Устранение проблем групповой адресации ASA и типичные проблемы

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Условные обозначения
Информация о функциональной возможности
Операция разреженного режима многоадресной рассылки (PIM sparse)
Операция тупикового режима IGMP
Методика устранения проблем
Информация, обязательная для сбора при устранении проблем проблем групповой адресации
Анализ данных
Типичные неполадки
Дополнительные сведения

Введение

Этот документ объясняет возможности групповой адресации Устройства адаптивной защиты (ASA), а также потенциальные проблемы, с которыми можно встретиться при использовании функции.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- ASA передан в многоадресном режиме

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Условные обозначения

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

Информация о функциональной возможности

Руководство по конфигурации Командной строки ASA выделяет функцию multicast-routing и как настроить его:

http://www. cisco . com/en/US/docs/security/asa/asa90/configuration/guide/route_multicast.html

Групповая адресация на ASA может быть настроена в одном из двух режимов:

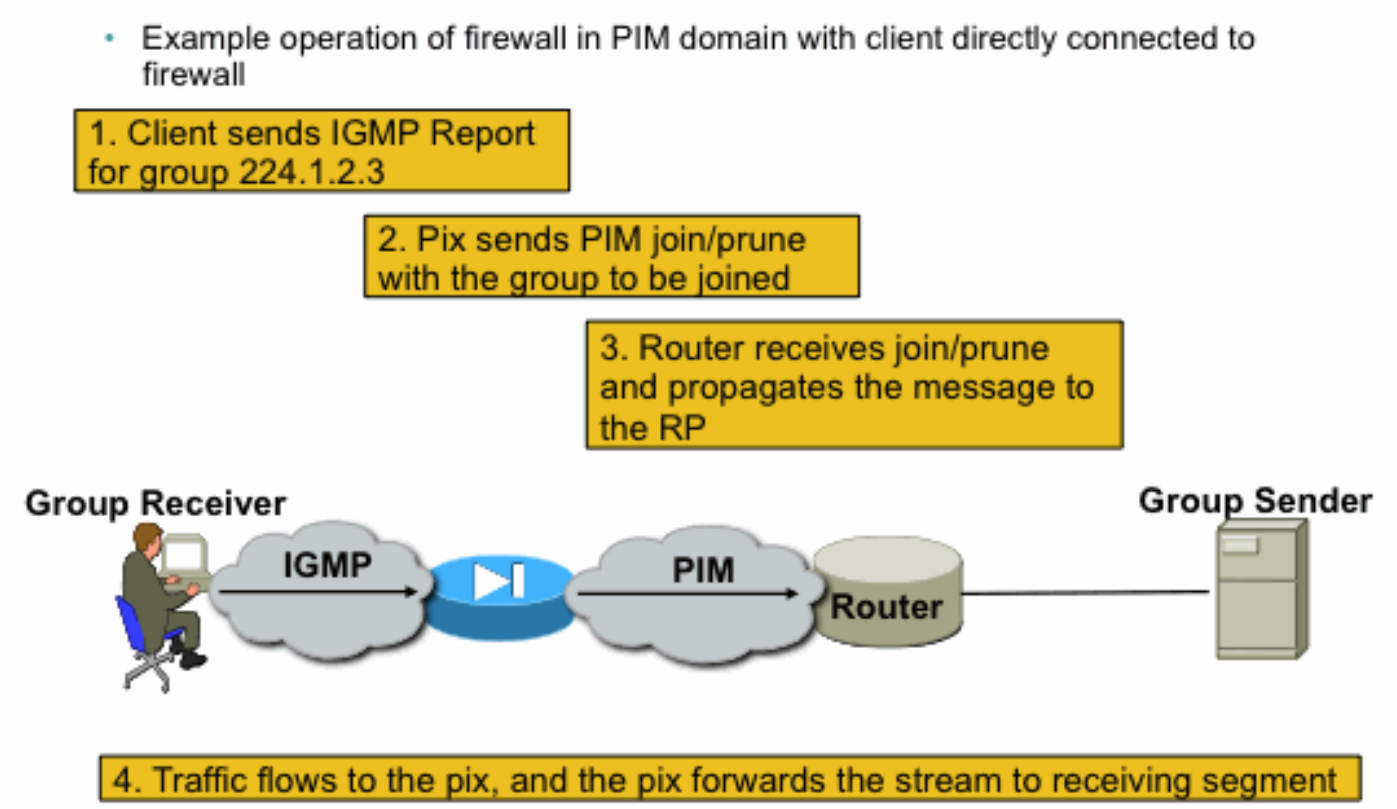
- Разреженный режим многоадресной рассылки (PIM sparse) (предпочтен)
- Тупиковый режим IGMP (протокол управления группами Интернет, RFC 2236 IGMPv2)

Разреженный режим многоадресной рассылки (PIM sparse) является рекомендуемым выбором, потому что ASA связывается с соседними узлами, использующими истинный протокол многоадресной маршрутизации (PIM). Тупиковый режим IGMP был единственной опцией конфигурирования многоадресной передачи, прежде чем версия ASA 7.0 освобождалась и управлялась путем простой передачи отчетов IGMP, полученных от клиентов к вышестоящим маршрутизаторам.

Операция разреженного режима многоадресной рассылки (PIM sparse)

- ASA поддерживает двунаправленный режим PIM и разреженный режим многоадресной рассылки (PIM sparse).
- Разреженный режим многоадресной рассылки (PIM sparse) и тупиковые командные режимы IGMP не должны быть настроены одновременно.
- С разреженным режимом многоадресной рассылки (PIM sparse) весь многоадресный трафик первоначально течет к Точке встречи (RP), затем передан к приемникам. Через какое-то время поток групповой адресации пойдет непосредственно с источника на приемники (обходящий RP).

Изображение ниже иллюстрирует обычное развертывание, где ASA имеет клиентов многоадресной передачи на одном интерфейсе и соседей PIM на другом:



[Пример конфигурации разреженного режима многоадресной рассылки (PIM sparse)]

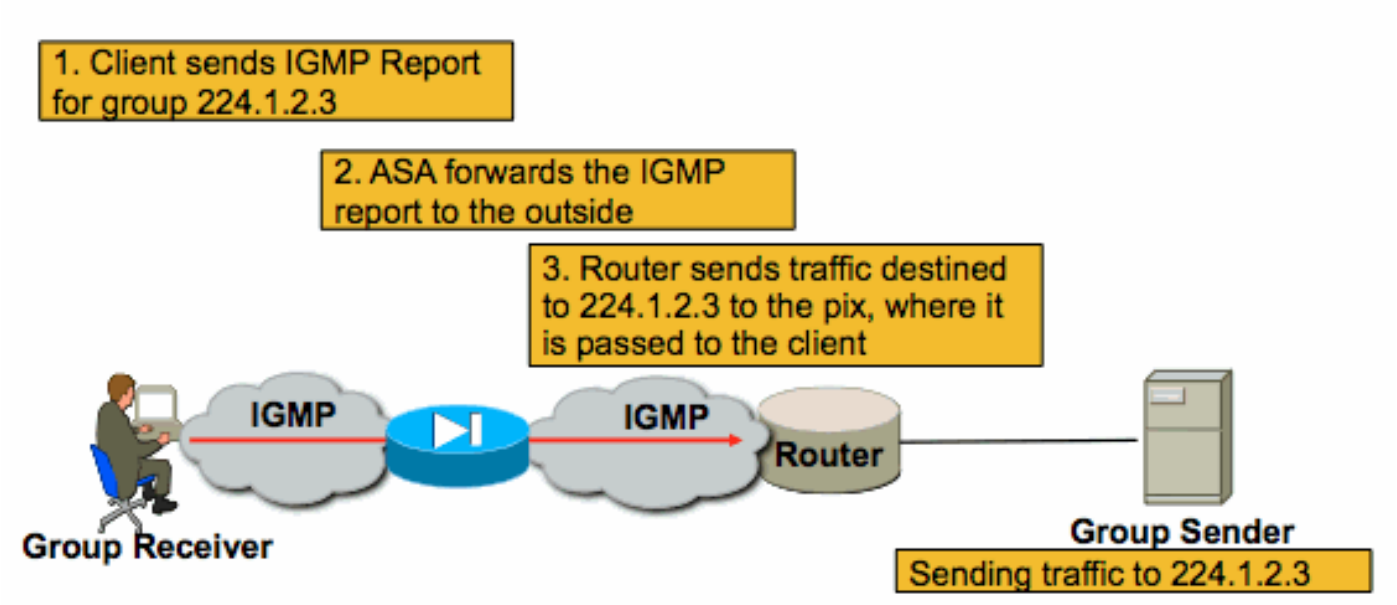
Выполните следующие действия:

1. Включите многоадресную маршрутизацию (режим глобальной конфигурации).`ASA(config)# multicast-routing`
2. Определите адрес Точки встречи PIM.`ASA(config)# pim rp-address 172.18.123.3`
3. Позвольте пакетам групповой адресации войти на соответствующем интерфейсе (необходимый, только если политика безопасности ASA блокирует входящие пакеты групповой адресации).`access-list 105 extended permit ip any host 224.1.2.3`
`access-group 105 in interface outside`

Операция тупикового режима IGMP

- В Тупиковом режиме IGMP ASA действует как клиент многоадресной передачи путем генерации или передачи отчетов IGMP (также известный как IGMP "соединения") к соседним маршрутизаторам, для инициирования приема многоадресного трафика
- Маршрутизаторы будут периодически передавать запросы к хостам, чтобы видеть, хочет ли какой-либо узел в сети продолжить получать многоадресный трафик.
- Тупиковый режим IGMP не рекомендуется, потому что разреженный режим многоадресной рассылки (PIM sparse) предлагает много преимуществ по Тупиковому режиму (включая более эффективные потоки многоадресного трафика, способность участвовать в PIM, и т.д.).

Изображение ниже иллюстрирует главную операцию ASA, настроенного для Тупикового режима IGMP.



