IPS 6.X 以降： IME 設定でのバーチャル センサーの例

目次

概要

このドキュメントでは、分析エンジンの機能と、Cisco IPS Manager Express（IME）の Cisco Secure Intrusion Prevention System（IPS）でバーチャル センサーを作成、編集、および削除する方法について説明します。 また、インターフェイスをバーチャル センサーに割り当てる方法についても説明します。

注: AIM-IPS および NME-IPS では、仮想化はサポートされません。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ソフトウェア バージョン 6.0 およびそれ以降が実行されている Cisco 4200 シリーズ IPS デバイス
- Cisco IPS Manager Express（IME）バージョン 6.1.1 およびそれ以降**注:** IME では、Cisco IPS 5.0 およびそれ以降で実行されているセンサー デバイスの監視に使用でき、IME で提供される新しい機能の一部は、Cisco IPS 6.1 またはそれ以降で実行されているセンサーでのみサポートされます。**注:** Cisco Secure Intrusion Prevention System（IPS）5.x では、デフォルト バーチャル センサー vs0 のみがサポートされます。 デフォルトの vs0 以外のバーチャル センサーは、IPS 6.x およびそれ以降でサポートされます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

関連製品

この設定は、次のセンサーにも使用できます。

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

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

分析エンジンについて

分析エンジンでは、パケット分析およびアラート検出が実行されます。 特定のインターフェイスを介して流されるトラフィックが監視されます。 分析エンジンに、バーチャル センサーを作成します。 各バーチャル センサーには、インターフェイスのリスト、インライン インターフェイス ペア、インライン VLAN ペア、およびそれに関連付けられている VLAN グループに固有の名前があります。 定義順序の問題を回避するため、割り当てには矛盾も重複も認められません。 インターフェイス、インライン インターフェイス ペア、インライン VLAN ペア、および VLAN グループを特定のバーチャル センサーに割り当て、複数のバーチャル センサーで処理されるパケットがないようにします。 各バーチャル センサーは、特別な名前を付けられたシグニチャ定義、イベント アクション ルール、およびアノマリー ディテクションの設定にも関連付けられます。 いずれのバーチャル センサーに割り当てられていないインターフェイス、インライン インターフェイス ペア、インライン VLAN ペア、および VLAN グループからのパケットは、インライン バイパス

設定に基づいて廃棄されます。

バーチャル センサーについて

センサーでは、1 つまたは多数の監視対象データ ストリームから、データ入力を受信できます。これらの監視対象データ ストリームは、物理インターフェイス ポートまたは仮想インターフェイス ポートのいずれかの場合があります。 たとえば、単一のセンサーでは、ファイアウォールの内側のトラフィック、ファイアウォールの外側のトラフィック、または、ファイアウォールの両側からのトラフィックを同時に監視できます。 単一のセンサーは、1 つまたは複数のデータ ストリームを監視できます。 この状況で、単一のセンサー ポリシーまたは設定は、すべての監視対象データ ストリームに適用されます。 バーチャル センサーは、設定ポリシーのセットによって定義されるデータの集まりです。 バーチャル センサーは、インターフェイス コンポーネントによって定義されるパケットのセットに適用されます。 バーチャル センサーでは、複数のセグメントを監視でき、単一の物理センサー内で、各バーチャル センサーの異なるポリシーまたは設定を適用できます。 分析下の監視対象セグメントごとに、異なるポリシーを設定できます。 また、たとえば sig0、rules0、または ad0 などの同じポリシー インスタンスを、異なるバーチャル センサーに適用することもできます。 インターフェイス、インライン インターフェイス ペア、インライン VLAN ペア、および VLAN グループを、バーチャル センサーに割り当てることもできます。

注: Cisco Secure Intrusion Prevention System（IPS）では、4 を超えるバーチャル センサーはサポートされません。 デフォルト バーチャル センサーは vs0 です。 デフォルト バーチャル センサーは削除できません。 インターフェイス リスト、アノマリー ディテクション動作モード、インライン TCP セッション トラッキング モード、およびバーチャル センサーの説明のみが、デフォルト バーチャル センターについて変更できる設定機能です。 シグニチャ定義、イベント アクション ルール、またはアノマリー ディテクション ポリシーは変更できません。

仮想化の利点と制約事項

仮想化の利点

仮想化には、次の利点があります。

- トラフィックの異なるセットに対し、異なる設定を適用できます。
- 1 つのセンサーで、重複している IP 領域の 2 つのネットワークを監視できます。
- ファイアウォールまたは NAT デバイスの内側および外側の両方を監視できます。

仮想化の制約事項

仮想化には、次の制約事項があります。

- 非対称トラフィックの両側を、同じバーチャル センサーに割り当てる必要があります。
- VACL キャプチャまたは SPAN（混合モード監視）は、VLAN タギングとの一貫性がなく、これによって VLAN グループに問題が発生します。Cisco IOS ソフトウェアを使用する場合、トランキングに対する設定が行われている場合でも、VACL キャプチャ ポートまたは SPAN ターゲットでは、タグ付けされたパケットを常に受信するわけではありません。MSFC を使用する場合、学習されたルートの高速スイッチング パスによって、VACL キャプチャおよび SPAN の動作が変更されます。
- 永続的な保存は制限されます。

仮想化の要件

仮想化には、次のトラフィック キャプチャ要件があります。

- バーチャル センサーでは、キャプチャ ポートのネイティブ VLAN 上のトラフィック以外の、802.1q ヘッダーがあるトラフィックを受信する必要があります。
- センサーは、指定されたセンサーの同じバーチャル センサーにある同じ VLAN グループのトラフィックの両方の方向を参照する必要があります。

設定

このセクションでは、バーチャル センターの追加、編集、および削除に関する情報について説明します。

バーチャル センサーの追加

バーチャル センサーを作成するには、サービス分析エンジン サブモードで virtual-sensor name コマンドを発行します。 バーチャル センサーにポリシー（アノマリー ディテクション、イベント アクション ルール、およびシグニチャ定義）を割り当てます。 次に、インターフェイス（混合モード、インライン インターフェイス ペア、インライン VLAN ペア、および VLAN グループ）を、バーチャル センサーに割り当てます。 バーチャル センサーにこれらを割り当てる前に、インライン インターフェイス ペアおよび VLAN ペアを設定する必要があります。 これらのオプションによって、次の設定が割り当てられます。

- **anomaly-detection**：アノマリー ディテクション パラメータ。**anomaly-detection-name** name：アノマリー ディテクション ポリシーの名前**operational-mode**：アノマリー ディテクション モード（**inactive、learn、detect**）
- **description**：バーチャル センサーの説明。
- **event-action-rules**：イベント アクション ルール ポリシーの名前。
- **inline-TCP-evasion-protection-mode**：トラフィックの検出に必要な次のノーマライザ モードのタイプを検出できます。**asymmetric**：双方向トラフィック フローの 1 つの方向のみを参照できます。 非対称モード保護によって、TCP レイヤでの回避保護が緩和されます。**注:** 非対称モードを使用すると、センサーによって、ステートをフローと同期でき、双方向が必要ではないこれらのエンジンの検査を管理できます。 完全保護では、トラフィックの両側の参照が必要なため、非対称モードによってセキュリティが低くなります。**strict**：パケットが何らかの理由で損失した場合、損失したパケット後のすべてのパケットは処理されません。 厳密な回避保護によって、TCP ステートおよびシーケンス監視が完全に実施されます。**注:** 順序が誤っているすべてのパケットまたはすべての損失パケットによって、ノーマライザ エンジン シグニチャ 1300 または 1330 の発行が生成され、これによって状況は修正されますが、拒否接続が発生する場合があります。
- **inline-TCP-session-tracking-mode**：インライン トラフィックで重複 TCP セッションを指定できるようにする高度な方式。 デフォルトはバーチャル センサーで、これが、ほとんどの場合、最善の選択肢です。**virtual-sensor**：同じセッションに属すバーチャル センター内の同じセッション キー（AaBb）を持つすべてのパケット。**interface-and-vlan**：同じ VLAN（またはインライン VLAN ペア）および同じセッションに属す同じインターフェイス上の、同じセッションキー（AaBb）を持つすべてのパケット。 同じキーを持つが、異なる VLAN またはインターフェイスにあるパケットは、独立して監視されます。**vlan-only**：同じセッションに属しているインターフェイスに関係なく、同じ VLAN（またはインライン VLAN ペア）および

同じセッションの、同じセッションキー（AaBb）を持つすべてのパケット。 同じキーを持つが異なる VLAN にあるパケットは、独立して監視されます。

- **signature-definition**：シグニチャ定義ポリシーの名前。
- **logical-interfaces**：論理インターフェイス（インライン インターフェイス ペア）の名前。
- **physical-interfaces**：物理インターフェイス（混合モード、インライン VLAN ペア、および VLAN グループ）の名前。**subinterface-number**：物理サブインターフェイスの番号。subinterface-type が none の場合、値 0 によって、インターフェイス全体が混合モードで割り当てられることを示します。**非**エントリか選択を取除きます

バーチャル センサーを追加するには、次の手順を実行します。

1. 管理者権限を持つアカウントで CLI に口グインします。
2. サービス分析モードを開始します。`sensor# **configure terminal** sensor(config)# **service analysis-engine** sensor(config-ana)#`
3. バーチャル センサーを追加します。`sensor(config-ana)# **virtual-sensor vs2** sensor(config-ana-vir)#`
4. このバーチャル センサーの説明を追加します。`sensor(config-ana-vir)# **description virtual sensor 2**`
5. アノマリー ディテクション ポリシーおよび動作モードを、このバーチャル センサーに割り当てます。`sensor(config-ana-vir)# **anomaly-detection** sensor(config-ana-vir-ano)# **anomaly-detection-name ad1** sensor(config-ana-vir-ano)# **operational-mode learn**`
6. イベント アクション ルール ポリシーを、このバーチャル センサーに割り当てます。`sensor(config-ana-vir-ano)# exit`

   `sensor(config-ana-vir)# **event-action-rules rules1**`
7. シグニチャ定義ポリシーを、このバーチャル センサーに割り当てます。`sensor(config-ana-vir)# **signature-definition sig1**`
8. インライン TCP セッション トラッキング モードを割り当てます。`sensor(config-ana-vir)# **inline-TCP-session-tracking-mode virtual-sensor**` デフォルトはバーチャル センサー モードで、ほとんどの場合、これが最善の選択肢です。
9. インライン TCP 回避保護モードを割り当てます。`sensor(config-ana-vir)# **inline-TCP-evasion-protection-mode strict**` デフォルトは strict モードで、ほとんどの場合、これが最善の選択肢です。
10. 使用可能なインターフェイスのリストが表示されます。`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. このバーチャル センサーに追加する混合モード インターフェイスを割り当てます。`sensor(config-ana-vir)# **physical-interface GigabitEthernet0/2**` このバーチャル センサーに割り当てるすべての混合モード インターフェイスについて、この手順を繰り返します。
12. このバーチャル センサーに追加するインライン インターフェイス ペアを割り当てます。`sensor(config-ana-vir)# **logical-interface inline_interface_pair_name**` インターフェイスはすでにペアにされている必要があります。
13. このバーチャル センサーに追加する、インライン VLAN ペアのサブインターフェイスまたはグループを、次のとおりに割り当てます。`sensor(config-ana-vir)# **physical-interface GigabitEthernet2/0 subinterface-number subinterface_number**` インターフェイスは VLAN ペアまたはグループにすでに分割されている必要があります。
14. バーチャル センサー設定を確認します。`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. 分析エンジン モードを終了します。`sensor(config-ana-vir)# exit sensor(config-ana)# exit sensor(config)# Apply Changes:?[yes]:`
16. 変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は [no] を入力します。

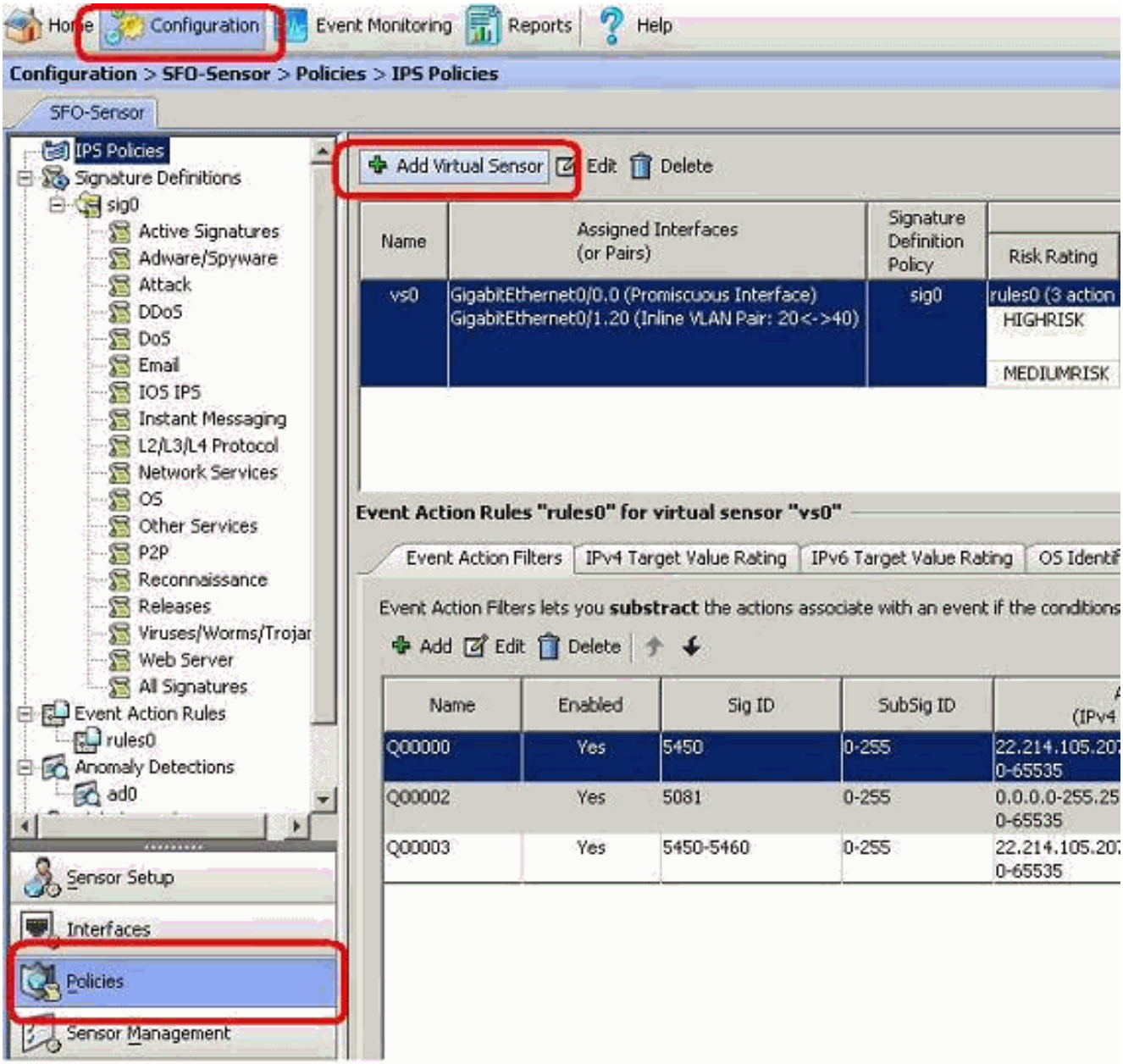
これで、Cisco Secure Intrusion Prevention System（IPS）にバーチャル センサーを追加する処理が終了しました。 さらにバーチャル センサーを追加するには、同じ手順を実行します。

注: Cisco Secure Intrusion Prevention System（IPS）では、4 を超えるバーチャル センサーはサポートされません。 デフォルト バーチャル センサーは vs0 です。

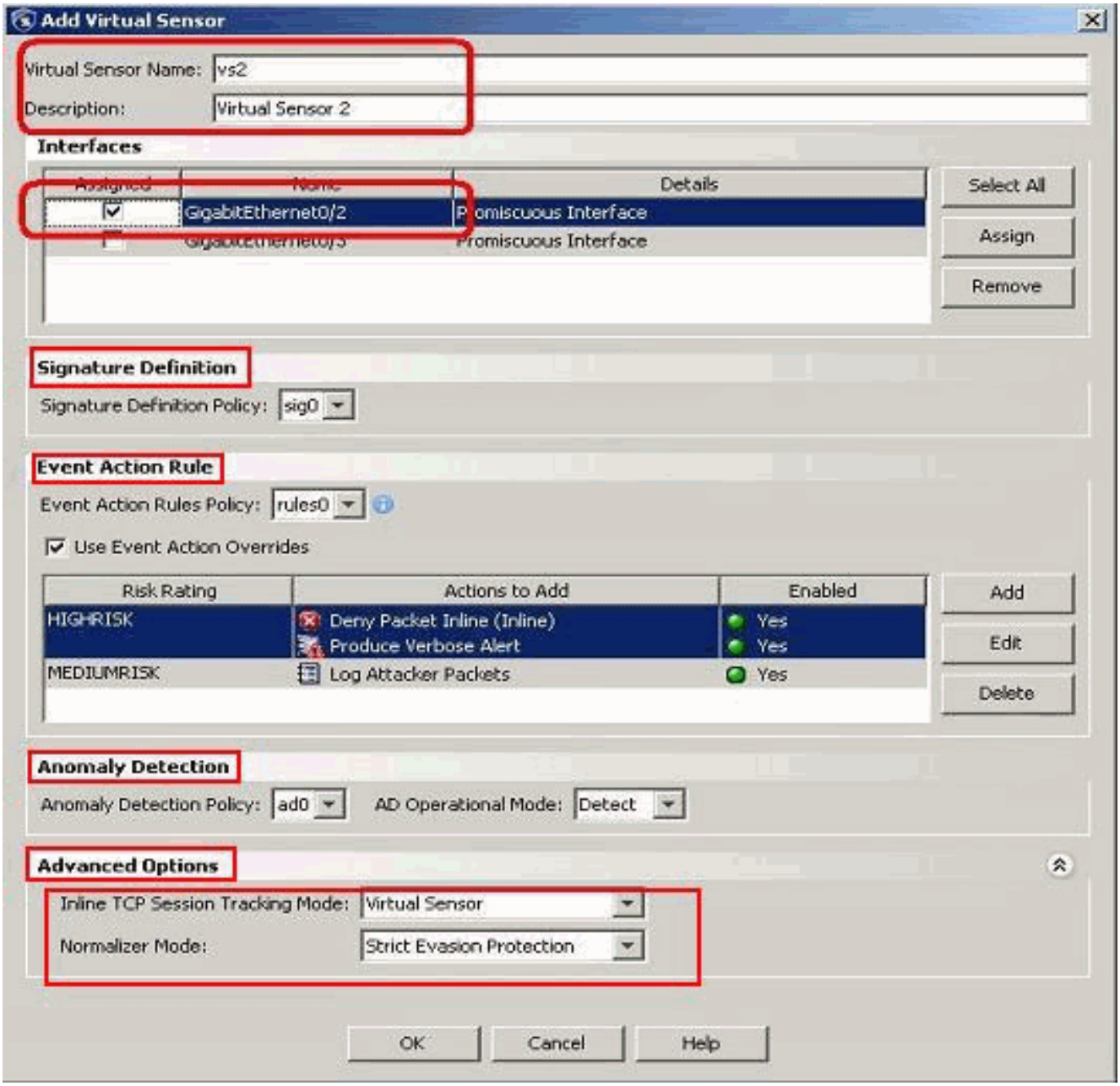
IME でのバーチャル センサーの追加

Cisco IPS Manager Express が使用されている Cisco Secure Intrusion Prevention System（IPS）に、バーチャル センサーを設定するには、次の手順を実行します。

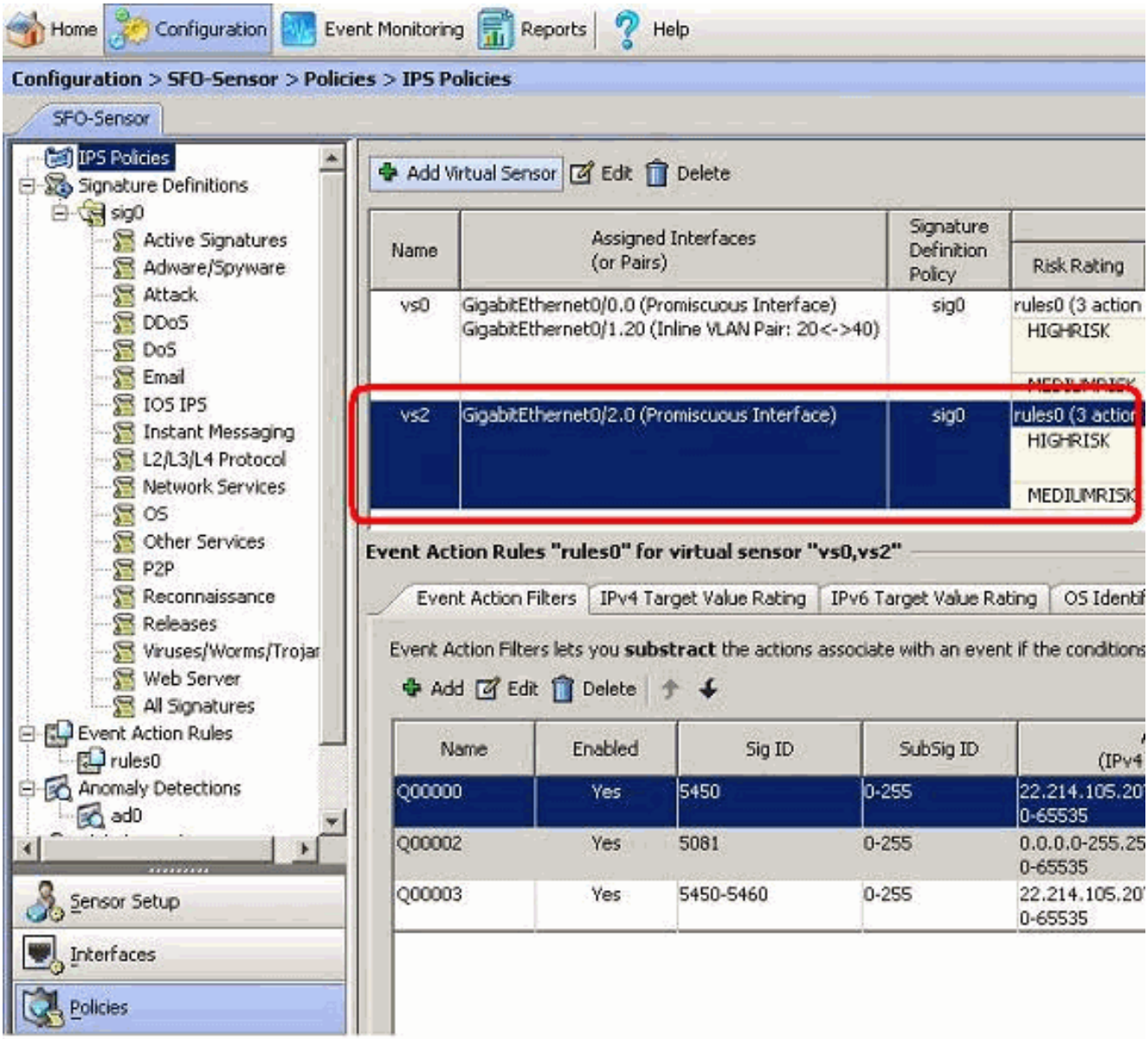
1. [Configuration] > [SFO-Sensor] > [Policies] > [IPS Policies] を選択します。 次に、スクリーンショットに示したように、[Add Virtual Sensor] をクリックします。



2. バーチャル センターに名前を付け（この例では vs2）、指定された領域にバーチャル センターに説明を追加します。 このバーチャル センサーに追加する混合モード インターフェイスも割り当てます。 ここでは、ギガビット イーサネット 0/2 が選択されています。 スクリーンショットに示したように、[Signature Definition]、[Event Action Rule]、[Anomaly Detection]、および [Advanced Options] の各セクションに詳細を指定します。[Advanced Options] に、TCP セッション トラッキング モードおよびノーマライザ モードに関する詳細を指定します。 ここでは、[TCP Session Tracking Mode] が [Virtual Sensor] で、[Normalizer Mode] が [Strict Evasion Protection] モードです。



3. [OK] をクリックします。
4. 新たに追加されたバーチャル センサー vs2 が、バーチャル センサーのリストに示されます。 [Apply] をクリックし、新しいバーチャル センサーの設定を Cisco Secure Intrusion Prevention System（IPS）に送信します。



これで、バーチャル センサーを追加する設定は完了しました。

バーチャル センサーの編集

次のバーチャル センサーのパラメータを編集できます。

- シグニチャ定義ポリシー
- イベント アクション ルール ポリシー
- アノマリー ディテクション ポリシー
- アノマリー ディテクション動作モード
- インライン TCP セッション トラッキング モード
- 説明
- 割り当てられるインターフェイス

バーチャル センサーを編集するには、次の手順を実行します。

1. 管理者権限を持つアカウントで CLI にログインします。
2. サービス分析モードを開始します。`sensor# **configure terminal** sensor(config)# **service analysis-engine** sensor(config-ana)#`
3. バーチャル センサーは vs1 を編集します。`sensor(config-ana)# **virtual-sensor vs2** sensor(config-ana-vir)#`

4. このバーチャル センサーの説明を編集します。sensor(config-ana-vir)# **description virtual sensor A**
5. このバーチャル センサーに割り当てられているアノマリー ディテクション ポリシーおよび動作モードを変更します。sensor(config-ana-vir)# anomaly-detection

   sensor(config-ana-vir-ano)# **anomaly-detection-name ad0** sensor(config-ana-vir-ano)# **operational-mode learn**
6. このバーチャル センサーに割り当てられている、イベント アクション ルール ポリシーを変更します。sensor(config-ana-vir-ano)# exit

   sensor(config-ana-vir)# **event-action-rules rules0**
7. このバーチャル センサーに割り当てられているシグニチャ定義ポリシーを変更します。sensor(config-ana-vir)# **signature-definition sig0**
8. インライン TCP セッション トラッキング モードを変更します。sensor(config-ana-vir)# **inline-TCP-session-tracking-mode interface-and-vlan** デフォルトはバーチャル センサー モードで、ほとんどの場合、これが最善の選択肢です。
9. 使用可能なインターフェイスのリストが表示されます。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. このバーチャル センサーに割り当てられている混合モード インターフェイスを変更します。sensor(config-ana-vir)# physical-interface GigabitEthernet0/2
11. このバーチャル センサーに割り当てられているインライン インターフェイス ペアを変更します。sensor(config-ana-vir)# **logical-interface inline_interface_pair_name** インターフェイスはすでにペアにされている必要があります。
12. このバーチャル センサーに割り当てられている、VLAN ペアまたはグループが使用されているサブインターフェイスを変更します。sensor(config-ana-vir)# physical-interface GigabitEthernet2/0 subinterface-number subinterface_numberインターフェイスは VLAN ペアまたはグループにすでに分割されている必要があります。
13. 編集するバーチャル センサーの設定を確認します。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. 分析エンジン モードを終了します。sensor(config-ana)# exit

    sensor(config)#

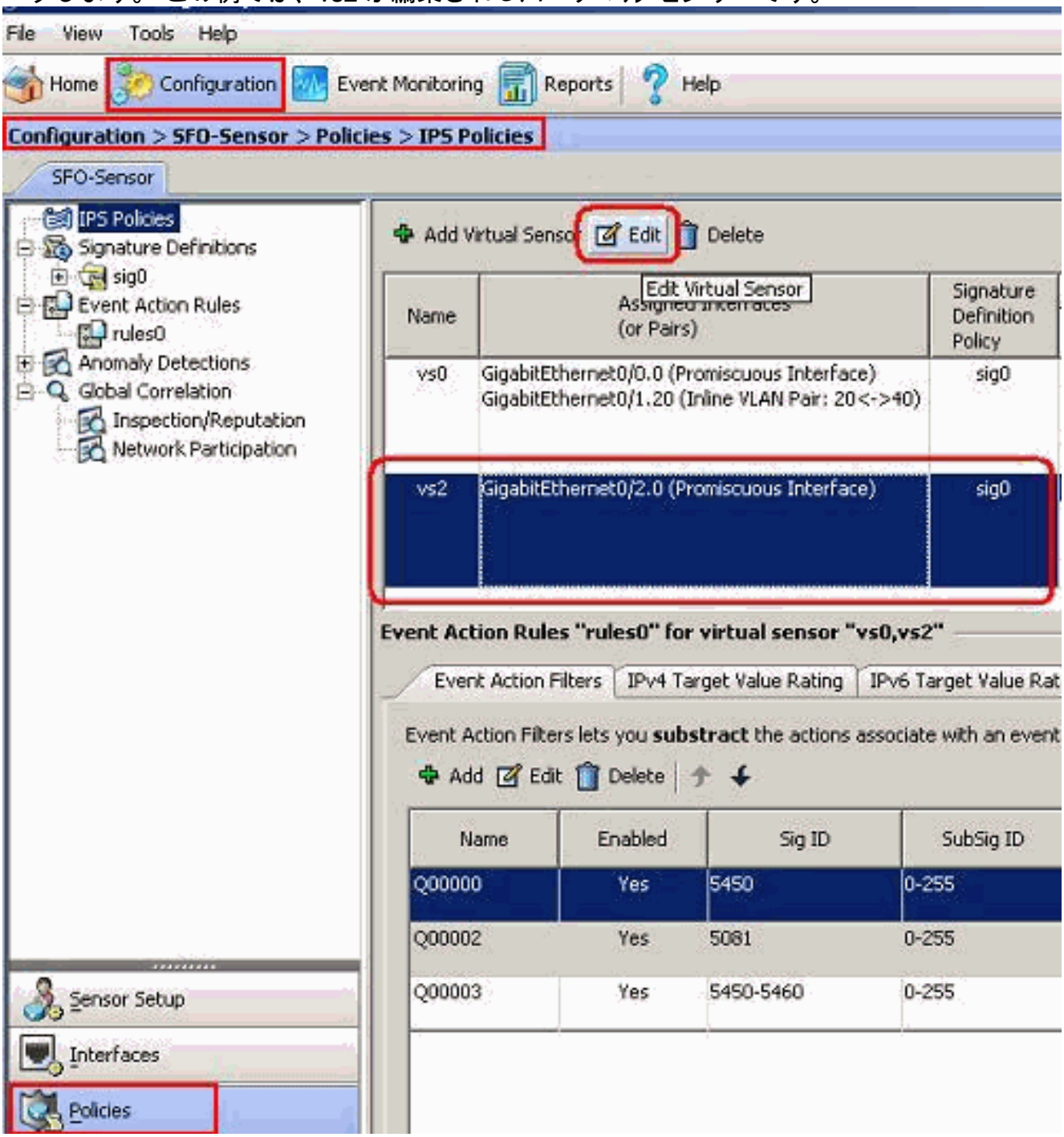
    Apply Changes:?[yes]:
15. 変更を適用する場合は Enter キーを押し、変更を廃棄する場合は [no] を入力します。

IME でのバーチャル センサーの編集

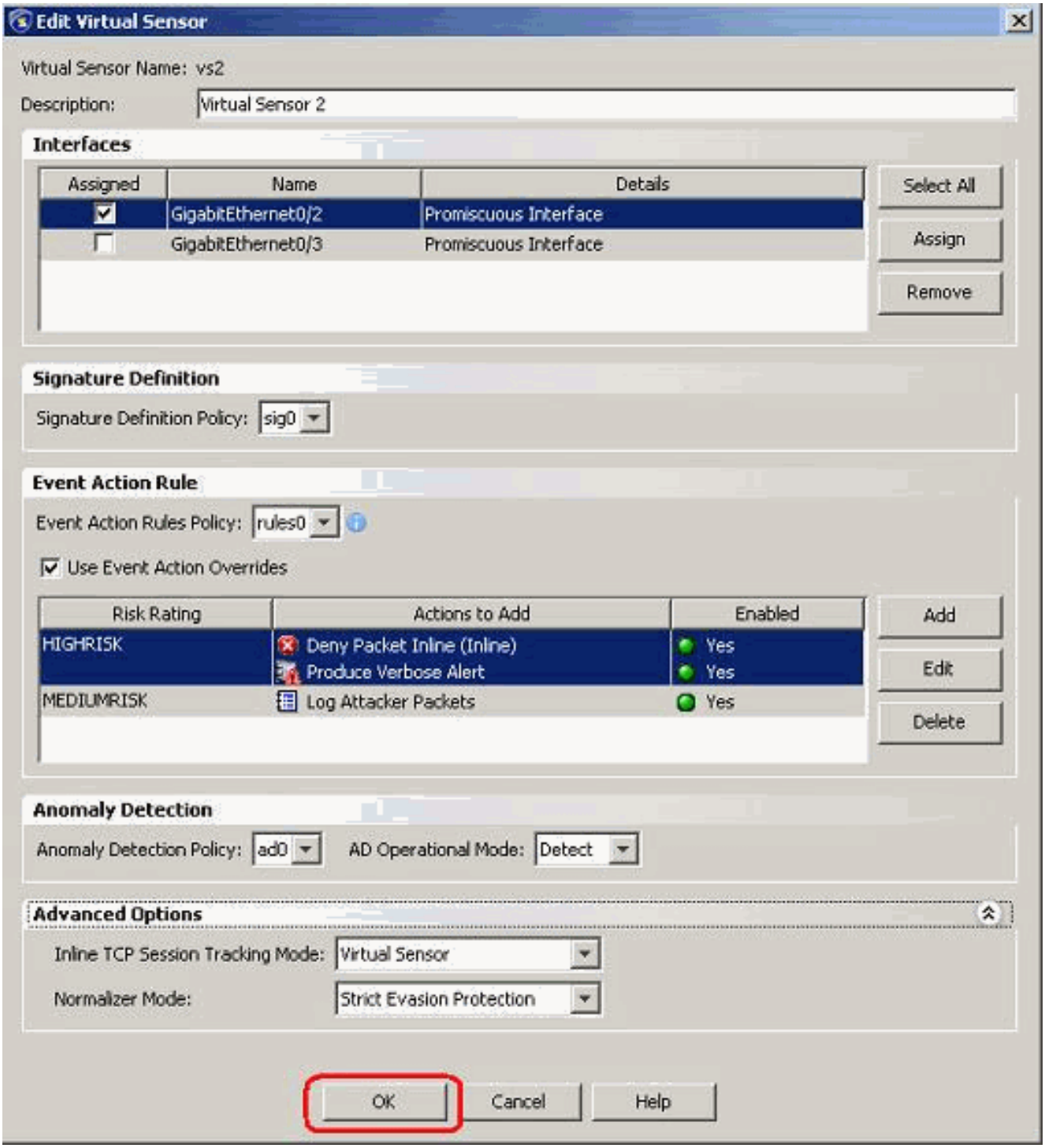
Cisco IPS Manager Express が使用されている Cisco Secure Intrusion Prevention

System（IPS）で、バーチャル センサーを編集するには、次の手順を実行します。

1. [Configuration] > [SFO-Sensor] > [Policies] > [IPS Policies] を選択します。
2. スクリーンショットに示したように、編集するバーチャル センサーを選択し、[Edit] をクリックします。 この例では、vs2 が編集されるバーチャル センサーです。



3. [Edit Virtual Sensor] ウィンドウの [Signature Definition] 、[Event Action Rule] 、[Anomaly Detection] 、および [Advanced Options] の各セクションで、存在するバーチャル センサーのパラメータを変更します。 [OK] をクリックして、[Apply] をクリックします。



これで、バーチャル センサーを編集する処理は完了しました。

バーチャル センサーの削除

バーチャル センサーを削除するには、次の手順を実行します。

1. バーチャル センサーを削除するには、**no virtual-sensor** コマンドを発行します。
   ```
   sensor(config-ana)# virtual-sensor vs2 sensor(config-ana-vir)# sensor(config-ana-vir)# exit
   sensor(config-ana)# no virtual-sensor vs2
   ```
2. 削除されるバーチャル センサーを確認します。`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)#` デフォルト バーチャル センサー **vs0** のみが存在しています。

3. 分析エンジン モードを終了します。`sensor(config-ana)# exit`

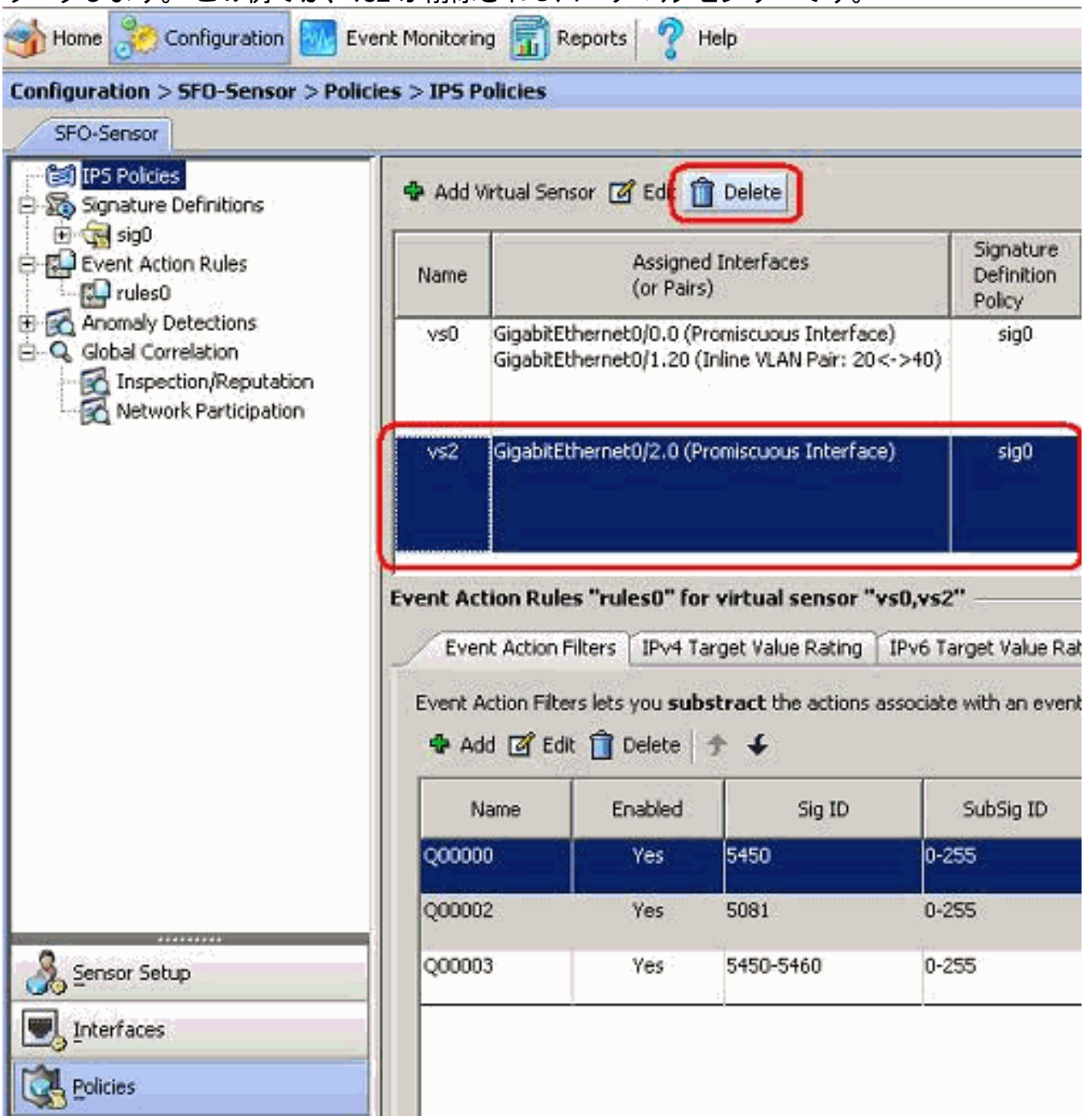
```
sensor(config)#
Apply Changes:?[yes]:
```

IME でのバーチャル センサーの削除

Cisco IPS Manager Express が使用されている Cisco Secure Intrusion Prevention System（IPS）で、バーチャル センサーを削除するには、次の手順を実行します。

1. [Configuration] > [SFO-Sensor] > [Policies] > [IPS Policies] を選択します。
2. スクリーンショットに示したように、削除するバーチャル センサーを選択し、[Delete] をク

リックします。 この例では、vs2 が削除されるバーチャル センサーです。



これで、バーチャル センサーを削除する処理は完了しました。 バーチャル センサーは vs2 が削除されます。

トラブルシューティング

IPS Manager Express が起動しない

問題

IME を介して IPS にアクセスしようとしたときに、IPS Manager Express が開始されず、次のエラー メッセージを受信する。

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

解決策

この問題を解決するには、IME ワークステーション PC をリロードします。

関連情報

- Cisco Intrusion Prevention System に関するサポート ページ
- Cisco IPS Manager Express に関するサポート ページ
- ネットワーク タイム プロトコル（NTP）
- Requests for Comments（RFC）
- テクニカルサポートとドキュメント - Cisco Systems