IPS Cisco Secure - исключение ошибочных сигналов тревоги

Содержание

Введение

Этот документ описывает исключение ложных положительных сигналов тревоги для Системы предотвращения вторжений (IPS) Cisco Secure.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на версии 7.0 Системы предотвращения вторжений (IPS) Cisco Secure и менеджере Cisco IPS Экспрессе 7.0.

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.

Ложные положительные и отрицательные аварийные сигналы

Когда данный пакет или последовательность пакетов совпадают с характеристиками профилей известного метода атаки, определенных в подписях IPS Cisco Secure, IPS Cisco Secure инициирует сигнал тревоги. Важный критерий проектирования подписи IPS должен минимизировать возникновение ошибочного допуска и нераспознаваний опасности.

Когда IPS сообщает об определенном неопасном действии как злонамеренном, ошибочные допуски (мягкие триггеры) происходят. Это требует, чтобы ручное вмешательство диагностировало событие. Большое число ошибочных допусков может значительно истощить ресурсы, и специализированные навыки, требуемые проанализировать их, являются дорогостоящими и трудными найти.

Когда IPS не обнаруживает и сообщает о фактических нежелательных действиях, ложные отрицательные происходят. Последствие этого может быть катастрофическим, и подписи должны постоянно обновляться как новое использование, и способы взламывания обнаружены. Сведение к минимуму числа ложных отрицательных сообщений об ошибках играет очень важную роль, иногда даже за счет повышения числа ложных положительных сообщений.

Из-за природы подписей, что использование IPSS для обнаружения нежелательных действий почти невозможно полностью устранить ошибочные допуски и отрицания, сильно не ухудшая эффективность IPS или сильно разрушая вычислительную инфраструктуру организации (такие как хосты и сети). Специализированная настройка, когда IPS развернут, минимизирует ошибочные допуски. Требуется периодическая перенастройка при изменениях компьютерной среды (например, при развертывании новых систем и приложений). IPS Cisco Secure предоставляет возможность гибкой настройки, которая может минимизировать ошибочные допуски во время установившихся операций.