[Тупиковая конфигурация режима IGMP]

Выполните следующие действия:

1. Включите многоадресную маршрутизацию (режим глобальной конфигурации).`ASA(config)# multicast-routing`
2. На интерфейсе, о котором вы получите отчеты IGMP, настройте команду прямого интерфейса igmp. Передайте пакеты интерфейс к источнику потока. В примере ниже, получатели групповой адресации напрямую подключаются к внутреннему интерфейсу, и источник групповой адресации вне внешнего интерфейса.`!`

```
interface Ethernet0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
 no pim
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.0.0.1 255.255.255.0
 no pim
 igmp forward interface outside !
```

3. Позвольте пакетам групповой адресации войти на соответствующем интерфейсе (только необходимый, если политика безопасности ASA запрещает входящий многоадресный трафик).`access-list 105 extended permit ip any host 224.1.2.3 access-group 105 in interface outside`Часто существует беспорядок вокруг других **команд igmp interface sub-mode**, и приведенный ниже рисунок пытается описать, когда использовать
каждого:

igmp forward interface <interface>

```
!
Interface FastEthernet0/1
 nameif inside
 security-level 100
 ip address 10.0.0.1
255.255.255.0
 igmp forward interface outside
!
```

Causes the firewall to forward IGMP reports received on the inside interface out the outside interface. You would use this command if multicast receivers were on the inside interface and the multicast source was somewhere out the outside interface

igmp join-group <group name>

```
!
Interface FastEthernet0/1
 nameif inside
 security-level 100
 ip address 10.0.0.1
255.255.255.0
 igmp join-group 224.1.2.3
!
```

Tells the firewall that there are hosts behind the inside interface that might want to receive the traffic for the group. It will send IGMP reports out the interface telling the LAN segment that the firewall wishes to receive the stream. It will also add the inside interface to the OIL list for the group. This method is not recommended; If you need to cause the firewall to add an interface to the OIL for an mroute, use the static-group command below

igmp static-group <group name>

```
!
Interface FastEthernet0/1
 nameif inside
 security-level 100
 ip address 10.0.0.1
255.255.255.0
 igmp static-group 224.1.2.3
!
```

Tells the firewall that there are hosts behind the inside interface that might want to receive the traffic for the group. It will simply add the inside interface to the OIL list for the group. This is useful for simulating a multicast receiver behind the inside interface.

Методика устранения проблем

Информация, обязательная для сбора при устранении проблем проблем групповой адресации

Чтобы полностью понять и диагностировать проблему переадресации широковещания на ASA, некоторые или вся эта информация могли бы быть необходимы:

- Описание топологии сети, включая местоположение fo отправители групповой адресации, приемники и точка встречи.
- Определенный IP-адрес группы трафик использует, а также используемые порты и протоколы.
- Системные журналы, генерируемые ASA в это время многоадресная рассылка, испытывают затруднения.
- Определенные выходные данные команды show от интерфейса командной строки ASA, включая:`show mroute`
  `show mfib`
  `show pim neighbor`
  `show route`
  `show tech-support`
- Захваты пакета, чтобы показать, поступают ли данные групповой адресации в ASA, и если пакеты переданы через ASA.
- Захваты пакета показывая IGMP и/или пакеты PIM.
- Информация от смежных устройств групповой адресации (маршрутизаторы), такие как 'покажите mroute' и 'покажите mfib'.
- Захваты пакета и/или команды показа, чтобы определить, отбрасывает ли ASA пакеты групповой адресации. Команда 'покажите отбрасывание гадюки' может использоваться,

чтобы определить, отбрасывает ли ASA пакеты. Кроме того, захваты пакета типа 'отбрасывание asp' могут использоваться для получения всех пакетов отбрасывания ASA, затем исследованные, чтобы видеть, присутствуют ли пакеты групповой адресации в перехвате отбрасывания.

Выходные данные полезной команды show

Выходные данные **команды show mroute** показывают различные группы и информацию перенаправления, и подобны **команде show mroute** IOS. **Команда show mfib** отображает состояние передачи различных групп многоадресной рассылки. Особенно важно наблюдать *Передающий* счетчик пакетов, а также *Другой* (который указывает на отбрасывания):

```
ciscoasa# show mfib
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, K - Keepalive
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.1.2.3) Flags: S K
   Forwarding: 0/0/0/0, Other: 0/0/0
   inside Flags: F
     Pkts: 0/0
(192.168.1.100,224.1.2.3) Flags: K
   Forwarding: 6749/18/1300/182, Other: 690/0/690
   outside Flags: A
   inside Flags: F
     Pkts: 6619/8
(*,232.0.0.0/8) Flags: K
   Forwarding: 0/0/0/0, Other: 0/0/0
ciscoasa#
```

Команда **clear mfib counter** может использоваться для очистки счетчиков, который очень полезен во время тестирования:

```
ciscoasa# clear mfib counters
ciscoasa#
```

Использование захватов пакета для получения многоадресного трафика

Встроенная утилита захвата пакета ASA очень полезна для устранения проблем проблем групповой адресации. В примере ниже, будут перехвачены все пакеты, поступающие в интерфейс DMZ ASA, предназначенный к 239.17.17.17:

```
ciscoasa# capture dmzcap interface dmz
ciscoasa# capture dmzcap match ip any host 239.17.17.17
ciscoasa# show cap dmzcap

324 packets captured

   1: 17:13:30.976618       802.1Q vlan#301 P0 10.1.123.129.2000 > 239.17.17.17.16384:
  udp 172
   2: 17:13:30.976679       802.1Q vlan#301 P0 10.1.123.129.2000 > 239.17.17.17.16384:
  udp 172
   3: 17:13:30.996606       802.1Q vlan#301 P0 10.1.123.129.2000 > 239.17.17.17.16384:
  udp 172
   4: 17:13:30.996652       802.1Q vlan#301 P0 10.1.123.129.2000 > 239.17.17.17.16384:
```

```
  udp 172
   5: 17:13:31.016676       802.1Q vlan#301 P0 10.1.123.129.2000 > 239.17.17.17.16384:
  udp 172
   6: 17:13:31.016722       802.1Q vlan#301 P0 10.1.123.129.2000 > 239.17.17.17.16384:
  udp 172
....
```

Захваты пакета также полезны для получения PIM и трафика IGMP. Перехват ниже показов внутренний интерфейс получил Пакет IGMP (Протокол "IP" 2) полученный от 10.0.0.2:

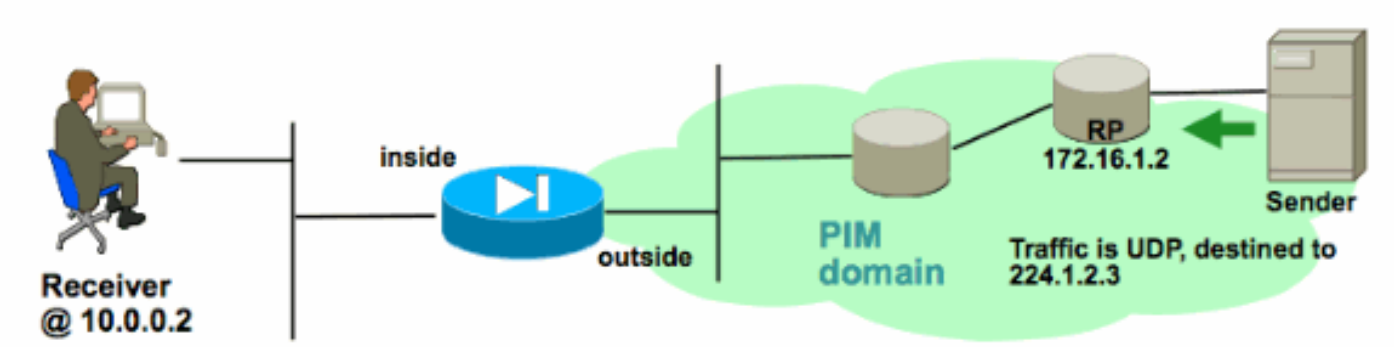
```
ciscoasa# capture capin interface inside
ciscoasa# capture capin match igmp any any
ciscoasa# show cap capin
1 packets captured
1: 10:47:53.540346 802.1Q vlan#15 P0 10.0.0.2 > 224.1.2.3:
  ip-proto-2, length 8
ciscoasa#
```

[Развертывания групповой адресации разреженного режима многоадресной рассылки (PIM sparse) ASA в качестве примера]

Приведенные ниже рисунки иллюстрируют, как ASA взаимодействует с соседними устройствами для получения многоадресного трафика, текущего с разреженным режимом многоадресной рассылки (PIM sparse). В этом определенном примере ASA получает.

Понимание топологии сети

Определите точно, где находятся отправитель и получатель определенной многоадресной рассылки, которую вы тестируете. Кроме того, определите IP-адрес группы многоадресной рассылки, используемый, а также местоположение точки встречи.



В этом случае данные должны быть получены во внешнем интерфейсе ASA и переданы к получателю групповой адресации на внутреннем интерфейсе. Поскольку получатель находится в той же IP-подсети как внутренний интерфейс ASA, ожидайте видеть отчет IGMP, полученный во Внутреннем интерфейсе ASA когда запросы клиента для получения потока. IP-адрес отправителя 192.168.1.50.

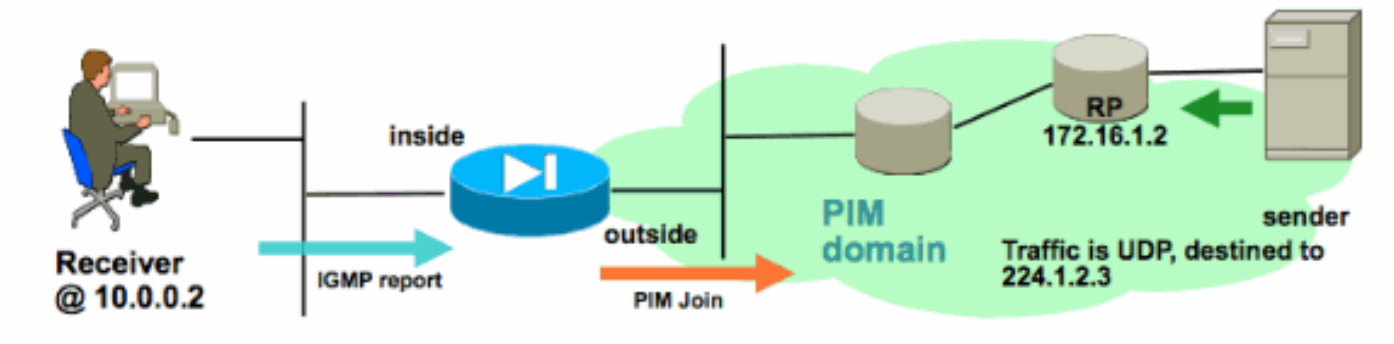
Проверка ASA получает отчет IGMP от получателя

В данном примере отчет IGMP генерируется получателем и обрабатывается ASA.

