Solución de problemas de Firepower Threat Defense y ASA Multicast PIM

Contenido

Introducción

Este documento describe cómo Firepower Threat Defence (FTD) y Adaptive Security Appliance (ASA) implementan Protocol Independent Multicast (PIM).

Prerequisites

Requirements

Conocimientos básicos sobre IP Routing.

Componentes Utilizados

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Firepower 4125 Threat Defense Versión 7.1.0.
- Firepower Management Center (FMC) versión 7.1.0.
- Software Cisco Adaptive Security Appliance Versión 9.17(1)9.

Antecedentes

Conceptos básicos del routing multidifusión

- La unidifusión reenvía los paquetes hacia el destino mientras que la **multidifusión** reenvía los paquetes lejos del origen.
- Los dispositivos de red de multidifusión (firewalls/routers, etc.) reenvían los paquetes a través de **Reenvío de ruta inversa (RPF).** Tenga en cuenta que RPF no es lo mismo que uRPF, que se utiliza en unidifusión para evitar tipos específicos de ataques. RPF se puede definir como un mecanismo que reenvía paquetes multicast lejos del origen de las interfaces que conducen hacia los receptores multicast. Su función principal es evitar bucles de tráfico y garantizar rutas de tráfico correctas.
- Un protocolo multicast como PIM tiene 3 funciones principales:

1. Busque la **interfaz ascendente** (interfaz más cercana al origen).

2. Encuentre las **interfaces descendentes** asociadas con un flujo multicast específico (interfaces hacia los receptores).

3. Mantenga el árbol de multidifusión (agregue o quite las ramas del árbol).

- Un árbol de multidifusión se puede crear y mantener mediante uno de los dos métodos: **uniones implícitas (saturación y separación)** o **uniones explícitas (modelo de extracción).** El modo denso de PIM (PIM-DM) utiliza uniones implícitas, mientras que el modo disperso de PIM (PIM-SM) utiliza uniones explícitas.
- Un árbol de multidifusión puede ser **compartido** o **basado en el origen:**
  - Los árboles compartidos utilizan el concepto de **Punto de encuentro (RP)** y se señalan como **(*, G)** donde G = IP de grupo multicast.
  - Los árboles basados en el origen tienen su raíz en el origen, no utilizan un RP y se señalan como **(S, G)** donde S = la IP del origen/servidor de multidifusión.
- Modelos de reenvío de multidifusión:
  - **El** modo de entrega **multidifusión de cualquier origen (ASM)** utiliza árboles compartidos (*, G) donde cualquier origen puede enviar el flujo de multidifusión.
  - **Source-Specific Multicast (SSM)** utiliza árboles basados en el origen (S, G) y el rango de IP 232/8.
  - **Bidireccional (BiDir)** es un tipo de árbol compartido (*, G) donde el tráfico del plano de control y del plano de datos pasa a través del RP.
- Un punto de encuentro se puede configurar o seleccionar con uno de estos métodos:
  - RP estático
  - RP automático
  - Router de arranque (BSR)

resumen de modos PIM

modo PIM	RP	Árbol compartido	Notación	IGMP	Compatible con ASA/FTD
Modo disperso de	Yes	Yes	(*, G) y (S,	v1/v2/v3	Yes

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

*RP automático = el tráfico RP automático puede pasar

** ASA/FTD no puede ser un dispositivo de último salto

resumen de configuración RP

Configuración del punto de encuentro	**ASA/FTD**
RP estático	Yes
RP automático	No, pero el tráfico del plano de control de RP automático puede pasar
BSR	Sí, pero no admite C-RP

Nota: Antes de comenzar a resolver cualquier problema de multidifusión, es muy importante tener una visión clara de la topología de multidifusión. Específicamente, como mínimo, necesita saber:
- ¿Cuál es la función del firewall en la topología de multidifusión?
- ¿Quién es el RP?
- ¿Quién es el remitente del flujo de multidifusión (IP de origen e IP de grupo de multidifusión)?
- ¿Quién es el receptor de la secuencia de multidifusión?
- ¿Tiene problemas con el plano de control (IGMP/PIM) o con el plano de datos (flujo de multidifusión) en sí?

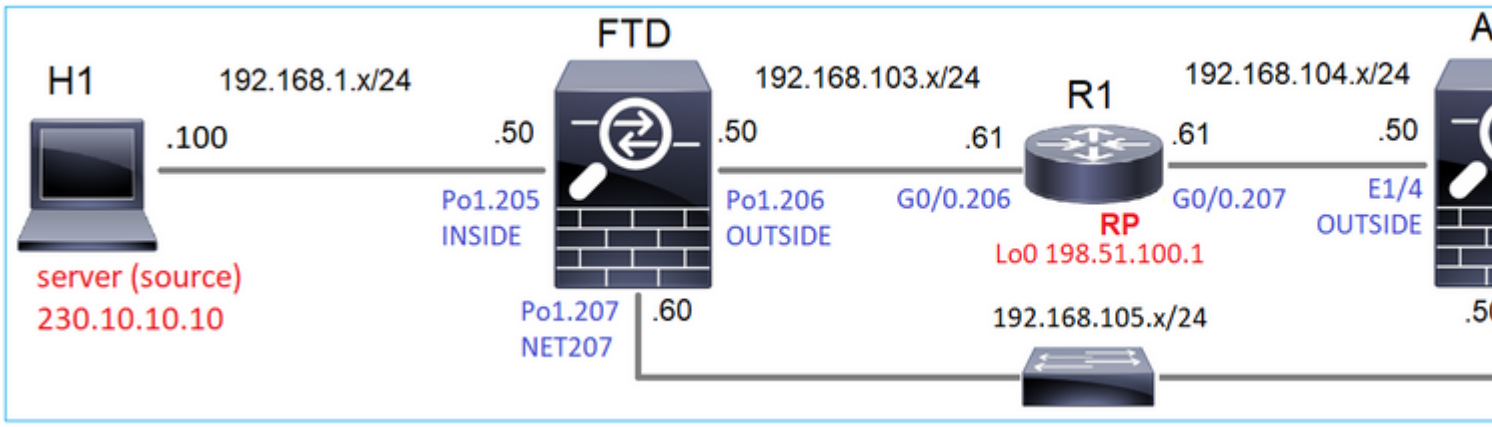
Abreviaturas/acrónimos

Acrónimos	**Explicación**
FHR	Router de primer salto: un salto conectado directamente al origen del

	tráfico de multidifusión.
LHR	Router de último salto: un salto conectado directamente a los receptores del tráfico de multidifusión.
RP	Punto de encuentro
DR.	Router designado
SPT	Árbol de ruta más corta
RPT	Árbol de punto de encuentro (RP), árbol compartido
RPF	Reenvío de Trayectoria Inversa
PETRÓLEO	Lista de interfaces salientes
MRIB	Base de Información de Ruteo Multicast
MFIB	Base de Información de Reenvío Multicast
ASM	Multidifusión de cualquier fuente
BSR	Bootstrap Router
SSM	Multidifusión desde un origen específico
FP	Ruta rápida
SP	Trayecto lento
CP	Punto de control
PPS	Velocidad de paquetes por segundo

Tarea 1: modo disperso de PIM (RP estático)

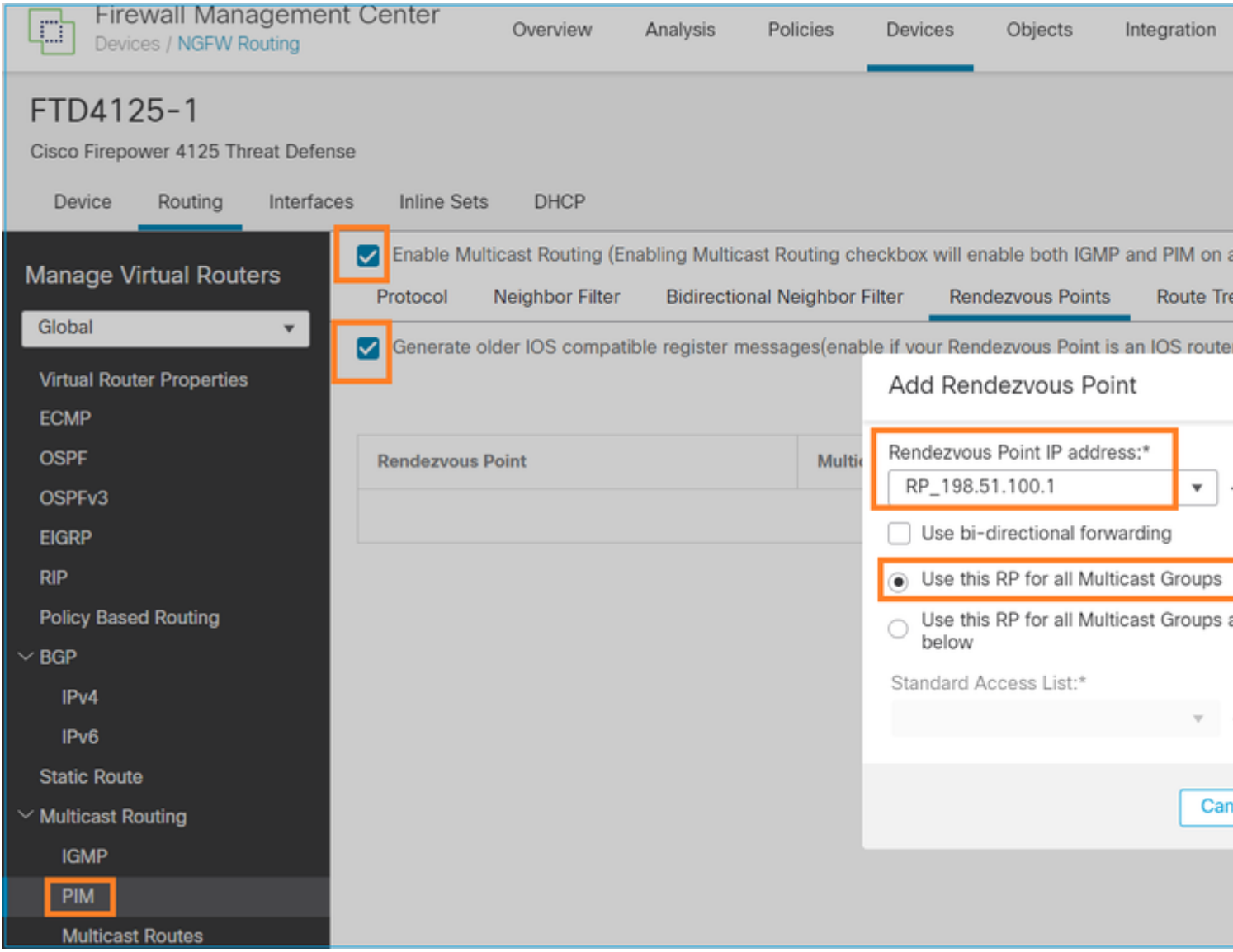
Topología



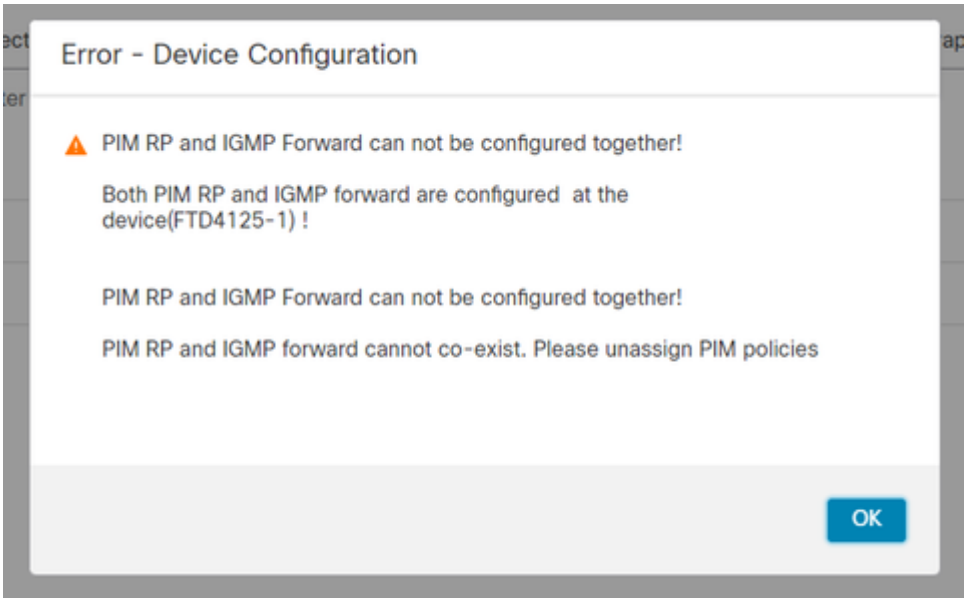
Configure el modo disperso de PIM multicast en la topología con R1 (198.51.100.1) como RP.

Solución

Configuración de FTD:



El ASA/FTD no se puede configurar para IGMP Stub Routing y PIM al mismo tiempo:



La configuración resultante en 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
```

En el firewall ASA hay una configuración similar:

```
<#root>

asa(config)#

multicast-routing


asa(config)#

pim rp-address 198.51.100.1
```

Configuración RP (router de 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
```

Verificación

Verifique el plano de control de multidifusión en FTD cuando no haya tráfico de multidifusión (remitentes o 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 los vecinos 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)
```

El RP anuncia todo el rango del 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
```

La tabla de rutas multicast del firewall tiene algunas entradas no relevantes (239.255.255.250 es el protocolo simple de detección de servicios (SSDP) utilizado por proveedores como MAC OS y 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
```

Hay un túnel PIM construido entre los firewalls y el 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

El túnel PIM también se puede ver en la tabla de conexión del 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

Verificación en el 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

Verificación RP (router de Cisco) RP. Hay algunos grupos multicast para SSDP y Auto-RP:

<#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
```

Verificación una vez que un receptor anuncia su presencia

> **Nota**: los comandos del firewall que se muestran en esta sección son totalmente aplicables a ASA y FTD.

El ASA obtiene el mensaje IGMP Membership Report y crea las entradas IGMP y 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

El firewall ASA crea una ruta multicast para el 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
```

Otra verificación del firewall es la salida de la topología 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
```

> **Nota**: Si el firewall no tiene una ruta hacia el RP, el resultado de **debug pim** muestra una falla de búsqueda de RPF

El error de búsqueda RPF en el resultado de **debug pim**:

```
<#root>
```

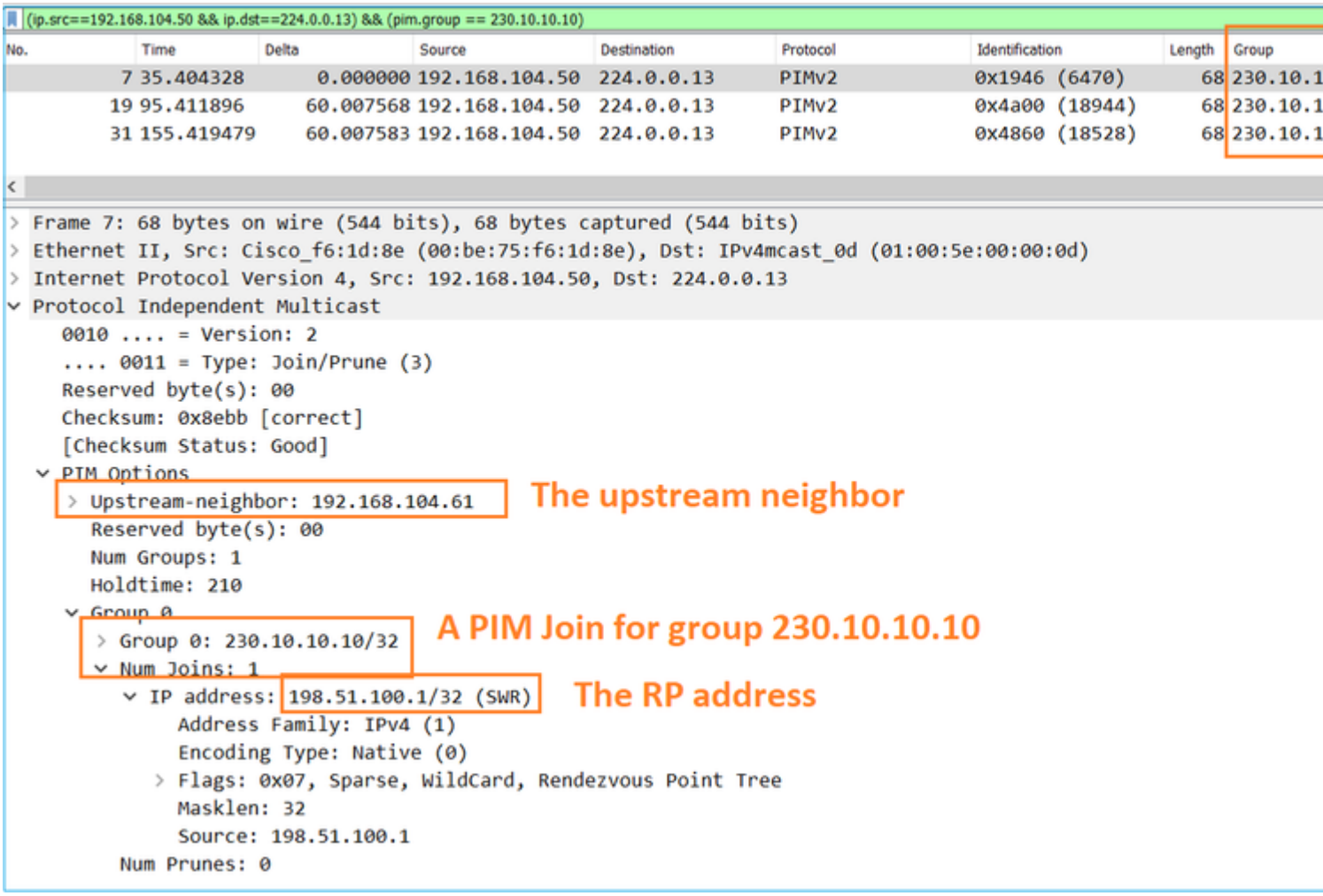
```
asa#
debug pim


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
```

En caso de que todo esté correcto, el firewall envía un mensaje PIM Join-Prune al 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
```

La captura muestra que los mensajes PIM Join se envían cada 1 min y PIM Hellos cada 30 segundos. PIM utiliza IP 224.0.0.13:



Sugerencia: filtro de visualización de Wireshark: (ip.src==192.168.104.50 && ip.dst==224.0.0.13) && (pim.group == 230.10.10.10)
- 192.168.104.50 es la IP de firewall de la interfaz de salida (hacia el vecino PIM ascendente)
- 224.0.0.13 es el grupo de multidifusión PIM al que se envían las porciones y uniones PIM
- 230.10.10.10 es el grupo multicast para el que enviamos el PIM Join/Prune

---

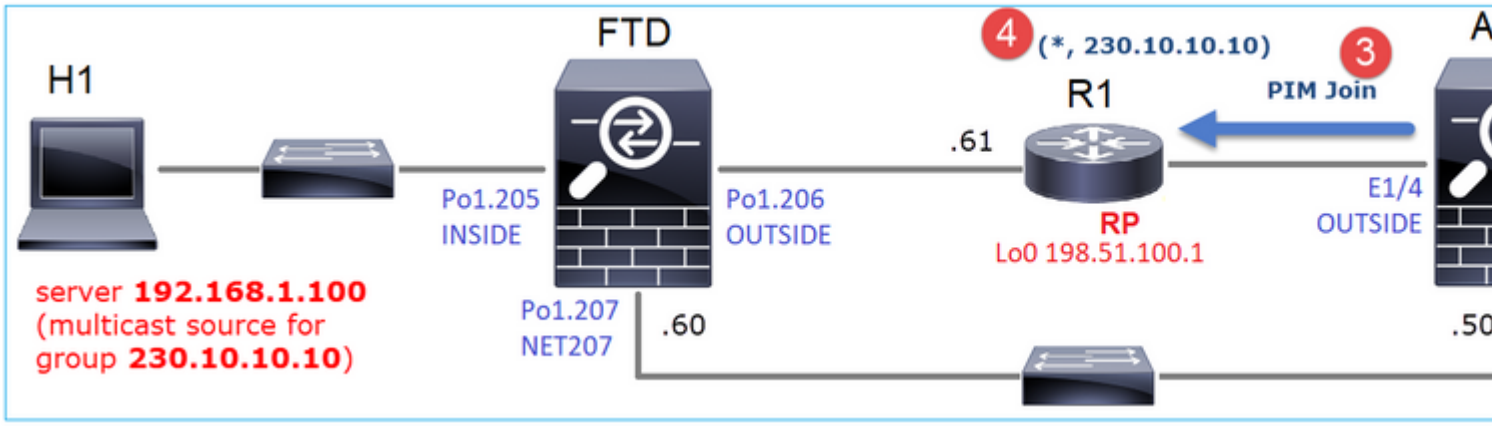
El RP crea una ruta multicast (*, G). Tenga en cuenta que, dado que aún no hay servidores, la interfaz entrante es nula:

<#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
```

Esto se puede visualizar como:



1. El informe IGMP se recibe en ASA.
2. Se agrega una ruta multicast (*, G).
3. El ASA envía un mensaje de unión PIM al RP (198.51.100.1).
4. El RP recibe el mensaje de unión y agrega una ruta multicast (*, G).

Al mismo tiempo, en FTD no hay rutas multicast ya que no se recibió ningún informe IGMP ni se recibió la incorporación PIM:

```
<#root>

firepower#

show mroute 230.10.10.10

No mroute entries found.
```

Verificación cuando el servidor envía una secuencia de multidifusión

El FTD obtiene el flujo multicast de H1 e inicia el **proceso de registro PIM** con el RP. El FTD envía un mensaje de **registro PIM de unidifusión** al RP. El RP envía un mensaje **PIM Join** al router de primer salto (FHR), que es el FTD en este caso, para unirse al árbol de multidifusión. A continuación, envía un mensaje **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**

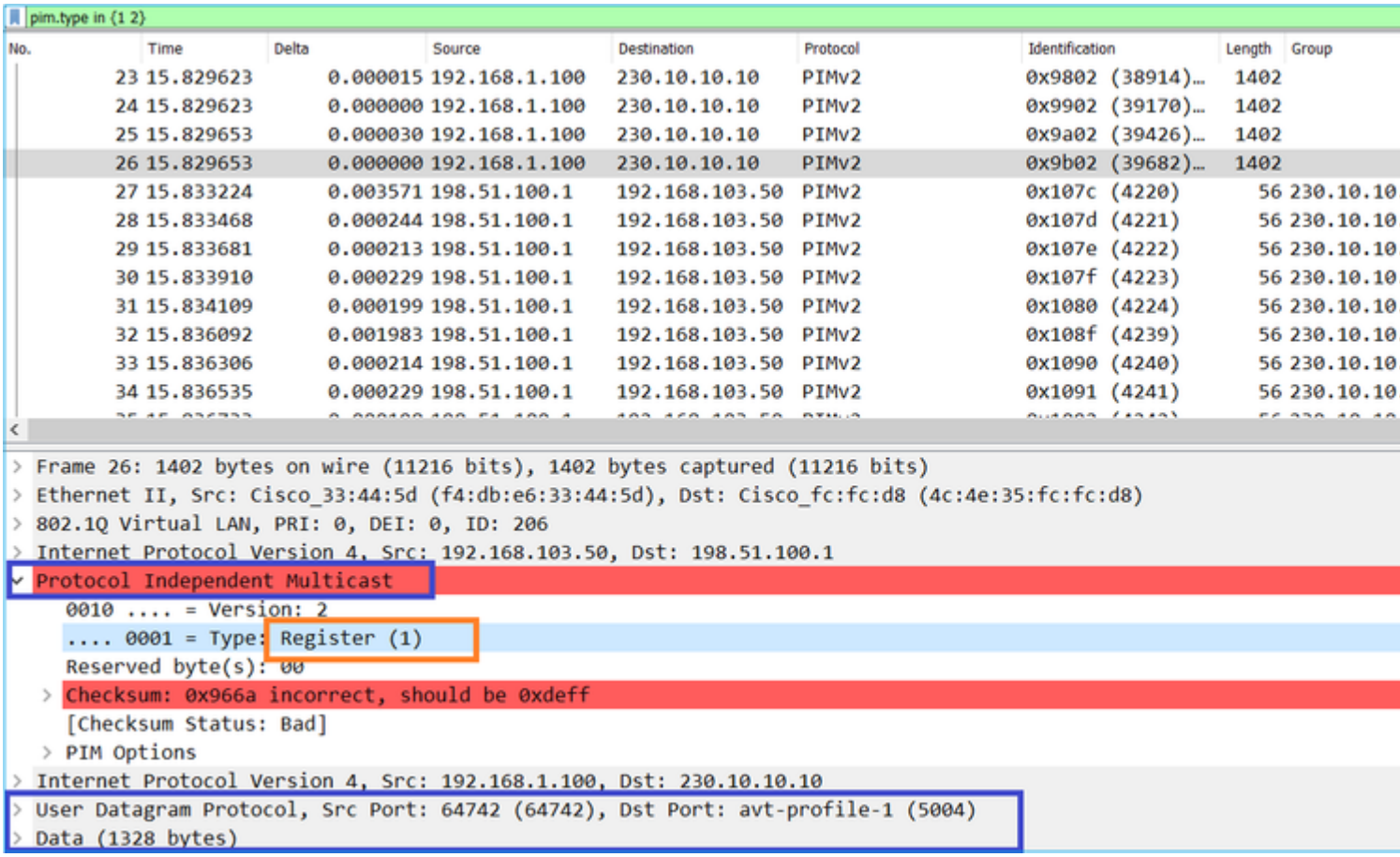
```
IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 J/P state changed from Null to Join
IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 FWD state change from Prune to Forward
IPv4 PIM: (192.168.1.100,230.10.10.10) Updating J/P status from Null to Join
IPv4 PIM: (192.168.1.100,230.10.10.10) J/P scheduled 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**

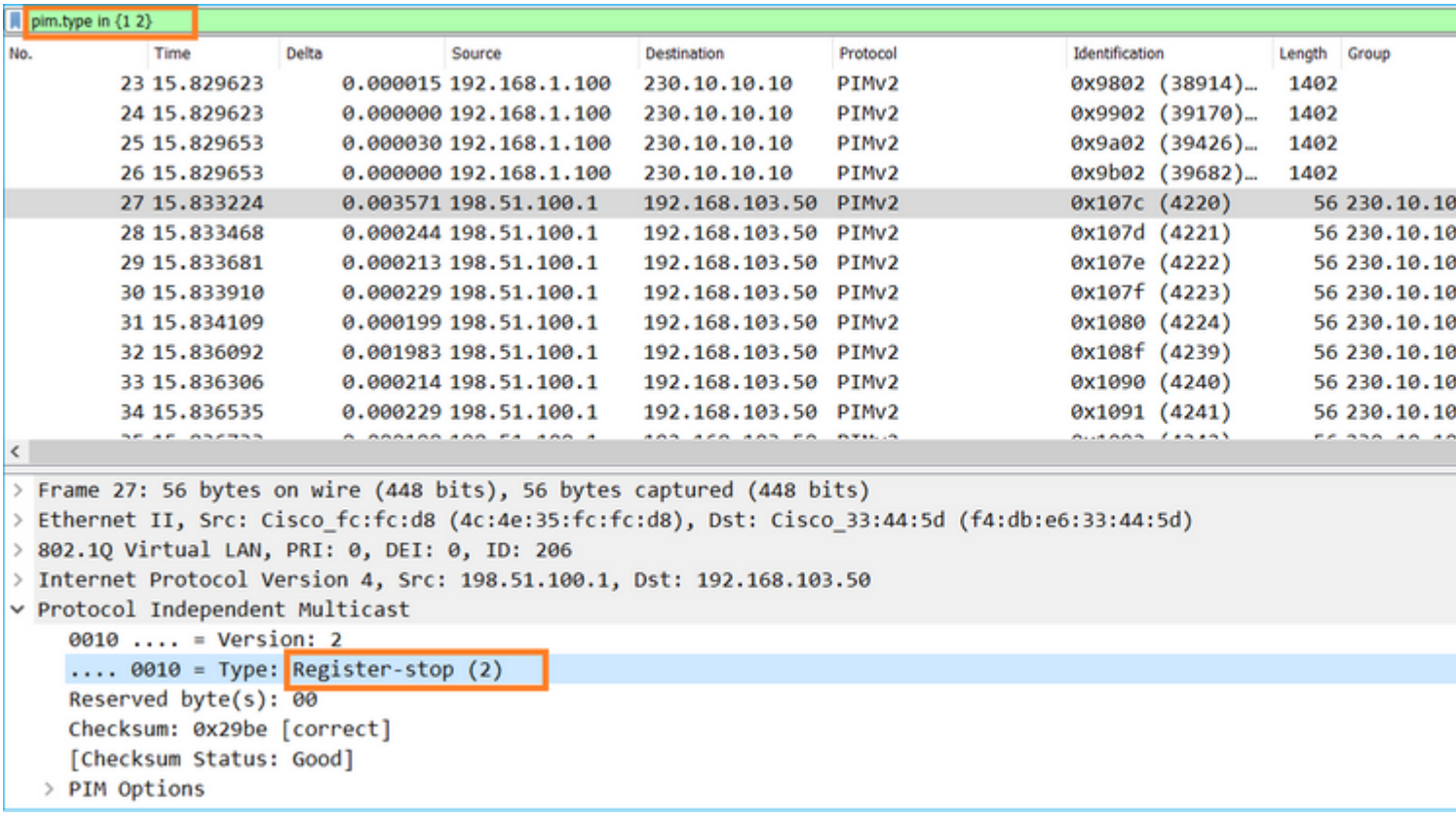
```
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE J/P state changed from Null to Join
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE FWD state change from Prune to Forward
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify F NS
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE Raise J/P 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)
```

El mensaje PIM Register es un mensaje PIM que transporta datos UDP junto con la información de registro PIM:



El mensaje PIM Register-Stop:



Sugerencia: para mostrar sólo los mensajes PIM Register y PIM Register-Stop en Wireshark, puede utilizar el filtro de presentación: pim.type en {1}

El firewall (router de último salto) obtiene la secuencia de multidifusión en la interfaz OUTSIDE e inicia el switchover del árbol de trayecto más corto (SPT) a la interfaz 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)
```

La depuración PIM en el FTD cuando ocurre el 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
```

La ruta multicast de FTD una vez que comienza el switchover SPT:

```
<#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
```

Al final del switchover SPT, solamente la interfaz NET207 se muestra en el 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

En el router de último salto (ASA), el bit SPT también está configurado:

<#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
```

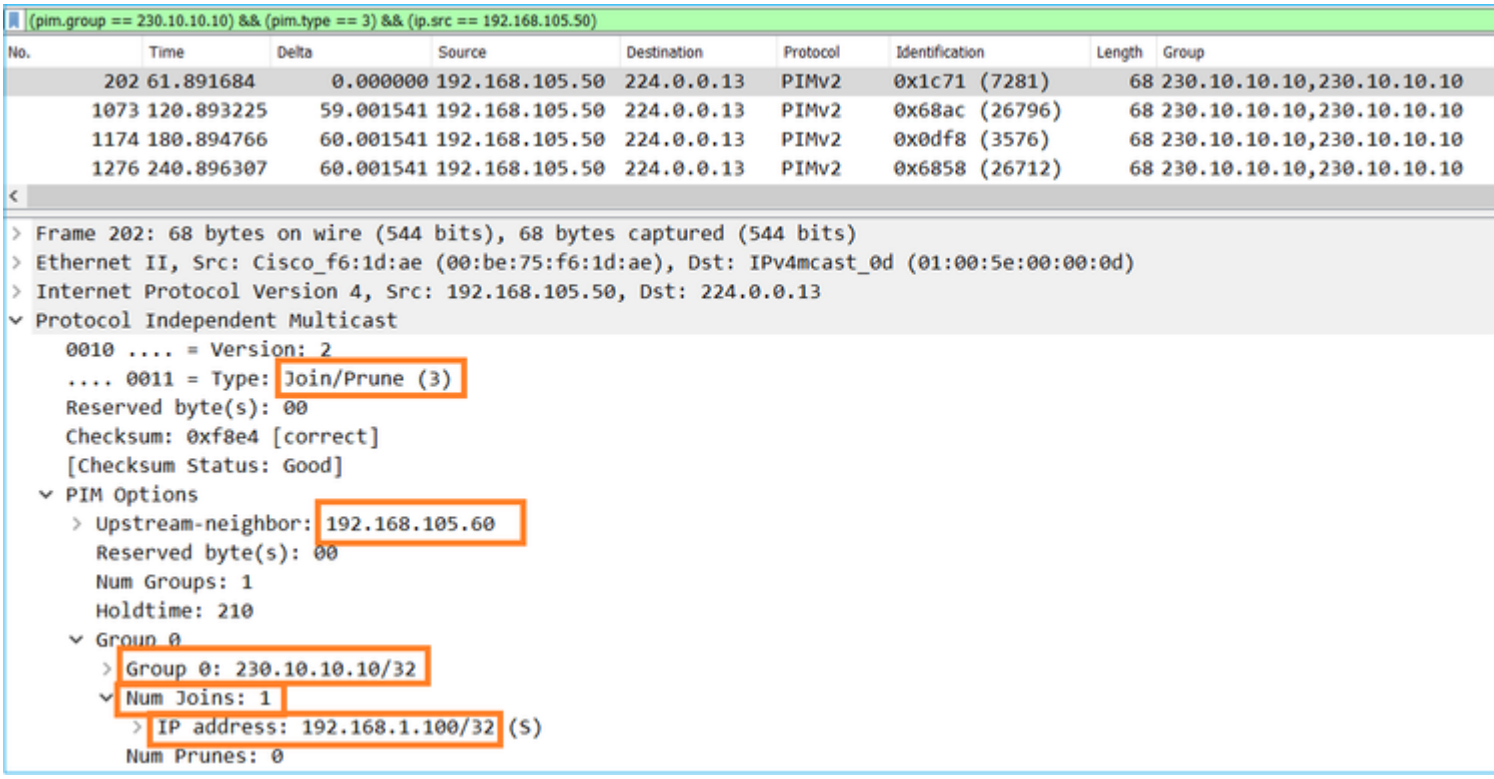
T   <-- SPT switchover for group 230.10.10.10

Incoming interface:

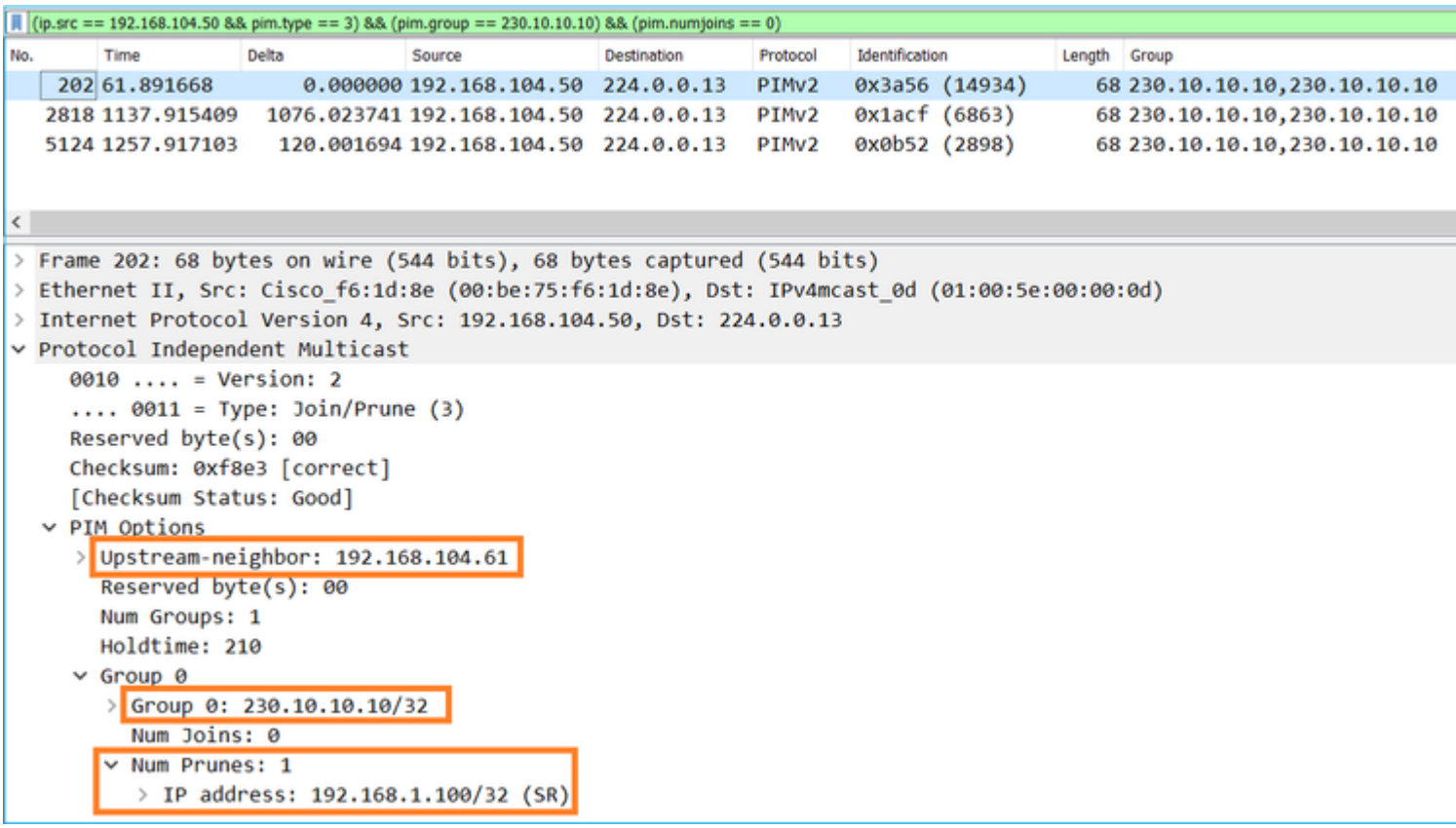
NET207   <-- The multicast packets arrive on interface NET207

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

El switchover de la interfaz ASA NET207 (el router de primer salto que realizó el switchover). Se envía un mensaje de incorporación de PIM al dispositivo ascendente (FTD):



En la interfaz OUTSIDE se envía un mensaje PIM Prune al RP para detener el flujo de multidifusión:



Verificación del tráfico 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 el número de paquetes manejados en Slow Path vs Fast Path vs Control Point:

<#root>

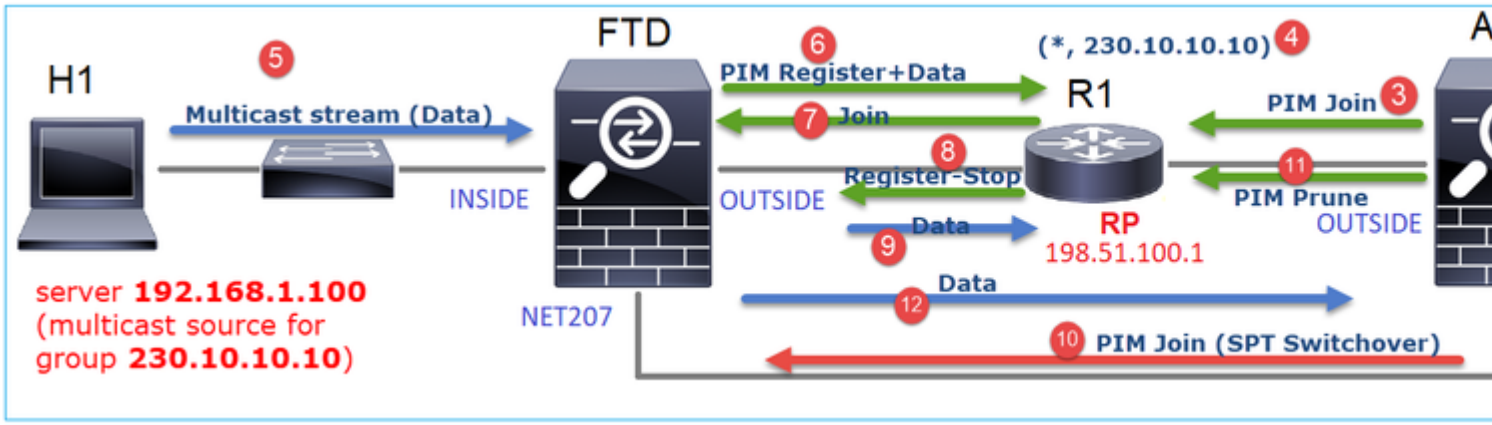
firepower#

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
```

Un diagrama que muestra lo que sucede paso a paso:



1. El host final (H2) envía un informe IGMP para unirse a la secuencia de multidifusión 230.10.10.10.
2. El router de último salto (ASA) que es PIM DR crea una entrada (*, 230.10.10.10).
3. El ASA envía un mensaje PIM Join hacia el RP para el grupo 230.10.10.10.
4. El RP crea la entrada (*, 230.10.10.10).
5. El servidor envía los datos de la secuencia de multidifusión.
6. El FTD encapsula los paquetes multicast en los mensajes de registro PIM y los envía (unidifusión) al RP. En este punto, el RP ve que tiene un receptor activo, desencapsula los paquetes multicast y los envía al receptor.
7. El RP envía un mensaje de unión de PIM al FTD para unirse al árbol de multidifusión.
8. El RP envía un mensaje PIM Register-Stop al FTD.
9. El FTD envía un flujo de multidifusión nativo (sin encapsulación PIM) hacia el RP.
10. El router de último salto (ASA) ve que el origen (192.168.1.100) tiene una mejor trayectoria desde la interfaz NET207 e inicia un switchover. Envía un mensaje de incorporación de PIM al dispositivo ascendente (FTD).
11. El router de último salto envía un mensaje PIM Prune al RP.
12. El FTD reenvía el flujo multicast hacia la interfaz NET207. ASA se desplaza del árbol compartido (árbol RP) al árbol de origen (SPT).

Tarea 2: Configuración del router de arranque PIM (BSR)

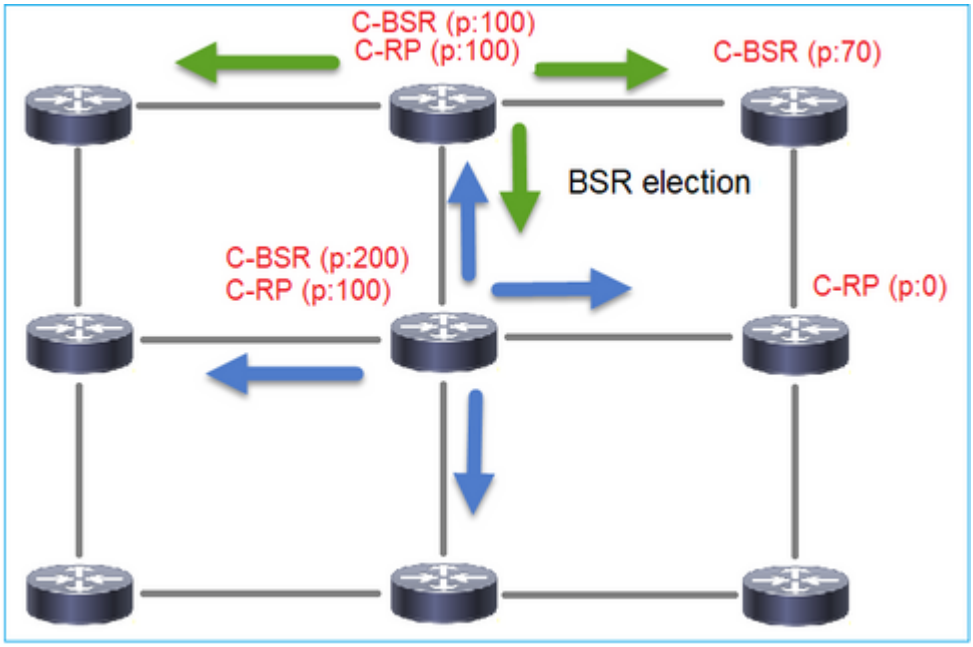
Conceptos básicos de BSR

- BSR (RFC 5059) es un mecanismo de multidifusión del plano de control que utiliza el protocolo PIM y permite a los dispositivos aprender la información RP dinámicamente.
- Definiciones de BSR:
  - RP candidato (C-RP): dispositivo que desea ser RP.
  - BSR candidato (C-BSR): dispositivo que desea ser BSR y anuncia conjuntos RP a otros dispositivos.
  - BSR: dispositivo que se elige como BSR entre muchos C-BSR. La **prioridad más alta de BSR gana** la elección.
  - RP-set: Una lista de todos los C-RPs y sus prioridades.
  - RP: El dispositivo con la **prioridad RP más baja gana** la elección.
  - Mensaje PIM de BSR (vacío): mensaje PIM utilizado en la elección de BSR.
  - Mensaje PIM de BSR (normal): mensaje PIM enviado a 224.0.0.13 IP y que contiene un conjunto RP e información BSR.

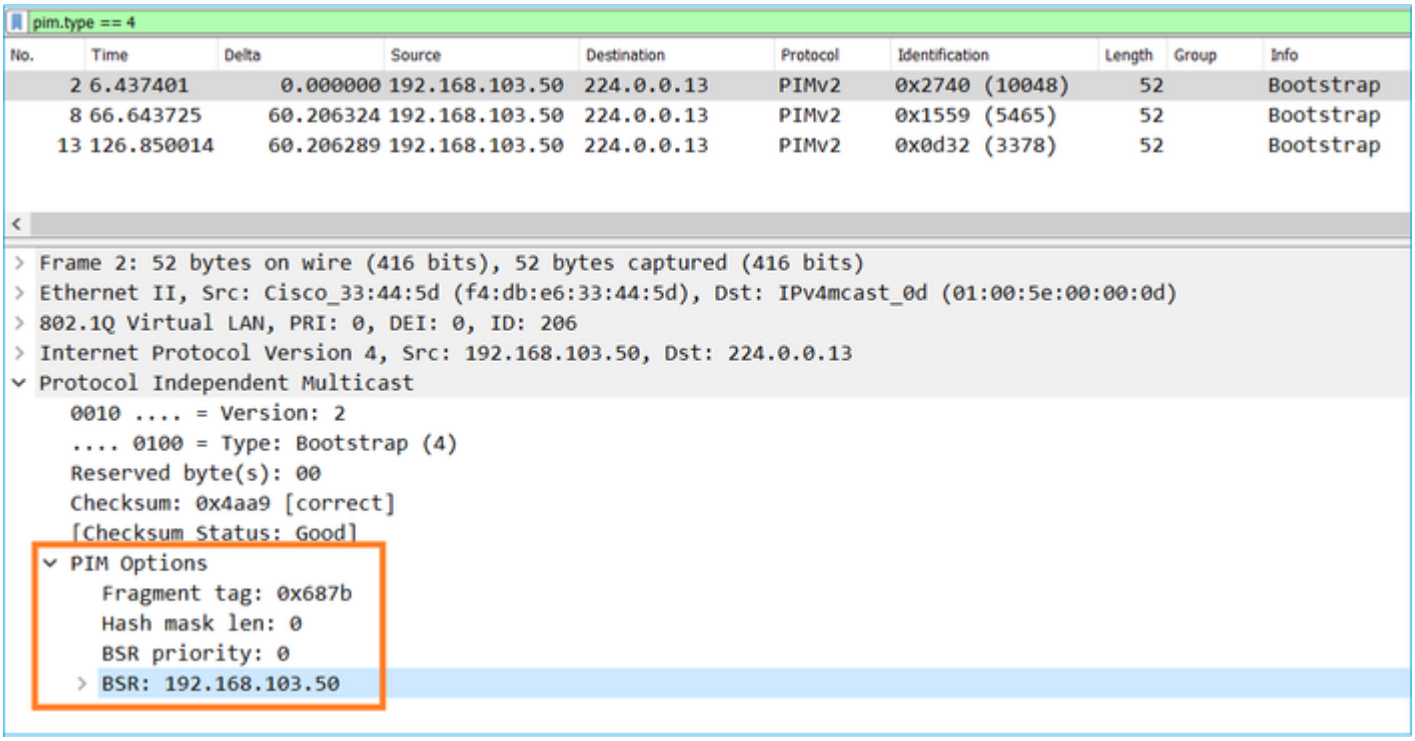
Cómo funciona BSR

1. Mecanismo de elección del BSR.

Cada C-BSR envía mensajes vacíos de PIM BSR que contienen una prioridad. El dispositivo con la prioridad más alta (el recurso alternativo es la IP más alta) gana la elección y se convierte en el BSR. El resto de los dispositivos no envían más mensajes BSR vacíos.

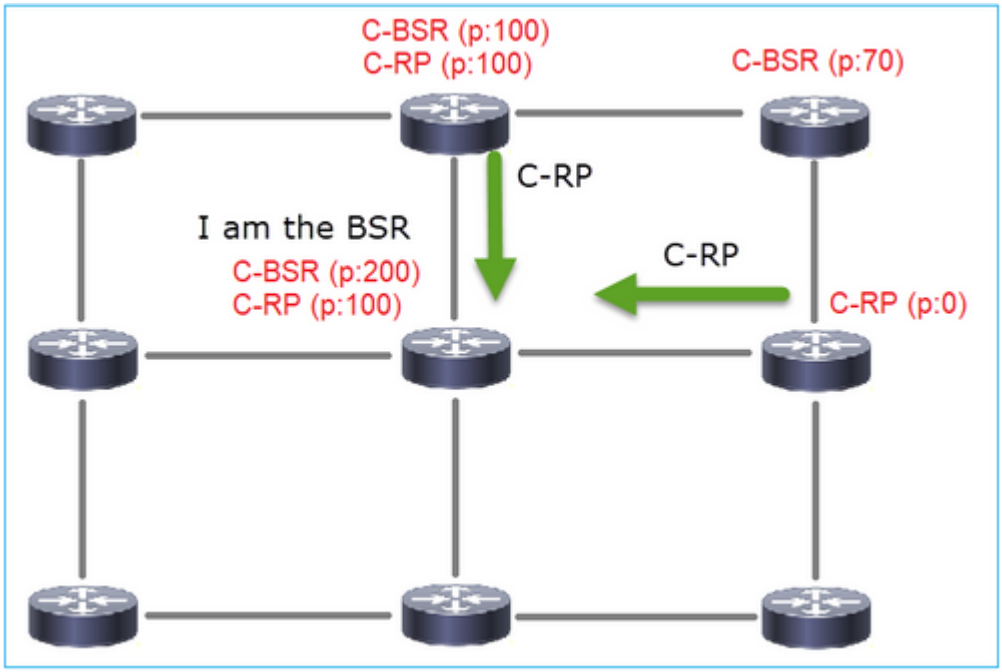


Un mensaje BSR utilizado en el proceso de elección contiene sólo información de prioridad de C-BSR:



Para mostrar mensajes BSR en Wireshark, utilice este filtro de visualización: pim.type == 4

2. Los C-RP envían mensajes BSR de **unidifusión** al BSR que contienen su prioridad C-RP:



Un mensaje RP candidato:

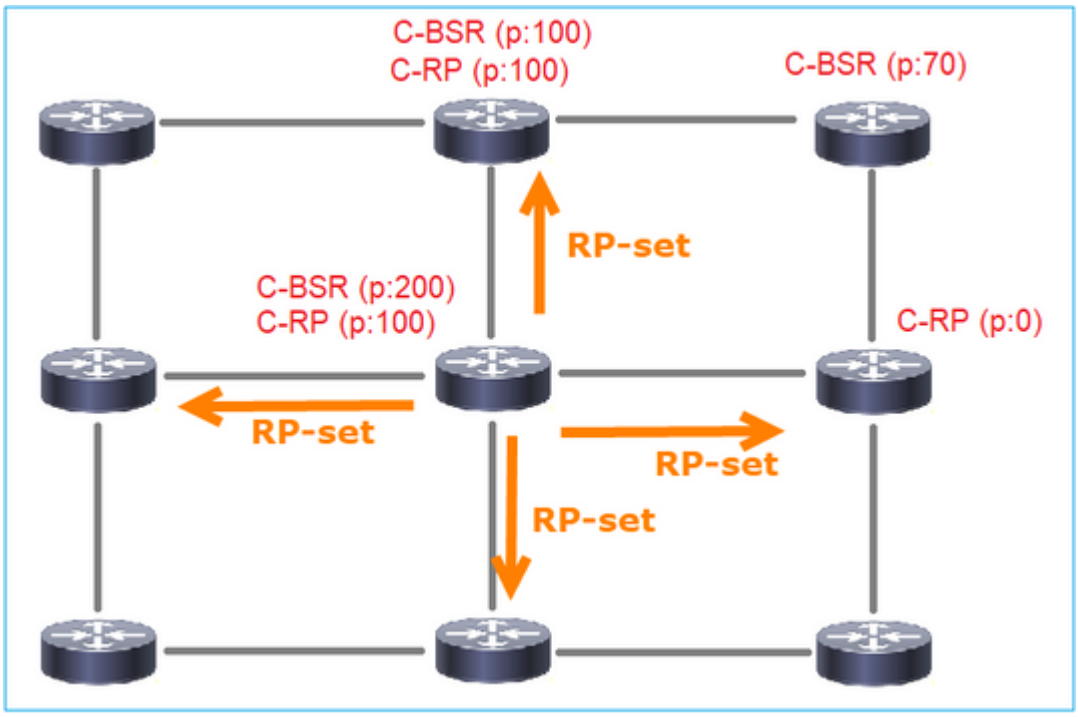
pim.type == 8

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 mostrar mensajes BSR en Wireshark, utilice este filtro de visualización: pim.type == 8

3. El BSR compone el conjunto RP y lo anuncia a todos los vecinos PIM:

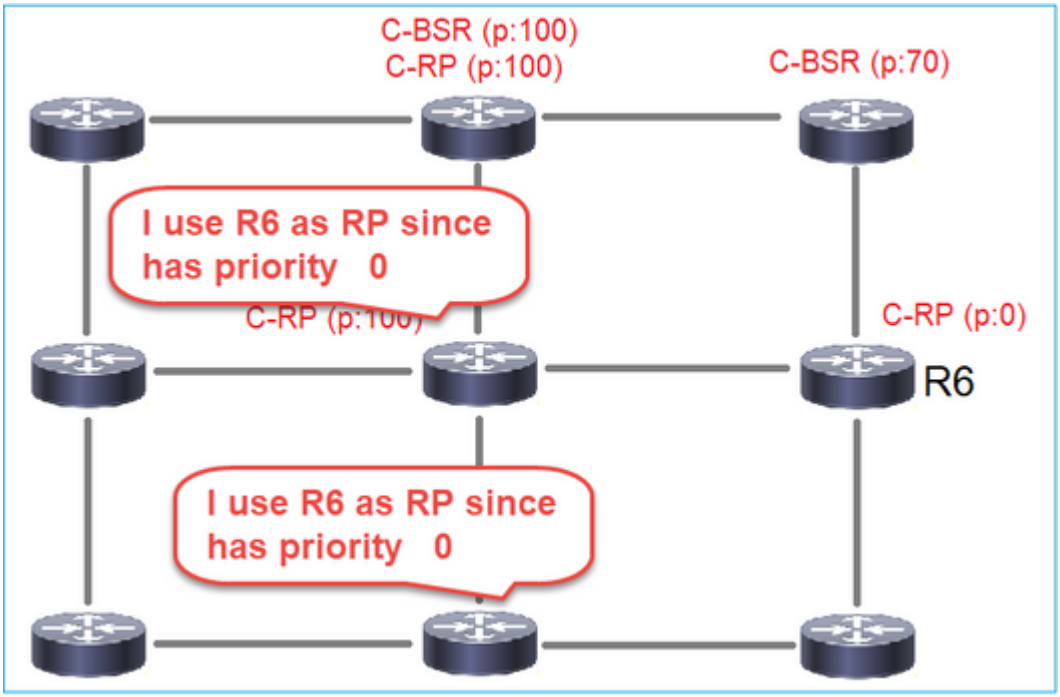


(ip.src == 192.168.105.60) && (pim.type == 4)

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

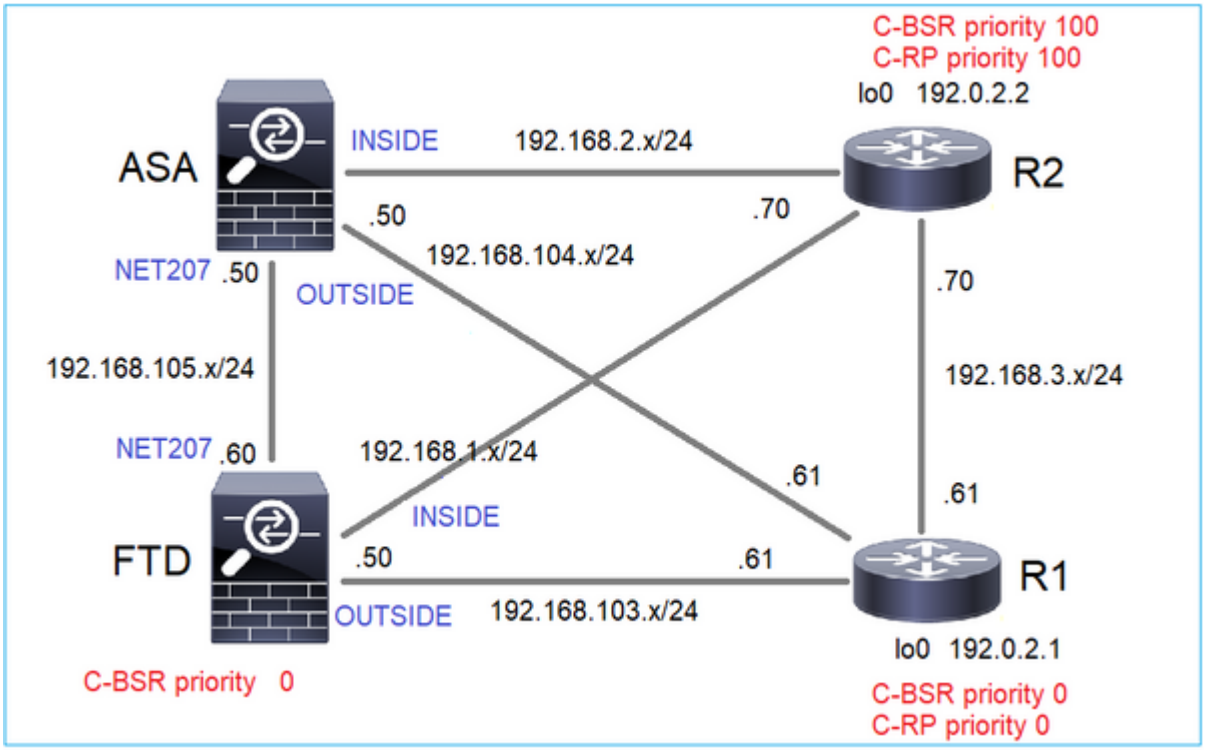
```
> Frame 152: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
> Ethernet II, Src: Cisco_33:44:5d (f4:db:e6:33:44:5d), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
> 802.1Q Virtual LAN, PRI: 6, DEI: 0, ID: 207
> Internet Protocol Version 4, Src: 192.168.105.60, Dst: 224.0.0.13
v Protocol Independent 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. Los routers/firewalls obtienen el conjunto RP y seleccionan el RP en función de la prioridad más baja:



Tarea requerida

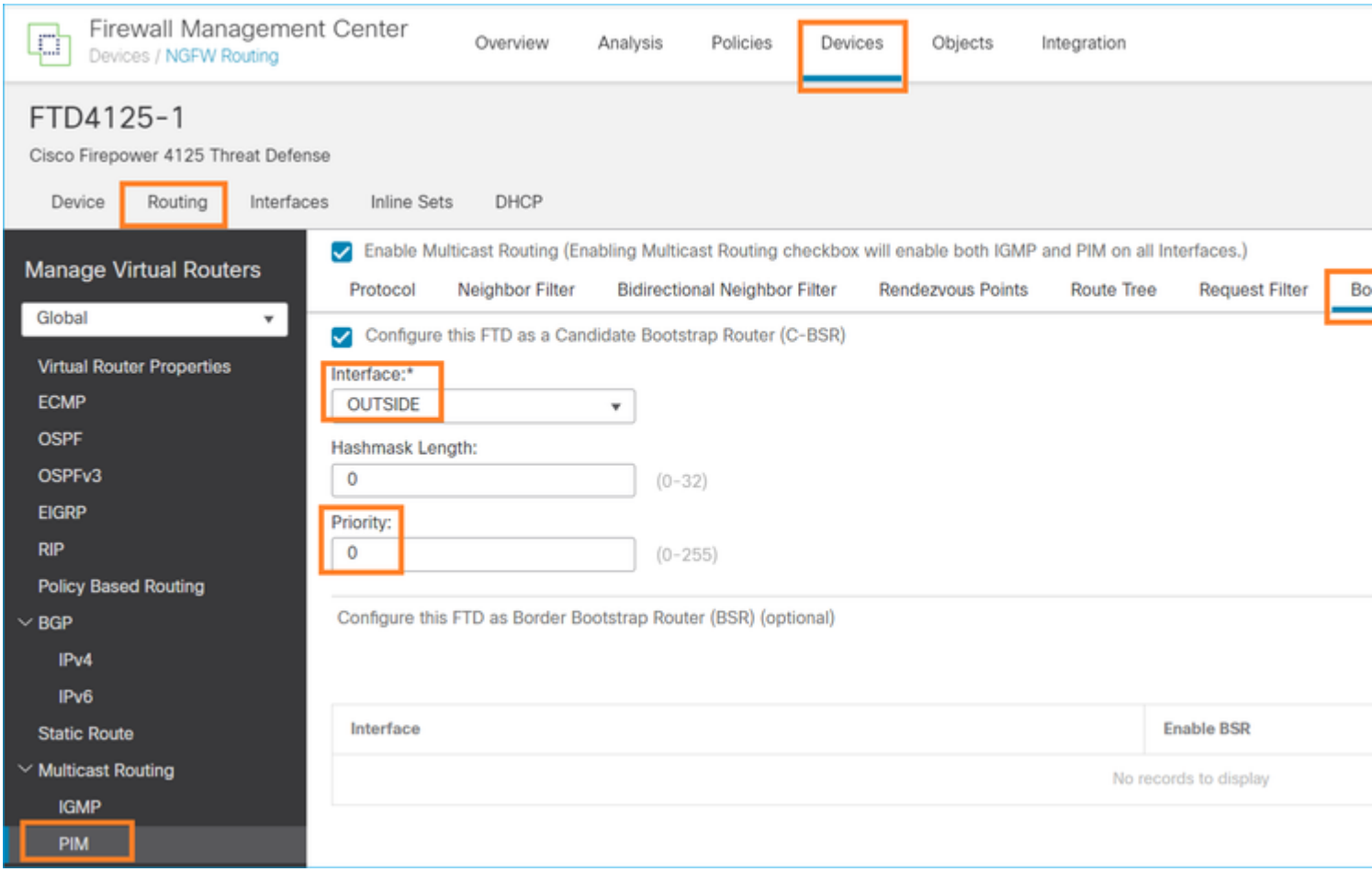
Configure los C-BSR y C-RP según esta topología:



para esta tarea, el FTD debe anunciarse como C-BSR en la interfaz OUTSIDE con prioridad BSR 0.

Solución

Configuración de FMC para FTD:



La configuración implementada:

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

Configuración en los otros 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)
```

Igual en R2, pero con prioridades C-BSR y C-RP diferentes

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

En ASA, la multidifusión está habilitada globalmente. Esto habilita el PIM en todas las interfaces:

```
multicast-routing
```

Verificación

R2 es el BSR elegido debido a la prioridad más 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 se elige como RP debido a la prioridad más baja:

```
<#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
```

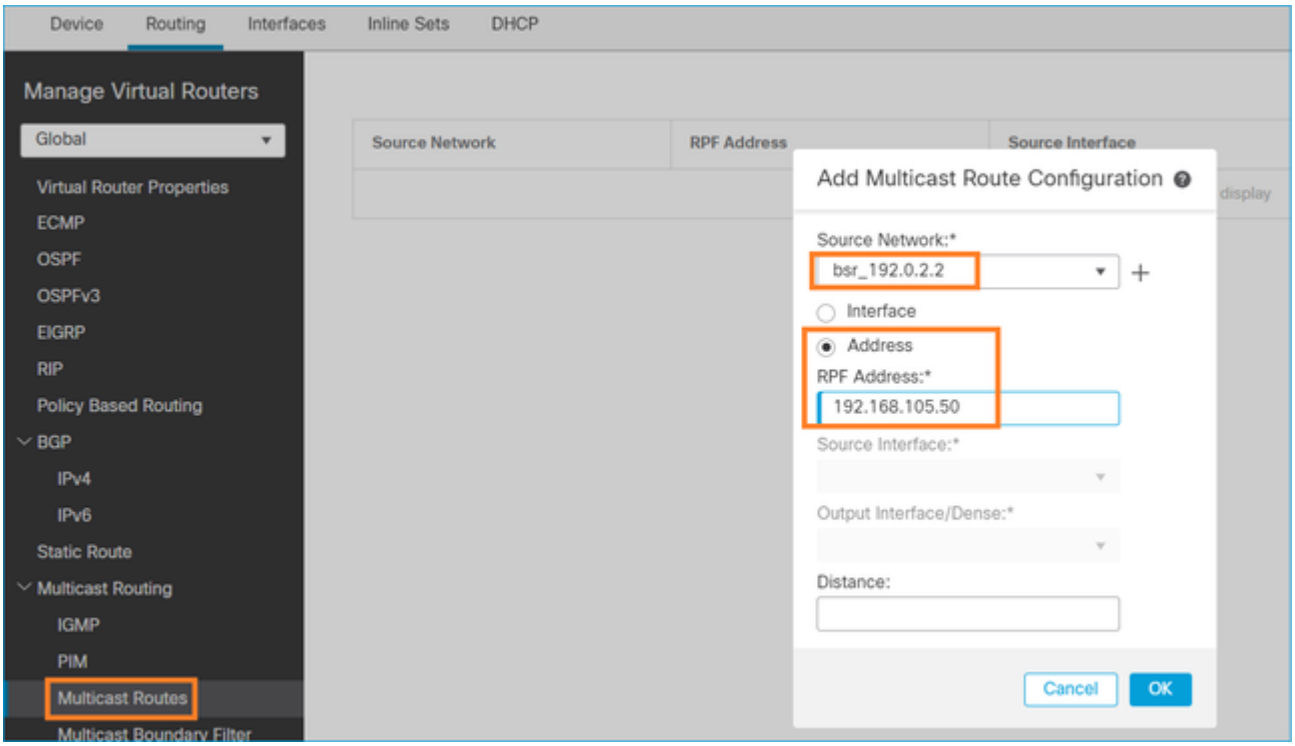
```
224.0.0.0/4

*

       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
```

Los mensajes BSR **están sujetos a la verificación RPF**. Puede habilitar **debug pim bsr** para verificar esto:

<#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
```

Si desea cambiar la interfaz RPF, puede configurar una ruta multicast estática. En este ejemplo, el firewall acepta mensajes BSR de IP 192.168.105.50:



<#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

Ahora se aceptan los mensajes BSR en la interfaz NET207, pero en INSIDE se descartan:

<#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

Habilite la captura con seguimiento en el firewall y verifique cómo se procesan los mensajes BSR:

<#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
```

Las conexiones PIM se terminan en el firewall, por lo que para que el seguimiento muestre información útil, es necesario borrar las conexiones al cuadro:

<#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
```

Si el paquete PIM se descarta debido a una falla de RPF, el seguimiento muestra:

```
<#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

La tabla ASP descarta y captura los paquetes con error 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 paquetes que se descartan debido a una falla 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
```

Metodología de Troubleshooting

La metodología de solución de problemas para el firewall depende principalmente de la función del firewall en la topología de multidifusión. Esta es la lista de pasos recomendados para la resolución de problemas:

1. Aclare los detalles de la descripción del problema y los síntomas. Intente reducir el alcance a los problemas del **plano de control (IGMP/PIM)** o del **plano de datos (secuencia de multidifusión)**.
2. El requisito obligatorio para solucionar problemas de multidifusión en el firewall es aclarar la topología de multidifusión. Como mínimo, debe identificar lo siguiente:
    - función del firewall en la topología de multidifusión: FHR, LHR, RP u otra función intermedia.
    - interfaces de entrada y salida de multidifusión esperadas en el firewall.
    - RP.
    - direcciones IP de origen del remitente.
    - grupos de multidifusión, direcciones IP y puertos de destino.
    - receptores de la secuencia de multidifusión.

3. Identifique el tipo de ruteo multicast - **Stub o PIM multicast routing:**

- **Routing de multidifusión Stub:** proporciona un registro de host dinámico y facilita el routing de multidifusión. Cuando se configura para el ruteo de multidifusión stub, el ASA actúa como un agente proxy IGMP. En lugar de participar completamente en el ruteo multicast, el ASA reenvía los mensajes IGMP a un router multicast ascendente, que configura la entrega de los datos multicast. Para identificar el ruteo del modo stub, utilice el comando **show igmp interface** y verifique la configuración de IGMP forward:

<#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)
```

PIM está habilitado en las interfaces; sin embargo, la vecindad no se establece:

<#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.
```

El reenvío de PIM-SM/Bidir e IGMP **no** se soporta simultáneamente.

No puede configurar opciones como la dirección RP:

<#root>

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

- **Routing de multidifusión PIM**: **el routing de multidifusión PIM es la implementación más común.** El firewall admite PIM-SM y PIM bidireccional. PIM-SM es un protocolo de routing multidifusión que utiliza la base de información de routing unidifusión subyacente o una base de información de routing con capacidad multidifusión independiente. Genera un árbol compartido unidireccional con raíz en un único punto de encuentro (RP) por grupo de multidifusión y, opcionalmente, crea árboles de ruta más corta por origen de multidifusión. En este modo de implementación, a diferencia del modo stub, los usuarios suelen configurar la configuración de la dirección RP y el firewall establece adyacencias PIM con los pares:

<#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 que la dirección IP del RP esté configurada y sea accesible:

```
<#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
```

Advertencia: el firewall no puede ser simultáneamente un **RP** y un **FHR**.

---

5. Comprobar salidas adicionales en función de la función del firewall en la topología de multidifusión y los síntomas del problema.

FHR

- Verifique el estado de la interfaz **Tunnel0**. Esta interfaz se utiliza para encapsular el tráfico multicast sin procesar dentro de la carga útil PIM y enviar el paquete unicast al RP para con el conjunto de bits de registro 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            10.10.10.1       192.168.2.2
```

- Comprobar rutas multicast:

<#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.
```

Cuando el firewall recibe el paquete PIM con el bit Register-Stop, Tunnel0 se elimina del OIL. A continuación, el firewall detiene la encapsulación y envía el tráfico de multidifusión sin procesar a través de la interfaz de salida:

<#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

- Verifique los 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 las capturas de paquetes PIM de unidifusión entre el firewall y el 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
```

- Recopile salidas adicionales (x.x.x.x es el grupo multicast, y.y.y.y es la IP RP). Se recomienda recopilar los resultados **varias veces**:

<#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

- Recopile paquetes de interfaz de multidifusión sin procesar y capturas de caídas de 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
```

- Mensajes de registro del sistema: los ID comunes son 302015, 302016 y 710005.

RP

- Verifique el estado del túnel0 de la interfaz. Esta interfaz se utiliza para encapsular el tráfico multicast sin procesar dentro de la carga útil de PIM y enviar el paquete de unidifusión a FHR para con el conjunto de bits PIM-stop:

```
<#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        -
```

- Comprobar rutas multicast:

```
<#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
```

- Compruebe los contadores de 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
```

- Recopile salidas adicionales (x.x.x.x es el grupo multicast, y.y.y.y es la IP RP). Se recomienda recopilar los resultados **varias veces**:

<#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
```

- Recopile paquetes de interfaz de multidifusión sin procesar y capturas de caídas de 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: los ID comunes son 302015, 302016 y 710005.

LHR

Considere los pasos mencionados en la sección para el RP y estas comprobaciones adicionales:

- 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
```

- Estadísticas de tráfico 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 solución de problemas de PIM (hoja de referencia)

Comando	**Descripción**
show running-config multicast-routing	Para ver si el enrutamiento de multidifusión está habilitado en el firewall
show run mroute	Para ver las rutas multicast estáticas configuradas en el firewall
show running-config pim	Para ver la configuración de PIM en el firewall
show pim interface	Para ver qué interfaces de firewall tienen habilitado PIM y los vecinos PIM.
show pim neighbor	Para ver los vecinos PIM
show pim group-map	Para ver los grupos de multidifusión asignados al RP
show mroute	Para ver la tabla de enrutamiento de multidifusión completa
show mroute 230.10.10.10	Para ver la tabla de multidifusión de un grupo de multidifusión específico
show pim tunnel	Para ver si hay un túnel PIM construido entre el firewall y el RP

show conn all detail address RP_IP_ADDRESS	Para ver si hay una conexión (túnel PIM) establecida entre el firewall y el RP
show pim topology	Para ver el resultado de la topología PIM del firewall
debug pim	Esta depuración muestra todos los mensajes PIM desde y hacia el firewall
debug pim group 230.10.10.10	Esta depuración muestra todos los mensajes PIM desde y hacia el firewall para el grupo multicast específico
show pim traffic	Para ver estadísticas sobre mensajes PIM recibidos y enviados
show asp cluster counter	Para verificar el número de paquetes manejados en la ruta lenta frente a la ruta rápida frente al punto de control
show asp drop	Para ver todas las caídas de nivel de software en el firewall
capture CAP interface INSIDE trace match pim any any	Para capturar y rastrear los paquetes de multidifusión PIM de entrada en el firewall
capture CAP interface INSIDE trace match udp host 224.1.2.3 any	Para capturar y rastrear el flujo de multidifusión de entrada
show pim bsr-router	Para verificar quién es el router BSR seleccionado
show conn all address 224.1.2.3	Para mostrar la conexión de multidifusión principal
show local-host 224.1.2.3	Para mostrar las conexiones de multidifusión secundarias/stub

Para obtener más información sobre capturas de firewall, consulte: Trabaje con capturas de Firepower Threat Defence y Packet Tracer

Problemas conocidos

Limitaciones de multidifusión de Firepower:

- No admite IPv6.

- La multidifusión PIM/IGMP no se admite en las interfaces de una zona de tráfico (EMCP).
- El firewall no puede ser simultáneamente un RP y un FHR.
- El comando **show conn all** muestra solamente las conexiones multicast de identidad. Para mostrar la conexión stub/secondary multicast, utilice el comando **show local-host <*group IP*>**.

PIM no es compatible con vPC Nexus

Si intenta implementar una adyacencia PIM entre un vPC Nexus y el firewall, existe una limitación de Nexus, como se describe a continuación:

Topologías admitidas para el routing por canal de puertos virtuales en plataformas Nexus

Desde el punto de vista de NGFW, puede ver en la captura con seguimiento esta caída:

<#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

El firewall no puede completar el registro RP:

<#root>

```
firepower#
```

show mroute 224.1.2.3

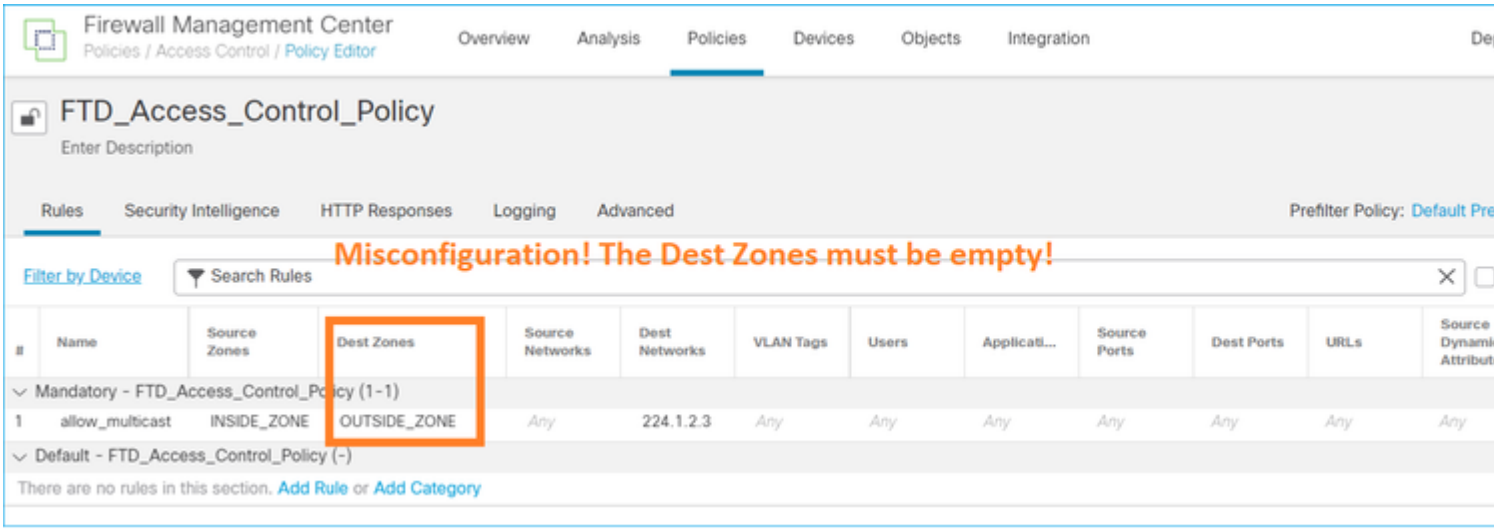
```
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface,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

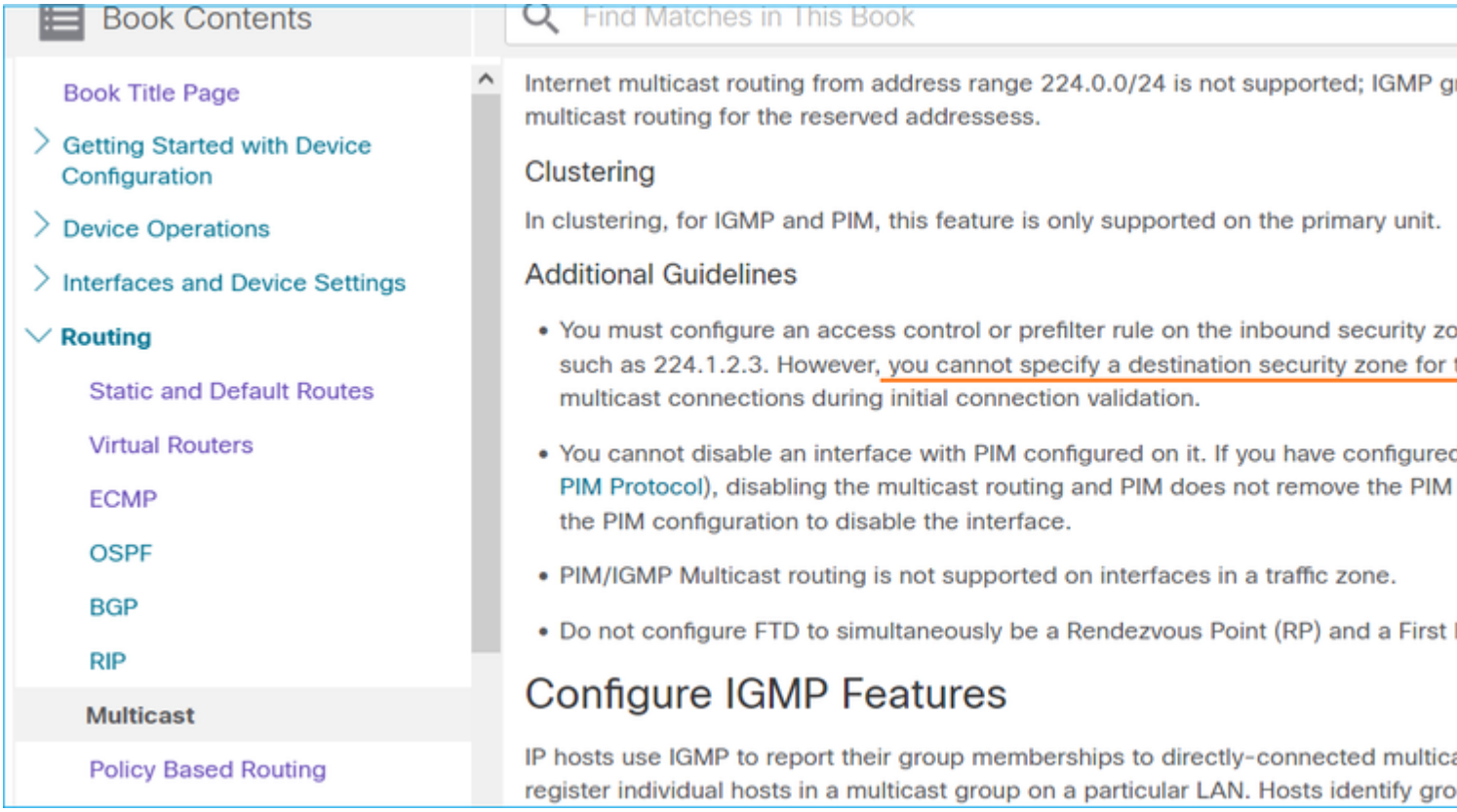
```
  Immediate Outgoing interface list:
    Tunnel0, Forward, 00:39:15/never
```

No se admiten zonas de destino

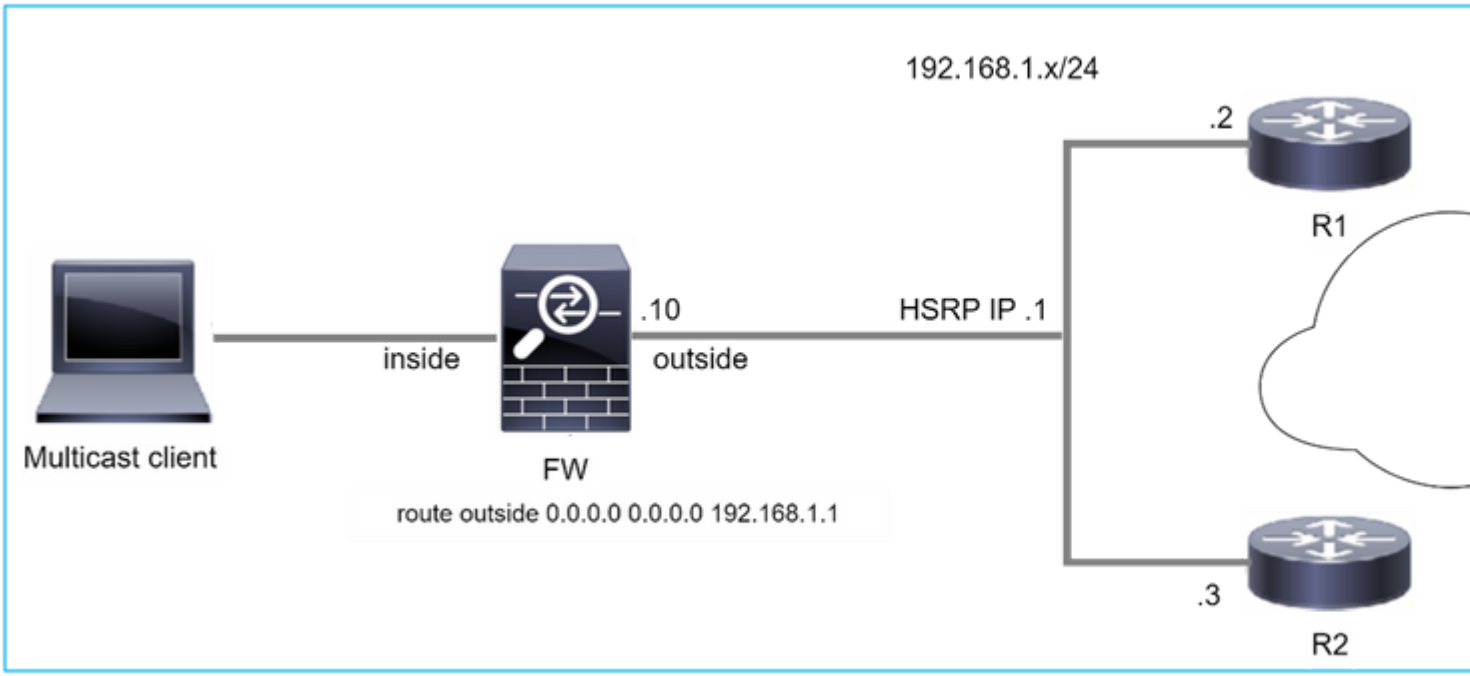
No puede especificar una zona de seguridad de destino para la regla de directiva de control de acceso que coincida con el tráfico de multidifusión:



Esto también se documenta en la guía del usuario de FMC:



El firewall no envía mensajes PIM hacia los routers ascendentes debido a HSRP



En este caso, el firewall tiene una ruta predeterminada a través de la IP 192.168.1.1 del Protocolo de redundancia en espera en caliente (HSRP) y la vecindad PIM con los routers R1 y R2:

```
<#root>

firepower#

show run route

route outside 0.0.0.0 0.0.0.0 192.168.1.1 1
```

El firewall tiene adyacencia PIM entre la IP externa y la interfaz física en R1 y 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)
```

El firewall no envía el mensaje de incorporación de PIM a la red ascendente. El comando de depuración PIM **debug pim** muestra este resultado:

```
<#root>

firepower#

debug pim
```

```
...

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

RFC 2362 establece que *"un router envía un mensaje periódico de unión/separación a cada vecino RPF distinto asociado con cada entrada (S,G), (*,G) y (*,*,RP). Los mensajes Join/Prune se envían solamente si el vecino RPF es un vecino PIM."*

Para mitigar el problema, el usuario puede agregar una entrada de ruta multicast estática en el firewall. El router debe apuntar a una de las dos direcciones IP de interfaz del router, 192.168.1.2 o 192.168.1.3, normalmente la IP del router HSRP activo.

Ejemplo:

<#root>

```
firepower#
```

`show run mroute`

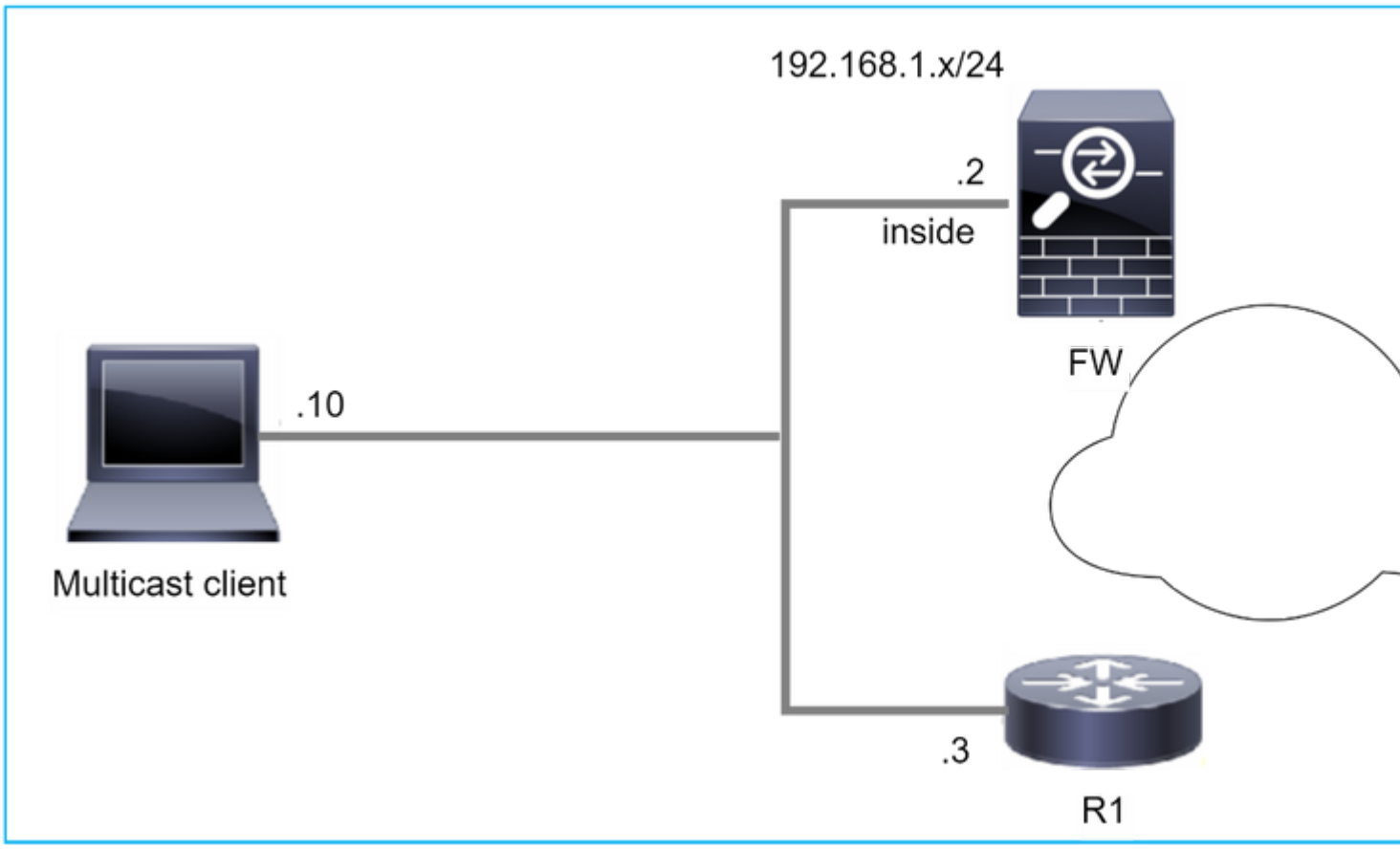
```
firepower#
```

`mroute 172.16.1.1 255.255.255.255 192.168.1.2`

Una vez que la configuración de ruta multicast estática está en su lugar, para la búsqueda RPF, el firewall da preferencia a la tabla de ruteo multicast en lugar de a la tabla de ruteo unicast del ASA y envía los mensajes PIM directamente al vecino 192.168.1.2.

> **Nota:** La ruta multicast estática es en cierta medida contraria a la utilidad de la redundancia HSRP, ya que la ruta multicast acepta solamente 1 salto siguiente por combinación de dirección/máscara de red. Si el salto siguiente especificado en el comando mroute falla o se vuelve inalcanzable, el firewall no retrocede al otro router.

El firewall no se considera LHR cuando no es DR en el segmento LAN



El firewall tiene R1 como vecinos PIM en el segmento LAN. R1 es el DR PIM:

```
<#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)
```

Si se recibe una solicitud de unión IGMP del cliente, el firewall no se convierte en el LHR.

La ruta multicast muestra **Null** adicional como OIL y tiene el indicador **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 que el firewall sea el LHR, se puede aumentar la prioridad DR de la interfaz.

<#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

El comando de depuración PIM **debug pim** muestra este resultado:

<#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
```

El indicador Pruned y el valor Null se eliminan de la ruta multicast:

<#root>

firepower#

show mroute

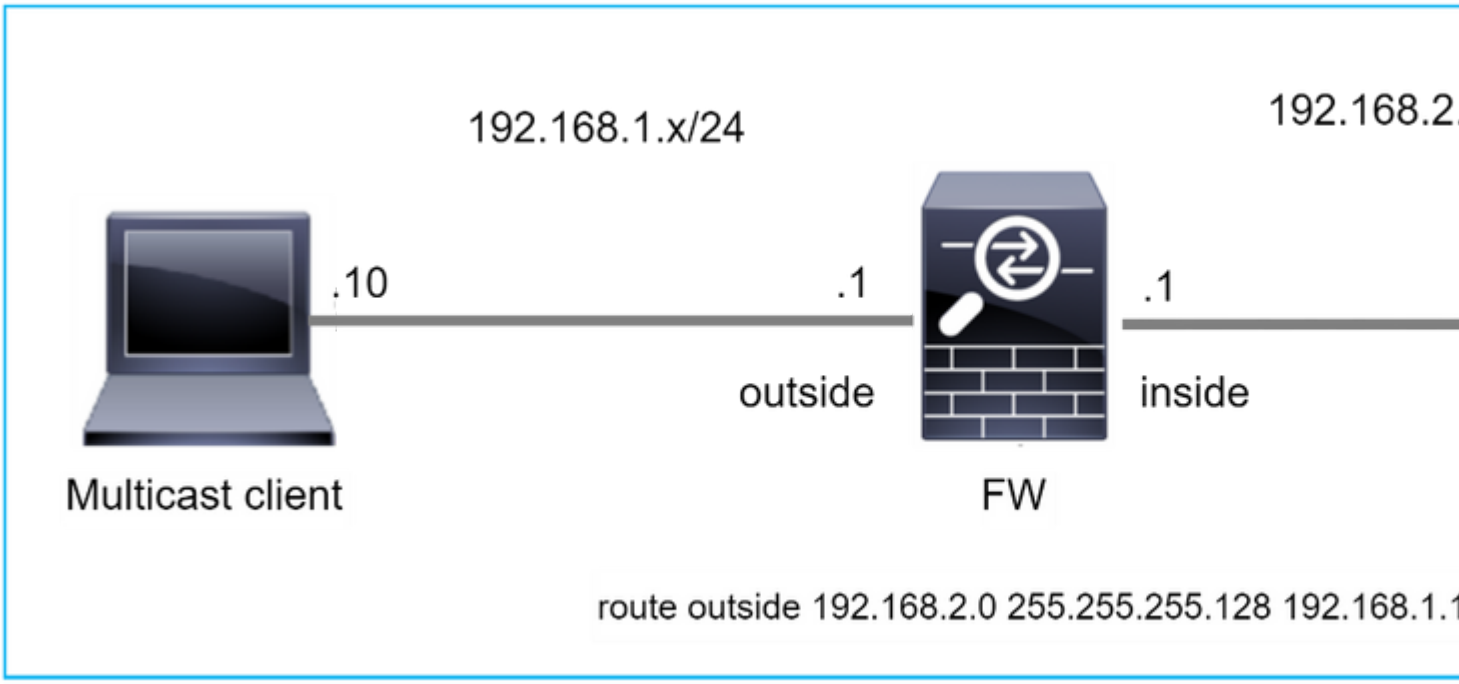
```
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface,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

Firewall descarta paquetes de multidifusión debido a una falla de verificación de reenvío de trayecto inverso



En este caso, los paquetes de multidifusión UDP se descartan debido a una falla de RPF, ya que el firewall tiene una ruta más específica con la máscara 255.255.255.128 a través de la interfaz 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
```

Las capturas de caídas de ASP muestran el motivo de caída **violado por rpf**:

```
<#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
```

Los contadores de RPF fallidos en la salida MFIB aumentan:

```
<#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
```

La solución es reparar la falla de verificación RPF. Una opción es eliminar la ruta estática.

Si no hay más falla de verificación RPF, los paquetes se reenvían y el contador **Forwarding** en la salida MFIB aumenta:

<#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,

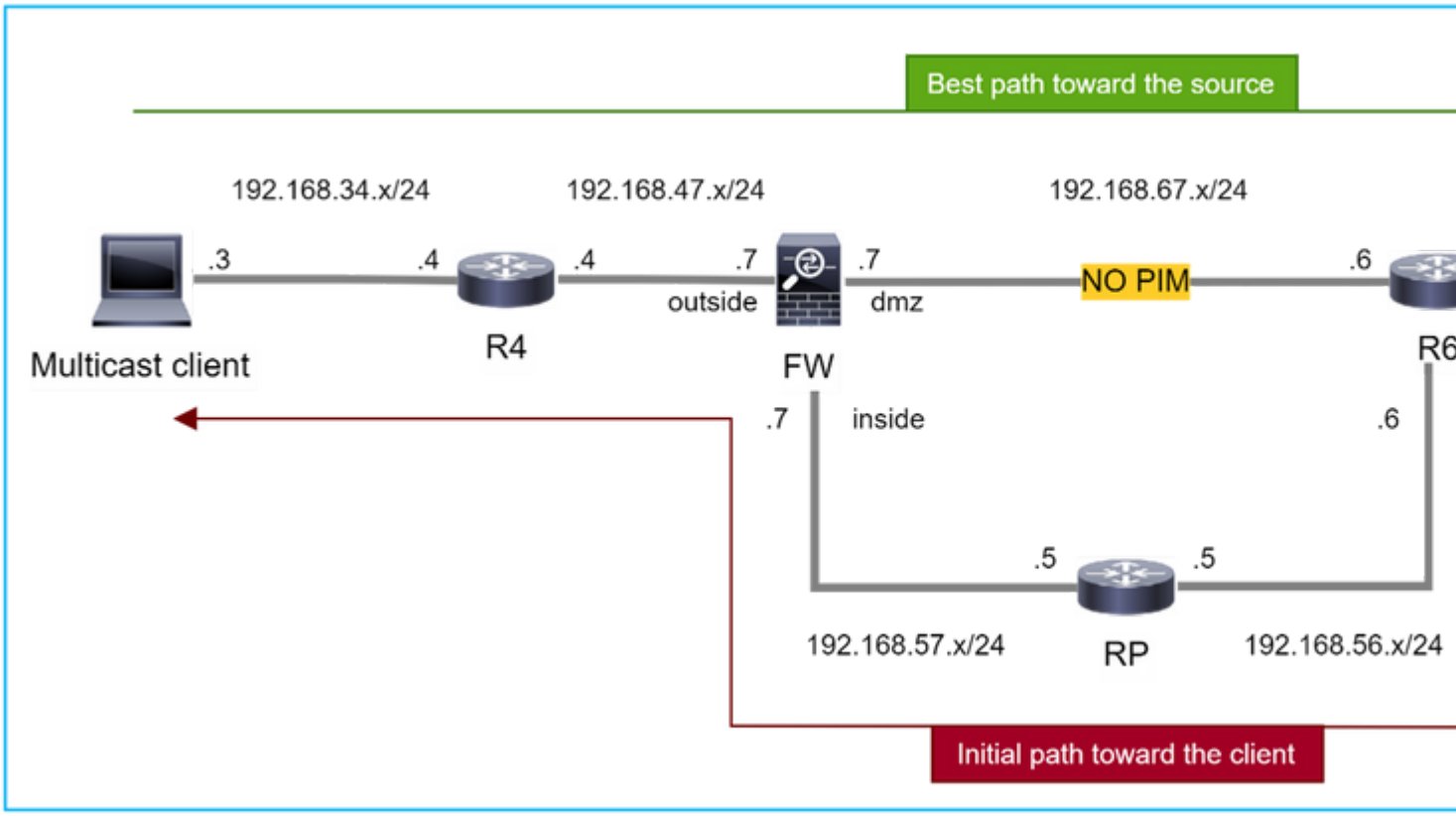
Forwarding: 1044/10/528/41

```
, Other: 0/0/0
```

<--- Forward counter increased

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

El firewall no genera la unión de PIM al conmutar PIM al árbol de origen



En este caso, el firewall aprende la trayectoria hacia el origen multicast a través de la interfaz **dmz R4 > FW > R6**, mientras que la trayectoria de tráfico inicial del origen al cliente es **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

R4 inicia el switchover SPT y envía el mensaje de unión PIM específico de la fuente una vez que se alcanza el umbral de switchover SPT. En el firewall el switchover SPT no tiene lugar, la ruta multicast (S,G) no tiene el indicador **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
```

El comando de depuración PIM **debug pim** muestra 2 solicitudes recibidas de unión PIM del par R4 - para **(*,G) y (S,G).** El firewall envió una solicitud de unión a PIM para (*,G) flujo ascendente y no pudo enviar una solicitud específica del origen debido a un vecino no válido 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

El resultado de los comandos **show pim neighbor** carece de 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
```

PIM está habilitado en la interfaz 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
```

El PIM está inhabilitado en la interfaz 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
```

La solución es habilitar PIM en la interfaz GigabitEthernet0/3 en 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
```

El firewall instala el indicador T, que indica el 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
```

Firewall descarta los primeros paquetes debido al límite de velocidad de punteo

Cuando el firewall recibe los primeros paquetes de un **nuevo** flujo de multidifusión en FP, se puede requerir un procesamiento adicional por parte del CP. En este caso, el FP dirige los paquetes al CP a través de SP (FP > SP > CP) para operaciones adicionales:

- Creación de una conexión **padre** en FP entre las interfaces de ingreso y las interfaces de identidad.
- Comprobaciones adicionales específicas de multidifusión, como la validación RPF, la encapsulación PIM (en el caso de que el firewall sea FHR), la comprobación OIL, etc.
- Creación de una entrada (S,G) con las interfaces de entrada y salida en la tabla de ruta multicast.
- Creación de una conexión **hijo/stub** en FP entre las interfaces entrante y saliente.

Como parte de la protección del plano de control, el firewall limita internamente la velocidad del paquete enviado a la CPU.

Los paquetes que exceden la velocidad se descartan en el con la razón de la caída **punt-rate-limit**:

<#root>

firepower#

show asp drop

Frame drop:

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

Utilice el comando **show asp cluster counter** para verificar el número de paquetes multicast impulsados a CP desde 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
```

Utilice el comando **show asp event dp-cp punt** para verificar el número de paquetes en la cola FP > CP y la velocidad 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
```

Cuando la ruta multicast se completa y las conexiones padre/hijo se establecen en el FP, los paquetes se reenvían en el FP como parte de las conexiones existentes. En este caso, FP no envía los paquetes al CP.

¿Cómo procesa el firewall los primeros paquetes de un nuevo flujo de multidifusión?

Cuando el firewall recibe los primeros paquetes de un **nuevo** flujo de multidifusión en datapath, el firewall realiza estas acciones:

1. Comprueba si la directiva de seguridad permite paquetes.
2. Introduce los paquetes en el CP a través del trayecto FP.
3. Crea una conexión **primaria** entre las interfaces de ingreso y las interfaces de identidad:

```
<#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

Registros del sistema:

<#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

Esta conexión es visible en el resultado del 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. El CP interacciona con el proceso de multidifusión para realizar comprobaciones específicas de multidifusión adicionales, como la validación RPF, la encapsulación PIM (en el caso de que el firewall sea el FHR), la comprobación OIL, etc.
5. El CP crea una entrada (S,G) con las interfaces entrante y saliente en la ruta multicast:

<#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. El CP instruye al FP a través de CP > SP > FP path para crear una conexión **hijo/stub** entre las interfaces de entrada y de salida:

Esta conexión es visible solamente en la salida del 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
```

En las versiones de software con la corrección del Id. de bug Cisco CSCwe21280 , también se genera el mensaje syslog 302015 para la conexión hijo/stub:

```
<#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

Cuando se establecen las conexiones principal y secundaria/stub, los paquetes de ingreso coinciden con la conexión existente y se reenvían en 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 tráfico multidifusión ICMP

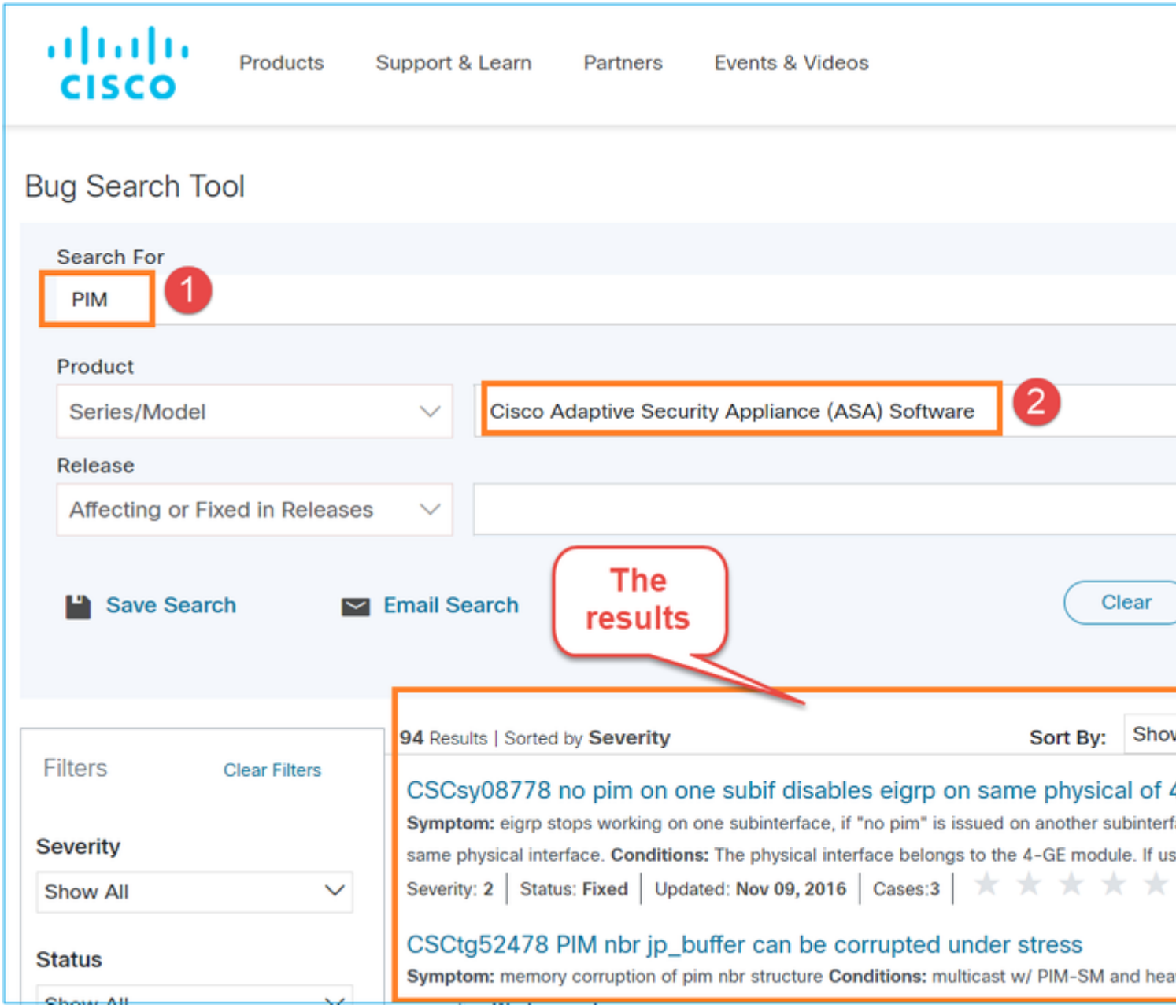
No puede filtrar el tráfico de multidifusión ICMP con una ACL. Debe utilizar la política de plano de control (ICMP):

El ID de bug de Cisco CSCsl26860 ASA no filtra los paquetes ICMP multicast

Defectos de multidifusión PIM conocidos

Puede utilizar la Herramienta de Búsqueda de Errores para detectar defectos conocidos: https://bst.cloudapps.cisco.com/bugsearch

La mayoría de los defectos de ASA y FTD se enumeran bajo el producto 'Cisco Adaptive Security Appliance (ASA) Software':



Información Relacionada

- Resolución de problemas comunes y de multidifusión ASA

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).