IPS 6.X und höher - Konfigurieren virtueller Sensoren mit IME

Inhalt

Einleitung

In diesem Dokument werden die Funktionen der Analysis Engine und das Erstellen, Bearbeiten und Löschen virtueller Sensoren im Cisco Secure Intrusion Prevention System (IPS) mit Cisco IPS Manager Express (IME) erläutert. Außerdem wird erläutert, wie einem virtuellen Sensor Schnittstellen zugewiesen werden.

Hinweis: AIM-IPS und NME-IPS unterstützen die Virtualisierung nicht.

Voraussetzungen

Anforderungen

Es sind keine besonderen Voraussetzungen erforderlich, um den Inhalt dieses Dokuments nachzuvollziehen.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco IPS-Gerät der Serie 4200 mit Softwareversion 6.0 und höher
- Cisco IPS Manager Express (IME) Version 6.1.1 und höher**Hinweis:** Obwohl IME zum Überwachen von Sensorgeräten verwendet werden kann, auf denen Cisco IPS 5.0 und höher ausgeführt wird, werden einige der neuen Funktionen und Funktionen von IME nur auf Sensoren unterstützt, auf denen Cisco IPS 6.1 oder höher ausgeführt wird.**Hinweis:** Cisco Secure Intrusion Prevention System (IPS) 5.x unterstützt nur den virtuellen Standardsensor vs.0. Virtuelle Sensoren, die nicht der Standard vs0 sind, werden in IPS 6.x und höher unterstützt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Verwandte Produkte

Diese Konfiguration kann auch mit den folgenden Sensoren verwendet werden:

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

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Informationen zum Analysis Engine

Analysis Engine führt Paketanalysen durch und gibt Warnmeldungen aus. Er überwacht den Datenverkehr, der über bestimmte Schnittstellen fließt. Sie erstellen virtuelle Sensoren in Analysis Engine. Jeder virtuelle Sensor hat einen eindeutigen Namen mit einer Liste von Schnittstellen, Inline-Schnittstellenpaaren, Inline-VLAN-Paaren und zugehörigen VLAN-Gruppen. Um Probleme bei der Definitionsbestellung zu vermeiden, sind bei der Zuweisung keine Konflikte oder Überschneidungen zulässig. Sie weisen einem bestimmten virtuellen Sensor Schnittstellen, Inline-Schnittstellenpaare, Inline-VLAN-Paare und VLAN-Gruppen zu, sodass kein Paket von mehr als einem virtuellen Sensor verarbeitet wird. Jeder virtuelle Sensor ist auch einer speziell benannten

Signaturdefinition, Ereignisaktionsregeln und einer Anomalie-Erkennungskonfiguration zugeordnet. Pakete von Schnittstellen, Inline-Schnittstellenpaaren, Inline-VLAN-Paaren und VLAN-Gruppen, die keinem virtuellen Sensor zugewiesen sind, werden basierend auf der Inline-Bypass-Konfiguration freigegeben.

Über virtuelle Sensoren

Der Sensor kann Dateneingaben von einem oder mehreren überwachten Datenströmen empfangen. Diese überwachten Datenströme können entweder physische Schnittstellen-Ports oder virtuelle Schnittstellenports sein. Ein einzelner Sensor kann beispielsweise den Datenverkehr vor der Firewall, hinter der Firewall oder vor und hinter der Firewall gleichzeitig überwachen. Ein einzelner Sensor kann einen oder mehrere Datenströme überwachen. In dieser Situation wird eine einzelne Sensorrichtlinie oder -konfiguration auf alle überwachten Datenströme angewendet. Ein virtueller Sensor ist eine Sammlung von Daten, die durch einen Satz von Konfigurationsrichtlinien definiert wird. Der virtuelle Sensor wird auf eine Gruppe von Paketen angewendet, die durch die Schnittstellenkomponente definiert sind. Ein virtueller Sensor kann mehrere Segmente überwachen und für jeden virtuellen Sensor innerhalb eines physischen Sensors eine andere Richtlinie oder Konfiguration anwenden. Sie können für jedes überwachte Segment, das analysiert wird, eine andere Richtlinie einrichten. Sie können dieselbe Richtlinieninstanz, z. B. sig0, rules0 oder ad0, auch auf verschiedene virtuelle Sensoren anwenden. Sie können einem virtuellen Sensor Schnittstellen, Inline-Schnittstellenpaare, Inline-VLAN-Paare und VLAN-Gruppen zuweisen.

Hinweis: Das Cisco Secure Intrusion Prevention System (IPS) unterstützt nicht mehr als vier virtuelle Sensoren. Der virtuelle Standardsensor ist vs0. Der virtuelle Standardsensor kann nicht gelöscht werden. Die Schnittstellenliste, der Betriebsmodus zur Erkennung ungewöhnlicher Ereignisse, der Inline-TCP-Sitzungsverfolgungsmodus und die Beschreibung der virtuellen Sensoren sind die einzigen Konfigurationsfunktionen, die Sie für den virtuellen Standardsensor ändern können. Sie können die Signaturdefinition, die Ereignisaktionsregeln oder die Richtlinien zur Erkennung ungewöhnlicher Ereignisse nicht ändern.

Vorteile und Einschränkungen der Virtualisierung

Vorteile der Virtualisierung

Virtualisierung bietet folgende Vorteile:

- Sie können verschiedene Konfigurationen auf unterschiedliche Datenverkehrsmengen anwenden.
- Sie können zwei Netzwerke mit sich überschneidenden IP-Bereichen mit einem Sensor überwachen.
- Sie können sowohl innerhalb als auch außerhalb einer Firewall oder eines NAT-Geräts überwachen.

Einschränkungen der Virtualisierung

Für die Virtualisierung gelten folgende Einschränkungen:

- Sie müssen beide Seiten des asymmetrischen Datenverkehrs demselben virtuellen Sensor zuweisen.

