ZBFW для руководства устранения неполадок конфигурации XE IOS

Содержание

Введение

Этот документ описывает, как лучше всего устранить неполадки Зонального Базирующегося Межсетевого экрана (ZBFW) функция на Маршрутизаторе агрегации (ASR) 1000 с командами, которые используются для опроса аппаратных счетчиков сбросов на ASR. ASR1000 является аппаратной передающей платформой. Конфигурация ПО Cisco IOS-XE® программирует аппаратные специализированные интегральные схемы (квантовый процессор потока (QFP) для выполнения передающей функциональности функции. Это обеспечивает более высокую пропускную способность и лучшую производительность. Недостаток к этому - то, что это представляет собой большую проблему для устранения проблем. Традиционные Команды Cisco IOS использовали опрашивать текущие сеансы, и счетчики сбросов через зональный Межсетевой экран (ZBFW) больше не действительны, поскольку отбрасывания больше не находятся в программном обеспечении.

Ссылки и документация

Справочники по командам

- Справочники по командам сервисных маршрутизаторов агрегации Cisco ASR серии 1000
- Cisco IOS XE 3S Справочники по командам

Шаги устранения неполадок канала передачи данных

Для устранения проблем канала передачи данных необходимо определить, передают ли трафик должным образом через код Cisco IOS XE и ASR. Определенный для характеристик межсетевого экрана, устранение проблем канала передачи данных выполняет эти действия:

1. **Проверьте, что Конфигурация** - Собирает конфигурацию и исследует выходные данные для проверки соединения.

2. **Проверьте Состояние соединения** - Если трафик проходит должным образом, Cisco IOS XE открывает соединение на функции ZBFW. Это соединение отслеживает трафик и информацию о состоянии между клиентом и сервером.

3. **Проверьте Счетчики сбросов** - Когда трафик не проходит должным образом, Cisco IOS XE регистрирует счетчик сбросов для любых отброшенных пакетов. Проверьте эти выходные данные для изоляции причины сбоя трафика.

4. **Регистрация** - Собирает системные журналы для предоставления большей гранулированной информации о сборках соединения и отбрасывании пакета.

5. **Отброшенные пакеты Трассировки пакетов** - пакетное отслеживание Использования для ловли отброшенных пакетов.

6. **Отладки** - Заключают, что отладки являются большей частью подробного варианта. Отладки могут быть получены условно для подтверждения точного пути переадресации для пакетов.

Проверка конфигурации

Выходные данные **межсетевого экрана поддержки покажите технологию** суммированы здесь:

```
-------- show clock --------
-------- show version -------
-------- show running-config --------
-------- show parameter-map type inspect --------
-------- show policy-map type inspect -------
-------- show class-map type inspect --------
-------- show zone security --------
-------- show zone-pair security --------
-------- show policy-firewall stats global --------
-------- show policy-firewall stats zone --------
-------- show platform hardware qfp active feature firewall datapath <submode> --------
```

```
-------- show platform software firewall RP <submode> --------
```

Проверьте состояние соединения

Информация о соединении может быть получена так, чтобы были перечислены все соединения на ZBFW. Введите эту команду:

```
ASR#show policy-firewall sessions platform
--show platform hardware qfp active feature firewall datapath scb any any any any any all any --
[s=session i=imprecise channel c=control channel d=data channel]
 14.38.112.250 41392 14.36.1.206 23 proto 6 (0:0)   [sc]
```

Это показывает соединение TELNET TCP от 14.38.112.250 до 14.36.1.206.

> **Примечание:** Знайте, что, если вы выполняете эту команду, будет требоваться много времени, если будет много соединений на устройстве. Cisco рекомендует выполнить эту команду с определенными фильтрами, как выделено здесь.

Таблица подключений может быть отфильтрована к определенному адресу источника или назначения. Используйте фильтры после подрежима **платформы**. Опции для фильтрации:

```
radar-ZBFW1#show policy-firewall sessions platform ?
 all                     detailed information
 destination-port        Destination Port Number
 detail                  detail on or off
 icmp                    Protocol Type ICMP
 imprecise               imprecise information
 session                 session information
 source-port             Source Port
 source-vrf              Source Vrf ID
 standby                 standby information
 tcp                     Protocol Type TCP
 udp                     Protocol Type UDP
 v4-destination-address IPv4 Desination Address
 v4-source-address       IPv4 Source Address
 v6-destination-address IPv6 Desination Address
 v6-source-address       IPv6 Source Address
 |                       Output modifiers
 <cr>
```

Эта таблица подключений фильтруется поэтому, только соединения, полученные от 14.38.112.250, отображены:

```
ASR#show policy-firewall sessions platform v4-source-address 14.38.112.250
--show platform hardware qfp active feature firewall datapath scb 14.38.112.250
any any any any all any --
[s=session i=imprecise channel c=control channel d=data channel]
 14.38.112.250 41392 14.36.1.206 23 proto 6 (0:0)   [sc]
```

Как только таблица подключений фильтруется, подробная информация о соединении может быть получена для более всестороннего анализа. Для отображения этих выходных данных используйте **подробное** ключевое слово.

```
ASR#show policy-firewall sessions platform v4-source-address 14.38.112.250 detail
--show platform hardware qfp active feature firewall datapath scb 14.38.112.250
any any any any all any detail--
[s=session i=imprecise channel c=control channel d=data channel]
 14.38.112.250 41426 14.36.1.206 23 proto 6 (0:0)      [sc]
 pscb : 0x8c5d4f20, bucket : 64672, fw_flags: 0x204 0x20419441,
```

```
      scb state: active, scb debug: 0
nxt_timeout: 360000, refcnt: 1, ha nak cnt: 0, rg: 0, sess id: 117753
hostdb: 0x0, L7: 0x0, stats: 0x8e118e40, child: 0x0
l4blk0: 78fae7a7 l4blk1: e36df99c l4blk2: 78fae7ea l4blk3: 39080000
l4blk4: e36df90e l4blk5: 78fae7ea l4blk6: e36df99c l4blk7: fde0000
l4blk8: 0 l4blk9: 1
root scb: 0x0 act_blk: 0x8e1115e0
ingress/egress intf: GigabitEthernet0/0/2 (1021), GigabitEthernet0/0/0 (131065)
current time 34004163065573 create tstamp: 33985412599209 last access: 33998256774622
nat_out_local_addr:port: 0.0.0.0:0 nat_in_global_addr:port: 0.0.0.0:0
syncookie fixup: 0x0
halfopen linkage: 0x0 0x0
cxsc_cft_fid: 0x0
tw timer: 0x0 0x0 0x372ba 0x1e89c181
Number of simultaneous packet per session allowed: 25
  bucket 125084 flags 1 func 1 idx 8 wheel 0x8ceb1120
```

Проверьте счетчики сбросов межсетевого экрана

Счетчик сбросов вывел измененный во время XE 3.9. Перед XE 3.9 причины отбрасывания межсетевого экрана были очень общего назначения. После XE 3.9 причины отбрасывания межсетевого экрана были расширены для становления более гранулированными.

Для проверки счетчиков сбросов выполните два шага:

1. Подтвердите глобальные счетчики сбросов в Cisco IOS XE. Эти счетчики показывают, какая функция отбросила трафик. Примеры функций включают Качество обслуживания (QoS), Технологию NAT, Межсетевой экран, и так далее.

2. Как только подфункция была определена, сделайте запрос гранулированных счетчиков сбросов, предлагаемых подфункцией. В этом руководстве проанализированной подфункцией является Характеристика межсетевого экрана.

Глобальные счетчики сбросов на QFP

Основная команда для доверия предоставляет все отбрасывания через QFP:

```
Router#show platform hardware qfp active statistics drop
```

Эта команда показывает вам отбрасывания общего назначения глобально через QFP. Эти отбрасывания могут быть на любой функции. Некоторые функции в качестве примера:

```
Router#show platform hardware qfp active statistics drop
```

Для наблюдения всех отбрасываний включайте счетчики, которые имеют значение нуля, используют команду:

```
show platform hardware qfp active statistics drop all
```

Для очистки счетчиков используйте эту команду. Это очищает выходные данные после показа его на экран. Эта команда ясна на чтении, таким образом, выходные данные перезагружены для обнуления **после того, как** это отображено на экран.

```
show platform hardware qfp active statistics drop all
```

Ниже список глобальных счетчиков сбросов межсетевого экрана QFP и пояснение:

Глобальная причина	Пояснение

отбрасывания межсетевого экрана	
FirewallBackpressure	Отбрасывание пакета из-за противодавления путем регистрации механизма.
FirewallInvalidZone	Никакая зона безопасности не настроена для интерфейса.
FirewallL4Insp	Политика L4 проверяет сбой. Посмотрите таблицу ниже по большему количеству гранулированных причин отбрасывания (Причины отбрасывания характеристики межсетевого экрана).
FirewallNoForwardingZone	Межсетевой экран является неинициализированным, и "no traffic" (нету трафика) позволяют пройти.
FirewallNonsession	Сбои создания сеанса. Это могло произойти из-за предела максимального числа сеансов, достиг или ошибка выделения памяти.
Firewall policy	Настроенная Политика межсетевого экрана является отбрасыванием.
FirewallL4	Сбой контроля L4. Посмотрите таблицу ниже по большему количеству гранулированных причин отбрасывания (Причины отбрасывания характеристики межсетевого экрана).
FirewallL7	Отбрасывание пакета из-за контроля L7. Посмотрите ниже для списка большего количества гранулированных причин отбрасывания L7 (Причины отбрасывания характеристики межсетевого экрана).
FirewallNotInitiator	Не инициатор сеанса или для TCP, UDP или для ICMP. Никакой сеанс не создан. Например, для ICMP первым полученным пакетом не является ECHO или МЕТКА ВРЕМЕНИ. Для TCP это не SYN. Это могло произойти в обработке стандартного пакета или неточной обработке канала.
FirewallNoNewSession	Высокая доступность межсетевого экрана не позволяет новые сеансы.
FirewallSyncookieMaxDst	Для обеспечения основанной на хосте защиты от переполнения SYN существует для каждого назначения скорость SYN как предел атаки SYN flood. Когда количество записей назначения достигает предела, новые SYN - пакеты отброшены.
FirewallSyncookie	Логика SYNCOOLIE инициирована. Это указывает, что SYN/ACK с cookie SYN передавался, и исходный SYN - пакет отброшен.
FirewallARStandby	Асимметричная маршрутизация не включена, и Группа резервирования не находится в активном состоянии.

Счетчики сбросов характеристики межсетевого экрана на QFP

Ограничение с глобальным счетчиком сбросов QFP - то, что нет никакой глубины детализации в причинах отбрасывания, и некоторые причины отбрасывания, такие как **FirewallL4** становятся настолько перегруженными до такой степени, что это мало полезно для устранения проблем. Это было с тех пор улучшено в Cisco IOS XE 3.9 (15.3 (2) S), где были добавлены счетчики сбросов Характеристики межсетевого экрана. Это дает намного больше гранулированного набора причин отбрасывания:

```
ASR#show platform hardware qfp active feature firewall drop all
-----------------------------------------------------------------------------
Drop Reason Packets
-----------------------------------------------------------------------------
Invalid L4 header 0
Invalid ACK flag 0
```

```
Invalid ACK number 0
....
```

Ниже список причин отбрасывания Характеристики межсетевого экрана и пояснения:

Причина отбрасывания характеристики межсетевого экрана	Пояснение
Недопустимая Длина заголовка	Дейтаграмма является столь маленькой, что она не могла содержать уровень 4TCP, UDP или Заголовок ICMP. Это могло быть вызвано: 1. Длина заголовка TCP <20 2. Длина заголовка UDP/ICMP <8
Недопустимая длина данных UDP	Длина дейтаграммы UDP не совпадает с длиной, заданной в заголовке UDP.
Недопустимый номер ACK	Это отбрасывание могло быть вызвано одной из этих причин: 1. ACK не равняется next_seq# узла TCP. 2. ACK больше, чем новый SEQ#, передаваемый узлом TCP. В SYNSENT TCP и состоянии SYNRCVD, ожидается, что ACK# равен ISN+1, но это не.
Недопустимый флаг ACK	Это отбрасывание могло быть вызвано одной из этих причин: 1. Флаг Expecting ACK, но "not set" в другом состоянии TCP. 2. Кроме флага ACK, также установлен другой флаг (как RST).
Недопустимый инициатор TCP	Это происходит когда: 1. Первый пакет от инициатора TCP не является SYN (Сегмент TCP Неначальных получен без действительного сеанса). 2. Начальному SYN - пакету установили флаг ACK.
SYN с данными	SYN - пакет содержит информационное наполнение. Это не поддерживается.
Недопустимые флаги TCP	Недопустимые флаги TCP могут быть вызваны: 1. SYN - пакет начальной буквы TCP имеет флаги кроме SYN. 2. В TCP слушают состояние, узел TCP получает RST или ACK. 3. Пакет другого респондента получен перед SYN/ACK. 4. Ожидаемый SYN/ACK не получен от респондента.
Недопустимый Сегмент в состоянии SYNSENT	Недопустимый сегмент TCP в состоянии SYNSENT вызван: 1. SYN/ACK имеет информационное наполнение. 2. SYN/ACK имеет другие флаги (PSH, URG, FIN) набор. 3. Получите транзитный SYN с информационным наполнением. 4. Получите не-SYN - пакет от инициатора.
Недопустимый Сегмент в состоянии SYNRCVD	Недопустимый сегмент TCP в состоянии SYNRCVD мог быть вызван: 1. Получите перетранзитный SYN с информационным наполнением от инициатора. 2. Получите недопустимый сегмент, который не является SYN/ACK, RST или FIN от респондента.
Недопустимый SEQ	Когда сегменты прибывают от инициатора, это происходит в состоянии SYNRCVD. Это вызвано: 1. Seq# является меньше, чем ISN. 2. Если размер окна rcvd получателя 0 и: Сегмент имеет информационное наполнение, или

	Неисправный сегмент (seq# больше, чем LASTACK получателя. 3. Если размер окна rcvd получателя 0 и падения seq# вне окна. 4. Seq# равняется ISN, но не SYN - пакету.
Недопустимая опция масштаба окна	Недопустимая опция масштаба окна TCP вызвана неправильной длиной байта опции масштаба окна.
TCP из окна	Пакет слишком стар - одно окно позади ACK другой стороны. Это могло произойти в УСТАНОВЛЕННОМ, CLOSEWAIT и состоянии LASTACK.
TCP дополнительное информационное наполнение после FIN передан	Информационное наполнение, полученное после FIN, передано. Это могло произойти в состоянии CLOSEWAIT.
Переполнение окна TCP	Когда входящий размер сегмента переполняет окна получателя, это происходит. Однако, если vTCP включен, это условие позволено, потому что межсетевой экран должен буферизовать сегмент для ALG для потребления позже.
Retran с недопустимыми флагами	Ретранслируемый пакет был уже подтвержден получателем.
TCP неисправный Сегмент	Поврежденный пакет собирается быть отправленным L7 для контроля. Если L7 не позволит сегмент OOO, то этот пакет будет отброшен.
Атака SYN	Под синхронной атакой TCP. При определенных условиях, когда текущие соединения к этому хосту превысит настроенное полуоткрытое значение, межсетевой экран отклонит любые новые соединения к этому IP-адресу сроком на время. В результате пакеты будут отброшены.
Внутренний Err - synflood проверяет Отказавшее распределение	Во время проверки synflood, выделения сбоев hostdb. Рекомендуемое действие: проверьте "show platform hardware qfp активная память межсетевого экрана функции" для проверки статуса памяти.
Отбрасывание отключения питания Synflood	Если настроенные полуоткрытые соединения превышены, и время отключения питания настроено, все новое соединение к этому IP-адресу отброшены.
Полуоткрытый предел сеанса превышает	Пакет понизился из-за позволенных превышенных частично открытых сеансов. Также проверьте параметры настройки "max-incomplete высокий/низкий" и "одна минута высокий/низкий", чтобы удостовериться, что # частично открытых сеансов не регулируют эти конфигурации.
Слишком многие Pkt на поток	Максимальное число inspectable пакетов, позволенных на поток, превышено. Максимальное число равняется 25.
Слишком много пакетов ошибки ICMP на поток	Максимальное число пакетов ошибки ICMP, позволенных на поток, превышено. Максимальное число равняется 3.
Не ожидайте Содержимое tcp от Rsp до Init	В состоянии SYNRCVD TCP получает пакет с информационным наполнением от респондента к направлению инициатора.
Внутренняя ошибка - неопределенное направление	Неопределенное направление пакетов.

SYN в текущем окне	SYN - пакет замечен в окне уже установленного TCP - подключения.
RST в текущем окне	Пакет RST наблюдается в окне уже установленного TCP - подключения.
Случайный сегмент	Сегмент TCP получен, который не должен был быть получен через машину состояния TCP, такую как Пакет TCP SYN, получаемый в слушать состоянии от респондента.
Внутренняя ошибка ICMP - Пропущенный ICMP информация NAT	Пакет ICMP является nat'ed, но отсутствует внутренняя информация NAT. Это - внутренняя ошибка.
Пакет ICMP в SCB закрывает состояние	Полученный пакет ICMP в SCB ЗАКРЫВАЮТ состояние.
Пропущенный IP - заголовок в пакете ICMP	Недостающий IP - заголовок в пакете ICMP.
Ошибка ICMP никакой IP или ICMP	Пакет ошибки ICMP без IP или ICMP в информационном наполнении. Вероятно, вызванный неправильном сформированным пакет или атакой.
Pkt Err ICMP также короткое замыкание	Пакет Ошибки ICMP слишком короток.
Err ICMP превышает пакетный предел	Ошибка ICMP PKT превышает пакетный предел 10.
Недостижимый Err ICMP	Ошибка ICMP недостижимое PKT превышает предел. Только 1-му недостижимому пакету позволяют пройти.
Err ICMP недопустимый Seq#	Seq# встроенного пакета не совпадает с seq# пакета, который инициирует ошибку ICMP.
Err ICMP недопустимый Ack	Недопустимый ACK в Ошибке ICMP встроил пакет.
Отбрасывание действия ICMP	Настроенное действие ICMP является отбрасыванием.
Зонально-парный без policy-map	Политика, не существующая на зонально-парном. это могло произойти из-за ALG (Шлюз уровня приложения), не настраиваемый для открытия крошечного отверстия для канала данных прикладной программы, или ALG не открыл крошечное отверстие правильно, или никакое крошечное отверстие не открыто из-за проблем масштабирования.
Пропущенный сеанс и политика, не существующая	Поиск сеанса отказал, и никакая политика не присутствует для осмотра этого пакета.
Ошибка ICMP и политика, не существующая	Ошибка ICMP без политики, настроенной на зонально-парном.
Отказавшая классификация	Сбой классификации в данной зональной паре, когда Межсетевой экран пытается определить, inspectable ли протокол.
Отбрасывание действия	Действие классификации является отбрасыванием.

классификации	
Политика безопасности Misconfig	Отказавшая классификация из-за неверной конфигурации политики безопасности. Это не могло также произойти ни из-за какого pinpole для канала данных L7.
Передайте RST респонденту	Передайте RST респонденту в состоянии SYNSENT, когда ACK# не будет равен ISN+1.
Отбрасывание политики межсетевого экрана	Действие политики должно понизиться.
Отбрасывание фрагмента	Фрагменты оставлений отбрасывания, когда отброшен первый фрагмент.
ICMP отбрасывание политики Firwall	Действие политики встроенного пакета ICMP является ОТБРАСЫВАНИЕМ.
Контроль L7 возвращает ОТБРАСЫВАНИЕ	L7 (ALG) решает отбросить пакет. Причина могла быть найдена от другой статистики ALG.
Pkt сегмента L7 не позволяет	Полученный сегментированный пакет, когда ALG не соблюдает его.
Pkt фрагмента L7 не позволяет	Полученный фрагментированный (или VFR) пакеты, когда ALG не соблюдает его.
Неизвестный тип Proto L7	Неопознанный тип протокола.

Отбрасывания межсетевого экрана устранения неполадок

Как только причина отбрасывания определена от вышеупомянутого глобального или счетчиков сбросов характеристики межсетевого экрана, шаги дополнительного устранения проблем могли бы быть необходимы, если эти отбрасывания неожиданны. Кроме проверки конфигурации для обеспечения конфигурация корректна для включенных функциональных возможностей межсетевого экрана, это часто требуется, чтобы брать захваты пакета для рассматриваемого трафика, чтобы видеть, неправильно сформированы ли пакеты или если существуют любые проблемы реализации протокола или внедрения приложения.

Регистрация

Функциональность регистрации ASR генерирует системные журналы для записи отброшенных пакетов. Эти системные журналы предоставляют больше подробную информацию о том, почему был отброшен пакет. Существует два типа записей в системный журнал:

1. Локальная буферизированная запись в системный журнал

2. Удаленная высокоскоростная регистрация

Локальная буферизированная запись в системный журнал

Для изоляции причины отбрасываний можно использовать устранение проблем ZBFW

общего назначения, такое как включение регистрационных отбрасываний. Существует два способа настроить регистрацию отбрасывания пакета.

Способ 1: Используйте осматривать-глобальную карту параметра для регистрации всех отброшенных пакетов.

```
ASR#show platform hardware qfp active feature firewall drop all
-----------------------------------------------------------------------------
Drop Reason Packets
-----------------------------------------------------------------------------
Invalid L4 header 0
Invalid ACK flag 0
Invalid ACK number 0
....
```

Способ 2: Используйте пользовательский, осматривают карту параметра для регистрации отброшенных пакетов для только определенного класса.

```
parameter-map type inspect LOG_PARAM
log dropped-packets
!
policy-map type inspect ZBFW_PMAP
class type inspect ZBFW_CMAP
inspect LOG_PARAM
```

Эти сообщения передаются журналу или консоли в зависимости от того, как ASR настроен для регистрации. Вот пример сообщения журнала отбрасывания.

```
parameter-map type inspect LOG_PARAM
log dropped-packets
!
policy-map type inspect ZBFW_PMAP
class type inspect ZBFW_CMAP
inspect LOG_PARAM
```

Ограничения локальной буферизированной записи в системный журнал

1. Эти журналы являются скоростью, ограниченной согласно идентификатору ошибки Cisco CSCud09943.

2. Эти журналы не могли бы распечатать, пока не применена определенная конфигурация. Например, пакеты, отброшенные пакетами class-default, не будут зарегистрированы, пока не будет задано **регистрационное** ключевое слово:

```
policy-map type inspect ZBFW_PMAP
class class-default
drop log
```

Удаленная высокоскоростная Регистрация

Высокоскоростная регистрация (HSL) генерирует системные журналы непосредственно от QFP и передает его к настроенному коллектору HSL netflow. Это - рекомендуемое решение для регистрации для ZBFW на ASR.

Для HSL используйте эту конфигурацию:

```
policy-map type inspect ZBFW_PMAP
```

```
class class-default
drop log
```

Для использования этой конфигурации сборщик данных в режиме NetFlow, способный к Версии 9 Netflow, требуется. Это детализировано в

Руководство по конфигурации: Zone-Based Policy межсетевой экран, выпуск 3S Cisco IOS XE (ASR 1000) Регистрация высокой скорости межсетевого экрана

Пакет, отслеживающий Использование условного соответствия

Включите условные отладки, чтобы включить пакетное отслеживание и затем включить пакетное отслеживание для этих функций:

```
policy-map type inspect ZBFW_PMAP
class class-default
drop log
```

> **Примечание:** Условие соответствия может использовать IP-адрес непосредственно, поскольку ACL не необходим. Это будет совпадать как источник или назначение, которое обеспечивает двунаправленные трассировки. Если нельзя изменить конфигурацию, этот метод может использоваться. Пример: ipv4 address условия платформы отладки 192.168.1.1/32.

Включите отслеживающую пакет функцию:

```
policy-map type inspect ZBFW_PMAP
class class-default
drop log
```

Существует два способа использовать эту функцию:

1. Введите команду **отбрасывания трассировки пакетов платформы отладки** для отслеживания только отброшенных пакетов.

2. Исключение **отбрасывания трассировки пакетов платформы отладки** команды отследит любой пакет, который совпадает с условием, которое включает, которые осмотрены/переданы устройством.

Включите условные отладки:

```
policy-map type inspect ZBFW_PMAP
class class-default
drop log
```

Запустите тест, затем выключите отладки:

```
policy-map type inspect ZBFW_PMAP
class class-default
drop log
```

Теперь информация может быть отображена на экран. В данном примере пакеты ICMP были отброшены из-за политики межсетевого экрана:

```
Router#show platform packet-trace statistics
Packets Summary
```

```
 Matched 2
 Traced  2
Packets Received
 Ingress 2
 Inject  0
Packets Processed
 Forward 0
 Punt    0
 Drop    2
   Count      Code Cause
   2          183  FirewallPolicy
 Consume 0

Router#show platform packet-trace summary
Pkt  Input           Output          State Reason
0    Gi0/0/2         Gi0/0/0         DROP  183 (FirewallPolicy)
1    Gi0/0/2         Gi0/0/0         DROP  183 (FirewallPolicy)

Router#show platform packet-trace packet 0
Packet: 0          CBUG ID: 2980
Summary
 Input    : GigabitEthernet0/0/2
 Output   : GigabitEthernet0/0/0
 State    : DROP 183 (FirewallPolicy)
 Timestamp
   Start  : 1207843476722162 ns (04/15/2014 12:37:01.103864 UTC)
   Stop   : 1207843477247782 ns (04/15/2014 12:37:01.104390 UTC)
Path Trace
 Feature: IPV4
   Source     : 10.1.1.1
   Destination : 192.168.1.1
   Protocol   : 1 (ICMP)
 Feature: ZBFW
   Action : Drop
   Reason : ICMP policy drop:classify result
   Zone-pair name : INSIDE_OUTSIDE_ZP
   Class-map name : class-default
Packet Copy In
 c89c1d51 5702000c 29f9d528 08004500 00540000 40004001 ac640e26 70fa0e24
 01010800 172a2741 00016459 4d5310e4 0c000809 0a0b0c0d 0e0f1011 12131415
Packet Copy Out
 c89c1d51 5702000c 29f9d528 08004500 00540000 40003f01 ad640e26 70fa0e24
 01010800 172a2741 00016459 4d5310e4 0c000809 0a0b0c0d 0e0f1011 12131415
```

Пакетный <num> трассировки пакетов show platform декодирует команду, декодирует информацию о заголовке пакета и содержание. Эта функция была представлена в XE3.11:

```
Router#show platform packet-trace packet all decode
Packet: 0          CBUG ID: 2980
Summary
 Input    : GigabitEthernet0/0/2
 Output   : GigabitEthernet0/0/0
 State    : DROP 183 (FirewallPolicy)
 Timestamp
   Start  : 1207843476722162 ns (04/15/2014 12:37:01.103864 UTC)
   Stop   : 1207843477247782 ns (04/15/2014 12:37:01.104390 UTC)
Path Trace
 Feature: IPV4
   Source     : 10.1.1.1
   Destination : 192.168.1.1
   Protocol   : 1 (ICMP)
 Feature: ZBFW
   Action : Drop
   Reason : ICMP policy drop:classify result
```

```
   Zone-pair name : INSIDE_OUTSIDE_ZP
   Class-map name : class-default
Packet Copy In
 c89c1d51 5702000c 29f9d528 08004500 00540000 40004001 ac640e26 70fa0e24
 01010800 172a2741 00016459 4d5310e4 0c000809 0a0b0c0d 0e0f1011 12131415
 ARPA
   Destination MAC    : c89c.1d51.5702
   Source MAC         : 000c.29f9.d528
   Type               : 0x0800 (IPV4)
 IPv4
   Version            : 4
   Header Length      : 5
   ToS                : 0x00
   Total Length       : 84
   Identifier         : 0x0000
   IP Flags           : 0x2 (Don't fragment)
   Frag Offset        : 0
   TTL                : 64
   Protocol           : 1 (ICMP)
   Header Checksum    : 0xac64
   Source Address     : 10.1.1.1
   Destination Address : 192.168.1.1
 ICMP
   Type               : 8 (Echo)
   Code               : 0 (No Code)
   Checksum           : 0x172a
   Identifier         : 0x2741
   Sequence           : 0x0001
Packet Copy Out
 c89c1d51 5702000c 29f9d528 08004500 00540000 40003f01 ad640e26 70fa0e24
 01010800 172a2741 00016459 4d5310e4 0c000809 0a0b0c0d 0e0f1011 12131415
 ARPA
   Destination MAC    : c89c.1d51.5702
   Source MAC         : 000c.29f9.d528
   Type               : 0x0800 (IPV4)
 IPv4
   Version            : 4
   Header Length      : 5
   ToS                : 0x00
   Total Length       : 84
   Identifier         : 0x0000
   IP Flags           : 0x2 (Don't fragment)
   Frag Offset        : 0
   TTL                : 63
   Protocol           : 1 (ICMP)
   Header Checksum    : 0xad64
   Source Address     : 10.1.1.1
   Destination Address : 192.168.1.1
 ICMP
   Type               : 8 (Echo)
   Code               : 0 (No Code)
   Checksum           : 0x172a
   Identifier         : 0x2741
   Sequence           : 0x0001
```

Встроенный захват пакета

Встроенная поддержка Захвата пакета была добавлена в Cisco IOS XE 3.7 (15.2 (4) S). Для получения дополнительной информации посмотрите

Встроенный захват пакета для Cisco IOS и примера конфигурации XE IOS.

Отладка

Условные отладки

В XE3.10 будут представлены условные отладки. Условные операторы могут использоваться, чтобы гарантировать, что функция ZBFW только регистрирует сообщения отладки, которые относятся к условию. Условные отладки используют ACL для ограничения журналов, которые совпадают с элементами ACL. Кроме того, до XE3.10 сообщения отладки было более трудно считать. Выходные данные отладки были улучшены в XE3.10 для создания их легче понять.

Для включения этих отладок выполните эту команду:

```
Router#show platform packet-trace packet all decode
Packet: 0          CBUG ID: 2980
Summary
 Input    : GigabitEthernet0/0/2
 Output   : GigabitEthernet0/0/0
 State    : DROP 183 (FirewallPolicy)
 Timestamp
   Start  : 1207843476722162 ns (04/15/2014 12:37:01.103864 UTC)
   Stop   : 1207843477247782 ns (04/15/2014 12:37:01.104390 UTC)
Path Trace
 Feature: IPV4
   Source     : 10.1.1.1
   Destination : 192.168.1.1
   Protocol   : 1 (ICMP)
 Feature: ZBFW
   Action : Drop
   Reason : ICMP policy drop:classify result
   Zone-pair name : INSIDE_OUTSIDE_ZP
   Class-map name : class-default
Packet Copy In
 c89c1d51 5702000c 29f9d528 08004500 00540000 40004001 ac640e26 70fa0e24
 01010800 172a2741 00016459 4d5310e4 0c000809 0a0b0c0d 0e0f1011 12131415
 ARPA
   Destination MAC    : c89c.1d51.5702
   Source MAC         : 000c.29f9.d528
   Type               : 0x0800 (IPV4)
 IPv4
   Version            : 4
   Header Length      : 5
   ToS                : 0x00
   Total Length       : 84
   Identifier         : 0x0000
   IP Flags           : 0x2 (Don't fragment)
   Frag Offset        : 0
   TTL                : 64
   Protocol           : 1 (ICMP)
   Header Checksum    : 0xac64
   Source Address     : 10.1.1.1
   Destination Address : 192.168.1.1
 ICMP
   Type               : 8 (Echo)
   Code               : 0 (No Code)
   Checksum           : 0x172a
   Identifier         : 0x2741
   Sequence           : 0x0001
```

```
Packet Copy Out
 c89c1d51 5702000c 29f9d528 08004500 00540000 40003f01 ad640e26 70fa0e24
 01010800 172a2741 00016459 4d5310e4 0c000809 0a0b0c0d 0e0f1011 12131415
 ARPA
   Destination MAC    : c89c.1d51.5702
   Source MAC         : 000c.29f9.d528
   Type               : 0x0800 (IPV4)
 IPv4
   Version            : 4
   Header Length      : 5
   ToS                : 0x00
   Total Length       : 84
   Identifier         : 0x0000
   IP Flags           : 0x2 (Don't fragment)
   Frag Offset        : 0
   TTL                : 63
   Protocol           : 1 (ICMP)
   Header Checksum    : 0xad64
   Source Address     : 10.1.1.1
   Destination Address : 192.168.1.1
 ICMP
   Type               : 8 (Echo)
   Code               : 0 (No Code)
   Checksum           : 0x172a
   Identifier         : 0x2741
   Sequence           : 0x0001
```

Заметьте, что команда условия должна быть установлена через ACL и направленность. Условные отладки не будут внедрены, пока они не запущены с **условия платформы отладки** команды**, запускаются**. Для выключения использования условных отладок**, условие платформы отладки** команды **останавливается**.

```
debug platform condition stop
```

Для выключения условных отладок **НЕ** используйте **команду undebug all**. Для выключения всех условных отладок используйте команду:

```
ASR#clear platform condition all
```

До XE3.14, **ха** и отладок **события** не условное выражение. В результате **функция условия платформы отладки** команды **fw dataplane подрежим все** причины все журналы, которые будут созданы, независимый от условия, выбранного ниже. Это могло создать дополнительный шум, который делает отладку трудной.

По умолчанию условный уровень регистрации является **информацией**. Для увеличения уровня регистрации используйте команду:

```
debug platform condition feature fw dataplane submode all [verbose | warning]
```

Соберите и просмотрите отладки

Файлы отладки не распечатают к консоли или монитору. Все отладки записаны в жесткий диск ASR. Отладки записаны в жесткий диск под папкой **tracelogs** с **названием cpp_cp_F0-0.log. <дата>**. Для просмотра файла, где отладки записаны, используйте выходные данные:

```
debug platform condition feature fw dataplane submode all [verbose | warning]
```

Каждый файл отладки будет храниться как **cpp_cp_F0-0.log. <дата>** файл. Это файлы обычного текста, которые могут быть скопированы от ASR с TFTP. Максимум файла журнала на ASR составляет 1 МБ. После 1 МБ отладки записаны в новый файл журнала. Именно поэтому к каждому файлу журнала добавляют метку времени для указания на

запуск файла.

Файлы журнала могли бы существовать в этих местоположениях:

debug platform condition feature fw dataplane submode all [verbose | warning]
Так как файлы журнала только отображены после того, как они повернуты, файл журнала может быть вручную повернут с этой командой:

```
ASR# test platform software trace slot f0 cpp-control-process rotate
```

Это сразу создает "cpp_cp" файл журнала и запускает новый на QFP. Пример:

```
ASR#test platform software trace slot f0 cpp-control-process rotate
 Rotated file from: /tmp/fp/trace/stage/cpp_cp_F0-0.log.7311.20140408134406,
Bytes: 82407, Messages: 431

ASR#more tracelogs/cpp_cp_F0-0.log.7311.20140408134406
04/02 10:22:54.462 : btrace continued for process ID 7311 with 159 modules
04/07 16:52:41.164 [cpp-dp-fw]: (info): QFP:0.0 Thread:110 TS:00000531990811543397
:FW_DEBUG_FLG_HA:[]: HA[1]: Changing HA state to 9
04/07 16:55:23.503 [cpp-dp-fw]: (info): QFP:0.0 Thread:120 TS:00000532153153672298
:FW_DEBUG_FLG_HA:[]: HA[1]: Changing HA state to 10
04/07 16:55:23.617 [buginf]: (debug): [system] Svr HA bulk sync CPP(0) complex(0)
epoch(0) trans_id(26214421) rg_num(1)
```

Эта команда позволяет файлам отладки быть объединенными в отдельный файл для более легкой обработки. Это объединяет все файлы в каталоге и чередует их основанный вовремя. Когда журналы очень многословны и созданы через множественные файлы, это может помочь:

```
ASR#request platform software trace slot rp active merge target bootflash:MERGED_OUTPUT.log
Creating the merged trace file: [bootflash:MERGED_OUTPUT.log]
 including all messages

Done with creation of the merged trace file: [bootflash:MERGED_OUTPUT.log]
```