Опции для сокращения проникновений ошибочного допуска

Содержание

Введение

Система предотвращения вторжений может генерировать чрезмерные предупреждения на определенном правиле Фырканья. Предупреждения могли быть истинны положительный или ошибочный допуск. При получении многих предупреждений ошибочного допуска существует несколько опций, доступных для вас для сокращения их. Эта статья предоставляет сводку преимуществ и недостатков каждой опции.

Опции для сокращения предупреждений ошибочного допуска

> **Примечание:** Эти опции обычно являются не лучшим выбором, они могут быть единственным решением при определенных обстоятельствах.

1. Сообщите технической поддержке Cisco

Если вы находите, что Фырканье постановляет, что триггерные предупреждения на мягком трафике, сообщите о нем технической поддержке Cisco. После того, как сообщаемый, Инженер службы поддержки передает проблему Исследовательской группе уязвимости (VRT). Возможные усовершенствования исследований VRT к правилу. Улучшенные правила, как правило, доступны генератору отчетов, как только они доступны, и также добавлены к следующему обновлению официального правила.

2. Доверяйте или позвольте правило

Наилучший вариант для разрешения доверяемого трафика пройти через устройство Sourcefire без контроля включает **Доверие**, или **Позвольте** действие без связанной Политики Проникновения. Чтобы настроить Доверие или Позволить правило, перейдите к **Политике>, Управление доступом> Добавляет Правило**.

Примечание: Трафик, совпадающий с Доверием или, Позволяет правила, которые не настроены для соответствия с Пользователями, Приложениями, или URL будут иметь минимальное воздействие на общей производительности устройства Sourcefire, потому что такие правила могут быть обработаны в аппаратных средствах FirePOWER.

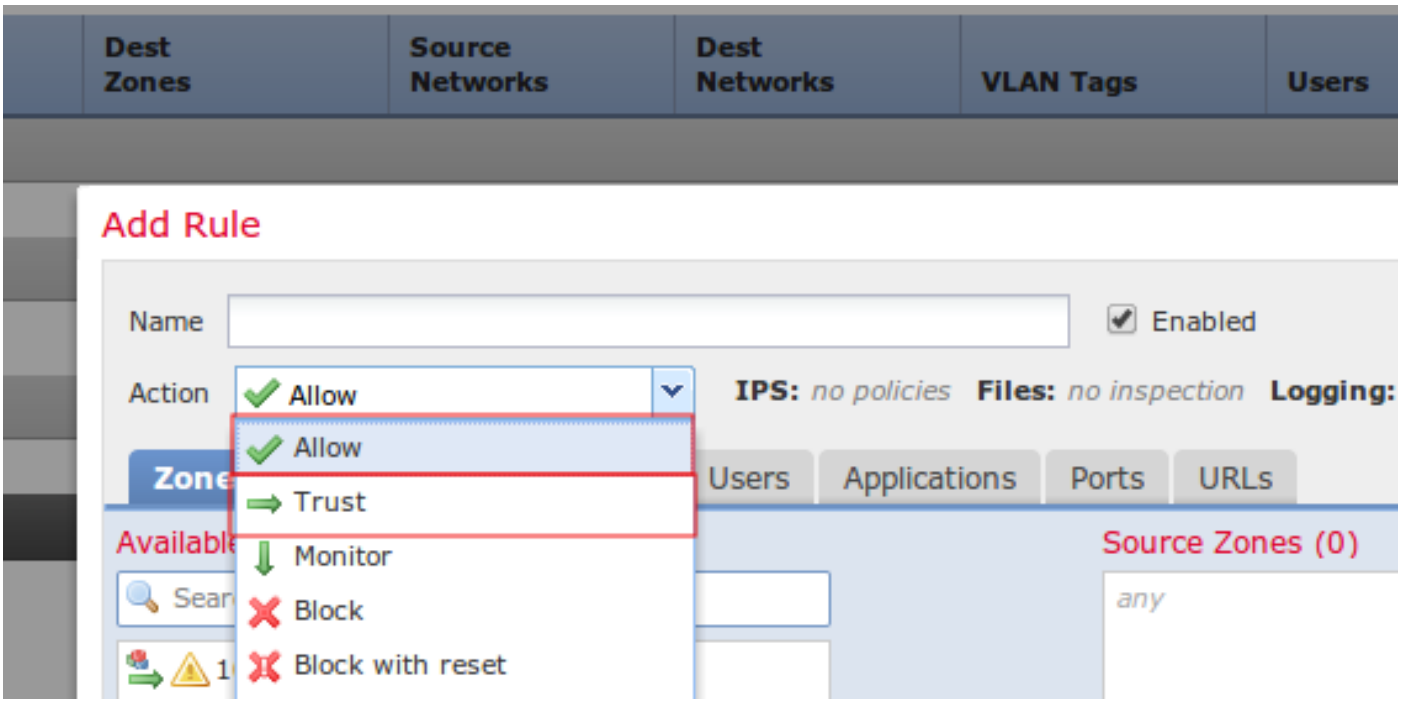

Рисунок: конфигурация трастового правила

3. Отключите ненужные правила

Можно отключить правила Фырканья что целевые старые и исправленные уязвимости. Это улучшает производительность и уменьшает ошибочные допуски. Использование рекомендаций FireSIGHT может помочь с этой задачей. Кроме того, правила, которые часто генерируют предупреждения низкого приоритета или предупреждения, которые не являются преступными, могут быть хорошими кандидатами на удаление из политики Проникновения.

4. Порог

Можно использовать **Порог** для сокращения количества событий проникновения. Это - хорошая опция для настройки, когда правило, как ожидают, регулярно инициирует ограниченное число событий на обычном трафике, но могло быть индикацией относительно проблемы, если больше, чем определенное число пакетов совпадут с правилом. Можно использовать эту опцию для сокращения количества событий, инициированных шумными правилами.

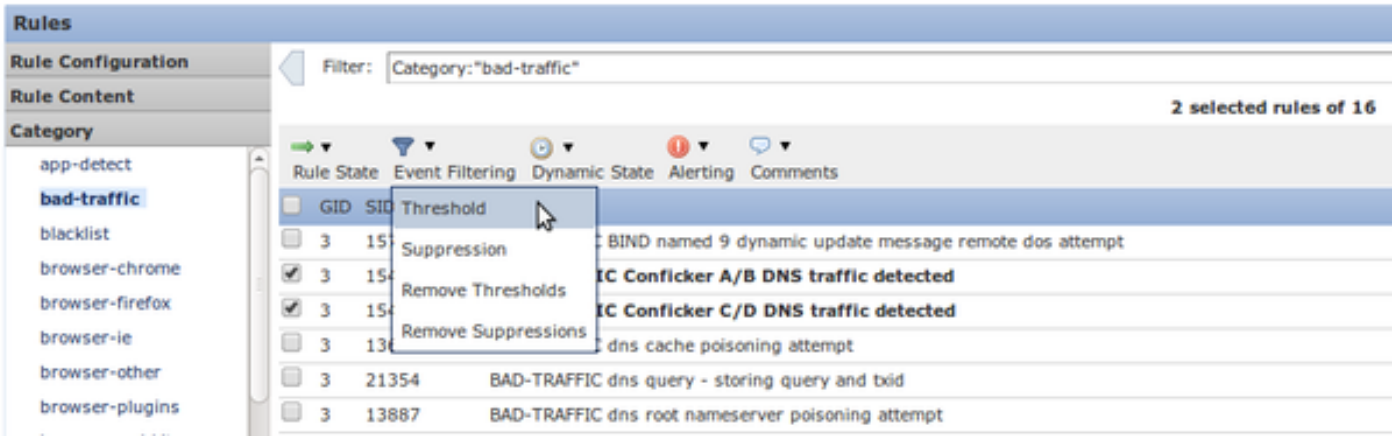

Рисунок: конфигурация порога

5. Подавление

Можно использовать **Подавление** для завершенного устранения уведомления о событиях. Это настроено подобное **опции Threshold**.

> **Внимание. :** Подавление может вести проблемы производительности, потому что, в то время как никакие события не генерируются, Фырканье все еще должно обработать трафик.

> **Примечание:** Подавление не препятствует правилам отбрасывания отбросить трафик, таким образом, трафик может быть тихо отброшен, когда это совпадает с правилом отбрасывания.

6. Правила Fast-Path

Подобный, чтобы Доверять и Позволить правила Политики контроля доступа, правила Fast-Path могут также контроль обходов. Техническая поддержка Cisco обычно не рекомендует использовать правила Fast-Path, потому что они настроены в окне **Advanced** страницы **Device** и могут быть легко пропущены, в то время как правила Управления доступом почти всегда достаточны.

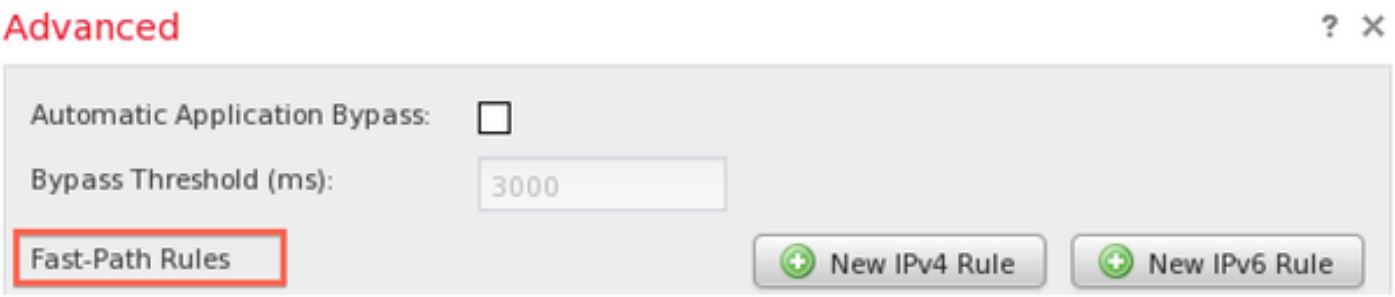

Рисунок: опция Fast-Path Rules в окне Advanced.

Единственное преимущество для использования правил fast-path состоит в том, что они могут обработать большую максимальную громкость трафика. Трафик процесса правил fast-path в аппаратном уровне (известный как NMSB) и может теоретически обработать до 200 Гбит/с трафика. Напротив, правила с **Доверием** и **Позволяют**, что действиям способствуют

на Механизм сетевого потока (NFE) и могут обработать максимум 40 Гбит/с трафика.

Примечание: Правила Fast-Path только доступны на устройствах серии 8000 и 3D9900.

7. Правила прохода

Для препятствования определенному правилу включить трафик от определенного хоста (в то время как другой трафик от того хоста должен быть осмотрен), используйте правило Фырканья типа *прохода.* Фактически, это - единственный способ выполнить его. В то время как правила прохода являются эффективными, их может быть очень трудно поддержать, потому что вручную записаны правила прохода. Кроме того, если исходные правила правил прохода модифицируются обновлением правила, все связанные правила прохода должны быть обновлены вручную. В противном случае они могут стать неэффективными.

8. Переменная SNORT_BPF

Переменная `Snort_BPF` в политике проникновения позволяет определенному трафику обойти контроль. В то время как эта переменная была одним из предпочтительных вариантов на версиях наследуемого программного обеспечения, техническая поддержка Cisco рекомендует использовать правило Политики контроля доступа обойти контроль, потому что это более гранулировано, более видимо, и намного легче настроить.