- Die Verwendung der VACL-Erfassung oder des SPAN (Promiscuous Monitoring) ist im Hinblick auf das VLAN-Tagging inkonsistent, was zu Problemen mit VLAN-Gruppen führt.Wenn Sie die Cisco IOS-Software verwenden, werden bei einem VACL-Erfassungsport oder einem SPAN-Ziel nicht immer getaggte Pakete empfangen, selbst wenn dieser für das Trunking konfiguriert ist.Wenn Sie die MSFC verwenden, ändert das schnelle Pfad-Switching von gelernten Routen das Verhalten der VACL-Erfassung und des SPAN.
- Das permanente Geschäft ist begrenzt.

Virtualisierungsanforderungen

Die Virtualisierung hat folgende Anforderungen an die Erfassung des Datenverkehrs:

- Der virtuelle Sensor muss Datenverkehr mit 802.1q-Headern empfangen, der nicht über den Datenverkehr im nativen VLAN des Erfassungsports hinausgeht.
- Der Sensor muss für jeden Sensor beide Datenverkehrsrichtungen in derselben VLAN-Gruppe im gleichen virtuellen Sensor anzeigen.

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Hinzufügen, Bearbeiten und Löschen virtueller Sensoren.

Virtuelle Sensoren hinzufügen

Geben Sie den **Befehl** virtual-sensor name **in service analysis engine submode ein, um einen virtuellen Sensor zu erstellen.** Sie weisen dem virtuellen Sensor Richtlinien (Anomalieerkennung, Ereignishandlungsregeln und Signaturdefinition) zu. Anschließend weisen Sie dem virtuellen Sensor Schnittstellen (Promiscuous, Inline-Schnittstellenpaare, Inline-VLAN-Paare und VLAN-Gruppen) zu. Sie müssen die Inline-Schnittstellenpaare und die VLAN-Paare konfigurieren, bevor Sie sie einem virtuellen Sensor zuweisen können. Diese Optionen gelten für:

- **Anomalie-Erkennung** - Anomalie-Erkennungsparameter.**anomaly-detect-name** - Name der Anomaly Detection-Richtlinie**Betriebsmodus** - Anomalie-Erkennungsmodus (**inaktiv, lernen, erkennen**)
- **description** - Beschreibung des virtuellen Sensors
- **event-action-rules** - Name der Ereignisaktivitätsrichtlinie
- **inline-TCP-evasion-protection-mode** - Ermöglicht Ihnen die Auswahl des Normalizer-Modus, den Sie für die Überprüfung des Datenverkehrs benötigen:**asymmetrisch** - Es kann nur eine Richtung des bidirektionalen Datenverkehrsflusses angezeigt werden. Durch den Schutz des asymmetrischen Modus wird der Umgehungsschutz auf der TCP-Schicht gelockert.**Hinweis:** Im asymmetrischen Modus kann der Sensor den Zustand mit dem Fluss synchronisieren und die Prüfungen für Motoren aufrechterhalten, die nicht beide Richtungen erfordern. Der asymmetrische Modus verringert die Sicherheit, da bei vollständigem Schutz beide Seiten des Datenverkehrs sichtbar sind.**strict**: Wenn ein Paket aus irgendeinem Grund verpasst wird, werden alle Pakete nach dem verpassten Paket nicht verarbeitet. Der strikte Umgehungsschutz ermöglicht die vollständige Durchsetzung des TCP-Status und der Sequenzverfolgung.**Hinweis:** Alle Pakete oder verpassten Pakete, die nicht in der Bestellung sind, können 1300- oder 1330-Signaturen des Normalizer-Moduls erzeugen, die versuchen,

die Situation zu korrigieren, aber zu verweigerten Verbindungen führen können.

- **inline-TCP-session-tracking-mode** - Eine erweiterte Methode, mit der Sie doppelte TCP-Sitzungen im Inline-Datenverkehr identifizieren können. Der Standardwert ist "Virtual Sensor" (virtueller Sensor), was fast immer die beste Wahl ist.**virtual-sensor** - Alle Pakete mit demselben Sitzungsschlüssel (AaBb) innerhalb eines virtuellen Sensors gehören derselben Sitzung an.**interface-and-vlan** - Alle Pakete mit demselben Sitzungsschlüssel (AaBb) im gleichen VLAN (oder Inline-VLAN-Paar) und auf derselben Schnittstelle gehören zur gleichen Sitzung. Pakete mit demselben Schlüssel, die sich jedoch auf unterschiedlichen VLANs oder Schnittstellen befinden, werden unabhängig verfolgt.**VLAN-only**: Alle Pakete mit demselben Sitzungsschlüssel (AaBb) im gleichen VLAN (oder Inline-VLAN-Paar), unabhängig von der Schnittstelle, gehören zur gleichen Sitzung. Pakete mit demselben Schlüssel, die sich jedoch in unterschiedlichen VLANs befinden, werden unabhängig verfolgt.
- **Signaturdefinition** - Name der Signaturdefinitionsrichtlinie
- **logisch-interfaces** - Name der logischen Schnittstellen (Inline-Schnittstellenpaare)
- **Physische Schnittstellen** - Name der physischen Schnittstellen (Promiscuous, Inline-VLAN-Paare und VLAN-Gruppen)**subinterface-number** - Die Nummer der physischen Subschnittstelle. Wenn der Subschnittstellentyp none ist, gibt der Wert 0 an, dass die gesamte Schnittstelle im Promiscuous-Modus zugewiesen wird.**no** - Entfernt einen Eintrag oder eine Auswahl

Gehen Sie wie folgt vor, um einen virtuellen Sensor hinzuzufügen:

1. Melden Sie sich bei der CLI mit einem Konto mit Administratorrechten an.
2. Wechseln Sie in den Dienstanalysemodus.
```
sensor# configure terminal

        sensor(config)# service analysis-engine

        sensor(config-ana)#
```
3. Fügen Sie einen virtuellen Sensor hinzu.
```
sensor(config-ana)# virtual-sensor vs2

        sensor(config-ana-vir)#
```
4. Fügen Sie eine Beschreibung für diesen virtuellen Sensor hinzu.
```
sensor(config-ana-vir)# description virtual sensor 2
```
5. Weisen Sie diesem virtuellen Sensor eine Anomalie-Erkennungsrichtlinie und einen Betriebsmodus zu.
```
sensor(config-ana-vir)# anomaly-detection

        sensor(config-ana-vir-ano)# anomaly-detection-name ad1

        sensor(config-ana-vir-ano)# operational-mode learn
```
6. Weisen Sie diesem virtuellen Sensor eine Richtlinie für Ereignisaktionsregeln zu.
```
sensor(config-ana-vir-ano)# exit

        sensor(config-ana-vir)# event-action-rules rules1
```
7. Weisen Sie diesem virtuellen Sensor eine Signaturdefinitionsrichtlinie zu.
```
sensor(config-ana-vir)# signature-definition sig1
```
8. Weisen Sie den inline TCP-Sitzungsverfolgungsmodus zu.

```
sensor(config-ana-vir)# inline-TCP-session-tracking-mode virtual-sensor
```

Der Standardwert ist "Virtual Sensor Mode" (virtueller Sensormodus). Diese Option ist fast immer die beste.

9. Weisen Sie den Inline-TCP-Umgehungsschutzmodus zu.
```
sensor(config-ana-vir)# inline-TCP-evasion-protection-mode strict
```

Der Standardwert ist "strict mode" (strikter Modus). Dies ist fast immer die beste Wahl.

10. Anzeigen der Liste der verfügbaren Schnittstellen
```
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. Weisen Sie diesem virtuellen Sensor die Schnittstellen im Promiscuous-Modus zu, die hinzugefügt werden sollen.
```
sensor(config-ana-vir)# physical-interface GigabitEthernet0/2
```

Wiederholen Sie diesen Schritt für alle Promiscuous-Schnittstellen, die Sie diesem virtuellen Sensor zuweisen möchten.

12. Weisen Sie diesem virtuellen Sensor die Inline-Schnittstellenpaare zu, die Sie hinzufügen möchten.
```
sensor(config-ana-vir)# logical-interface inline_interface_pair_name
```

Sie müssen die Schnittstellen bereits gepaart haben.

13. Weisen Sie dem virtuellen Sensor die Subschnittstellen der Inline-VLAN-Paare oder -Gruppen zu, die Sie wie folgt hinzufügen möchten:
```
sensor(config-ana-vir)# physical-interface GigabitEthernet2/0 subinterface-number
subinterface_number
```

Sie müssen alle Schnittstellen bereits in VLAN-Paare oder -Gruppen unterteilt haben.

14. Überprüfen Sie die Einstellungen für den virtuellen 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. Beenden Sie den Analysemodus.

```
sensor(config-ana-vir)# exit

        sensor(config-ana)# exit

        sensor(config)#

        Apply Changes:?[yes]:
```

16. Drücken Sie **die Eingabetaste**, um die Änderungen anzuwenden, oder geben Sie **no** ein, um sie zu verwerfen.

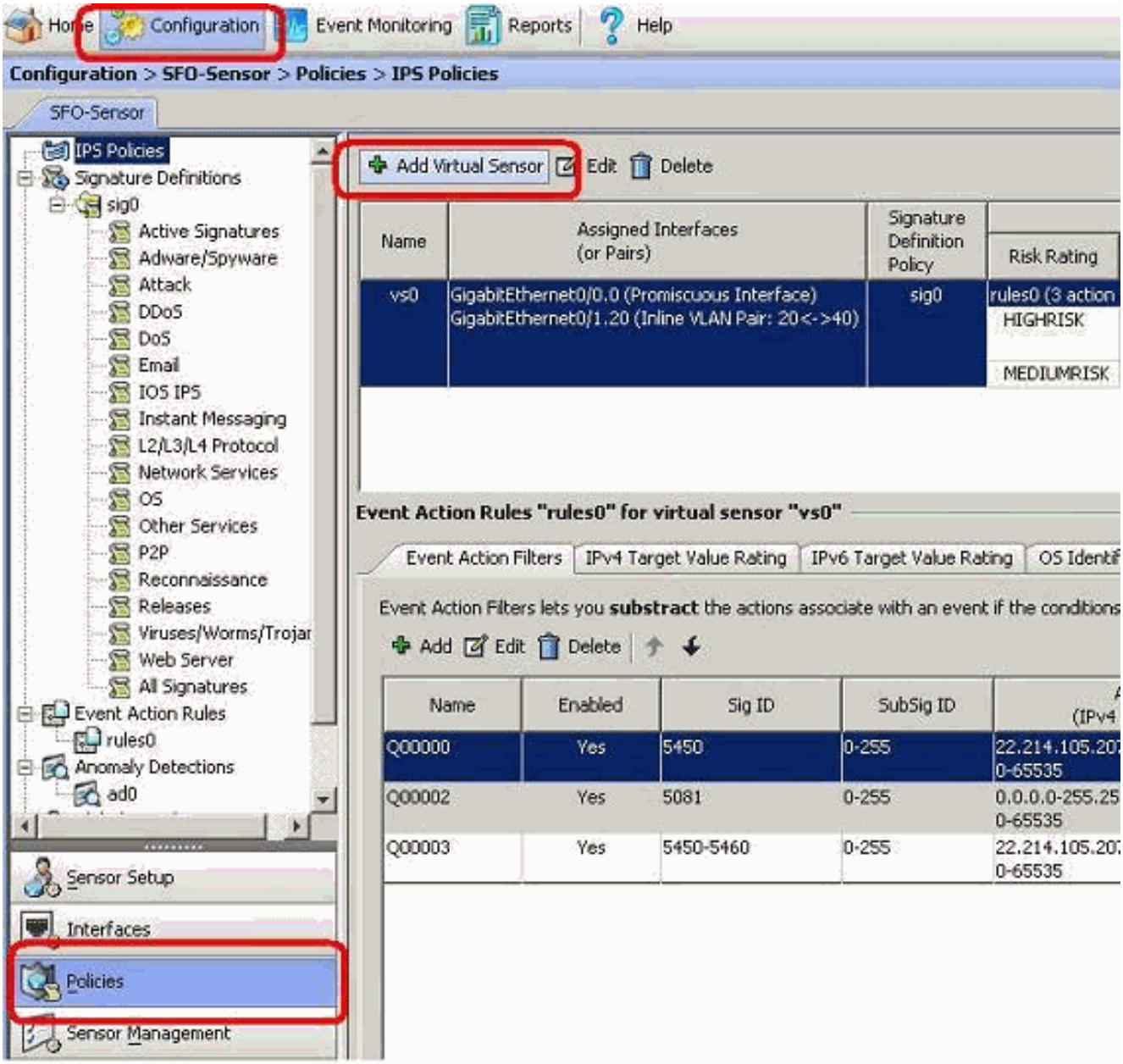
Damit ist das Hinzufügen eines virtuellen Sensors zum Cisco Secure Intrusion Prevention System (IPS) abgeschlossen. Führen Sie das gleiche Verfahren aus, um weitere virtuelle Sensoren hinzuzufügen.

Hinweis: Das Cisco Secure Intrusion Prevention System (IPS) unterstützt nicht mehr als vier virtuelle Sensoren. Der virtuelle Standardsensor ist vs0.

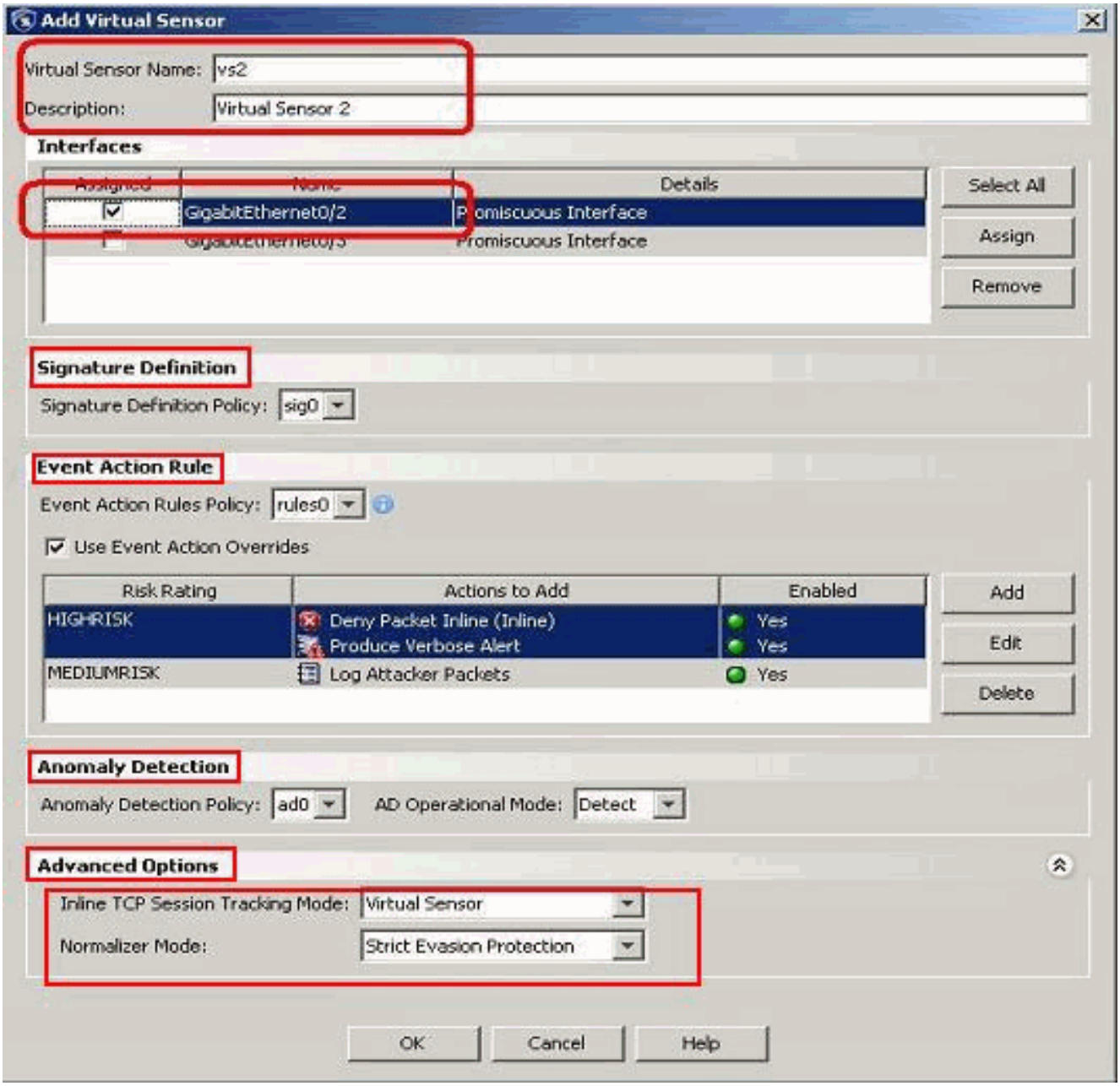
Virtuellen Sensor mit IME hinzufügen

Gehen Sie wie folgt vor, um einen virtuellen Sensor auf dem Cisco Secure Intrusion Prevention System (IPS) mit Cisco IPS Manager Express zu konfigurieren:

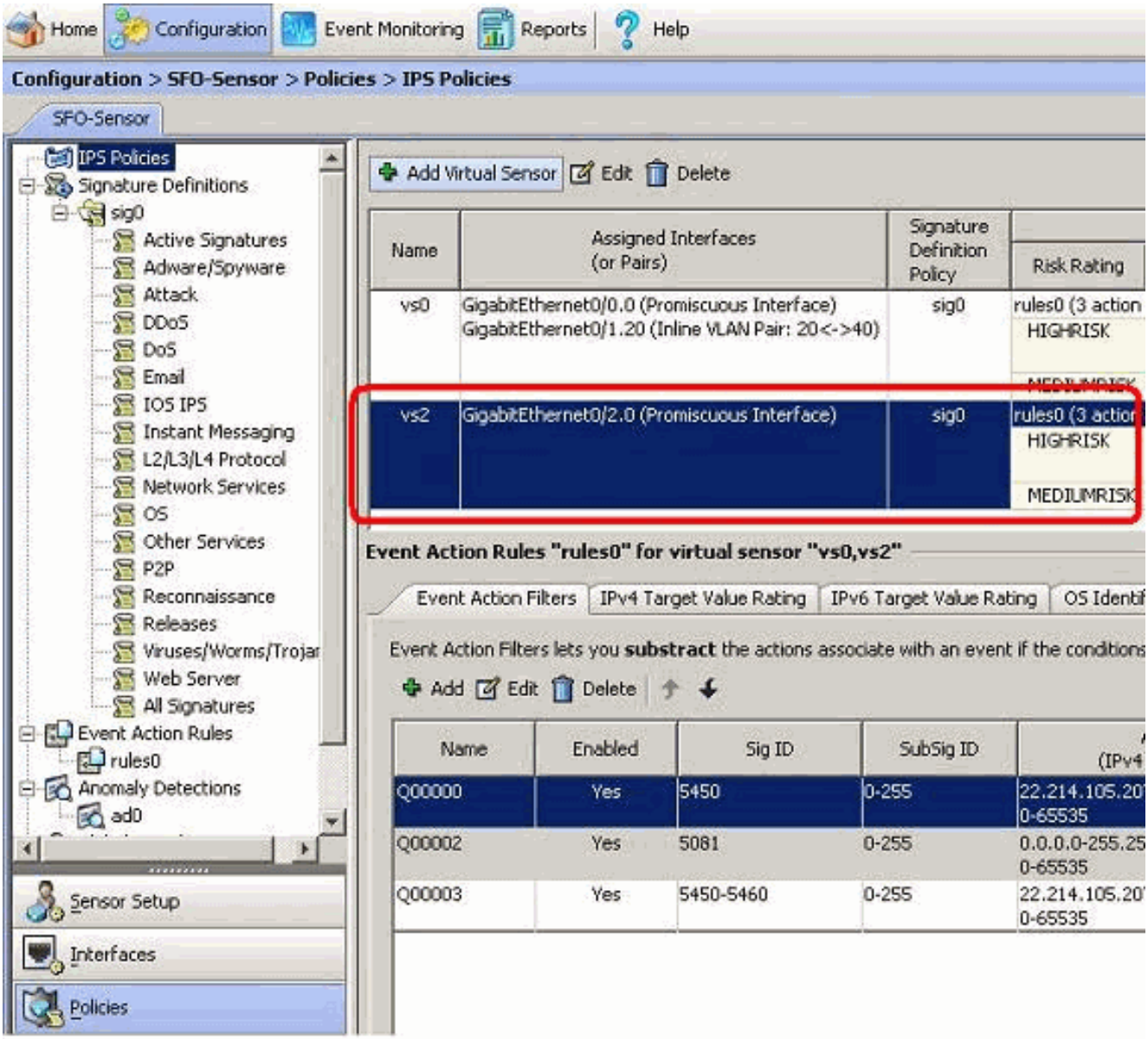
1. Wählen Sie **Configuration > SFO-Sensor> Policies > IPS Policies (Konfiguration > SFO-Sensor > Richtlinien > IPS-Richtlinien)**. Klicken Sie dann auf **Virtuellen Sensor hinzufügen**, wie im Screenshot
gezeigt.



2. Benennen Sie den virtuellen Sensor (in diesem Beispiel vs2), und fügen Sie dem virtuellen Sensor im dafür vorgesehenen Bereich eine Beschreibung hinzu. Weisen Sie diesem virtuellen Sensor auch die Schnittstellen des Promiscuous-Modus zu, die Sie hinzufügen möchten. Hier wird Gigabit Ethernet 0/2 ausgewählt. Geben Sie nun die Details in den Abschnitten **Signaturdefinition**, **Ereignishandlungsregel**, **Anomalieerkennung** und **Erweiterte Optionen** an, wie im Screenshot gezeigt.Geben Sie unter **Erweiterte Optionen** Details zum TCP-Sitzungs-Überwachungsmodus und zum Normalizer-Modus an. Hier ist der **TCP-Sitzungsverfolgungsmodus virtueller Sensor** und der **Normalizer-Modus** der **Modus Strict Evasion Protection**.



3. Klicken Sie auf **OK**.
4. Der neu hinzugefügte virtuelle Sensor vs2 wird in der Liste der virtuellen Sensoren angezeigt. Klicken Sie auf **Apply**, um die neue Konfiguration der virtuellen Sensoren an das Cisco Secure Intrusion Prevention System (IPS) zu senden.



Damit ist die Konfiguration zum Hinzufügen eines virtuellen Sensors abgeschlossen.

Virtuelle Sensoren bearbeiten

Die folgenden Parameter eines virtuellen Sensors können bearbeitet werden:

- Signaturdefinitionsrichtlinie
- Regeln für Ereignisaktionen
- Anomalie-Erkennungsrichtlinie
- Betriebsmodus zur Erkennung von Anomalien
- Inline-TCP-Sitzungsverfolgungsmodus
- Beschreibung
- Zugewiesene Schnittstellen

Gehen Sie wie folgt vor, um einen virtuellen Sensor zu bearbeiten:

1. Melden Sie sich bei der CLI mit einem Konto mit Administratorrechten an.
2. Wechseln Sie in den Dienstanalysemodus.

```
sensor# configure terminal

        sensor(config)# service analysis-engine
```

```
        sensor(config-ana)#
```

3. Bearbeiten Sie den virtuellen Sensor im Vergleich zu 1.
```
sensor(config-ana)# virtual-sensor vs2

        sensor(config-ana-vir)#
```
4. Bearbeiten Sie die Beschreibung dieses virtuellen Sensors.
```
sensor(config-ana-vir)# description virtual sensor A
```

5. Ändern Sie die Richtlinien zur Erkennung von Anomalien und den Betriebsmodus, der diesem virtuellen Sensor zugewiesen ist.
```
sensor(config-ana-vir)# anomaly-detection

        sensor(config-ana-vir-ano)# anomaly-detection-name ad0

        sensor(config-ana-vir-ano)# operational-mode learn
```

6. Ändern Sie die Ereignishandlerregelrichtlinie, die diesem virtuellen Sensor zugewiesen ist.
```
sensor(config-ana-vir-ano)# exit

        sensor(config-ana-vir)# event-action-rules rules0
```

7. Ändern Sie die Signaturdefinitionsrichtlinie, die diesem virtuellen Sensor zugewiesen ist.
```
sensor(config-ana-vir)# signature-definition sig0
```

8. Ändern Sie den inline TCP-Sitzungsverfolgungsmodus.
```
sensor(config-ana-vir)# inline-TCP-session-tracking-mode interface-and-vlan
```

   Der Standardwert ist "Virtual Sensor Mode" (virtueller Sensormodus). Diese Option ist fast immer die beste.
9. Anzeigen der Liste der verfügbaren Schnittstellen
```
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. Ändern Sie die Schnittstellen im Promiscuous-Modus, die diesem virtuellen Sensor zugewiesen sind.
```
sensor(config-ana-vir)# physical-interface GigabitEthernet0/2
```
11. Ändern Sie die diesem virtuellen Sensor zugewiesenen Inline-Schnittstellenpaare.
```
sensor(config-ana-vir)# logical-interface inline_interface_pair_name
```

    Sie müssen die Schnittstellen bereits gepaart haben.
12. Ändern Sie die Subschnittstelle mit den Inline-VLAN-Paaren oder -Gruppen, die diesem virtuellen Sensor zugewiesen sind.
```
sensor(config-ana-vir)# physical-interface GigabitEthernet2/0 subinterface-number
subinterface_number
```

Sie müssen alle Schnittstellen bereits in VLAN-Paare oder -Gruppen unterteilt haben.

13. Überprüfen Sie die geänderten Einstellungen für virtuelle Sensoren.

```
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. Beenden Sie den Analysemodus.

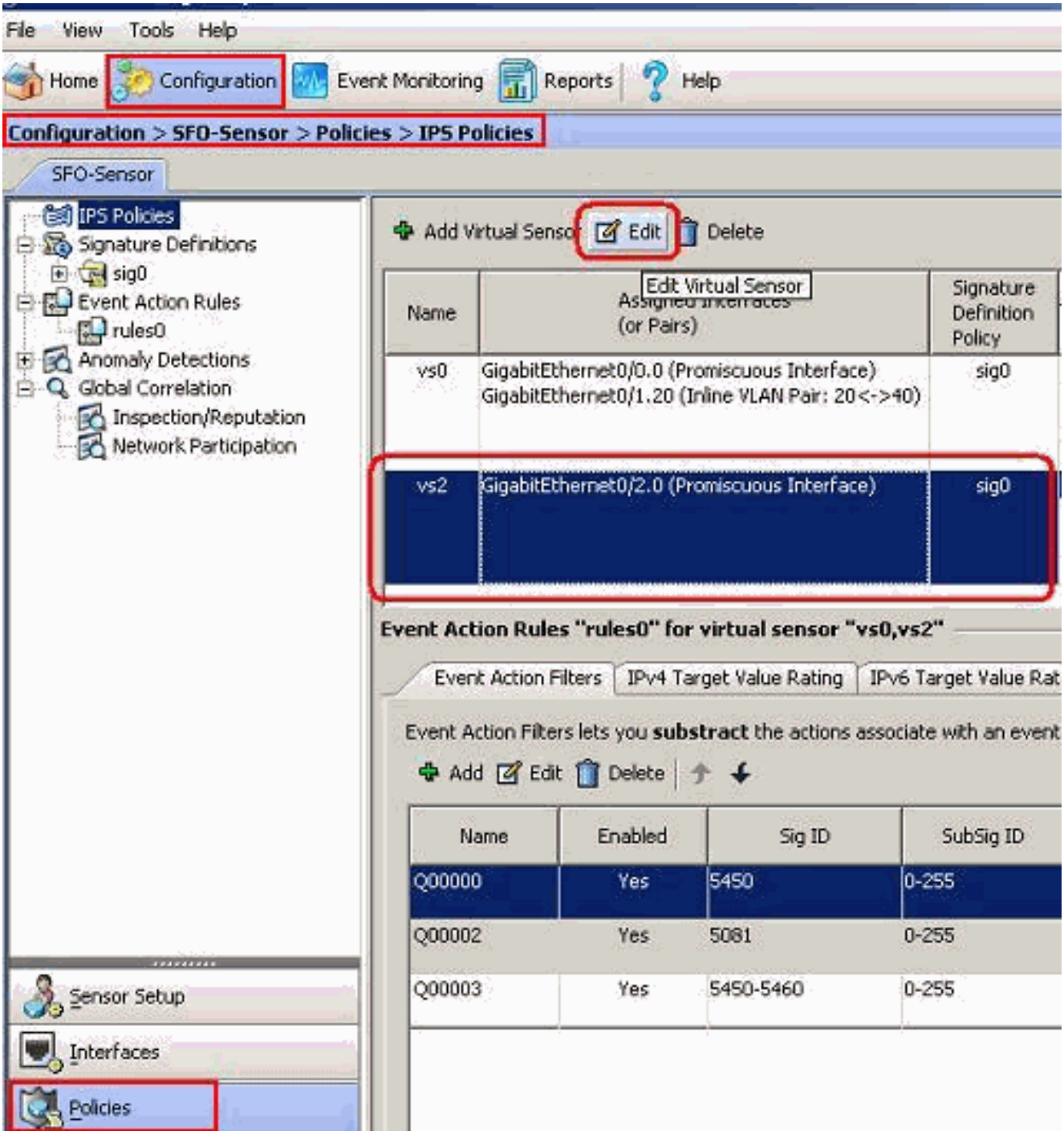
```
sensor(config-ana)# exit

        sensor(config)#

        Apply Changes:?[yes]:
```

15. Drücken Sie **die Eingabetaste**, um die Änderungen anzuwenden, oder geben Sie **no** ein, um sie zu verwerfen.

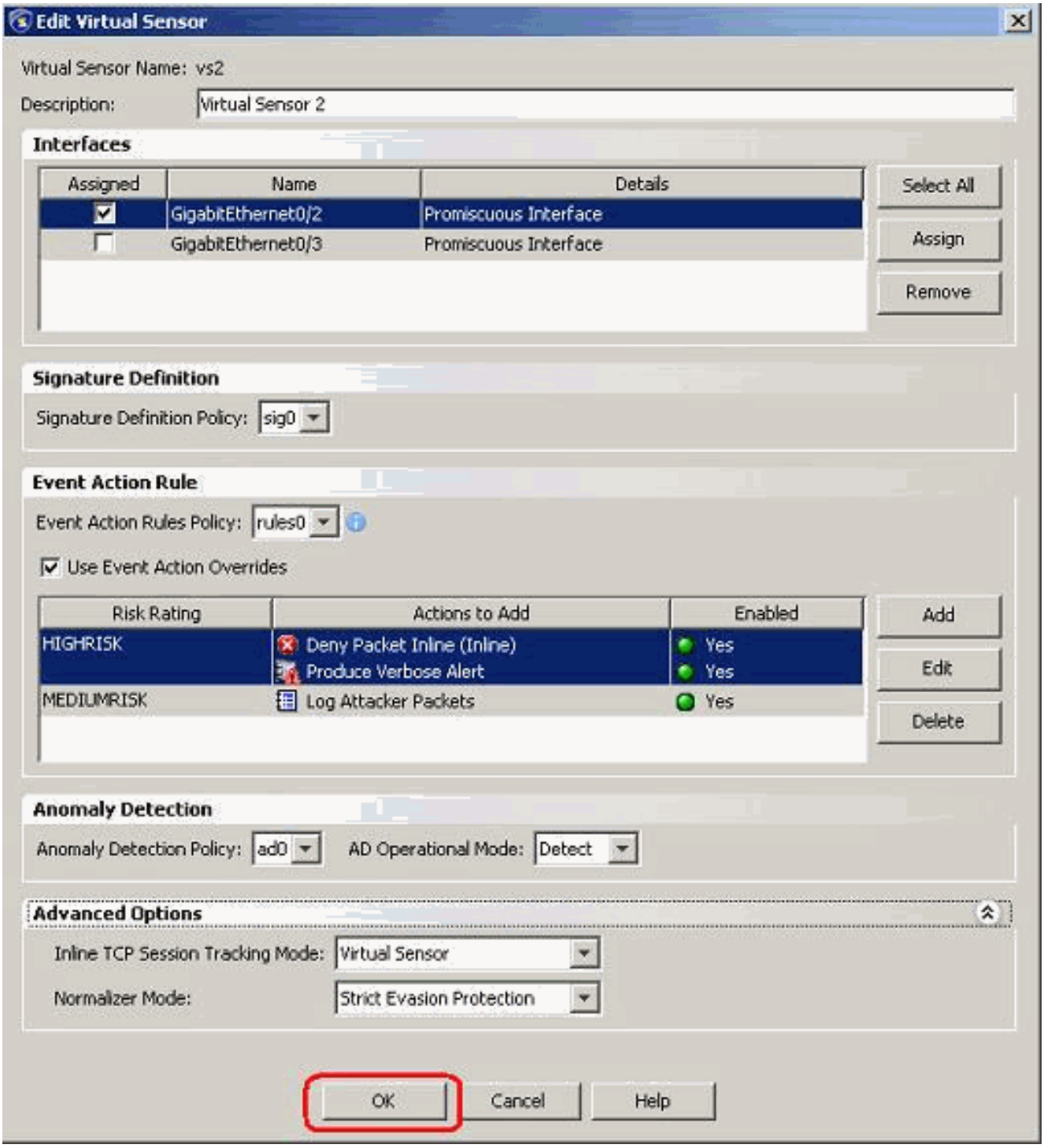
Virtuellen Sensor mit IME bearbeiten

Gehen Sie wie folgt vor, um einen virtuellen Sensor auf dem Cisco Secure Intrusion Prevention System (IPS) mit Cisco IPS Manager Express zu bearbeiten:

1. Wählen Sie **Configuration > SFO-Sensor> Policies > IPS Policies (Konfiguration > SFO-Sensor > Richtlinien > IPS-Richtlinien)**.
2. Wählen Sie den zu bearbeitenden virtuellen Sensor aus, und klicken Sie dann auf **Bearbeiten**, wie im Screenshot gezeigt. In diesem Beispiel ist vs2 der virtuelle Sensor, der bearbeitet werden
soll.



3. Nehmen Sie im Fenster **Virtuelle Sensor bearbeiten** Änderungen an den Parametern für den virtuellen Sensor vor, die unter den Abschnitten **Signaturdefinition**, **Ereignishandlungsregel**, **Anomalieerkennung** und **Erweiterte Optionen** angezeigt werden. Klicken Sie auf **OK** und dann auf
Übernehmen.



Damit ist der Prozess zum Bearbeiten eines virtuellen Sensors abgeschlossen.

Virtuelle Sensoren löschen

Gehen Sie wie folgt vor, um einen virtuellen Sensor zu löschen:

1. Um einen virtuellen Sensor zu löschen, geben Sie den Befehl **no virtual-sensor** ein.

```
sensor(config-ana)# virtual-sensor vs2

        sensor(config-ana-vir)#

        sensor(config-ana-vir)# exit

        sensor(config-ana)# no virtual-sensor vs2
```

2. Überprüfen Sie den gelöschten virtuellen Sensor.

```
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)#
```

Nur der virtuelle Standardsensor **vs0** ist vorhanden.

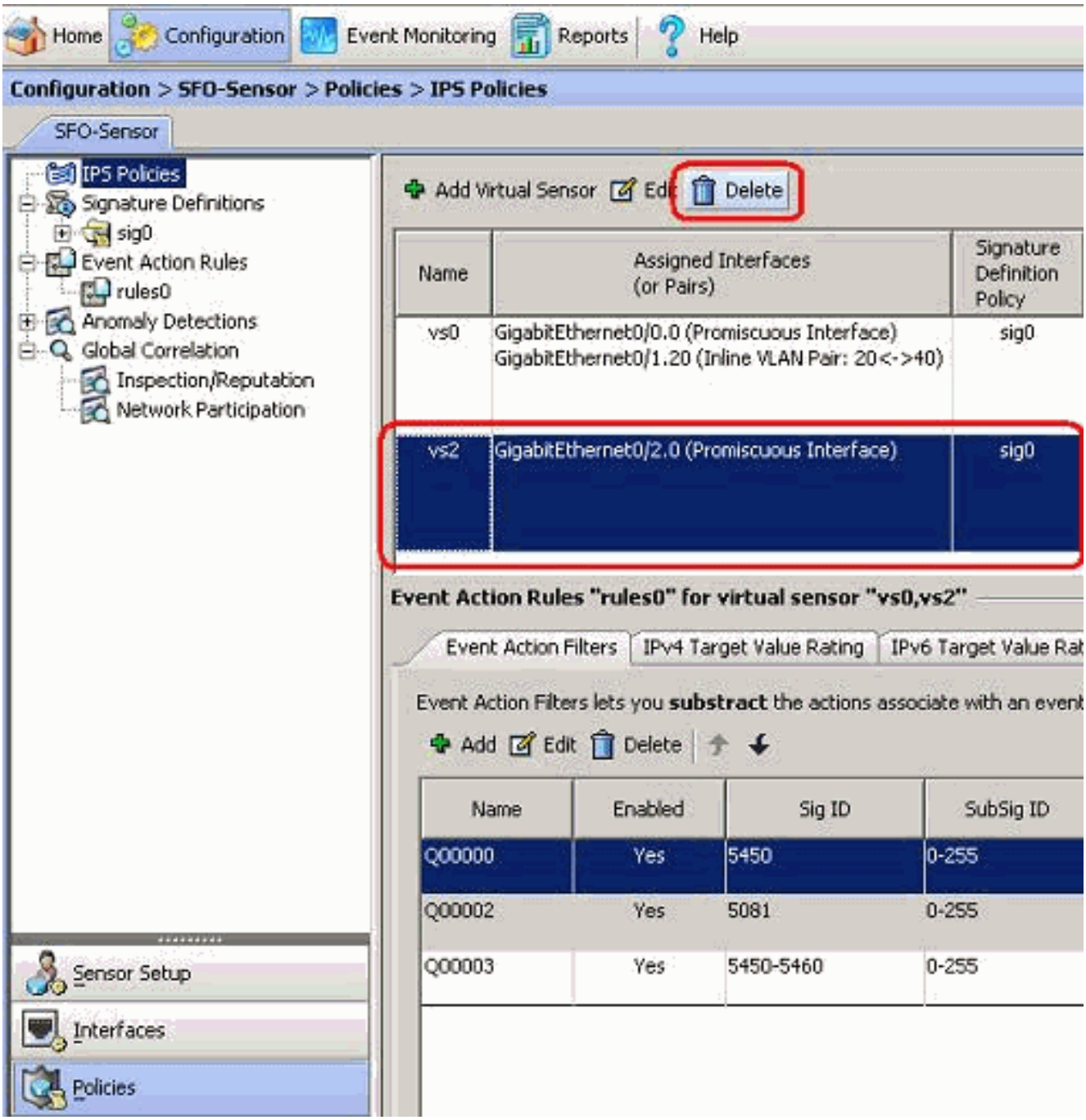
3. Beenden Sie den Analysemodus.

```
sensor(config-ana)# exit

        sensor(config)#

        Apply Changes:?[yes]:
```

Virtuellen Sensor mit IME löschen

Gehen Sie wie folgt vor, um einen virtuellen Sensor auf dem Cisco Secure Intrusion Prevention System (IPS) mit Cisco IPS Manager Express zu löschen:

1. Wählen Sie **Configuration > SFO-Sensor> Policies > IPS Policies (Konfiguration > SFO-Sensor > Richtlinien > IPS-Richtlinien)**.
2. Wählen Sie den zu löschenden virtuellen Sensor aus, und klicken Sie dann auf **Löschen**, wie im Screenshot gezeigt. In diesem Beispiel ist vs2 der virtuelle Sensor, der gelöscht werden soll.



Damit ist das Löschen eines virtuellen Sensors abgeschlossen. Der virtuelle Sensor vs2 wird gelöscht.

Fehlerbehebung

IPS Manager Express wird nicht gestartet.

Problem

Wenn versucht wird, über das IME auf das IPS zuzugreifen, startet IPS Manager Express nicht, und die Fehlermeldung wird angezeigt:

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

Lösung

Laden Sie zum Beheben dieses Problems den IME-Workstation-PC neu.

Zugehörige Informationen

- Support-Seite für das Cisco Intrusion Prevention System
- Support-Seite für Cisco IPS Manager Express
- Network Time Protocol (NTP)
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation für Cisco Systeme