Содержание

[Введение](#)
[Предварительные условия](#)
[Требования](#)
[Используемые компоненты](#)
[Общие сведения](#)
[Включите встроенную нормализацию](#)
[Включите встроенную нормализацию в версиях 5.4 и позже](#)
[Включите встроенную нормализацию в версиях 5.3 и ранее](#)
[Включите контроль пост-ACK и контроль предACK](#)
[Поймите Контроль пост-ACK (Нормализуйте Отключенное Содержимое tcp TCP/Нормализовать),](#)
[Поймите Контроль предACK (Нормализуйте Включенное Содержимое tcp TCP/Нормализовать),](#)

Введение

Этот документ описывает, как включить встроенный препроцессор нормализации и помогает вам понимать различие и влияние двух расширенных настроек встроенной нормализации.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с системой Огневой мощи Cisco и Фырканьем.

Используемые компоненты

Сведения в этом документе основываются на устройствах Центра управления и Огневой мощи Cisco FireSIGHT.

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.

Общие сведения

Встроенный препроцессор нормализации нормализует трафик для сведения к минимуму вероятности, что атакующий может уклониться от обнаружения с помощью встроенных развертываний. Нормализация сразу происходит после пакетного декодирования и перед любыми другими препроцессорами и продолжается из внутренних уровней исходящего пакета. Встроенная нормализация не генерирует события, но она готовит пакеты к использованию другими препроцессорами.

При применении политики проникновения со встроенным включенным препроцессором нормализации устройство Огневой мощи тестирует эти два условия, чтобы гарантировать, что вы используете встроенные развертывания:

- Для Версий 5.4 и позже, *Встроенный Режим* включен в Политике анализа сети (NAP), и *Отбрасывание, когда Встроенный* также настроено в политике проникновения, если политика проникновения собирается отбросить трафик. Для Версий 5.3 и ранее, *Отбрасывание, когда* опция *Inline* включена в политике проникновения.

- Политике применяются к встроенное (или встроенная с failopen) интерфейсный набор.

Поэтому в дополнение к включению и конфигурации встроенного препроцессора нормализации, необходимо также гарантировать, что эти требования удовлетворены, или препроцессор не нормализует трафик:

- Ваша политика должна собираться отбросить трафик во встроенных развертываниях.

- Необходимо применить политику к встроенному набору.

Включите встроенную нормализацию

В этом разделе описывается включить встроенную нормализацию для Версий 5.4 и позже, и также для Версий 5.3 и ранее.

Включите встроенную нормализацию в версиях 5.4 и позже

Большинство параметров настройки препроцессора настроено в NAP для Версий 5.4 и позже. Выполните эти шаги для включения встроенной нормализации в NAP:

1. Войдите к веб-UI вашего Центра управления FireSIGHT.

2. Перейдите к **Политике> Управление доступом**.

3. Нажмите **Network Analysis Policy** около верхней правой области страницы.

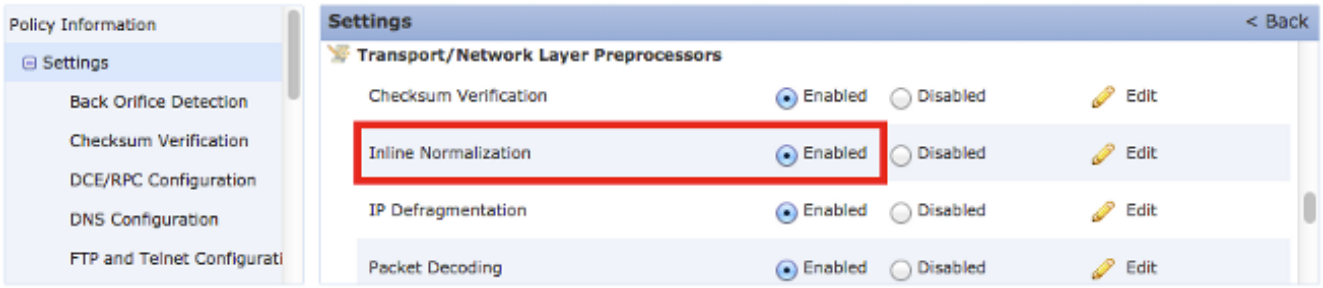
4. Выберите *Network Analysis Policy*, что вы хотите примениться к своему управляемому устройству.

5. Нажмите *значок карандаша* для начала редактирования, и *страница Policy Редактирования* появляется.

6. Нажмите **Settings** на левой части экрана, и *Страница настроек* появляется.

7. Найдите **Встроенную опцию Normalization** в области *Transport/Network Layer Preprocessor*.

8. Установите переключатель **Enabled** для активации этой опции:



NAP со встроенной нормализацией должен быть добавлен к вашей политике контроля доступа для встроенной нормализации для появления. NAP может быть добавлен через политику контроля доступа *Вкладка Дополнительно*:

Политика контроля доступа должна тогда быть применена к устройству осмотра.

> **Примечание:** Для Версии 5.4 или позже, можно включить встроенную нормализацию для определенного трафика и отключить его для другого трафика. Если вы хотите включить его для определенного трафика, добавьте *правило анализа сети* и установите критерии трафика и политику к той, которая имеет встроенную включенную нормализацию. Если вы хотите включить его глобально, то установленный *аналитическая политика сети по умолчанию* в ту, которая имеет встроенную нормализацию, включила.

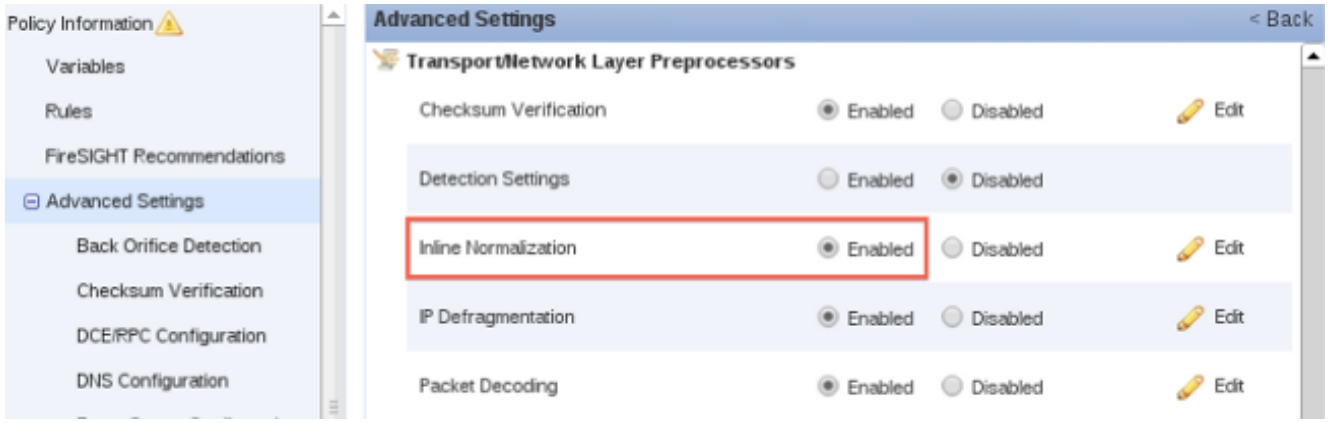
Включите встроенную нормализацию в версиях 5.3 и ранее

Выполните эти шаги для включения встроенной нормализации в политике проникновения:

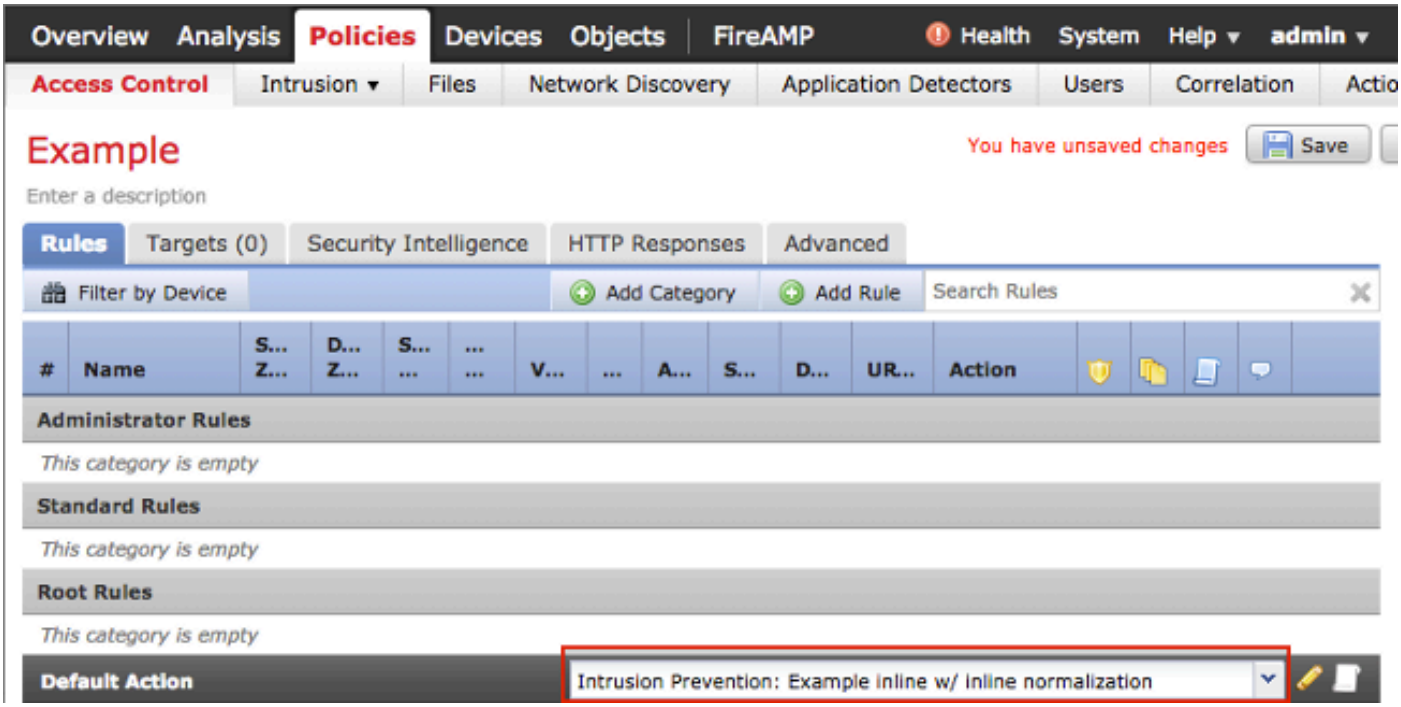
1. Войдите к веб-UI вашего Центра управления FireSIGHT.
2. Перейдите к **Политике> Проникновение> Политика Проникновения**.
3. Выберите *политику проникновения*, что вы хотите примениться к своему управляемому устройству.
4. Нажмите *значок карандаша* для начала редактирования, и *страница Policy Редактирования* появляется.
5. Нажмите **Advanced Settings**, и страница ***Advanced Settings*** появляется.

6. Найдите **Встроенную опцию Normalization** в области *Transport/Network Layer Preprocessor*.

7. Установите переключатель **Enabled** для активации этой опции:



Как только политика проникновения настроена для встроенной нормализации, это должно быть добавленный как действие по умолчанию в политике контроля доступа:



Политика контроля доступа должна тогда быть применена к устройству осмотра.

Можно настроить встроенный препроцессор нормализации для нормализации IPv4, IPv6, Версии 4 (ICMPv4), ICMPv6 Internet Control Message Protocol и Трафика TCP в любой комбинации. Когда та нормализация протокола включена, нормализация каждого протокола происходит автоматически.

Включите контроль пост-ACK и контроль предACK

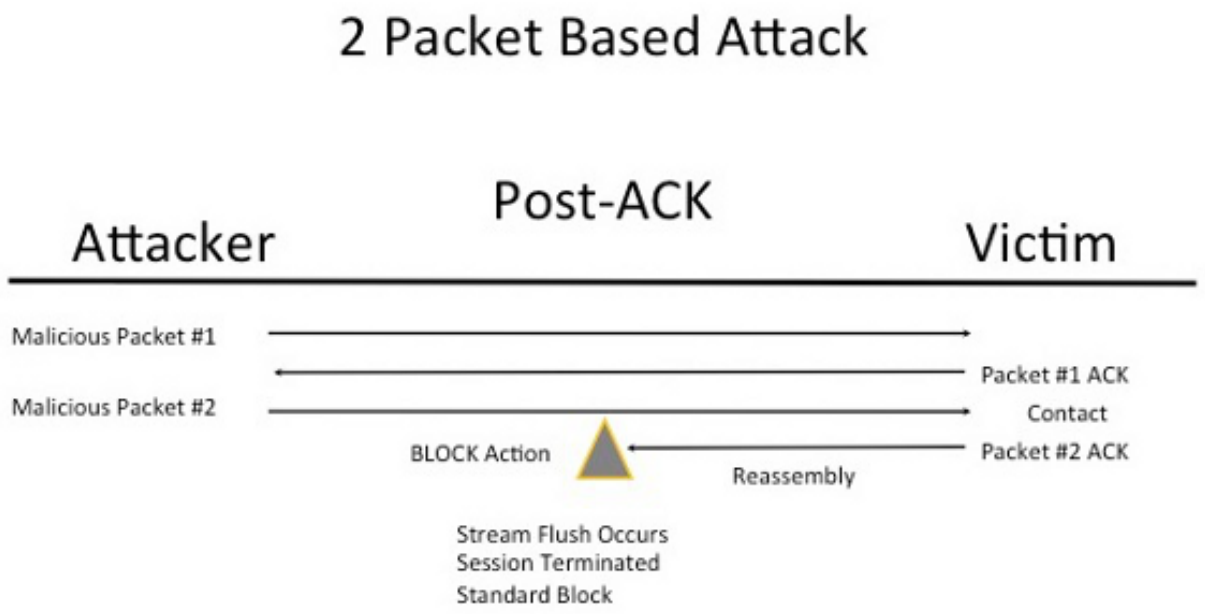
После включения встроенного препроцессора нормализации можно отредактировать параметры настройки для включения опции *Normalize TCP Payload*. Эта опция во встроенном препроцессоре нормализации переключается между двумя другими режимами

контроля:

- Почтовое подтверждение (пост-ACK)
- Пред подтверждение (предACK)

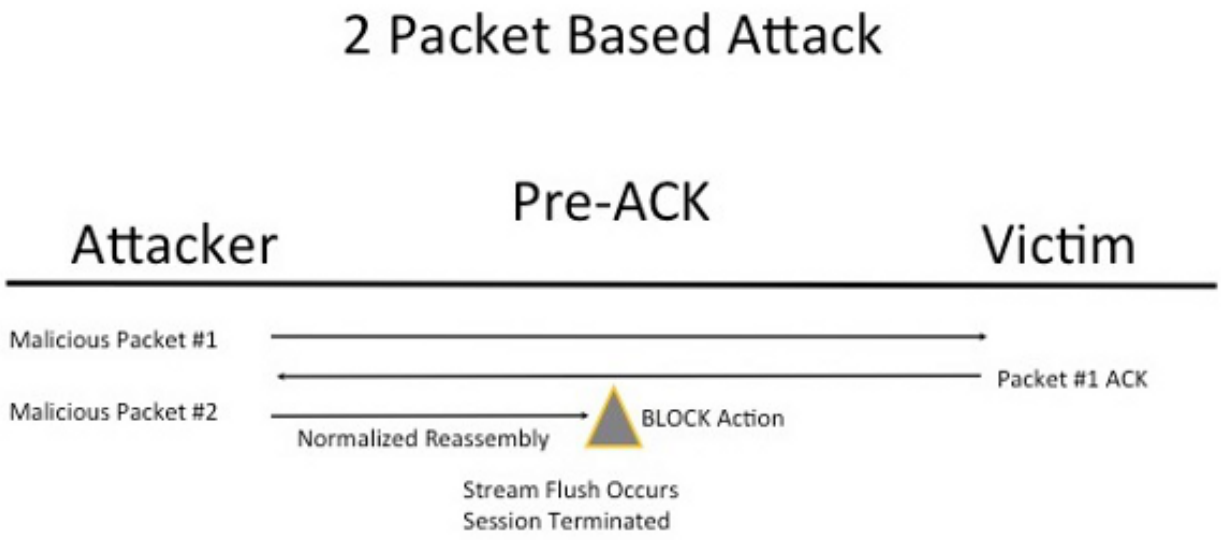
Поймите Контроль пост-ACK (Нормализуйте Отключенное Содержимое tcp TCP/Нормализовать),

В контроле пост-ACK, повторной сборке потока пакетов, сброс (передают к остатку инспекционного процесса) и обнаружение в Фырканье происходит после того, как подтверждение (ACK) от жертвы к пакету, который завершает атаку, получено Системой предотвращения вторжений (IPS). Прежде чем потоковый сброс происходит, незаконный пакет уже достиг жертвы. Поэтому предупреждение/отбрасывание происходит после того, как незаконный пакет достиг жертвы. Когда ACK от жертвы к незаконному пакету достигает IPS, это действие происходит.



Поймите Контроль предACK (Нормализуйте Включенное Содержимое tcp TCP/Нормализовать),

Эта функция сразу нормализует трафик после пакетного декодирования и прежде чем любая другая функция Snort будет обработана для уменьшения усилий по уклонению TCP. Это гарантирует, что пакеты, достигающие IPS, совпадают с теми, которые переданы жертве. Фырканье отбрасывает трафик на пакете, который завершает атаку, прежде чем атака достигнет своей жертвы.



Когда вы включаете*, Нормализуют TCP*, трафик, который совпадает с этими условиями, также отброшен:

- Ретранслируемые копии ранее отброшенных пакетов
- Трафик, который пытается продолжить ранее отброшенный сеанс
- Трафик, который совпадает с любым из этих потоковых правил препроцессора TCP:

  129:1129:3129:4129:6129:8129:11129:14 через 129:19

  Примечание: Для включения предупреждений для потоковых правил TCP, которые отброшены препроцессором нормализации, необходимо активировать опцию *Аномалий Проверки трафика потоком* в потоковой конфигурации TCP.