Настройте IPS для предотвращения ошибочного допуска Использование фильтра действия события

Содержание

Введение

Этот документ предоставляет шаги, требуемые для настройки Системы предотвращения вторжений (IPS) для Предотвращения Ошибочного допуска с помощью диспетчера устройств IPS (IDM) или IPS Manager Express (IME). Ошибочный допуск, настраивающийся на IPS, достигнут функцией, названной Фильтром действия события (EAF).

Перед началом работы

Требования

Читатели данной документации должны ознакомиться с Cisco IPS.

Используемые компоненты

Сведения в этом документе не на основе определенных версий программного и аппаратного обеспечения.

Условные обозначения

Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips Conventions.

Понимание EAFs

EAFs настроены прежде всего для настройки ошибочного допуска. EAF предоставляет способность иметь особую подпись **не**, берут необходимые действия для подмножества трафика.

EAFs полезны в ситуациях, где это требуется, чтобы удовлетворять множественные условия, такие как:

- Подпись x **не** принимает меры у для желаемой подсети трафика.
- Подпись x принимает меры у для всего другого трафика.

EAFs полезны имея дело с мягким инициированием подписи.

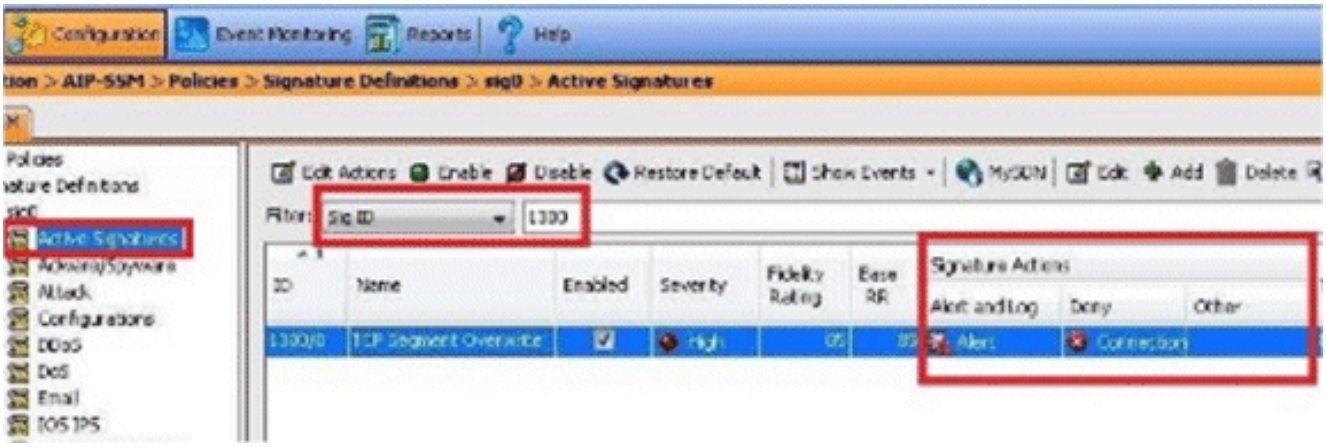
!--- конфигурацию

Пример: Событие Ошибочного допуска: Подпись 1300 инициирует для трафика, прибывающего от и до известных надежных хостов.

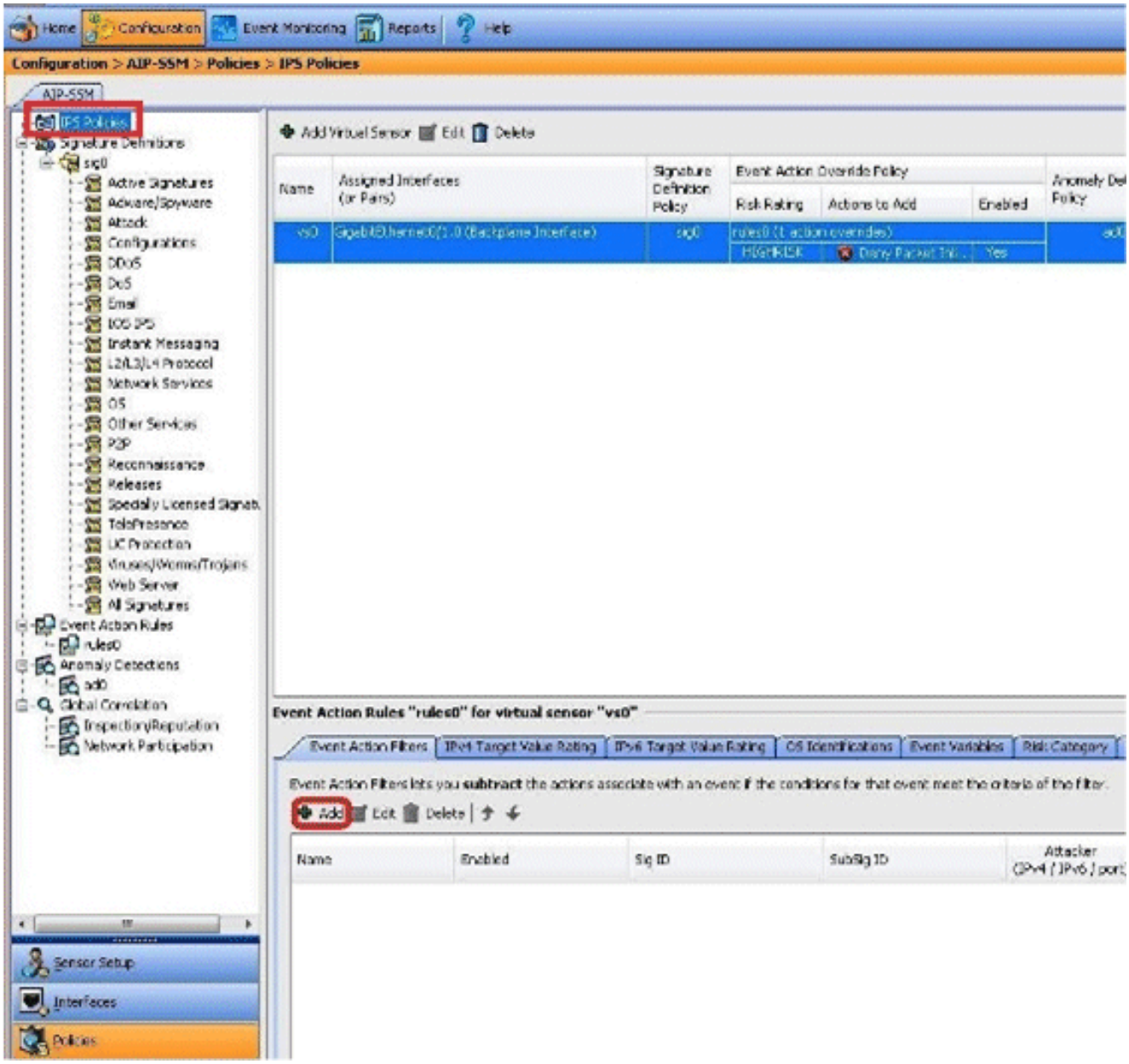
Примечание: Это - просто демонстрационный пример цели только. Если вы не уверены, мягко ли определенное событие из-за триггера подписи или нет, обратитесь в техническую поддержку Cisco для дальнейшего анализа.

Примечание: См. Подписи системы предотвращения вторжений Cisco (IPS) для дополнительных сведений относительно подписей IPS.

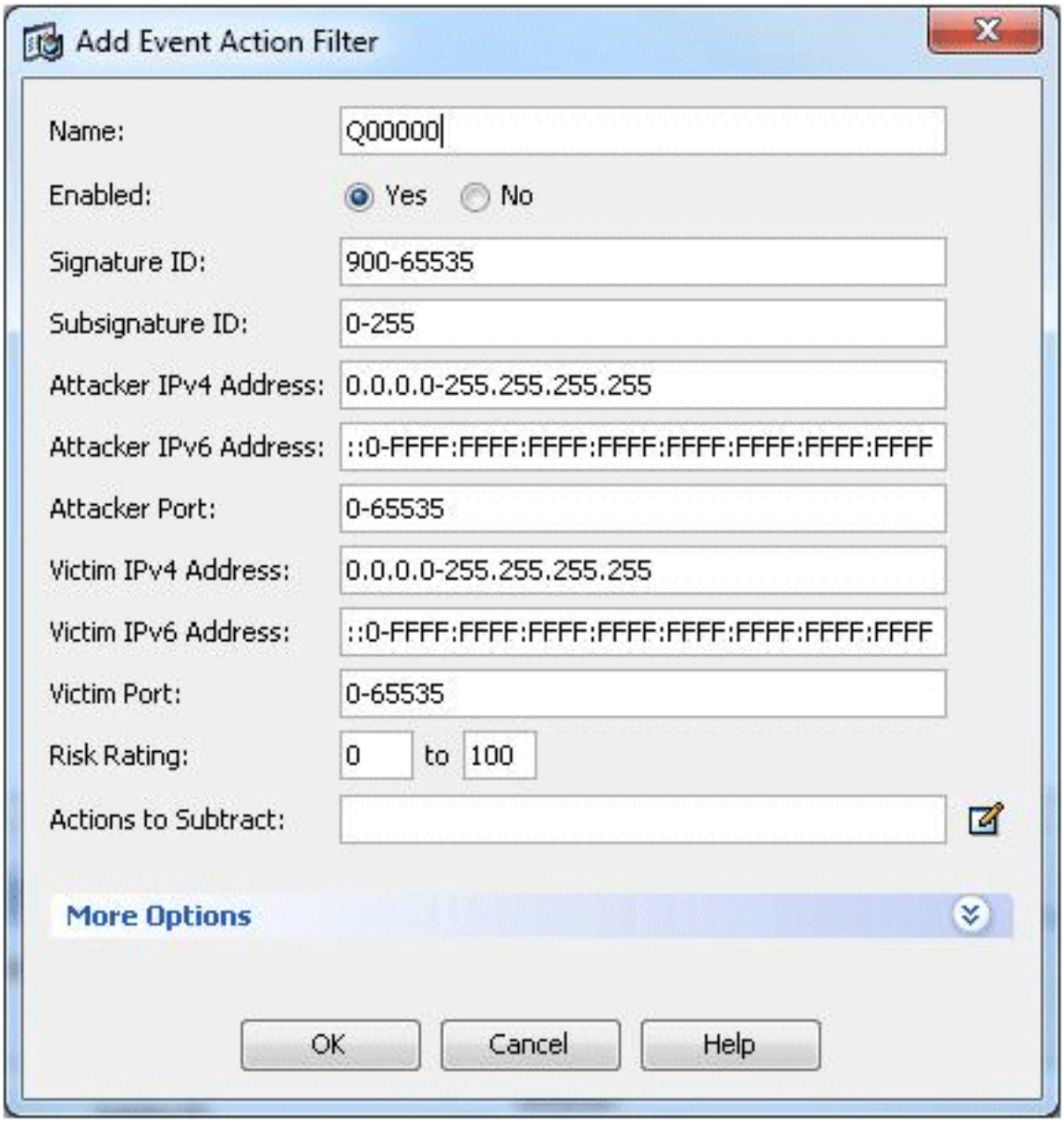
Выполните следующие действия:

1. Проверьте действия по умолчанию для подписи (1300, в данном примере), для которого должен быть настроен
   EAF.
   

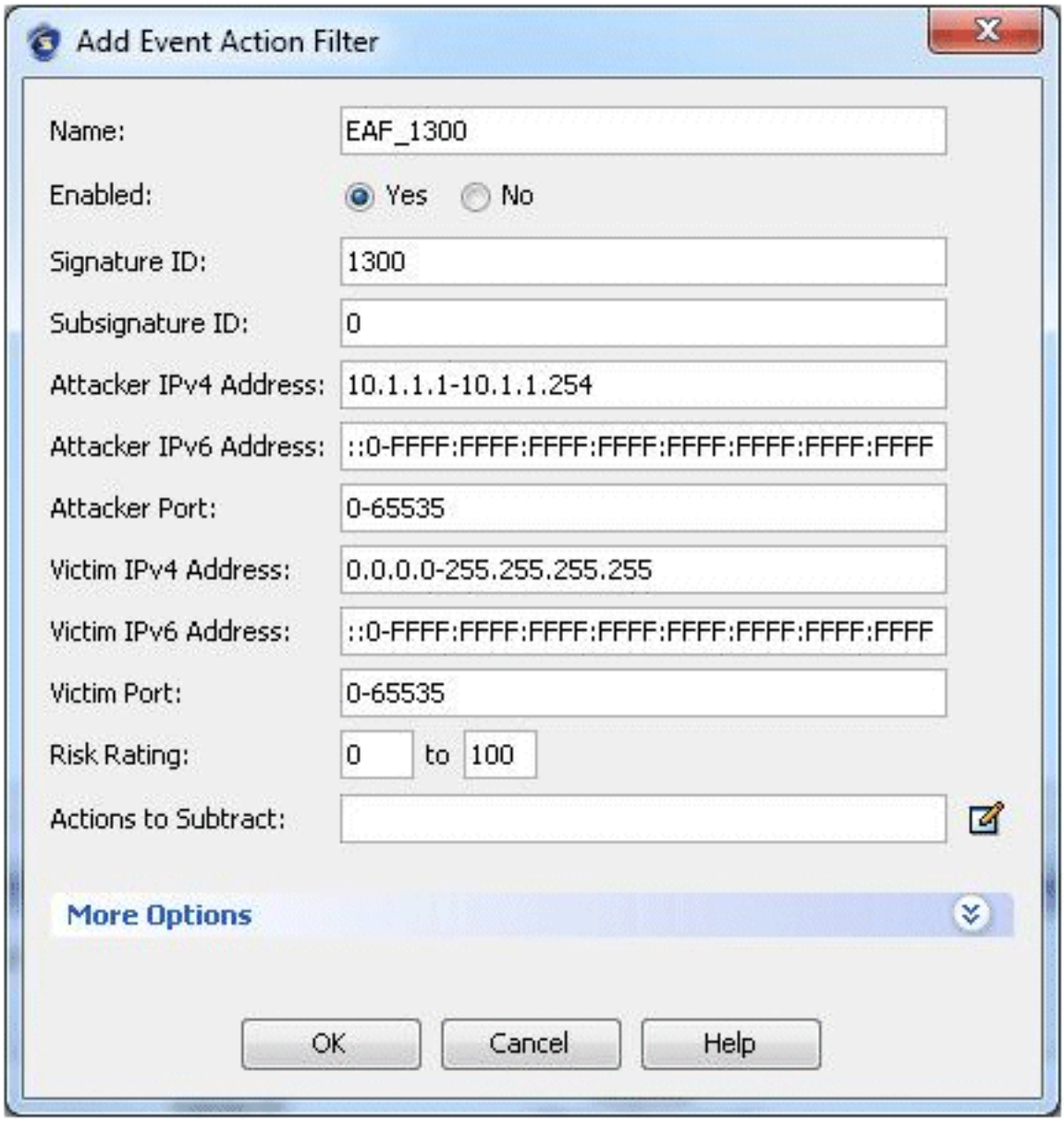
   Действия по умолчанию подписи 1300 включают**, Производят Предупреждение** и **Запрещают Встроенное Соединение**.
2. Определите хосты, для которых не должна срабатывать эта подпись. Например, вы **не** хотите, чтобы подпись сработала для трафика, прибывающего из доверяемой подсети, такой как 10.1.1.1-10.1.1.254.
3. Создайте EAF для критериев, описанных в Шаге 2:От IDM/IME перейдите **к Конфигурации> Политика> Политика IPS**. Нажмите вкладку **Event Action Filters**. Под этой вкладкой **нажмите**
   Add.



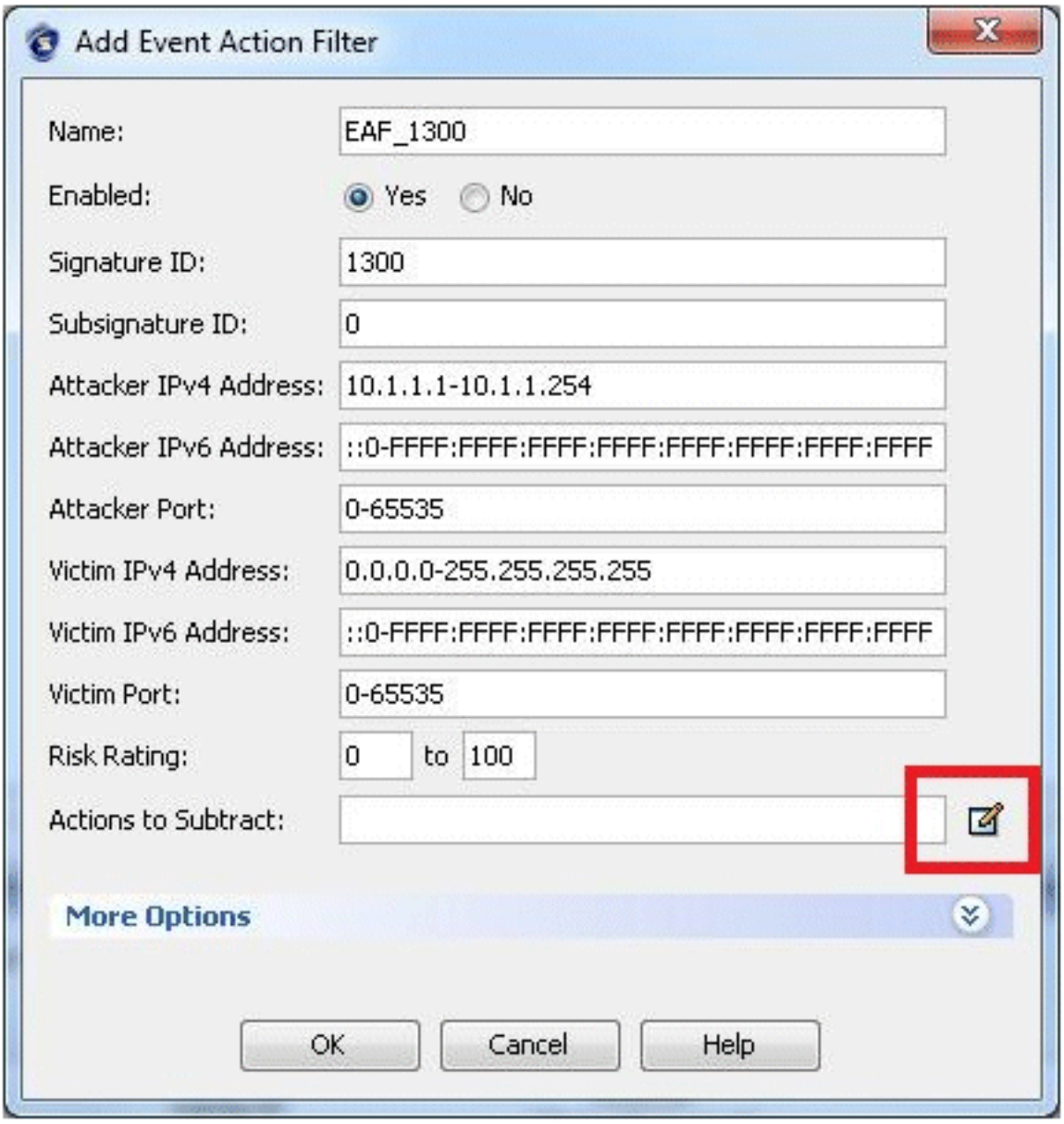
Это окно отображено:



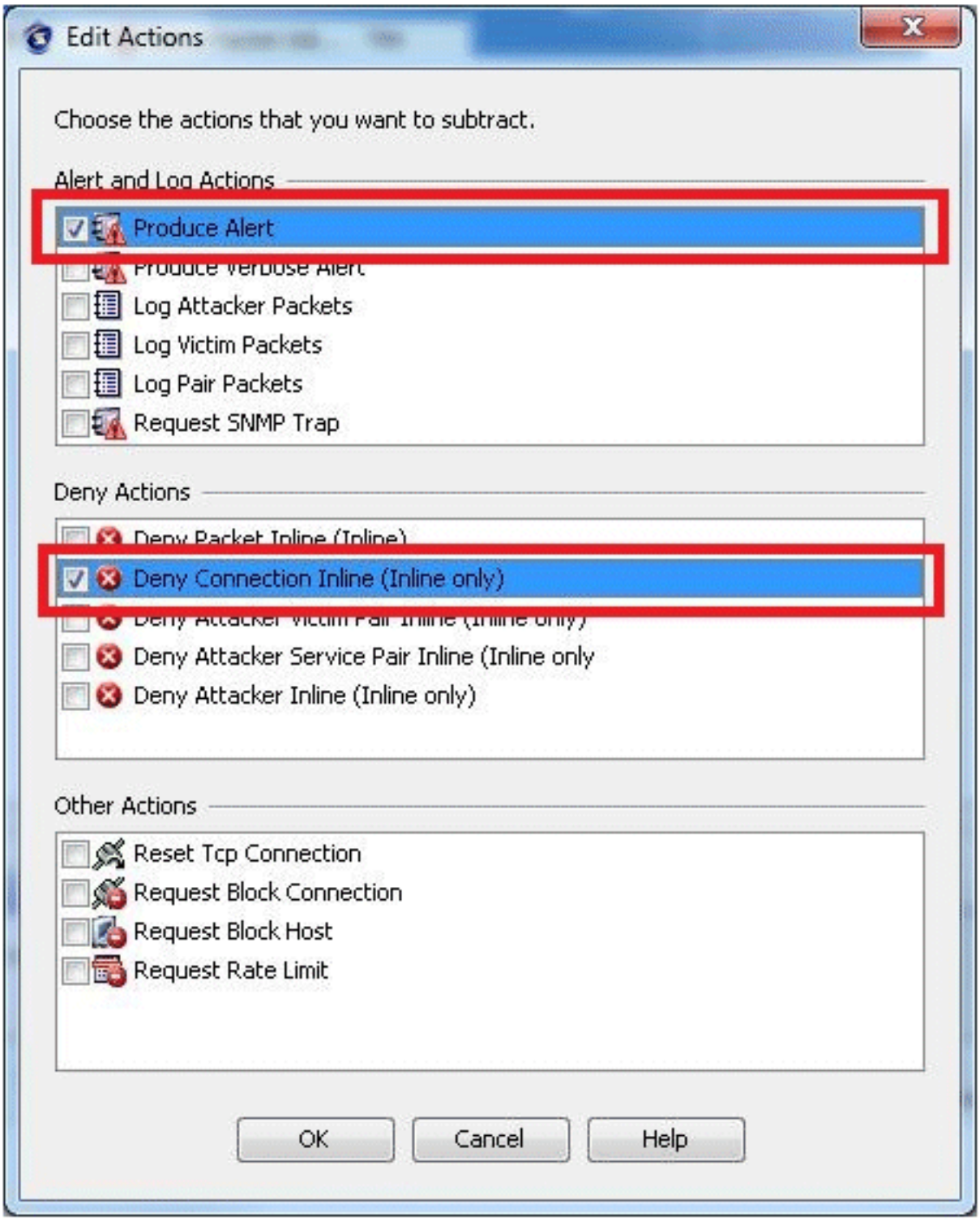
Настройте различные поля, такие как **Название**, **Идентификатор подписи**, **IP Атакующего**, и



т.д. Нажми те значок направо от поля **Actions to Subtract** для открытия диалогового окна Edit

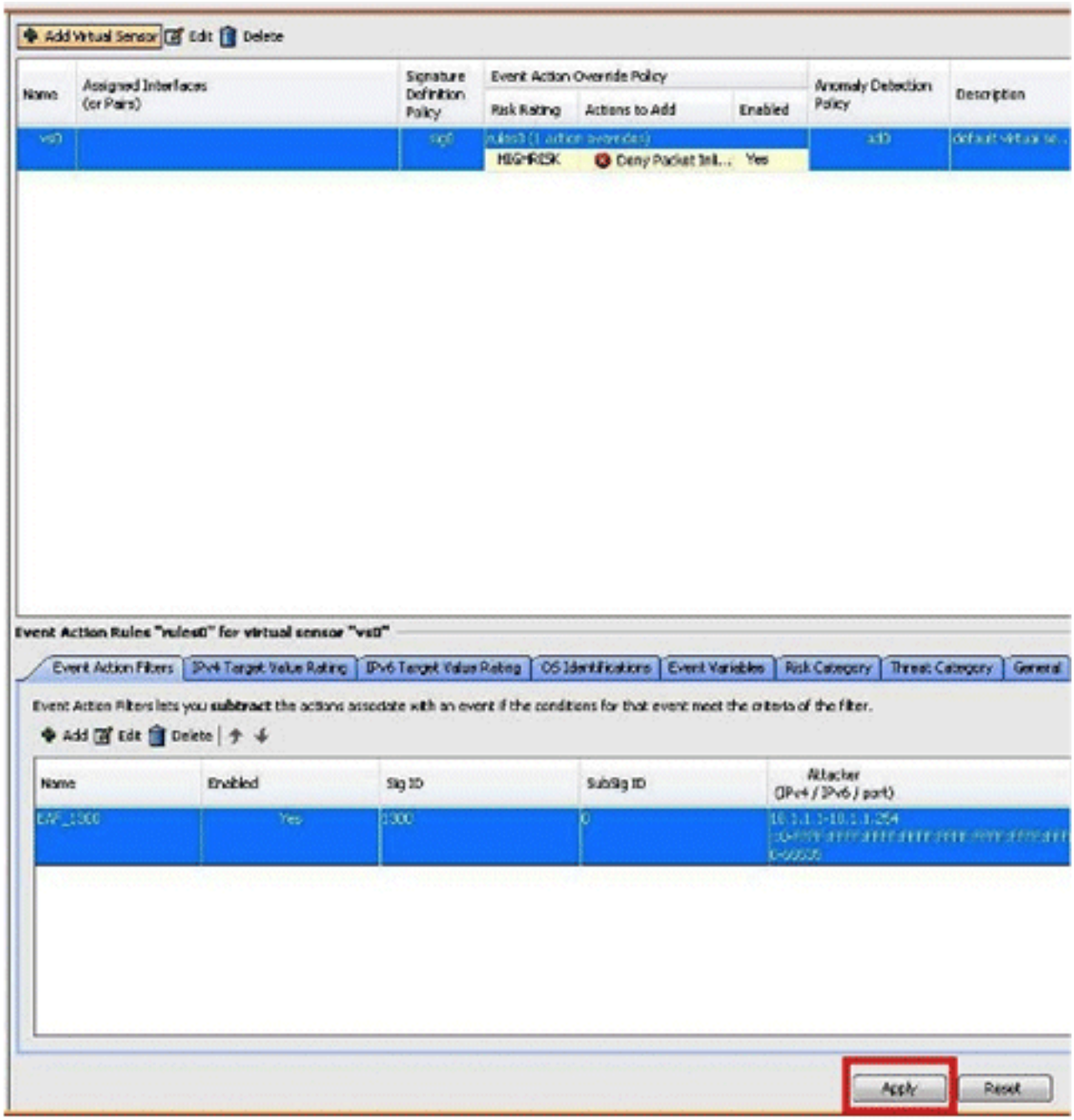


Actions. В этом окне можно задать Действия подписи, которые вы **не** хотите, чтобы IPS выполнил.**Примечание:** Для корректного выбора действий подписи, которые вы хотите вычесть, необходимо понять действия подписей по умолчанию, как описано в Шаге 1.В данном примере мы выбрали **Produce Alert** и **Deny Connection**



Inline. Если подпись 1300 года инициирует для трафика, прибывающего от 10.1.1.1-10.1.1.254, IPS **не** примет эти меры.Для всего другого трафика, действия подписи по умолчанию **Предупреждения Продукта** и **Запрещают Встроенное Соединение**, все еще применится.После выбора Produce Alert и Deny Packet Inline вы будете видеть, что эти действия заполняют у основания экрана

EAF: **Нажмите OK**, и затем **Применитесь** для сохранения изменений.



Для конфигурации Фильтра Действия События с помощью CLI обратитесь к разделу Интерфейса командной строки IPS на странице Configuration Guides. От соответствующего Руководства по конфигурации нажмите **Configuring Event Action Rules** и поиск "Фильтров Действия События Настройки".

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация