

# IPS 6.X en hoger - Configuratie van virtuele sensoren met IME

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Verwante producten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[Over de analyse-engine](#)

[Over virtuele sensoren](#)

[Voordelen en beperkingen van virtualisatie](#)

[Voordelen van virtualisatie](#)

[Beperkingen van virtualisatie](#)

[Virtualisatievereisten](#)

[Configureren](#)

[Virtuele sensoren toevoegen](#)

[Virtuele sensor met IME toevoegen](#)

[Virtuele sensoren bewerken](#)

[Virtuele sensor met IME bewerken](#)

[Virtuele sensoren verwijderen](#)

[Virtuele sensor met IME verwijderen](#)

[Problemen oplossen](#)

[IPS Manager Express lanceert niet](#)

[Gerelateerde informatie](#)

## [Inleiding](#)

Dit document verklaart de functie van Analysis Engine en hoe u virtuele sensoren kunt maken, bewerken en verwijderen op het Cisco Secure Inbraakpreventiesysteem (IPS) met Cisco IPS Manager Express (IME). Het legt ook uit hoe interfaces aan een virtuele sensor worden toegewezen.

**Opmerking:** AIM-IPS en NME-IPS ondersteunen virtualisatie niet.

## [Voorwaarden](#)

## [Vereisten](#)

Er zijn geen specifieke voorwaarden van toepassing op dit document.

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 4200 Series IPS-apparaat waarmee softwareversie 6.0 en hoger wordt uitgevoerd
- Cisco IPS Manager Express (IME) versie 6.1.1 en hoger**Opmerking:** Hoewel IME kan worden gebruikt om sensorapparaten te bewaken die Cisco IPS 5.0 en hoger uitvoeren, worden sommige nieuwe functies en functies die in IME worden geleverd alleen ondersteund op sensoren die Cisco IPS 6.1 of hoger uitvoeren.**Opmerking:** Cisco Secure Inbraakpreventiesysteem (IPS) 5.x ondersteunt alleen de standaard virtuele sensor vs0. Virtuele sensoren anders dan de standaard vs0 worden ondersteund in IPS 6.x en later.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## Verwante producten

Deze configuratie kan ook met deze sensoren worden gebruikt:

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

## Conventies

Raadpleeg de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

## Achtergrondinformatie

### Over de analyse-engine

Analyse Engine voert pakketanalyse uit en signaleert detectie. Het controleert verkeer dat door gespecificeerde interfaces stroomt. U maakt virtuele sensoren in Analysis Engine. Elke virtuele sensor heeft een unieke naam met een lijst van interfaces, inline interfaceparen, inline VLAN paren, en VLAN groepen verbonden aan het. Om te voorkomen dat een definitie problemen oplegt, zijn er geen conflicten of overlappingsen bij opdrachten toegestaan. U kent interfaces, inline interfaceparen, inline VLAN-paren en VLAN-groepen toe aan een specifieke virtuele sensor, zodat er geen pakket door meer dan één virtuele sensor wordt verwerkt. Elke virtuele sensor wordt ook geassocieerd met een specifiek genoemde kenmerkende definitie, gebeurtenis actieregels, en anomalie detectie configuratie. Packets van interfaces, inline interfacepaarten, inline VLAN-paren en VLAN-groepen die niet aan een virtuele sensor zijn toegewezen, worden op basis van de inline bypassconfiguratie verwijderd.

## Over virtuele sensoren

De sensor kan gegevensinvoer uit een of meer gecontroleerde gegevensstromen ontvangen. Deze gecontroleerde gegevensstromen kunnen fysieke interfacepoorten of virtuele interfacepoorten zijn. Een enkele sensor kan bijvoorbeeld verkeer controleren vanaf voor de firewall, vanaf achter de firewall of vanaf voor en achter de firewall. Een enkele sensor kan één of meer gegevensstromen bewaken. In deze situatie wordt op alle gecontroleerde gegevensstromen één enkel sensorbeleid of één enkele configuratie toegepast. Een virtuele sensor is een verzameling gegevens die wordt gedefinieerd door een aantal configuratiebeleidsmaatregelen. De virtuele sensor wordt toegepast op een verzameling pakketten zoals gedefinieerd door de interfacecomponent. Een virtuele sensor kan meerdere segmenten bewaken. Je kan een ander beleid of configuratie toepassen voor elke virtuele sensor in één fysieke sensor. U kunt een ander beleid instellen per gecontroleerd segment onder analyse. U kunt ook dezelfde beleidsinstantie toepassen, bijvoorbeeld, sig0, regels0 of ad0, op verschillende virtuele sensoren. U kunt interfaces, inline interfacepaarten, inline VLAN-paren en VLAN-groepen toewijzen aan een virtuele sensor.

**Opmerking:** Cisco Secure Inbraakpreventiesysteem (IPS) biedt geen ondersteuning voor meer dan vier virtuele sensoren. De standaard virtuele sensor is vs0. U kunt de standaard virtuele sensor niet verwijderen. De interfacelijst, de operationele modus voor de detectie van abnormaliteiten, de modus voor het opsporen van TCP-sessie in het inline trainen en de beschrijving van de virtuele sensor zijn de enige configuratiefuncties die u kunt wijzigen voor de standaard virtuele sensor. U kunt de kenmerkende definitie, de regels van de gebeurtenis, of het beleid voor de detectie van abnormaliteiten niet wijzigen.

## Voordelen en beperkingen van virtualisatie

### Voordelen van virtualisatie

Virtualisatie heeft deze voordelen:

- U kunt verschillende configuraties toepassen op verschillende verkeersgroepen.
- U kunt twee netwerken met overlappende IP-ruimtes met één sensor bewaken.
- U kunt zowel binnen als buiten een firewall of NAT-apparaat bewaken.

### Beperkingen van virtualisatie

Virtualisatie kent deze beperkingen:

- U moet beide kanten van asymmetrisch verkeer aan dezelfde virtuele sensor toewijzen.
- Het gebruik van VACL-opname of SPAN (veelbelovende bewaking) is niet in overeenstemming met VLAN-markering, wat problemen met VLAN-groepen veroorzaakt. Wanneer u Cisco IOS-software gebruikt, ontvangen een VACL-opnamepoort of een SPAN-doel niet altijd gelabelde pakketten, zelfs als deze zijn geconfigureerd voor trunking. Wanneer u MSFC gebruikt, veranderen de snelle weg omschakeling van geleerde routes het gedrag van VACL vangt en SPAN.
- Persistent opslaan is beperkt.

## Virtualisatievereisten

Virtualisatie heeft deze vereisten voor verkeersopnamen:

- De virtuele sensor moet verkeer ontvangen dat 802.1q kopregels heeft, anders dan verkeer op het inheemse VLAN van de haven van de vangst.
- De sensor moet beide richtingen van verkeer in dezelfde VLAN-groep in dezelfde virtuele sensor zien voor een bepaalde sensor.

## Configureren

In deze sectie wordt u voorgesteld met de informatie om virtuele sensoren toe te voegen, te bewerken en te verwijderen.

### Virtuele sensoren toevoegen

Geef de opdracht [virtuele-sensornaam](#) uit in de testmodemsubmodus om een virtuele sensor te maken. U verdeelt beleid (anomalie-detectie, gebeurtenissen-actieregels en signatuur definitie) aan de virtuele sensor. Vervolgens wijst u interfaces (veelbelovende, inline interfaceparen, inline VLAN-paren en VLAN-groepen) aan de virtuele sensor toe. U dient de inline interfaceparen en VLAN-paren te configureren voordat u ze aan een virtuele sensor kunt toewijzen. Deze opties zijn van toepassing:

- **detectie van abnormaliteiten**—parameters voor detectie van abnormaliteiten. Naam van de anomalie-detectienaam **operationeel-mode**—analoge detectiemodus (**inactief, leert, detecteert**)
- **Beschrijving** —Beschrijving van de virtuele sensor
- **gebeurtenis-actie-regels**-Naam van het beleid van de gebeurtenis-regels
- **Inline-TCP-on-evsion-protection-mode** - **Hiermee** kunt u kiezen welk type van de modus Normalizer u nodig hebt voor een verkeerscontrole: **asymmetrisch** —Kan slechts één richting van bidirectionele verkeersstroom zien. Met de bescherming van de symmetrische modus wordt de ontwijkingsbescherming in de TCP-laag versoepeld. **Opmerking:** Met de asymmetrische modus kan de sensor synchroon met de stroom worden gepositioneerd en kan er controle worden uitgevoerd op motoren die niet beide richtingen nodig hebben. Asymmetric mode verlaagt de beveiliging omdat de volledige bescherming beide kanten van het verkeer vereist om te zien. **strikt** - Als een pakje om het even welke reden gemist wordt, worden alle pakketten na het gemiste pakket niet verwerkt. Streng ontduikingsbescherming voorziet in volledige handhaving van TCP staat en sequentie tracking. **Opmerking:** Alle buiten orde gestelde pakketten of gemiste pakketten kunnen de handtekening van de motor van Normalizer 1300 of 1330 leveren, die de situatie proberen te corrigeren, maar kunnen leiden tot ontkende aansluitingen.
- **inline-TCP-sessie-tracking-mode**-geavanceerde methode waarmee u dubbele TCP-sessie in inline verkeer kunt identificeren. Standaard wordt de virtuele sensor gebruikt, wat vrijwel altijd de beste keuze is. **virtueel-sensor** — Alle pakketten met dezelfde sessiesleutel (AaBb) binnen een virtuele sensor behoren tot dezelfde sessie. **interface-en-VLAN**-Alle pakketten met dezelfde sessiesleutel (AaBb) in hetzelfde VLAN (of inline VLAN-paar) en op dezelfde interface behoren tot dezelfde sessie. Packets met dezelfde toets maar op verschillende VLAN's of interfaces worden afzonderlijk gevolgd. Alle pakketten met dezelfde sessie (AaBb) in hetzelfde VLAN (of inline VLAN-paar) ongeacht de interface behoren tot dezelfde sessie. Packets met dezelfde toets maar op verschillende VLAN's worden afzonderlijk gevolgd.
- **signatuur-definitie**—Naam van het beleid inzake de kenmerking van de handtekening

- **logische interfaces**—naam van de logische interfaces (inline interfaceparen)
- **fysisch-interfaces**—naam van de fysieke interfaces (veelbelovende, inline VLAN-paren, en VLAN-groepen)**subinterface-nummer**—het fysieke subinterfacenummer. Als het subinterface-type geen is, wijst de waarde van 0 erop dat de gehele interface in veelbelovende modus wordt toegewezen.**Nee** - Verwijdert een ingang of selectie

Voltooi de volgende stappen om een virtuele sensor toe te voegen:

1. Meld u aan bij de CLI met een account met Administrator-rechten.
2. Geef de modus voor serviceanalyse op.

```
sensor# configure terminal

        sensor(config)# service analysis-engine

        sensor(config-ana)#
```

3. Voeg een virtuele sensor toe.

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

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

4. Voeg een beschrijving toe voor deze virtuele sensor.

```
sensor(config-ana-vir)# description virtual sensor 2
```

5. Aan deze virtuele sensor een beleid en operationele modus voor de detectie van abnormaliteiten toewijzen.

```
sensor(config-ana-vir)# anomaly-detection

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

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

6. Het beleid van een evenement aan deze virtuele sensor toewijzen.

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

        sensor(config-ana-vir)# event-action-rules rules1
```

7. Een beleid met een kenmerkende definitie aan deze virtuele sensor toewijzen.

```
sensor(config-ana-vir)# signature-definition sig1
```

8. Toewijzen de inline TCP sessie tracking-modus.

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

Standaard wordt de virtuele sensor gebruikt, wat vrijwel altijd de beste optie is om te kiezen.

9. Pas de inline TCP-beschermingsmodus aan.

```
sensor(config-ana-vir)# inline-TCP-evasion-protection-mode strict
```

Dit is een strikte modus die bijna altijd de beste optie is om te kiezen.

10. Toont de lijst met beschikbare interfaces.

```
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. Wijs de veelbelovende wijze interfaces toe die u aan deze virtuele sensor wilt toevoegen.

```
sensor(config-ana-vir)# physical-interface GigabitEthernet0/2
```

Herhaal deze stap voor alle veelbelovende interfaces die u aan deze virtuele sensor wilt toewijzen.

12. Pas de inline-interfaceparen aan die u aan deze virtuele sensor wilt toevoegen.

```
sensor(config-ana-vir)# logical-interface inline_interface_pair_name
```

U moet de interfaces al hebben gekoppeld.

13. Pas de subinterfaces aan van de inline VLAN-paren of groepen die u aan deze virtuele sensor wilt toevoegen, zoals hieronder wordt getoond:

```
sensor(config-ana-vir)# physical-interface GigabitEthernet2/0 subinterface-number  
subinterface_number
```

U moet alle interfaces al in VLAN-paren of -groepen hebben onderverdeeld.

14. Controleer de instellingen van de virtuele 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. Modus van de uitlaatmotor.

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

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

```
sensor(config)#
```

```
Apply Changes:[yes]:
```

16. Druk op **ENTER** om de wijzigingen toe te passen of **nee** in te voeren om ze weg te gooien. Dit voltooit het proces om een virtuele sensor aan het Cisco Secure Inbraakpreventiesysteem (IPS) toe te voegen. Volg dezelfde procedure om meer virtuele sensoren toe te voegen.

**Opmerking:** Cisco Secure Inbraakpreventiesysteem (IPS) biedt geen ondersteuning voor meer dan vier virtuele sensoren. De standaard virtuele sensor is vs0.

### [Virtuele sensor met IME toevoegen](#)

Voltooi deze stappen om een virtuele sensor op Cisco Secure Inbraakpreventiesysteem (IPS) te configureren met Cisco IPS Manager Express:

1. Kies **Configuration > SFO-Sensor> beleidslijnen> IPS-beleid**. Klik vervolgens op **virtuele sensor toevoegen** zoals in de screenshot aangegeven.

The screenshot shows the SFO-Sensor configuration interface. The 'Configuration' tab is selected. The breadcrumb path is 'Configuration > SFO-Sensor > Policies > IPS Policies'. The left sidebar shows a tree view of 'Signature Definitions' and 'Event Action Rules'. The 'Add Virtual Sensor' button is highlighted with a red box. Below it, a table lists virtual sensors:

Name	Assigned Interfaces (or Pairs)	Signature Definition Policy	Risk Rating
vs0	GigabitEthernet0/0.0 (Promiscuous Interface) GigabitEthernet0/1.20 (Inline VLAN Pair: 20<->40)	sig0	rules0 (3 action) HIGHRISK MEDIUMRISK

Below the table, the 'Event Action Rules "rules0" for virtual sensor "vs0"' section is visible, showing a table of event action filters:

Name	Enabled	Sig ID	SubSig ID	(IPv4)
Q00000	Yes	5450	0-255	22.214.105.207 0-65535
Q00002	Yes	5081	0-255	0.0.0.0-255.255 0-65535
Q00003	Yes	5450-5460	0-255	22.214.105.207 0-65535

2. Geef de virtuele sensor (vs2 in dit voorbeeld) een naam en voeg een beschrijving toe aan de virtuele sensor in de meegeleverde ruimte. Geef ook de veelbelovende wijze interfaces toe die u aan deze virtuele sensor wilt toevoegen. Gigabit Ethernet 0/2 is hier geselecteerd. Geef nu de details in de **signatuur-definitie**, **Event Action Rule**, **Anomaly Detectie** en **Geavanceerde opties** zoals getoond in het schermshot. Typ onder **Geavanceerde opties** de informatie over de TCP-sessietraceringsmodus en de modus Normalizer. Hier is de **TCP-sessie Tracking-modus** een virtuele sensor en de **Normalizer-modus** is de **strikte Evasion Protection-modus**.



**Add Virtual Sensor**

Virtual Sensor Name: vs2  
 Description: Virtual Sensor 2

**Interfaces**

Assigned	Name	Details
<input checked="" type="checkbox"/>	GigabitEthernet0/2	Promiscuous Interface
<input type="checkbox"/>	GigabitEthernet0/3	Promiscuous Interface

Select All  
Assign  
Remove

**Signature Definition**

Signature Definition Policy: sig0

**Event Action Rule**

Event Action Rules Policy: rules0

Use Event Action Overrides

Risk Rating	Actions to Add	Enabled
HIGHRISK	Deny Packet Inline (Inline) Produce Verbose Alert	Yes Yes
MEDIUMRISK	Log Attacker Packets	Yes

Add  
Edit  
Delete

**Anomaly Detection**

Anomaly Detection Policy: ad0 AD Operational Mode: Detect

**Advanced Options**

Inline TCP Session Tracking Mode: Virtual Sensor  
 Normalizer Mode: Strict Evasion Protection

OK Cancel Help

3. Klik op **OK**.

4. De nieuw toegevoegde virtuele sensor vs2 is opgenomen in de lijst van virtuele sensoren. Klik op **Toepassen** voor de nieuwe configuratie van de virtuele sensor die naar het Cisco Secure Inbraakpreventiesysteem (IPS) moet worden verzonden.

The screenshot shows the SFO-Sensor configuration interface. The left sidebar displays a tree view of configuration options, including Signature Definitions (sig0) and Event Action Rules (rules0). The main area shows the configuration for virtual sensors. A table lists the sensors:

Name	Assigned Interfaces (or Pairs)	Signature Definition Policy	Risk Rating
vs0	GigabitEthernet0/0.0 (Promiscuous Interface) GigabitEthernet0/1.20 (Inline VLAN Pair: 20<->40)	sig0	rules0 (3 action) HIGH RISK
vs2	GigabitEthernet0/2.0 (Promiscuous Interface)	sig0	rules0 (3 action) HIGH RISK

Below the table, the Event Action Rules for virtual sensor "vs0,vs2" are shown. The filters table is as follows:

Name	Enabled	Sig ID	SubSig ID	(IPv4)
Q00000	Yes	5450	0-255	22.214.105.20 0-65535
Q00002	Yes	5081	0-255	0.0.0.0-255.25 0-65535
Q00003	Yes	5450-5460	0-255	22.214.105.20 0-65535

Hiermee wordt de configuratie voltooid om een virtuele sensor toe te voegen.

## [Virtuele sensoren bewerken](#)

Deze parameters van een virtuele sensor kunnen worden bewerkt:

- Vastleggingsbeleid voor de ondertekening
- Beleid inzake noodmaatregelen
- Detectiebeleid voor abnormaliteiten
- Operationele modus voor detectie van abnormaliteiten
- Inline TCP-sessie-traceringsmodus
- Beschrijving
- Getoegewezen interfaces

Voltooi de volgende stappen om een virtuele sensor te bewerken:

1. Meld u aan bij de CLI met een account met Administrator-rechten.
2. Geef de modus voor serviceanalyse op.

```
sensor# configure terminal
```

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

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

### 3. Bewerk de virtuele sensor vs1.

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

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

### 4. Bewerk de beschrijving van deze virtuele sensor.

```
sensor(config-ana-vir)# description virtual sensor A
```

### 5. Verander het anomalie-detectiebeleid en de operationele modus die aan deze virtuele sensor zijn toegewezen.

```
sensor(config-ana-vir)# anomaly-detection
```

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

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

### 6. Wijzig het aan deze virtuele sensor toegewezen beleid van de regels van de gebeurtenis.

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

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

### 7. Verander het kenmerkende beleid dat aan deze virtuele sensor is toegewezen.

```
sensor(config-ana-vir)# signature-definition sig0
```

### 8. Verander de inline TCP sessie tracking-modus.

```
sensor(config-ana-vir)# inline-TCP-session-tracking-mode interface-and-vlan
```

Standaard wordt de virtuele sensor gebruikt, wat vrijwel altijd de beste optie is om te kiezen.

### 9. Toont de lijst met beschikbare interfaces.

```
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. Verander de veelbelovende wijze interfaces die aan deze virtuele sensor zijn toegewezen.

```
sensor(config-ana-vir)# physical-interface GigabitEthernet0/2
```

### 11. Verander de inline interfaceparen die aan deze virtuele sensor zijn toegewezen.

```
sensor(config-ana-vir)# logical-interface inline_interface_pair_name
```

U moet de interfaces al hebben gekoppeld.

### 12. Verander de subinterface met de inline VLAN-paren of groepen die aan deze virtuele sensor zijn toegewezen.

```
sensor(config-ana-vir)# physical-interface GigabitEthernet2/0 subinterface-number  
subinterface_number
```

U moet alle interfaces al in VLAN-paren of -groepen hebben onderverdeeld.

### 13. Controleer de bewerkte virtuele sensorinstellingen.

```
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. Modus van de uitlaatmotor.

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

```
sensor(config)#
```

```
Apply Changes:[yes]:
```

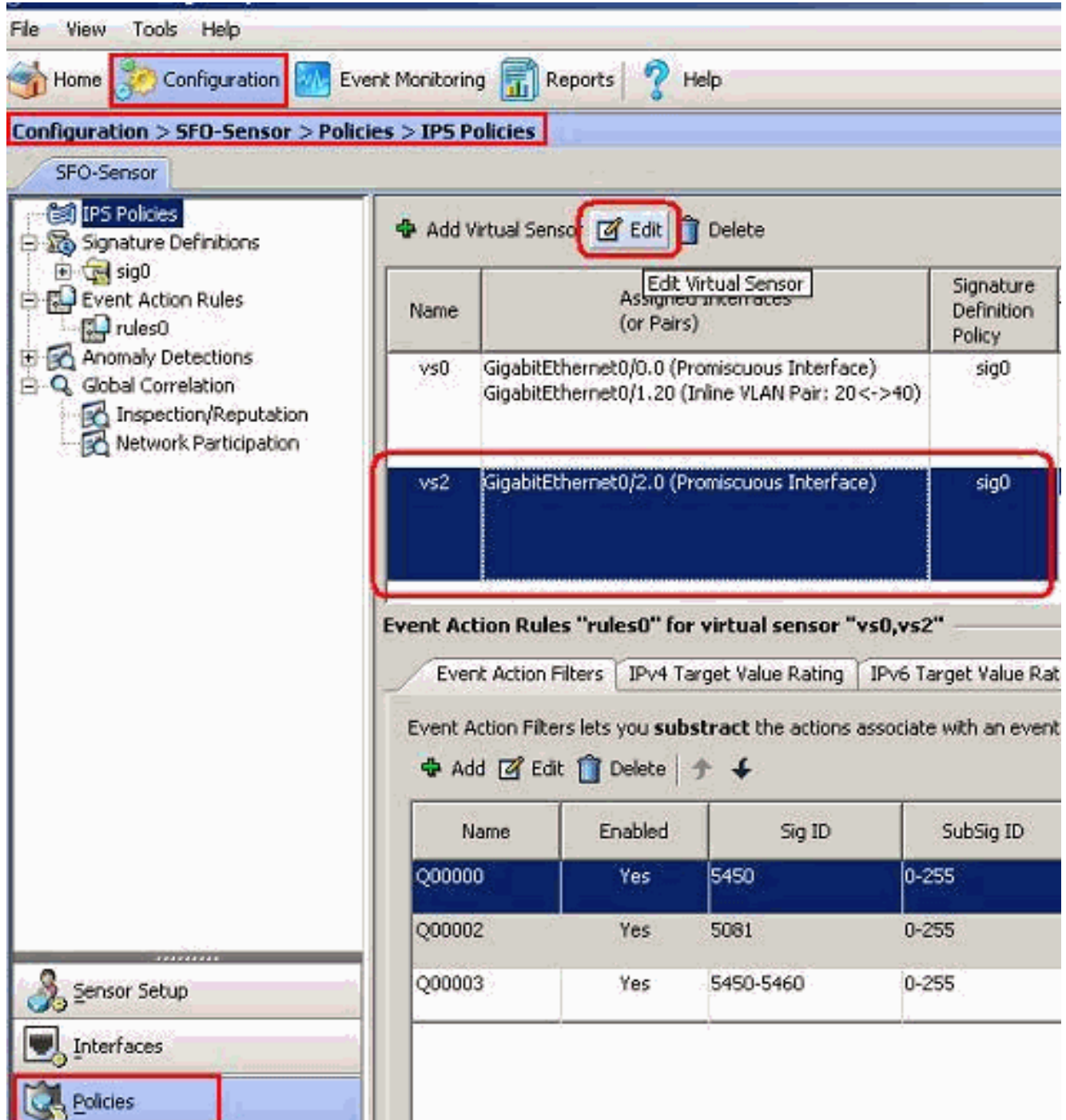
15. Druk op **ENTER** om de wijzigingen toe te passen of **nee** in te voeren om ze weg te gooien.

## [Virtuele sensor met IME bewerken](#)

Voltooi deze stappen om een virtuele sensor op Cisco Secure Inbraakpreventiesysteem (IPS) te bewerken met Cisco IPS Manager Express:

1. Kies **Configuration > SFO-Sensor> beleidslijnen> IPS-beleid**.
2. Kies de virtuele sensor die wordt bewerkt en klik vervolgens op **Bewerken** zoals in de

screenshot. In dit voorbeeld vs2 is de virtuele sensor die moet worden bewerkt.



3. Wijzig in het venster **Virtuele sensor bewerken** de parameters voor de virtuele sensor die aanwezig is onder de **definitie van onderdeel, Event Action Rule, Anomaly Detectie en Geavanceerde opties**. Klik op **OK** en vervolgens op **Toepassen**.

**Edit Virtual Sensor**

Virtual Sensor Name: vs2  
 Description: Virtual Sensor 2

**Interfaces**

Assigned	Name	Details
<input checked="" type="checkbox"/>	GigabitEthernet0/2	Promiscuous Interface
<input type="checkbox"/>	GigabitEthernet0/3	Promiscuous Interface

Select All  
Assign  
Remove

**Signature Definition**

Signature Definition Policy: sig0

**Event Action Rule**

Event Action Rules Policy: rules0

Use Event Action Overrides

Risk Rating	Actions to Add	Enabled
HIGH RISK	Deny Packet Inline (Inline)	Yes
	Produce Verbose Alert	Yes
MEDIUM RISK	Log Attacker Packets	Yes

Add  
Edit  
Delete

**Anomaly Detection**

Anomaly Detection Policy: ad0 AD Operational Mode: Detect

**Advanced Options**

Inline TCP Session Tracking Mode: Virtual Sensor  
 Normalizer Mode: Strict Evasion Protection

OK Cancel Help

Hiermee wordt het proces voor het bewerken van een virtuele sensor voltooid.

## [Virtuele sensoren verwijderen](#)

Voltooi de volgende stappen om een virtuele sensor te verwijderen:

1. Om een virtuele sensor te verwijderen, dient u de **geen virtuele sensor** opdracht uit te voeren.

```

sensor(config-ana)# virtual-sensor vs2

sensor(config-ana-vir)#

sensor(config-ana-vir)# exit

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

```

## 2. Controleer de verwijderde virtuele 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)#
```

Alleen de standaard virtuele sensor, **vs0**, is aanwezig.

## 3. Modus van de uitlaatmotor.

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

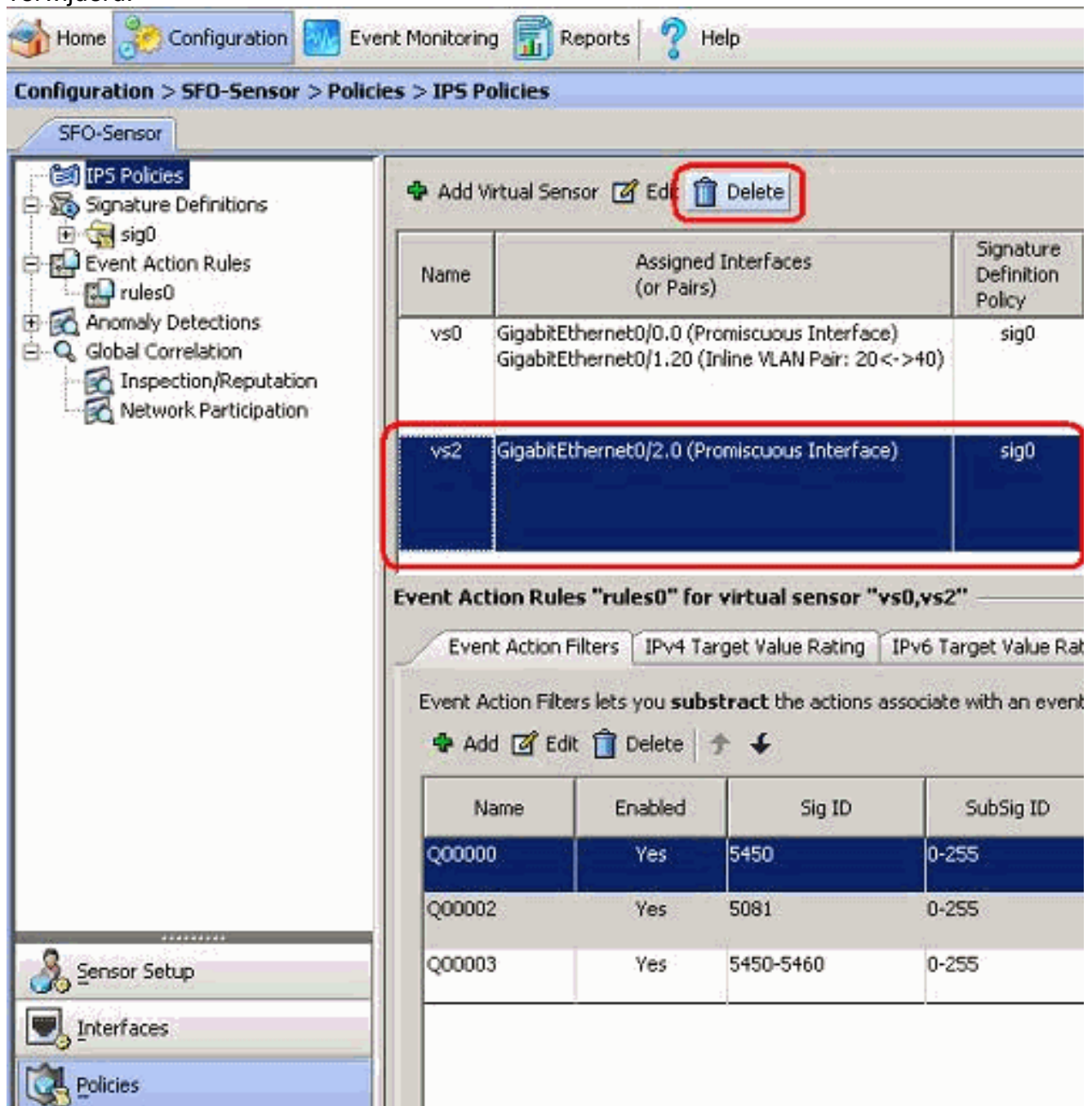
```
sensor(config)#
```

Apply Changes:?[yes]:

## Virtuele sensor met IME verwijderen

Voltooi deze stappen om een virtuele sensor op Cisco Secure Inbraakpreventiesysteem (IPS) te verwijderen met Cisco IPS Manager Express:

1. Kies **Configuration > SFO-Sensor> beleidslijnen> IPS-beleid**.
2. Kies de virtuele sensor die moet worden verwijderd en klik vervolgens op **Verwijderen**, zoals in de screenshot wordt weergegeven. In dit voorbeeld vs2 is de virtuele sensor die moet worden verwijderd.



The screenshot shows the Cisco IPS Manager Express interface. The breadcrumb navigation is **Configuration > SFO-Sensor > Policies > IPS Policies**. The left sidebar shows a tree view with **IPS Policies** expanded. The main content area has a table of virtual sensors. The **Delete** button is highlighted in red. The row for **vs2** is also highlighted in red.

Name	Assigned Interfaces (or Pairs)	Signature Definition Policy
vs0	GigabitEthernet0/0.0 (Promiscuous Interface) GigabitEthernet0/1.20 (Inline VLAN Pair: 20<->40)	sig0
vs2	GigabitEthernet0/2.0 (Promiscuous Interface)	sig0

Event Action Rules "rules0" for virtual sensor "vs0,vs2"

Event Action Filters | IPv4 Target Value Rating | IPv6 Target Value Rating

Event Action Filters lets you **subtract** the actions associate with an event

+ Add | Edit | Delete | ↑ ↓

Name	Enabled	Sig ID	SubSig ID
Q00000	Yes	5450	0-255
Q00002	Yes	5081	0-255
Q00003	Yes	5450-5460	0-255

Dit voltooit het proces om een virtuele sensor te verwijderen. De virtuele sensor vs2 wordt verwijderd.



# Problemen oplossen

## IPS Manager Express lanceert niet

### Probleem

Wanneer een poging wordt gedaan om IPS via IME te bereiken, begint IPS Manager Express niet en wordt deze foutmelding ontvangen:

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

### Oplossing

Herladen van de IME-werkstation om dit op te lossen.

## Gerelateerde informatie

- [Categoriepagina voor Cisco-inbraakpreventiesysteem](#)
- [Ondersteuning van Cisco IPS Manager Express](#)
- [Network Time Protocol \(NTP\)](#)
- [Verzoeken om opmerkingen \(RFC's\)](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)