Захваты пакета и выходные данные igmp отладки могут использоваться, чтобы проверить, что ASA, полученный, и успешно, обработал сообщение IGMP.

Проверка ASA передает сообщение присоединения PIM к точке встречи

ASA интерпретирует отчет IGMP и генерирует сообщение присоединения PIM, затем передает ему интерфейс к RP.

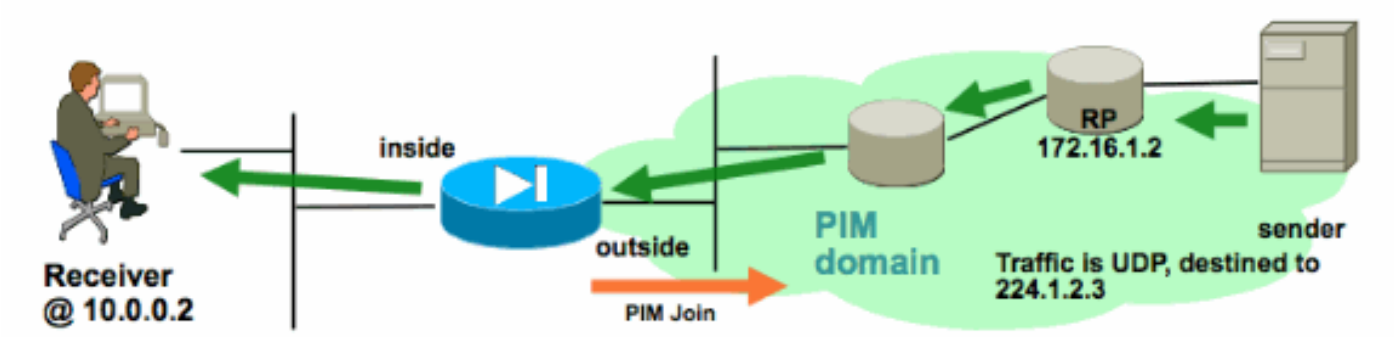


Выходные данные ниже от группы pim отладки 224.1.2.3 и показывают ASA, успешно передавая сообщение присоединения PIM. Отправитель многоадресной рассылки 192.168.1.50

```
IPv4 PIM: (*,224.1.2.3) J/P processing
IPv4 PIM: (*,224.1.2.3) Periodic J/P scheduled in 50 secs
IPv4 PIM: (*,224.1.2.3) J/P adding Join on outside
IPv4 PIM: (*,224.1.2.3) inside Processing timers
IPv4 PIM: Sending J/P message for neighbor 10.2.3.2 on outside for 1 groups
IPv4 PIM: [0] (192.168.1.50,224.1.2.3/32) MRIB update (a=0,f=0,t=1)
IPv4 PIM: [0] (192.168.1.50,224.1.2.3/32) outside MRIB update (f=20,c=20)
IPv4 PIM: [0] (192.168.1.50,224.1.2.3) Signal present on outside
IPv4 PIM: (192.168.1.50,224.1.2.3) Create entry
IPv4 PIM: [0] (192.168.1.50,224.1.2.3/32) outside MRIB modify NS
IPv4 PIM: Adding monitor for 192.168.1.5
```

Проверка ASA получает и вперед многоадресная рассылка

ASA начинает получать многоадресный трафик на внешнем интерфейсе (проиллюстрированный зелеными стрелками) и передавать его приемникам на внутренней части.



Команды покажите mroute и show mfib, а также захваты пакета, могут использоваться, чтобы проверить, что ASA получает и вперед пакеты групповой адресации.

Соединение будет создано в таблице подключений ASA для представления многоадресной рассылки:

```
ciscoasa# show conn
59 in use, 29089 most used
...
UDP outside:192.168.1.50/52075 inside:224.1.2.3/1234 flags -
...
```

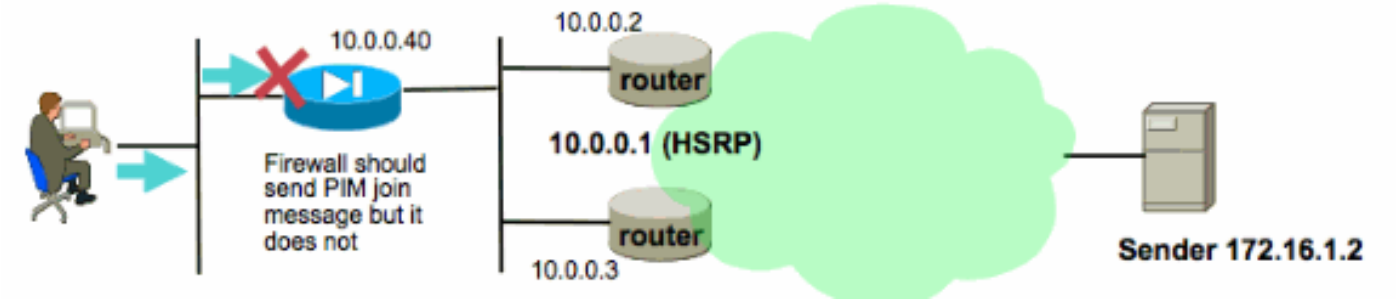
Анализ данных

Типичные неполадки

Этот раздел предоставляет серию реальных связанных проблем групповой адресации ASA, с которыми администраторы сети встретились в прошлом.

ASA не в состоянии передавать сообщения PIM к вышестоящим маршрутизаторам из-за HSRP

Когда с этой проблемой встречаются, ASA не в состоянии передавать любым сообщениям PIM интерфейс. Приведенный ниже рисунок показывает, что ASA не может передать сообщения PIM к отправителю, но та же проблема может быть замечена, когда ASA должен передать сообщение PIM к RP.



Выходные данные **pim отладки** показывают, что ASA не может передать сообщение PIM к восходящему маршрутизатору следующего перехода:

```
IPv4 PIM: Sending J/P to an invalid neighbor: outside 10.0.0.1
```

Эта проблема не является определенной для ASA, и также влияет на маршрутизаторы. Проблема инициирована комбинацией конфигурации таблицы маршрутизации ASA и конфигурации HSRP, используемой соседями PIM.

Таблица маршрутизации ASA указывает к IP HSRP 10.0.0.1 как устройство следующего узла:

```
ciscoasa# sh run route
route outside 0.0.0.0 0.0.0.0 10.0.0.1 1
```

Однако отношение соседа PIM сформировано между IP-адресами физического интерфейса маршрутизаторов, а не IP HSRP:

```
ciscoasa# sh pim neighbor
Neighbor Address  Interface          Uptime    Expires DR pri Bidir
10.0.0.2          outside            01:18:27  00:01:25 1
10.0.0.3          outside            01:18:03  00:01:29 1 (DR)
```

См. то, почему разреженный режим многоадресной рассылки (PIM sparse) не работает со статическим маршрутом к адресу HSRP? дополнительные сведения.

Выборка из документа:

Почему маршрутизатор не отправляет сообщение Join/Prune? RFC 2362 сообщает, что "маршрутизатор передает периодическое Сообщение присоединения/отключения к каждому отдельному окружению RPF, привязанному к каждому (S, G), (, G) и (*, *, RP) запись.*

Сообщения Join/Prune посылаются, только если соседний узел RPF – это соседний узел PIM."

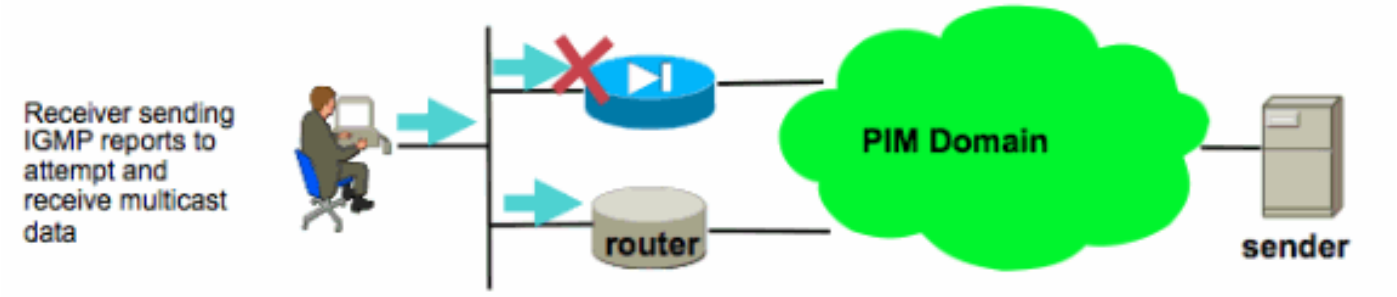
Для смягчения проблемы добавьте статическую mroute запись на ASA для рассматриваемого трафика. Удостоверьтесь, что это указывает к одному из IP-адресов интерфейса двух маршрутизаторов (10.0.0.2 или 10.0.0.3 в приведенном выше примере). В этом случае следующая команда позволяет ASA передавать сообщения PIM, направленные к отправителю групповой адресации на 172.16.1.2:

```
ciscoasa(config)# mroute 172.16.1.2 255.255.255.255 10.0.0.3
```

Как только это сделано, таблица многоадресной маршрутизации отвергнет таблицу одноадресной маршрутизации ASA, и ASA передаст сообщения PIM непосредственно этим 10.0.0.3 соседним узлам.

ASA игнорирует отчеты IGMP, поскольку это не выделенный маршрутизатор на сегменте LAN

Для этой проблемы ASA получает отчет IGMP от непосредственно связанного получателя групповой адресации, все же это игнорирует его. Выходные данные No debug будут генерироваться, и пакет просто отброшен, и потоковые сбои приема.



Для этой проблемы ASA игнорирует пакет, потому что это не PIM, избранный выделенным маршрутизатором на сегменте LAN, где находятся клиенты.

Выходные данные ASA CLI ниже показов, что другим устройством является Выделенный маршрутизатор (обозначенный "DR") в сети внутреннего интерфейса:

```
ciscoasa#show pim neighbor

 Neighbor Address  Interface          Uptime    Expires DR pri Bidir
 192.168.1.2       outside         01:18:27  00:01:25 N/A>
 10.0.0.2          inside             01:18:03  00:01:29 1 (DR)
```

По умолчанию, когда **команда multicast-routing** добавлена к конфигурации ASA, PIM включен на всех интерфейсах ASA. Если существуют другие соседи PIM (другие маршрутизаторы или ASA) на внутреннем интерфейсе ASA (где клиенты находятся), и один из тех соседних узлов были избраны, потому что DR для того сегмента, то другой, невыделенные маршрутизаторы отбросят отчеты IGMP. Решение состоит в том, чтобы отключить PIM на интерфейсе ASA (с **командой no pim** на включенном интерфейсе), или сделать ASA DR для сегмента с помощью **команды pim dr-priority interface**.

Сбои ASA Для Передачи Многоадресного трафика В 232. x. x. Диапазон x/8

Этот диапазон адресов для использования с Source Specific Multicast (SSM), который в

настоящее время не поддерживает ASA.

Выходные данные **igmp отладки** покажут эту ошибку:

```
IGMP: Exclude report on inside ignored for SSM group 232.179.89.253
```

ASA отбрасывает пакеты групповой адресации из-за проверки пересылки по обратному пути

В этом случае ASA получает многоадресный трафик на интерфейсе, но это не передано на получателе. Пакеты отброшены ASA, потому что они отказывают проверку защиты Пересылки по обратному пути (RPF). RPF включен на всех интерфейсах для многоадресного трафика и не может быть отключен (для одноадресных пакетов, на которых проверка не находится по умолчанию и включена с **командой ip verify reverse-path interface**).

Из-за Проверки переадресации по обратному пути, когда многоадресный трафик получен в интерфейсе, проверки ASA, чтобы видеть, что это имеет маршрут назад к источнику трафика многоадресного трафика (это проверяет индивидуальную рассылку и таблицу многоадресной маршрутизации) на том интерфейсе. Если это не имеет маршрута к отправителю, это отбрасывает пакет. Эти отбрасывания могут быть замечены как счетчик в выходных данных **отбрасывания asp показа**:

```
ciscoasa(config)# show asp drop

Frame drop:
  Invalid UDP Length                                     2
  No valid adjacency                                    36
  No route to host                                    4469
  Reverse-path verify failed                        121012
```

Эта проблема может быть смягчена путем добавления определенной записи таблицы многоадресной маршрутизации в ASA для отправителя трафика. В примере ниже, команда mroute используется для удовлетворения Проверки переадресации по обратному пути для многоадресного трафика, полученного от 172.16.1.2 полученных на внешнем интерфейсе:

```
ciscoasa(config)# mroute 172.16.1.2 255.255.255.255 outside
```

ASA не генерирует соединение PIM после переключателя PIM к исходному дереву

Первоначально, пакеты групповой адресации разреженного режима многоадресной рассылки (PIM sparse) будут вытекать из отправителя групповой адресации к RP, затем с RP на получатель через совместно используемое дерево групповой адресации. Однако, как только составная битовая скорость достигает определенного порога, маршрутизатор, самый близкий к получателю групповой адресации, попытается получить трафик вдоль специфичного для источника дерева. Этот маршрутизатор будет генерировать новое соединение PIM для группы и передавать ее к отправителю многоадресной рассылки (а не к RP, как прежде).

В зависимости от топологии сети отправитель многоадресного трафика мог бы находиться на другом интерфейсе ASA, чем RP. Когда ASA получает PIM, соединяют для коммутации к источнику определенного дерева, ASA должен иметь маршрут к IP-адресу отправителя. Если этот маршрут не будет найден, то пакет соединения PIM будет отброшен, и следующее сообщение будет замечено в выходных данных **pim отладки**:

```
NO RPF Neighbor to send J/P
```

Решение для этой проблемы состоит в том, чтобы добавить статическую mroute запись для отправителя потока, указав на интерфейс ASA прочь, которого находится отправитель.

ASA отбрасывает пакеты групповой адресации из-за превышенного времени жизни (TTL)

В этом случае многоадресный трафик отказывает, потому что TTL пакетов слишком низок. Это вызывает ASA или некоторое другое устройство в сети, для отбрасывания их.

Часто пакеты групповой адресации имеют заданное значение IP TTL очень низко приложением, которое передало им. Иногда это сделано по умолчанию, чтобы помочь гарантировать, что многоадресный трафик не перемещается слишком далеко хотя сеть. Например, по умолчанию Видео приложение Клиента LAN (популярный передатчик групповой адресации и инструмент тестирования) устанавливает TTL в пакете IP к 1 по умолчанию.

ASA испытывает высокую загрузку ЦП и отброшенные пакеты из-за определенной топологии групповой адресации

ASA мог бы испытать высокую загрузку CPU, и многоадресная рассылка могла бы испытать отбрасывание пакета, если весь из ниже приводится истинный о топологии групповой адресации:

1. ASA действует как RP.
2. ASA является первым получателем перехода многоадресной рассылки. Это означает, что отправитель групповой адресации находится в той же IP-подсети интерфейс ASA.
3. ASA является маршрутизатором последнего перехода многоадресной рассылки. Это означает, что получатель групповой адресации находится в той же IP-подсети как интерфейс ASA.

Если все вышеупомянутое истинно, то должный делают проектные ограничения, которые ASA будет вынужден обработать, коммутируют многоадресный трафик. Это приводит к высоким многоадресным рассылкам скорости передачи данных для испытания отбрасывания пакета. Счетчик сбросов asp показа, который инкрементно увеличивается, когда эти пакеты отброшены, является rate-limit избыточного направления.

Чтобы определить, испытывает ли ASA эту проблему, выполните эти шаги:

Шаг 1: Проверьте, является ли ASA RP при помощи этих двух команд:

```
show run pim
show pim tunnel
```

Шаг 2: Проверьте, является ли ASA маршрутизатором последнего перехода при помощи этой команды:

```
show igmp group <mcast_group_IP>
```

Шаг 3: Проверьте, является ли ASA первым маршрутизатором перехода при помощи этой команды:

```
show mroute <mcast_group_IP>
```

Разъединяющий получатель групповой адресации прерывает прием группы многоадресной рассылки на других интерфейсах

Только ASA, работающие в Тупиковом режиме IGMP, испытывают эту проблему. На ASA, которые участвуют в многоадресной маршрутизации PIM, не влияют.

Проблема определена дефектом CSCeg48235 - IGMP: Остановка группы rcvr прерывает прием группы на других интерфейсах

Это - Комментарии к выпуску от дефекта, который объясняет проблему:

```
Symptom:
When a PIX or ASA firewall is configured for IGMP stub mode multicast reception and
traffic from a multicast group is forwarded to more than one interface, if a host
behind a receiving interface sends an IGMP Leave message for the group, it could
temporarily interrupt the reception for that group on other interfaces of the firewall.

The problem is triggered when the firewall forwards the IGMP leave for the group
towards the upstream device; that device then sends a IGMP query to determine if any
other receivers exist out that interface towards the firewall, but the firewall does
not report that it still has valid receivers.

Conditions:
The PIX or ASA must be configured for IGMP stub mode multicast. IGMP stub mode is a
legacy multicast forwarding technique, whereby IGMP packets from receivers are forwarded
through the firewall towards the source of the stream. It is recommended to use PIM
multicast routing instead of stub igmp forwarding.

Workarounds:
1) Use PIM multicast routing instead of IGMP stub mode.
2) Decrease multicast IGMP query timers so that the receivers are queried more frequently,
causing their IGMP reports to be forwarded towards the sender more frequently, thus
restarting the stream quicker.
```

ASA отбрасывает пакеты групповой адресации из-за политики безопасности исходящего Access-list

С этим конкретным вопросом ASA правильно отбрасывает пакеты групповой адресации (на настроенную политику безопасности). Однако для администратора сети трудно определить причину для отбрасывания пакета. В этом случае ASA отбрасывает пакеты из-за исходящего access-list, настроенного для интерфейса. Обходной путь должен разрешить многоадресную рассылку в исходящем access-list.

Когда это произойдет, пакеты групповой адресации будут отброшены, и счетчик сбросов ASP будет "FP, никакой mcast не вывел intrf (no-mcast-intrf)".

Когда многоадресная рассылка сначала запущена, ASA отбрасывает первые несколько пакетов

Когда первые пакеты многоадресной рассылки поступают в ASA, ASA должен создать то определенное многоадресное соединение и связанную запись mroute для передачи пакетов. В то время как запись создается, некоторые пакеты групповой адресации могли бы быть отброшены, пока mroute и соединения не были установлены (обычно, это берет меньше, чем секунда). Как только настройка многоадресной рассылки завершена, пакеты больше не будут ограниченной скоростью.

Пакеты, отброшенные поэтому, будут иметь причину отбрасывания ASP" (rate-limit избыточного направления), ограничение скорости Избыточного направления превысило". Ниже выходные данные **asp show capture** (где asp является перехватом отбрасывания ASP, настроенным на ASA для получения отброшенных пакетов), и вы видите пакеты групповой адресации, которые были отброшены поэтому:

```
ASA # sh capture asp
```

```
2 packets captured
   1: 16:14:49.419091 10.23.2.2.810 > 239.255.123.123.890:  udp 32 Drop-reason:
 (punt-rate-limit) Punt rate limit exceeded
   2: 16:14:49.919172 10.23.2.2.810 > 239.255.123.123.890:  udp 32 Drop-reason:
 (punt-rate-limit) Punt rate limit exceeded
2 packets shown
```

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация