IPS 5.x и более поздние версии: Настройка сигнатуры с фильтром действий при возникновении событий с помощью интерфейса командной строки и IDM

Содержание

Введение

Этот документ описывает, как настроиться, подпись с Действием События Просачиваются система предотвращения вторжений Cisco (IPS) (IPS) с Интерфейсом командной строки (CLI) и IDS Device Manager (IDM).

Предварительные условия

Требования

Этот документ предполагает, что Cisco IPS установлен и работает должным образом.

Используемые компоненты

Сведения в этом документе основываются на Cisco Устройство IDS/ДЮЙМ В СЕКУНДУ серии 4200, которое работает под управлением ПО версии 5.0 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.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Фильтры действия события

Понимание фильтров действия события

Фильтры действия события обработаны как упорядоченный список, и можно переместить фильтры вверх или вниз в списке.

Фильтры позволяют датчику выполнить определенные действия в ответ на событие, не требуя, чтобы датчик выполнил все действия или удалил все событие. Фильтры работают удалением действий от события. Фильтр, который удаляет все действия из события эффективно, использует событие.

Примечание: При фильтрации подписей развертки Cisco рекомендует не фильтровать адреса назначения (DA). Если существуют несколько адресов назначения, только последний адрес используется для соответствия с фильтром.

Вы можете фильтры действия события configure, чтобы удалить определенные действия из события или сбросить от всего события и предотвратить дальнейшую обработку датчиком. Можно использовать переменные действия события, которые вы определили к групповым адресам для ваших фильтров. Для процедуры, о том, как переменным действия события configure, посмотрите Добавление, Редактирование и Удаление раздела Переменных Действия События.

Примечание: Необходимо снабдить переменную предисловием со знаком доллара ($), чтобы указать на использование переменной, а не строки. В противном случае вы получаете .

Действие события фильтрует конфигурацию Использование CLI

Выполните эти шаги чтобы к фильтрам действия события configure:

1. Войдите к CLI с учетной записью, которая имеет администраторские привилегии.
2. Введите подрежим правил действия события:`sensor#`**`configure terminal`** `sensor(config)#`**`service event-action-rules rules1`** `sensor(config-eve)#`
3. Создайте название фильтра:`sensor(config-eve)#`**`filters insert name1 begin`** Используйте **name1, name2**, и т.д для именования фильтров действия события. Используйте **начинание | конец | неактивный | прежде | после** ключевых слов для определения, где вы хотите вставить фильтр.
4. Задайте значения для этого фильтра:Задайте диапазон идентификатора подписи:`sensor(config-eve-fil)#`**`signature-id-range 1000-1005`** По умолчанию 900 - 65535.Задайте диапазон подыдентификатора подписи:`sensor(config-eve-fil)#`**`subsignature-id-range 1-5`** По умолчанию от 0 до 255.Задайте диапазон адресов атакующего:`sensor(config-eve-fil)#`**`attacker-address-range 10.89.10.10-10.89.10.23`** Значение по умолчанию — 0. 0.0.0 к 255.255.255.255.Задайте диапазон адресов

жертвы:`sensor(config-eve-fil)#`**`victim-address-range 192.56.10.1-192.56.10.255`** Значение по умолчанию — 0. 0.0.0 к 255.255.255.255.Задайте диапазон портов жертвы:`sensor(config-eve-fil)#`**`victim-port-range 0-434`** По умолчанию от 0 до 65535.Задайте уместность ОС:`sensor(config-eve-fil)#`**`os-relevance relevant`** По умолчанию от 0 до 100.Задайте диапазон оценки риска.`sensor(config-eve-fil)#`**`risk-rating-range 85-100`** По умолчанию от 0 до 100.Задайте действия для удаления:`sensor(config-eve-fil)#`**`actions-to-remove reset-tcp-connection`** Если вы фильтруете запрещать действие, устанавливаете процент от, запрещают действия, которые вы хотите:`sensor(config-eve-fil)#`**`deny-attacker-percentage 90`** Значение по умолчанию – 100.Задайте статус фильтра или к отключенному или к включенному.`sensor(config-eve-fil)#`**`filter-item-status {enabled | disabled}`** По умолчанию включен.Задайте остановку на параметре соответствия.`sensor(config-eve-fil)#`**`stop-on-match {true | false}`** Если этот элемент совпадает, **истинный** говорит датчику прекращать обрабатывать фильтры. Даже если этот элемент совпадает, **ложь** говорит датчику продолжать обрабатывать фильтры.Добавьте любые замечания, которые вы хотите использовать для объяснения этого фильтра:`sensor(config-eve-fil)#`**`user-comment NEW FILTER`**

5. Проверьте параметры настройки для фильтра:`sensor(config-eve-fil)#`**`show settings`** `NAME: name1 ---------- signature-id-range: 1000-10005 default: 900-65535 subsignature-id-range: 1-5 default: 0-255 attacker-address-range: 10.89.10.10-10.89.10.23 default: 0.0.0.0-255.255.255.255 victim-address-range: 192.56.10.1-192.56.10.255 default: 0.0.0.0-255.255.255.255 attacker-port-range: 0-65535 <defaulted> victim-port-range: 1-343 default: 0-65535 risk-rating-range: 85-100 default: 0-100 actions-to-remove: reset-tcp-connection default: deny-attacker-percentage: 90 default: 100 filter-item-status: Enabled default: Enabled stop-on-match: True default: False user-comment: NEW FILTER default: os-relevance: relevant default: relevant|not-relevant|unknown ---------- senor(config-eve-fil)#`
6. Для редактирования существующего фильтра:`sensor(config-eve)#`**`filters edit name1`**
7. Отредактируйте параметры и посмотрите Шаги 4a через 4 л для получения дополнительной информации.
8. Для продвижения фильтра или вниз в списке фильтров:`sensor(config-eve-fil)#`**`exit`** `sensor(config-eve)#`**`filters move name5 before name1`**
9. Проверьте перемещение фильтров:`sensor(config-eve-fil)#`**`exit`** `sensor(config-eve)#`**`show settings`** `---------- filters (min: 0, max: 4096, current: 5 - 4 active, 1 inactive) ---------- ACTIVE list-contents ---------- NAME: name5 ---------- signature-id-range: 900-65535 <defaulted> subsignature-id-range: 0-255 <defaulted> attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted> victim-address-range: 0.0.0.0-255.255.255.255 <defaulted> attacker-port-range: 0-65535 <defaulted> victim-port-range: 0-65535 <defaulted> risk-rating-range: 0-100 <defaulted> actions-to-remove: <defaulted> filter-item-status: Enabled <defaulted> stop-on-match: False <defaulted> user-comment: <defaulted> ---------- ---------- NAME: name1 ---------- signature-id-range: 900-65535 <defaulted> subsignature-id-range: 0-255 <defaulted> attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted> victim-address-range: 0.0.0.0-255.255.255.255 <defaulted> attacker-port-range: 0-65535 <defaulted> victim-port-range: 0-65535 <defaulted> risk-rating-range: 0-100 <defaulted> actions-to-remove: <defaulted> filter-item-status: Enabled <defaulted> stop-on-match: False <defaulted> user-comment: <defaulted> ---------- ---------- NAME: name2 ---------- signature-id-range: 900-65535 <defaulted> subsignature-id-range: 0-255 <defaulted> attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted> victim-address-range: 0.0.0.0-255.255.255.255 <defaulted> attacker-port-range: 0-65535 <defaulted> victim-port-range: 0-65535 <defaulted> risk-rating-range: 0-100 <defaulted> actions-to-remove: <defaulted> filter-item-status: Enabled <defaulted> stop-on-match: False <defaulted> user-comment: <defaulted> ---------- ----------`

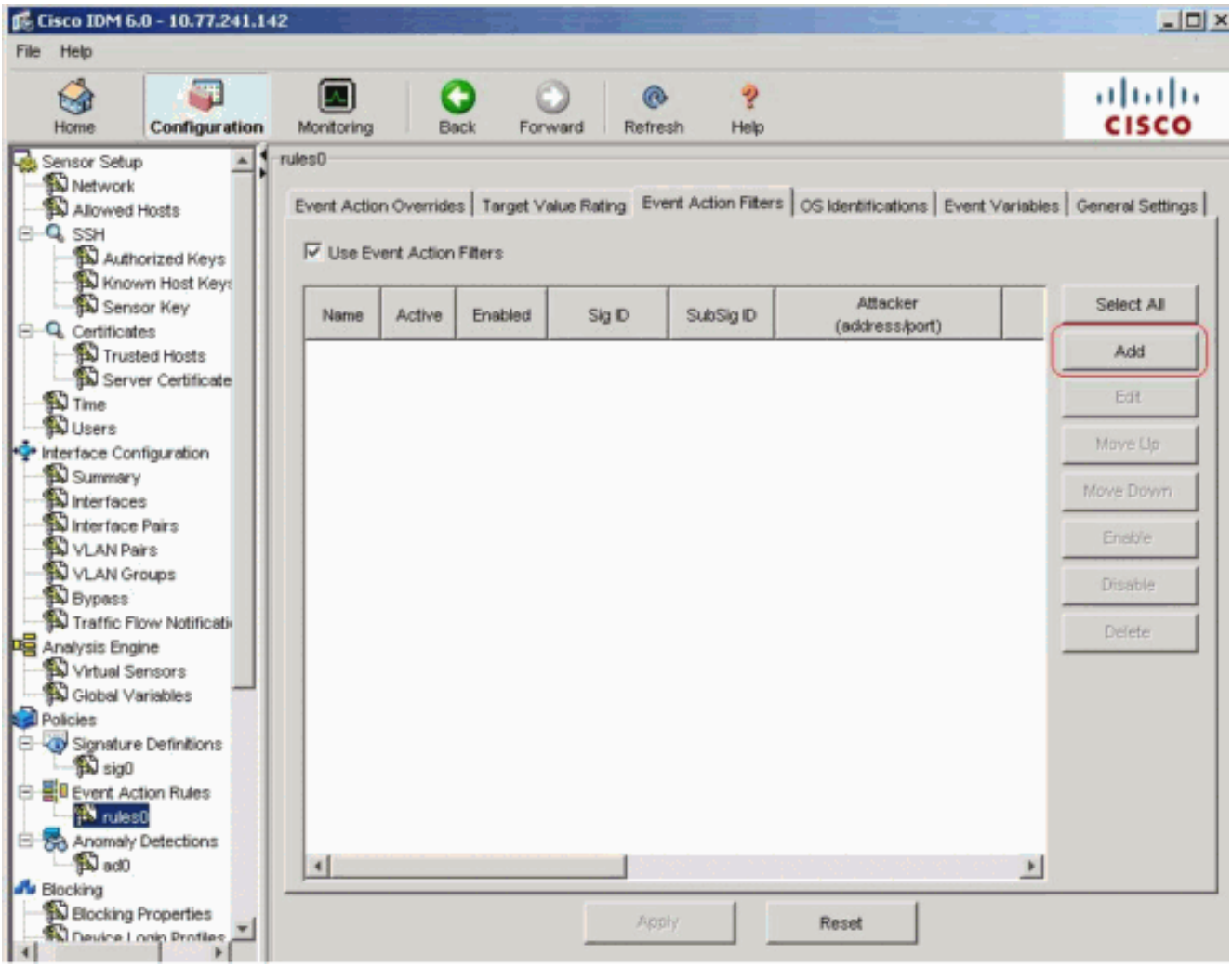
```
--------------- ---------------------------------------------- INACTIVE list-contents ---
----------------------------------------- ------------------------------------------
- sensor(config-eve)#
```

10. Для перемещения фильтра в неактивный список:`sensor(config-eve)#` **`filters move name1 inactive`**
11. Проверьте, что фильтр переместился в неактивный список:`sensor(config-eve-fil)#` **`exit`**
    ```
    sensor(config-eve)#show settings ---------------------------------------------- INACTIVE
    list-contents ---------------------------------------------- ----------------------------
    ------------------ NAME: name1 ---------------------------------------------- signature-
    id-range: 900-65535 <defaulted> subsignature-id-range: 0-255 <defaulted> attacker-address-
    range: 0.0.0.0-255.255.255.255 <defaulted> victim-address-range: 0.0.0.0-255.255.255.255
    <defaulted> attacker-port-range: 0-65535 <defaulted> victim-port-range: 0-65535
    <defaulted> risk-rating-range: 0-100 <defaulted> actions-to-remove: <defaulted> filter-
    item-status: Enabled <defaulted> stop-on-match: False <defaulted> user-comment:
    <defaulted> ---------------------------------------------- ----------------------------
    ----------------- sensor(config-eve)#
    ```
12. Действие события Exit управляет подрежимом:`sensor(config-eve)#` **`exit`** `Apply Changes:?[yes]:`
13. Нажмите **Enter**, чтобы применить ваши изменения или войти **не** для отмены от них.

Действие события фильтрует конфигурацию Использование IDM

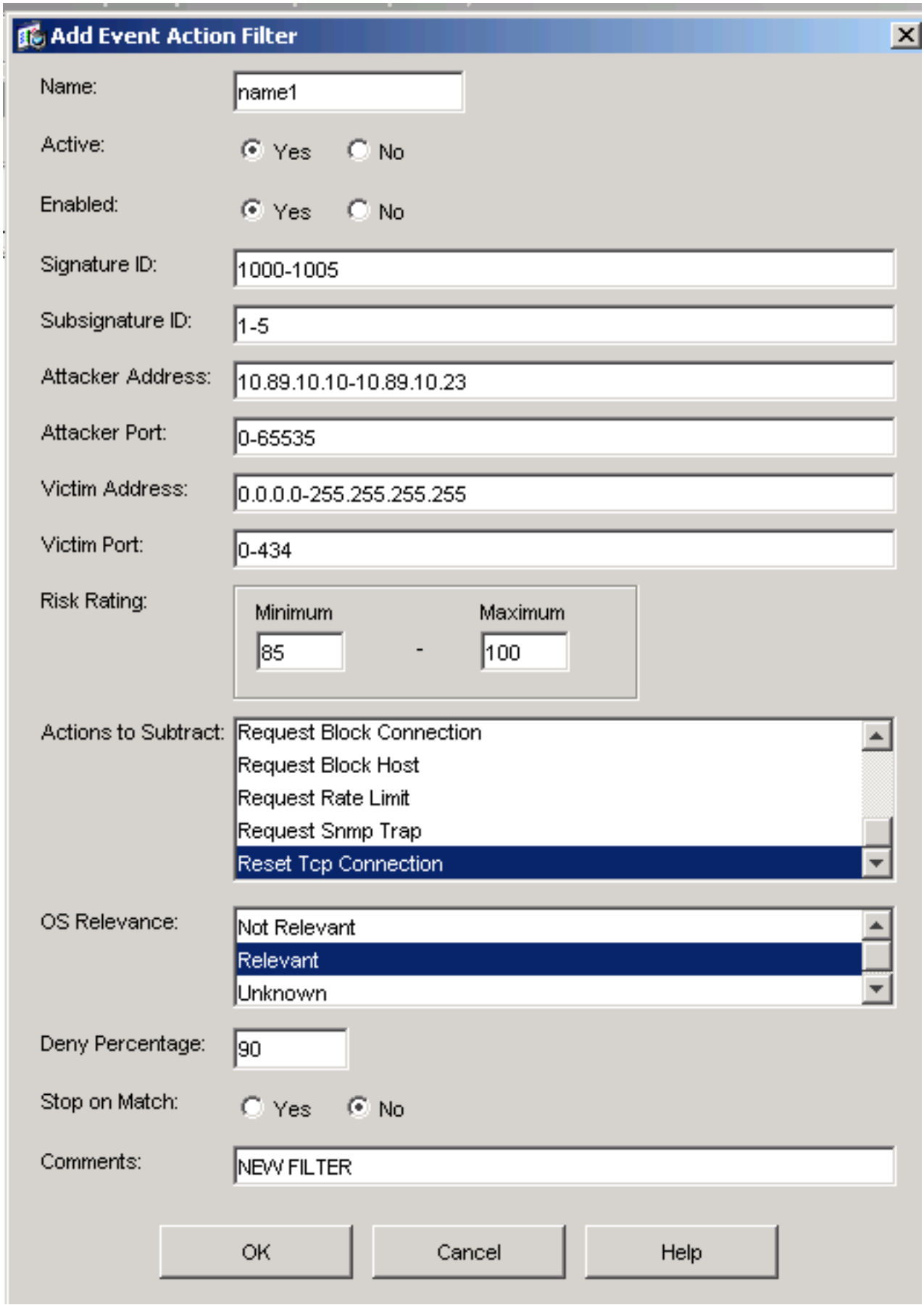
Выполните эти шаги, чтобы добавить, отредактировать, удалите, включите, отключите, и фильтры действия события move:

1. Войдите к IDM с учетной записью, которая имеет привилегии администратора или оператора.
2. Выберите **Configuration> Policies> Event Action Rules> rules0> Фильтры Действия События**, если версия программного обеспечения равняется 6. x. Для версии программного обеспечения 5.x выберите **Configuration> Event Action Rules> Event Action Filters.**Вкладка Event Action Filters появляется как показано.

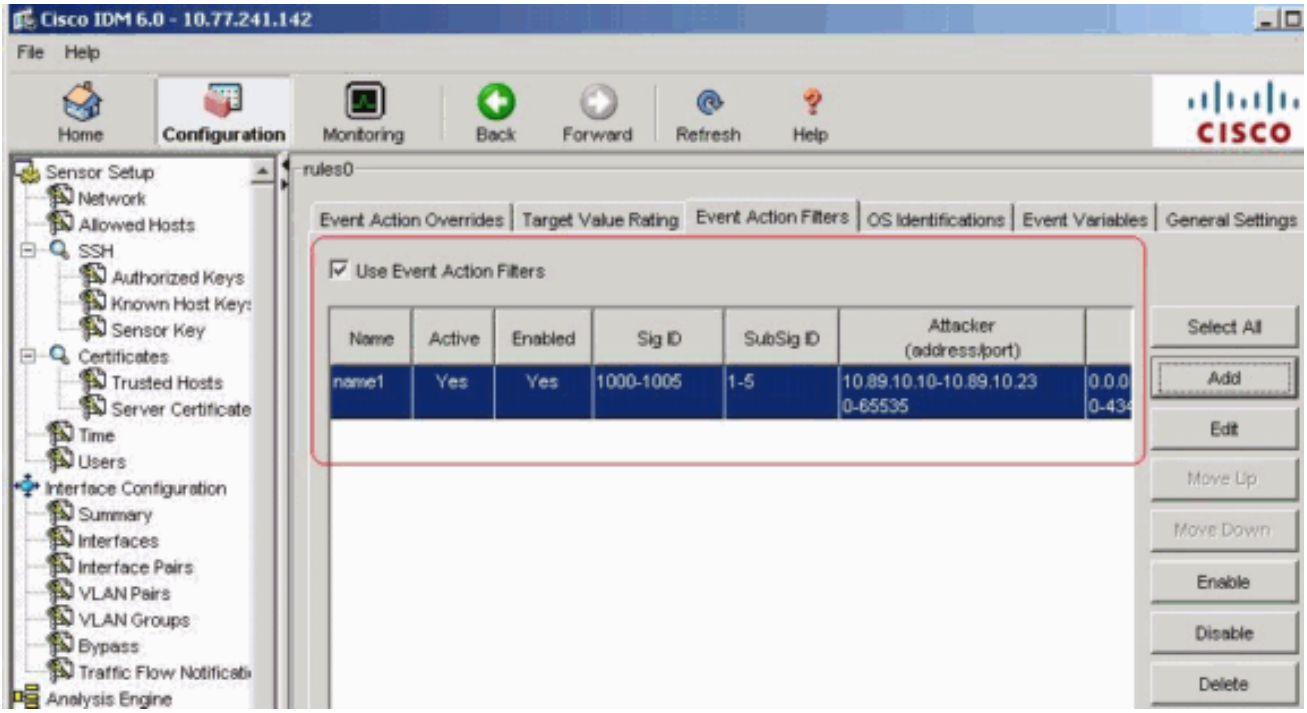


3. **Нажмите Add** для добавления фильтра действия события.Диалоговое окно Add Event Action Filter появляется.
4. В Поле имени введите имя как **name1** для фильтра действия события.Имя по умолчанию предоставлено, но можно изменить его на больше понятного имени.
5. В Активном поле нажмите кнопку с зависимой фиксацией **Yes** для добавления этого фильтра к списку так, чтобы это вступило в силу при фильтрации событий.
6. В поле Enabled нажмите кнопку с зависимой фиксацией **Yes** для включения фильтра.**Примечание:** Необходимо также проверить флажок **Use Event Action Filters** на вкладке Event Action Filters, или ни один из фильтров действия события не становится включенным независимо от того, проверяете ли вы флажок **Yes** в диалоговом окне Add Event Action Filter.
7. В поле Signature ID введите идентификаторы подписи всех подписей, к которым должен быть применен этот фильтр.Можно использовать список, например, 1000, 1005, или диапазон, например, **1000-1005** или одна из переменных SIG при определении их на вкладке Event Variables. Снабдите переменную предисловием с $.
8. В поле SubSignature Id введите подыдентификаторы подписи подподписей, к которым должен быть применен этот фильтр. Например, **1-5**.
9. В Поле адреса Атакующего введите IP-адрес исходного хоста.Можно использовать одну из переменных при определении их на вкладке Event Variables. Снабдите переменную предисловием с $. Можно также ввести диапазон адресов, например, **10.89.10.10-10.89.10.23**. Значение по умолчанию — 0. 0.0.0-255.255.255.255.
10. В поле Attacker Port введите номер порта, используемый атакующим для передачи незаконного пакета.

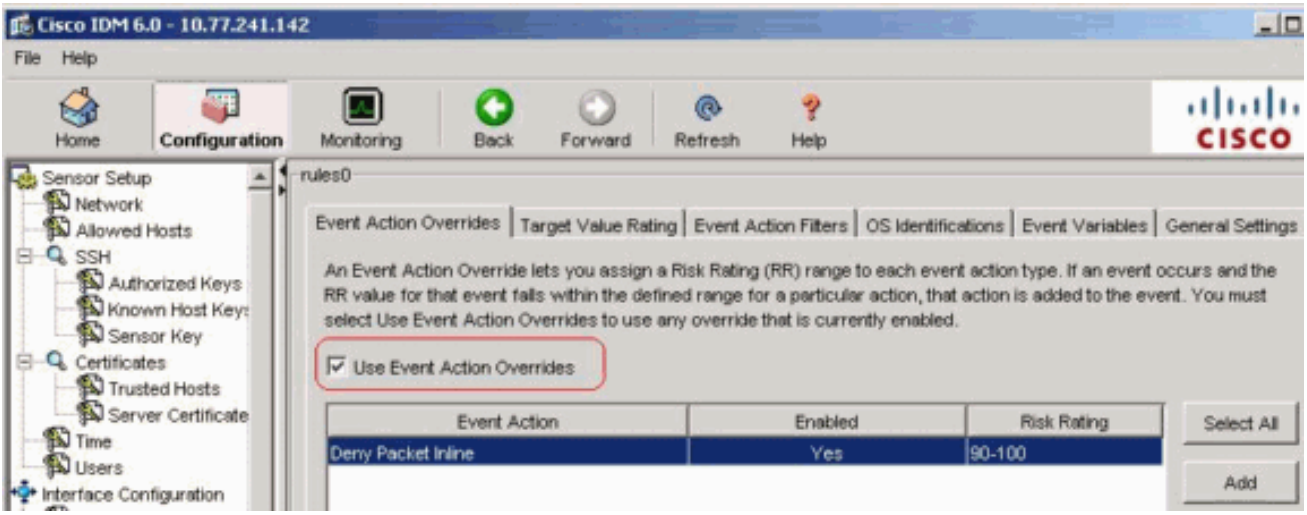
11. В Поле адреса Жертвы введите IP-адрес хоста получателя.Можно использовать одну из переменных при определении их на вкладке Event Variables. Снабдите переменную предисловием с $. Можно также ввести диапазон адресов, например, **192.56.10.1-192.56.10.255**. Значение по умолчанию — 0. 0.0.0-255.255.255.255.
12. В поле Victim Port введите номер порта, используемый атакуемым хостом для получения незаконного пакета. Например, **0-434**.
13. В поле Risk Rating введите диапазон RR для этого фильтра. Например, **85-100**.Если RR для события находится в пределах диапазона, вы задаете, событие обработано против критериев этого фильтра.
14. От Действий для Вычитания выпадающего списка выберите действия, которые вы хотите, чтобы этот фильтр удалил из события. Например, выберите **Reset TCP connection**.**Совет:** Удержите в нажатом состоянии **клавишу CTRL** для выбора нескольких действий события в списке.
15. В выпадающем списке Уместности ОС выберите, хотите ли вы знать, относится ли предупреждение к ОС, который был определен для жертвы. Например, выберите **Relevant**.
16. В поле Deny Percentage введите процент пакетов для запрета для, запрещают функции атакующего. Например, **90**.По умолчанию составляет 100 процентов.
17. На Остановке на Match field выберите одну из этих кнопок с зависимой фиксацией:**Да** — Если вы хотите, чтобы компонент Фильтров Действия События прекратил обрабатывать после того, как действия этого определенного фильтра удаленыЛюбые фильтры, которые остаются, не обработаны; поэтому, никакие дополнительные действия не могут быть удалены из события.**Нет** — Если вы хотите продолжить обрабатывать дополнительные фильтры
18. В поле Comments введите любые замечания, которые вы хотите сохранить этим фильтром, таким как цель этого фильтра или почему вы настроили, это просачивается определенный путь. Например, **ФИЛЬТР NEW**.**Совет:** Нажмите **Cancel**, чтобы отменить ваши изменения и закрыть диалоговое окно Add Event Action Filter.



19. **Нажмите кнопку ОК.**Новый фильтр действия события теперь появляется в списке на вкладке Event Action Filters как
показано.

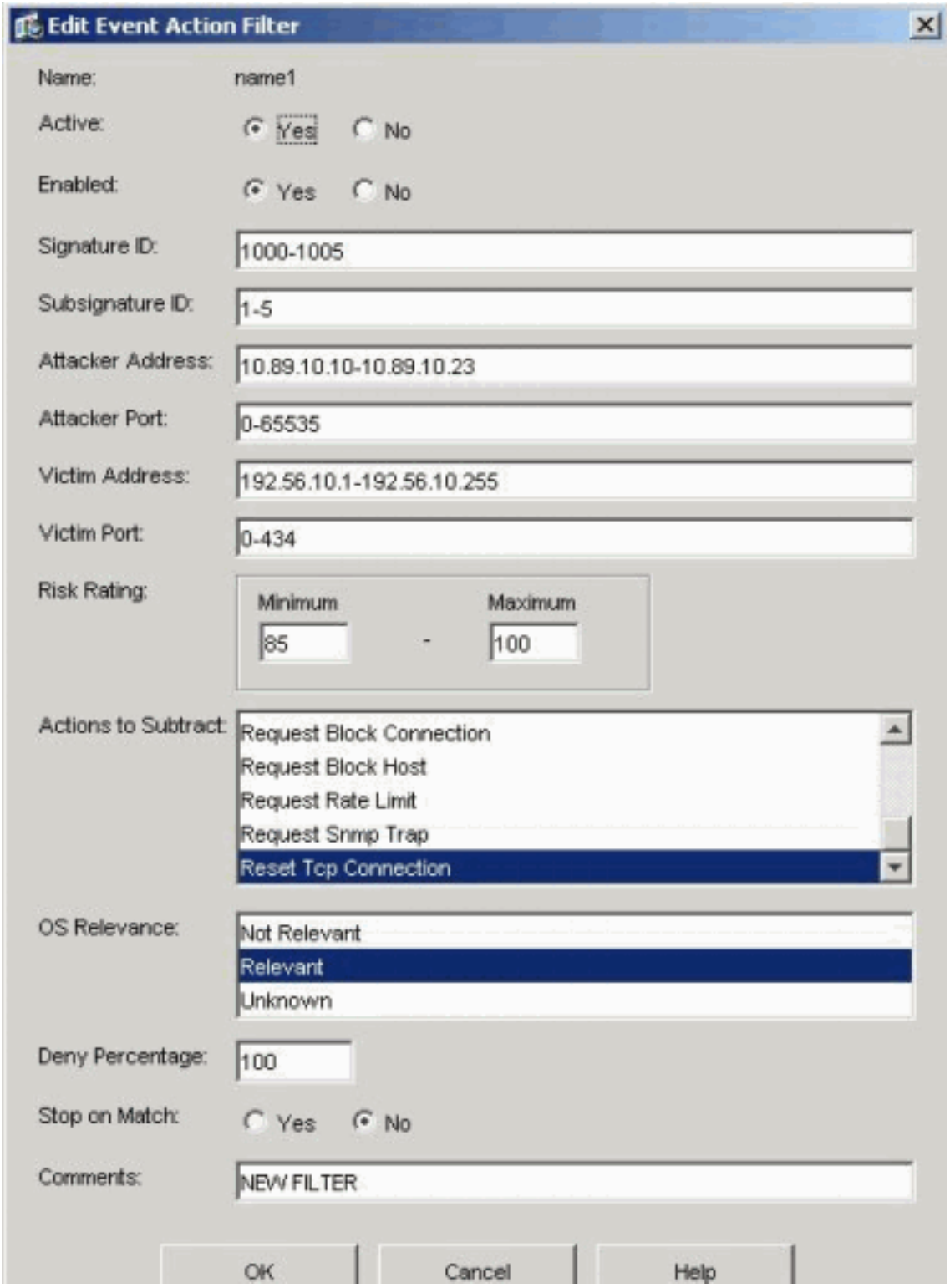


20. Проверьте флажок **Use Event Action Overrides** как показано.



Примечание: Необходимо проверить флажок **Use Event Action Overrides** на вкладке Event Action Overrides, или ни одно из переопределений действия при событии не становится включенным независимо от значения, которое вы устанавливаете в диалоговом окне Add Event Action Filter.

21. Выберите существующее действие события просачиваются список, чтобы отредактировать его, и затем нажать **Edit**.Диалоговое окно Edit Event Action Filter появляется.