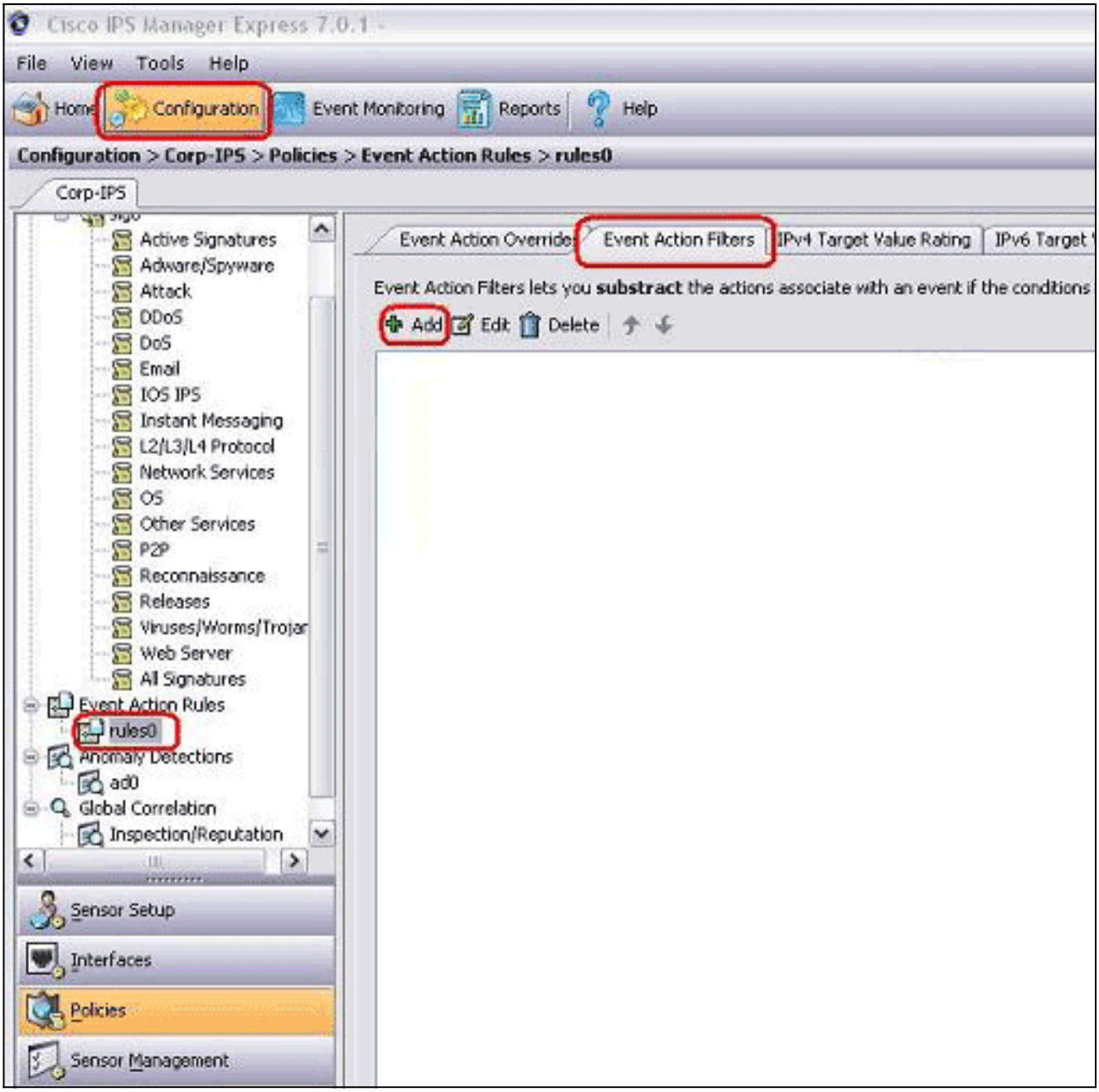
IPS Cisco Secure исключает механизм

IPS Cisco Secure предоставляет возможность исключить определенную подпись от или до определенные адреса узла или сетевые адреса. Исключенные подписи не создают значки аварийного состояния или записи журнала, если они запускаются с хостов или сетей, которые специально исключены с помощью этого механизма. Например, станция управления сетью могла бы выполнить обнаружение сети рабочими развернутая проверками доступности адресата (ping sweep), которые инициируют Получение сетевых настроек ICMP с подписью Эха (идентификатор подписи 2100). При исключении подписи вы не должны проанализировать сигнал тревоги и удалить его каждый раз выполнения процесса обнаружения устройства в сети.

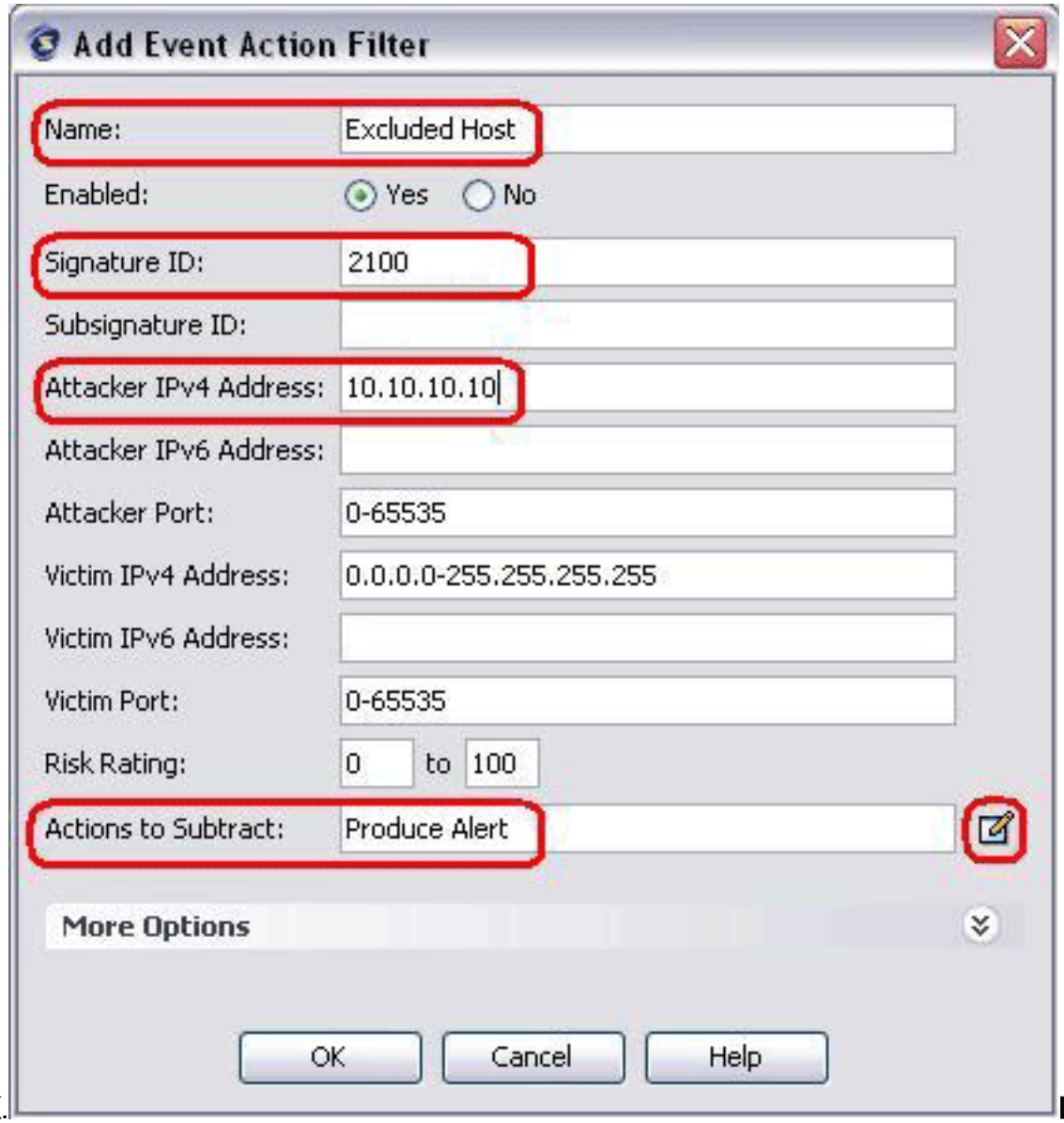
Исключите хост

Выполните эти шаги для исключения определенного хоста (IP - адрес источника) от генерации определенного предупреждения о подписи:

1. Выберите **Configuration> Corp-IPS> Policies> Event Action Rules> rules0** и нажмите вкладку **Event Action**
   Filters.



2. **Нажмите Add.**
3. Введите имя фильтра, идентификатор подписи, адрес IPv4 атакующего и действие, чтобы вычесть в соответствующих полях, и затем нажать



OK.**Примечание:** Если необходимо исключить несколько IP - адресовы из других сетей, можно использовать запятую в качестве разделителя. Однако, если вы используете запятую, избегаете замыкающего пробел после запятой; иначе, вы могли бы получить ошибку.**Примечание:** Кроме того, можно использовать переменные, определенные в конечном счете вкладка Variables. Когда то же значение должно быть повторено в фильтрах действия несколька событий, эти переменные полезны. Необходимо использовать знак доллара ($) в качестве префикса к переменной. Переменная может быть одним из этих форматов:Полный IP-адрес; например, 10.77.23.23.Диапазон IP-адресов; например, 10.9.2.10-10.9.2.155.Набор диапазона IP-адресов; например, 172.16.33.15-172.16.33.100,192.168.100.1-192.168.100.11.

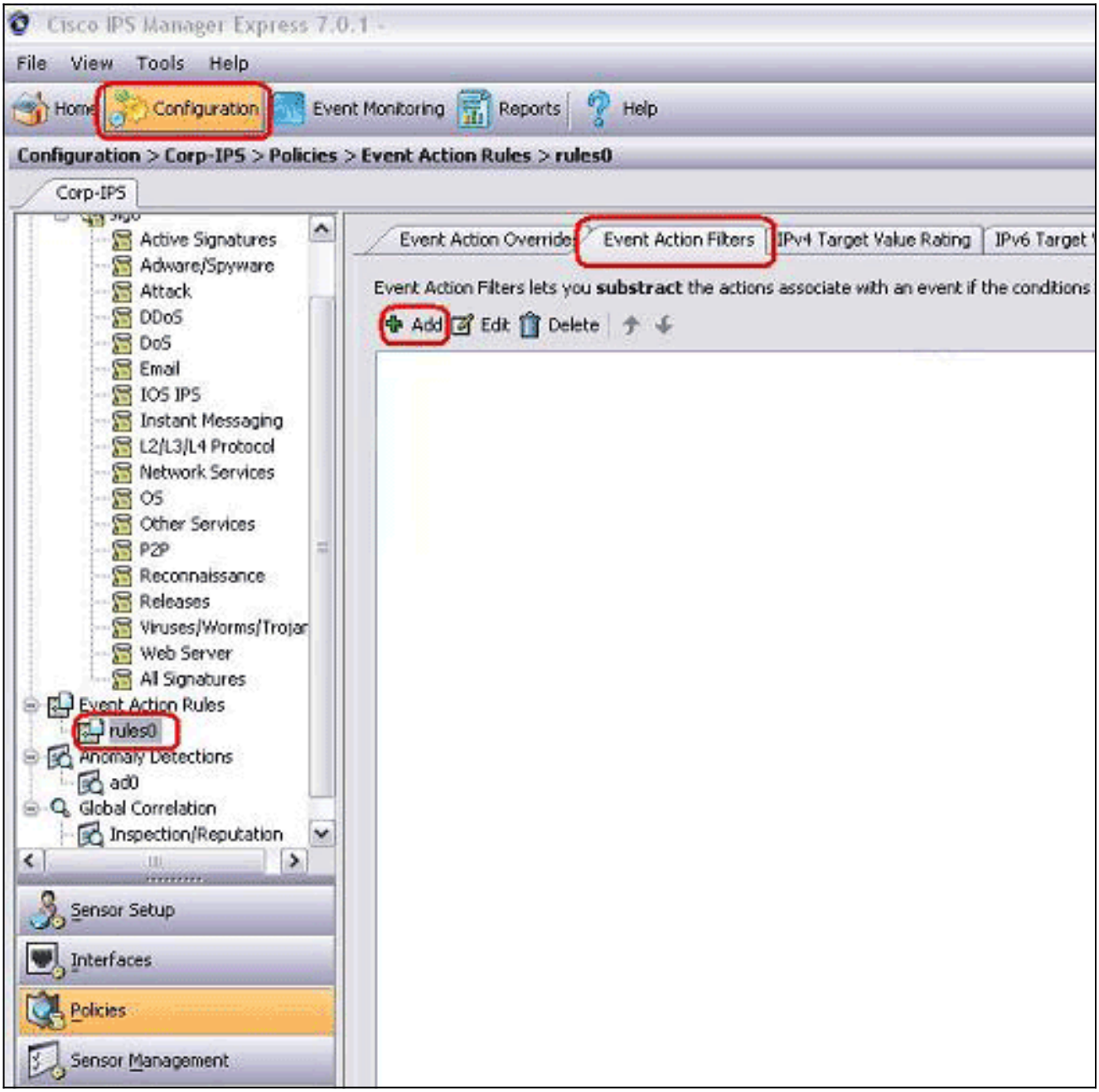
Исключите сеть

Фильтр Действия События также исключает определенные подписи для увольнения сигнала тревоги на основе сетевого адреса источника или назначений.

Выполните эти шаги для исключения сети из генерации определенного предупреждения о подписи:

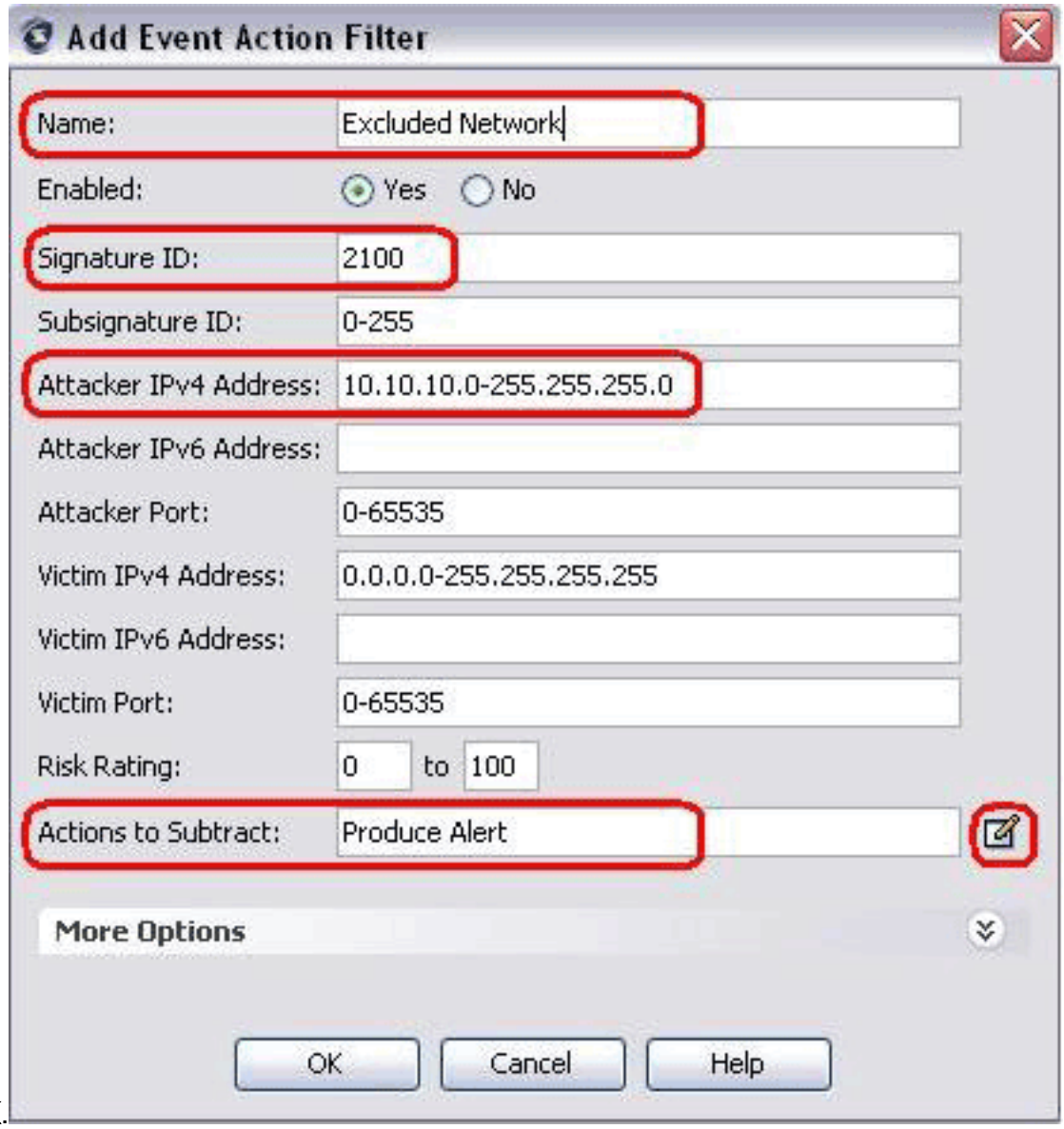
1. Нажмите вкладку **Event Action**

Filters.



2. Нажмите Add.
3. Введите имя фильтра, идентификатор подписи, сетевой адрес с маской подсети и действие, чтобы вычесть в соответствующих полях, и затем нажать

OK.



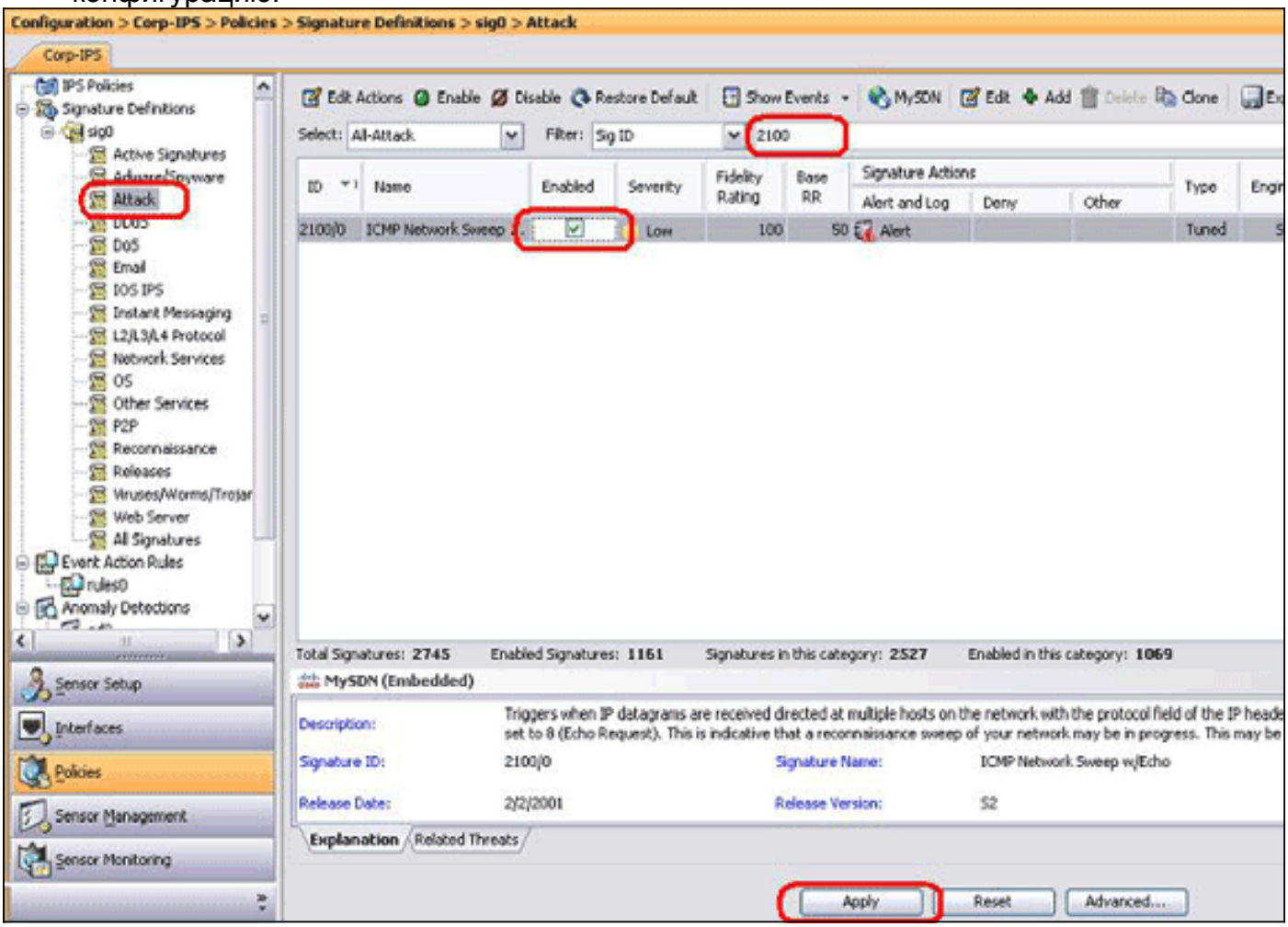
Глобально отключите подписи

Вы могли бы хотеть отключить подпись от аварийной сигнализации в любое время. Для включения отключите, и исключите подписи, выполните эти шаги:

1. Войдите в систему IME использование учетной записи с привилегиями Администратора или Оператора.
2. Выберите **Configuration> sensor_name> Политика> Определения Подписи> sig0> Все Подписи**.
3. Для определения местоположения подписи выберите опцию сортировки из выпадающего списка Фильтра. Например, если вы ищете подпись Получения сетевых настроек ICMP, выбираете **All Signatures** под sig0, затем ищете идентификатором подписи или названием. sig0 разделяют на области обновления и показы только те подписи, которые совпадают с вашими критериями сортировки.
4. Чтобы включить или отключить существующую подпись, выбирает подпись и выполняет эти шаги:Просмотрите столбец Enabled для определения статуса подписи. Подписи, которая включена, проверили флажок.Для включения подписи, которая отключена, проверьте флажок **Enabled**.Для отключения подписи, которая включена, снимите флажок с флажком **Enabled**.Для исключения одной или более подписей

выберите подпись (подписи), щелкните правой кнопкой мыши, и затем нажмите **Change Status To> Retired**.

5. Нажмите **Apply**, чтобы применить ваши изменения и сохранить пересмотренную конфигурацию.



Дополнительные сведения

- Конец продажи для управляющего узла Cisco Secure IDS
- Страница поддержки системы обнаружения несанкционированного доступа Cisco
- Cisco Systems – техническая поддержка и документация