IPS 6. X и позже: Действительные Датчики с Примером конфигурации IME

Содержание

Введение

Этот документ объясняет функцию Аналитического Механизма и как создать, отредактировать, и удалить действительные датчики на Системе предотвращения вторжений (IPS) Cisco Secure с Cisco IPS Manager Express (IME). Это также объясняет, как назначить интерфейсы на действительный датчик.

Примечание: IPS AIM и IPS NME не поддерживают виртуализацию.

Предварительные условия

Требования

Для данного документа отсутствуют предварительные условия.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Устройство IPS Cisco серии 4200, которое работает под управлением ПО версии 6.0 и позже
- Cisco IPS Manager Express (IME) версия 6.1.1 и позже**Примечание:** В то время как IME может использоваться к устройствам контрольного датчика, которые выполняют Cisco IPS 5.0 и позже, некоторые новые характеристики и функциональность, отправленная в IME, только поддерживаются на датчиках, которые выполняют Cisco IPS 6.1 или позже.**Примечание:** Система предотвращения вторжений (IPS) Cisco Secure 5.x поддерживает только действительный датчик по умолчанию vs0. Действительные датчики кроме по умолчанию vs0 поддерживаются в IPS 6.x и позже.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Родственные продукты

Эта конфигурация может также использоваться с этими датчиками:

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

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Общие сведения

Об аналитическом механизме

Аналитический Механизм выполняет пакетный анализ и аварийное обнаружение. Это контролирует трафик, который течет через заданные интерфейсы. Вы создаете действительные датчики в Аналитическом Механизме. Каждый действительный датчик имеет уникальное имя со списком интерфейсов, встроенных интерфейсных пар, встроенных пар VLAN и Групп VLAN, привязанных к нему. Во избежание определения, упорядочивая проблемы, никакие конфликты или наложения не позволены в присвоениях. Вы назначаете интерфейсы, встраиваете интерфейсных пар, встраиваете пар VLAN и Группы VLAN к определенному действительному датчику так, чтобы никакой пакет не был обработан

несколькими действительными датчиками. Каждый действительный датчик также привязан к в частности именованному определению подписи, правилам действия события и конфигурации обнаружения отклонения. Пакеты от интерфейсов, встройте интерфейсных пар, от встроенных пар VLAN и Групп VLAN, которые не назначены ни на какой действительный датчик, избавляются на основе встроенной обходной конфигурации.

О действительных датчиках

Датчик может получить входные данные от одного или нескольких отслеживаемых потоков данных. Эти отслеживаемые потоки данных могут или быть портами физического интерфейса или портами виртуального интерфейса. Например, одиночный датчик может контролировать трафик от перед межсетевым экраном из-за межсетевого экрана, или от перед и позади межсетевого экрана одновременно. И одиночный датчик может контролировать один или несколько потоков данных. В этой ситуации, одиночной политике датчика или конфигурации применен ко всем отслеживаемым потокам данных. Действительный датчик является набором данных, который определен рядом политики конфигурации. Действительный датчик применен к ряду пакетов, как определено интерфейсным компонентом. Действительный датчик может контролировать множественные сегменты, и можно применить другую политику или конфигурацию для каждого действительного датчика в одиночном физическом датчике. Можно установить другую политику на отслеживаемый сегмент при анализе. Можно также применить тот же экземпляр политики, например, sig0, rules0, или ad0, к другим действительным датчикам. Можно назначить интерфейсы, встроенных интерфейсных пар, встроенных пар VLAN и Группы VLAN к действительному датчику.

Примечание: Система предотвращения вторжений (IPS) Cisco Secure не поддерживает больше чем четыре действительных датчика. Действительный датчик по умолчанию является vs0. Вы не можете удалить действительный датчик по умолчанию. Список интерфейсов, операционный режим обнаружения отклонения, встроенный режим отслеживания сеанса TCP и действительное описание датчика являются единственными функциями конфигурации, которые можно изменить для действительного датчика по умолчанию. Вы не можете изменить определение подписи, правила действия события или политику обнаружения отклонения.

Преимущества и ограничения виртуализации

Преимущества виртуализации

Виртуализация имеет эти преимущества:

- Можно применить другие конфигурации к другим наборам трафика.
- Можно контролировать две сети с перекрывающимися пробелами IP с одним датчиком.
- Можно контролировать и внутри и снаружи межсетевого экрана или устройства NAT.

Ограничения виртуализации

Виртуализация имеет эти ограничения:

- Необходимо назначить обе стороны асимметричного трафика к тому же действительному датчику.

- Использование перехвата VACL или SPAN (разнородный мониторинг) противоречиво относительно маркирования VLAN, которое вызывает проблемы с Группами VLAN.При использовании программного обеспечения Cisco IOS порт перехвата VACL или цель SPAN не всегда получают маркированные тегами пакеты, даже если это настроено для транкинга.При использовании MSFC коммутация быстрого маршрута полученных маршрутов изменяет поведение перехватов VACL и SPAN.
- Персистентное хранилище ограничено.

Требования виртуализации

Виртуализация имеет эти требования перехвата трафика:

- Действительный датчик должен получить трафик, который имеет 802.1q заголовки кроме трафика на собственном VLAN порта перехвата.
- Датчик должен видеть оба направления трафика в той же Группе VLAN в том же действительном датчике для любого данного датчика.

Настройка

В этом разделе вам предоставляют информацию, чтобы добавить, отредактировать, и удалить действительные датчики.

Добавьте действительные датчики

Выполните команду названия действительного датчика в обслуживании аналитический подрежим механизма для создания действительного датчика. Вы назначаете политику (обнаружение отклонения, правила действия события и определение подписи) к действительному датчику. Затем вы назначаете интерфейсы (разнородные, встроенные интерфейсные пары, встройте пар VLAN и Группы VLAN) к действительному датчику. Необходимо настроить встроенных интерфейсных пар и пар VLAN, прежде чем можно будет назначить их на действительный датчик. Эти опции применяются:

- **обнаружение отклонения** — параметры Обнаружения отклонения.название **названия обнаружения отклонения** — Название политики обнаружения отклонения**операционный режим** — режим Обнаружения отклонения (**неактивный, изучите, обнаружьте**),
- **описание** действительного датчика
- **правила event-action** — Название действия события управляет политикой
- **inline-TCP-evasion-protection-mode** — Позволяет вам выбрать, в каком типе режима Нормализатора вы нуждаетесь для контроля трафика:**асимметричный** — Может только видеть одно направление потока двунаправленного трафика. Асимметричная защита режима ослабляет защиту уклонения на уровне TCP.**Примечание:** Асимметричный режим позволяет датчику синхронизировать состояние с потоком и поддержать контроль для тех механизмов, которые не требуют обоих направлений. Асимметричный режим понижает безопасность, потому что полная защита требует, чтобы были замечены обе стороны трафика.**строгий** — Если пакет пропущен по какой-либо причине, все пакеты после того, как пропущенный пакет не обработан. Строгая защита уклонения предоставляет полное осуществление отслеживания последовательности и состояния TCP.**Примечание:** Любые поврежденные пакеты или пропущенные пакеты могут

произвести взрывы подписей 1300 или 1330 механизма Нормализатора, которые пытаются исправить ситуацию, но могут привести к запрещенным соединениям.

- **inline-TCP-session-tracking-mode** — Передовой метод, который позволяет вам определять двойной сеанс TCP во встроенном трафике. По умолчанию является действительным датчиком, который является почти всегда лучшим выбором.**действительный датчик** — Все пакеты с тем же ключом сеанса (AaBb) в действительном датчике принадлежат тому же сеансу.**интерфейс-и-vlan** — Все пакеты с тем же ключом сеанса (AaBb) в той же VLAN (или встроенная пара VLAN) и на том же интерфейсе принадлежат тому же сеансу. Пакеты с тем же ключом, но на других VLAN или интерфейсах отслежены независимо.**только для vlan** — Все пакеты с тем же ключом сеанса (AaBb) в той же VLAN (или встроенная пара VLAN) независимо от интерфейса принадлежат тому же сеансу. Пакеты с тем же ключом, но на других VLAN отслежены независимо.
- **определение подписи** — Название политики определения подписи
- **логические интерфейсы** — Название логических интерфейсов (встраивают интерфейсных пар),
- **физические интерфейсы** — Название физических интерфейсов (разнородные, встроенные пары VLAN и Группы VLAN)**номер подинтерфейса** — физический номер подинтерфейса. Если тип подинтерфейса не ни один, значение 0 указывает, что весь интерфейс назначен в случайном режиме.**нет** — Удаляет запись или выбор

Для добавления действительного датчика выполните эти шаги:

1. Войдите к CLI с учетной записью с администраторскими привилегиями.
2. Поступите в эксплуатацию аналитический режим.`sensor# **configure terminal** sensor(config)# **service analysis-engine** sensor(config-ana)#`
3. Добавьте действительный датчик.`sensor(config-ana)# **virtual-sensor vs2** sensor(config-ana-vir)#`
4. Добавьте описание для этого действительного датчика.`sensor(config-ana-vir)# **description virtual sensor 2**`
5. Назначьте политику обнаружения отклонения и операционный режим к этому действительному датчику.`sensor(config-ana-vir)# **anomaly-detection** sensor(config-ana-vir-ano)# **anomaly-detection-name ad1** sensor(config-ana-vir-ano)# **operational-mode learn**`
6. Назначьте политику правил действия события на этот действительный датчик.`sensor(config-ana-vir-ano)# exit`

   `sensor(config-ana-vir)# **event-action-rules rules1**`
7. Назначьте политику определения подписи на этот действительный датчик.`sensor(config-ana-vir)# **signature-definition sig1**`
8. Назначьте встроенный режим отслеживания сеанса TCP.`sensor(config-ana-vir)# **inline-TCP-session-tracking-mode virtual-sensor**` По умолчанию является действительным режимом датчика, который является почти всегда наилучшим вариантом выбрать.
9. Назначьте встроенный режим защиты уклонения TCP.`sensor(config-ana-vir)# **inline-TCP-evasion-protection-mode strict**` По умолчанию является строгим режимом, который является почти всегда наилучшим вариантом выбрать.
10. Отобразите список доступных интерфейсов.`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. Назначьте интерфейсы случайного режима, которые вы хотите добавить к этому действительному датчику.`sensor(config-ana-vir)# physical-interface GigabitEthernet0/2` Повторите этот шаг для всех разнородных интерфейсов, которые вы хотите назначить на этот действительный датчик.
12. Назначьте встроенных интерфейсных пар, которых вы хотите добавить к этому действительному датчику.`sensor(config-ana-vir)# logical-interface inline_interface_pair_name` Вы, должно быть, уже соединили интерфейсы.
13. Назначьте подинтерфейсы встроенных пар VLAN или групп, которые вы хотите добавить к этому действительному датчику как показано ниже:`sensor(config-ana-vir)# physical-interface GigabitEthernet2/0 subinterface-number subinterface_number` Вы, должно быть, уже подразделили любые интерфейсы на пар VLAN или группы.
14. Проверьте действительные параметры настройки датчика.`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. Выходной аналитический режим механизма.`sensor(config-ana-vir)# exit sensor(config-ana)# exit sensor(config)# Apply Changes:?[yes]:`
16. Нажмите **Enter**, чтобы применить изменения или войти **не** для отмены от них.

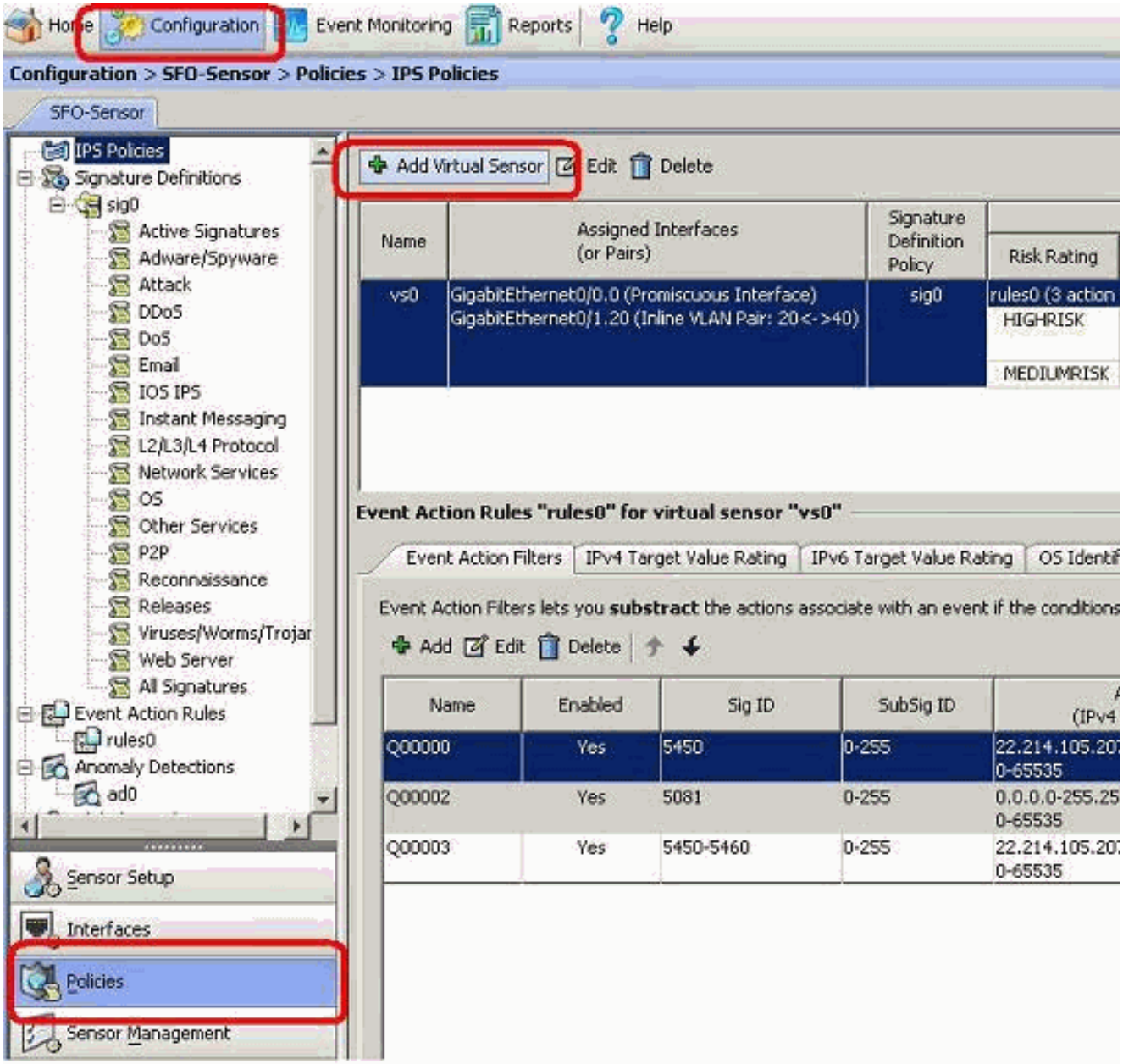
Это завершает процесс для добавления Действительного датчика к Системе предотвращения вторжений (IPS) Cisco Secure. Завершите ту же процедуру для добавления большего количества действительных датчиков.

Примечание: Система предотвращения вторжений (IPS) Cisco Secure не поддерживает больше чем четыре действительных датчика. Действительный датчик по умолчанию является vs0.

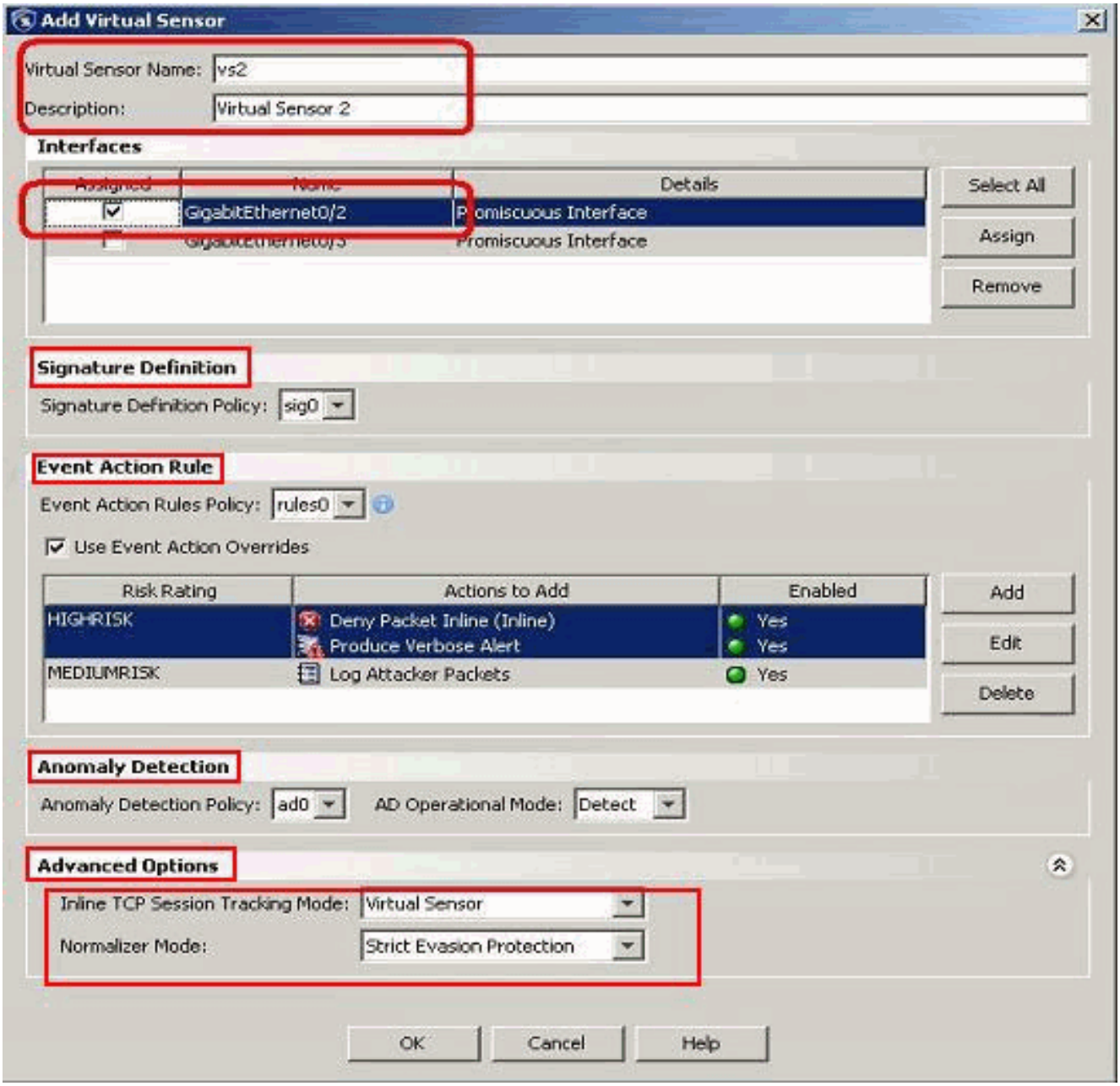
Добавьте действительный датчик с IME

Выполните эти шаги для настройки действительного датчика на Системе предотвращения вторжений (IPS) Cisco Secure с Cisco IPS Manager Express:

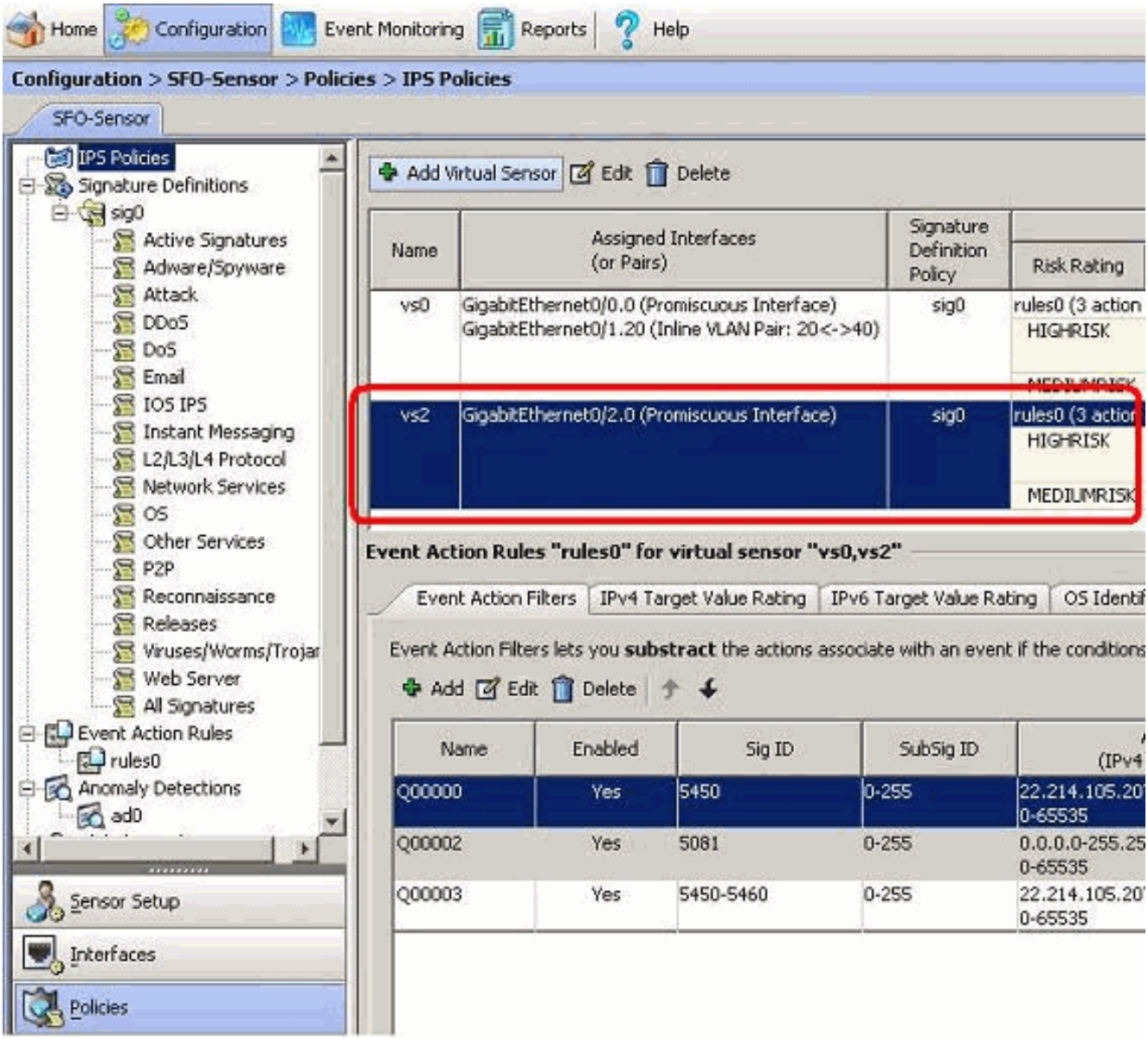
1. Выберите **Configuration> SFO-Sensor> Policies> IPS Policies**. Затем щелкните **по Add действительный датчик** как показано в снимке экрана.



2. Назовите действительный датчик (vs2 в данном примере) и добавьте описание к действительному датчику в предоставленном пространстве. Также назначьте интерфейсы случайного режима, которые вы хотите добавить к этому действительному датчику. Гигабитный Ethernet 0/2 выбран здесь. Теперь предоставьте подробную информацию в **определении подписи**, **Правиле Действия События**, **Обнаружении отклонения** и разделах **Расширенных настроек** как показано в снимке экрана.Под **Расширенными настройками** предоставляют подробную информацию о Режиме отслеживания Сеанса TCP и Режиме Нормализатора. Здесь **Режим отслеживания Сеанса TCP** является **действительным датчиком**, и **режим Нормализатора** является **Строгим Режимом защиты Уклонения**.



3. **Нажмите кнопку OK.**
4. Недавно добавленный действительный датчик vs2 показывают в списке действительных датчиков. Нажмите **Apply** для новой действительной конфигурации сенсора, которая будет передаваться Системе предотвращения вторжений (IPS) Cisco Secure.



Это завершает конфигурацию для добавления действительного датчика.

Отредактируйте действительные датчики

Эти параметры действительного датчика могут быть отредактированы:

- Политика определения подписи
- Действие события управляет политикой
- Политика обнаружения отклонения
- Операционный режим обнаружения отклонения
- Встроенный режим отслеживания сеанса TCP
- Описание
- Интерфейсы назначены

Для редактирования действительного датчика выполните эти шаги:

1. Войдите к CLI с учетной записью с администраторскими привилегиями.
2. Поступите в эксплуатацию аналитический режим.`sensor# configure terminal`
   `sensor(config)# service analysis-engine sensor(config-ana)#`
3. Отредактируйте действительный датчик, vs1.`sensor(config-ana)# virtual-sensor vs2`
   `sensor(config-ana-vir)#`

4. Отредактируйте описание этого действительного датчика.`sensor(config-ana-vir)# **description virtual sensor A**`
5. Измените политику обнаружения отклонения и операционный режим, назначенный на этот действительный датчик.`sensor(config-ana-vir)# anomaly-detection`

   `sensor(config-ana-vir-ano)# **anomaly-detection-name ad0** sensor(config-ana-vir-ano)# **operational-mode learn**`
6. Измените правила действия события, заданные политикой на этот действительный датчик.`sensor(config-ana-vir-ano)# exit`

   `sensor(config-ana-vir)# **event-action-rules rules0**`
7. Измените определение подписи, заданное политикой на этот действительный датчик.`sensor(config-ana-vir)# **signature-definition sig0**`
8. Измените встроенный режим отслеживания сеанса TCP.`sensor(config-ana-vir)# **inline-TCP-session-tracking-mode interface-and-vlan**` По умолчанию является действительным режимом датчика, который является почти всегда наилучшим вариантом выбрать.
9. Отобразите список доступных интерфейсов.`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. Измените интерфейсы случайного режима, назначенные на этот действительный датчик.`sensor(config-ana-vir)# physical-interface GigabitEthernet0/2`
11. Измените встроенных интерфейсных пар, назначенных на этот действительный датчик.`sensor(config-ana-vir)# **logical-interface inline_interface_pair_name**` Вы, должно быть, уже соединили интерфейсы.
12. Измените подинтерфейс со встроенными парами VLAN или группами, назначенными на этот действительный датчик.`sensor(config-ana-vir)# physical-interface GigabitEthernet2/0 subinterface-number subinterface_number`Вы, должно быть, уже подразделили любые интерфейсы на пар VLAN или группы.
13. Проверьте отредактированные действительные параметры настройки датчика.`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. Выходной аналитический режим механизма.`sensor(config-ana)# exit`

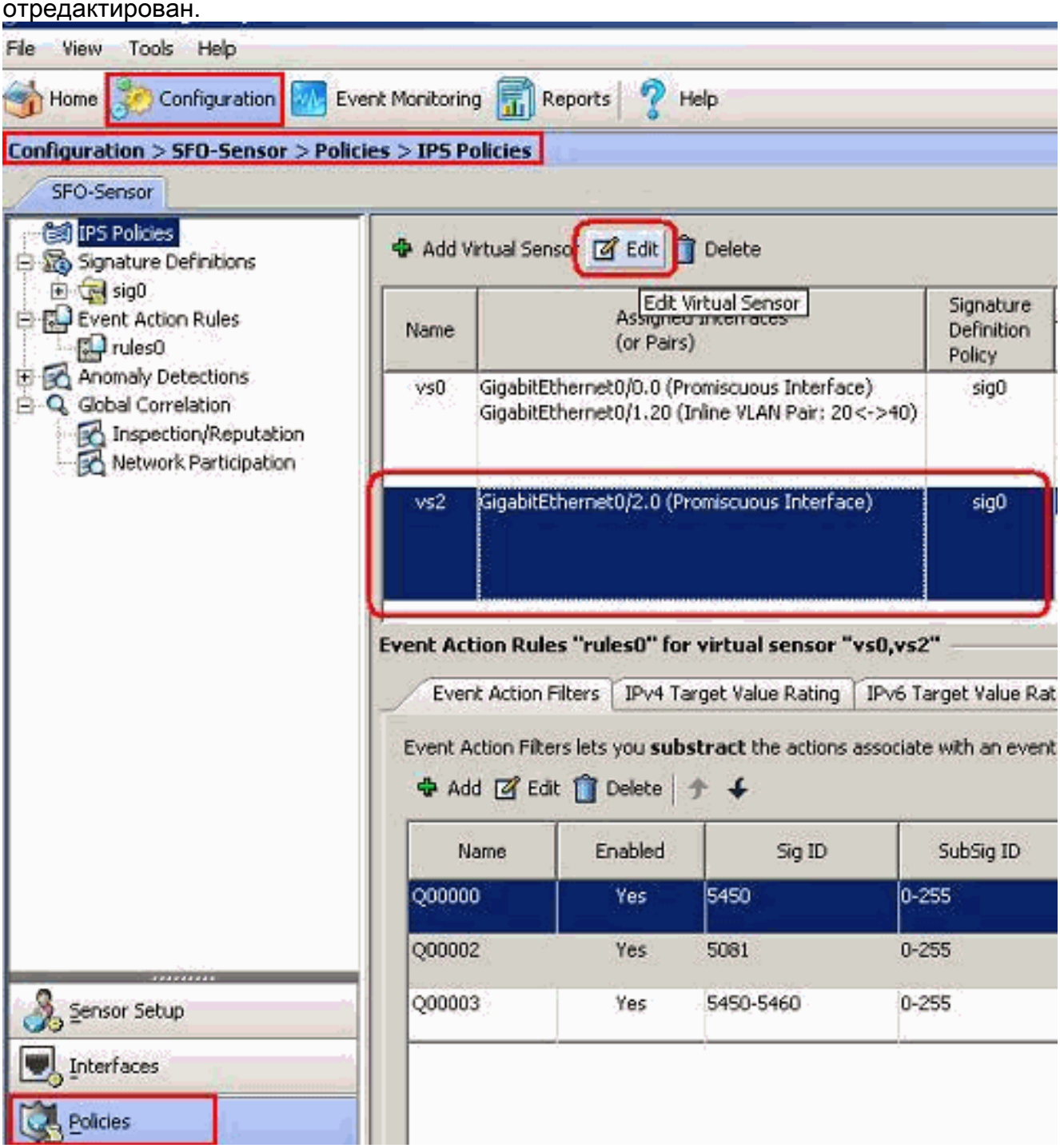
    `sensor(config)#`

    `Apply Changes:?[yes]:`
15. Нажмите **Enter**, чтобы применить изменения или войти **не** для отмены от них.

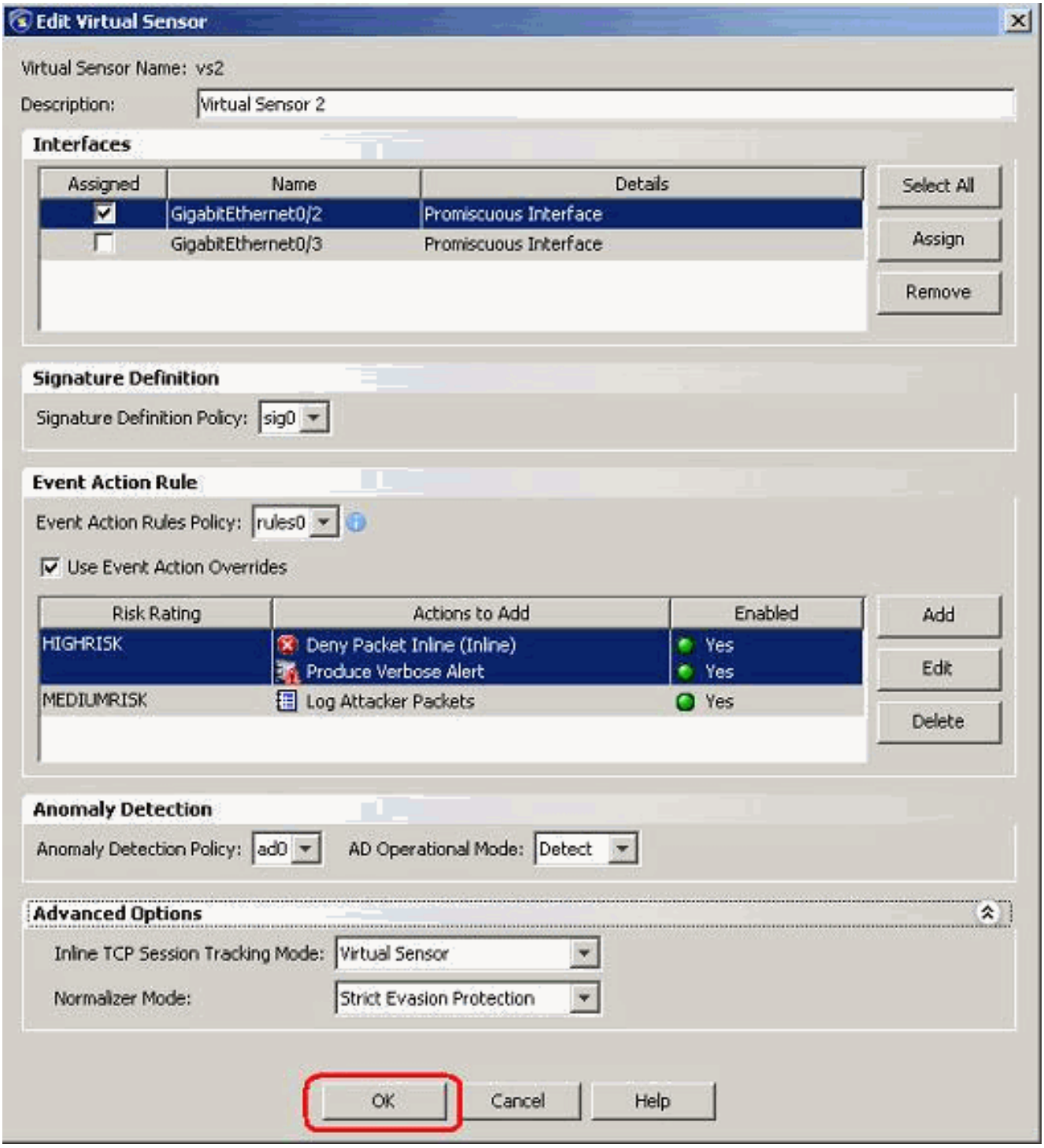
Отредактируйте действительный датчик с IME

Выполните эти шаги для редактирования действительного датчика на Системе предотвращения вторжений (IPS) Cisco Secure с Cisco IPS Manager Express:

1. Выберите **Configuration> SFO-Sensor> Policies> IPS Policies**.
2. Выберите действительный датчик, который будет отредактирован, и затем нажмет **Edit** как показано в снимке экрана. В данном примере vs2 является действительным датчиком, который будет отредактирован.



3. В **Редактировании действительное** окно **датчика** внесите изменения в параметры для действительного подарка датчика в соответствии с **определением подписи** разделов, **Правилом Действия События**, **Обнаружением отклонения** и **Расширенными настройками**. **Нажмите кнопку OK, а затем нажмите Apply.**



Это завершает процесс для редактирования действительного датчика.

Удалите действительные датчики

Для удаления действительного датчика выполните эти шаги:

1. Для удаления действительного датчика выполните **команду no virtual-sensor**.`sensor(config-ana)# virtual-sensor vs2 sensor(config-ana-vir)# sensor(config-ana-vir)# exit sensor(config-ana)# no virtual-sensor vs2`
2. Проверьте удаленный действительный датчик.`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)#` Только действительный датчик по умолчанию, **vs0**, присутствует.

3. Выходной аналитический режим механизма.`sensor(config-ana)# exit`

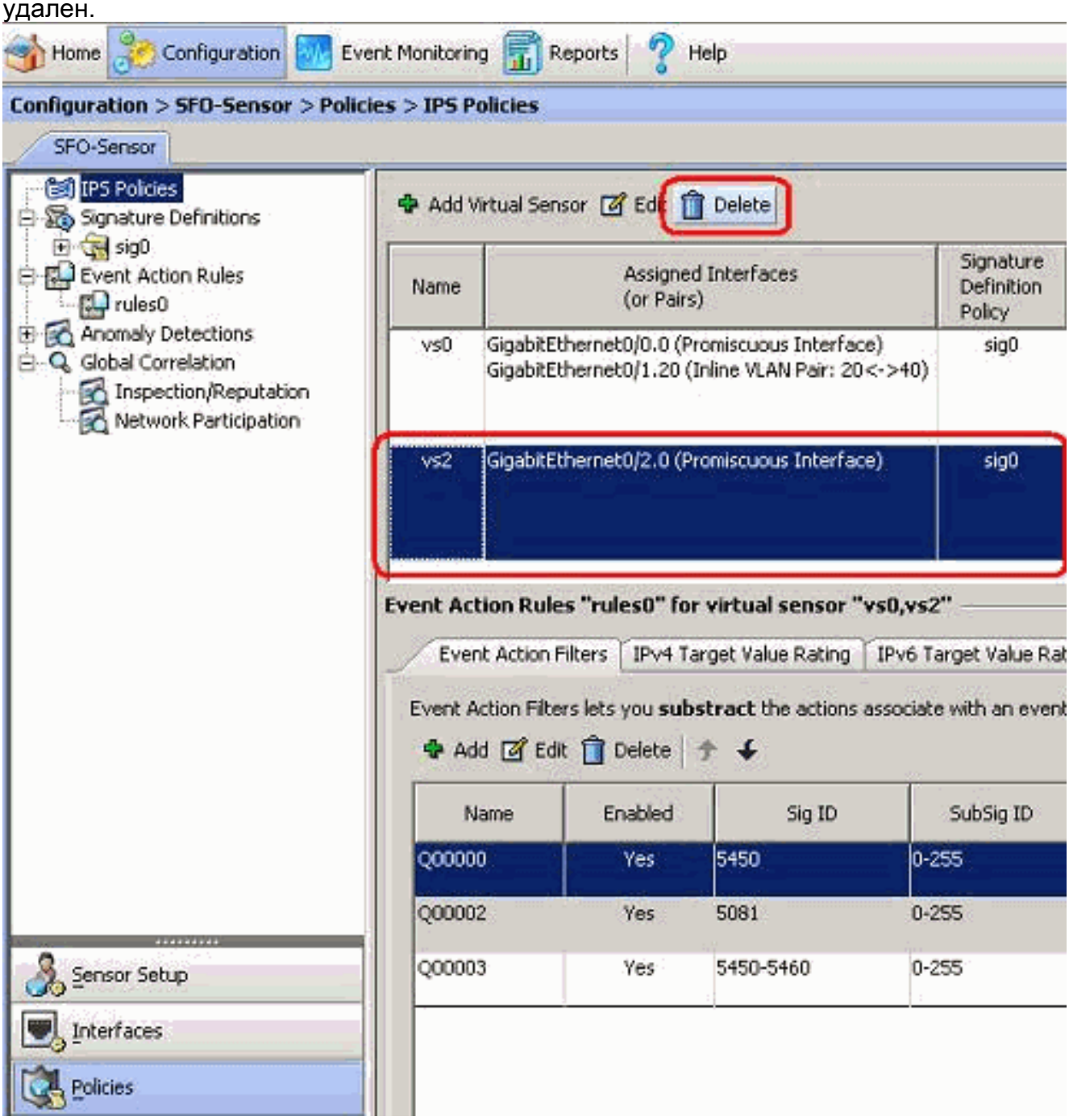
```
sensor(config)#
Apply Changes:?[yes]:
```

Удалите действительный датчик с IME

Завершите это шагает для удаления действительного датчика на Системе предотвращения вторжений (IPS) Cisco Secure с Cisco IPS Manager Express:

1. Выберите **Configuration> SFO-Sensor> Policies> IPS Policies**.

2. Выберите действительный датчик, который будет удален, и затем нажмет **Delete**, как показано в снимке экрана. В данном примере vs2 является действительным датчиком, который будет
удален.



Это завершает процесс для удаления действительного датчика. Действительный датчик vs2 удален.

Устранение неполадок

IPS Manager Express не Запускает

Проблема

Когда попытка предпринята для доступа к IPS через IME, IPS Manager Express не запускается, и это сообщение об ошибках получено:

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

Решение

Для решения этого повторно загрузите ПК рабочей станции IME.

Дополнительные сведения

- Страница технической поддержки системы предотвращения вторжений Cisco (IPS)
- Страница технической поддержки Cisco IPS Manager Express
- Network Time Protocol (NTP)
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация