Solucionar problemas do Firepower Threat Defense e do ASA Multicast PIM

Contents

Introdução

Este documento descreve como o Firepower Threat Defense (FTD) e o Adaptive Security Appliance (ASA) implementam o Protocol Independent Multicast (PIM).

Pré-requisitos

Requisitos

Conhecimento básico de roteamento IP.

Componentes Utilizados

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

As informações neste documento são baseadas nestas versões de software e hardware:

- Defesa contra ameaças do Cisco Firepower 4125 versão 7.1.0.
- Firepower Management Center (FMC) versão 7.1.0.
- Software Cisco Adaptive Security Appliance Versão 9.17(1)9.

Informações de Apoio

Conceitos básicos de roteamento multicast

- O unicast encaminha pacotes para o destino enquanto o **multicast** encaminha pacotes para longe da origem.
- Os dispositivos de rede multicast (firewalls/roteadores e assim por diante) encaminham os pacotes via **Reverse Path Forwarding (RPF).** Observe que o RPF não é o mesmo que o uRPF usado no unicast para evitar tipos específicos de ataques. O RPF pode ser definido como um mecanismo que encaminha pacotes multicast para longe da origem, fora das interfaces que levam em direção aos receptores multicast. Sua função principal é evitar loops de tráfego e garantir caminhos de tráfego corretos.
- Um protocolo multicast como o PIM tem 3 funções principais:

1. Localize a **interface upstream** (interface mais próxima à origem).

2. Localize as **interfaces downstream** associadas a um fluxo multicast específico (interfaces para os receptores).

3. Mantenha a árvore multicast (adicione ou remova os ramos da árvore).

- Uma árvore multicast pode ser construída e mantida por um dos dois métodos: **junções implícitas (flood-and-prune)** ou **junções explícitas (modelo pull).** O PIM Dense Mode (PIM-DM) usa junções implícitas, enquanto o PIM Sparse Mode (PIM-SM) usa junções explícitas.
- Uma árvore multicast pode ser **compartilhada** ou **baseada na origem:**
  - As árvores compartilhadas usam o conceito de **Ponto de Reunião (RP)** e são anotadas como **(*, G)** onde G = IP de grupo multicast.
  - As árvores baseadas na origem são enraizadas na origem, não usam um RP e são observadas como **(S, G)**, onde S = o IP da origem/servidor multicast.
- Modelos de encaminhamento multicast:
  - **O** modo de entrega **Multicast de qualquer origem (ASM)** usa árvores compartilhadas (*, G) onde qualquer origem pode enviar o fluxo multicast.
  - **O Source-Specific Multicast (SSM)** usa árvores baseadas em origem (S, G) e o intervalo IP 232/8.
  - **Bidirecional (BiDir)** é um tipo de árvore compartilhada (*, G) onde o tráfego do plano de controle e do plano de dados passa pelo RP.
- Um ponto de encontro pode ser configurado ou escolhido com um destes métodos:
  - RP estático
  - RP automático
  - Roteador de bootstrap (BSR)

Resumo de modos PIM

modo PIM	**RP**	**Árvore compartilhada**	**Notação**	**IGMP**	**ASA/FTD com suporte**
Modo escasso do	Yes	Yes	(*, G) e (S,	v1/v2/v3	Yes

PIM			G)		
Modo denso de PIM	No	No	S, G)	v1/v2/v3	Não*
Modo bidirecional PIM	Yes	Yes	(*, G)	v1/v2/v3	Yes
Modo PIM Source-Specific-Multicast (SSM)	No	No	S, G)	v3	Não**

*RP automático = O tráfego RP automático pode passar

** ASA/FTD não pode ser um dispositivo de último salto

resumo de configuração de RP

Configuração do ponto de encontro	**ASA/FTD**
RP estático	Yes
RP automático	Não, mas o tráfego do plano de controle de RP automático pode passar
BSR	Sim, mas não suporte a C-RP

> **Observação**: antes de começar a solucionar qualquer problema multicast, é muito importante ter uma visão clara da topologia multicast. Especificamente, no mínimo, você precisa saber:
> - Qual é a função do firewall na topologia multicast?
> - Quem é o RP?
> - Quem é o remetente do fluxo multicast (IP de origem e IP de grupo multicast)?
> - Quem é o receptor do fluxo multicast?
> - Você tem problemas com o plano de controle (IGMP/PIM) ou o plano de dados (fluxo multicast) em si?

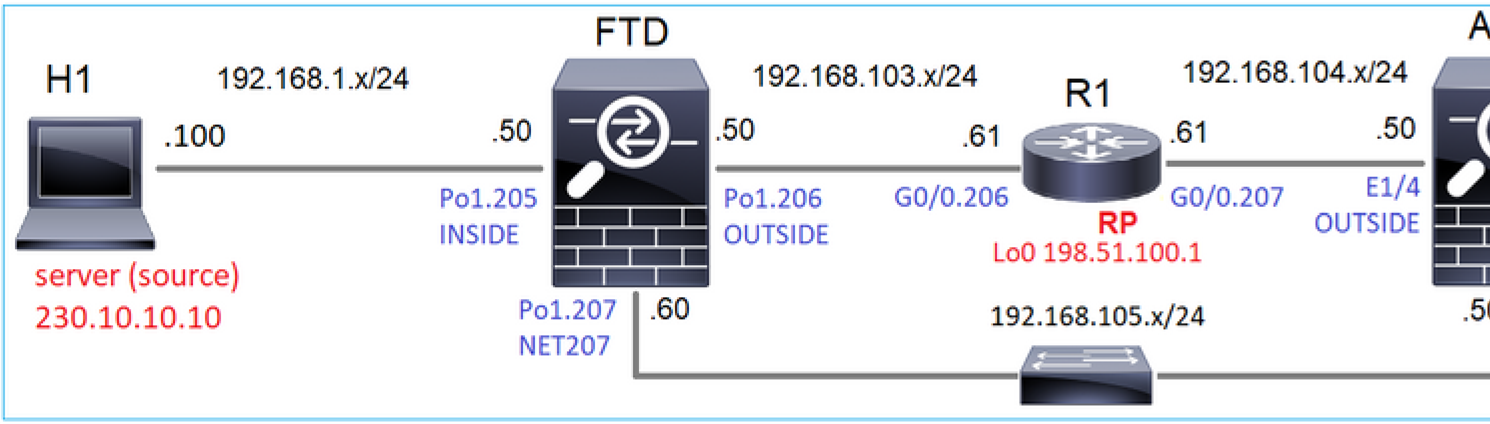
Abreviações/acrônimos

Acrônimos	**Explicação**
FHR	Roteador de primeiro salto - um salto diretamente conectado à origem

	do tráfego multicast.
LHR	Roteador de último salto - um salto diretamente conectado aos receptores do tráfego multicast.
RP	Ponto de reunião
DR.	Roteador designado
SPT	Árvore de caminho mais curto
RPT	Árvore Rendezvous-Point (RP), árvore de compartilhamento
RPF	Encaminhamento de caminho reverso
ÓLEO	Lista de interface de saída
MRIB	Base de Informações de Roteamento Multicast
MFIB	Base de Informações de Encaminhamento Multicast
ASM	Multicast de qualquer origem
BSR	Roteador Bootstrap
SSM	Multicast específico da origem
FP	Caminho rápido
SP	Caminho Lento
CP	Ponto de controle
PPS	Taxa de pacotes por segundo

Tarefa 1 - Modo PIM escasso (RP estático)

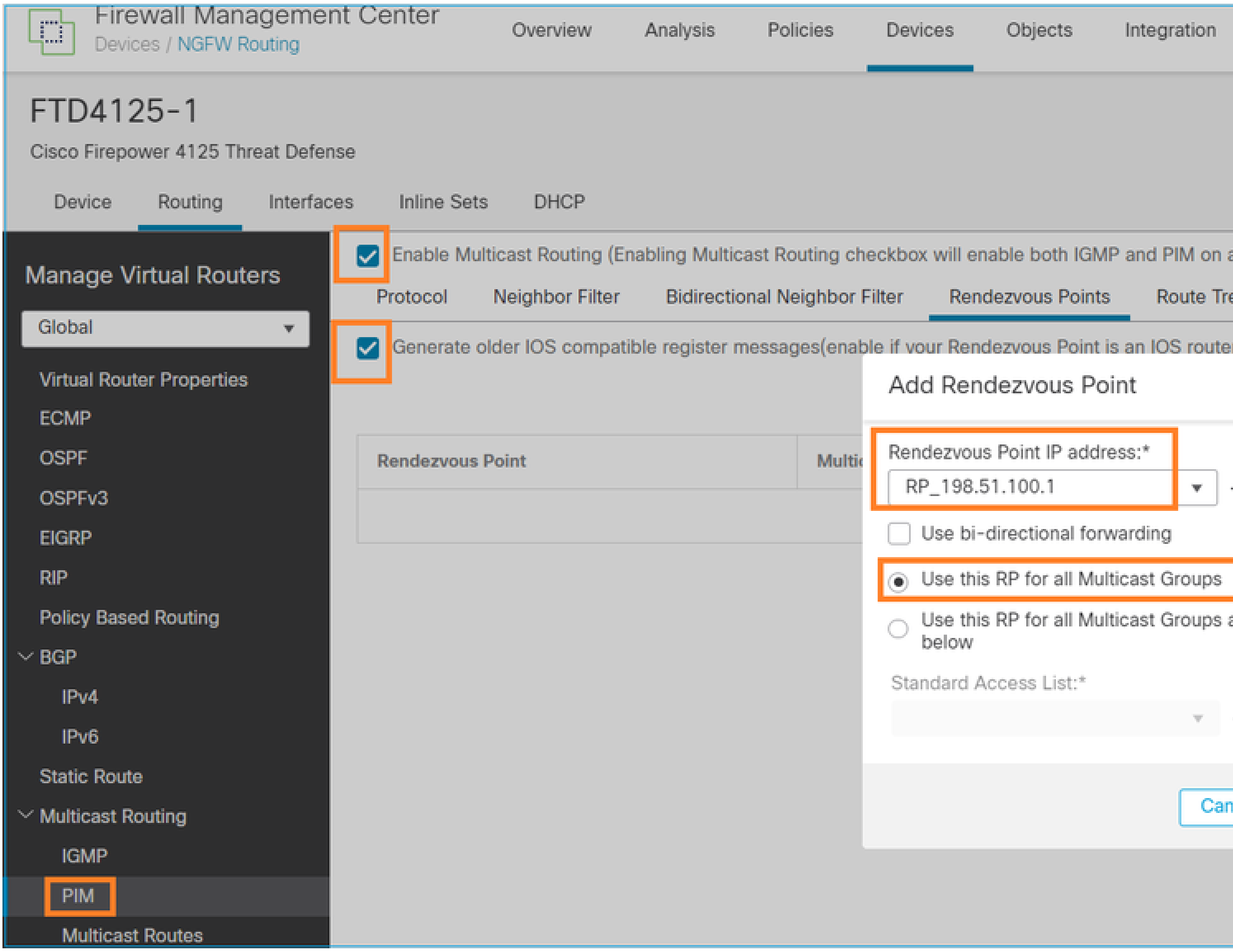
Topologia



Configure o modo escasso de PIM multicast na topologia com R1 (198.51.100.1) como RP.

Solução

Configuração de FTD:



☑ Enable Multicast Routing (Enabling Multicast Routing checkbox will enable both IGMP and PIM on a

☑ Generate older IOS compatible register messages(enable if your Rendezvous Point is an IOS route

Add Rendezvous Point

Rendezvous Point IP address:* RP_198.51.100.1

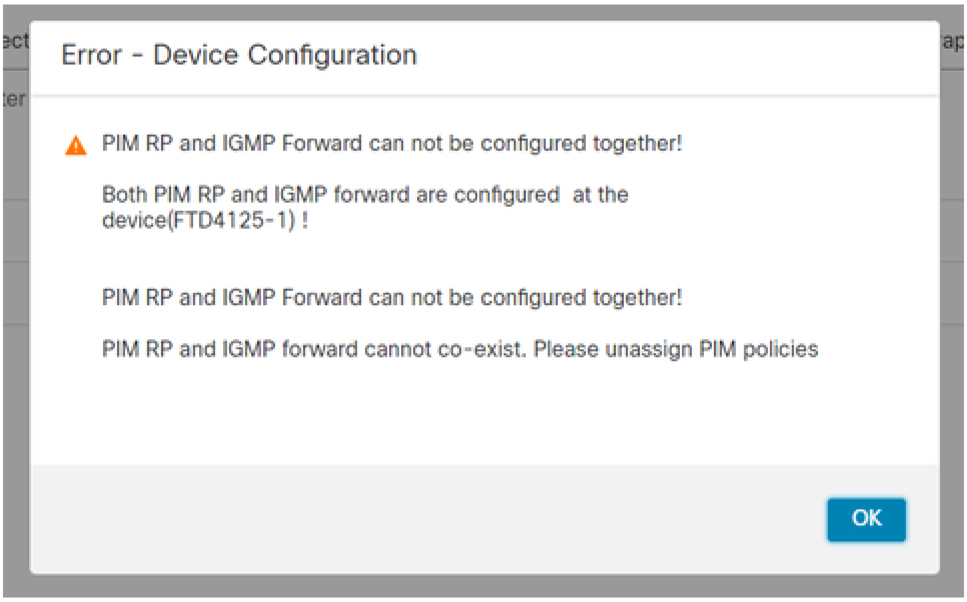
□ Use bi-directional forwarding

● Use this RP for all Multicast Groups

○ Use this RP for all Multicast Groups a below

Standard Access List:*

O ASA/FTD não pode ser configurado para roteamento stub IGMP e PIM ao mesmo tempo:



Error - Device Configuration

PIM RP and IGMP Forward can not be configured together!

Both PIM RP and IGMP forward are configured at the device(FTD4125-1) !

PIM RP and IGMP Forward can not be configured together!

PIM RP and IGMP forward cannot co-exist. Please unassign PIM policies

A configuração resultante no FTD:

<#root>

```
firepower#

show running-config multicast-routing


multicast-routing


<-- Multicast routing is enabled globally on the device

firepower#

show running-config pim


pim rp-address 198.51.100.1              <-- Static RP is configured on the firewall



firepower#

ping 198.51.100.1


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.51.100.1, timeout is 2 seconds:

!!!!!                                    <-- The RP is reachable


Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

No firewall ASA, há uma configuração semelhante:

<#root>

```
asa(config)#

multicast-routing


asa(config)#

pim rp-address 198.51.100.1
```

Configuração do RP (roteador Cisco):

<#root>

```
ip multicast-routing

ip pim rp-address 198.51.100.1           <-- The router is the RP

!
interface GigabitEthernet0/0.206
 encapsulation dot1Q 206
 ip address 192.168.103.61 255.255.255.0

 ip pim sparse-dense-mode                <-- The interface participates in multicast routing

 ip ospf 1 area 0
!
interface GigabitEthernet0/0.207
 encapsulation dot1Q 207
 ip address 192.168.104.61 255.255.255.0

 ip pim sparse-dense-mode                <-- The interface participates in multicast routing

 ip ospf 1 area 0
!
interface Loopback0


ip address 198.51.100.1 255.255.255.255

<-- The router is the RP


ip pim sparse-dense-mode                <-- The interface participates in multicast routing

 ip ospf 1 area 0
```

Verificação

Verifique o plano de controle multicast no FTD quando não houver tráfego multicast (remetentes ou receptores):

<#root>

```
firepower#

show pim interface

Address            Interface         PIM  Nbr   Hello  DR          DR
                                          Count Intvl  Prior

192.168.105.60     NET207            on   1     30     1           this system


<-- PIM enabled on the interface. There is 1 PIM neighbor

192.168.1.50       INSIDE            on   0     30     1           this system       <-- PIM enabled on t

0.0.0.0            diagnostic        off  0     30     1           not elected

192.168.103.50     OUTSIDE           on   1     30     1           192.168.103.61    <-- PIM enabled on t
```

Verifique os vizinhos PIM:

<#root>

```
firepower#

show pim neighbor

Neighbor Address    Interface          Uptime    Expires DR pri Bidir
192.168.105.50      NET207             00:05:41  00:01:28 1      B
192.168.103.61      OUTSIDE            00:05:39  00:01:32 1 (DR)
```

O RP anuncia todo o intervalo do grupo multicast:

<#root>

```
firepower#

show pim group-map

Group Range         Proto   Client   Groups RP address      Info
224.0.1.39/32*      DM      static   0      0.0.0.0
224.0.1.40/32*      DM      static   0      0.0.0.0
224.0.0.0/24*       L-Local static   1      0.0.0.0
232.0.0.0/8*        SSM     config   0      0.0.0.0

224.0.0.0/4*        SM      config   2      198.51.100.1    RPF: OUTSIDE,192.168.103.61     <-- The mult

224.0.0.0/4         SM      static   0      0.0.0.0         RPF: ,0.0.0.0
```

A tabela mroute do firewall tem algumas entradas não relevantes (239.255.255.250 é o protocolo SSDP usado por fornecedores como MAC OS e Microsoft Windows):

<#root>

```
firepower#

show mroute
```

```
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(*, 239.255.255.250), 00:17:35/never, RP 198.51.100.1, flags: SCJ
  Incoming interface: OUTSIDE
  RPF nbr: 192.168.103.61
  Immediate Outgoing interface list:
    INSIDE, Forward, 00:17:35/never
```

Há um túnel PIM construído entre os firewalls e o RP:

<#root>

```
firepower#

show pim tunnel

Interface           RP Address        Source Address

Tunnel0             198.51.100.1      192.168.103.50


<-- PIM tunnel between the FTD and the RP
```

O túnel PIM também pode ser visto na tabela de conexão do firewall:

<#root>

```
firepower#

 show conn all detail address 198.51.100.1
...
PIM OUTSIDE: 198.51.100.1/0 NP Identity Ifc: 192.168.103.50/0,


<-- PIM tunnel between the FTD and the RP
, flags , idle 16s, uptime 3m8s, timeout 2m0s, bytes 6350
Connection lookup keyid: 153426246
```

Verificação no firewall ASA:

<#root>

```
asa#

show pim neighbor
```

```
Neighbor Address   Interface      Uptime     Expires DR pri Bidir
192.168.105.60     NET207         2d21h      00:01:29 1 (DR) B
192.168.104.61     OUTSIDE        00:00:18   00:01:37 1 (DR)
```

<#root>

```
asa#

show pim tunnel

Interface          RP Address        Source Address

Tunnel0            198.51.100.1      192.168.104.50


<-- PIM tunnel between the ASA and the RP
```

Verificação RP (Cisco router) RP. Existem alguns grupos multicast para SSDP e RP automático:

<#root>

```
Router1#

show ip pim rp

Group: 239.255.255.250, RP: 198.51.100.1, next RP-reachable in 00:01:04
Group: 224.0.1.40, RP: 198.51.100.1, next RP-reachable in 00:00:54
```

Verificação após o receptor anunciar sua presença

> **Observação**: os comandos de firewall mostrados nesta seção são totalmente aplicáveis ao ASA e ao FTD.

O ASA recebe a mensagem de Relatório de Associação IGMP e cria as entradas IGMP e mroute (*, G):

<#root>

```
asa#

show igmp group 230.10.10.10

IGMP Connected Group Membership
Group Address    Interface           Uptime    Expires   Last Reporter

230.10.10.10     INSIDE              00:01:15  00:03:22  192.168.2.100     <-- Host 192.168.2.100 repor
```

O firewall ASA cria uma mroute para o grupo multicast:

<#root>

```
asa#

show mroute 230.10.10.10


Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State


(*, 230.10.10.10)

, 00:00:17/never,

RP 198.51.100.1

, flags: SCJ

<-- The mroute for group 230.10.10.10



Incoming interface: OUTSIDE



<-- Expected interface for a multicast packet from the source. If the packet is not received on this int

  RPF nbr: 192.168.104.61


 Immediate Outgoing interface list:                                 <-- The OIL points towards the recei
    INSIDE, Forward, 00:01:17/never
```

Outra verificação de firewall é a saída da topologia PIM:

<#root>

```
asa#

show pim topology 230.10.10.10

...

(*,230.10.10.10) SM Up: 00:07:15 RP: 198.51.100.1                   <-- An entry for multicast group 23

JP: Join(00:00:33) RPF: OUTSIDE,192.168.104.61 Flags: LH
  INSIDE             00:03:15  fwd LI LH
```

> **Observação**: se o firewall não tiver uma rota em direção ao RP, a saída **debug pim** mostrará uma falha de pesquisa de RPF

Falha de pesquisa de RPF na saída de **debug pim**:

<#root>

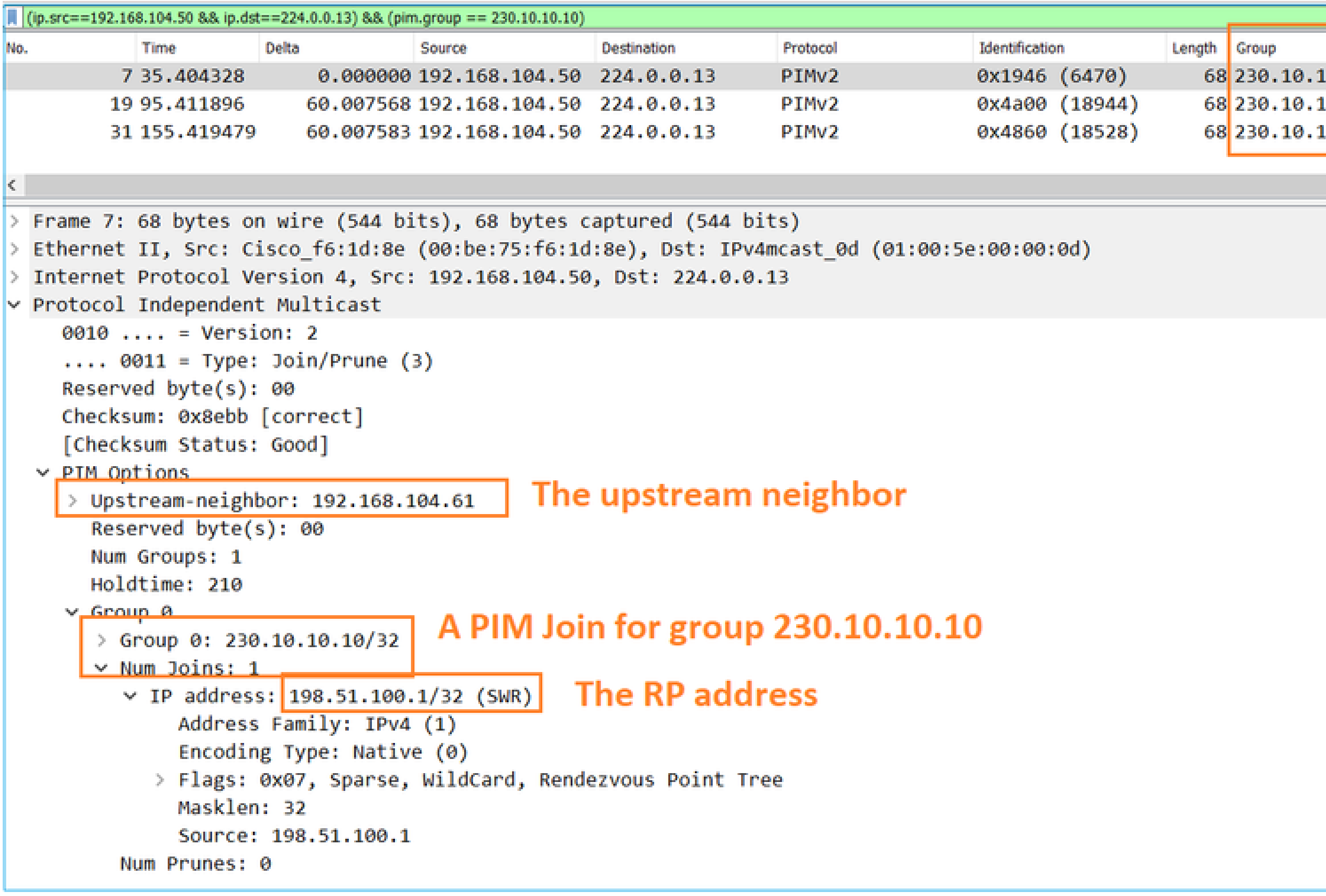
```
asa#

debug pim



IPv4 PIM: RPF lookup failed for root 198.51.100.1                    <-- The RPF look fails because ther

IPv4 PIM: RPF lookup failed for root 198.51.100.1



IPv4 PIM: (*,230.10.10.10) Processing Periodic Join-Prune timer
IPv4 PIM: (*,230.10.10.10) J/P processing
IPv4 PIM: (*,230.10.10.10) Periodic J/P scheduled in 50 secs
IPv4 PIM: (*,230.10.10.10) No RPF neighbor to send J/P
```

Caso tudo esteja OK, o firewall envia uma mensagem PIM Join-Prune ao RP:

<#root>

```
asa#

debug pim group 230.10.10.10


IPv4 PIM group debugging is on
for group 230.10.10.10

IPv4 PIM: (*,230.10.10.10) J/P scheduled in 0.0 secs
IPv4 PIM: [0] (*,230.10.10.10/32) MRIB modify A NS
IPv4 PIM: [0] (*,230.10.10.10/32) NULLIF-skip MRIB modify !A !NS
IPv4 PIM: [0] (*,230.10.10.10/32) OUTSIDE MRIB modify A NS
IPv4 PIM: (*,230.10.10.10) Processing timers
IPv4 PIM: (*,230.10.10.10) J/P processing
IPv4 PIM: (*,230.10.10.10) Periodic J/P scheduled in 50 secs

IPv4 PIM: (*,230.10.10.10) J/P adding Join on OUTSIDE
```

A captura mostra que as mensagens PIM Join são enviadas a cada 1 min e PIM Hellos a cada 30 segundos.
O PIM usa o IP 224.0.0.13:



```
(ip.src==192.168.104.50 && ip.dst==224.0.0.13) && (pim.group == 230.10.10.10)

No.    Time          Delta      Source          Destination  Protocol  Identification   Length  Group
     7 35.404328     0.000000  192.168.104.50  224.0.0.13   PIMv2     0x1946 (6470)        68  230.10.1
    19 95.411896    60.007568  192.168.104.50  224.0.0.13   PIMv2     0x4a00 (18944)       68  230.10.1
    31 155.419479   60.007583  192.168.104.50  224.0.0.13   PIMv2     0x4860 (18528)       68  230.10.1

> Frame 7: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
> Ethernet II, Src: Cisco_f6:1d:8e (00:be:75:f6:1d:8e), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
> Internet Protocol Version 4, Src: 192.168.104.50, Dst: 224.0.0.13
v Protocol Independent Multicast
    0010 .... = Version: 2
    .... 0011 = Type: Join/Prune (3)
    Reserved byte(s): 00
    Checksum: 0x8ebb [correct]
    [Checksum Status: Good]
  v PIM Options
    > Upstream-neighbor: 192.168.104.61
      Reserved byte(s): 00
      Num Groups: 1
      Holdtime: 210
    v Group 0
      > Group 0: 230.10.10.10/32
      v Num Joins: 1
        v IP address: 198.51.100.1/32 (SWR)
            Address Family: IPv4 (1)
            Encoding Type: Native (0)
          > Flags: 0x07, Sparse, WildCard, Rendezvous Point Tree
            Masklen: 32
            Source: 198.51.100.1
        Num Prunes: 0
```

Dica: filtro de exibição do Wireshark: (ip.src==192.168.104.50 && ip.dst==224.0.0.13) && (pim.group == 230.10.10.10)
- 192.168.104.50 é o IP de firewall da interface de saída (em direção ao vizinho PIM upstream)
- 224.0.0.13 é o grupo multicast PIM para o qual as junções e remoções PIM são enviadas
- 230.10.10.10 é o grupo multicast para o qual enviamos a junção/remoção PIM

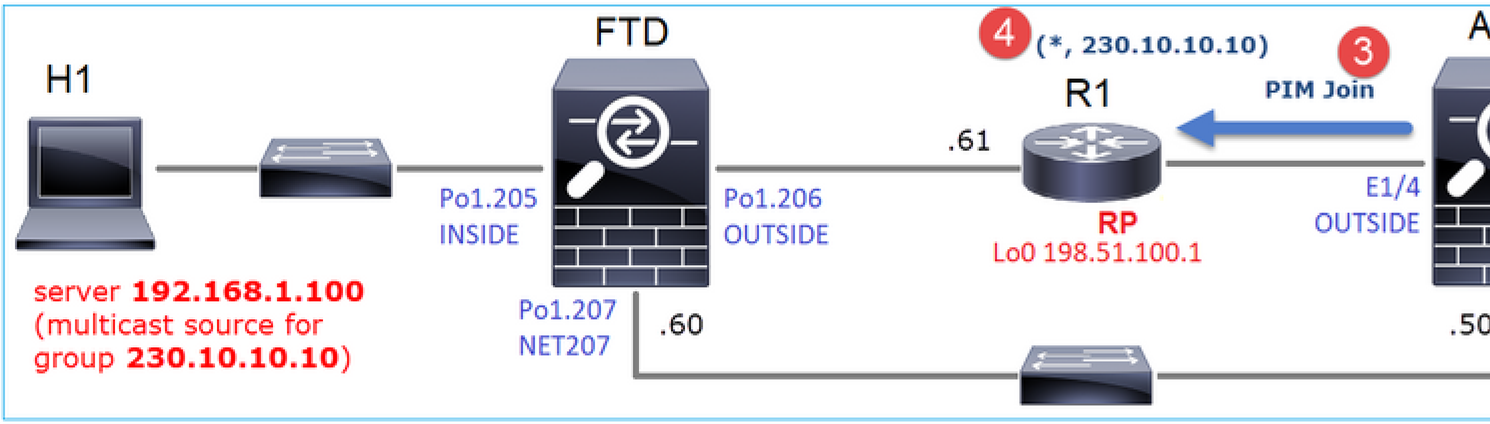
O RP cria um mroute (*, G). Observe que como ainda não há nenhum servidor, a interface de entrada é nula:

<#root>

```
Router1#

show ip mroute 230.10.10.10 | b \(



(*, 230.10.10.10), 00:00:27/00:03:02, RP 198.51.100.1, flags: S          <-- The mroute for the multicas



Incoming interface: Null

, RPF nbr 0.0.0.0         <-- No incoming multicast stream


Outgoing interface list:
```

```
GigabitEthernet0/0.207

, Forward/Sparse-Dense, 00:00:27/00:03:02

<-- There was a PIM Join on this interface
```

Isso pode ser visualizado da seguinte maneira:



1. O relatório IGMP é recebido no ASA.
2. Um (*, G) mroute é adicionado.
3. O ASA envia uma mensagem PIM Join para o RP (198.51.100.1).
4. O RP recebe a mensagem Join e adiciona um mroute (*, G).

Ao mesmo tempo, no FTD, não há mroutes, pois não houve Relatório IGMP nem PIM Join recebido:

<#root>

```
firepower#

show mroute 230.10.10.10

No mroute entries found.
```

Verificação de quando o servidor envia um fluxo multicast

O FTD obtém o fluxo multicast de H1 e inicia o **processo de Registro PIM** com o RP. O FTD envia uma mensagem **unicast PIM Register** ao RP. O RP envia uma mensagem de **PIM Join** para o First-Hop-Router (FHR), que é o FTD neste caso, para se unir à árvore multicast. Em seguida, ele envia uma mensagem **Register-Stop**.

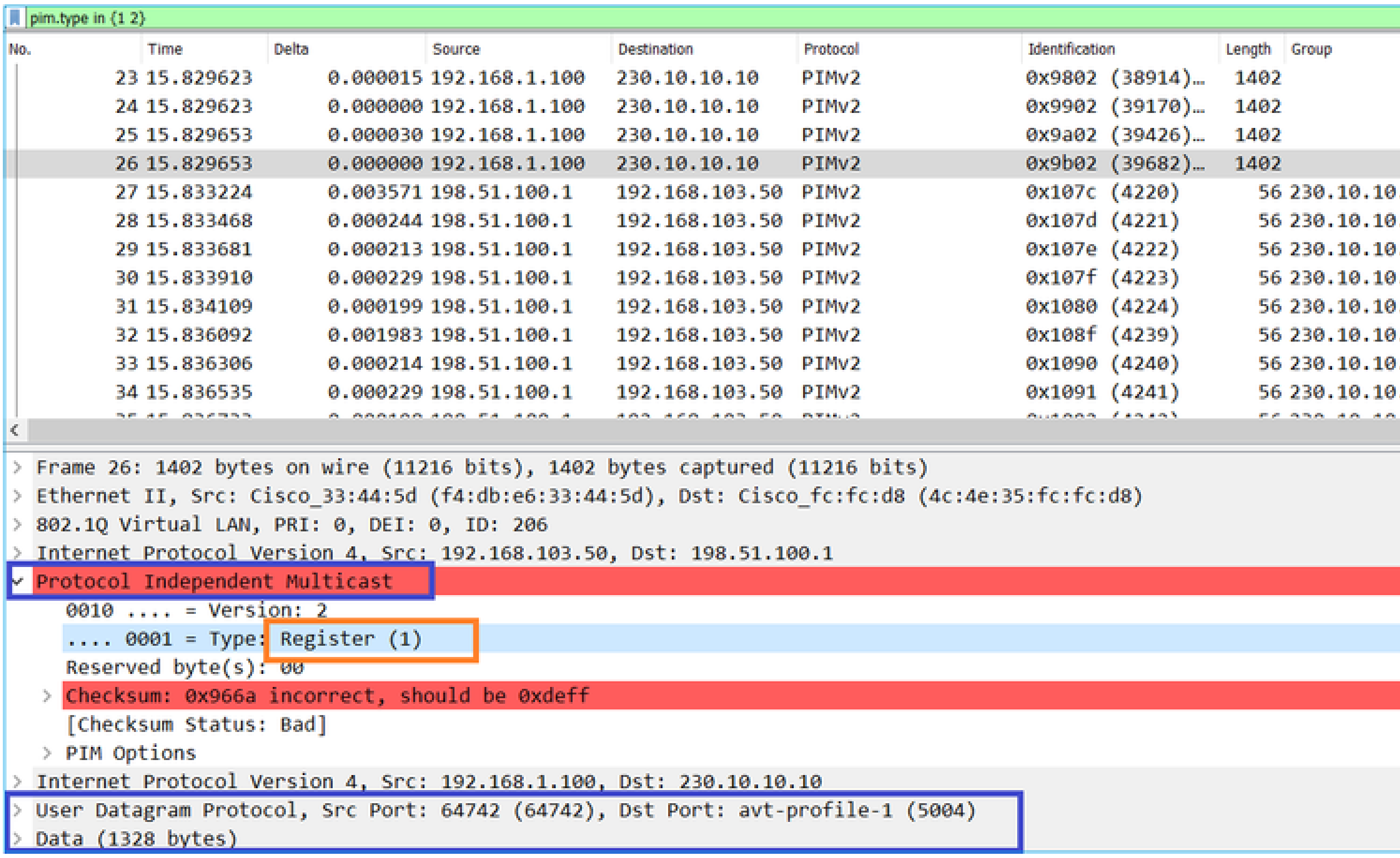
<#root>

```
firepower#

debug pim group 230.10.10.10


IPv4 PIM group debugging is on
for group 230.10.10.10
```

```
firepower#
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB update (f=20,c=20)
IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on INSIDE
IPv4 PIM: (192.168.1.100,230.10.10.10) Create entry

IPv4 PIM: (192.168.1.100,230.10.10.10) RPF changed from 0.0.0.0/- to 192.168.1.100/INSIDE



<-- The FTD receives a multicast stream on INSIDE interface for group 230.10.10.10


IPv4 PIM: (192.168.1.100,230.10.10.10) Connected status changed from off to on
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify NS
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) MRIB modify DC
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify A NS
IPv4 PIM: (192.168.1.100,230.10.10.10) Set alive timer to 210 sec
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify !NS
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) MRIB modify !DC

IPv4 PIM: (192.168.1.100,230.10.10.10) Start registering to 198.51.100.1                    <-- The FTD


IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 J/P state changed from Null to Join
IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 FWD state change from Prune to Forward
IPv4 PIM: (192.168.1.100,230.10.10.10) Updating J/P status from Null to Join
IPv4 PIM: (192.168.1.100,230.10.10.10) J/P scheduled in 0.0 secs
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB modify NS
IPv4 PIM: (192.168.1.100,230.10.10.10) Set SPT bit
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) MRIB modify NS
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify !A
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB modify A !NS
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) Tunnel0 MRIB modify F NS
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB modify !SP
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB update (f=2,c=20)

IPv4 PIM: J/P entry: Join root: 192.168.1.100 group: 230.10.10.10 flags: S                  <-- The FTD


IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE J/P state changed from Null to Join
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE FWD state change from Prune to Forward
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify F NS
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE Raise J/P expiration timer to 210 seconds
IPv4 PIM: J/P entry: Join root: 192.168.1.100 group: 230.10.10.10 flags: S
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE Raise J/P expiration timer to 210 seconds
IPv4 PIM: (192.168.1.100,230.10.10.10) Processing timers
IPv4 PIM: (192.168.1.100,230.10.10.10) J/P processing
IPv4 PIM: (192.168.1.100,230.10.10.10) Suppress J/P to connected source
IPv4 PIM: (192.168.1.100,230.10.10.10) Suppress J/P to connected source
IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 Processing timers
IPv4 PIM: J/P entry: Join root: 192.168.1.100 group: 230.10.10.10 flags: S
IPv4 PIM: (192.168.1.100,230.10.10.10) NET207 J/P state changed from Null to Join
IPv4 PIM: (192.168.1.100,230.10.10.10) NET207 FWD state change from Prune to Forward
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify F NS
IPv4 PIM: (192.168.1.100,230.10.10.10) NET207 Raise J/P expiration timer to 210 seconds
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=29,c=20)
IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on NET207
IPv4 PIM: (192.168.1.100,230.10.10.10) Send [0/0] Assert on NET207
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify !SP
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=9,c=20)
IPv4 PIM: J/P entry: Prune root: 192.168.1.100 group: 230.10.10.10 flags: S
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE J/P state changed from Join to Null
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE FWD state change from Forward to Prune
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify !F !NS
```

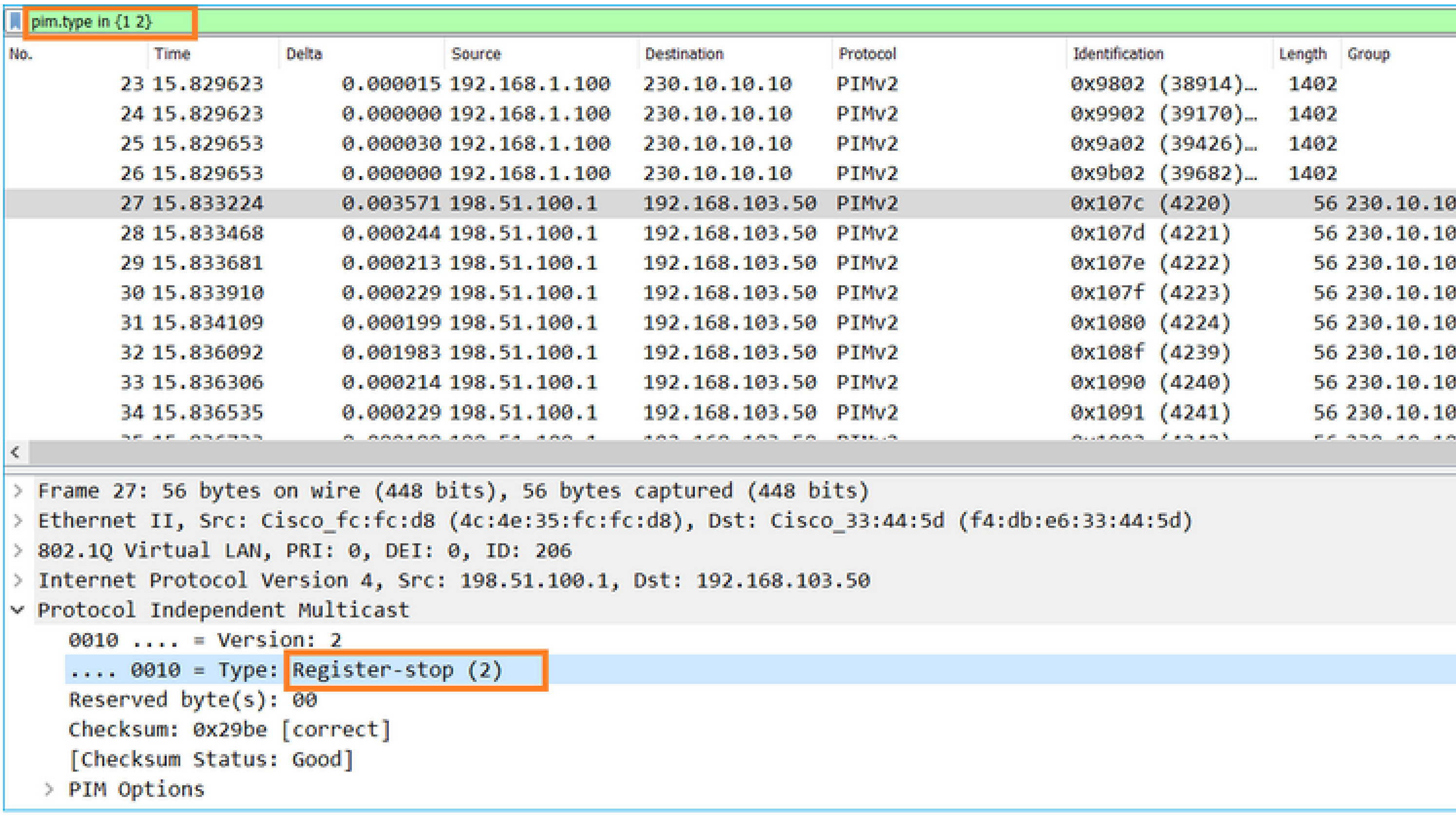
```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=29,c=20)
IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on NET207
IPv4 PIM: (192.168.1.100,230.10.10.10) Send [0/0] Assert on NET207
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify !SP
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=9,c=20)
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE Processing timers

IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop                               <-- The RP s


IPv4 PIM: (192.168.1.100,230.10.10.10) Stop registering


IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 J/P state changed from Join to Null
IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 FWD state change from Forward to Prune
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) Tunnel0 MRIB modify !F !NS
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 Processing timers
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB update (f=22,c=20)
IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on INSIDE
IPv4 PIM: (192.168.1.100,230.10.10.10) Set alive timer to 210 sec
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB modify !SP
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB update (f=2,c=20)
```

A mensagem PIM Register é uma mensagem PIM que transporta dados UDP juntamente com as informações de PIM Register:



```
pim.type in {1 2}
No.     Time      Delta    Source         Destination     Protocol  Identification    Length Group
     23 15.829623 0.000015 192.168.1.100  230.10.10.10    PIMv2     0x9802 (38914)…   1402
     24 15.829623 0.000000 192.168.1.100  230.10.10.10    PIMv2     0x9902 (39170)…   1402
     25 15.829653 0.000030 192.168.1.100  230.10.10.10    PIMv2     0x9a02 (39426)…   1402
     26 15.829653 0.000000 192.168.1.100  230.10.10.10    PIMv2     0x9b02 (39682)…   1402
     27 15.833224 0.003571 198.51.100.1   192.168.103.50  PIMv2     0x107c (4220)       56 230.10.10
     28 15.833468 0.000244 198.51.100.1   192.168.103.50  PIMv2     0x107d (4221)       56 230.10.10
     29 15.833681 0.000213 198.51.100.1   192.168.103.50  PIMv2     0x107e (4222)       56 230.10.10
     30 15.833910 0.000229 198.51.100.1   192.168.103.50  PIMv2     0x107f (4223)       56 230.10.10
     31 15.834109 0.000199 198.51.100.1   192.168.103.50  PIMv2     0x1080 (4224)       56 230.10.10
     32 15.836092 0.001983 198.51.100.1   192.168.103.50  PIMv2     0x108f (4239)       56 230.10.10
     33 15.836306 0.000214 198.51.100.1   192.168.103.50  PIMv2     0x1090 (4240)       56 230.10.10
     34 15.836535 0.000229 198.51.100.1   192.168.103.50  PIMv2     0x1091 (4241)       56 230.10.10

> Frame 26: 1402 bytes on wire (11216 bits), 1402 bytes captured (11216 bits)
> Ethernet II, Src: Cisco_33:44:5d (f4:db:e6:33:44:5d), Dst: Cisco_fc:fc:d8 (4c:4e:35:fc:fc:d8)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 206
> Internet Protocol Version 4, Src: 192.168.103.50, Dst: 198.51.100.1
v Protocol Independent Multicast
    0010 .... = Version: 2
    .... 0001 = Type: Register (1)
    Reserved byte(s): 00
  > Checksum: 0x966a incorrect, should be 0xdeff
    [Checksum Status: Bad]
  > PIM Options
> Internet Protocol Version 4, Src: 192.168.1.100, Dst: 230.10.10.10
> User Datagram Protocol, Src Port: 64742 (64742), Dst Port: avt-profile-1 (5004)
> Data (1328 bytes)
```

A mensagem PIM Register-Stop:



```
pim.type in {1 2}
No.     Time      Delta    Source         Destination     Protocol  Identification    Length Group
     23 15.829623 0.000015 192.168.1.100  230.10.10.10    PIMv2     0x9802 (38914)…   1402
     24 15.829623 0.000000 192.168.1.100  230.10.10.10    PIMv2     0x9902 (39170)…   1402
     25 15.829653 0.000030 192.168.1.100  230.10.10.10    PIMv2     0x9a02 (39426)…   1402
     26 15.829653 0.000000 192.168.1.100  230.10.10.10    PIMv2     0x9b02 (39682)…   1402
     27 15.833224 0.003571 198.51.100.1   192.168.103.50  PIMv2     0x107c (4220)       56 230.10.10
     28 15.833468 0.000244 198.51.100.1   192.168.103.50  PIMv2     0x107d (4221)       56 230.10.10
     29 15.833681 0.000213 198.51.100.1   192.168.103.50  PIMv2     0x107e (4222)       56 230.10.10
     30 15.833910 0.000229 198.51.100.1   192.168.103.50  PIMv2     0x107f (4223)       56 230.10.10
     31 15.834109 0.000199 198.51.100.1   192.168.103.50  PIMv2     0x1080 (4224)       56 230.10.10
     32 15.836092 0.001983 198.51.100.1   192.168.103.50  PIMv2     0x108f (4239)       56 230.10.10
     33 15.836306 0.000214 198.51.100.1   192.168.103.50  PIMv2     0x1090 (4240)       56 230.10.10
     34 15.836535 0.000229 198.51.100.1   192.168.103.50  PIMv2     0x1091 (4241)       56 230.10.10

> Frame 27: 56 bytes on wire (448 bits), 56 bytes captured (448 bits)
> Ethernet II, Src: Cisco_fc:fc:d8 (4c:4e:35:fc:fc:d8), Dst: Cisco_33:44:5d (f4:db:e6:33:44:5d)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 206
> Internet Protocol Version 4, Src: 198.51.100.1, Dst: 192.168.103.50
v Protocol Independent Multicast
    0010 .... = Version: 2
    .... 0010 = Type: Register-stop (2)
    Reserved byte(s): 00
    Checksum: 0x29be [correct]
    [Checksum Status: Good]
  > PIM Options
```

Dica: para exibir somente mensagens PIM Register e PIM Register-Stop no Wireshark, você pode usar o filtro de exibição: pim.type em {1 2}

O firewall (roteador do último salto) obtém o fluxo de multicast na interface EXTERNA e inicia o switchover da Shortest Path Tree (SPT) para a interface NET207:

<#root>

```
asa#

debug pim group 230.10.10.10


IPv4 PIM group debugging is on
for group 230.10.10.10

IPv4 PIM: (*,230.10.10.10) Processing Periodic Join-Prune timer
IPv4 PIM: (*,230.10.10.10) J/P processing
IPv4 PIM: (*,230.10.10.10) Periodic J/P scheduled in 50 secs
IPv4 PIM: (*,230.10.10.10) J/P adding Join on OUTSIDE

<-- A PIM Join message is sent from the interface OUTSIDE


IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB update (f=20,c=20)

IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on OUTSIDE                          <-- The m


IPv4 PIM: (192.168.1.100,230.10.10.10) Create entry
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify NS

IPv4 PIM: (192.168.1.100,230.10.10.10) RPF changed from 0.0.0.0/- to 192.168.105.60/NET207



<-- The SPT switchover starts from the interface OUTSIDE to the interface NET207


IPv4 PIM: (192.168.1.100,230.10.10.10) Source metric changed from [0/0] to [110/20]
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) MRIB modify DC
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify A NS
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB modify F NS
IPv4 PIM: (192.168.1.100,230.10.10.10) Set alive timer to 210 sec
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify !NS
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) MRIB modify !DC
IPv4 PIM: (192.168.1.100,230.10.10.10) Updating J/P status from Null to Join
IPv4 PIM: (192.168.1.100,230.10.10.10) J/P scheduled in 0.0 secs
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify NS
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify !SP
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB update (f=2,c=20)
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=28,c=20)
IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on NET207
IPv4 PIM: (192.168.1.100,230.10.10.10)

Set SPT bit                                             <-- The SPT bit is set


IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) MRIB modify !SP
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify !A
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify A !NS
IPv4 PIM: (192.168.1.100,230.10.10.10)RPT Updating J/P status from Null to Prune
IPv4 PIM: (192.168.1.100,230.10.10.10)RPT Create entry
IPv4 PIM: (192.168.1.100,230.10.10.10)RPT J/P scheduled in 0.0 secs
IPv4 PIM: (192.168.1.100,230.10.10.10) Set alive timer to 210 sec
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify !SP
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=2,c=20)
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10)RPT Processing timers
IPv4 PIM: (192.168.1.100,230.10.10.10)RPT J/P processing
```

IPv4 PIM: (192.168.1.100,230.10.10.10)RPT J/P adding Prune on OUTSIDE

<-- A PIM Prune message is sent from the interface OUTSIDE

```
IPv4 PIM: (192.168.1.100,230.10.10.10)RPT Delete entry
IPv4 PIM: (192.168.1.100,230.10.10.10) Processing timers
IPv4 PIM: (192.168.1.100,230.10.10.10) J/P processing
IPv4 PIM: (192.168.1.100,230.10.10.10) Periodic J/P scheduled in 50 secs
```

IPv4 PIM: (192.168.1.100,230.10.10.10) J/P adding Join on NET207

<-- A PIM Join message is sent from the interface NET207

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=22,c=20)
IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on NET207
IPv4 PIM: (192.168.1.100,230.10.10.10) Set alive timer to 210 sec
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify !SP
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=2,c=20)
```

A depuração PIM no FTD quando ocorre o switchover:

<#root>

```
IPv4 PIM: J/P entry: Join root: 192.168.1.100 group: 230.10.10.10 flags: S
```

IPv4 PIM: (192.168.1.100,230.10.10.10) NET207 J/P state changed from Null to Join

<-- A PIM Join message is sent from the interface NET207

IPv4 PIM: (192.168.1.100,230.10.10.10) NET207 FWD state change from Prune to Forward

<-- The packets are sent from the interface NET207

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify F NS
IPv4 PIM: (192.168.1.100,230.10.10.10) NET207 Raise J/P expiration timer to 210 seconds
IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 Processing timers
...
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=9,c=20)
IPv4 PIM: J/P entry: Prune root: 192.168.1.100 group: 230.10.10.10 flags: S
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE J/P state changed from Join to Null
```

IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE FWD state change from Forward to Prune

<-- A PIM Prune message is sent from the interface OUTSIDE

O FTD mroute assim que o switchover de SPT inicia:

<#root>

```
firepower#

show mroute 230.10.10.10


Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(192.168.1.100, 230.10.10.10), 00:00:06/00:03:23, flags: SF

T                <-- SPT-bit is set when the switchover occurs


  Incoming interface: INSIDE
  RPF nbr: 192.168.1.100, Registering
  Immediate Outgoing interface list:


NET207, Forward, 00:00:06/00:03:23                                        <-- Both interfaces are shown in




OUTSIDE, Forward, 00:00:06/00:03:23                                       <-- Both interfaces are shown in


    Tunnel0, Forward, 00:00:06/never
```

No final do switchover de SPT, apenas a interface NET207 é mostrada no OIL de FTD:

<#root>

```
firepower#

show mroute 230.10.10.10



Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State
```

```
(192.168.1.100, 230.10.10.10), 00:00:28/00:03:01, flags: SFT
  Incoming interface: INSIDE
  RPF nbr: 192.168.1.100
  Immediate Outgoing interface list:
```

NET207, Forward

```
, 00:00:28/00:03:01
```

<-- The interface NET207 forwards the multicast stream after the SPT switchover

No roteador do último salto (ASA), o bit SPT também é definido:

<#root>

```
asa#
```

show mroute 230.10.10.10

```
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(*, 230.10.10.10), 01:43:09/never, RP 198.51.100.1, flags: SCJ
  Incoming interface: OUTSIDE
  RPF nbr: 192.168.104.61
  Immediate Outgoing interface list:
    INSIDE, Forward, 01:43:09/never
```

(192.168.1.100, 230.10.10.10)

```
, 00:00:03/00:03:27, flags: SJ
```

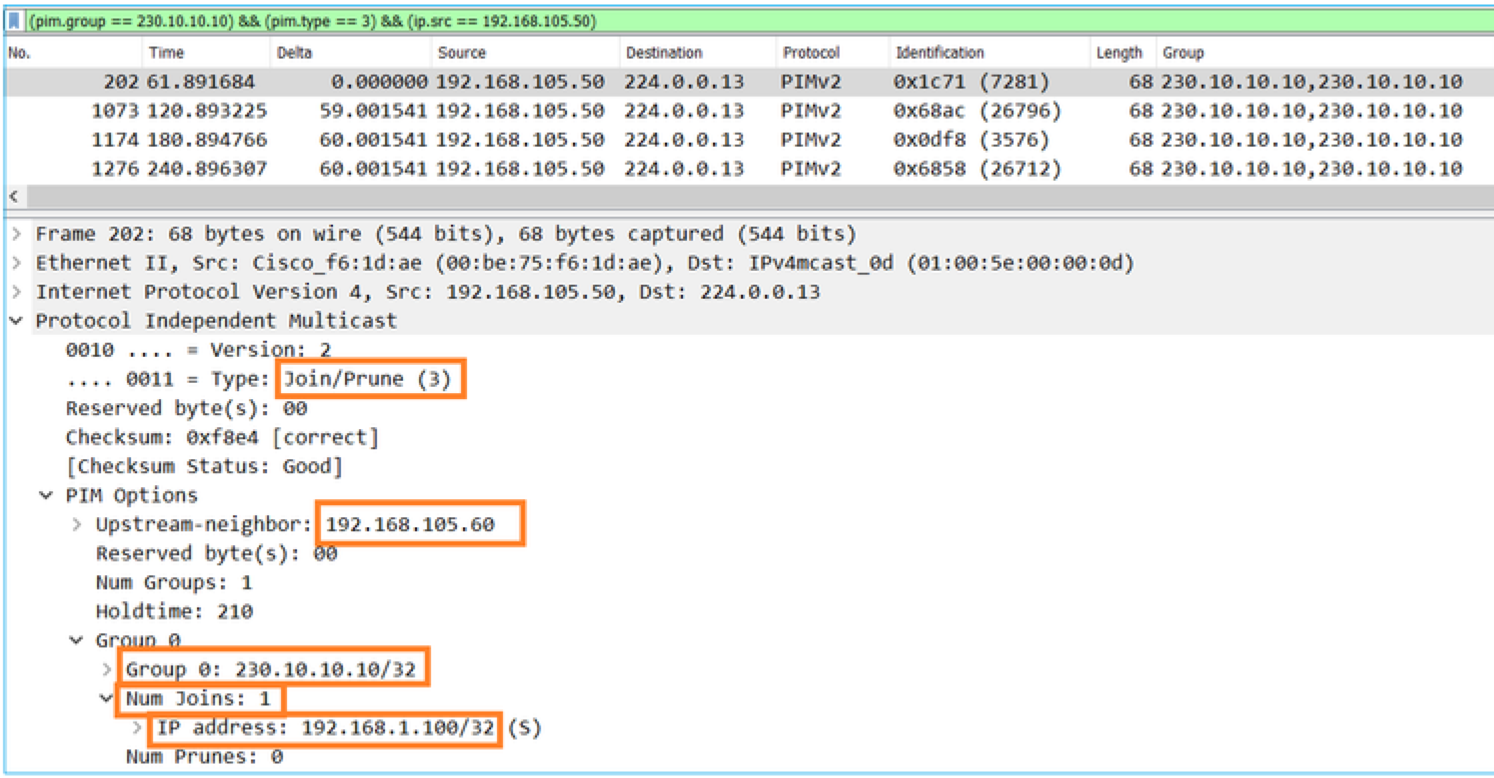
T   <-- SPT switchover for group 230.10.10.10

Incoming interface:

NET207   <-- The multicast packets arrive on interface NET207

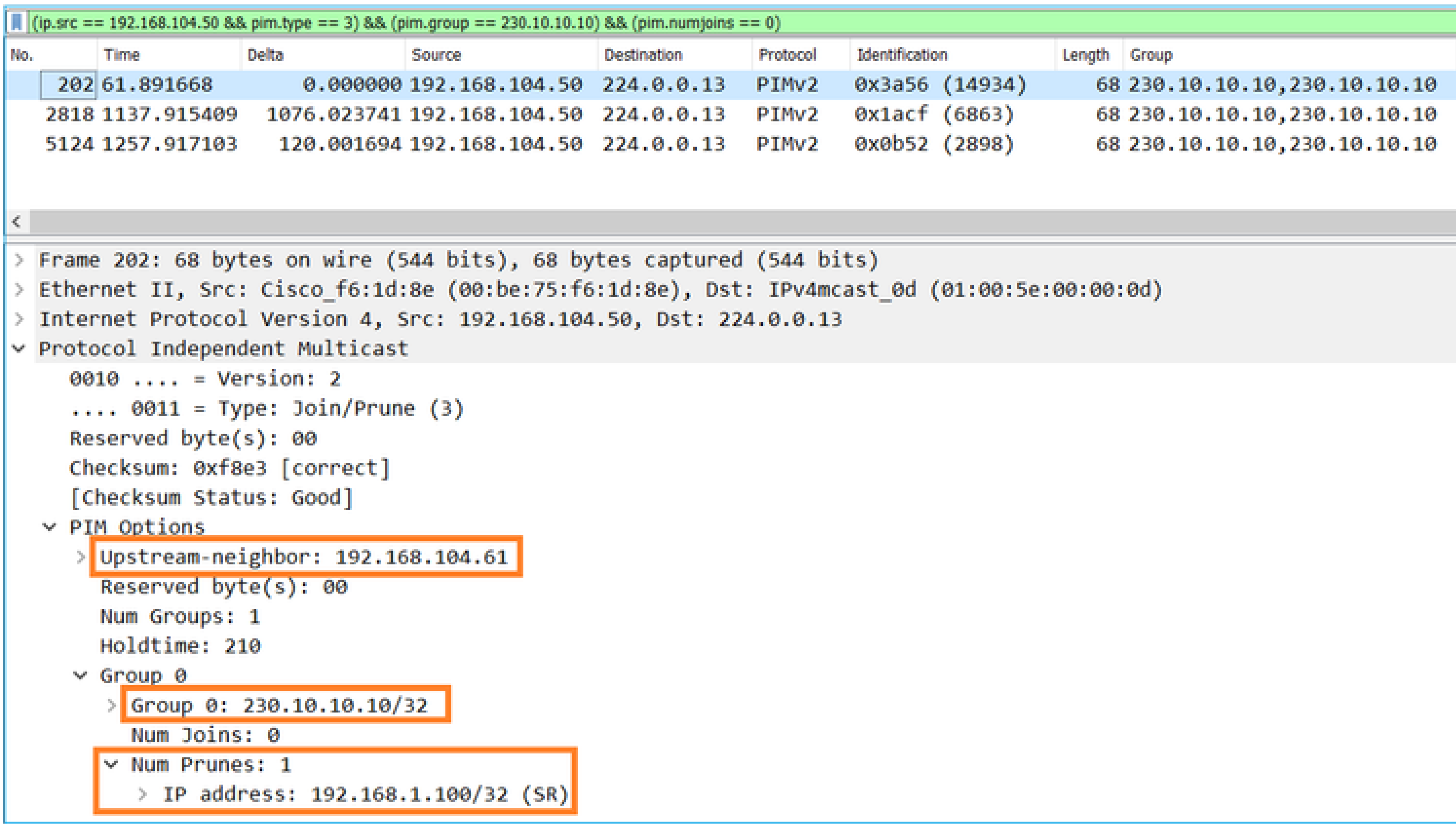
```
  RPF nbr: 192.168.105.60
  Inherited Outgoing interface list:
    INSIDE, Forward, 01:43:09/never
```

O switchover da interface do ASA NET207 (o roteador do primeiro salto que fez o switchover). Uma mensagem PIM Join é enviada para o dispositivo upstream (FTD):



```
(pim.group == 230.10.10.10) && (pim.type == 3) && (ip.src == 192.168.105.50)
No.        Time        Delta      Source          Destination  Protocol  Identification   Length  Group
   202  61.891684   0.000000  192.168.105.50  224.0.0.13   PIMv2     0x1c71 (7281)        68  230.10.10.10,230.10.10.10
  1073 120.893225  59.001541  192.168.105.50  224.0.0.13   PIMv2     0x68ac (26796)       68  230.10.10.10,230.10.10.10
  1174 180.894766  60.001541  192.168.105.50  224.0.0.13   PIMv2     0x0df8 (3576)        68  230.10.10.10,230.10.10.10
  1276 240.896307  60.001541  192.168.105.50  224.0.0.13   PIMv2     0x6858 (26712)       68  230.10.10.10,230.10.10.10

> Frame 202: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
> Ethernet II, Src: Cisco_f6:1d:ae (00:be:75:f6:1d:ae), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
> Internet Protocol Version 4, Src: 192.168.105.50, Dst: 224.0.0.13
v Protocol Independent Multicast
    0010 .... = Version: 2
    .... 0011 = Type: Join/Prune (3)
    Reserved byte(s): 00
    Checksum: 0xf8e4 [correct]
    [Checksum Status: Good]
  v PIM Options
    > Upstream-neighbor: 192.168.105.60
      Reserved byte(s): 00
      Num Groups: 1
      Holdtime: 210
    v Group 0
      > Group 0: 230.10.10.10/32
      v Num Joins: 1
        > IP address: 192.168.1.100/32 (S)
        Num Prunes: 0
```

Na interface EXTERNA, uma mensagem PIM Prune é enviada ao RP para interromper o fluxo multicast:



```
(ip.src == 192.168.104.50 && pim.type == 3) && (pim.group == 230.10.10.10) && (pim.numjoins == 0)
No.        Time          Delta      Source          Destination  Protocol  Identification   Length  Group
   202   61.891668     0.000000  192.168.104.50  224.0.0.13   PIMv2     0x3a56 (14934)       68  230.10.10.10,230.10.10.10
  2818 1137.915409  1076.023741  192.168.104.50  224.0.0.13   PIMv2     0x1acf (6863)        68  230.10.10.10,230.10.10.10
  5124 1257.917103   120.001694  192.168.104.50  224.0.0.13   PIMv2     0x0b52 (2898)        68  230.10.10.10,230.10.10.10

> Frame 202: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
> Ethernet II, Src: Cisco_f6:1d:8e (00:be:75:f6:1d:8e), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
> Internet Protocol Version 4, Src: 192.168.104.50, Dst: 224.0.0.13
v Protocol Independent Multicast
    0010 .... = Version: 2
    .... 0011 = Type: Join/Prune (3)
    Reserved byte(s): 00
    Checksum: 0xf8e3 [correct]
    [Checksum Status: Good]
  v PIM Options
    > Upstream-neighbor: 192.168.104.61
      Reserved byte(s): 00
      Num Groups: 1
      Holdtime: 210
    v Group 0
      > Group 0: 230.10.10.10/32
        Num Joins: 0
      v Num Prunes: 1
        > IP address: 192.168.1.100/32 (SR)
```

Verificação do tráfego PIM:

<#root>

```
firepower#
```

show pim traffic

```
PIM Traffic Counters
Elapsed time since counters cleared: 1w2d

                              Received     Sent
Valid PIM Packets             53934        63983
Hello                         36905        77023

Join-Prune                    6495         494          <-- PIM Join/Prune messages



Register                      0            2052         <-- PIM Register messages



Register Stop                 1501         0            <-- PIM Register Stop messages


Assert                        289          362
Bidir DF Election             0            0

Errors:
Malformed Packets                           0
Bad Checksums                               0
Send Errors                                 0
Packet Sent on Loopback Errors              0
Packets Received on PIM-disabled Interface  0
Packets Received with Unknown PIM Version   0
Packets Received with Incorrect Addressing  0
```

Para verificar o número de pacotes tratados no Slow Path vs Fast Path vs Control Point:

<#root>

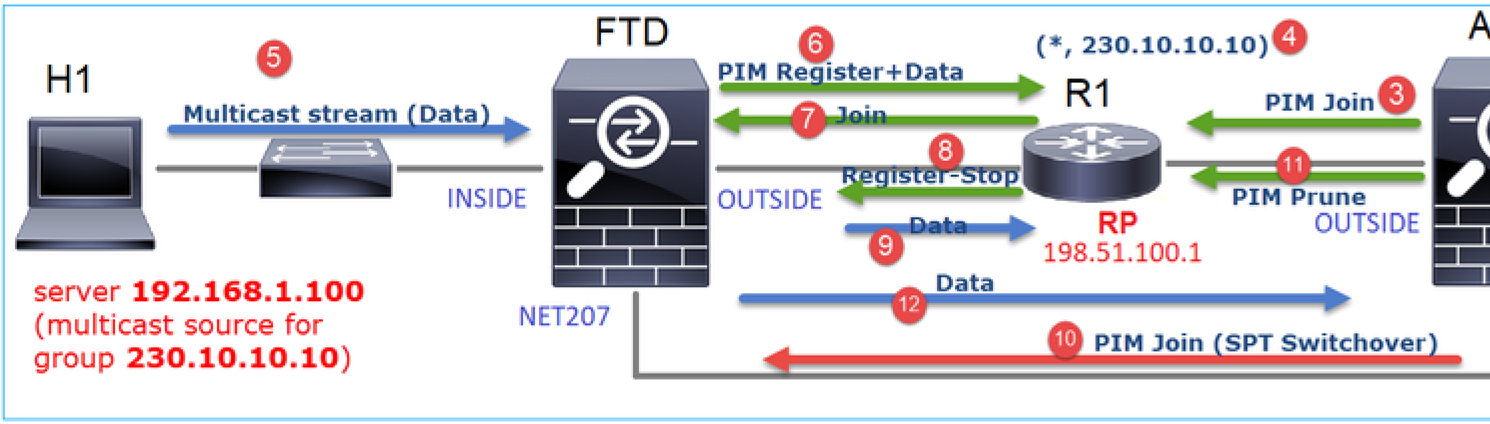
firepower#

show asp cluster counter

```
Global dp-counters:


Context specific dp-counters:
MCAST_FP_FROM_PUNT                      2712    Number of multicast packets punted from CP to FP
MCAST_FP_FORWARDED                      94901   Number of multicast packets forwarded in FP
MCAST_FP_TO_SP                          1105138 Number of multicast packets punted from FP to SP
MCAST_SP_TOTAL                          1107850 Number of total multicast packets processed in SP
MCAST_SP_FROM_PUNT                      2712    Number of multicast packets punted from CP to SP
MCAST_SP_FROM_PUNT_FORWARD              2712    Number of multicast packets coming from CP that are forw
MCAST_SP_PKTS                           537562  Number of multicast packets that require slow-path atter
MCAST_SP_PKTS_TO_FP_FWD                 109     Number of multicast packets that skip over punt rule and
MCAST_SP_PKTS_TO_CP                     166981  Number of multicast packets punted to CP from SP
MCAST_FP_CHK_FAIL_NO_HANDLE             567576  Number of multicast packets failed with no flow mcast_ha
MCAST_FP_CHK_FAIL_NO_ACCEPT_IFC         223847  Number of multicast packets failed with no accept interf
MCAST_FP_CHK_FAIL_NO_SEQ_NO_MATCH       131     Number of multicast packets failed with no matched seque
MCAST_FP_CHK_FAIL_NO_FP_FWD             313584  Number of multicast packets that cannot be fast-path for
```

```
MCAST_FP_UPD_FOR_UNMATCH_IFC          91      Number of times that multicast flow's ifc_out  cannot be
```

Um diagrama que mostra o que acontece passo a passo:



1. O host final (H2) envia um Relatório IGMP para ingressar no fluxo multicast 230.10.10.10.
2. O roteador do último salto (ASA), que é o PIM DR, cria uma entrada (*, 230.10.10.10).
3. O ASA envia uma mensagem PIM Join para o RP do grupo 230.10.10.10.
4. O RP cria a entrada (*, 230.10.10.10).
5. O servidor envia os dados de fluxo multicast.
6. O FTD encapsula os pacotes multicast em mensagens PIM Register e os envia (unicast) ao RP. Neste ponto, o RP vê que tem um receptor ativo, desencapsula os pacotes multicast e os envia ao receptor.
7. O RP envia uma mensagem PIM Join ao FTD para se unir à árvore multicast.
8. O RP envia uma mensagem PIM Register-Stop ao FTD.
9. O FTD envia um fluxo multicast nativo (sem encapsulamento PIM) para o RP.
10. O roteador do último salto (ASA) vê que a origem (192.168.1.100) tem um caminho melhor da interface NET207 e inicia um switchover. Envia uma mensagem PIM Join para o dispositivo upstream (FTD).
11. O roteador do último salto envia uma mensagem PIM Prune ao RP.
12. O FTD encaminha o fluxo multicast para a interface NET207. O ASA é movido da árvore compartilhada (árvore RP) para a árvore de origem (SPT).

Tarefa 2 - Configurar o roteador de bootstrap PIM (BSR)

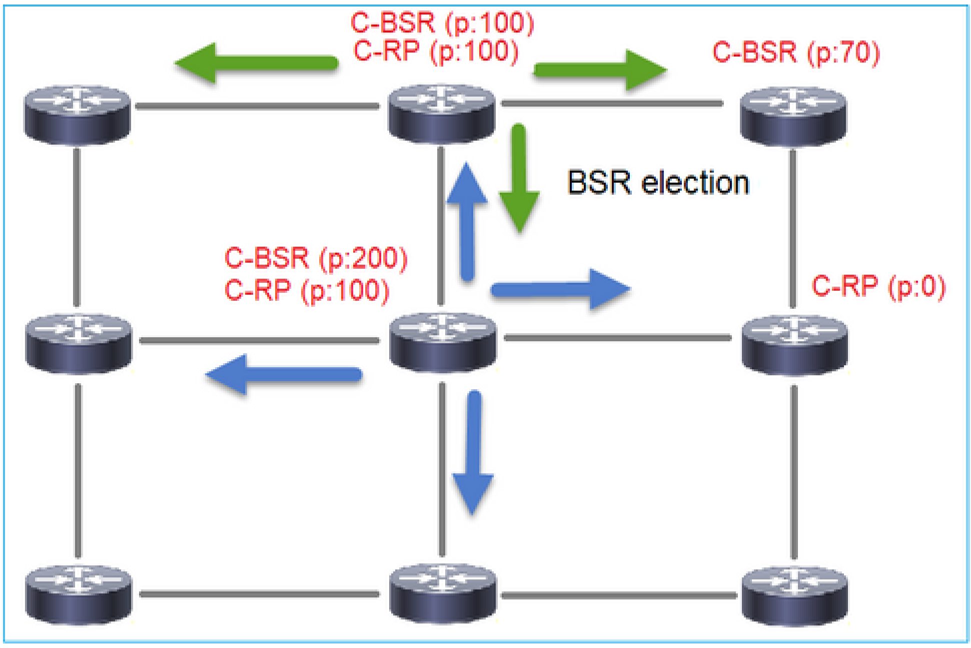
Conceitos básicos de BSR

- O BSR (RFC 5059) é um mecanismo multicast de plano de controle que usa o protocolo PIM e permite que os dispositivos aprendam dinamicamente as informações de RP.
- Definições de BSR:
  - RP candidato (C-RP): um dispositivo que deseja ser um RP.
  - BSR candidato (C-BSR): um dispositivo que deseja ser um BSR e anuncia conjuntos de RP para outros dispositivos.
  - BSR: Um dispositivo que é eleito como um BSR entre muitos C-BSRs. A **maior prioridade de BSR vence** a eleição.
  - RP-set: uma lista de todos os C-RPs e suas prioridades.
  - RP: o dispositivo com a **prioridade RP mais baixa vence** a eleição.
  - Mensagem PIM de BSR (vazia): uma mensagem PIM usada na eleição de BSR.
  - Mensagem PIM BSR (normal): uma mensagem PIM enviada ao IP 224.0.0.13 e contém um conjunto RP e informações BSR.

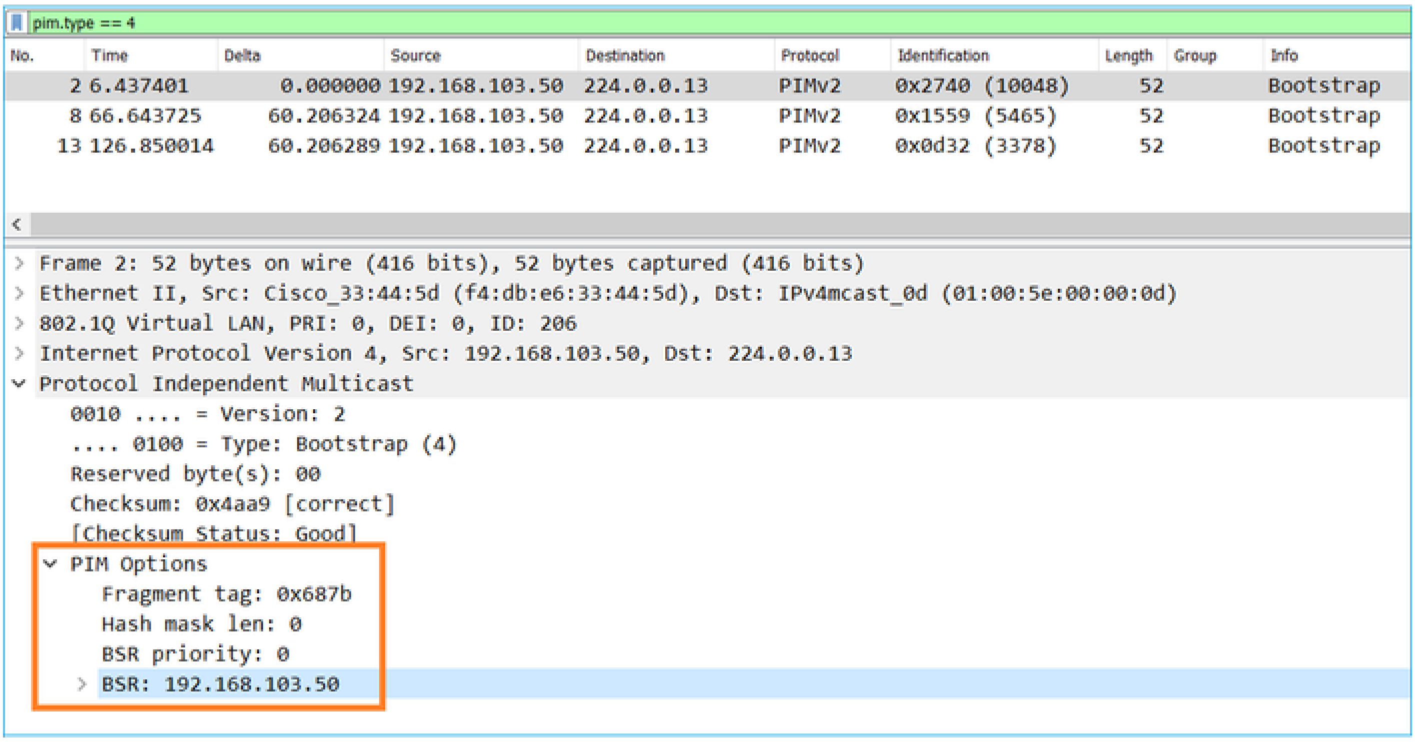
Como o BSR funciona

1. Mecanismo de eleição da RSB.

Cada C-BSR envia mensagens PIM BSR vazias que contêm uma prioridade. O dispositivo com a prioridade mais alta (fallback é o IP mais alto) vence a eleição e se torna o BSR. O restante dos dispositivos não envia mais nenhuma mensagem de BSR vazia.



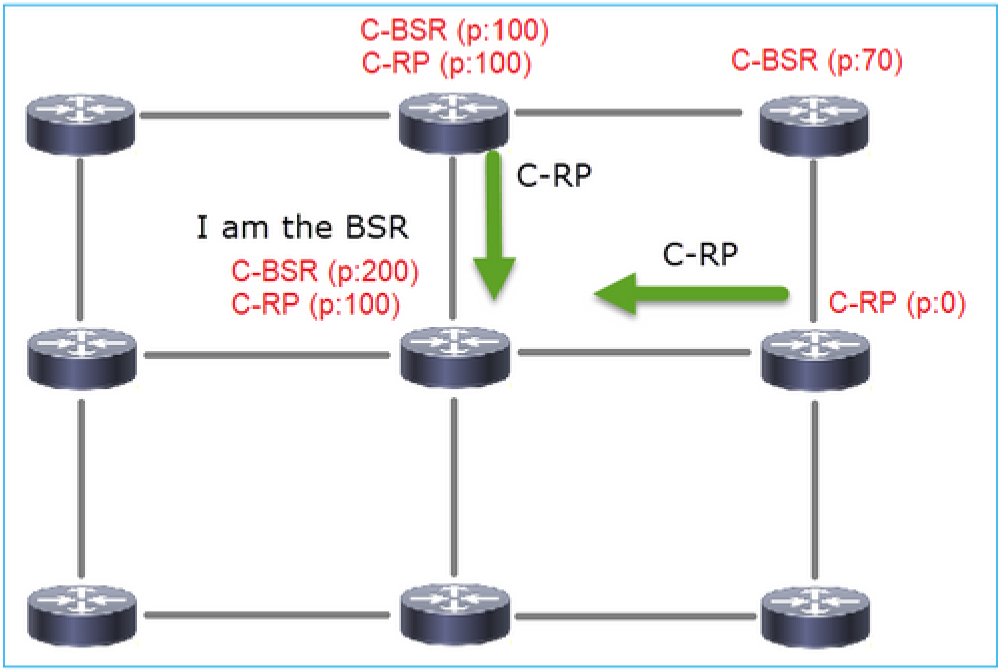
Uma mensagem BSR usada no processo de eleição contém somente informações de prioridade C-BSR:



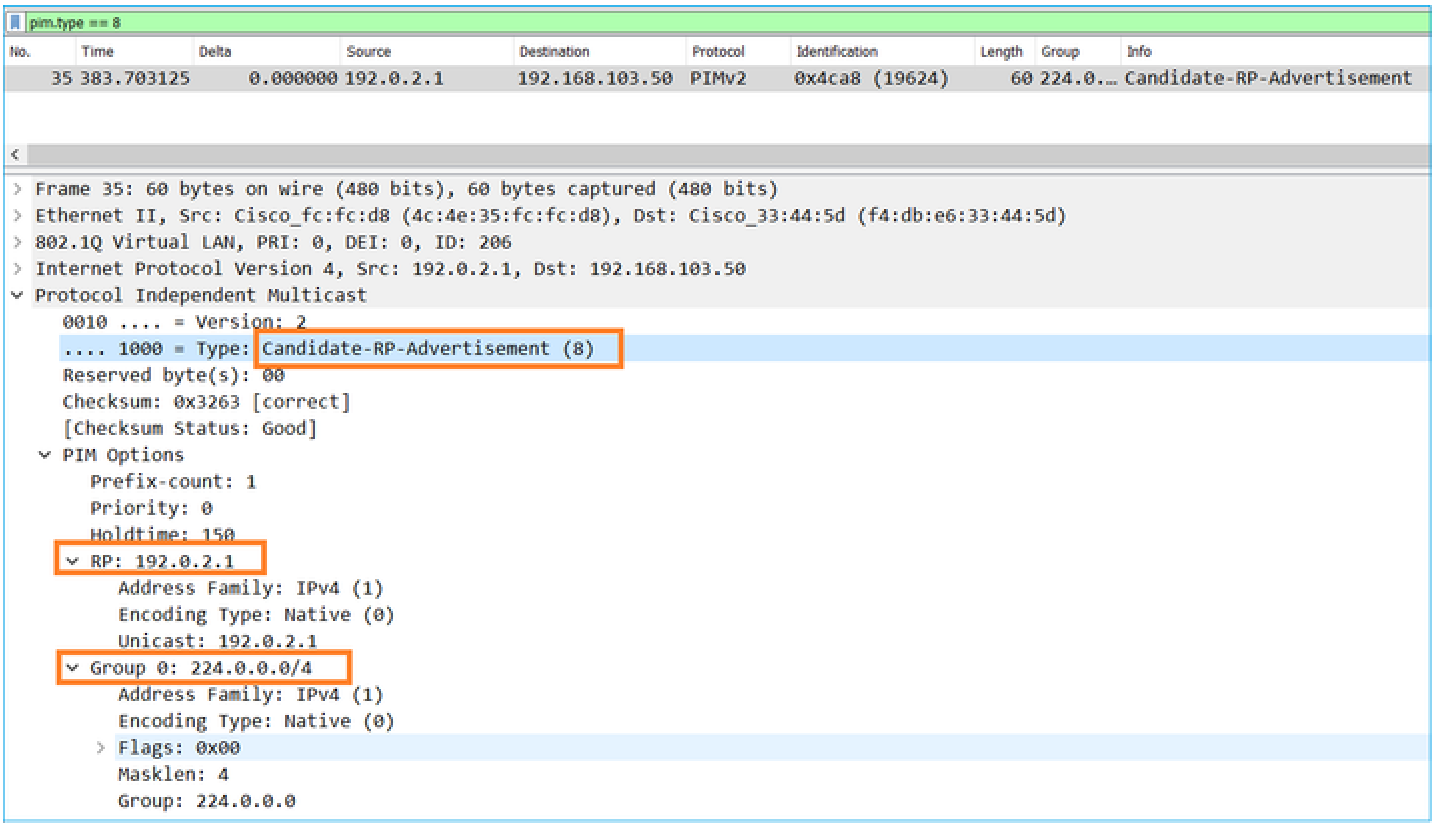
```
pim.type == 4
No.   Time        Delta     Source          Destination  Protocol  Identification   Length  Group  Info
    2 6.437401    0.000000  192.168.103.50  224.0.0.13   PIMv2     0x2740 (10048)       52         Bootstrap
    8 66.643725  60.206324  192.168.103.50  224.0.0.13   PIMv2     0x1559 (5465)        52         Bootstrap
   13 126.850014 60.206289  192.168.103.50  224.0.0.13   PIMv2     0x0d32 (3378)        52         Bootstrap

> Frame 2: 52 bytes on wire (416 bits), 52 bytes captured (416 bits)
> Ethernet II, Src: Cisco_33:44:5d (f4:db:e6:33:44:5d), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 206
> Internet Protocol Version 4, Src: 192.168.103.50, Dst: 224.0.0.13
v Protocol Independent Multicast
    0010 .... = Version: 2
    .... 0100 = Type: Bootstrap (4)
    Reserved byte(s): 00
    Checksum: 0x4aa9 [correct]
    [Checksum Status: Good]
  v PIM Options
      Fragment tag: 0x687b
      Hash mask len: 0
      BSR priority: 0
    > BSR: 192.168.103.50
```

Para exibir mensagens BSR no Wireshark, use este filtro de exibição: pim.type == 4

2. Os C-RPs enviam mensagens **unicast** BSR ao BSR que contêm sua prioridade C-RP:



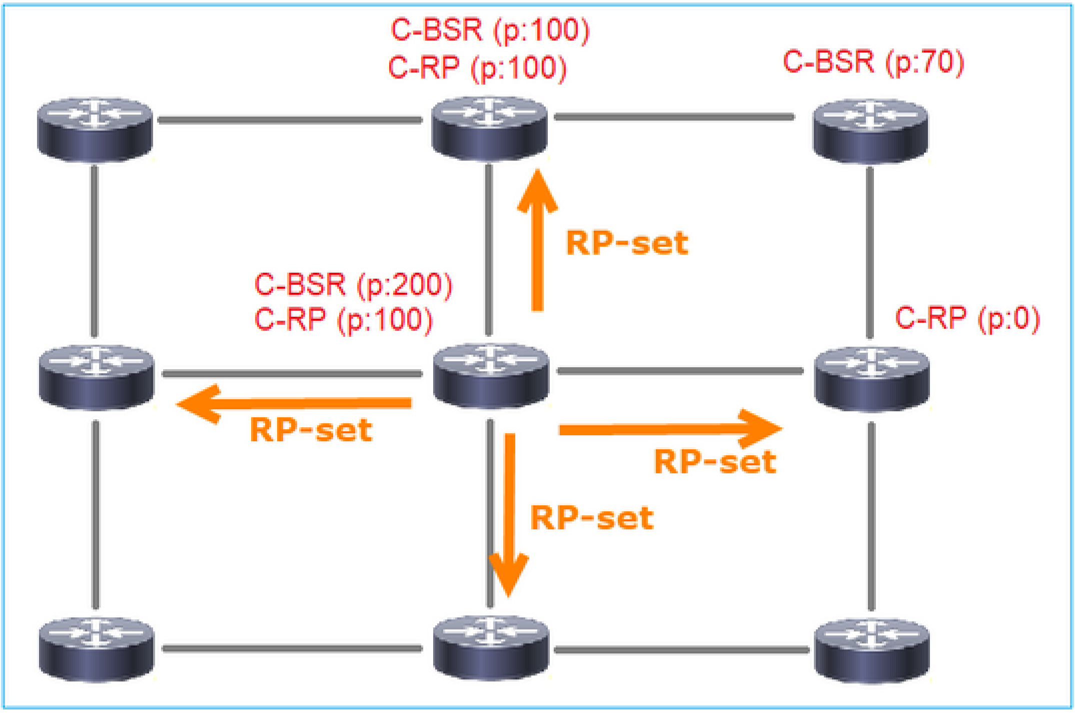
Uma mensagem RP candidata:

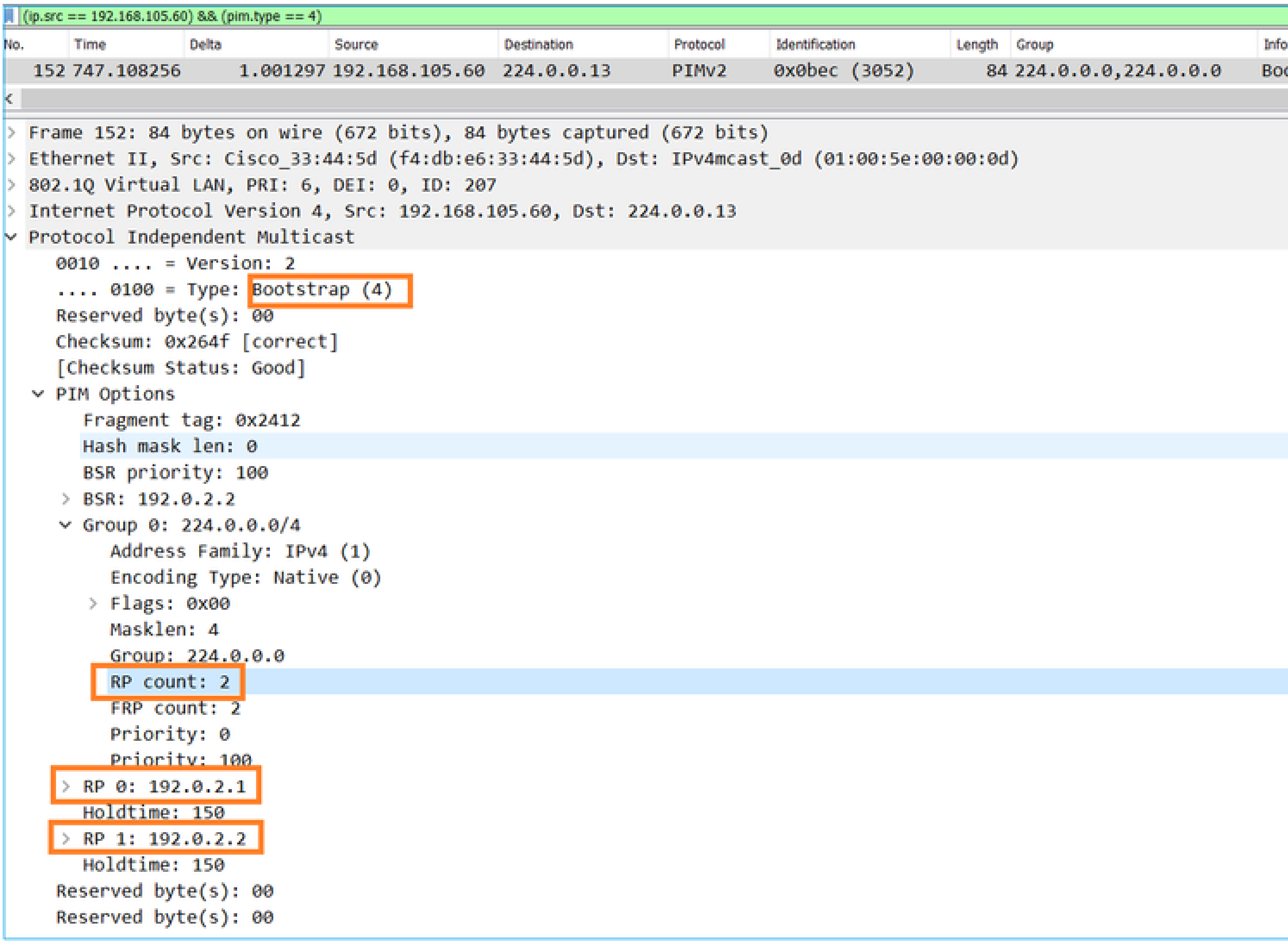


```
pim.type == 8
No.   Time        Delta     Source     Destination     Protocol  Identification   Length Group      Info
   35 383.703125  0.000000  192.0.2.1  192.168.103.50  PIMv2     0x4ca8 (19624)       60 224.0.…  Candidate-RP-Advertisement

> Frame 35: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: Cisco_fc:fc:d8 (4c:4e:35:fc:fc:d8), Dst: Cisco_33:44:5d (f4:db:e6:33:44:5d)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 206
> Internet Protocol Version 4, Src: 192.0.2.1, Dst: 192.168.103.50
v Protocol Independent Multicast
    0010 .... = Version: 2
    .... 1000 = Type: Candidate-RP-Advertisement (8)
    Reserved byte(s): 00
    Checksum: 0x3263 [correct]
    [Checksum Status: Good]
  v PIM Options
      Prefix-count: 1
      Priority: 0
      Holdtime: 150
    v RP: 192.0.2.1
        Address Family: IPv4 (1)
        Encoding Type: Native (0)
        Unicast: 192.0.2.1
    v Group 0: 224.0.0.0/4
        Address Family: IPv4 (1)
        Encoding Type: Native (0)
      > Flags: 0x00
        Masklen: 4
        Group: 224.0.0.0
```

Para exibir mensagens BSR no Wireshark, use este filtro de exibição: pim.type == 8

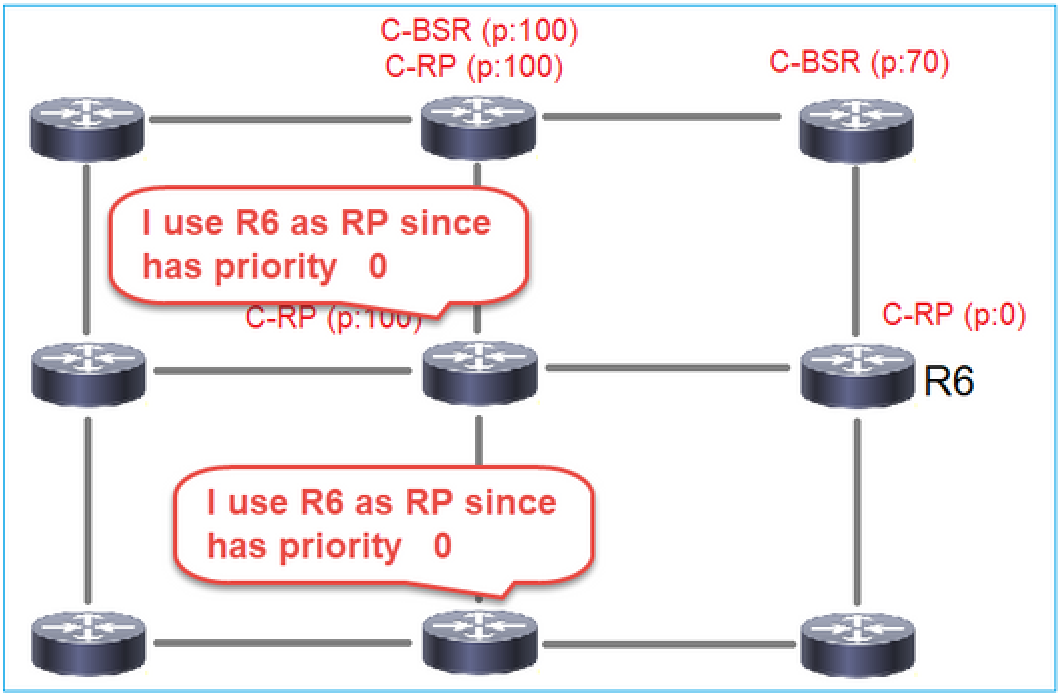
3. O BSR compõe o conjunto RP e o anuncia a todos os vizinhos PIM:





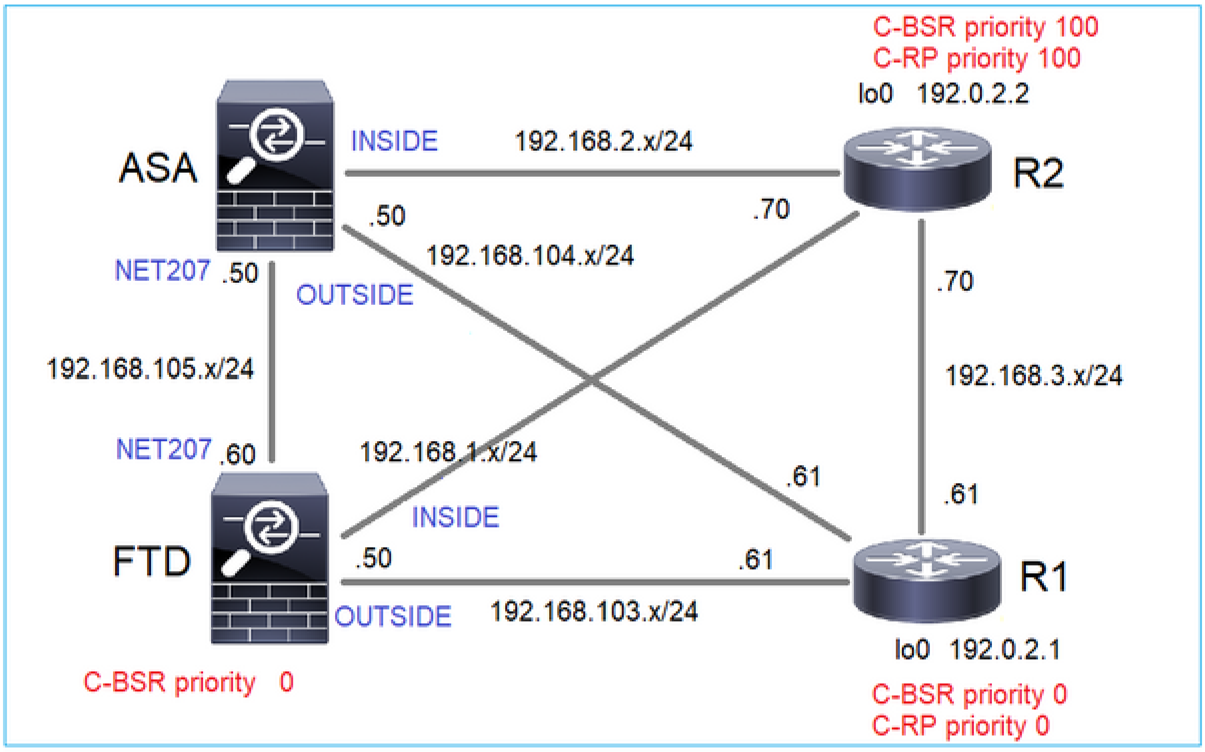
```
(ip.src == 192.168.105.60) && (pim.type == 4)
No.    Time        Delta     Source          Destination  Protocol  Identification   Length Group                  Info
   152 747.108256   1.001297 192.168.105.60  224.0.0.13   PIMv2     0x0bec (3052)        84 224.0.0.0,224.0.0.0    Boo

> Frame 152: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
> Ethernet II, Src: Cisco_33:44:5d (f4:db:e6:33:44:5d), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
> 802.1Q Virtual LAN, PRI: 6, DEI: 0, ID: 207
> Internet Protocol Version 4, Src: 192.168.105.60, Dst: 224.0.0.13
v Protocol Independent Multicast
    0010 .... = Version: 2
    .... 0100 = Type: Bootstrap (4)
    Reserved byte(s): 00
    Checksum: 0x264f [correct]
    [Checksum Status: Good]
  v PIM Options
      Fragment tag: 0x2412
      Hash mask len: 0
      BSR priority: 100
    > BSR: 192.0.2.2
    v Group 0: 224.0.0.0/4
        Address Family: IPv4 (1)
        Encoding Type: Native (0)
      > Flags: 0x00
        Masklen: 4
        Group: 224.0.0.0
        RP count: 2
        FRP count: 2
        Priority: 0
        Priority: 100
    > RP 0: 192.0.2.1
      Holdtime: 150
    > RP 1: 192.0.2.2
      Holdtime: 150
    Reserved byte(s): 00
    Reserved byte(s): 00
```

4. Os roteadores/firewalls obtêm o conjunto RP e elegem o RP com base na prioridade mais baixa:


C-BSR (p:100)
C-RP (p:100)
C-BSR (p:70)
I use R6 as RP since has priority 0
C-RP (p:100)
C-RP (p:0)
R6
I use R6 as RP since has priority 0

Requisito da tarefa

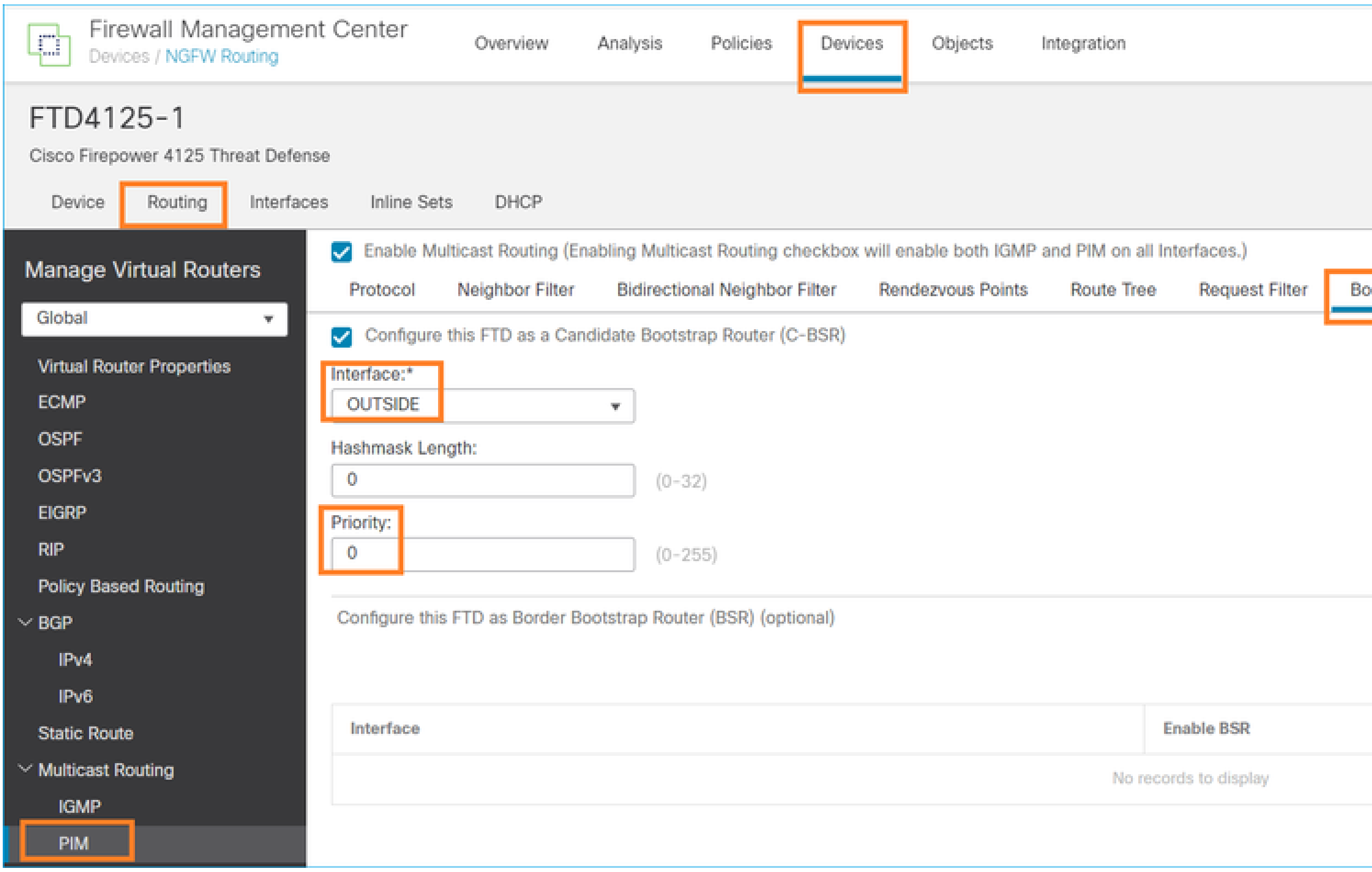
Configure os C-BSRs e C-RPs de acordo com esta topologia:



para esta tarefa, o FTD deve anunciar-se como C-BSR na interface EXTERNA com prioridade 0 de BSR.

Solução

Configuração do FMC para o FTD:



☑ Enable Multicast Routing (Enabling Multicast Routing checkbox will enable both IGMP and PIM on all Interfaces.)

☑ Configure this FTD as a Candidate Bootstrap Router (C-BSR)

Interface:* OUTSIDE

Hashmask Length: 0 (0-32)

Priority: 0 (0-255)

Configure this FTD as Border Bootstrap Router (BSR) (optional)

Interface	Enable BSR
No records to display	

A configuração implantada:

```
multicast-routing
!
pim bsr-candidate OUTSIDE 0 0
```

Configuração nos outros dispositivos:

R1

```
ip multicast-routing
ip pim bsr-candidate Loopback0 0
ip pim rp-candidate Loopback0
!
interface Loopback0
 ip address 192.0.2.1 255.255.255.255
 ip pim sparse-mode
!
! PIM is also enabled on the transit interfaces (e.g. G0/0.203, G0/0.207, G0/0.205)
```

O mesmo em R2, mas com prioridades C-BSR e C-RP diferentes

```
ip pim bsr-candidate Loopback0 0 100
ip pim rp-candidate Loopback0 priority 100
```

No ASA, há apenas multicast globalmente habilitado. Isso ativa o PIM em todas as interfaces:

```
multicast-routing
```

Verificação

R2 é o BSR eleito devido à prioridade mais alta:

<#root>

```
firepower#

show pim bsr-router


PIMv2 BSR information

BSR Election Information


BSR Address: 192.0.2.2             <-- This is the IP of the BSR (R1 lo0)

     Uptime: 00:03:35, BSR Priority: 100

,

Hash mask length: 0
     RPF: 192.168.1.70,INSIDE

<-- The interface to the BSR

     BS Timer: 00:01:34
  This system is candidate BSR
      Candidate BSR address: 192.168.103.50, priority: 0, hash mask length: 0
```

R1 é eleito como RP devido à prioridade mais baixa:

<#root>

```
firepower#

show pim group-map



Group Range         Proto    Client    Groups RP address    Info

224.0.1.39/32*      DM       static    0      0.0.0.0
224.0.1.40/32*      DM       static    0      0.0.0.0
224.0.0.0/24*       L-Local  static    1      0.0.0.0
232.0.0.0/8*        SSM      config    0      0.0.0.0
```

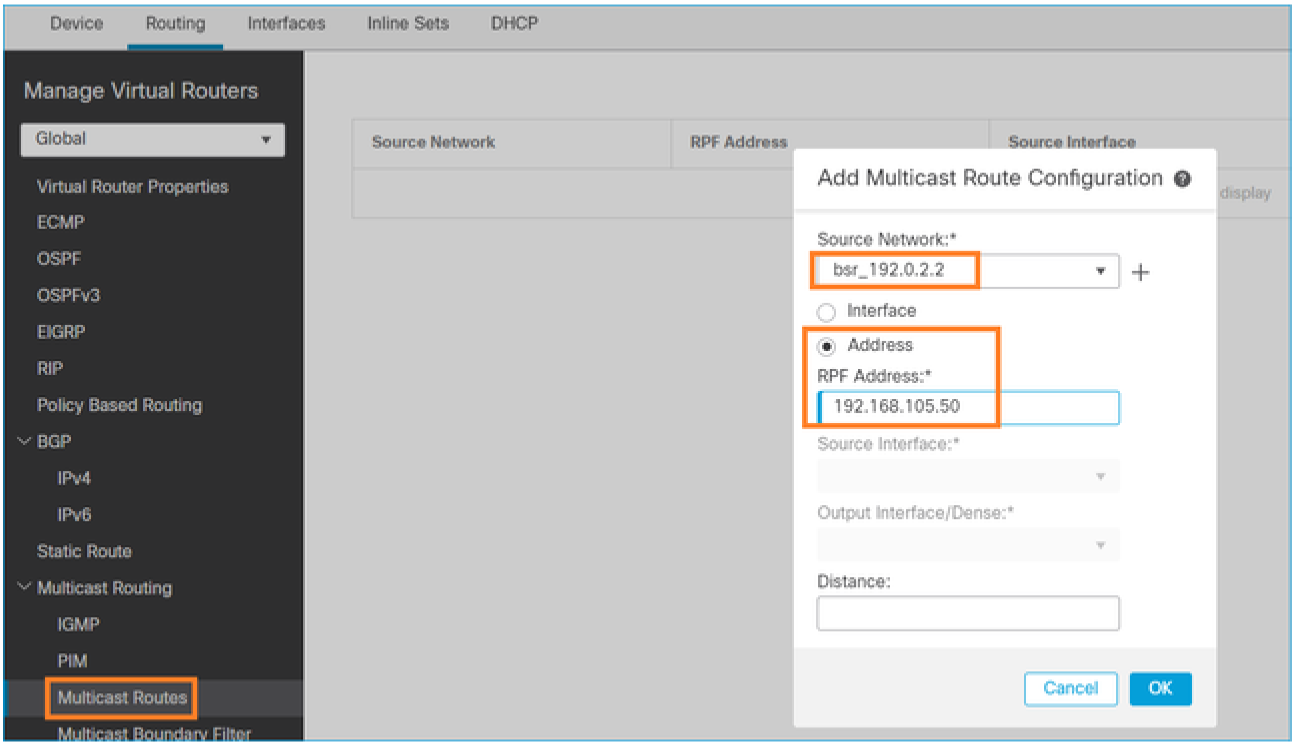
```
224.0.0.0/4

*

       SM

BSR

 0

192.0.2.1

     RPF: OUTSIDE,192.168.103.61

<-- The elected BSR


224.0.0.0/4        SM       BSR       0      192.0.2.2     RPF: INSIDE,192.168.1.70
224.0.0.0/4        SM       static    0      0.0.0.0       RPF: ,0.0.0.0
```

As mensagens BSR **estão sujeitas à verificação de RPF**. Você pode habilitar **debug pim bsr** para verificar isso:

<#root>

```
IPv4 BSR: Received BSR message from 192.168.105.50 for 192.0.2.2, BSR priority 100 hash mask length 0
IPv4 BSR:

BSR message

 from 192.168.105.50/

NET207

 for 192.0.2.2

RPF failed, dropped



<-- The RPF check for the received BSR message failed
```

Se desejar alterar a interface RPF, você pode configurar uma mroute estática. Neste exemplo, o firewall aceita mensagens BSR do IP 192.168.105.50:



Source Network:* bsr_192.0.2.2

○ Interface

● Address

RPF Address:* 192.168.105.50

Source Interface:*

Output Interface/Dense:*

Distance:

<#root>

```
firepower#

show run mroute

mroute 192.0.2.2 255.255.255.255 192.168.105.50
```

<#root>

```
firepower#

show pim bsr-router



PIMv2 BSR information

BSR Election Information
     BSR Address: 192.0.2.2
     Uptime: 01:21:38, BSR Priority: 100, Hash mask length: 0


RPF: 192.168.105.50,NET207

<-- The RPF check points to the static mroute
     BS Timer: 00:01:37
This system is candidate BSR
      Candidate BSR address: 192.168.103.50, priority: 0, hash mask length: 0
```

Agora as mensagens de BSR na interface NET207 são aceitas, mas no INTERIOR são descartadas:

<#root>

```
IPv4 BSR: Received BSR message from 192.168.1.70 for 192.0.2.2, BSR priority 100 hash mask length 0
```

```
IPv4 BSR: BSR message from 192.168.1.70/INSIDE for 192.0.2.2 RPF failed, dropped
```

```
...
```

```
IPv4 BSR: Received BSR message from 192.168.105.50 for 192.0.2.2, BSR priority 100 hash mask length 0
```

```
<-- RPF check is OK
```

Ative a captura com rastreamento no firewall e verifique como as mensagens BSR são processadas:

<#root>

```
firepower#
```

```
show capture
```

```
capture CAPI type raw-data trace interface INSIDE [Capturing - 276 bytes]
  match pim any any
capture CAPO type raw-data trace interface OUTSIDE [Capturing - 176 bytes]
  match pim any any
```

As conexões PIM são encerradas no firewall, portanto, para que o rastreamento mostre informações úteis, é necessário limpar as conexões à caixa:

<#root>

```
firepower#
```

```
show conn all | i PIM
```

```
firepower# show conn all | include PIM
PIM OUTSIDE 192.168.103.61 NP Identity Ifc 224.0.0.13, idle 0:00:23, bytes 116802, flags
PIM NET207 192.168.104.50 NP Identity Ifc 224.0.0.13, idle 0:00:17, bytes 307296, flags
PIM NET207 192.168.104.61 NP Identity Ifc 224.0.0.13, idle 0:00:01, bytes 184544, flags
PIM NET207 192.168.105.50 NP Identity Ifc 224.0.0.13, idle 0:00:18, bytes 120248, flags
PIM INSIDE 192.168.1.70 NP Identity Ifc 224.0.0.13, idle 0:00:27, bytes 15334, flags
PIM OUTSIDE 224.0.0.13 NP Identity Ifc 192.168.103.50, idle 0:00:21, bytes 460834, flags
PIM INSIDE 224.0.0.13 NP Identity Ifc 192.168.1.50, idle 0:00:00, bytes 441106, flags
PIM NET207 224.0.0.13 NP Identity Ifc 192.168.105.60, idle 0:00:09, bytes 458462, flags
```

```
firepower#
```

```
clear conn all addr 224.0.0.13
```

```
8 connection(s) deleted.
firepower#
```

```
clear cap /all
```

<#root>

```
firepower#

show capture CAPI packet-number 2 trace


6 packets captured

2: 11:31:44.390421 802.1Q vlan#205 P6

192.168.1.70 > 224.0.0.13

 ip-proto-103, length 38

<-- Ingress PIM packet


Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 4880 ns
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 4880 ns
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: ROUTE-LOOKUP
Subtype: No ECMP load balancing
Result: ALLOW
Elapsed time: 9760 ns
Config:
Additional Information:
Destination is locally connected. No ECMP load balancing.
Found next-hop 192.168.1.70 using egress ifc INSIDE(vrfid:0)

Phase: 4
Type: CLUSTER-DROP-ON-SLAVE
Subtype: cluster-drop-on-slave
Result: ALLOW
Elapsed time: 4392 ns
Config:
Additional Information:

Phase: 5
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 4392 ns
Config:
Implicit Rule
Additional Information:

Phase: 6
Type: NAT
```

```
Subtype: per-session
Result: ALLOW
Elapsed time: 4392 ns
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Elapsed time: 4392 ns
Config:
Additional Information:

Phase: 8
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Elapsed time: 18056 ns
Config:
Additional Information:

Phase: 9

Type: MULTICAST             <-- The multicast process


Subtype: pim


Result: ALLOW
Elapsed time: 976 ns
Config:
Additional Information:

Phase: 10
Type: MULTICAST
Subtype:
Result: ALLOW
Elapsed time: 488 ns
Config:
Additional Information:

Phase: 11
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 20008 ns
Config:
Additional Information:
New flow created with id 25630, packet dispatched to next module

Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
output-interface: INSIDE(vrfid:0)
output-status: up
output-line-status: up

Action: allow
```

```
Time Taken: 76616 ns
```

Se o pacote PIM for descartado devido a uma falha de RPF, o rastreamento mostrará:

<#root>

```
firepower#

show capture NET207 packet-number 4 trace


85 packets captured

4: 11:31:42.385951 802.1Q vlan#207 P6

192.168.104.61 > 224.0.0.13 ip-proto-103

, length 38

<-- Ingress PIM packet


Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 5368 ns
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 5368 ns
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: INPUT-ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Elapsed time: 11224 ns
Config:
Additional Information:
Found next-hop 192.168.103.61 using egress ifc OUTSIDE(vrfid:0)

Phase: 4
Type: INPUT-ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Elapsed time: 3416 ns
Config:
Additional Information:
Found next-hop 192.168.103.61 using egress ifc OUTSIDE(vrfid:0)

Result:
input-interface: NET207(vrfid:0)
```

```
input-status: up
input-line-status: up
output-interface: OUTSIDE(vrfid:0)
output-status: up
output-line-status: up
Action: drop
Time Taken: 25376 ns

Drop-reason: (rpf-violated) Reverse-path verify failed, Drop-location: frame 0x0000558f240d6e15 flow (NA


<-- the packet is dropped due to RPF check failure
```

A tabela ASP descarta e captura pacotes com falha de RPF:

<#root>

```
firepower#

show asp drop


Frame drop:


 Reverse-path verify failed (rpf-violated)                                 122

 <-- Multicast RPF drops
  Flow is denied by configured rule (acl-drop)                              256
  FP L2 rule drop (l2_acl)                                                  768
```

Para capturar pacotes que são descartados devido à falha de RPF:

<#root>

```
firepower#

capture ASP type asp-drop rpf-violated
```

<#root>

```
firepower#

show capture ASP | include 224.0.0.13


2: 11:36:20.445960 802.1Q vlan#207 P6 192.168.104.50 > 224.0.0.13 ip-proto-103, length 38
10: 11:36:38.787846 802.1Q vlan#207 P6 192.168.104.61 > 224.0.0.13 ip-proto-103, length 38
15: 11:36:48.299743 802.1Q vlan#207 P6 192.168.104.50 > 224.0.0.13 ip-proto-103, length 46
16: 11:36:48.300063 802.1Q vlan#207 P6 192.168.104.61 > 224.0.0.13 ip-proto-103, length 46
```

Metodologia de Troubleshooting

A metodologia de identificação e solução de problemas do firewall depende principalmente da função do firewall na topologia de multicast. Esta é a lista de etapas recomendadas para solução de problemas:

1. Esclareça os detalhes da descrição e dos sintomas do problema. Tente reduzir o escopo para os problemas do **plano de controle (IGMP/PIM)** ou do **plano de dados (fluxo multicast)**.
2. O pré-requisito obrigatório para solucionar problemas de multicast no firewall é esclarecer a topologia de multicast. No mínimo, você precisa identificar:
   - função do firewall na topologia multicast - FHR, LHR, RP ou outra função intermediária.
   - interfaces de entrada e saída multicast esperadas no firewall.
   - RP.
   - endereços IP de origem do remetente.
   - multicast agrupa endereços IP e portas de destino.
   - receptores do fluxo multicast.

3. Identifique o tipo de roteamento multicast **- Stub ou multicast PIM roteamento:**

- **Stub Multicast Routing -** fornece registro de host dinâmico e facilita o roteamento multicast. Quando configurado para o roteamento multicast stub, o ASA atua como um agente proxy IGMP. Em vez de participar totalmente do roteamento multicast, o ASA encaminha mensagens IGMP para um roteador multicast upstream, que configura a entrega dos dados multicast. Para identificar o roteamento do modo stub, use o comando **show igmp interface** e verifique a configuração de encaminhamento IGMP:

<#root>

```
firepower#

show igmp interface


inside is up, line protocol is up
  Internet address is 192.168.2.2/24
  IGMP is disabled on interface
outside is up, line protocol is up
  Internet address is 192.168.3.1/24
  IGMP is enabled on interface
  Current IGMP version is 2
  IGMP query interval is 125 seconds
  IGMP querier timeout is 255 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1 seconds
  Inbound IGMP access group is:
  IGMP limit is 500, currently active joins: 0
  Cumulative IGMP activity: 0 joins, 0 leaves


IGMP forwarding on interface inside


  IGMP querying router is 192.168.3.1 (this system)
```

O PIM é ativado nas interfaces; no entanto, a vizinhança não é estabelecida:

<#root>

```
firepower#
```

```
show pim interface


Address          Interface          PIM  Nbr   Hello  DR         DR
                                         Count Intvl  Prior

192.168.2.2      inside             on   0     30     1          this system
192.168.3.1      outside            on   0     30     1          this system

firepower# show pim neighbor

No neighbors found.
```

O encaminhamento PIM-SM/Bidir e IGMP **não** são suportados simultaneamente.

Você não pode configurar opções como o endereço RP:

```
<#root>

%Error: PIM-SM/Bidir and IGMP forwarding are not supported concurrently
```

- **Roteamento multicast PIM - O roteamento multicast PIM é a implantação mais comum.** O firewall suporta PIM-SM e PIM bidirecional. PIM-SM é um protocolo de roteamento multicast que usa a base de informações de roteamento unicast subjacente ou uma base de informações de roteamento separada com capacidade de multicast. Ele cria uma árvore compartilhada unidirecional com raiz em um único ponto de encontro (RP) por grupo multicast e, opcionalmente, cria árvores de caminho mais curto por origem multicast. Neste modo de implantação, ao contrário do modo stub, os usuários geralmente configuram a configuração do endereço RP e o firewall estabelece adjacências PIM com os correspondentes:

```
<#root>

firepower#

show run pim


pim rp-address 10.10.10.1

firepower#

show pim group-map


Group Range        Proto   Client   Groups RP address      Info
224.0.1.39/32*     DM      static   0      0.0.0.0
224.0.1.40/32*     DM      static   0      0.0.0.0
224.0.0.0/24*      L-Local static   1      0.0.0.0
232.0.0.0/8*       SSM     config   0      0.0.0.0

224.0.0.0/4*       SM      config   1      10.10.10.1     RPF: inside,192.168.2.1 <--- RP address is 10


224.0.0.0/4        SM      static   0      0.0.0.0         RPF: ,0.0.0.0

firepower#
```

```
show pim neighbor


Neighbor Address  Interface          Uptime    Expires DR pri Bidir
192.168.2.1       inside             00:02:52  00:01:19 1
192.168.3.100     outside            00:03:03  00:01:39 1 (DR)
```

4. Verifique se o endereço IP do RP está configurado e acessível:

<#root>

```
firepower#

show run pim


pim rp-address 10.10.10.1

firepower#

show pim group-map



Group Range         Proto   Client   Groups RP address      Info
224.0.1.39/32*      DM      static   0      0.0.0.0
224.0.1.40/32*      DM      static   0      0.0.0.0
224.0.0.0/24*       L-Local static   1      0.0.0.0
232.0.0.0/8*        SSM     config   0      0.0.0.0

224.0.0.0/4*        SM      config   1      10.10.10.1     RPF: inside,192.168.2.1 <--- RP is 10.10.10.1


224.0.0.0/4         SM      static   0      0.0.0.0         RPF: ,0.0.0.0
```

<#root>

```
firepower#

show pim group-map



Group Range         Proto   Client   Groups RP address      Info
224.0.1.39/32*      DM      static   0      0.0.0.0
224.0.1.40/32*      DM      static   0      0.0.0.0
224.0.0.0/24*       L-Local static   1      0.0.0.0
232.0.0.0/8*        SSM     config   0      0.0.0.0

224.0.0.0/4*        SM      config   1      192.168.2.2     RPF: Tunnel0,192.168.2.2 (us) <--- â€œusâ€�


224.0.0.0/4         SM      static   0      0.0.0.0         RPF: ,0.0.0.0
```

> **Aviso**: o firewall não pode ser simultaneamente um **RP** e um **FHR**.

---

5. Verifique saídas adicionais dependendo da função do firewall na topologia multicast e dos sintomas do problema.

FHR

- Verifique o status da interface **Tunnel0**. Esta interface é usada para encapsular o tráfego multicast bruto dentro do payload PIM e enviar o pacote unicast ao RP para com o conjunto de bits PIM-register:

<#root>

```
firepower#

show interface detail  | b Interface Tunnel0



Interface Tunnel0 "", is up, line protocol is up


  Hardware is   Available but not configured via nameif
        MAC address 0000.0000.0000, MTU not set
        IP address unassigned
  Control Point Interface States:
        Interface number is un-assigned
        Interface config status is active
        Interface state is active

firepower#

show pim tunnel


Interface          RP Address        Source Address
Tunnel0            10.10.10.1       192.168.2.2
```

- Verificar mroutes:

<#root>

```
firepower#

show mroute


Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(192.168.2.1, 230.1.1.1), 00:00:07/00:03:22, flags: SFT
  Incoming interface: inside

  RPF nbr: 192.168.2.1, Registering <--- Registering state
  Immediate Outgoing interface list:
    outside, Forward, 00:00:07/00:03:26

    Tunnel0, Forward, 00:00:07/never <--- Tunnel0 is in OIL, that indicates raw traffic is encapsulated.
```

Quando o firewall recebe o pacote PIM com bit de Register-Stop, o Tunnel0 é removido do OIL. Em seguida, o firewall interrompe o encapsulamento e envia o tráfego multicast bruto através da interface de saída:

<#root>

```
firepower#

show mroute


Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(192.168.2.1, 230.1.1.1), 00:07:26/00:02:59, flags: SFT
  Incoming interface: inside
  RPF nbr: 192.168.2.1
  Immediate Outgoing interface list:


outside, Forward, 00:07:26/00:02:59
```

- Verificar contadores de registro PIM:

<#root>

```
firepower#

show pim traffic



PIM Traffic Counters
Elapsed time since counters cleared: 00:13:13

                              Received     Sent
Valid PIM Packets             42           58
Hello                         27           53
Join-Prune                    9            0

Register                      0            8  <--- Sent to the RP



Register Stop                 6            0  <--- Received from the RP


Assert                        0            0
```

```
Bidir DF Election             0           0

Errors:
Malformed Packets                          0
Bad Checksums                              0
Send Errors                                0
Packet Sent on Loopback Errors             0
Packets Received on PIM-disabled Interface  0
Packets Received with Unknown PIM Version   0
Packets Received with Incorrect Addressing  0
```

- Verifique as capturas de pacotes PIM unicast entre o firewall e o RP:

<#root>

```
firepower#

capture capo interface outside match pim any host 10.10.10.1 <--- RP IP


firepower#

show capture  capi



4 packets captured


  1: 09:53:28.097559       192.168.3.1 > 10.10.10.1  ip-proto-103, length 50     <--- Unicast to RP


  2: 09:53:32.089167       192.168.3.1 > 10.10.10.1  ip-proto-103, length 50
  3: 09:53:37.092890       192.168.3.1 > 10.10.10.1  ip-proto-103, length 50

  4: 09:53:37.095850       10.10.10.1 > 192.168.3.1  ip-proto-103, length 18     <--- Unicast from RP
```

- Colete saídas adicionais (x.x.x.x é o grupo multicast, y.y.y.y é o IP RP). Recomenda-se coletar as saídas **algumas vezes**:

<#root>

```
show conn all protocol udp address x.x.x.x



show local-host x.x.x.x



show asp event dp-cp



show asp drop



show asp cluster counter
show asp table routing y.y.y.y
```

```
show route y.y.y.y
```

```
show mroute
```

```
show pim interface
```

```
show pim neighbor
show pim traffic
```

```
show igmp interface
```

```
show mfib count
```

- Colete pacotes de interface multicast brutos e capturas de queda ASP.

<#root>

```
capture capi interface




      buffer 32000000 match udp host X host Z <--- (ingress capture for multicast UDP traffic from host




capture capo interface




      buffer 32000000 match udp host X host Z <--- (egress capture for multicast UDP traffic from host X
capture asp type asp-drop buffer 32000000 match udp host X host Z <--- (ASP drop capture for multicast U
```

- Mensagens de syslog - IDs comuns são 302015, 302016 e 710005.

RP

- Verifique o status da interface Tunnel0. Esta interface é usada para encapsular o tráfego multicast bruto dentro do payload PIM e enviar o pacote unicast para o FHR para com o conjunto de bits de parada PIM:

<#root>

```
firepower#

show interface detail  | b Interface Tunnel0



Interface Tunnel0 "", is up, line protocol is up


  Hardware is   Available but not configured via nameif
        MAC address 0000.0000.0000, MTU not set
        IP address unassigned
  Control Point Interface States:
        Interface number is un-assigned
        Interface config status is active
        Interface state is active

firepower#

 show pim tunnel


Interface          RP Address        Source Address


Tunnel0            192.168.2.2       192.168.2.2


Tunnel0            192.168.2.2        -
```

- Verificar mroutes:

<#root>

```
firepower#

show mroute



Multicast Routing Table
```

```
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(*, 230.1.1.1), 01:04:30/00:02:50, RP 192.168.2.2, flags: S <--- *,G entry



Incoming interface: Tunnel0


  RPF nbr: 192.168.2.2
  Immediate Outgoing interface list:


outside

, Forward, 01:04:30/00:02:50


(192.168.1.100, 230.1.1.1), 00:00:04/00:03:28, flags: ST S <--- S,G entry


  Incoming interface:

inside


  RPF nbr: 192.168.2.1
  Immediate Outgoing interface list:


outside, Forward, 00:00:03/00:03:25
```

- Verificar contadores PIM:

<#root>

```
firepower #

show pim traffic


PIM Traffic Counters
Elapsed time since counters cleared: 02:24:37

                              Received     Sent

Valid PIM Packets             948          755



Hello                         467          584



Join-Prune                    125          32
```

```
Register                      344         16


Register Stop                 12          129


Assert                        0           0
Bidir DF Election             0           0

Errors:
Malformed Packets                           0
Bad Checksums                               0
Send Errors                                 0
Packet Sent on Loopback Errors              0
Packets Received on PIM-disabled Interface  0
Packets Received with Unknown PIM Version   0
Packets Received with Incorrect Addressing  0
```

- Colete saídas adicionais (x.x.x.x é o grupo multicast, y.y.y.y é o IP RP). Recomenda-se coletar as saídas **algumas vezes**:

<#root>

```
show conn all protocol udp address x.x.x.x



show conn all | i PIM



show local-host x.x.x.x



show asp event dp-cp



show asp drop



show asp cluster counter



show asp table routing y.y.y.y



show route y.y.y.y



show mroute



show pim interface



show pim neighbor
show igmp interface
```

```
show mfib count
```

- Colete pacotes de interface multicast brutos e capturas de queda ASP:

<#root>

```
capture capi interface

      buffer 32000000 match udp host X host Z <--- (ingress capture for multicast UDP traffic from host

capture capo interface

      buffer 32000000 match udp host X host Z <--- (egress capture for multicast UDP traffic from host X

capture asp type asp-drop buffer 32000000 match udp host X host Z <--- (ASP drop capture for multicast U
```

- Syslog - IDs comuns são 302015, 302016 e 710005.

LHR

Considere as etapas mencionadas na seção para o RP e estas verificações adicionais:

- Mroutes:

<#root>

```
firepower#

show mroute



Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State


(*, 230.1.1.1), 00:23:30/never, RP 10.10.10.1, flags: SCJ <--- C flag means connected receiver


  Incoming interface:

inside


  RPF nbr: 192.168.2.1
  Immediate Outgoing interface list:


outside

, Forward, 00:23:30/never


(192.168.1.100, 230.1.1.1), 00:00:36/00:03:04, flags: SJT <--- J flag indicates switchover to SPT, T fla


  Incoming interface:

inside


  RPF nbr: 192.168.2.1
  Inherited Outgoing interface list:


outside

, Forward, 00:23:30/never


(*, 230.1.1.2), 00:01:50/never, RP 10.10.10.1, flags: SCJ <--- C flag means connected receiver


  Incoming interface:

inside


  RPF nbr: 192.168.2.1
  Immediate Outgoing interface list:


outside

, Forward, 00:01:50/never


(192.168.1.100, 230.1.1.2), 00:00:10/00:03:29, flags: SJT <--- <--- J flag indicates switchover to SPT,
  Incoming interface:
inside

  RPF nbr: 192.168.2.1
  Inherited Outgoing interface list:

outside
, Forward, 00:01:50/never
```

- Grupos IGMP:

<#root>

```
firepower#
show igmp groups detail <--- The list of IGMP groups

Interface:      outside
Group:          230.1.1.1

Uptime:         00:21:42
Router mode:    EXCLUDE (Expires: 00:03:17)
Host mode:      INCLUDE
Last reporter:  192.168.3.100 <--- Host joined group 230.1.1.1

Source list is empty
Interface:      outside

Group:          230.1.1.2

Uptime:         00:00:02
Router mode:    EXCLUDE (Expires: 00:04:17)
Host mode:      INCLUDE
Last reporter:  192.168.3.101 <--- Host joined group 230.1.1.2

Source list is empty
```

- Estatísticas de tráfego IGMP:

<#root>

```
firepower#
show igmp traffic
```

```
IGMP Traffic Counters
Elapsed time since counters cleared: 1d04h

                              Received     Sent
Valid IGMP Packets            2468         856
Queries                       2448         856
Reports                       20           0
Leaves                        0            0
Mtrace packets                0            0
DVMRP packets                 0            0
PIM packets                   0            0

Errors:
Malformed Packets             0
Martian source                0
Bad Checksums                 0
```

Comandos de identificação e solução de problemas do PIM (Folha de especificações)

Comando	**Descrição**
show running-config multicast-routing	Para ver se o roteamento multicast está ativado no firewall
show run mroute	Para ver as rotas estáticas configuradas no firewall
show running-config pim	Para ver a configuração PIM no firewall
show pim interface	Para ver quais interfaces de firewall têm o PIM ativado e os vizinhos PIM.
show pim neighbor	Para ver os vizinhos PIM
show pim group-map	Para ver os grupos multicast mapeados para o RP
show mroute	Para ver a tabela completa de roteamento multicast
show mroute 230 10 10 10	Para ver a tabela multicast de um grupo multicast específico
show pim tunnel	Para ver se há um túnel PIM construído entre o firewall e o RP

show conn all detail address RP_IP_ADDRESS	Para ver se há uma conexão (túnel PIM) estabelecida entre o firewall e o RP
show pim topology	Para ver a saída da topologia PIM do firewall
debug pim	Esta depuração mostra todas as mensagens PIM de e para o firewall
debug pim group 230.10.10.10	Esta depuração mostra todas as mensagens PIM de e para o firewall do grupo multicast específico
show pim traffic	Para ver estatísticas sobre mensagens PIM recebidas e enviadas
show asp cluster counter	Para verificar o número de pacotes tratados no Slow Path vs Fast Path vs Control Point
show asp drop	Para ver todas as quedas de nível de software no firewall
capture CAP interface INSIDE trace match pim any any	Para capturar e rastrear pacotes multicast PIM de entrada no firewall
capture CAP interface INSIDE trace match udp host 224.1.2.3 any	Para capturar e rastrear o fluxo multicast de entrada
show pim bsr-router	Para verificar quem é o roteador BSR eleito
show conn all address 224.1.2.3	Para mostrar a conexão multicast pai
show local-host 224.1.2.3	Mostrar as conexões multicast filho/stub

Para obter mais informações sobre capturas de firewall, verifique: Trabalhe com capturas do Firepower Threat Defense e Packet Tracer

Problemas conhecidos

Limitações de multicast do Firepower:

- Não suporta IPv6.

- O multicast PIM/IGMP não é suportado em interfaces em uma zona de tráfego (EMCP).
- O firewall não pode ser simultaneamente um RP e um FHR.
- O comando **show conn all** mostra apenas as conexões de multicast de identidade. Para mostrar a conexão multicast stub/secundária, use o comando **show local-host <*group IP*>** .

PIM não é suportado em um vPC Nexus

Se você tentar implantar uma adjacência de PIM entre um Nexus vPC e o Firewall, há uma limitação do Nexus, conforme descrito aqui:

Topologias compatíveis com o roteamento por Virtual Port Channel nas plataformas Nexus

Do ponto de vista do NGFW, você vê na captura com trace este drop:

<#root>

```
Result:
input-interface: NET102
input-status: up
input-line-status: up
output-interface: NET102
output-status: up
output-line-status: up
Action: drop

Drop-reason: (no-mcast-intrf) FP no mcast output intrf      <-- The ingress multicast packet is dropped
```

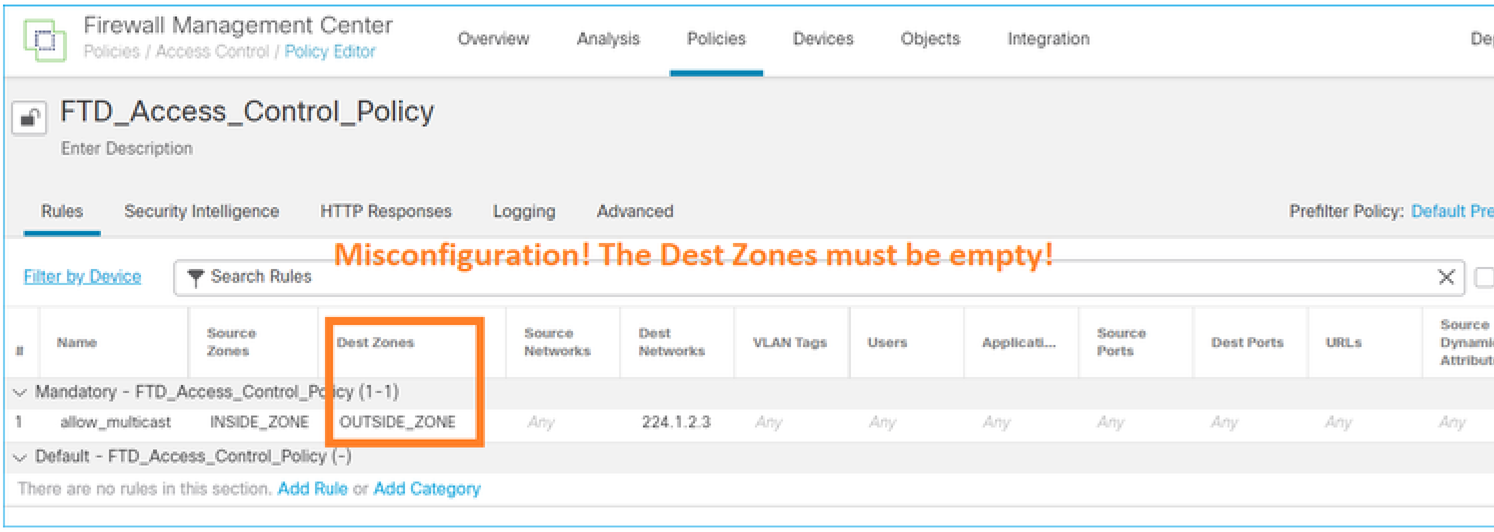
O firewall não pode concluir o registro RP:

<#root>

```
firepower#

show mroute 224.1.2.3


Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(*, 224.1.2.3), 01:05:21/never, RP 10.1.0.209, flags: SCJ
  Incoming interface: OUTSIDE
  RPF nbr: 10.1.104.10
  Immediate Outgoing interface list:
    Server_102, Forward, 01:05:21/never

(10.1.1.48, 224.1.2.3), 00:39:15/00:00:04, flags: SFJT
  Incoming interface: NET102

  RPF nbr: 10.1.1.48, Registering         <-- The RP Registration is stuck

  Immediate Outgoing interface list:
    Tunnel0, Forward, 00:39:15/never
```

Zonas de destino sem suporte

Você não pode especificar uma zona de segurança de destino para a regra da Política de Controle de Acesso que corresponde ao tráfego multicast:



Firewall Management Center
Policies / Access Control / Policy Editor
Overview
Analysis
Policies
Devices
Objects
Integration
De

FTD_Access_Control_Policy

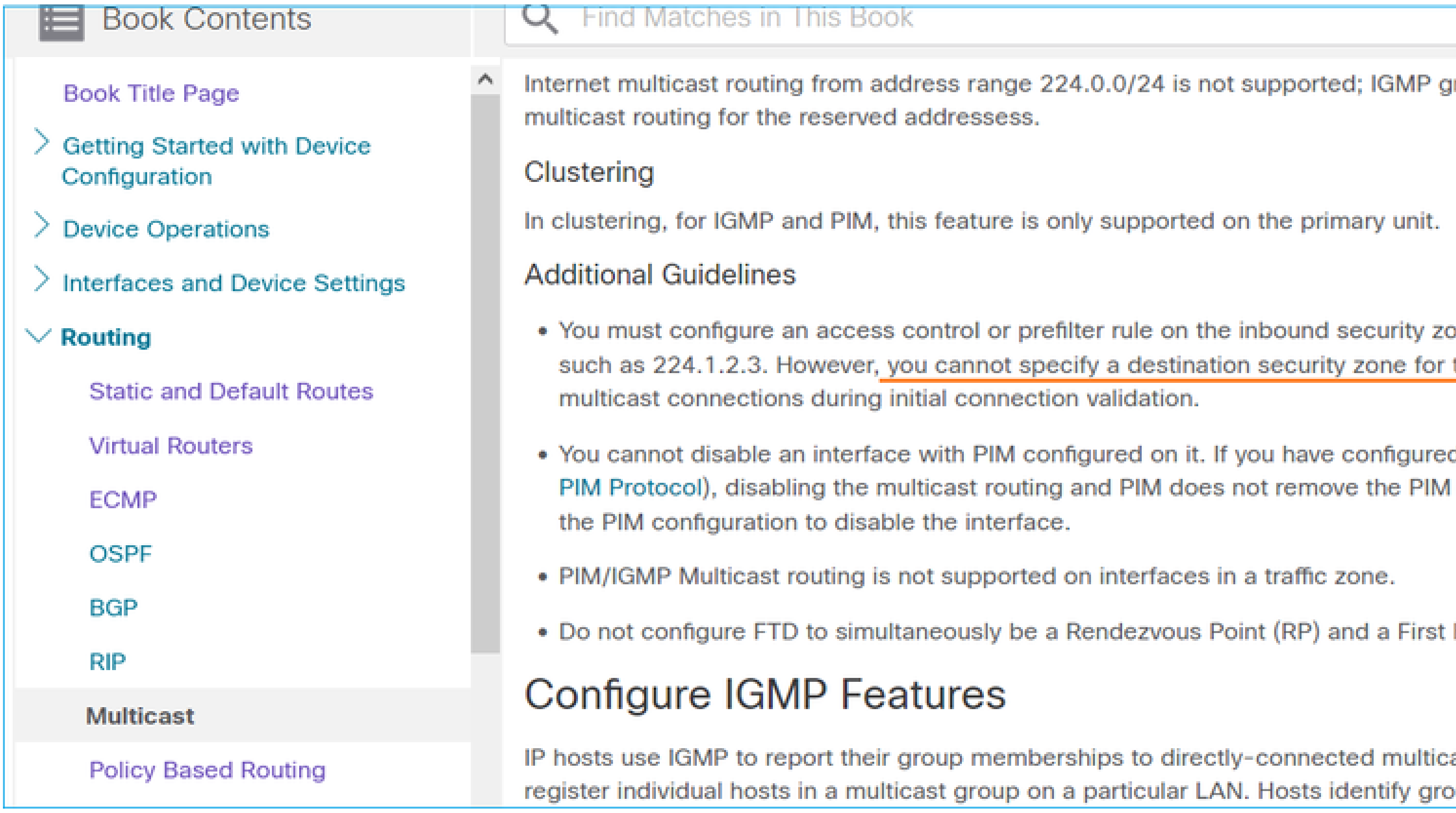
Enter Description

Misconfiguration! The Dest Zones must be empty!

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source Ports	Dest Ports	URLs	Source Dynami Attribut
Mandatory - FTD_Access_Control_Policy (1-1)												
1	allow_multicast	INSIDE_ZONE	OUTSIDE_ZONE	Any	224.1.2.3	Any	Any	Any	Any	Any	Any	Any
Default - FTD_Access_Control_Policy (-)												

There are no rules in this section. Add Rule or Add Category

Este fato está igualmente documentado no guia do utilizador do FMC:



Book Contents
Find Matches in This Book
Book Title Page
Getting Started with Device Configuration
Device Operations
Interfaces and Device Settings
Routing
Static and Default Routes
Virtual Routers
ECMP
OSPF
BGP
RIP
Multicast
Policy Based Routing

Internet multicast routing from address range 224.0.0/24 is not supported; IGMP g multicast routing for the reserved addressess.

Clustering

In clustering, for IGMP and PIM, this feature is only supported on the primary unit.

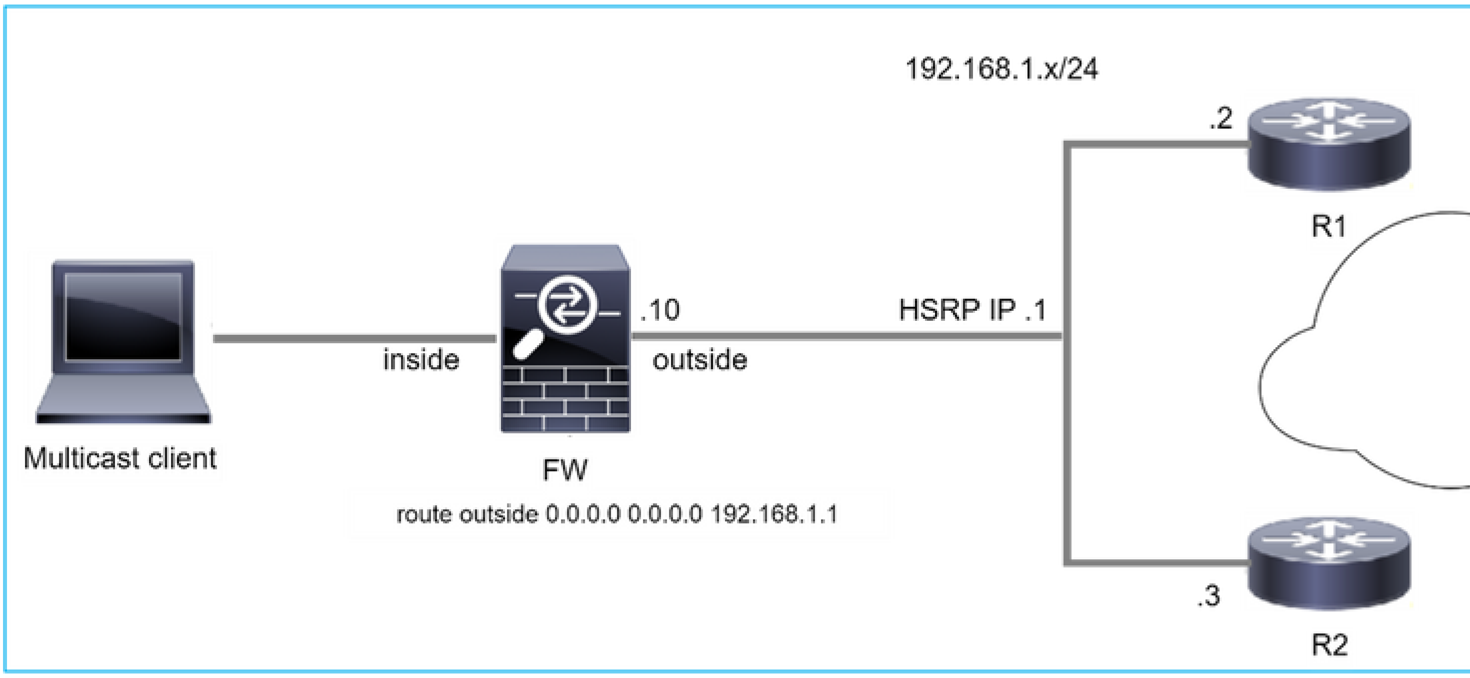
Additional Guidelines

- You must configure an access control or prefilter rule on the inbound security zo such as 224.1.2.3. However, you cannot specify a destination security zone for t multicast connections during initial connection validation.
- You cannot disable an interface with PIM configured on it. If you have configured PIM Protocol), disabling the multicast routing and PIM does not remove the PIM the PIM configuration to disable the interface.
- PIM/IGMP Multicast routing is not supported on interfaces in a traffic zone.
- Do not configure FTD to simultaneously be a Rendezvous Point (RP) and a First l

Configure IGMP Features

IP hosts use IGMP to report their group memberships to directly-connected multica register individual hosts in a multicast group on a particular LAN. Hosts identify gro

O Firewall não envia mensagens PIM para roteadores upstream devido ao HSRP



Nesse caso, o firewall tem uma rota padrão através do protocolo Hot Standby Redundancy Protocol (HSRP) IP 192.168.1.1 e vizinhança PIM com os roteadores R1 e R2:

<#root>

```
firepower#

show run route

route outside 0.0.0.0 0.0.0.0 192.168.1.1 1
```

O firewall tem adjacência PIM entre o IP externo e o IP da interface física em R1 e R2:

<#root>

```
firepower#

show pim neighbor

Neighbor Address  Interface          Uptime    Expires DR pri Bidir
192.168.1.1       outside            01:18:27  00:01:25 1
192.168.1.2       outside            01:18:03  00:01:29 1 (DR)
```

O firewall não envia a mensagem PIM Join para a rede upstream. O comando de depuração PIM **debug pim** mostra esta saída:

<#root>

```
firepower#

debug pim
```

```
...

IPv4 PIM: Sending J/P to an invalid neighbor: outside 192.168.1.1
```

O RFC 2362 afirma que *"um roteador envia uma mensagem periódica de Junção/Remoção para cada vizinho RPF distinto associado a cada entrada (S,G), (*,G) e (*,*,RP). Mensagens de junção e remoção são enviadas somente se o vizinho de RPF for um vizinho de PIM.*

Para atenuar o problema, o usuário pode adicionar uma entrada mroute estática no firewall. O roteador deve apontar para um dos dois endereços IP da interface do roteador, 192.168.1.2 ou 192.168.1.3, normalmente o IP do roteador ativo do HSRP.

Exemplo:

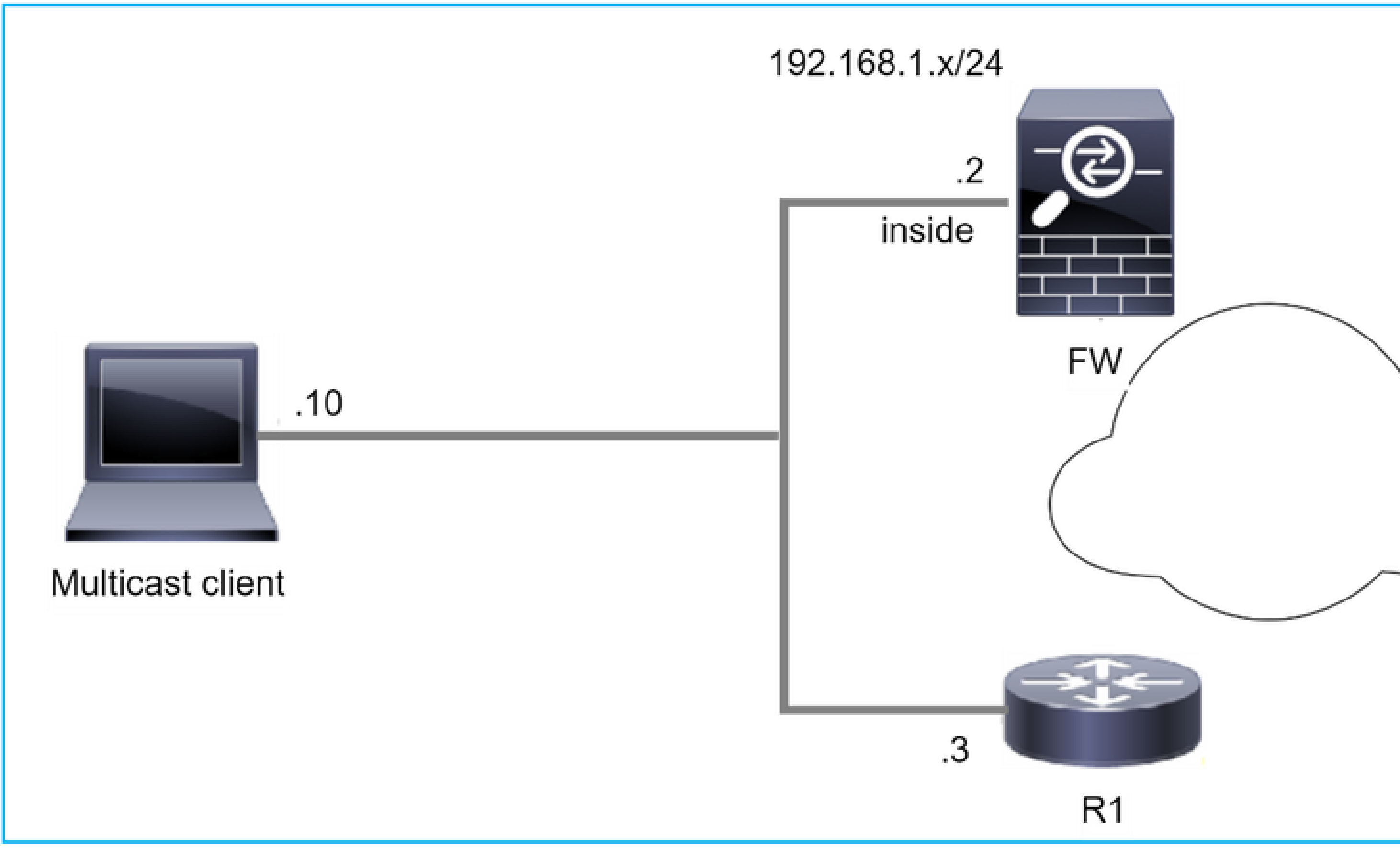
<#root>

```
firepower#

show run mroute


firepower#

mroute 172.16.1.1 255.255.255.255 192.168.1.2
```

Uma vez que a configuração mroute estática está em vigor, para a pesquisa de RPF, o firewall dá preferência à tabela de roteamento multicast em vez da tabela de roteamento unicast do ASA e envia as mensagens PIM diretamente ao vizinho 192.168.1.2.

Observação: o mroute estático, em certa medida, anula a utilidade da redundância de HSRP, já que o mroute aceita apenas 1 próximo salto por combinação de endereço/máscara de rede. Se o próximo salto especificado no comando mroute falhar ou se tornar inalcançável, o firewall não voltará para o outro roteador.

O firewall não é considerado como LHR quando não é o DR no segmento de LAN



O firewall tem R1 como vizinhos PIM no segmento de LAN. R1 é o PIM DR:

<#root>

```
firepower#

show pim neighbor

Neighbor Address  Interface          Uptime    Expires DR pri Bidir

192.168.1.3       inside             00:12:50  00:01:38 1 (DR)
```

Se a solicitação de união IGMP do cliente for recebida, o firewall não se tornará o LHR.

O mroute mostra **Null** adicional como o OIL e tem o sinalizador **Pruned**:

<#root>

```
firepower#

show mroute

Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State


(*, 230.1.1.1), 00:06:30/never, RP 0.0.0.0,

flags

: S

P

C
  Incoming interface: Null
  RPF nbr: 0.0.0.0
  Immediate Outgoing interface list:


inside, Null, 00:06:30/never <--- OIL has inside and Null
```

Para tornar o firewall o LHR, a prioridade do DR da interface pode ser aumentada.

<#root>

```
firepower#

interface GigabitEthernet0/0


firepower#

pim dr-priority 2



firepower#

show pim neighbor


Neighbor Address  Interface          Uptime    Expires DR pri Bidir

192.168.1.3       inside             17:05:28  00:01:41 1
```

O comando de depuração PIM **debug pim** mostra esta saída:

<#root>

```
firepower#

debug pim

firepower#


IPv4 PIM: (*,230.1.1.1) inside Start being last hop <--- Firewall considers itself as the lasp hop
```

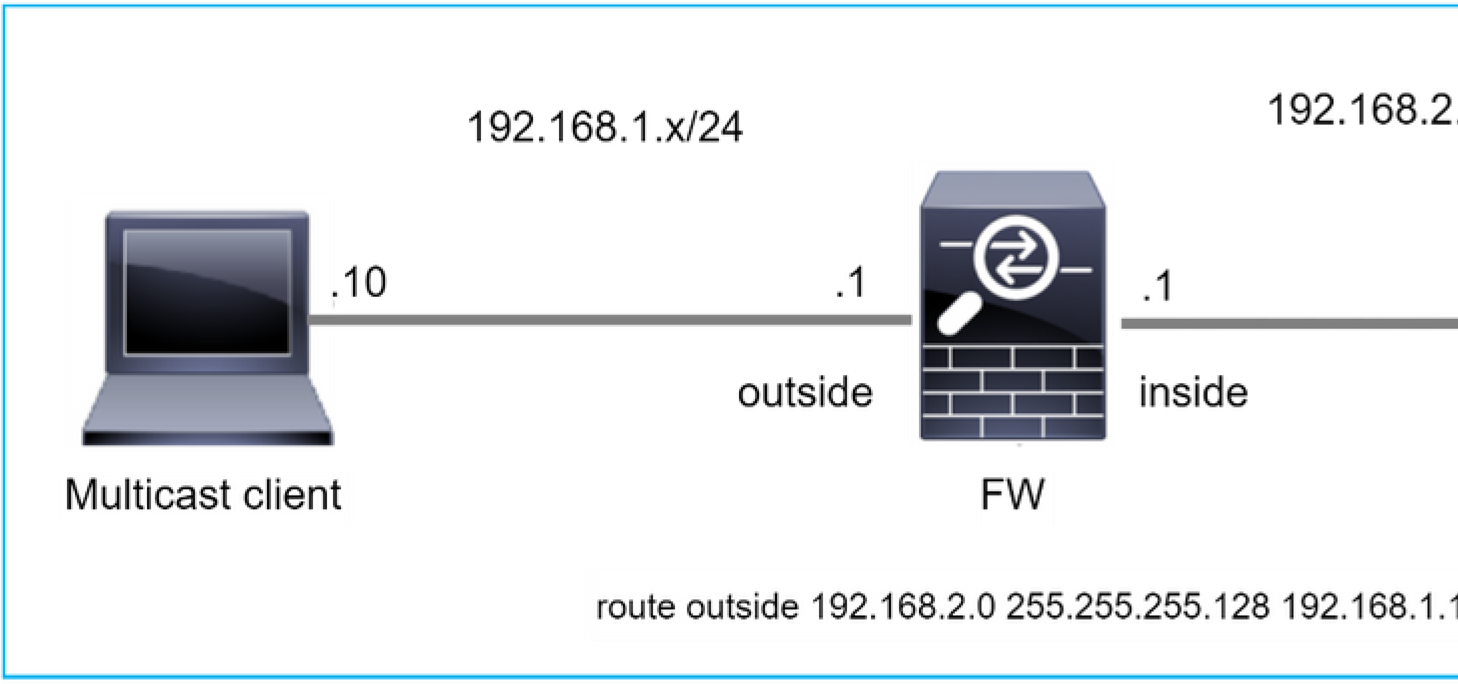
```
IPv4 PIM: (*,230.1.1.1) Start being last hop


IPv4 PIM: (*,230.1.1.1) Start signaling sources
IPv4 PIM: [0] (*,230.1.1.1/32) NULLIF-skip MRIB modify NS
IPv4 PIM: (*,230.1.1.1) inside FWD state change from Prune to Forward
IPv4 PIM: [0] (*,230.1.1.1/32) inside MRIB modify F NS
IPv4 PIM: (*,230.1.1.1) Updating J/P status from Null to Join
IPv4 PIM: (*,230.1.1.1) J/P scheduled in 0.0 secs
IPv4 PIM: (*,230.1.1.1) Processing timers
IPv4 PIM: (*,230.1.1.1) J/P processing
IPv4 PIM: (*,230.1.1.1) Periodic J/P scheduled in 50 secs
IPv4 PIM: (*,230.1.1.1) No RPF interface to send J/P
```

O sinalizador Removido e o Nulo são removidos do mroute:

<#root>

```
firepower#

show mroute



Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(*, 230.1.1.1), 16:48:23/never, RP 0.0.0.0, flags:

SCJ


  Incoming interface: Null
  RPF nbr: 0.0.0.0
  Immediate Outgoing interface list:

    inside, Forward, 16:48:23/never
```

O firewall descarta pacotes multicast devido à falha de verificação de encaminhamento de caminho reverso



Nesse caso, os pacotes UDP multicast são descartados devido à falha de RPF, pois o firewall tem uma rota mais específica com a máscara 255.255.255.128 através da interface externa.

<#root>

```
firepower#

capture capi type raw-data trace interface inside match udp any any


firepower#

show captureture capi packet-number 1 trace



106 packets captured
   1: 08:57:18.867234       192.168.2.2.12345 > 230.1.1.1.12354:  udp 500
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 2684 ns
Config:
Additional Information:
MAC Access list


Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 2684 ns
Config:
Implicit Rule
Additional Information:
MAC Access list
```

```
Phase: 3
Type: INPUT-ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Elapsed time: 13664 ns
Config:
Additional Information:
Found next-hop 192.168.1.100 using egress ifc  outside

Phase: 4
Type: INPUT-ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Elapsed time: 8296 ns
Config:
Additional Information:
Found next-hop 192.168.1.100 using egress ifc  outside

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: drop
Time Taken: 27328 ns
```

Drop-reason: (rpf-violated) Reverse-path verify failed, Drop-location: frame 0x0000556bcb1069dd flow

```
(NA)/NA
```

```
firepower#
```

show route static

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is not set
```

S   192.168.2.0 255.255.255.128 [1/0] via 192.168.1.100, outside

As capturas de queda de ASP mostram a razão de queda de **rpf-violated**:

<#root>

```
firepower#
```

show capture asp

```
Target:     OTHER
```

```
Hardware:   ASAv
Cisco Adaptive Security Appliance Software Version 9.19(1)
ASLR enabled, text region 556bc9390000-556bcd0603dd

21 packets captured



1: 09:00:53.608290       192.168.2.2.12345 > 230.1.1.1.12354:  udp 500 Drop-reason: (rpf-violated) Rever


   2: 09:00:53.708032       192.168.2.2.12345 > 230.1.1.1.12354:  udp 500 Drop-reason: (rpf-violated) Re
   3: 09:00:53.812152       192.168.2.2.12345 > 230.1.1.1.12354:  udp 500 Drop-reason: (rpf-violated) Re
   4: 09:00:53.908613       192.168.2.2.12345 > 230.1.1.1.12354:  udp 500 Drop-reason: (rpf-violated) Re
```

Os contadores com falha de RPF nos aumentos de saída de MFIB:

<#root>

```
firepower#

show mfib 230.1.1.1 count


IP Multicast Statistics
7 routes, 4 groups, 0.00 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group: 230.1.1.1


  RP-tree:

   Forwarding: 0/0/0/0, Other: 6788/6788/0



...
firepower#

show mfib 230.1.1.1 count


IP Multicast Statistics
7 routes, 4 groups, 0.00 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Group: 230.1.1.1
  RP-tree:


Forwarding: 0/0/0/0, Other: 6812/6812/0 <--- RPF failed counter increased
```

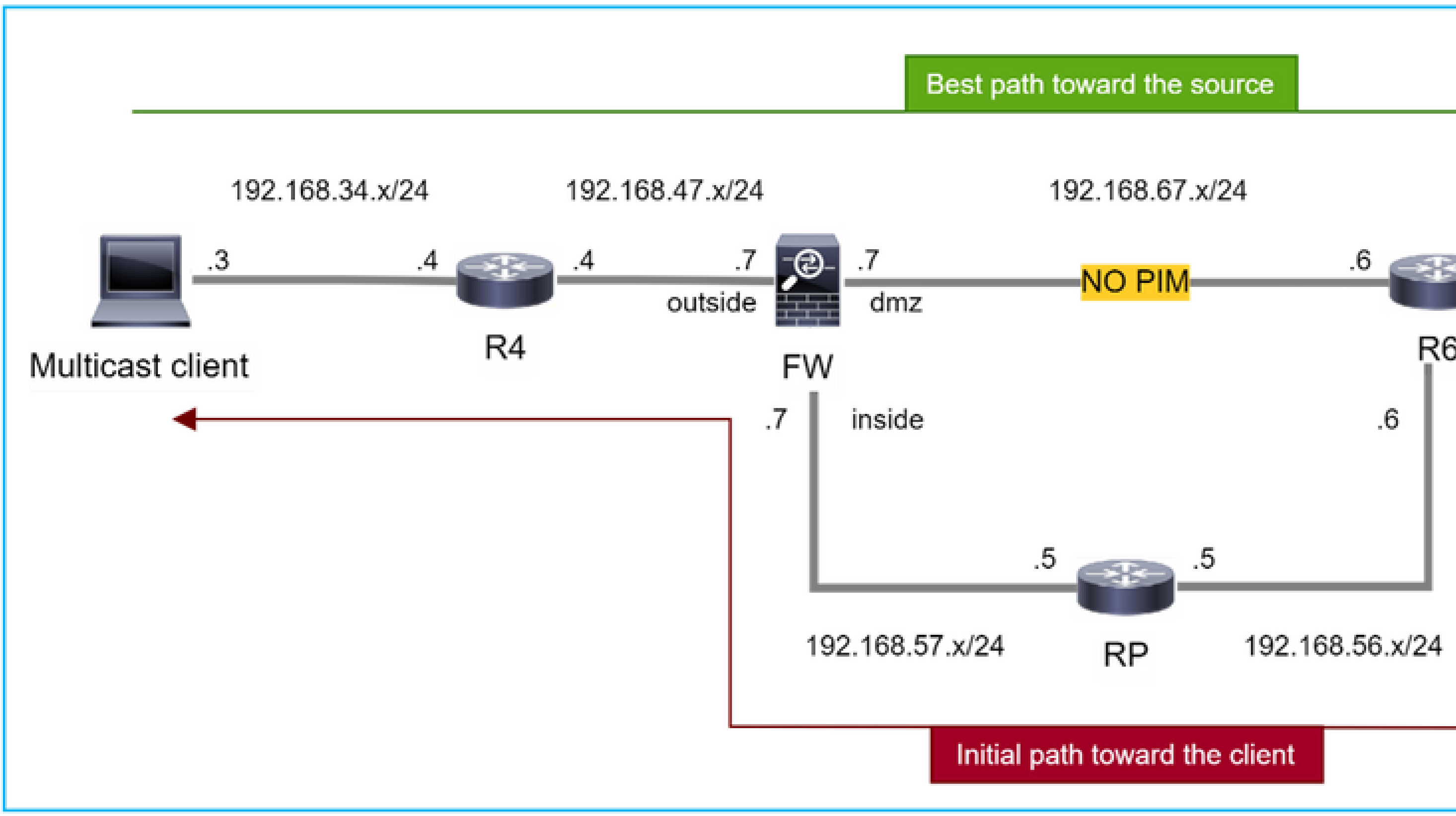
A solução é corrigir a falha de verificação de RPF. Uma opção é remover a rota estática.

Se não houver mais falha de verificação de RPF, os pacotes serão encaminhados e o contador **Forwarding** na saída de MFIB aumentará:

<#root>

```
firepower#

show mfib 230.1.1.1 count


IP Multicast Statistics
8 routes, 4 groups, 0.25 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Group: 230.1.1.1
  RP-tree:
   Forwarding: 0/0/0/0, Other: 9342/9342/0

  Source: 192.168.2.2,



   Forwarding: 1033/9/528/39

, Other: 0/0/0
  Tot. shown: Source count: 1, pkt count: 0
...
firepower#

show mfib 230.1.1.1 count


IP Multicast Statistics
8 routes, 4 groups, 0.25 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Group: 230.1.1.1
  RP-tree:
   Forwarding: 0/0/0/0, Other: 9342/9342/0

  Source: 192.168.2.2,



   Forwarding: 1044/10/528/41

, Other: 0/0/0

<--- Forward counter increased


  Tot. shown: Source count: 1, pkt count: 0
```

Firewall não gera união PIM ao alternar PIM para árvore de origem



Nesse caso, o firewall aprende o caminho em direção à origem de multicast através da interface **dmz R4** > **FW** > **R6**, enquanto o caminho de tráfego inicial da origem para o cliente é **R6** > **RP** > **DW** > **R4:**

<#root>

```
firepower#

show route 192.168.6.100



Routing entry for 192.168.6.0 255.255.255.0
  Known via "ospf 1", distance 110, metric 11, type intra area


Last update from 192.168.67.6 on dmz, 0:36:22 ago


  Routing Descriptor Blocks:


* 192.168.67.6, from 192.168.67.6, 0:36:22 ago, via dmz


      Route metric is 11, traffic share count is 1
```

O R4 inicia o switchover SPT e envia a mensagem de junção PIM específica da origem assim que o limite de switchover SPT é atingido. No firewall, o switchover de SPT não ocorre, a rota (S,G) mroute não tem o sinalizador **T**:

<#root>

```
firepower#

show mroute


Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(*, 230.1.1.1), 00:00:05/00:03:24, RP 10.5.5.5, flags: S
  Incoming interface: inside
  RPF nbr: 192.168.57.5
  Immediate Outgoing interface list:
    outside, Forward, 00:00:05/00:03:24


(192.168.6.100, 230.1.1.1), 00:00:05/00:03:24, flags: S


  Incoming interface: dmz
  RPF nbr: 192.168.67.6
  Immediate Outgoing interface list:
    outside, Forward, 00:00:05/00:03:2
```

O comando de depuração PIM **debug pim** mostra 2 solicitação de junção PIM recebida do peer R4 - para **(*,G) e (S,G).** O firewall enviou a solicitação de PIM Join para (*,G) upstream e falhou ao enviar a solicitação específica de origem devido ao vizinho inválido 192.168.67.6:

<#root>

```
firepower#

debug pim



IPv4 PIM: Received J/P on outside from 192.168.47.4 target: 192.168.47.7 (to us) <--- 1st PIM join to th



IPv4 PIM: J/P entry: Join root: 10.5.5.5 group: 230.1.1.1 flags:  RPT WC S <--- 1st PIM join with root a


IPv4 PIM: (*,230.1.1.1) Create entry
IPv4 PIM: [0] (*,230.1.1.1/32) MRIB modify DC
IPv4 PIM: [0] (*,230.1.1.1/32) inside MRIB modify A
IPv4 PIM: (*,230.1.1.1) outside J/P state changed from Null to Join
IPv4 PIM: (*,230.1.1.1) outside Raise J/P expiration timer to 210 seconds
IPv4 PIM: (*,230.1.1.1) outside FWD state change from Prune to Forward
IPv4 PIM: [0] (*,230.1.1.1/32) outside MRIB modify F NS
IPv4 PIM: (*,230.1.1.1) Updating J/P status from Null to Join
IPv4 PIM: (*,230.1.1.1) J/P scheduled in 0.0 secs
IPv4 PIM: (*,230.1.1.1) Processing timers
IPv4 PIM: (*,230.1.1.1) J/P processing
IPv4 PIM: (*,230.1.1.1) Periodic J/P scheduled in 50 secs
IPv4 PIM: (*,230.1.1.1) J/P adding Join on inside
```

```
IPv4 PIM: Sending J/P message for neighbor 192.168.57.5 on inside for 1 groups   <--- PIM Join sent from
```

```
IPv4 PIM: Received J/P on outside from 192.168.47.4 target: 192.168.47.7 (to us) <--- 1st PIM join to th
```

```
IPv4 PIM: J/P entry: Join root: 192.168.6.100 group: 230.1.1.1 flags:  S         <--- 1st PIM join with
```

```
IPv4 PIM: (192.168.6.100,230.1.1.1) Create entry
IPv4 PIM: Adding monitor for 192.168.6.100
IPv4 PIM: RPF lookup for root 192.168.6.100: nbr 192.168.67.6, dmz via the rib
IPv4 PIM: (192.168.6.100,230.1.1.1) RPF changed from 0.0.0.0/- to 192.168.67.6/dmz
IPv4 PIM: (192.168.6.100,230.1.1.1) Source metric changed from [0/0] to [110/11]
IPv4 PIM: [0] (192.168.6.100,230.1.1.1/32) MRIB modify DC
IPv4 PIM: [0] (192.168.6.100,230.1.1.1/32) inside MRIB modify A
IPv4 PIM: [0] (192.168.6.100,230.1.1.1/32) outside MRIB modify F NS
IPv4 PIM: (192.168.6.100,230.1.1.1) outside J/P state changed from Null to Join
IPv4 PIM: (192.168.6.100,230.1.1.1) outside Imm FWD state change from Prune to Forward
IPv4 PIM: (192.168.6.100,230.1.1.1) Updating J/P status from Null to Join
IPv4 PIM: (192.168.6.100,230.1.1.1) J/P scheduled in 0.0 secs
IPv4 PIM: [0] (192.168.6.100,230.1.1.1/32) dmz MRIB modify NS
IPv4 PIM: (192.168.6.100,230.1.1.1) outside Raise J/P expiration timer to 210 seconds
IPv4 PIM: (192.168.6.100,230.1.1.1) Processing timers
IPv4 PIM: (192.168.6.100,230.1.1.1) J/P processing
IPv4 PIM: (192.168.6.100,230.1.1.1) Periodic J/P scheduled in 50 secs
IPv4 PIM: (192.168.6.100,230.1.1.1) J/P adding Join on dmz
```

```
IPv4 PIM: Sending J/P to an invalid neighbor: dmz 192.168.67.6
```

```
<--- Invalid neighbor
```

A saída dos comandos **show pim neigbour** não tem R6:

<#root>

```
firepower#
```

```
show pim neighbor
```

```
Neighbor Address  Interface          Uptime    Expires DR pri Bidir
192.168.47.4      outside            00:21:12  00:01:44 1
192.168.57.5      inside             02:43:43  00:01:15 1
```

O PIM está habilitado na interface de firewall dmz:

<#root>

```
firepower#
```

```
show pim interface
```

```
Address          Interface          PIM  Nbr   Hello  DR         DR
                                         Count Intvl  Prior

192.168.47.7     outside            on   1     30     1          this system

192.168.67.7     dmz                on   0     30     1          this system


192.168.57.7     inside             on   1     30     1          this system
```

O PIM está desabilitado na interface R6:

<#root>

```
R6#

show ip interface brief


Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         192.168.6.1     YES manual up                    up
GigabitEthernet0/1         192.168.56.6    YES manual up                    up
GigabitEthernet0/2         unassigned      YES unset  administratively down down

GigabitEthernet0/3         192.168.67.6    YES manual up                    up


Tunnel0                    192.168.56.6    YES unset  up                    up

R6#

show ip pim interface GigabitEthernet0/3 detail


GigabitEthernet0/3 is up, line protocol is up
  Internet address is 192.168.67.6/24
  Multicast switching: fast
  Multicast packets in/out: 0/123628
  Multicast TTL threshold: 0


PIM: disabled <--- PIM is disabled


  Multicast Tagswitching: disabled
```

A solução é ativar o PIM na interface GigabitEthernet0/3 em R6:

<#root>

```
R6(config-if)#

interface GigabitEthernet0/3


R6(config-if)#

ip pim sparse-mode
```

```
R6(config-if)#
*Apr 21 13:17:14.575: %PIM-5-NBRCHG: neighbor 192.168.67.7 UP on interface GigabitEthernet0/3
```

```
*Apr 21 13:17:14.577: %PIM-5-DRCHG: DR change from neighbor 0.0.0.0 to 192.168.67.7 on interface Gigabit
```

O firewall instala a flag T, que indica o switchover SPT**:**

<#root>

```
firepower#
```

```
show mroute
```

```
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(*, 230.1.1.1), 00:26:30/00:02:50, RP 10.5.5.5, flags: S
  Incoming interface: inside
  RPF nbr: 192.168.57.5
  Immediate Outgoing interface list:
    outside, Forward, 00:26:30/00:02:50
```

```
(192.168.6.100, 230.1.1.1), 00:26:30/00:03:29, flags: ST
```

```
  Incoming interface: dmz
  RPF nbr: 192.168.67.6
  Immediate Outgoing interface list:
    outside, Forward, 00:26:30/00:02:39
```

O firewall descarta os primeiros pacotes devido ao limite da taxa de punt

Quando o firewall recebe os primeiros pacotes de um **novo** fluxo multicast no FP, o processamento adicional pelo CP pode ser exigido. Nesse caso, o FP direciona os pacotes para o PC via SP (FP > SP > CP) para operações adicionais:

- Criação de uma **conexão pai** no FP entre as interfaces de entrada e as interfaces de identidade.
- Verificações adicionais específicas de multicast, como validação de RPF, encapsulamento de PIM (no caso de o firewall ser o FHR), verificação de OIL e assim por diante.
- Criação de uma entrada (S,G) com as interfaces de entrada e saída na tabela mroute.
- Criação de uma conexão **filho/stub** no FP entre as interfaces de entrada e saída.

Como parte da proteção do plano de controle, o firewall limita internamente a taxa de pacotes apontados para o PC.

Os pacotes que excedem a taxa são descartados no com o motivo de descarte **punt-rate-limit**:

<#root>

```
firepower#

show asp drop


Frame drop:


Punt rate limit exceeded (punt-rate-limit) 2062
```

Use o comando **show asp cluster counter** para verificar o número de pacotes multicast enviados para o CP do SP:

<#root>

```
firepower#

show asp cluster counter


Global dp-counters:

Context specific dp-counters:

MCAST_FP_FROM_PUNT               30      Number of multicast packets punted from CP to FP
MCAST_FP_TO_SP                   2680    Number of multicast packets punted from FP to SP
MCAST_SP_TOTAL                   2710    Number of total multicast packets processed in SP

MCAST_SP_FROM_PUNT               30      Number of multicast packets punted from CP to SP <--- Number of


MCAST_SP_FROM_PUNT_FORWARD       30      Number of multicast packets coming from CP that are forwarded
MCAST_SP_PKTS                    30      Number of multicast packets that require slow-path attention
MCAST_SP_PKTS_TO_CP              30      Number of multicast packets punted to CP from SP
MCAST_FP_CHK_FAIL_NO_HANDLE      2650    Number of multicast packets failed with no flow mcast_handle
MCAST_FP_CHK_FAIL_NO_FP_FWD      30      Number of multicast packets that cannot be fast-path forwarded
```

Use o comando **show asp event dp-cp punt** para verificar o número de pacotes na fila FP > CP e a taxa de 15 segundos:

<#root>

```
firepower#

show asp event dp-cp punt | begin EVENT-TYPE


EVENT-TYPE          ALLOC ALLOC-FAIL ENQUEUED ENQ-FAIL  RETIRED 15SEC-RATE
punt                  24452        0      24452      0      10852     1402


multicast

           23800        0

23800

      0      10200
```

```
1402


  pim                 652          0      652        0      652          0
```

Quando a mroute é preenchida e as conexões pai/filho são estabelecidas no FP, os pacotes são encaminhados no FP como parte das conexões existentes. Nesse caso, o FP não aponta os pacotes para o PC.

Como o firewall processa os primeiros pacotes de um novo fluxo multicast?

Quando o firewall recebe os primeiros pacotes de um **novo** fluxo multicast no caminho de dados, o firewall executa estas ações:

1. Verifica se a política de segurança permite pacotes.
2. Cobra os pacotes para o PC através do caminho FP.
3. Cria uma conexão **pai** entre as interfaces de entrada e as interfaces de identidade:

<#root>

```
firepower#

show capture capi packet-number 1 trace


10 packets captured

   1: 08:54:15.007003       192.168.1.100.12345 > 230.1.1.1.12345:  udp 400


Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: INPUT-ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 192.168.2.1 using egress ifc  inside


Phase: 4
Type: ACCESS-LIST
Subtype:
Result: ALLOW
```

```
Config:
Implicit Rule
Additional Information:

Phase: 5
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: QOS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 9
```

Type: MULTICAST

```
Subtype:
Result: ALLOW
Config:
Additional Information:


Phase: 10
```

Type: FLOW-CREATION

```
Subtype:
Result: ALLOW
Config:
Additional Information:
```

New flow created with id 19, packet dispatched to next module <--- New flow

```
Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
```

```
Action: allow
```

Syslogs:

<#root>

```
firepower# Apr 24 2023 08:54:15: %ASA-7-609001: Built local-host inside:192.168.1.100
Apr 24 2023 08:54:15: %FTD-7-609001: Built local-host identity:230.1.1.1

Apr 24 2023 08:54:15: %FTD-6-302015: Built inbound UDP connection 19 for inside:192.168.1.100/12345 (192
```

Essa conexão é visível na saída do comando **show conn all**:

<#root>

```
firepower#

show conn all protocol udp


13 in use, 17 most used


UDP inside  192.168.1.100:12345 NP Identity Ifc  230.1.1.1:12345, idle 0:00:02, bytes 0, flags â€“
```

4. O CP ativa o processo de multicast para verificações adicionais específicas de multicast, como a validação de RPF, o encapsulamento PIM (no caso do firewall ser o FHR), a verificação OIL e assim por diante.
5. O CP cria uma entrada (S,G) com as interfaces de entrada e saída no mroute:

<#root>

```
firepower#

show mroute



Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(*, 230.1.1.1), 00:19:28/00:03:13, RP 192.168.192.168, flags: S
  Incoming interface: inside
  RPF nbr: 192.168.2.1
  Immediate Outgoing interface list:
    outside, Forward, 00:19:28/00:03:13


(192.168.1.100, 230.1.1.1), 00:08:50/00:03:09, flags: ST
```

```
  Incoming interface: inside


  RPF nbr: 192.168.2.1
  Immediate Outgoing interface list:

    outside, Forward, 00:00:32/00:02:57
```

6. O CP instrui o FP via CP > SP > caminho FP para criar uma conexão **filho/stub** entre as interfaces de entrada e saída:

Essa conexão é visível apenas na saída do comando **show local-host**:

<#root>

```
firepower#

show local-host



Interface outside: 5 active, 5 maximum active
local host: <224.0.0.13>,
local host: <192.168.3.100>,
local host: <230.1.1.1>,

  Conn:



    UDP outside  230.1.1.1:12345 inside  192.168.1.100:12345, idle

 0:00:04, bytes 4000, flags -
local host: <224.0.0.5>,
local host: <224.0.0.1>,
Interface inside: 4 active, 5 maximum active
local host: <192.168.1.100>,


  Conn:



    UDP outside  230.1.1.1:12345 inside  192.168.1.100:12345, idle

 0:00:04, bytes 4000, flags -
local host: <224.0.0.13>,
local host: <192.168.2.1>,
local host: <224.0.0.5>,
Interface nlp_int_tap: 0 active, 2 maximum active
Interface any: 0 active, 0 maximum active
```

Nas versões de software com a correção do bug da Cisco ID CSCwe21280 , a mensagem de syslog 302015 para a conexão filho/stub também é gerada:

<#root>

```
Apr 24 2023 08:54:15: %FTD-6-302015:

Built outbound UDP connection 20 for outside:230.1.1.1/12345 (230.1.1.1/12345) to inside:192.168.1.100/1
```

Quando as conexões pai e filho/stub são estabelecidas, os pacotes de entrada correspondem à conexão existente e são encaminhados no FP:

<#root>

```
firepower#

show capture capi trace packet-number 2


10 packets captured
   2: 08:54:15.020567       192.168.1.100.12345 > 230.1.1.1.12345:  udp 400
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list


Phase: 3



Type: FLOW-LOOKUP


Subtype:
Result: ALLOW
Config:
Additional Information:

Found flow with id 19, using existing flow <--- Existing flow




Result:
input-interface: inside
input-status: up
input-line-status: up
Action: allow
```

Filtrar tráfego multicast ICMP

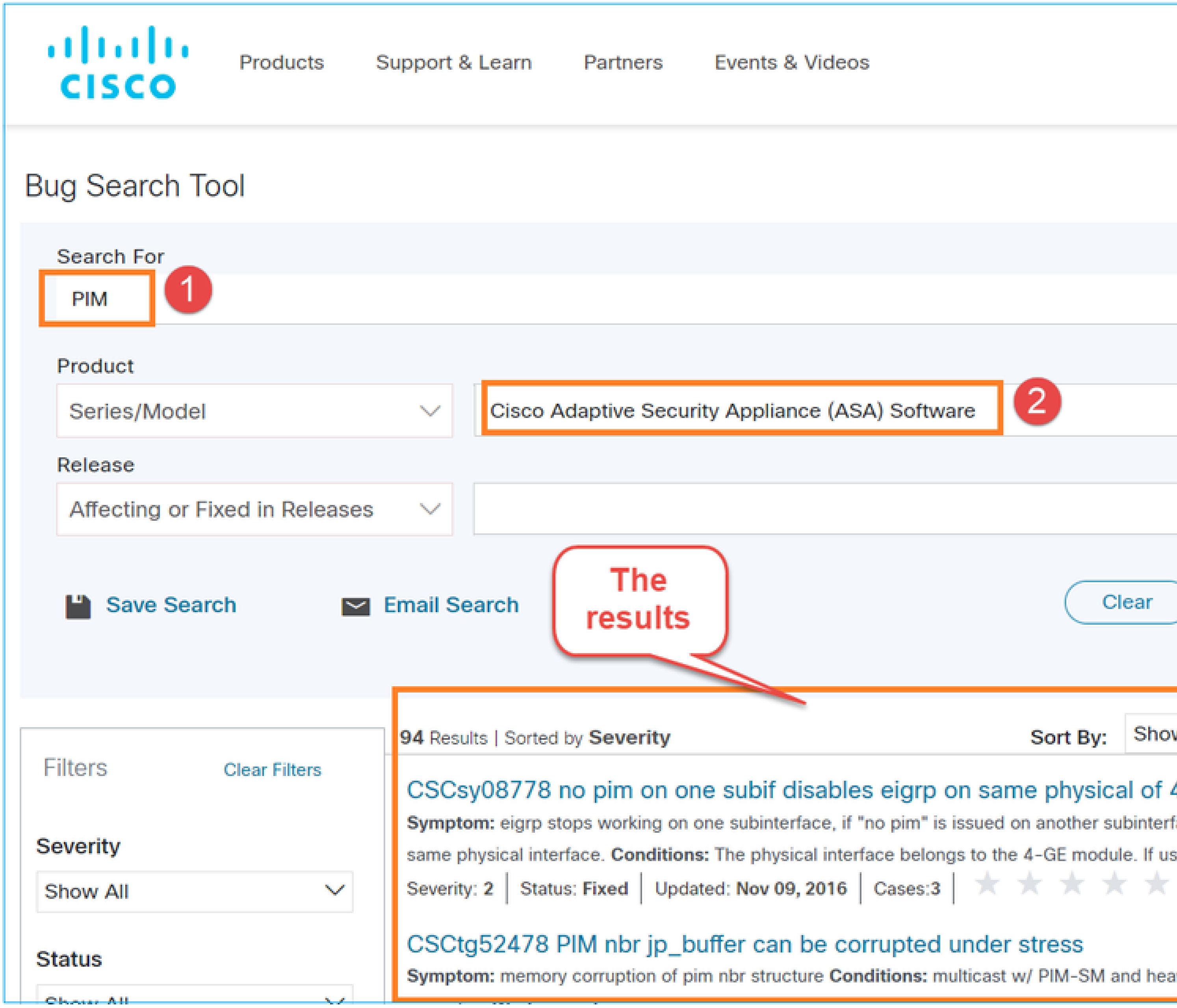
Não é possível filtrar o tráfego multicast ICMP com uma ACL. Você deve usar a política de plano de controle (ICMP):

O bug da Cisco ID CSCsl26860 ASA não filtra pacotes ICMP multicast

Defeitos conhecidos de Multicast PIM

Você pode usar a ferramenta Bug Search para defeitos conhecidos: https://bst.cloudapps.cisco.com/bugsearch

A maioria dos defeitos do ASA e do FTD estão relacionados no produto 'Cisco Adaptive Security Appliance (ASA) Software':



Bug Search Tool

Search For
PIM

Product
Series/Model
Cisco Adaptive Security Appliance (ASA) Software

Release
Affecting or Fixed in Releases

Severity
Show All

Status
Show All

94 Results | Sorted by Severity

CSCsy08778 no pim on one subif disables eigrp on same physical of

Symptom: eigrp stops working on one subinterface, if "no pim" is issued on another subinterf same physical interface. Conditions: The physical interface belongs to the 4-GE module. If us

Severity: 2 | Status: Fixed | Updated: Nov 09, 2016 | Cases:3 | ☆ ☆ ☆ ☆ ☆

CSCtg52478 PIM nbr jp_buffer can be corrupted under stress

Symptom: memory corruption of pim nbr structure Conditions: multicast w/ PIM-SM and hea

Informações Relacionadas

- Troubleshooting de Multicast ASA e Problemas Comuns

- Multicast do Firepower Management Center
- Resumo dos sinalizadores multicast do Firepower