IPS 6.X和以后：带IME的虚拟传感器配置示例

目录

简介

本文解释分析引擎的功能和如何创建，编辑和删除在Cisco Secure入侵防御系统(IPS)的虚拟传感器与Cisco IPS Manager Express (IME)。它也解释分配如何建立接口到一个虚拟传感器。

注意： AIM-IPS和NME-IPS不支持虚拟化。

先决条件

要求

本文档没有任何特定的前提条件。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本6.0及以后的Cisco 4200系列IPS设备
- Cisco IPS Manager Express (IME)版本6.1.1和以上**注意：** 当IME可以用于监控运行思科IPS 5.0及以上版本的传感器设备时，传送的运行思科IPS 6.1或以上的传感器只支持某些新特性在IME和功能。**注意：** Cisco Secure入侵防御系统(IPS) 5.x支持仅默认虚拟传感器vs0。IPS 6.x支持除默认vs0之外的虚拟传感器和以后。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

相关产品

此配置可能也与这些传感器一起使用：

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

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

关于分析引擎

分析引擎进行数据包分析和警报检测。它监控流经指定的接口的流量。您在分析引擎方面创建虚拟传感器。每个虚拟传感器有与接口列表、轴向接口对、轴向VLAN对和VLAN组的一唯一的名称关联与它。为了避免定义排序问题，冲突或交叠在分配没有允许。您分配接口、轴向接口对、轴向VLAN对和VLAN组到一个特定虚拟传感器，以便数据包没有由超过一个虚拟传感器处理。每个虚拟传感器也关联与一个特别地已命名签名定义、事件操作规则和异常情况检测配置。从接口、轴向接口对、轴向VLAN没有分配到任何虚拟传感器的对和VLAN组的数据包被处理根据轴向旁路配置。

关于虚拟传感器

传感器能接收从一个或许多受监视数据流的数据输入。这些受监视数据流可以是物理接口端口或虚拟接口端口。例如，单个传感器能监控从在防火墙前面的流量，从防火墙的后面，或者从在和在防火墙后同时前面。并且单个传感器能监控一个或更多数据流。在这种情况下，单个传感器策略或配置应用对所有受监视数据流。一个虚拟传感器是由一套配置策略定义的搜集数据。虚拟传感器应用对一套数据包如定义由接口组件。一个虚拟传感器能监控多个网段，并且您能申请一不同的策略或配置在单个物理传感器内的每个虚拟传感器。您能设置一项不同的策略每受监视分段在分析下。您能也适用于同一个策略实例，例如， sig0、rules0或者ad0，不同的虚拟传感器。您能分配接口、轴向接口对、轴向VLAN对和VLAN组到一个虚拟传感器。

注意： Cisco Secure入侵防御系统(IPS)不支持超过四个虚拟传感器。默认虚拟传感器是vs0。您不能删除默认虚拟传感器。接口列表、异常情况检测操作模式、轴向TCP会话跟踪模式和虚拟传感器说明是您能为默认虚拟传感器更改的唯一的配置功能。您不能更改签名定义、事件操作规则或者异常情况检测策略。

虚拟化的优点和限制

虚拟化优点

虚拟化有这些优点：

- 您能运用不同的配置到不同的套流量。
- 您能监控两网络以交迭IP空间与一个传感器。
- 您能监控在防火墙或NAT设备内外。

虚拟化的限制

虚拟化有这些限制：

- 您必须分配不对称流量两边到同一个虚拟传感器。
- 使用VACL捕获或SPAN (混乱监听)是不一致关于VLAN标记，引起问题由于VLAN组。当您使用Cisco IOS软件时， VACL捕获端口或SPAN目标总是不收到标记信息包，即使为中继配置。当您使用MSFC时，获取的路由快速路径交换更改VACL捕获和SPAN行为。
- 不变存储被限制。

虚拟化需求

虚拟化有这些流量捕获需求：

- 虚拟传感器必须收到有802.1q报头的流量，除在捕获端口的本地VLAN的流量之外。
- 传感器在同一个VLAN组中必须为所有给的传感器发现流量两个方向同一个虚拟传感器的。

配置

在此部分，您提交与信息添加，编辑，并且删除虚拟传感器。

添加虚拟传感器

发出虚拟传感器name命令在服务分析引擎从属方式为了创建一个虚拟传感器。您分配策略(异常情况检测、事件操作规则和签名定义)到虚拟传感器。然后您分配接口(混乱，线型接口对、轴向VLAN对和VLAN组)到虚拟传感器。在您能分配他们到一个虚拟传感器前，您必须配置轴向接口对和VLAN对。这些选项适用：

- **异常情况检测**—异常情况检测参数。**异常情况检测NAME**命名—异常情况检测策略的名称**操作模式**—异常情况检测模式(**非激活，请学习，检测**)
- **说明**—虚拟传感器的说明
- **事件操作规则**—事件操作规则策略的名称

- **线型TCP躲避保护模式**—让规整器模式的类型您为流量检查需要的您选择：**不对称**—能只看到双向数据流运输流量的一个方向。不对称模式保护放松躲避保护在TCP层。**注意：** 不对称模式让传感器与流同步状态和维护不要求两个方向的那些引擎的检查。因为全双工保护要求将被看到的流量两边不对称模式降低安全。**严格**—如果数据包因故未命中，所有信息包，在未接数据包没有处理后。严格躲避保护提供TCP状态和顺序跟踪的全双工实施。**注意：** 所有无序信息包或未接数据包导致规整器引擎签名1300或1330生火，设法校正情况，但是能导致已拒绝连接。
- **线型TCP会话跟踪模式**—允许您识别轴向流量的重复的TCP会话的先进的方法。默认是虚拟传感器，几乎总是最好的选择。**虚拟传感器**—有同一会话密钥的(AaBb)所有信息包在一个虚拟传感器内属于同一会话。**接口和VLAN** —有同一会话密钥的(AaBb)所有信息包在同样VLAN (或轴向VLAN对)和在同一个接口属于同一会话。有同样的数据包锁上，但是在不同的VLAN或接口独立地被跟踪。**VLAN** —有同一会话密钥的(AaBb)所有信息包在同样VLAN (或轴向VLAN对)不管接口属于同一会话。有同样的数据包锁上，但是在不同的VLAN独立地被跟踪。
- **签名定义**—签名定义策略的名称
- **逻辑接口**—逻辑接口(轴向接口对)的名称
- **物理接口**—物理接口(混乱，线型VLAN对和VLAN组的)名称**子接口编号**—物理子接口号。如果子接口类型是无，值为0指示整个接口在混杂模式分配。**NO-**删除条目或选择

为了添加一个虚拟传感器，请完成这些步骤：

1. 登陆对与一个帐户的CLI与管理员权限。
2. 输入服务分析模式。`sensor# **configure terminal** sensor(config)# **service analysis-engine** sensor(config-ana)#`
3. 添加一个虚拟传感器。`sensor(config-ana)# **virtual-sensor vs2** sensor(config-ana-vir)#`
4. 添加此虚拟传感器的一说明。`sensor(config-ana-vir)# **description virtual sensor 2**`
5. 分配异常情况检测策略和操作模式到此虚拟传感器。`sensor(config-ana-vir)# **anomaly-detection** sensor(config-ana-vir-ano)# **anomaly-detection-name ad1** sensor(config-ana-vir-ano)# **operational-mode learn**`
6. 分配事件操作规则策略到此虚拟传感器。`sensor(config-ana-vir-ano)# exit`

   `sensor(config-ana-vir)# **event-action-rules rules1**`
7. 分配签名定义策略到此虚拟传感器。`sensor(config-ana-vir)# **signature-definition sig1**`
8. 分配轴向TCP会话跟踪模式。`sensor(config-ana-vir)# **inline-TCP-session-tracking-mode virtual-sensor** 默认是虚拟传感器模式，几乎总是最好的选择的选项。`
9. 分配轴向TCP躲避保护模式。`sensor(config-ana-vir)# **inline-TCP-evasion-protection-mode strict** 默认是严格模式，几乎总是最好的选择的选项。`
10. 显示可用的接口列表。`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. 分配混杂模式建立接口您想要添加到此虚拟传感器。`sensor(config-ana-vir)# **physical-interface GigabitEthernet0/2** 重复所有混乱接口的此步骤您想要分配到此虚拟传感器。`
12. 分配轴向接口配对您想要添加到此虚拟传感器。`sensor(config-ana-vir)# **logical-interface inline_interface_pair_name** 您一定已经配对接口。`
13. 分配轴向VLAN对的子接口或分组您想要添加到此虚拟传感器如下所示：`sensor(config-ana-vir)# **physical-interface GigabitEthernet2/0 subinterface-number subinterface_number** 您一定已经细分所有接口到VLAN对或组。`
14. 验证虚拟传感器设置。`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. 按回车为了应用更改或输入**不**丢弃他们。

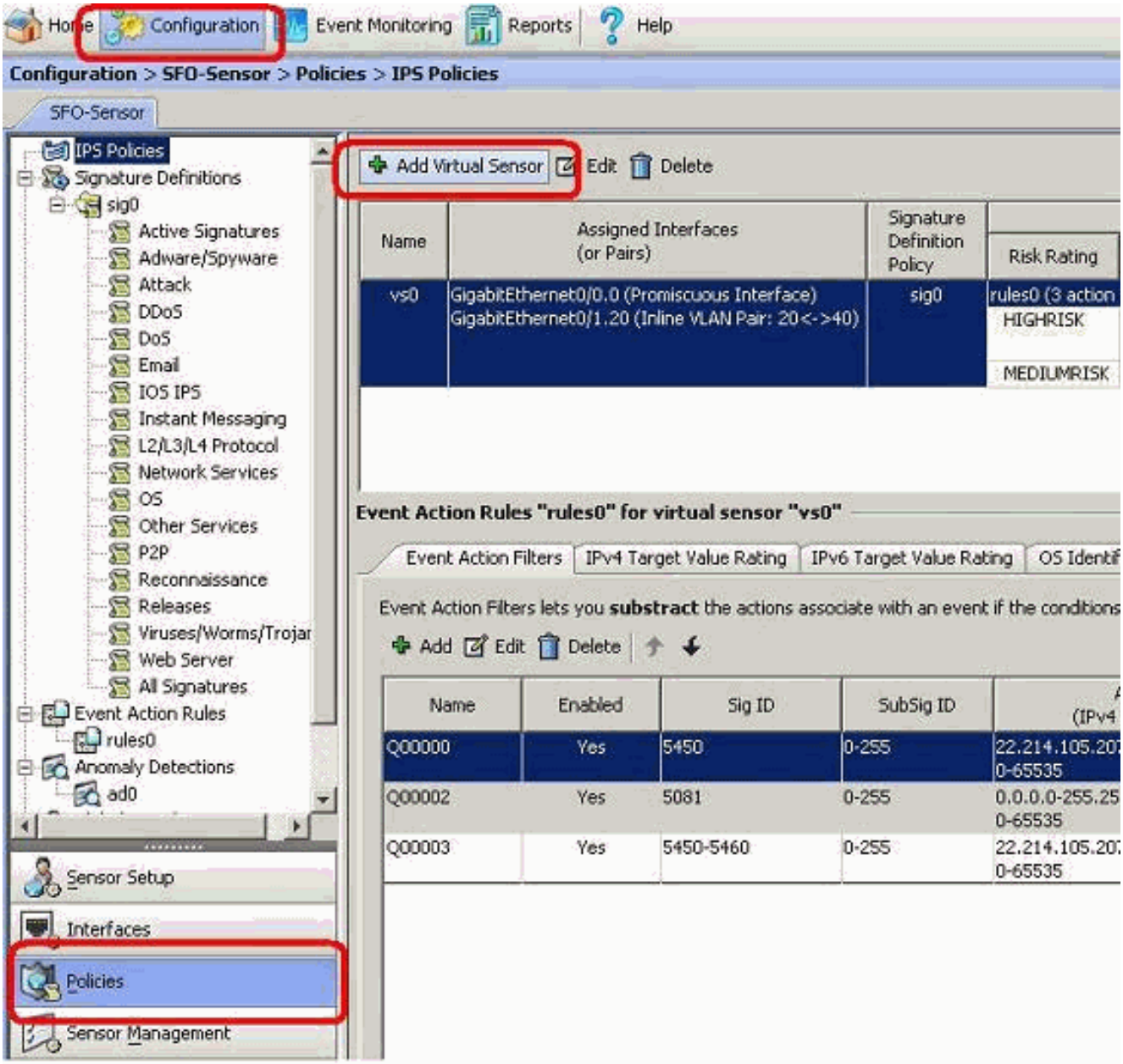
这完成进程添加一个虚拟传感器对Cisco Secure入侵防御系统(IPS)。完成同样步骤添加更加虚拟的传感器。

注意： Cisco Secure入侵防御系统(IPS)不支持超过四个虚拟传感器。默认虚拟传感器是vs0。

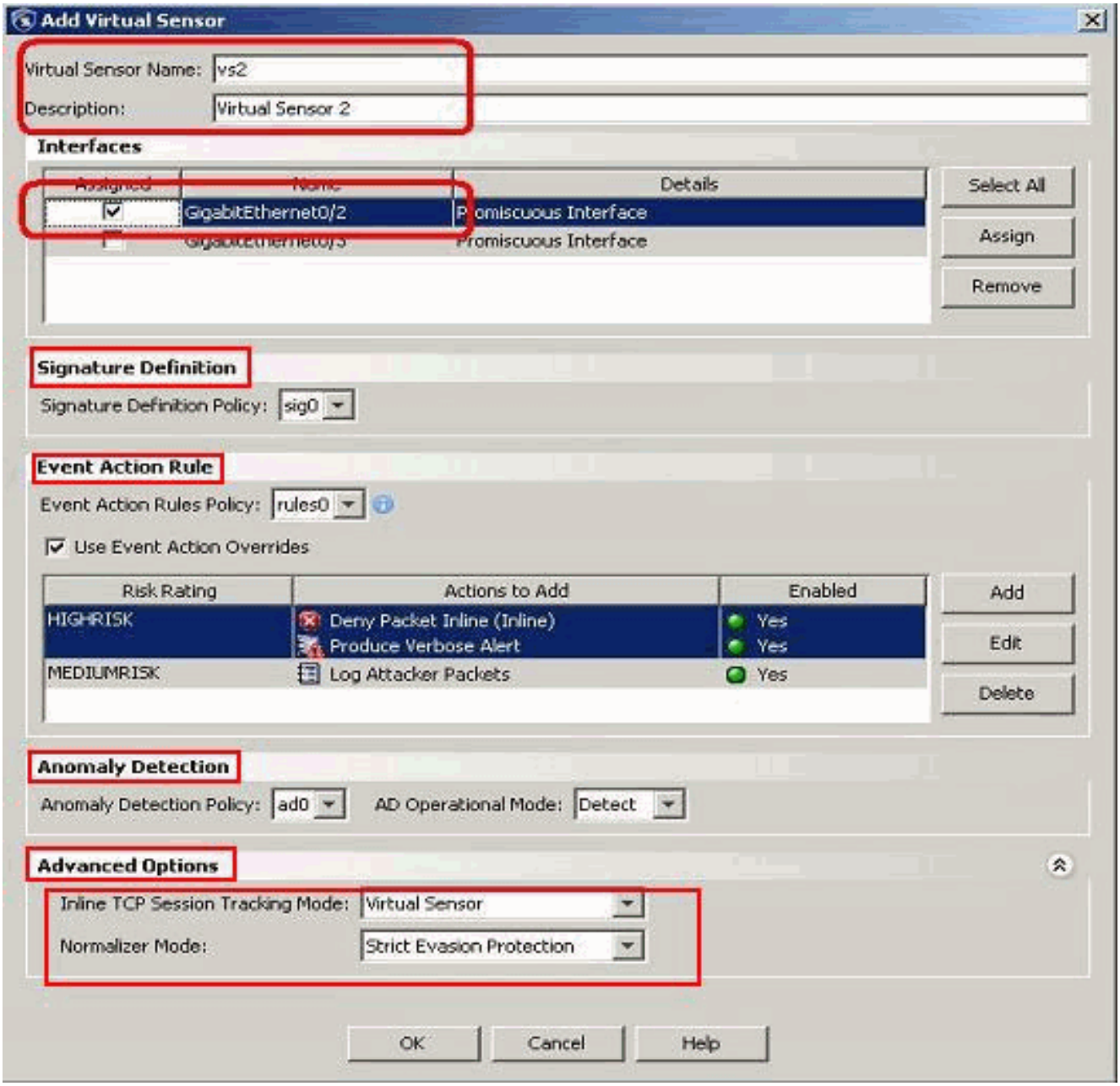
添加与IME的虚拟传感器

完成这些步骤为了配置在Cisco Secure入侵防御系统(IPS)的一个虚拟传感器与Cisco IPS Manager Express ：

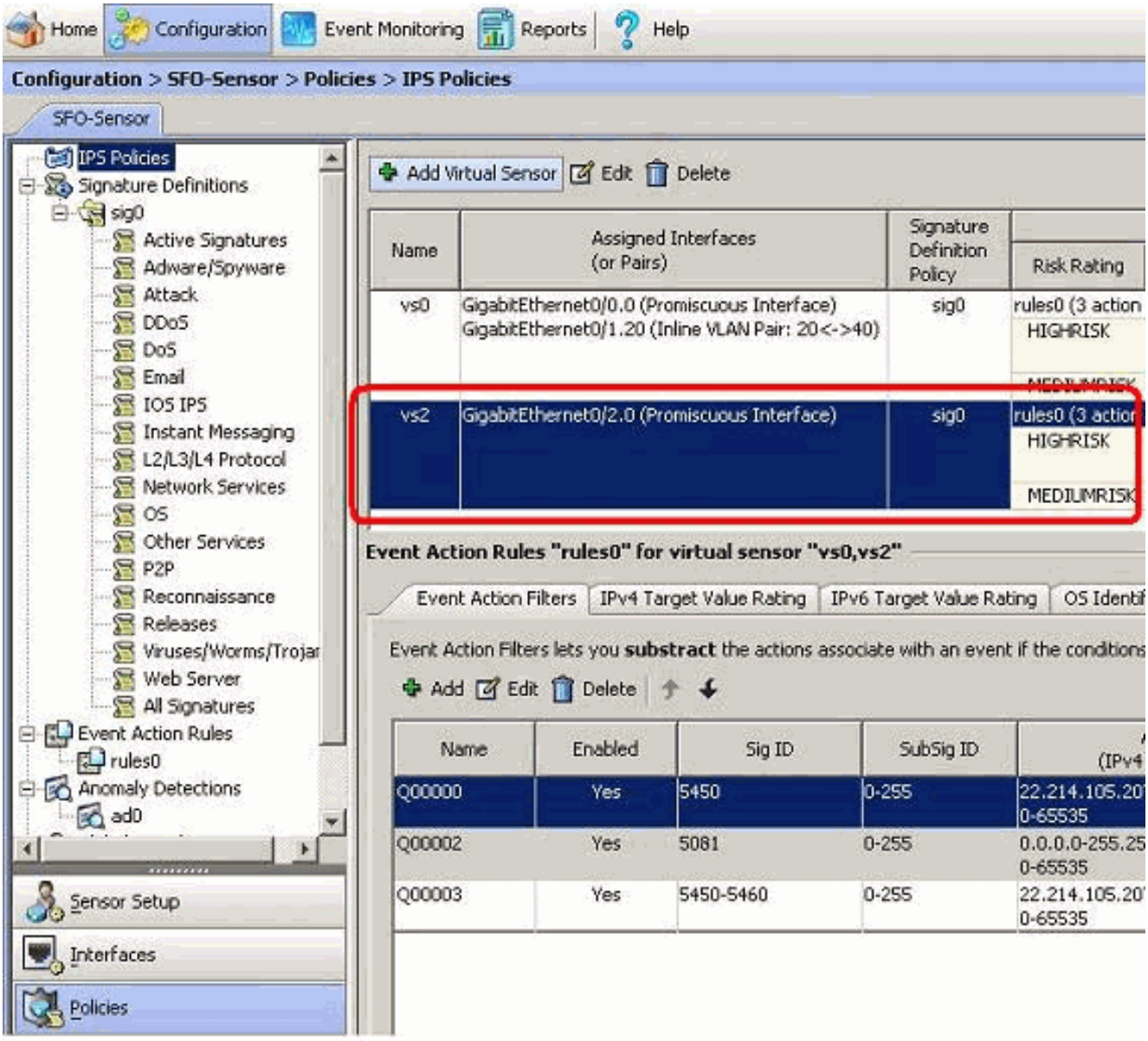
1. 选择**Configuration> SFO-Sensor> Policies> IPS策略**。然后，如屏幕画面所显示，请点击**Add虚拟传感器**。



2. 名叫虚拟传感器(在本例中的vs2)并且添加说明到在提供的空间的虚拟传感器。并且请分配混杂模式建立接口您想要添加到此虚拟传感器。千兆以太网0/2选择此处。如屏幕画面所显示，现在请提供在**签名定义**、**事件操作规则**、**异常情况检测**和**高级选项**部分的细节。在**高级选项下请**提供关于TCP会话跟踪模式和规整器模式的细节。在这里**TCP会话跟踪模式虚拟传感器，**并且**规整器模式**是**严格躲避保护**模式。



3. 单击 **Ok**。
4. 新加的虚拟传感器vs2在虚拟传感器列表显示。单击**申请**新的虚拟传感器配置将发送对Cisco Secure入侵防御系统(IPS)。



这完成配置添加一个虚拟传感器。

编辑虚拟传感器

一个虚拟传感器的这些参数可以编辑：

- 签名定义策略
- 事件操作规则策略
- 异常情况检测策略
- 异常情况检测操作模式
- 轴向TCP会话跟踪模式
- 说明
- 分配的接口

为了编辑一个虚拟传感器，请完成这些步骤：

1. 登陆对与一个帐户的CLI与管理员权限。
2. 输入服务分析模式。`sensor# **configure terminal** sensor(config)# **service analysis-engine** sensor(config-ana)#`
3. 编辑虚拟传感器， vs1。`sensor(config-ana)# **virtual-sensor vs2** sensor(config-ana-vir)#`
4. 编辑此虚拟传感器的说明。`sensor(config-ana-vir)# **description virtual sensor A**`

5. 更改异常情况检测策略和操作模式分配到此虚拟传感器。sensor(config-ana-vir)# anomaly-detection

   sensor(config-ana-vir-ano)# **anomaly-detection-name ad0** sensor(config-ana-vir-ano)# **operational-mode learn**
6. 更改事件操作规则策略分配到此虚拟传感器。sensor(config-ana-vir-ano)# exit

   sensor(config-ana-vir)# **event-action-rules rules0**
7. 更改签名定义策略分配到此虚拟传感器。sensor(config-ana-vir)# **signature-definition sig0**
8. 更改轴向TCP会话跟踪模式。sensor(config-ana-vir)# **inline-TCP-session-tracking-mode interface-and-vlan** 默认是虚拟传感器模式，几乎总是最好的选择的选项。
9. 显示可用的接口列表。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. 更改混杂模式接口分配到此虚拟传感器。sensor(config-ana-vir)# physical-interface GigabitEthernet0/2
11. 更改轴向接口对分配到此虚拟传感器。sensor(config-ana-vir)# **logical-interface inline_interface_pair_name** 您一定已经配对接口。
12. 更改与轴向VLAN对或组的子接口分配到此虚拟传感器。sensor(config-ana-vir)# physical-interface GigabitEthernet2/0 subinterface-number subinterface_number您一定已经细分所有接口到VLAN对或组。
13. 验证编辑的虚拟传感器设置。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

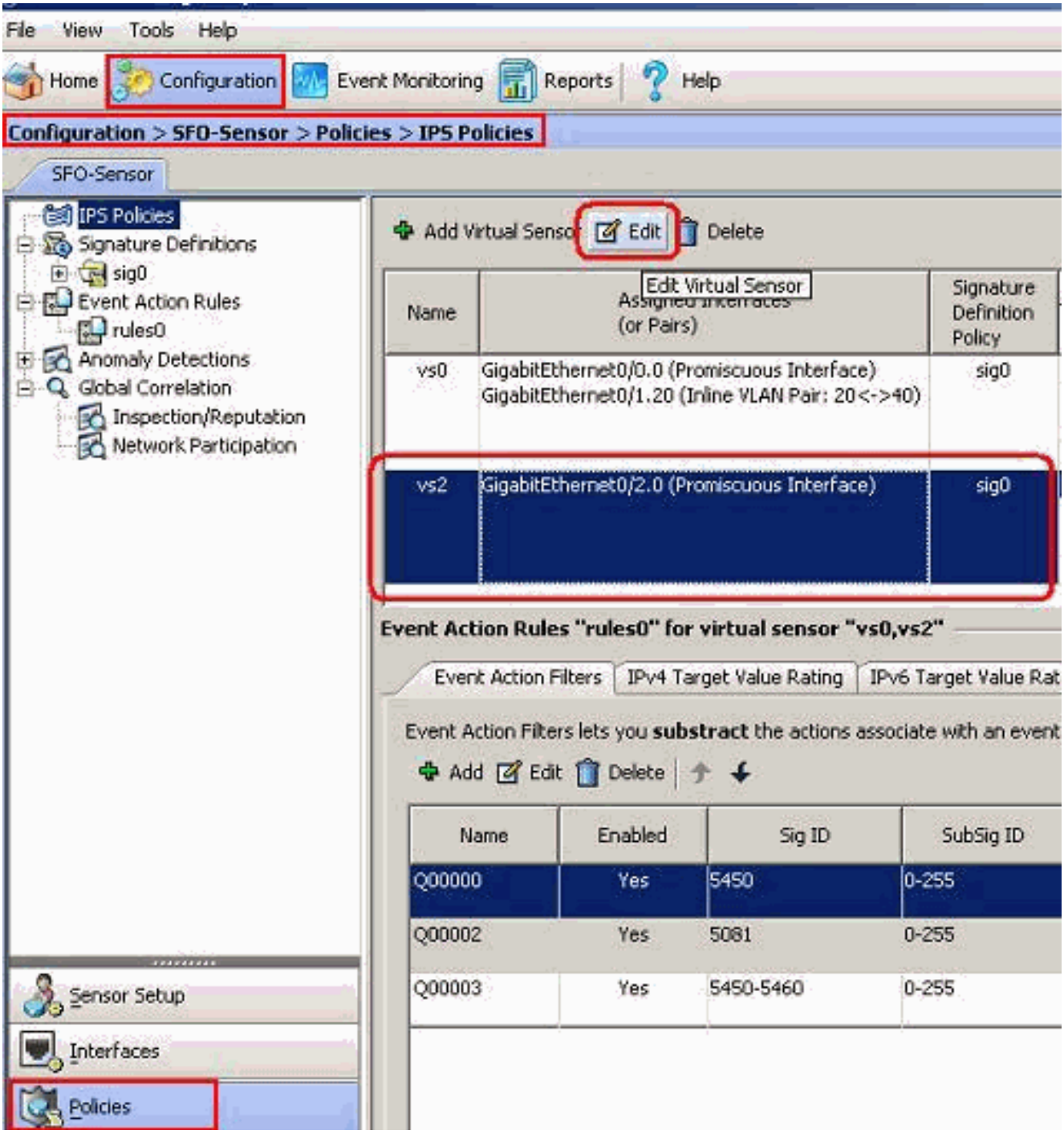
    sensor(config)#

    Apply Changes:?[yes]:
15. 按回车为了应用更改或输入**不**丢弃他们。

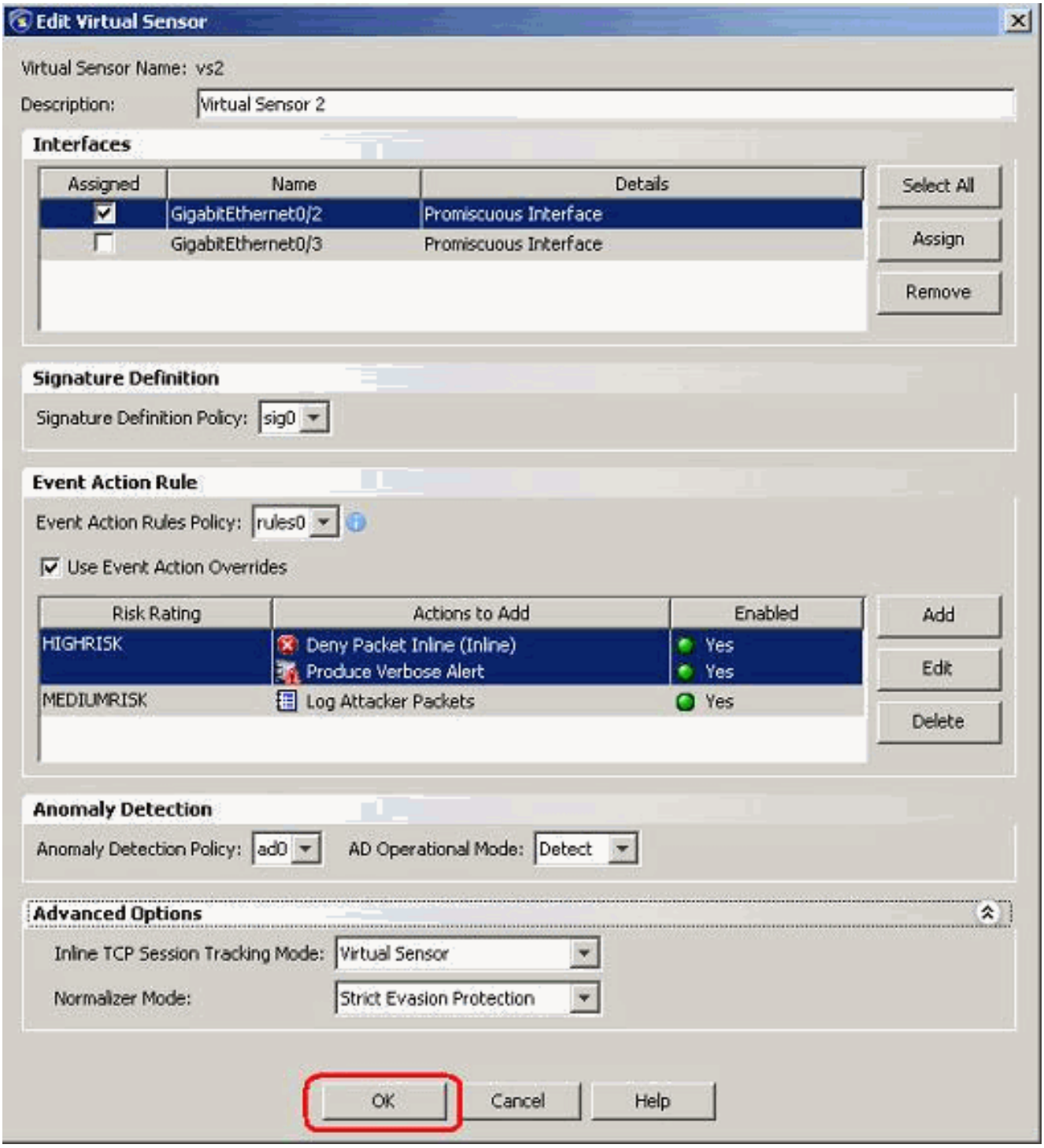
编辑与IME的虚拟传感器

完成这些步骤为了编辑在Cisco Secure入侵防御系统(IPS)的一个虚拟传感器与Cisco IPS Manager Express ：

1. 选择**Configuration> SFO-Sensor> Policies> IPS策略**。
2. 如屏幕画面所显示，选择将编辑的虚拟传感器，然后单击**编辑**。在本例中vs2是将编辑的虚拟传感器。



3. 在**编辑虚拟传感器**窗口，请做对参数的变动虚拟传感器的现在部分**签名定义**、**事件操作规则**、**异常情况检测**和**高级选项**下。单击 **OK**，然后单击 Apply。



这完成进程编辑一个虚拟传感器。

删除虚拟传感器

为了删除一个虚拟传感器，请完成这些步骤：

1. 为了删除一个虚拟传感器，请勿发出**虚拟传感器**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. 验证删除的虚拟传感器。`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)# 仅默认虚拟传感器， **vs0**，存在。

3. 退出分析引擎模式。sensor(config-ana)# exit

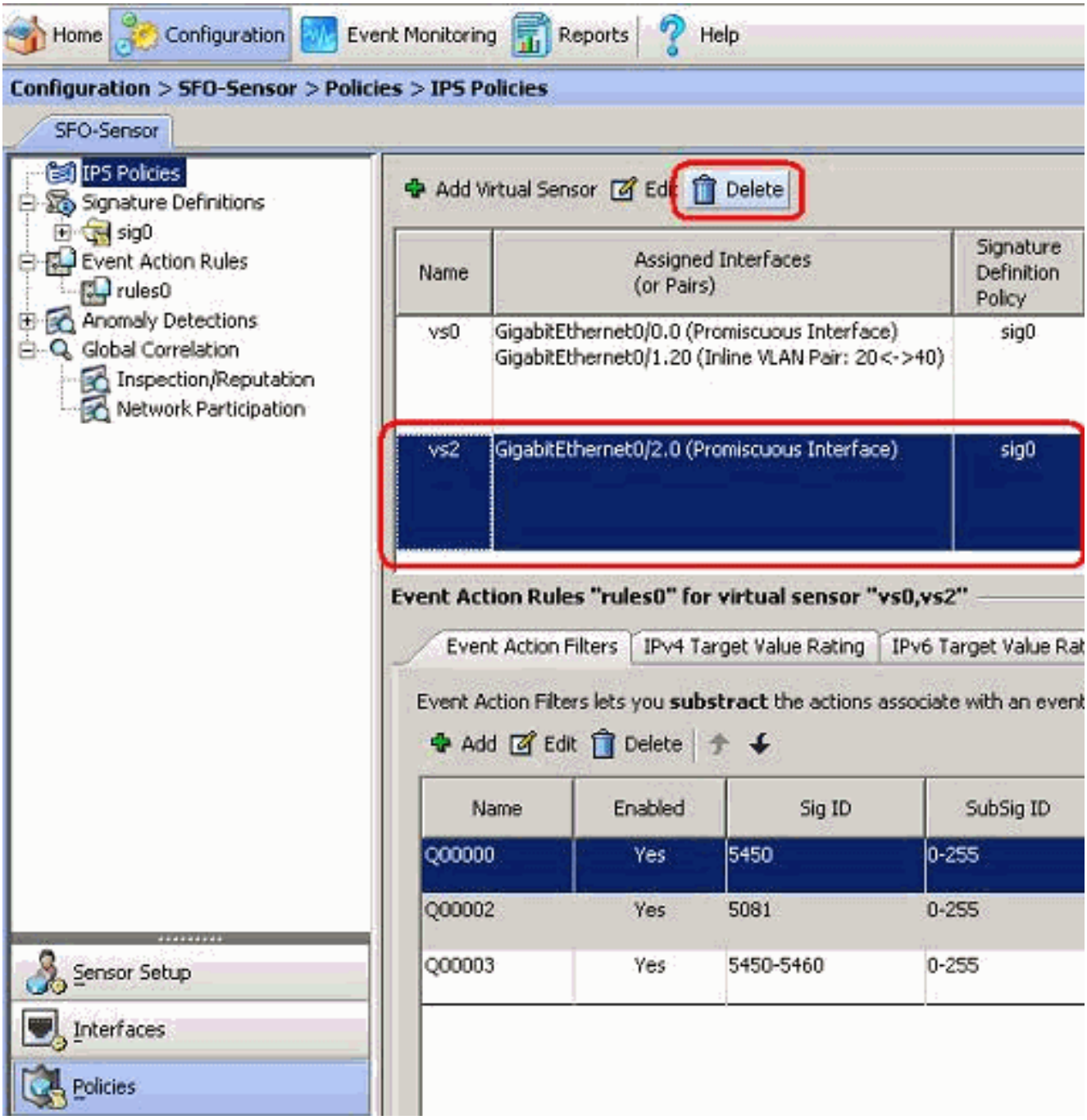
```
sensor(config)#
Apply Changes:?[yes]:
```

与IME的删除虚拟传感器

完成此步骤为了删除在Cisco Secure入侵防御系统(IPS)的一个虚拟传感器与Cisco IPS Manager Express ：

1. 选择**Configuration> SFO-Sensor> Policies> IPS策略**。
2. 如屏幕画面所显示，选择将删除的虚拟传感器，然后单击**删除**。在本例中vs2是将删除的虚拟

传感器。



这完成进程删除一个虚拟传感器。虚拟传感器vs2删除。

故障排除

IPS管理器Express不启动

问题

当尝试做出通过IME时访问IPS， IPS管理器Express不开始，并且此错误消息接收：

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

解决方案

为了解决此，请重新加载IME工作站PC。

相关信息

- Cisco 入侵防御系统支持页
- Cisco IPS Manager Express支持页面
- 网络时间协议 (NTP)
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems