME)**Nota:** Quando IME puder ser usado para monitorar os dispositivos de sensor que executam o ips Cisco 5.0 e mais atrasado, alguma dos novos recursos e da funcionalidade entregados em IME é apoiada somente nos sensores que executam o ips Cisco 6.1 ou mais atrasado.**Nota:** O Intrusion Prevention System (IPS) seguro 5.x de Cisco apoia somente o sensor virtual vs0 do padrão. Os sensores virtuais diferentes do padrão vs0 são apoiados em IPS 6.x e mais tarde.

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

Esta configuração pode igualmente ser usada com estes sensores:

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

Convenções

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

Informações de Apoio

Sobre o motor da análise

O motor da análise executa a análise do pacote e a detecção alerta. Monitora o tráfego que corre através de interfaces especificadas. Você cria sensores virtuais no motor da análise. Cada sensor virtual tem um nome exclusivo com uma lista de relações, de pares inline da relação, de pares inline VLAN, e de grupos vlan associados com ele. A fim evitar edições pedindo da definição, nenhum conflito ou as sobreposições são permitidos nas atribuições. Você atribui relações, pares inline da relação, pares inline VLAN, e grupos vlan a um sensor virtual específico de modo que nenhum pacote seja processado por mais de um sensor virtual. Cada sensor virtual é associado igualmente com uma definição especificamente Nomeado da assinatura, as regras da ação do evento, e a configuração da detecção de anomalia. Os pacotes das relações, dos pares inline da relação, dos pares inline VLAN, e dos grupos vlan que não são atribuídos a nenhum sensor virtual são dispostos basearam na configuração inline do desvio.

Sobre sensores virtuais

O sensor pode receber entradas de dados de um ou muito fluxo de dados monitorado. Estes fluxos de dados monitorados podem ser portas da interface física ou portas da interface virtual. Por exemplo, um único sensor pode monitorar o tráfego na frente do Firewall, atrás do Firewall, ou de na frente e atrás do Firewall de simultaneamente. E um único sensor pode monitorar uns ou vários fluxos de dados. Nesta situação, uma única política do sensor ou configuração são aplicadas a todos os fluxos de dados monitorados. Um sensor virtual é um levantamento de dados que seja definido por um grupo de políticas da configuração. O sensor virtual é aplicado a um grupo de pacotes como definido pelo componente da relação. Um sensor virtual pode monitorar segmentos múltiplos, e você pode aplicar uma política ou uma configuração diferente para cada sensor virtual dentro de um único sensor físico. Você pode estabelecer uma política diferente pelo segmento monitorado sob a análise. Você pode igualmente aplicar o mesmo exemplo da política, por exemplo, sig0, rules0, ou ad0, aos sensores virtuais diferentes. Você pode atribuir relações, pares inline da relação, pares inline VLAN, e grupos vlan a um sensor virtual.

Nota: O Intrusion Prevention System (IPS) seguro de Cisco não apoia mais de quatro sensores virtuais. O sensor virtual do padrão é vs0. Você não pode suprimir do sensor virtual do padrão. A lista de interface, o modo operacional da detecção de anomalia, o modo de seguimento da sessão de TCP inline, e a descrição virtual do sensor são as únicas características que de configuração você pode mudar para o sensor virtual do padrão. Você não pode mudar a definição da assinatura, as regras da ação do evento, ou as políticas da detecção de anomalia.

Vantagens e limitações da virtualização

Vantagens da virtualização

A virtualização tem estas vantagens:

- Você pode aplicar configurações diferentes aos grupos diferentes de tráfego.
- Você pode monitorar duas redes com sobreposição de espaços IP com o um sensor.
- Você pode monitorar tanto dentro como fora de um Firewall ou do dispositivo NAT.

Limitações da virtualização

A virtualização tem estas limitações:

- Você deve atribuir ambos os lados do tráfego assimétrico ao mesmo sensor virtual.
- O uso da captação VACL ou do PERÍODO (monitoração promíscuo) é incompatível no que diz respeito ao VLAN que etiqueta, que causa problemas com grupos vlan.Quando você usa o Cisco IOS Software, uma porta da captação VACL ou um alvo do PERÍODO não recebem sempre pacotes rotulados mesmo se é configurado para o entroncamento.Quando você usa o MSFC, o interruptor do caminho rápido das rotas aprendidas muda o comportamento de captações e de PERÍODO VACL.
- A loja persistente é limitada.

Exigências da virtualização

A virtualização manda estes traficar exigências da captação:

- O sensor virtual deve receber o tráfego que tem os encabeçamentos 802.1q, a não ser o tráfego no VLAN nativo da porta da captação.
- O sensor deve ver ambos sentidos do tráfego no mesmo grupo vlan no mesmo sensor virtual para todo o sensor dado.

Configurar

Nesta seção, você é presentado com a informação para adicionar, edita, e suprime de sensores virtuais.

Adicionar sensores virtuais

Emita o comando name do virtual-sensor no submode do motor da análise do serviço a fim criar um sensor virtual. Você atribui políticas (detecção de anomalia, regras da ação do evento, e definição da assinatura) ao sensor virtual. Então você atribui pares da relação das relações (promíscuo, inline, pares inline VLAN, e grupos vlan) ao sensor virtual. Você deve configurar os pares inline da relação e pares VLAN antes que você possa os atribuir a um sensor virtual. As seguintes opções se aplicam:

- **detecção de anomalia** — Parâmetros da detecção de anomalia.nome do anomalia-detecção-**nome** — Nome da política da detecção de anomalia**modo operacional** — Modo da detecção de anomalia (**inativo, aprenda, detecte**)
- **descrição** — Descrição do sensor virtual
- **evento-ação-regras** — O nome da ação do evento ordena a política
- **inline-TCP-EVASÃO-PROTEÇÃO-MODE** — Deixa-o escolher que o tipo de modo do normalizador você precisa para a inspeção do tráfego:**assimétrico** — Pode somente ver um sentido do fluxo de tráfego bidirecional. A proteção assimétrica do modo relaxa a proteção da evasão na camada TCP.**Nota:** O modo assimétrico deixa o estado do sincronizar do sensor com o fluxo e mantém a inspeção para aqueles motores que não exigem ambos sentidos. O modo assimétrico abaixa a Segurança porque a proteção completa exige ambos os lados do tráfego ser considerada.**restrito** — Se um pacote é faltado por qualquer razão, todos os pacotes depois que o pacote faltado não é processado. A proteção restrita da evasão fornece a aplicação completa do estado TCP e do seguimento da sequência.**Nota:** Todos os pacotes estragados ou pacotes faltados podem produzir os despedimentos das assinaturas 1300 ou 1330 do motor do normalizador, que tentam corrigir a situação, mas podem conduzir às conexões negadas.
- **inline-TCP-SESSÃO-SEGUIR-MODE** — Método avançado que permite que você identifique a sessão de TCP duplicada no tráfego inline. O padrão é o sensor virtual, que é quase sempre a melhor escolha.**virtual-sensor** — Todos os pacotes com a mesma chave de sessão (AaBb) dentro de um sensor virtual pertencem à mesma sessão.**relação-e-VLAN** — Todos os pacotes com a mesma chave de sessão (AaBb) no mesmo VLAN (ou em pares inline VLAN) e na mesma relação pertencem à mesma sessão. Os pacotes com a mesma chave mas em VLAN diferentes ou em relações são seguidos independentemente.**VLAN-somente** — Todos os pacotes com a mesma chave de sessão (AaBb) no mesmo VLAN (ou em pares inline VLAN) apesar da relação pertencem à mesma sessão. Os pacotes com a mesma chave mas em VLAN diferentes são seguidos independentemente.

- **assinatura-definição** — Nome da política da definição da assinatura
- **interfaces lógica** — Nome das interfaces lógica (pares inline da relação)
- **interfaces física** — Nome dos pares VLAN das interfaces física (promíscuo, inline, e dos grupos vlan)**subinterface-número** — O número físico da subinterface. Se o subinterface-tipo não é nenhum, o valor de 0 indica que a relação inteira está atribuída no modo misturado.**não** — Remove uma entrada ou uma seleção

A fim adicionar um sensor virtual, termine estas etapas:

1. Entre ao CLI com uma conta com privilégios do administrado.
2. Entre no modo da análise do serviço.`sensor# **configure terminal** sensor(config)# **service analysis-engine** sensor(config-ana)#`
3. Adicionar um sensor virtual.`sensor(config-ana)# **virtual-sensor vs2** sensor(config-ana-vir)#`
4. Adicionar uma descrição para este sensor virtual.`sensor(config-ana-vir)# **description virtual sensor 2**`
5. Atribua uma política e um modo operacional da detecção de anomalia 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. Atribua uma política das regras da ação do evento a este sensor virtual.`sensor(config-ana-vir-ano)# exit`

   `sensor(config-ana-vir)# **event-action-rules rules1**`
7. Atribua uma política da definição da assinatura a este sensor virtual.`sensor(config-ana-vir)# **signature-definition sig1**`
8. Atribua o modo de seguimento da sessão de TCP inline.`sensor(config-ana-vir)# **inline-TCP-session-tracking-mode virtual-sensor**` O padrão é o modo virtual do sensor, que é quase sempre a melhor opção a escolher.
9. Atribua o modo de proteção inline da evasão TCP.`sensor(config-ana-vir)# **inline-TCP-evasion-protection-mode strict**` O padrão é o modo restrito, que é quase sempre a melhor opção a escolher.
10. Indique a lista de relações disponíveis.`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. Atribua o modo misturado conecta-o querem adicionar a este sensor virtual.`sensor(config-ana-vir)# **physical-interface GigabitEthernet0/2**` Repita esta etapa para todas as relações promíscuos que você quer atribuir a este sensor virtual.
12. Atribua a relação inline emparelha-o querem adicionar a este sensor virtual.`sensor(config-ana-vir)# **logical-interface inline_interface_pair_name**` Você deve já ter emparelhado as relações.
13. Atribua as subinterfaces dos pares inline VLAN ou agrupe-o querem adicionar como mostrado a este sensor virtual abaixo:`sensor(config-ana-vir)# **physical-interface GigabitEthernet2/0 subinterface-number subinterface_number**` Você deve já ter subdividido todas as relações em pares ou em grupos VLAN.
14. Verifique os ajustes virtuais do 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. Retire o modo do motor da análise.`sensor(config-ana-vir)# exit sensor(config-ana)# exit sensor(config)# Apply Changes:?[yes]:`
16. A imprensa **entra** a fim aplicar as mudanças ou entrá-las **não** para rejeitá-las.

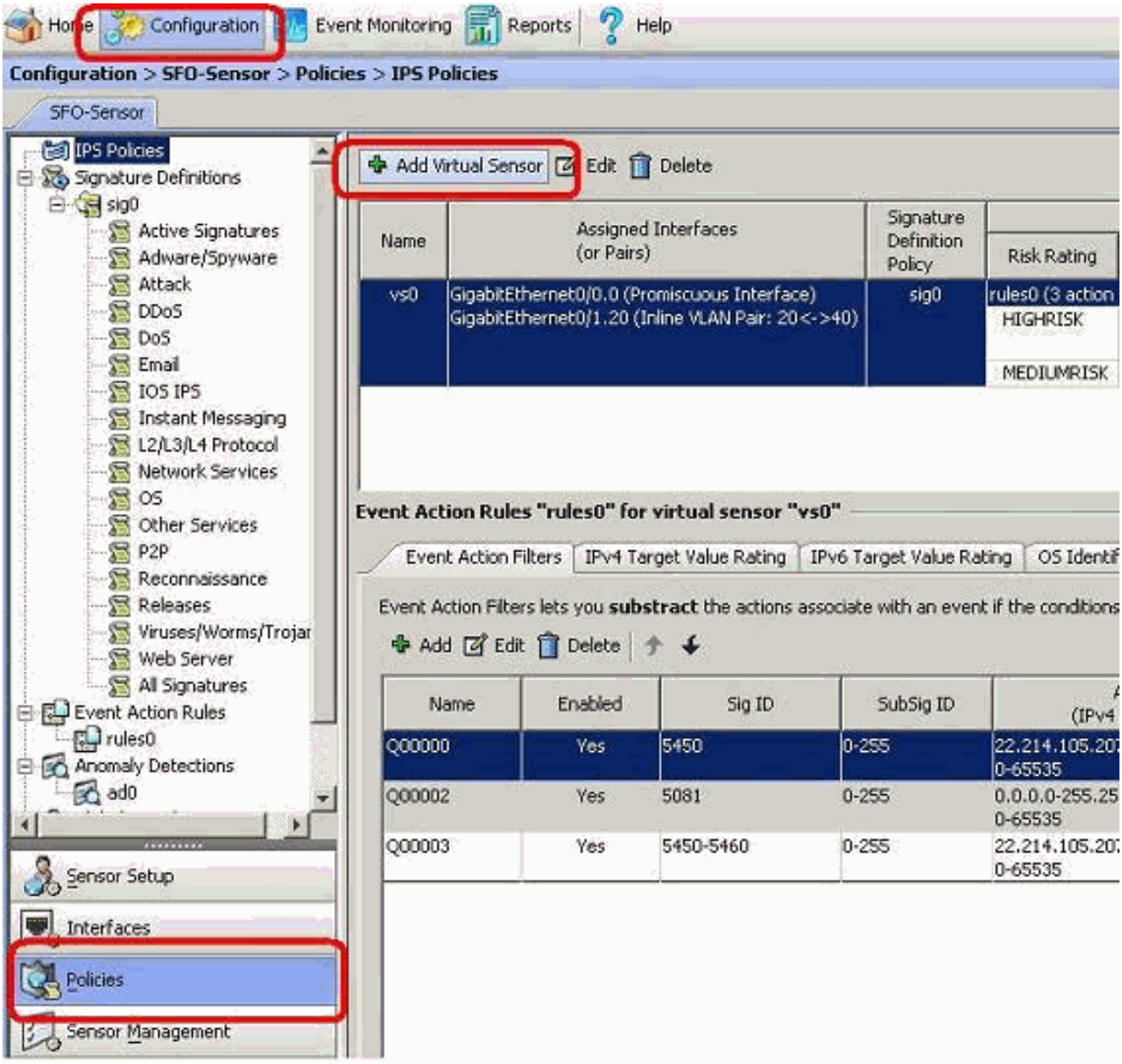
Isto termina o processo para adicionar um sensor virtual ao Intrusion Prevention System (IPS) seguro de Cisco. Termine o mesmo procedimento para adicionar uns sensores mais virtuais.

Nota: O Intrusion Prevention System (IPS) seguro de Cisco não apoia mais de quatro sensores virtuais. O sensor virtual do padrão é vs0.

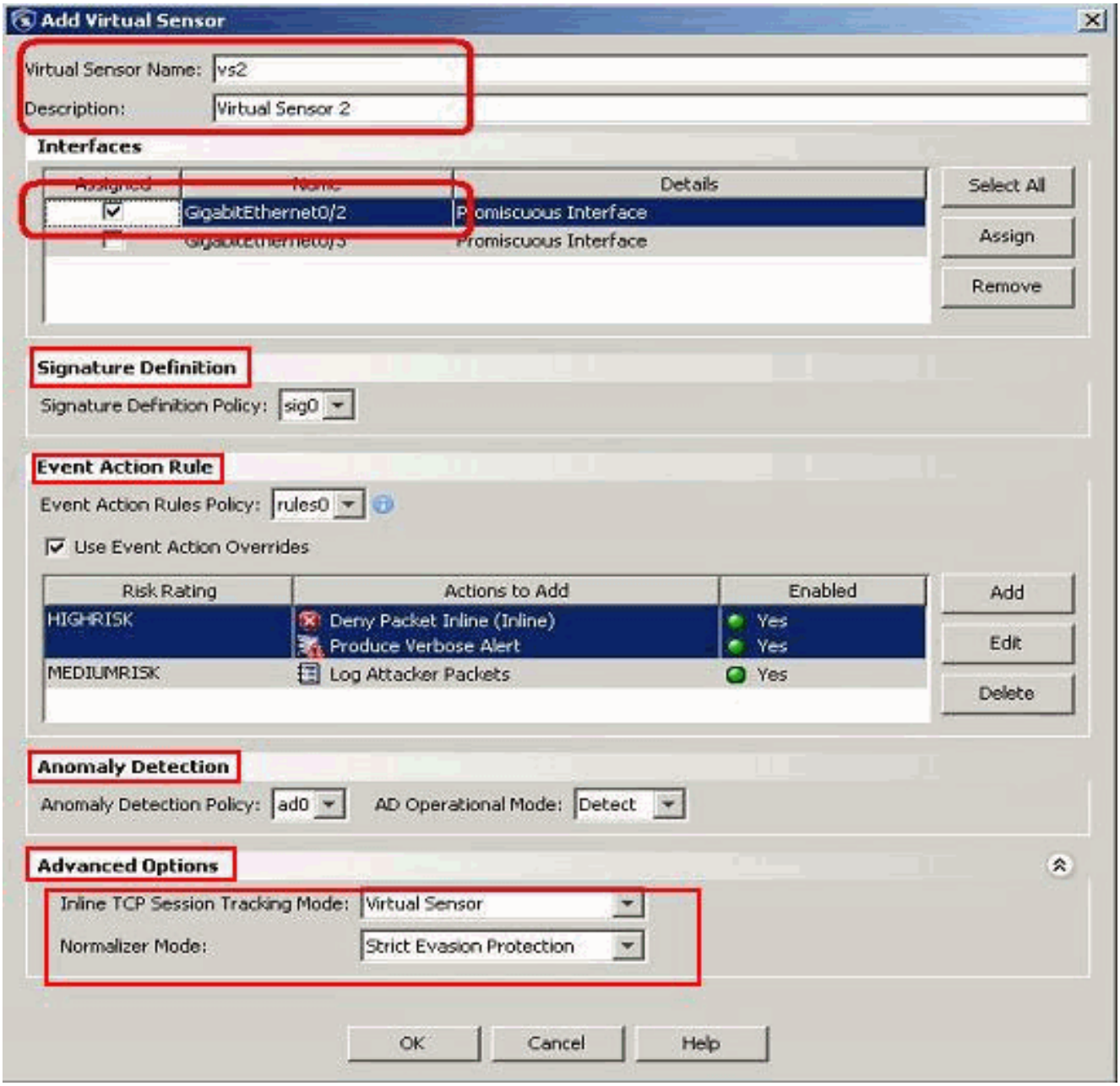
Adicionar o sensor virtual com IME

Termine estas etapas a fim configurar um sensor virtual no Intrusion Prevention System (IPS) seguro de Cisco com o gerente do ips Cisco expresso:

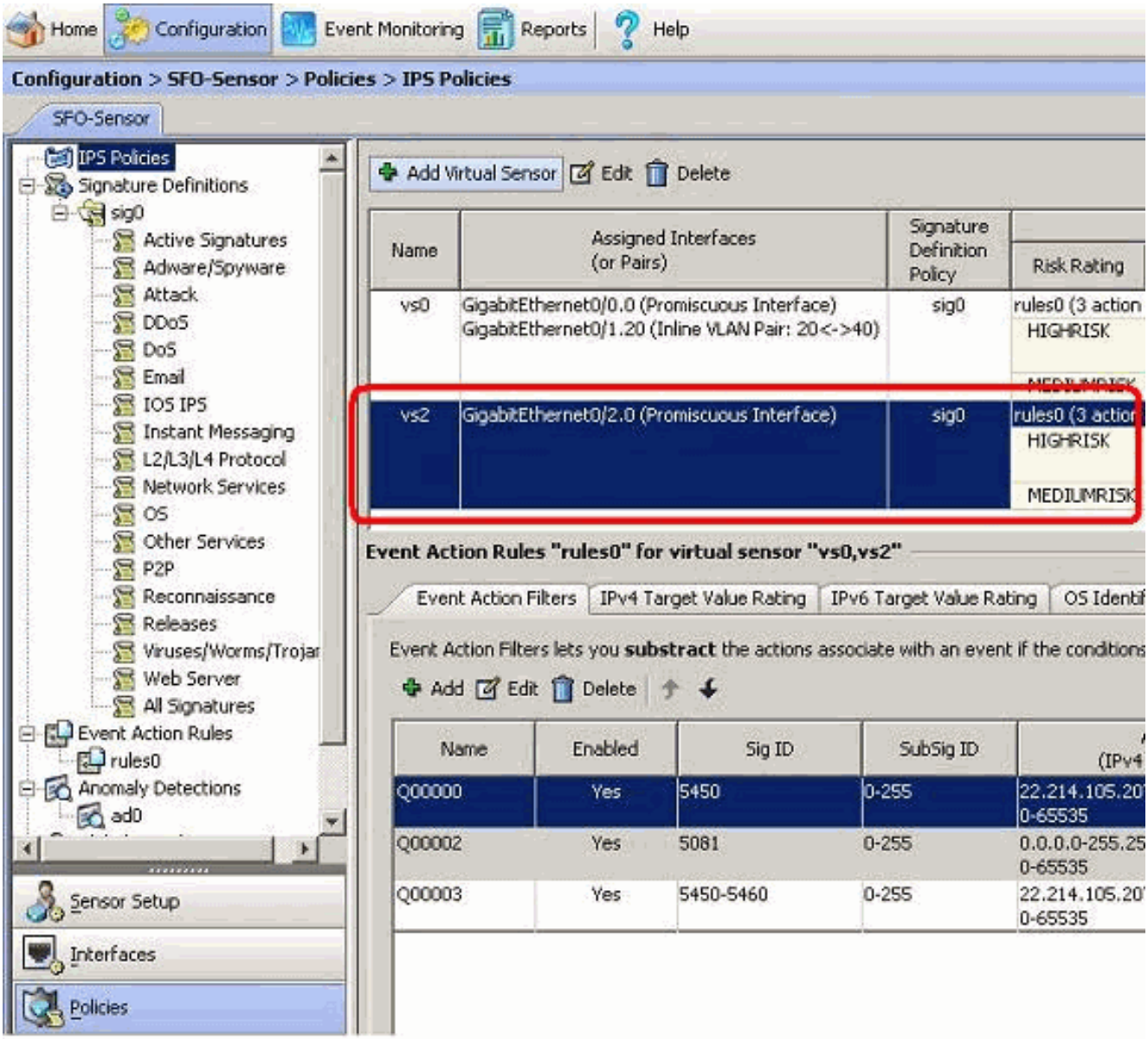
1. Escolha a **configuração > as políticas de SFO-Sensor> Policies> IPS**. Então, clique sobre o **sensor virtual Add** segundo as indicações do tiro de tela.



2. Nomeie o sensor virtual (vs2 neste exemplo) e adicionar uma descrição ao sensor virtual no espaço fornecido. Igualmente atribua o modo misturado conecta-o querem adicionar a este sensor virtual. O Gigabit Ethernet 0/2 é escolhido aqui. Forneça agora os detalhes na **definição da assinatura**, na **regra da ação do evento**, na **detecção de anomalia** e nas seções **avançadas das opções** segundo as indicações do screen shot.Sob **opções avançadas** forneça os detalhes sobre o modo de seguimento da sessão de TCP e o modo do normalizador. Aqui o **modo de seguimento da sessão de TCP** é **sensor virtual** e o **modo do normalizador** é **modo de proteção restrito da evasão**.



3. Clique em **OK**.
4. O sensor virtual recentemente adicionado vs2 é mostrado na lista de sensores virtuais. O clique **aplica-se** para que a configuração de sensor virtual nova seja enviada ao Intrusion Prevention System (IPS) seguro de
Cisco.



Isto termina a configuração para adicionar um sensor virtual.

Edite sensores virtuais

Estes parâmetros de um sensor virtual podem ser editados:

- Política da definição da assinatura
- A ação do evento ordena a política
- Política da detecção de anomalia
- Modo operacional da detecção de anomalia
- Modo de seguimento da sessão de TCP Inline
- Descrição
- Relações atribuídas

A fim editar um sensor virtual, termine estas etapas:

1. Entre ao CLI com uma conta com privilégios do administrado.
2. Entre no modo da análise do serviço.`sensor# configure terminal sensor(config)# service analysis-engine sensor(config-ana)#`
3. Edite o sensor virtual, vs1.`sensor(config-ana)# virtual-sensor vs2 sensor(config-ana-vir)#`
4. Edite a descrição deste sensor virtual.`sensor(config-ana-vir)# description virtual sensor A`

5. Mude a política e o modo operacional da detecção de anomalia atribuídos 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. Mude a política das regras da ação do evento atribuída a este sensor virtual.`sensor(config-ana-vir-ano)# exit`

   `sensor(config-ana-vir)# **event-action-rules rules0**`
7. Mude a política da definição da assinatura atribuída a este sensor virtual.`sensor(config-ana-vir)# **signature-definition sig0**`
8. Mude o modo de seguimento da sessão de TCP inline.`sensor(config-ana-vir)# **inline-TCP-session-tracking-mode interface-and-vlan**` O padrão é o modo virtual do sensor, que é quase sempre a melhor opção a escolher.
9. Indique a lista de relações disponíveis.`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. Mude as relações do modo misturado atribuídas a este sensor virtual.`sensor(config-ana-vir)# physical-interface GigabitEthernet0/2`
11. Mude os pares inline da relação atribuídos a este sensor virtual.`sensor(config-ana-vir)# **logical-interface inline_interface_pair_name**` Você deve já ter emparelhado as relações.
12. Mude a subinterface com os pares inline ou os grupos VLAN atribuídos a este sensor virtual.`sensor(config-ana-vir)# physical-interface GigabitEthernet2/0 subinterface-number subinterface_number`Você deve já ter subdividido todas as relações em pares ou em grupos VLAN.
13. Verifique os ajustes virtuais editados do 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. Retire o modo do motor da análise.`sensor(config-ana)# exit`

    `sensor(config)#`

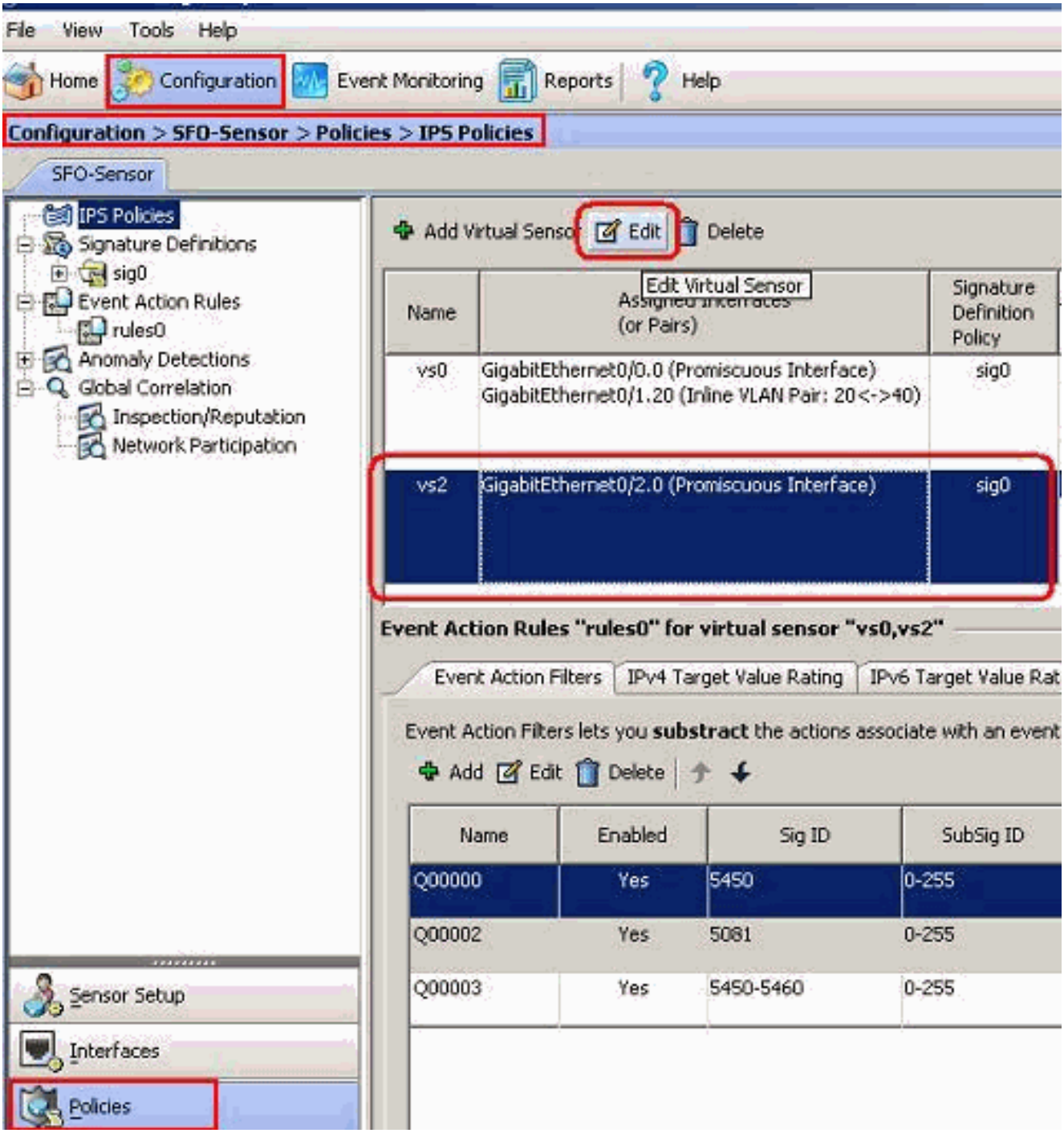
    `Apply Changes:?[yes]:`
15. A imprensa **entra** a fim aplicar as mudanças ou entrá-las **não** para rejeitá-las.

Edite o sensor virtual com IME

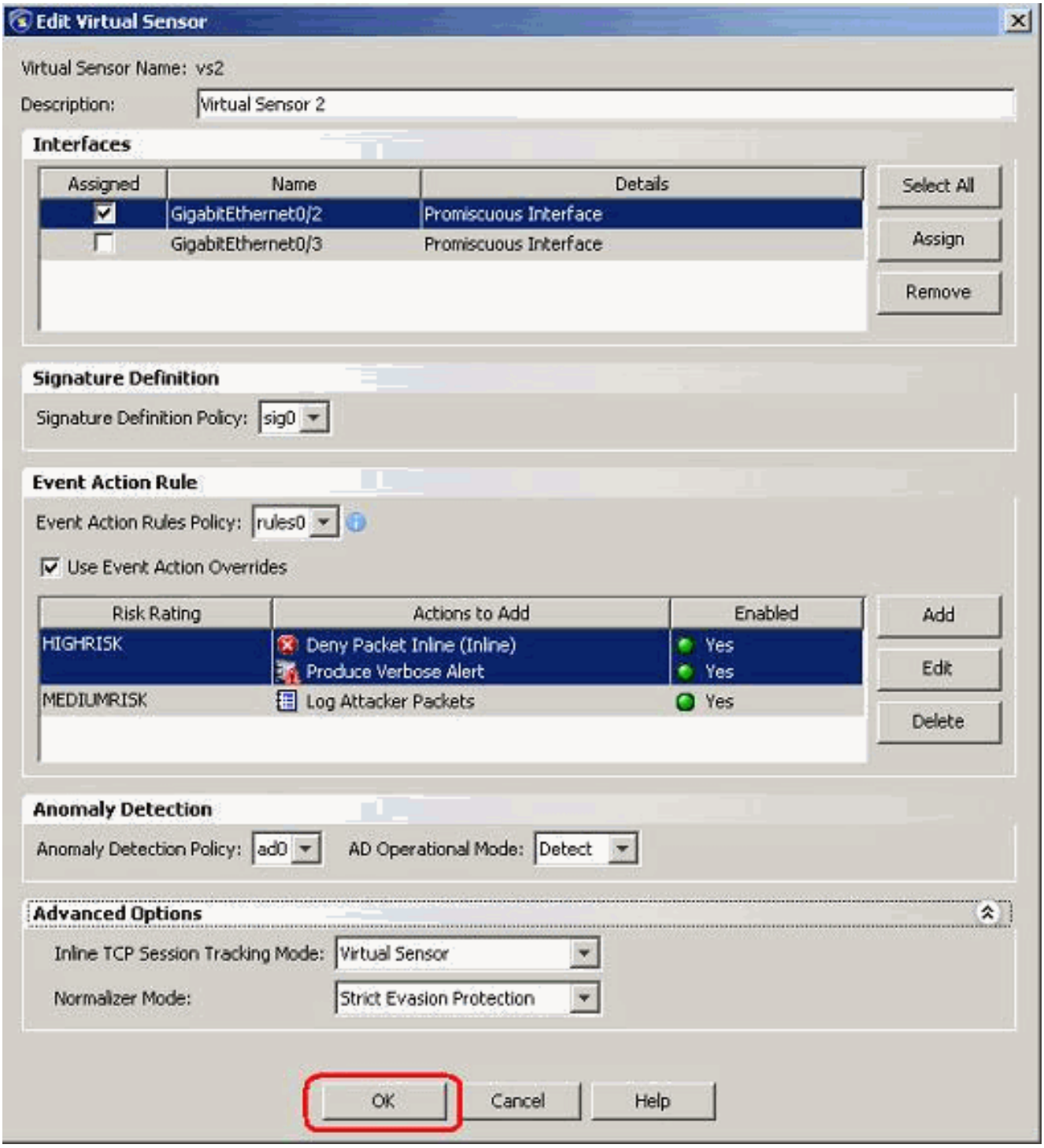
Termine estas etapas a fim editar um sensor virtual no Intrusion Prevention System (IPS) seguro de Cisco com o gerente do ips Cisco expresso:

1. Escolha a **configuração > as políticas de SFO-Sensor> Policies> IPS**.
2. Escolha o sensor virtual a ser editado, e clique-o então **editam** segundo as indicações do tiro

de tela. Neste exemplo vs2 é o sensor virtual a ser editado.



3. No indicador **virtual do sensor da edição**, faça mudanças aos parâmetros para o sensor virtual atual sob a **definição da assinatura das** seções, a **regra da ação do evento**, a **detecção de anomalia** e as **opções avançadas**. Clique a **APROVAÇÃO**, e clique-a então **aplicam-se**.



Isto termina o processo para editar um sensor virtual.

Sensores virtuais da supressão

A fim suprimir de um sensor virtual, termine estas etapas:

1. A fim suprimir de um sensor virtual, não emita **nenhum** comando do 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 o sensor virtual suprimido.`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)#` Somente o sensor virtual do padrão, **vs0**, esta presente.

3. Retire o modo do motor da análise.`sensor(config-ana)# exit`

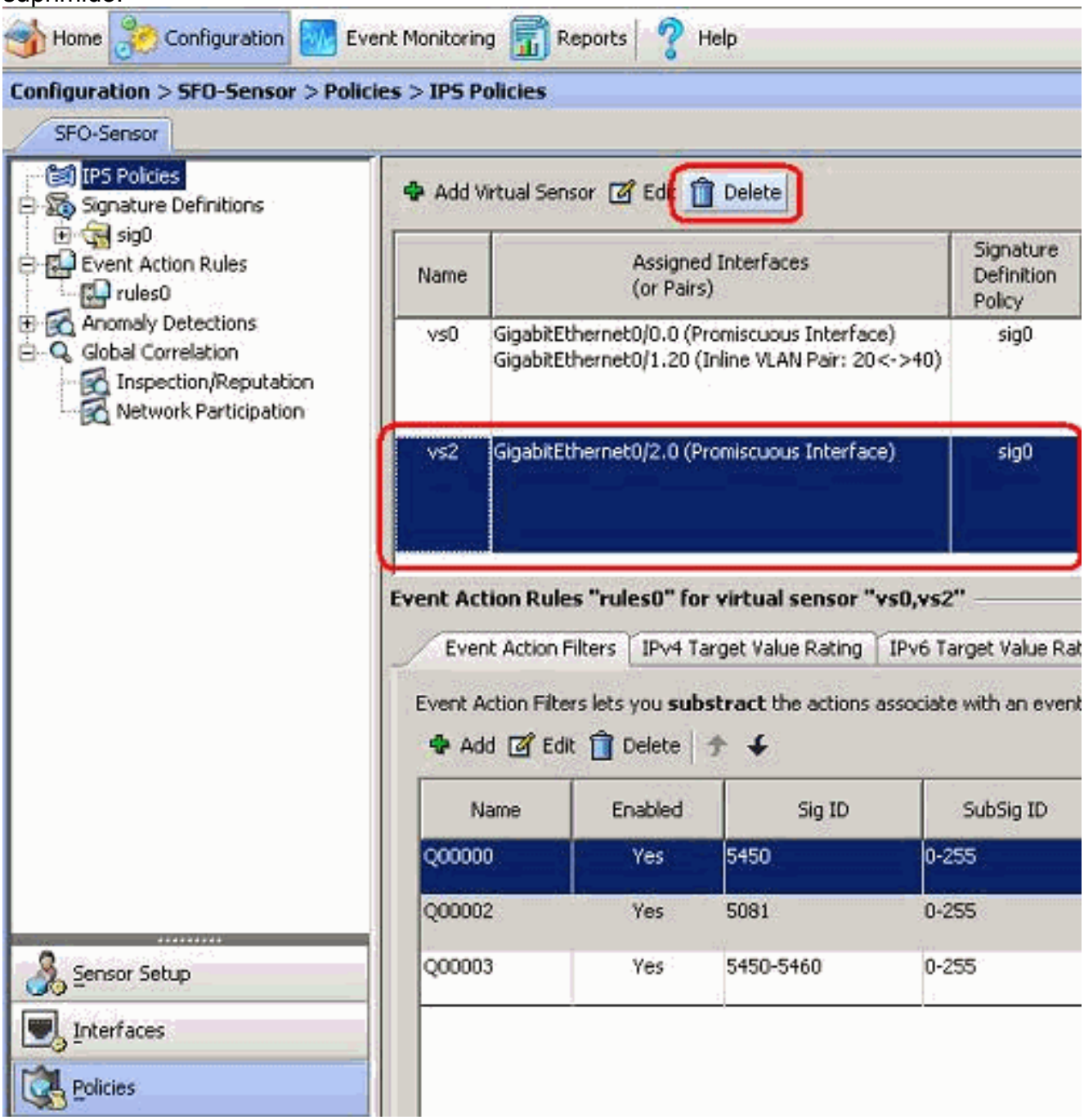
```
sensor(config)#
Apply Changes:?[yes]:
```

Suprima do sensor virtual com IME

Termine isto pisa a fim suprimir de um sensor virtual no Intrusion Prevention System (IPS) seguro de Cisco com o gerente do ips Cisco expresso:

1. Escolha a **configuração > as políticas de SFO-Sensor> Policies> IPS**.

2. Escolha o sensor virtual a ser suprimido, e clique então a **supressão**, segundo as indicações do tiro de tela. Neste exemplo vs2 é o sensor virtual a ser suprimido.



Isto termina o processo para suprimir de um sensor virtual. O sensor virtual vs2 é suprimido.

Troubleshooting

O gerente IPS expresso não se lança

Problema

Quando uma tentativa é feita para alcançar o IPS com o IME, o gerente IPS expresso não começa e este Mensagem de Erro é recebido:

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

Solução

A fim resolver isto, recarregue a estação de trabalho PC IME.

Informações Relacionadas

- Página de suporte do Sistema de prevenção de intrusões da Cisco
- Página de suporte expressa do gerente do ips Cisco
- Network Time Protocol (NTP)
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems