

IPS 6.X及更高版本 — 使用IME配置虛擬感測器

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[相關產品](#)

[慣例](#)

[背景資訊](#)

[關於分析引擎](#)

[關於虛擬感測器](#)

[虛擬化的優勢和限制](#)

[虛擬化的優勢](#)

[虛擬化的限制](#)

[虛擬化要求](#)

[設定](#)

[新增虛擬感測器](#)

[新增具有IME的虛擬感測器](#)

[編輯虛擬感測器](#)

[使用IME編輯虛擬感測器](#)

[刪除虛擬感測器](#)

[使用IME刪除虛擬感測器](#)

[疑難排解](#)

[IPS Manager Express未啟動](#)

[相關資訊](#)

簡介

本文檔介紹分析引擎的功能以及如何使用Cisco IPS Manager Express(IME)在Cisco Secure Intrusion Prevention System(IPS)上建立、編輯和刪除虛擬感測器。還說明了如何將介面分配給虛擬感測器。

注意： AIM-IPS和NME-IPS不支援虛擬化。

必要條件

需求

本文件沒有特定先決條件。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行軟體版本6.0及更高版本的Cisco 4200系列IPS裝置
- Cisco IPS Manager Express(IME)版本6.1.1及更高版本**注意**：IME可用於監控運行Cisco IPS 5.0及更高版本的感測器裝置，但只有運行Cisco IPS 6.1或更高版本的感測器才支援在IME中提供的一些新特性和功能。**注意**：Cisco Secure Intrusion Prevention System(IPS)5.x僅支援預設虛擬感測器vs0。IPS 6.x及更高版本支援預設虛擬感測器vs0以外的虛擬感測器。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

相關產品

此配置也可用於以下感測器：

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

慣例

請參閱[思科技術提示慣例](#)以瞭解更多有關文件慣例的資訊。

背景資訊

關於分析引擎

分析引擎執行資料包分析和警報檢測。它監控流經指定介面的流量。可以在分析引擎中建立虛擬感測器。每個虛擬感測器都有一個唯一的名稱，其中包含介面、內聯介面對、內聯VLAN對以及與其關聯的VLAN組的清單。為了避免定義排序問題，不允許分配中出現衝突或重疊。將介面、內聯介面對、內聯VLAN對和VLAN組分配給特定虛擬感測器，以便多個虛擬感測器不會處理任何資料包。每個虛擬感測器還與一個特別命名的特徵碼定義、事件操作規則和異常檢測配置相關聯。根據內聯旁路配置，丟棄來自介面、內聯介面對、內聯VLAN對以及未分配給任何虛擬感測器的VLAN組的資料包。

關於虛擬感測器

感測器可以接收來自一個或多個被監控的資料流的資料輸入。這些受監控的資料流可以是物理介面埠或虛擬介面埠。例如，單個感測器可以同時監控來自防火牆之前、防火牆之後或防火牆之前和之後的流量。並且單個感測器可以監視一個或多個資料流。在這種情況下，一個感測器策略或配置將應用於所有受監控的資料流。虛擬感測器是由一組配置策略定義的資料集合。虛擬感測器應用於由介面元件定義的一組資料包。虛擬感測器可以監視多個資料段，並且您可以為單個物理感測器中的每個虛擬感測器應用不同的策略或配置。您可以為正在分析的每個受監控段設定不同的策略。您還可以將相同的策略例項（例如sig0、rules0或ad0）應用到不同的虛擬感測器。您可以將介面、內聯介面對、內聯VLAN對和VLAN組分配給虛擬感測器。

注意：思科安全入侵防禦系統(IPS)不支援四個以上的虛擬感測器。預設虛擬感測器為vs0。您不能刪除預設虛擬感測器。介面清單、異常檢測操作模式、內聯TCP會話跟蹤模式和虛擬感測器描述是預設虛擬感測器可以更改的唯一配置功能。不能更改特徵碼定義、事件操作規則或異常檢測策略。

虛擬化的優勢和限制

虛擬化的優勢

虛擬化具有以下優勢：

- 您可以將不同的配置應用於不同的流量集。
- 您可以使用一個感測器監控具有重疊IP空間的兩個網路。
- 您可以監控防火牆或NAT裝置的內部和外部情況。

虛擬化的限制

虛擬化具有以下限制：

- 必須將非對稱通訊量的兩端分配給同一個虛擬感測器。
- VACL捕獲或SPAN (混雜監控) 的使用與VLAN標籤不一致，這會導致VLAN組問題。使用Cisco IOS軟體時，VACL擷取連線埠或SPAN目標不會一律接收已標籤的封包，即使已設定為主幹也是如此。使用MSFC時，學習路由的快速路徑交換會改變VACL捕獲和SPAN的行為。
- 持久儲存空間有限。

虛擬化要求

虛擬化具有以下流量捕獲要求：

- 虛擬感測器必須接收具有802.1q報頭的流量，捕獲埠的本徵VLAN上的流量除外。
- 對於任何給定感測器，感測器必須檢視位於同一虛擬感測器中同一VLAN組中的兩個通訊量方向。

設定

本節提供用於新增、編輯和刪除虛擬感測器的資訊。

新增虛擬感測器

在服務分析引擎子模式下發出[virtual-sensor name](#)命令，以建立虛擬感測器。將策略 (異常檢測、事件操作規則和特徵碼定義) 分配給虛擬感測器。然後將介面 (混雜、內聯介面對、內聯VLAN對和VLAN組) 分配給虛擬感測器。您必須先配置內聯介面對和VLAN對，然後才能將其分配給虛擬感測器。這些選項適用：

- **anomaly-detection** — 異常檢測引數。**anomaly-detection-name name** — 異常檢測策略的名稱
- **operational-mode** — 異常檢測模式(**inactive**、**learn**、**detect**)
- **description** — 虛擬感測器的說明
- **event-action-rules** — 事件操作規則策略的名稱

- **inline-TCP-evasion-protection-mode** — 用於選擇流量檢測所需的規範化器模式型別
： **asymmetric** — 只能看到雙向流量流的一個方向。非對稱模式保護會放鬆TCP層上的逃避保護。**注意**：非對稱模式允許感測器將狀態與流同步，並對不需要兩個方向的引擎進行維護檢查。非對稱模式降低了安全性，因為完全保護要求看到流量的兩端。**strict** — 如果由於任何原因丟失了資料包，則不會處理丟失資料包後的所有資料包。嚴格的逃避保護可全面實施TCP狀態和序列跟蹤。**注意**：任何順序錯誤的資料包或丟失的資料包都會產生Normalizer引擎簽名1300或1330發射，這會嘗試糾正這種情況，但可能會導致連線被拒絕。
- **inline-TCP-session-tracking-mode** — 允許識別內嵌流量中的重複TCP作業階段的進階方法。預設設定是虛擬感測器，幾乎總是最佳選擇。**virtual-sensor** — 虛擬感測器內具有相同會話金鑰(AaBb)的所有資料包都屬於同一會話。**interface-and-vlan** — 相同VLAN (或內嵌VLAN對)中且同一介面上具有相同作業階段金鑰(AaBb)的所有封包都屬於同一作業階段。對金鑰相同但位於不同VLAN或介面的資料包進行獨立跟蹤。**vlan-only** — 相同VLAN (或內聯VLAN對)中具有相同會話金鑰(AaBb)的所有資料包，無論介面是否屬於同一會話。對金鑰相同但位於不同VLAN的資料包進行獨立跟蹤。
- **signature-definition** — 簽名定義策略的名稱
- **logical-interfaces** — 邏輯介面的名稱 (內聯介面對)
- **physical-interfaces** — 物理介面的名稱 (混雜、內聯VLAN對和VLAN組) **subinterface-number** — 物理子介面編號。如果subinterface-type為none，則值0表示整個介面以混雜模式分配。**no** — 移除條目或選區

要新增虛擬感測器，請完成以下步驟：

1. 使用具有管理員許可權的帳戶登入到CLI。
2. 進入服務分析模式。

```
sensor# configure terminal
```

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

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

3. 新增虛擬感測器。

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

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

4. 新增此虛擬感測器的說明。

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

5. 為此虛擬感測器分配異常檢測策略和操作模式。

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

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

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

6. 為此虛擬感測器分配事件操作規則策略。

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

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

7. 為此虛擬感測器分配特徵碼定義策略。

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

8. 分配內聯TCP會話跟蹤模式。

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

預設設定為虛擬感測器模式，幾乎總是最佳選擇。

9. 分配內聯TCP規避保護模式。

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

預設值為嚴格模式，幾乎總是最佳選擇。

10. 顯示可用介面的清單。

```
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. 指定要新增到此虛擬感測器的混雜模式介面。

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

對要分配給此虛擬感測器的所有混雜介面重複此步驟。

12. 指定要新增到此虛擬感測器的內聯介面對。

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

您必須已經配對介面。

13. 分配要新增到此虛擬感測器的內聯VLAN對或組的子介面，如下所示：

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

您必須已經將任何介面細分為VLAN對或組。

14. 驗證虛擬感測器設定。

```
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. 退出分析引擎模式。

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

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

```
sensor(config)#
```

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

16. 按Enter以應用更改，或輸入no放棄更改。

此操作將完成向思科安全入侵防禦系統(IPS)新增虛擬感測器的過程。完成相同步驟以新增更多虛擬感測器。

注意：思科安全入侵防禦系統(IPS)不支援四個以上的虛擬感測器。預設虛擬感測器為vs0。

[新增具有IME的虛擬感測器](#)

完成以下步驟，以便使用Cisco IPS Manager Express在Cisco Secure Intrusion Prevention System(IPS)上配置虛擬感測器：

1. 選擇**Configuration > SFO-Sensor> Policies> IPS Policies**。然後，按一下**Add virtual sensor**，如螢幕截圖所示。

Configuration > SFO-Sensor > Policies > IPS Policies

SFO-Sensor

IPS Policies

Signature Definitions

- sig0
 - Active Signatures
 - Adware/Spyware
 - Attack
 - DDoS
 - DoS
 - Email
 - IOS IPS
 - Instant Messaging
 - L2/L3/L4 Protocol
 - Network Services
 - OS
 - Other Services
 - P2P
 - Reconnaissance
 - Releases
 - Viruses/Worms/Trojan
 - Web Server
 - All Signatures

Event Action Rules

- rules0

Anomaly Detections

- ad0

Sensor Setup

Interfaces

Policies

Sensor Management

+ Add Virtual Sensor Edit Delete

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

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

Event Action Filters IPv4 Target Value Rating IPv6 Target Value Rating OS Identif

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

+ Add Edit Delete ↑ ↓

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

- 為虛擬感測器命名（本例中為vs2），並在提供的空白處為虛擬感測器新增描述。還要指定要新增到此虛擬感測器的混雜模式介面。此處選擇了Gigabit Ethernet 0/2。現在，在**特徵碼定義**、**事件操作規則**、**異常檢測**和**高級選項**部分提供詳細資訊，如螢幕截圖所示。在**Advanced Options**下，提供有關TCP會話跟蹤模式和規範器模式的詳細資訊。這裡，**TCP會話跟蹤模式**是**virtual sensor**，而**Normalizer模式**是**Strict Evasion Protection**模式。

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

- 按一下「OK」(確定)。
- 新增的虛擬感測器vs2顯示在虛擬感測器清單中。按一下Apply，將新的虛擬感測器配置傳送到思科安全入侵防禦系統(IPS)。

The screenshot shows the SFO-Sensor configuration interface. The left sidebar displays a tree view of configuration options, including Signature Definitions, Event Action Rules, and Sensor Setup. The main area shows the configuration for a virtual sensor named 'vs2'. The sensor is assigned to the GigabitEthernet0/2.0 interface (Promiscuous Interface) and is associated with the 'sig0' signature definition policy. The risk rating is set to 'rules0 (3 action) HIGHRISK'. Below the sensor configuration, the 'Event Action Rules' section is visible, showing a table of rules for the virtual sensor 'vs0,vs2'.

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
vs2	GigabitEthernet0/2.0 (Promiscuous Interface)	sig0	rules0 (3 action) HIGHRISK

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

這將完成新增虛擬感測器的配置。

編輯虛擬感測器

可以編輯虛擬感測器的以下引數：

- 簽名定義策略
- 事件操作規則策略
- 異常檢測策略
- 異常檢測操作模式
- 內聯TCP會話跟蹤模式
- 說明
- 分配的介面

要編輯虛擬感測器，請完成以下步驟：

1. 使用具有管理員許可權的帳戶登入到CLI。
2. 進入服務分析模式。

```
sensor# configure terminal
```

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

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

3. 編輯虛擬感測器vs1。

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

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

4. 編輯此虛擬感測器的說明。

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

5. 更改分配給此虛擬感測器的異常檢測策略和操作模式。

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

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

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

6. 更改分配給此虛擬感測器的事件操作規則策略。

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

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

7. 更改分配給此虛擬感測器的特徵碼定義策略。

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

8. 更改內聯TCP會話跟蹤模式。

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

預設設定為虛擬感測器模式，幾乎總是最佳選擇。

9. 顯示可用介面的清單。

```
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. 更改分配給此虛擬感測器的混雜模式介面。

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

11. 更改分配給此虛擬感測器的內聯介面對。

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

您必須已經配對介面。

12. 使用分配給此虛擬感測器的內聯VLAN對或組更改子介面。

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

您必須已經將任何介面細分為VLAN對或組。

13. 驗證已編輯的虛擬感測器設定。

```
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. 退出分析引擎模式。

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

```
sensor(config)#
```

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

15. 按Enter以應用更改，或輸入no放棄更改。

[使用IME編輯虛擬感測器](#)

完成以下步驟，以便使用Cisco IPS Manager Express在Cisco Secure Intrusion Prevention System(IPS)上編輯虛擬感測器：

1. 選擇**Configuration > SFO-Sensor> Policies> IPS Policies**。
2. 選擇要編輯的虛擬感測器，然後按一下**Edit**，如螢幕截圖所示。在此示例中，vs2是要編輯的虛擬感測器。

File View Tools Help

Home Configuration Event Monitoring Reports Help

Configuration > SFO-Sensor > Policies > IPS Policies

SFO-Sensor

- IPS Policies
 - Signature Definitions
 - sig0
 - Event Action Rules
 - rules0
 - Anomaly Detections
 - Global Correlation
 - Inspection/Reputation
 - Network Participation

+ Add Virtual Sensor **Edit** Delete

Name	Assign to 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 ↑ ↓

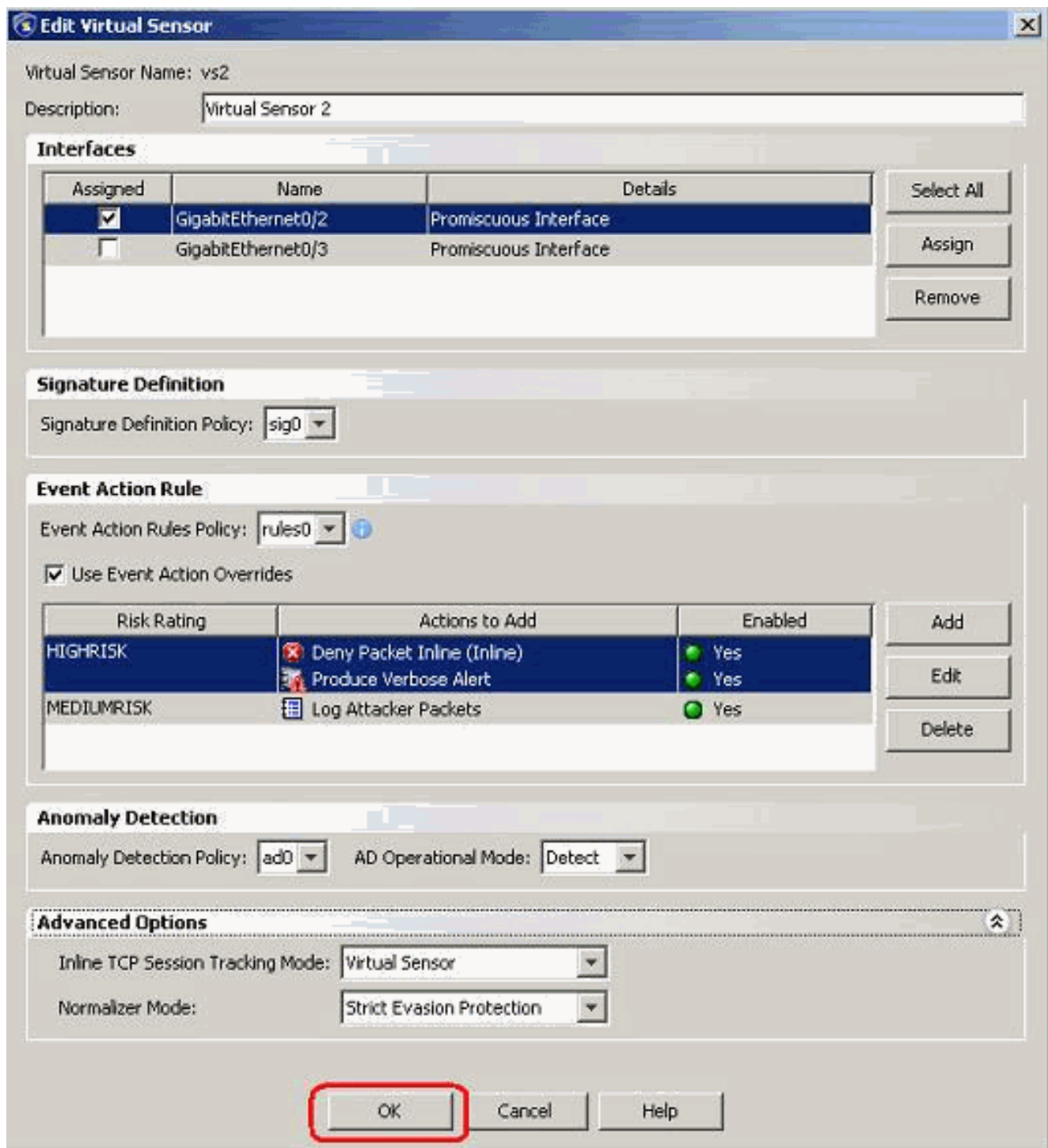
Name	Enabled	Sig ID	SubSig ID
Q00000	Yes	5450	0-255
Q00002	Yes	5081	0-255
Q00003	Yes	5450-5460	0-255

Sensor Setup

Interfaces

Policies

3. 在「編輯虛擬感測器」視窗中，對**特徵碼定義**、**Event Action Rule**、**Anomaly Detection**和**Advanced options**部分下存在的**虛擬感測器**引數進行更改。按一下「OK」，然後按一下「Apply」。



這將完成編輯虛擬感測器的過程。

刪除虛擬感測器

要刪除虛擬感測器，請完成以下步驟：

1. 要刪除虛擬感測器，請發出no virtual-sensor命令。

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

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

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

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

2. 驗證刪除的虛擬感測器。

```
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)#
```

只有預設虛擬感測器vs0存在。

3. 退出分析引擎模式。

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

```
sensor(config)#
```

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

使用IME刪除虛擬感測器

完成以下步驟，以便使用Cisco IPS Manager Express刪除思科安全入侵防禦系統(IPS)上的虛擬感測器：

1. 選擇Configuration > SFO-Sensor> Policies> IPS Policies。
2. 選擇要刪除的虛擬感測器，然後按一下Delete，如螢幕截圖所示。在此示例中，vs2是要刪除的虛擬感測器。

The screenshot shows the Cisco IPS Manager Express web interface. The breadcrumb navigation is Configuration > SFO-Sensor > Policies > IPS Policies. On the left, a tree view shows the configuration hierarchy. The main content area displays a table of virtual sensors. The 'Delete' button is highlighted with a red box. The row for 'vs2' is also highlighted with a red box. Below the table, there are tabs for 'Event Action Filters', 'IPv4 Target Value Rating', and 'IPv6 Target Value Rating'. The 'Event Action Filters' tab is active, showing a table of filters.

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

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

這將完成刪除虛擬感測器的過程。虛擬感測器vs2被刪除。

疑難排解

IPS Manager Express未啟動

問題

當嘗試通過IME訪問IPS時，IPS Manager Express不會啟動，並收到以下錯誤消息：

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

[解決方案](#)

為了解決此問題，請重新載入IME工作站PC。

[相關資訊](#)

- [思科入侵防禦系統支援頁面](#)
- [Cisco IPS管理員Express支援頁面](#)
- [網路時間協定\(NTP\)](#)
- [要求建議 \(RFC\)](#)
- [技術支援與文件 - Cisco Systems](#)