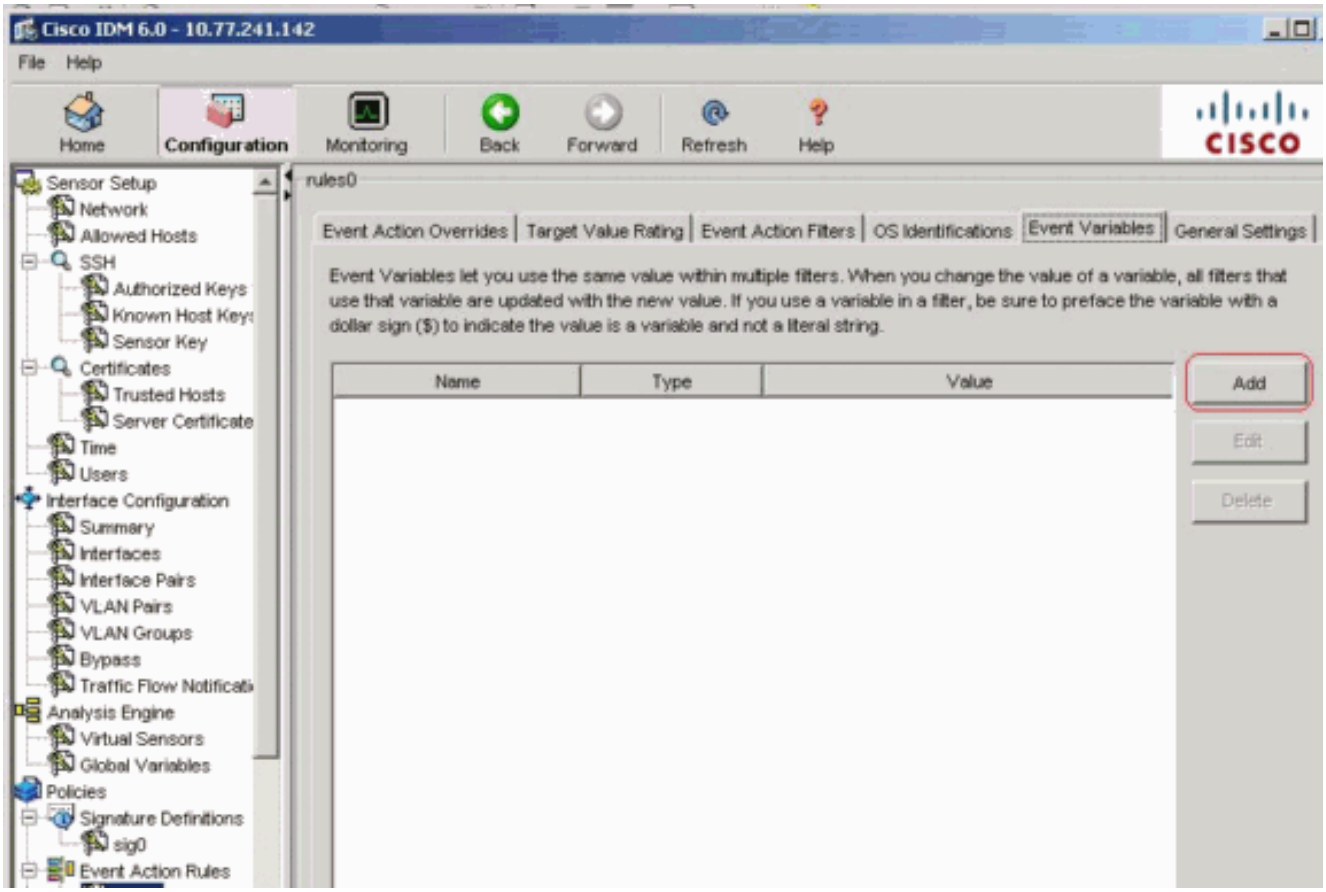
22. Измените любые значения в полях, которые необходимо изменить.Посмотрите шаги 4 - 18 для получения информации о том, как завершить поля.**Совет:** Нажмите **Cancel**, чтобы отменить ваши изменения и закрыть диалоговое окно Edit Event Action Filter.
23. **Нажмите кнопку OK.**Отредактированный фильтр действия события теперь появляется в списке на вкладке Event Action Filters.
24. Проверьте флажок **Use Event Action Overrides**.**Примечание:** Необходимо проверить флажок **Use Event Action Overrides** на вкладке Event Action Overrides, или ни одно из переопределений действия при событии не включено независимо от значения, которое вы устанавливаете в диалоговом окне Edit Event Action Filter.
25. Выберите действие события просачиваются список, чтобы удалить его, и затем нажать **Delete**.Фильтр действия события больше не появляется в списке на вкладке Event Action Filters.

26. Фильтруйте или вниз в списке, чтобы переместить действие события, выбрать его, и затем нажать **Move Up** или **Move Down**.**Совет:** Нажмите **Reset** для удаления изменений.
27. Нажмите **Apply**, чтобы применить ваши изменения и сохранить пересмотренную конфигурацию.

Переменная конфигурация события

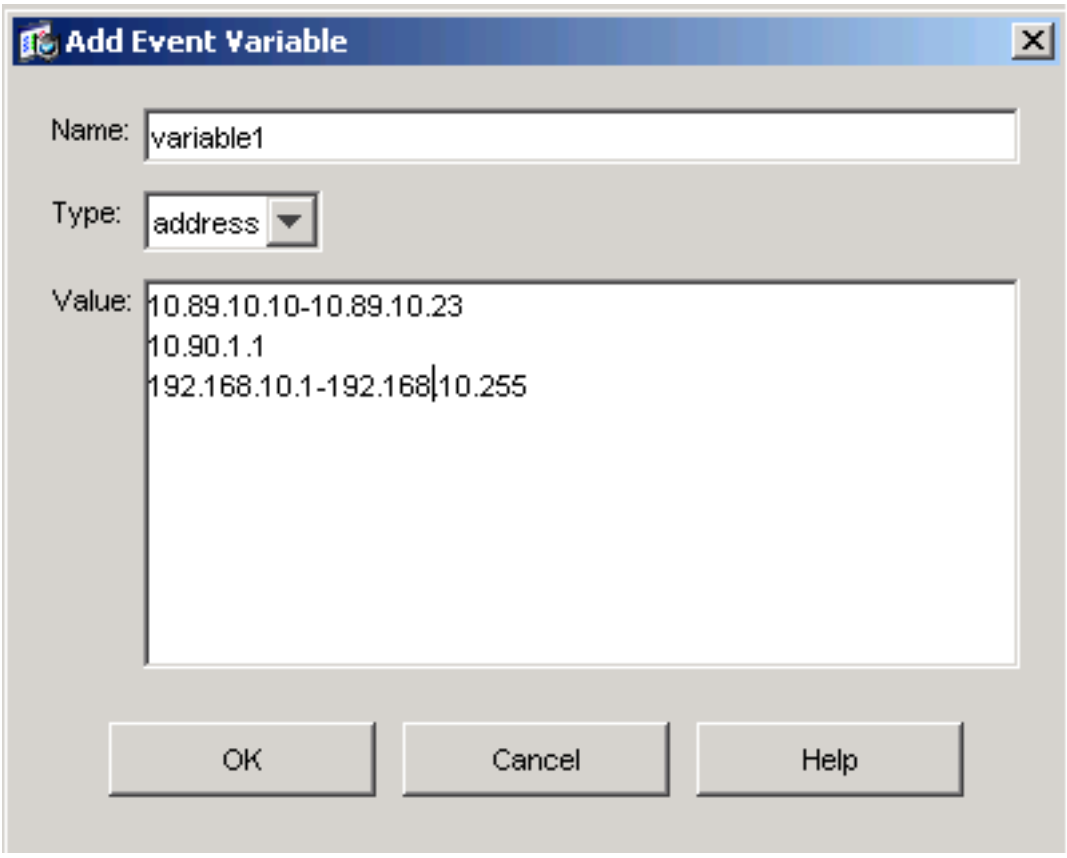
Выполните эти шаги, чтобы добавить, отредактировать, и переменные события delete:

1. Вход в систему. Например, используйте учетную запись с привилегиями администратора или оператора.
2. Выберите **Configuration> Policies> Event Action Rules> rules0> Переменные События**, если версия программного обеспечения равняется 6. x. Для версии программного обеспечения 5.x выберите **Configuration> Event Action Rules> Event Variables**.Вкладка Event Variables
появляется.

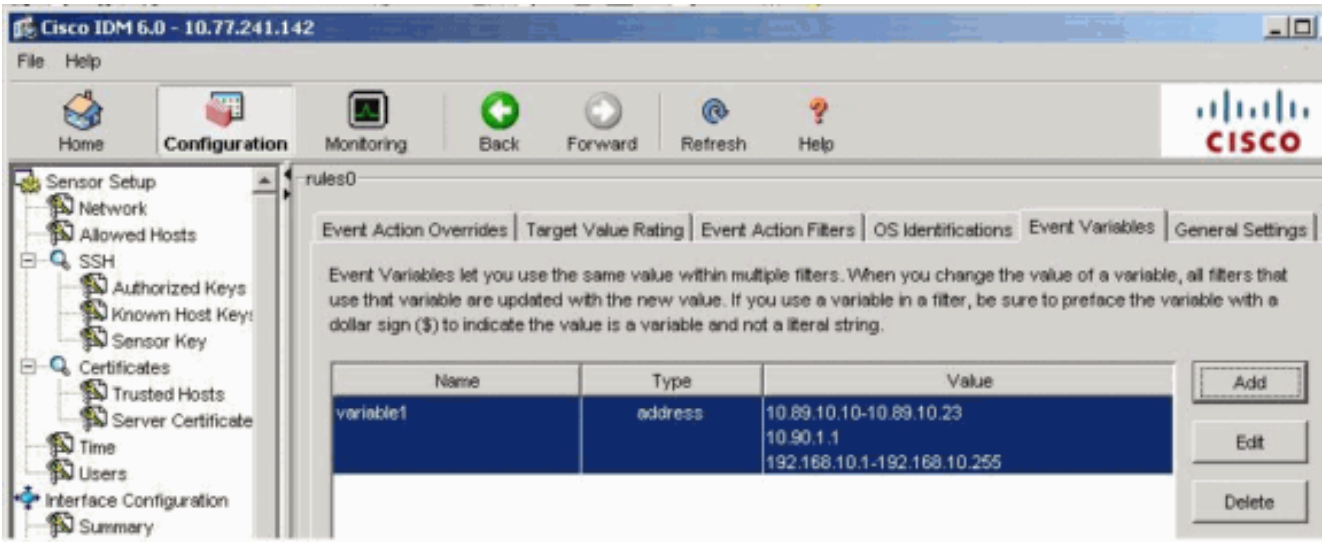


3. **Нажмите Add** для создания переменной.Диалоговое окно Add Variable появляется.
4. В Поле имени введите имя для этой переменной.**Примечание:** Допустимое название может только содержать номера или буквы. Можно также использовать дефис (-) или подчеркивание (_).
5. В Поле значения введите значения для этой переменной.Задайте полный IP-адрес или диапазоны или набор диапазонов. Пример:10.89.10.10-10.89.10.2310.90.1.1192.168.10.1-192.168.10.255**Примечание:** Можно использовать запятые в качестве разделителей. Удостоверьтесь, что после запятой нет никаких замыкающих пробел. В противном случае вы получаете сообщение об ошибках

.**Совет:** Нажмите **Cancel**, чтобы отменить ваши изменения и закрыть диалоговое окно Add Event Variable.



6. **Нажмите кнопку OK.**Новая переменная появляется в списке на вкладке Event Variables.



7. Выберите существующую переменную в списке, чтобы отредактировать его, и затем нажать **Edit**.Диалоговое окно Edit Event Variable появляется.
8. В Поле значения введите свои изменения в значение.
9. **Нажмите кнопку OK.**Отредактированная переменная события теперь появляется в списке на вкладке Event Variables.**Совет:** Выберите **Reset** для удаления изменений.
10. Нажмите **Apply**, чтобы применить ваши изменения и сохранить пересмотренную конфигурацию.

Дополнительные сведения

- Страница технической поддержки системы предотвращения вторжений Cisco (IPS)
- Cisco Systems – техническая поддержка и документация