IPS 6.X et version ultérieure : Exemple de configuration de capteurs virtuels avec IME

Contenu

Introduction

Ce document explique la fonction de l'engine d'analyse et comment créer, éditer, et supprimer les capteurs virtuels sur le Système de prévention d'intrusion (IPS) Cisco Secure avec le Cisco IPS Manager Express (IME). Il explique également comment assigner des interfaces à un capteur virtuel.

Remarque: AIM-IPS et NME-IPS ne prennent en charge pas la virtualisation.

Conditions préalables

Conditions requises

Aucune condition préalable spécifique n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Périphérique IPS de gamme Cisco 4200 qui exécute la version de logiciel 6.0 et plus tard
- Version 6.1.1 et ultérieures du Cisco IPS Manager Express (IME)**Remarque:** Tandis qu'IME peut être utilisé pour surveiller les périphériques de capteur qui exécutent le Cisco IPS 5.0 et plus tard, certaines des nouvelles fonctionnalités et caractéristiques fournies dans IME sont seulement prises en charge sur les capteurs qui exécutent le Cisco IPS 6.1 ou plus tard.**Remarque:** Le Système de prévention d'intrusion (IPS) Cisco Secure 5.x prend en charge seulement le capteur virtuel par défaut vs0. Des capteurs virtuels autres que le par défaut vs0 sont pris en charge dans IPS 6.x et plus tard.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Produits connexes

Cette configuration peut également être utilisée avec ces capteurs :

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

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Au sujet de l'engine d'analyse

L'engine d'analyse exécute l'analyse de paquet et la détection vigilante. Il surveille le trafic qui traverse des interfaces spécifiées. Vous créez les capteurs virtuels dans l'engine d'analyse. Chaque capteur virtuel a un nom unique avec une liste d'interfaces, des paires intégrées d'interface, des paires intégrées VLAN, et des groupes VLAN associés avec lui. Afin d'éviter les questions de commande de définition, on ne permet aucun conflit ou superpositions dans les affectations. Vous affectez des interfaces, des paires intégrées d'interface, des paires intégrées VLAN, et des groupes VLAN à un capteur virtuel spécifique de sorte qu'aucun paquet ne soit traité par plus d'un capteur virtuel. Chaque capteur virtuel est également associé avec une définition spécifiquement Désignée de signature, des règles d'action d'événement, et la configuration de

détection d'anomalie. Des paquets des interfaces, des paires intégrées d'interface, des paires intégrées VLAN, et des groupes VLAN qui ne sont assignés à aucun capteur virtuel sont rejetés ont basé sur la configuration intégrée de contournement.

Au sujet des capteurs virtuels

Le capteur peut recevoir des entrées de données d'un ou beaucoup de flux de données surveillés. Ces flux de données surveillés peuvent être des ports d'interface physique ou des ports d'interface virtuelle. Par exemple, un trafic à un seul capteur de moniteur de boîte de devant le Pare-feu, par derrière le Pare-feu, ou de devant et derrière le Pare-feu simultanément. Et un moniteur à un seul capteur de boîte un ou plusieurs flux de données. Dans cette situation, une stratégie ou une configuration à un seul capteur est appliquée à tous les flux de données surveillés. Un capteur virtuel est une collecte des données qui est défini par un ensemble de stratégies de configuration. Le capteur virtuel est appliqué à un ensemble de paquets comme défini par le composant d'interface. Un capteur virtuel peut surveiller de plusieurs segments, et vous pouvez appliquer une stratégie ou une configuration différente pour chaque capteur virtuel dans un capteur physique simple. Vous pouvez installer une stratégie différente par segment surveillé sous l'analyse. Vous pouvez également appliquer le même exemple de stratégie, par exemple, sig0, rules0, ou ad0, à différents capteurs virtuels. Vous pouvez affecter des interfaces, des paires intégrées d'interface, des paires intégrées VLAN, et des groupes VLAN à un capteur virtuel.

Remarque: Le Système de prévention d'intrusion (IPS) Cisco Secure ne prend en charge pas plus de quatre capteurs virtuels. Le capteur virtuel par défaut est vs0. Vous ne pouvez pas supprimer le capteur virtuel par défaut. La liste interface, le mode opérationnel de détection d'anomalie, le mode de cheminement de session TCP intégrée, et la description virtuelle de capteur sont les seules caractéristiques de configuration que vous pouvez changer pour le capteur virtuel par défaut. Vous ne pouvez pas changer la définition de signature, les règles d'action d'événement, ou les stratégies de détection d'anomalie.

Avantages et restrictions de virtualisation

Avantages de virtualisation

La virtualisation a ces avantages :

- Vous pouvez s'appliquer différentes configurations à différents ensembles du trafic.
- Vous pouvez surveiller deux réseaux avec superposer les espaces IP avec un capteur.
- Vous pouvez surveiller à l'intérieur et à l'extérieur d'un Pare-feu ou d'un périphérique NAT.

Restrictions de virtualisation

La virtualisation a ces restrictions :

- Vous devez assigner les deux côtés du trafic asymétrique au même capteur virtuel.
- L'utilisation de la capture VACL ou de l'ENVERGURE (surveillance promiscueuse) est contradictoire en ce qui concerne le VLAN étiquetant, qui pose des problèmes avec des groupes VLAN.Quand vous utilisez le logiciel de Cisco IOS, un port de capture VACL ou une cible d'ENVERGURE ne reçoit pas toujours des paquets balisés même si elle est configurée pour la jonction.Quand vous utilisez le MSFC, la commutation de chemin rapide des routes

apprises change le comportement des captures et de l'ENVERGURE VACL.
- La mémoire persistante est limitée.

Conditions requises de virtualisation

La virtualisation a ces exigences de capture du trafic :

- Le capteur virtuel doit recevoir le trafic qui a des en-têtes de 802.1Q, autre que le trafic sur le VLAN indigène du port de capture.
- Le capteur doit voir les deux directions du trafic au même groupe VLAN dans le même capteur virtuel pour n'importe quel capteur donné.

Configurez

Dans cette section, vous êtes présenté avec les informations pour ajouter, éditer, et supprimer les capteurs virtuels.

Ajoutez les capteurs virtuels

Émettez la commande de nom de virtuel-capteur dans le sous-mode d'engine d'analyse de service afin de créer un capteur virtuel. Vous assignez des stratégies (détection d'anomalie, règles d'action d'événement, et définition de signature) au capteur virtuel. Alors vous affectez des paires d'interface d'interfaces (promiscueux, en ligne, des paires intégrées VLAN, et des groupes VLAN) au capteur virtuel. Vous devez configurer les paires intégrées d'interface et des paires VLAN avant que vous puissiez les assigner à un capteur virtuel. Ces options s'appliquent :

- **anomalie-détection** — Paramètres de détection d'anomalie.nom d'anomalie-détection-**nom** — Nom de la stratégie de détection d'anomalie**opérationnel-mode** — Mode de détection d'anomalie (**inactif, apprenez, le détectez**)
- **description** — Description du capteur virtuel
- **événement-action-règles** — Le nom de l'action d'événement ordonne la stratégie
- **en ligne-TCP-ÉVASION-PROTECTION-mode** — Vous permet de choisir dont le type de mode de normalisateur vous a besoin pour l'inspection du trafic :**asymétrique** — Peut seulement voir une direction d'écoulement du trafic bidirectionnel. La protection asymétrique de mode détend la protection d'évasion à la couche de TCP.**Remarque:** Le mode asymétrique permet le capteur de synchroniser l'état avec l'écoulement et de mettre à jour l'inspection pour ces engines qui n'exigent pas les deux directions. Le mode asymétrique diminue la Sécurité parce que la pleine protection exige des deux côtés du trafic d'être vus.**strict** — Si un paquet est manqué pour une raison quelconque, tous les paquets après que le paquet manqué ne soient pas traités. La protection stricte d'évasion fournit la pleine application de l'état de TCP et du cheminement d'ordre.**Remarque:** Tous les paquets en panne ou paquets manqués peuvent produire les mises à feu des signatures 1300 ou 1330 d'engine de normalisateur, qui essayent de corriger la situation, mais peuvent avoir comme conséquence les connexions refusées.
- **en ligne-TCP-SESSION-DÉPISTER-mode** — Méthode avancée qui te permet pour identifier la session TCP en double dans le trafic intégré. Le par défaut est le capteur virtuel, qui est presque toujours le meilleur choix.**virtuel-capteur** — Tous les paquets avec la même clé de session (AaBb) dans un capteur virtuel appartiennent à la même session.**interface-et-VLAN** —

Tous les paquets avec la même clé de session (AaBb) dans le même VLAN (ou des paires intégrées VLAN) et sur la même interface appartiennent à la même session. Des paquets avec la même clé mais sur différents VLAN ou interfaces sont dépistés indépendamment.**réservé à la VLAN** — Tous les paquets avec la même clé de session (AaBb) dans le même VLAN (ou des paires intégrées VLAN) indépendamment de l'interface appartiennent à la même session. Des paquets avec la même clé mais sur différents VLAN sont dépistés indépendamment.

- **signature-définition** — Nom de la stratégie de définition de signature
- **interfaces logiques** — Nom des interfaces logiques (paires intégrées d'interface)
- **physicaux-interface** — Nom des paires VLAN d'interfaces physiques (promiscueux, en ligne, et des groupes VLAN)**numéro de sous-interface** — Le numéro de sous-interface physique. Si le sous-interface-type n'en est aucun, la valeur de 0 indique que l'interface entière est assignée en mode promiscueux.**NO-** retire une entrée ou une sélection

Afin d'ajouter un capteur virtuel, terminez-vous ces étapes :

1. Ouvrez une session au CLI avec un compte avec des privilèges d'administrateur.
2. Entrez le mode d'analyse de service.`sensor# **configure terminal** sensor(config)# **service analysis-engine** sensor(config-ana)#`
3. Ajoutez un capteur virtuel.`sensor(config-ana)# **virtual-sensor vs2** sensor(config-ana-vir)#`
4. Ajoutez une description pour ce capteur virtuel.`sensor(config-ana-vir)# **description virtual sensor 2**`
5. Assignez une stratégie de détection d'anomalie et un mode opérationnel à ce capteur virtuel.`sensor(config-ana-vir)# **anomaly-detection** sensor(config-ana-vir-ano)# **anomaly-detection-name ad1** sensor(config-ana-vir-ano)# **operational-mode learn**`
6. Assignez une stratégie de règles d'action d'événement à ce capteur virtuel.`sensor(config-ana-vir-ano)# exit`

   `sensor(config-ana-vir)# **event-action-rules rules1**`
7. Assignez une stratégie de définition de signature à ce capteur virtuel.`sensor(config-ana-vir)# **signature-definition sig1**`
8. Assignez le mode de cheminement de session TCP intégrée.`sensor(config-ana-vir)# **inline-TCP-session-tracking-mode virtual-sensor**` Le par défaut est le mode virtuel de capteur, qui est presque toujours la meilleure option de choisir.
9. Assignez le mode intégré de protection d'évasion de TCP.`sensor(config-ana-vir)# **inline-TCP-evasion-protection-mode strict**` Le par défaut est le mode strict, qui est presque toujours la meilleure option de choisir.
10. Affichez la liste d'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. Assignez le mode promiscueux vous relie veulent ajouter à ce capteur virtuel.`sensor(config-ana-vir)# **physical-interface GigabitEthernet0/2**` Répétez cette étape pour toutes les interfaces promiscueuses que vous voulez assigner à ce capteur virtuel.
12. Assignez l'interface intégrée vous appareille veulent ajouter à ce capteur virtuel.`sensor(config-ana-vir)# **logical-interface inline_interface_pair_name**` Vous devez avoir déjà appareillé les interfaces.
13. Assignez les sous-interfaces des paires de l'en ligne VLAN ou vous groupez veulent ajouter à ce capteur virtuel comme affiché ci-dessous :`sensor(config-ana-vir)# **physical-interface**`

GigabitEthernet2/0 subinterface-number subinterface_number Vous devez avoir déjà subdivisé toutes les interfaces en paires ou groupes VLAN.

14. Vérifiez les configurations virtuelles de capteur.`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. Annulez le mode d'engine d'analyse.`sensor(config-ana-vir)# **exit** sensor(config-ana)# exit sensor(config)# Apply Changes:?[yes]:`
16. Appuyez sur **entrent** afin d'appliquer les modifications ou entrer **non** pour les jeter.

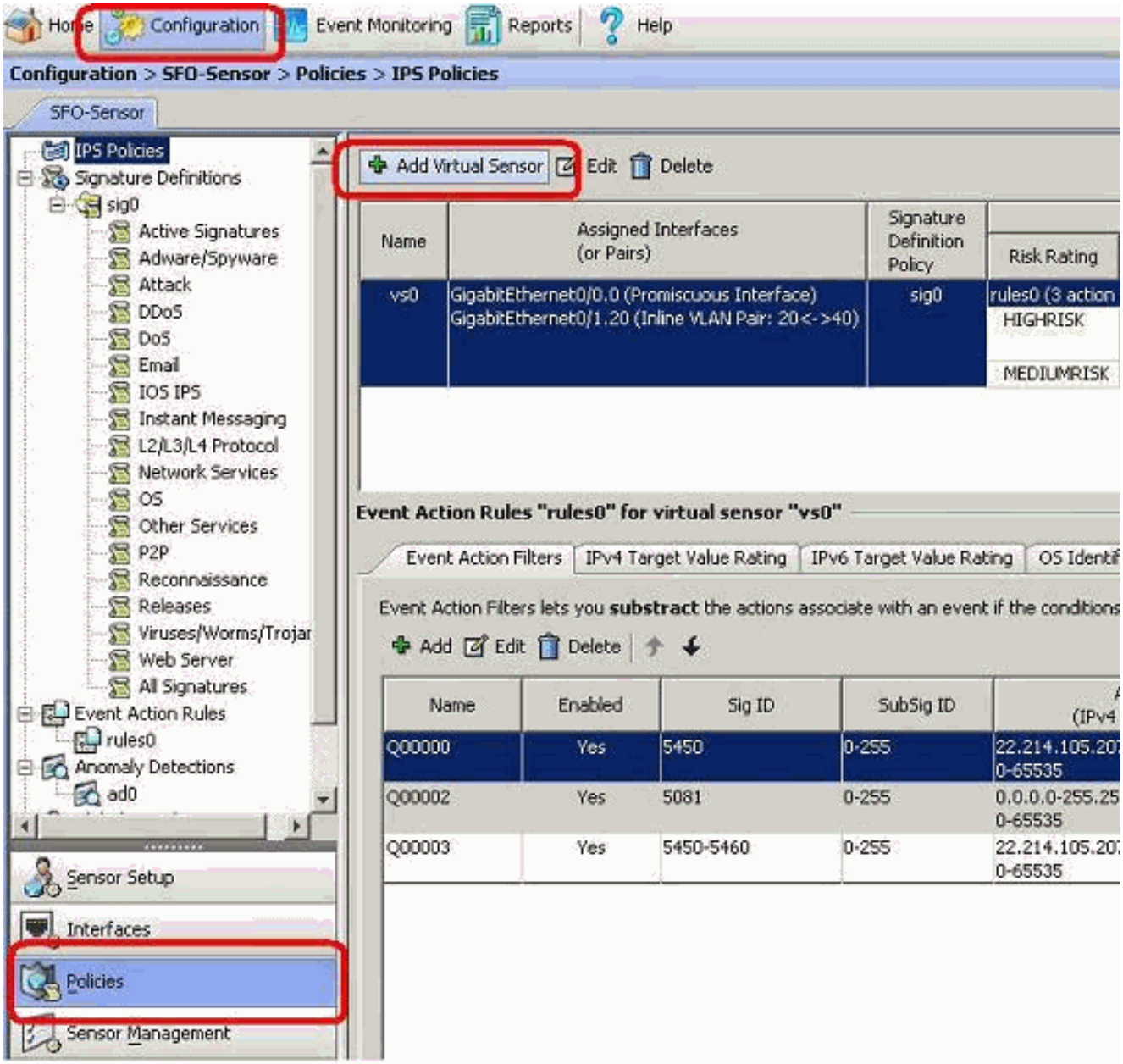
Ceci complète le processus pour ajouter un capteur virtuel au Système de prévention d'intrusion (IPS) Cisco Secure. Remplissez la même procédure pour ajouter des capteurs plus virtuels.

Remarque: Le Système de prévention d'intrusion (IPS) Cisco Secure ne prend en charge pas plus de quatre capteurs virtuels. Le capteur virtuel par défaut est vs0.

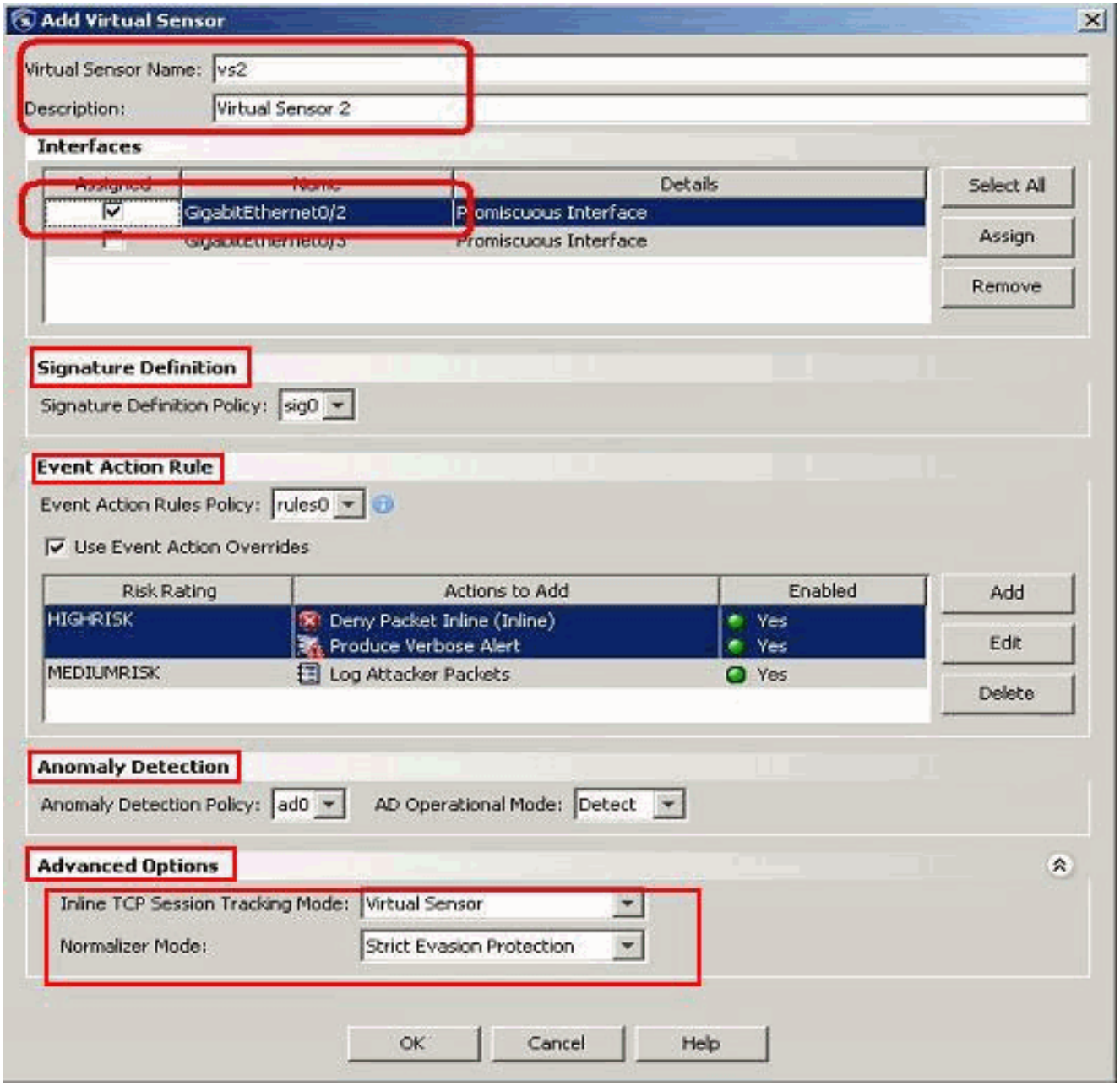
Ajoutez le capteur virtuel avec IME

Terminez-vous ces étapes afin de configurer un capteur virtuel sur le Système de prévention d'intrusion (IPS) Cisco Secure avec le Cisco IPS Manager Express :

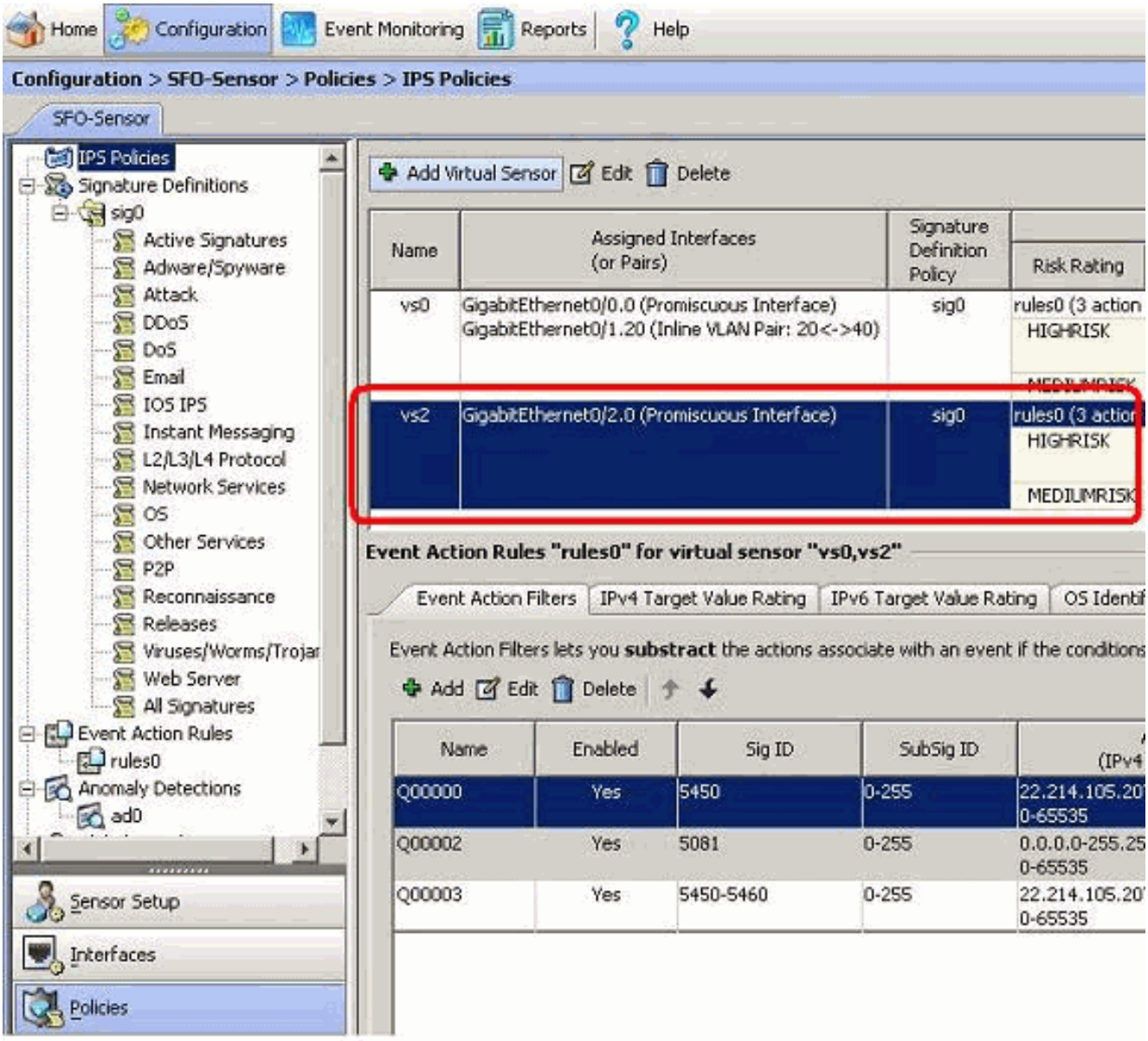
1. Choisissez la **configuration > les stratégies de SFO-Sensor> Policies> IPS**. Puis, cliquez sur en fonction le **capteur virtuel Add** suivant les indications du tir d'écran.



2. Nommez le capteur virtuel (vs2 dans cet exemple) et ajoutez une description au capteur virtuel dans l'espace prévu. Assignez également le mode promiscueux vous relie veulent ajouter à ce capteur virtuel. Le Gigabit Ethernet 0/2 est choisi ici. Fournissez maintenant les détails dans la **définition de signature**, la **règle d'action d'événement**, la **détection d'anomalie** et les sections **avancées d'options** suivant les indications de la copie d'écran.Sous des **options avancées** fournissez les détails au sujet du mode de cheminement de session TCP et du mode de normalisateur. Ici le **mode de cheminement de session TCP** est **capteur virtuel** et le **mode de normalisateur** est mode **strict de protection d'évasion**.



3. Cliquez sur **OK**.
4. Le capteur virtuel nouvellement ajouté vs2 est affiché dans la liste de capteurs virtuels. Cliquez sur Apply pour que la nouvelle configuration virtuelle de capteur soit envoyée au Système de prévention d'intrusion (IPS) Cisco
   Secure.



Ceci se termine la configuration pour ajouter un capteur virtuel.

Éditez les capteurs virtuels

Ces paramètres d'un capteur virtuel peuvent être édités :

- Stratégie de définition de signature
- L'action d'événement ordonne la stratégie
- Stratégie de détection d'anomalie
- Mode opérationnel de détection d'anomalie
- Mode de cheminement de session TCP intégrée
- Description
- Interfaces assignées

Afin d'éditer un capteur virtuel, terminez-vous ces étapes :

1. Ouvrez une session au CLI avec un compte avec des privilèges d'administrateur.
2. Entrez le mode d'analyse de service.`sensor# configure terminal sensor(config)# service analysis-engine sensor(config-ana)#`
3. Éditez le capteur virtuel, vs1.`sensor(config-ana)# virtual-sensor vs2 sensor(config-ana-vir)#`
4. Éditez la description de ce capteur virtuel.`sensor(config-ana-vir)# description virtual sensor`

A

5. Changez la stratégie de détection d'anomalie et le mode opérationnel assignés à ce capteur virtuel.`sensor(config-ana-vir)# anomaly-detection`

   `sensor(config-ana-vir-ano)# **anomaly-detection-name ad0** sensor(config-ana-vir-ano)# **operational-mode learn**`
6. Changez la stratégie de règles d'action d'événement assignée à ce capteur virtuel.`sensor(config-ana-vir-ano)# exit`

   `sensor(config-ana-vir)# **event-action-rules rules0**`
7. Changez la stratégie de définition de signature assignée à ce capteur virtuel.`sensor(config-ana-vir)# **signature-definition sig0**`
8. Changez le mode de cheminement de session TCP intégrée.`sensor(config-ana-vir)# **inline-TCP-session-tracking-mode interface-and-vlan**` Le par défaut est le mode virtuel de capteur, qui est presque toujours la meilleure option de choisir.
9. Affichez la liste d'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. Changez les interfaces promiscueuses de mode assignées à ce capteur virtuel.`sensor(config-ana-vir)# physical-interface GigabitEthernet0/2`
11. Changez les paires intégrées d'interface assignées à ce capteur virtuel.`sensor(config-ana-vir)# **logical-interface inline_interface_pair_name**` Vous devez avoir déjà appareillé les interfaces.
12. Changez la sous-interface avec les paires ou les groupes de l'en ligne VLAN assignés à ce capteur virtuel.`sensor(config-ana-vir)# physical-interface GigabitEthernet2/0 subinterface-number`
    `subinterface_number`Vous devez avoir déjà subdivisé toutes les interfaces en paires ou groupes VLAN.
13. Vérifiez les configurations virtuelles éditées de capteur.`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. Annulez le mode d'engine d'analyse.`sensor(config-ana)# exit`

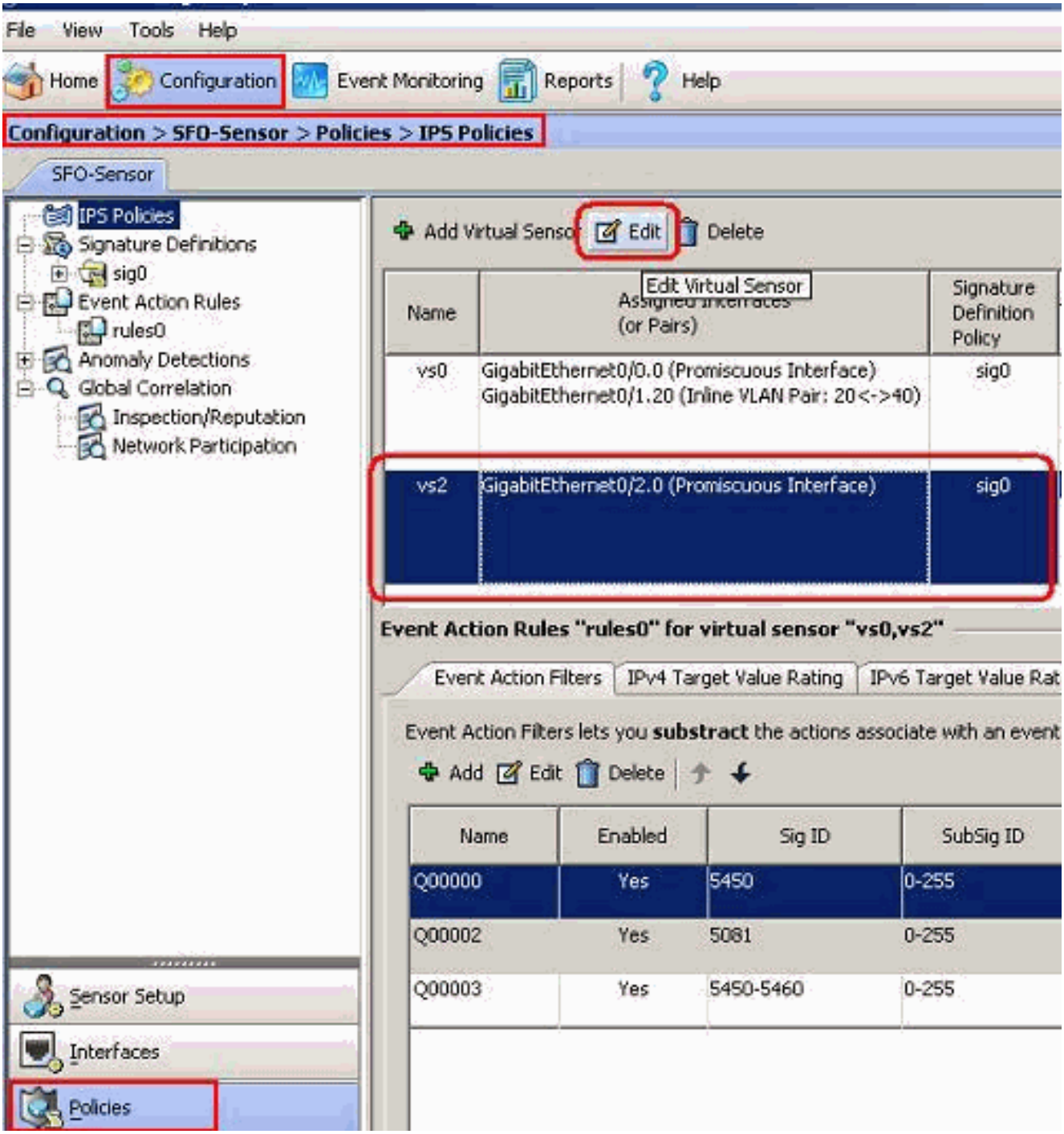
    `sensor(config)#`

    `Apply Changes:?[yes]:`
15. Appuyez sur **entrent** afin d'appliquer les modifications ou entrer **non** pour les jeter.

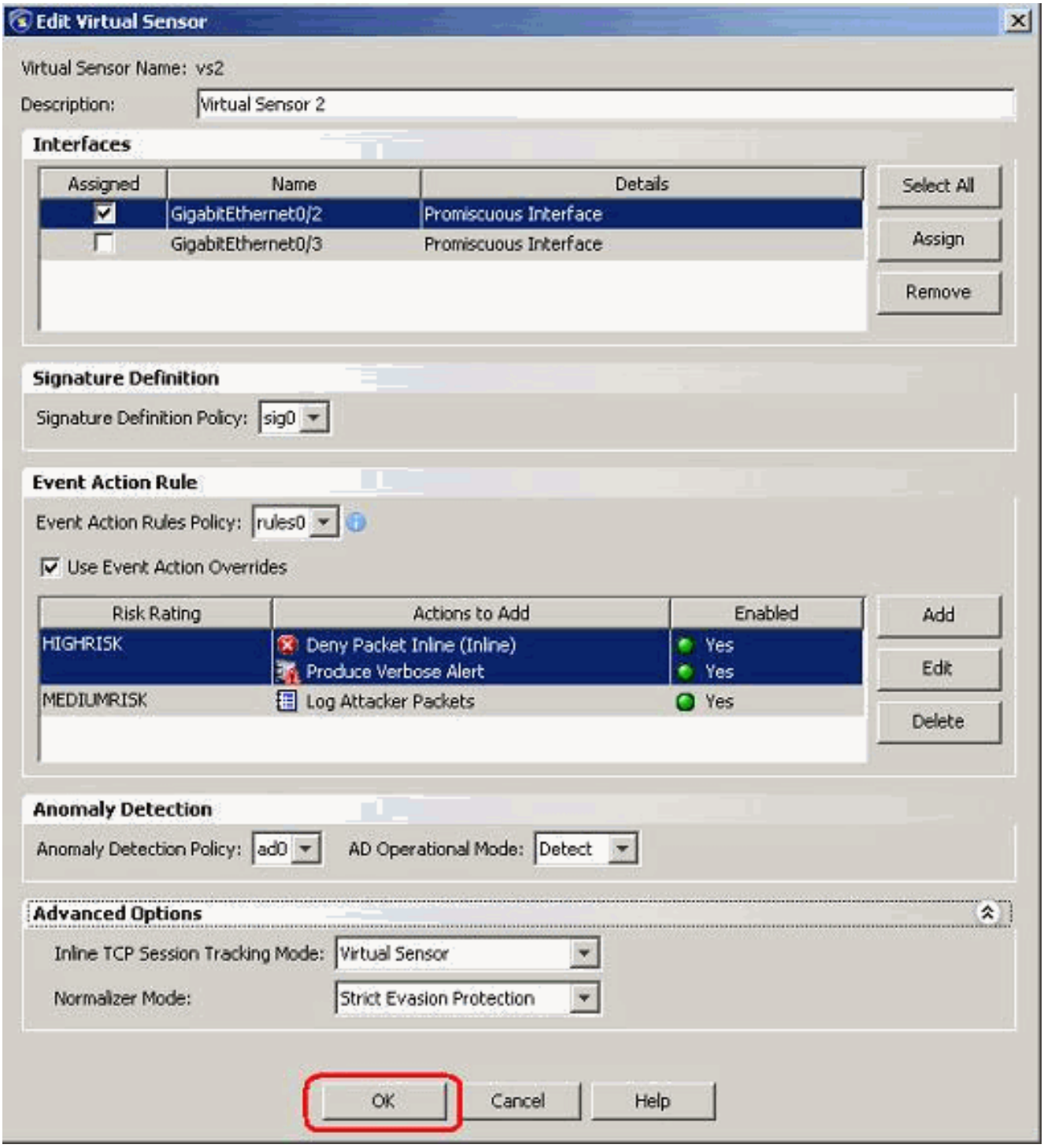
Éditez le capteur virtuel avec IME

Terminez-vous ces étapes afin d'éditer un capteur virtuel sur le Système de prévention d'intrusion (IPS) Cisco Secure avec le Cisco IPS Manager Express :

1. Choisissez la **configuration > les stratégies de SFO-Sensor> Policies> IPS**.
2. Choisissez le capteur virtuel à éditer, et puis cliquez sur Edit suivant les indications du tir d'écran. Dans cet exemple vs2 est le capteur virtuel à éditer.



3. Dans la fenêtre **virtuelle de capteur d'éditer**, apportez des modifications aux paramètres pour le capteur virtuel actuel sous la **définition de signature de** sections, la **règle d'action d'événement**, la **détection d'anomalie** et les **options avancées**. Cliquez sur **OK**, puis sur **Apply**.



Ceci complète le processus pour éditer un capteur virtuel.

Capteurs virtuels d'effacement

Afin de supprimer un capteur virtuel, terminez-vous ces étapes :

1. Afin de supprimer un capteur virtuel, n'émettez l'**aucune** commande de virtuel-**capteur**.`sensor(config-ana)# **virtual-sensor vs2** sensor(config-ana-vir)# sensor(config-ana-vir)# exit sensor(config-ana)# **no virtual-sensor vs2**`
2. Vérifiez le capteur virtuel supprimé.`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)#` Seulement le capteur virtuel par défaut, **vs0**, est présent.

3. Annulez le mode d'engine d'analyse.`sensor(config-ana)# exit`

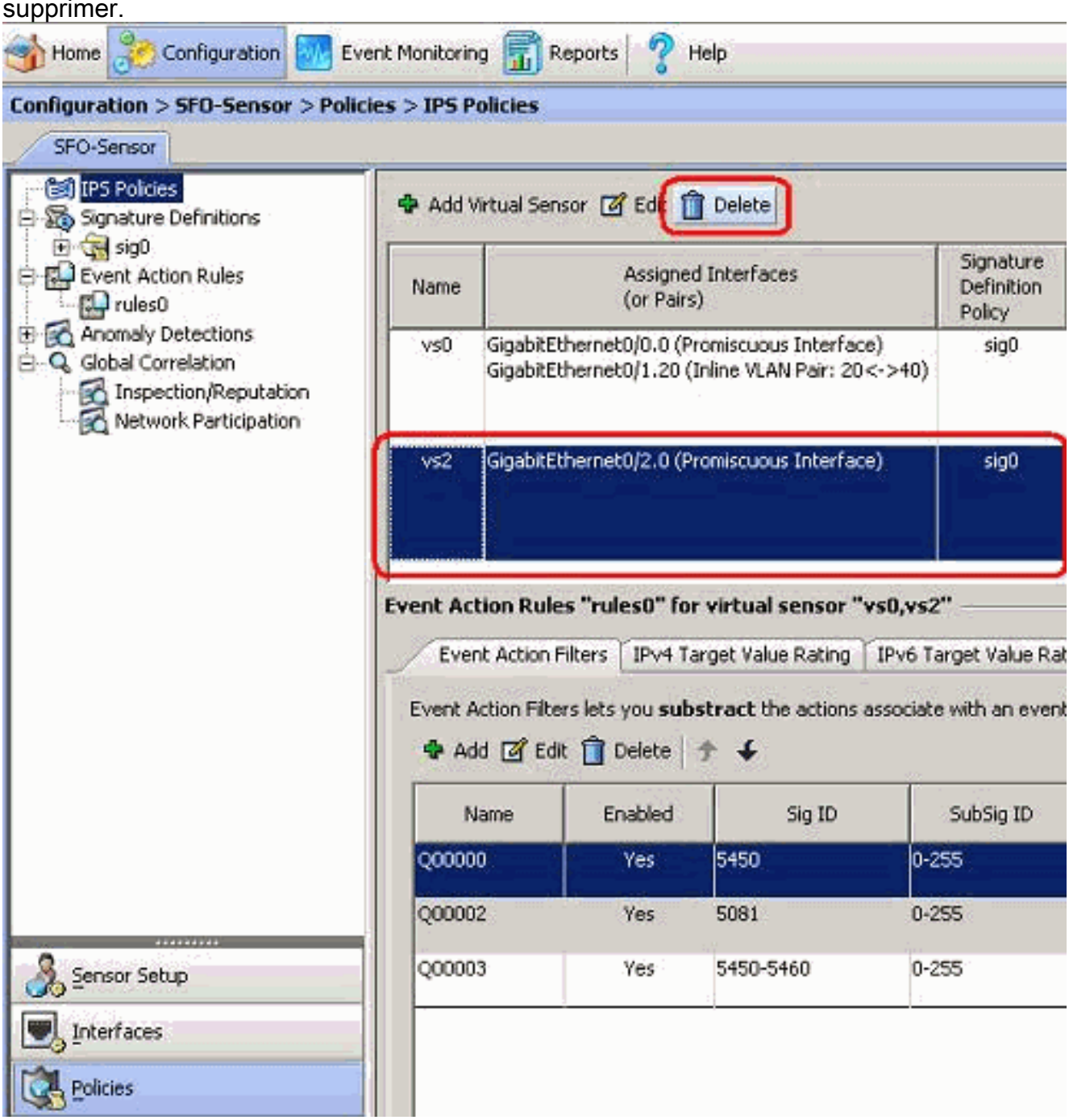
```
sensor(config)#
Apply Changes:?[yes]:
```

Capteur virtuel d'effacement avec IME

Terminez-vous ceci fait un pas afin de supprimer un capteur virtuel sur le Système de prévention d'intrusion (IPS) Cisco Secure avec le Cisco IPS Manager Express :

1. Choisissez la **configuration > les stratégies de SFO-Sensor> Policies> IPS**.

2. Choisissez le capteur virtuel à supprimer, et puis cliquez sur Delete, suivant les indications du tir d'écran. Dans cet exemple vs2 est le capteur virtuel à supprimer.



Ceci complète le processus pour supprimer un capteur virtuel. Le capteur virtuel vs2 est supprimé.

Dépannez

Le Manager Express IPS ne lance pas

Problème

Quand une tentative est faite pour accéder à l'IPS par l'IME, le Manager Express IPS ne commence pas et ce message d'erreur est reçu :

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

Solution

Afin de résoudre ceci, rechargez le PC de poste de travail IME.

Informations connexes

- Page de support de Système de protection contre les intrusions Cisco
- Page de support de Cisco IPS Manager Express
- Protocole NTP (Network Time Protocol)
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems