Troubleshoot Firepower Threat Defense and ASA Multicast PIM

Contents

Introduction

This document describes how Firepower Threat Defense (FTD) and Adaptive Security Appliance (ASA) implement Protocol Independent Multicast (PIM).

Prerequisites

Requirements

Basic IP routing knowledge.

Components Used

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

The information in this document is based on these software and hardware versions:

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

Background Information

Multicast Routing basics

- Unicast forwards packets towards the destination while **multicast forwards packets away from the source.**
- Multicast network devices (firewalls/routers, and so on) forward the packets via **Reverse Path Forwarding (RPF).** Note that RPF is not the same as uRPF which is used in unicast to prevent specific types of attacks. RPF can be defined as a mechanism that forwards multicast packets away from the source out of interfaces that lead toward multicast receivers. Its primary role is to prevent traffic loops and ensure correct traffic paths.
- A multicast protocol like PIM has 3 main functions:

1. Find the **upstream interface** (interface closest to the source).

2. Find the **downstream interfaces** associated with a specific multicast stream (interfaces towards the receivers).

3. Maintain the multicast tree (add or remove the tree branches).

- A multicast tree can be built and maintained by one of the 2 methods: **implicit joins (flood-and-prune)** or **explicit joins (pull model).** PIM Dense Mode (PIM-DM) uses implicit joins while PIM Sparse Mode (PIM-SM) uses explicit joins.
- A multicast tree can be either **shared** or **source-based:**
  - Shared trees use the concept of **Rendezvous Point (RP)** and are noted as **(*, G)** where G = multicast group IP.
  - Source-based trees are rooted at the source, donâ€™t use an RP, and are noted as **(S, G)** where S = the IP of the multicast source/server.
- Multicast forwarding models:
  - **Any-Source Multicast (ASM)** delivery mode uses shared trees (*, G) where any source can send the multicast stream.
  - **Source-Specific Multicast (SSM)** uses source-based trees (S, G) and the IP range 232/8.
  - **Bidirectional (BiDir)** is a type of shared tree (*, G) where both control-plane and data-plane traffic go through the RP.
- A Rendezvous Point can be configured or elected with one of these methods:
  - Static RP
  - Auto-RP
  - Bootstrap Router (BSR)

PIM modes summary

PIM mode	RP	Shared tree	Notation	IGMP	ASA/FTD supported
PIM Sparse Mode	Yes	Yes	(*, G) and (S, G)	v1/v2/v3	Yes

PIM Dense Mode	No	No	(S, G)	v1/v2/v3	No*
PIM Bidirectional Mode	Yes	Yes	(*, G)	v1/v2/v3	Yes
PIM Source-Specific-Multicast (SSM) Mode	No	No	(S, G)	v3	No**

*Auto-RP = Auto-RP traffic can pass through

** ASA/FTD cannot be a last-hop device

RP configuration summary

Rendezvous Point configuration	**ASA/FTD**
Static RP	Yes
Auto-RP	No, but Auto-RP control-plane traffic can pass through
BSR	Yes, but not C-RP support

Note: Before you start to troubleshoot any multicast issue, it is very important to have a clear view of the multicast topology. Specifically, at minimum, you need to know:
- What is the role of the firewall in the multicast topology?
- Who is the RP?
- Who is the sender of the multicast stream (source IP and multicast group IP)?
- Who is the receiver of the multicast stream?
- Do you have issues with the Control Plane (IGMP/PIM) or the Data Plane (multicast stream) itself?

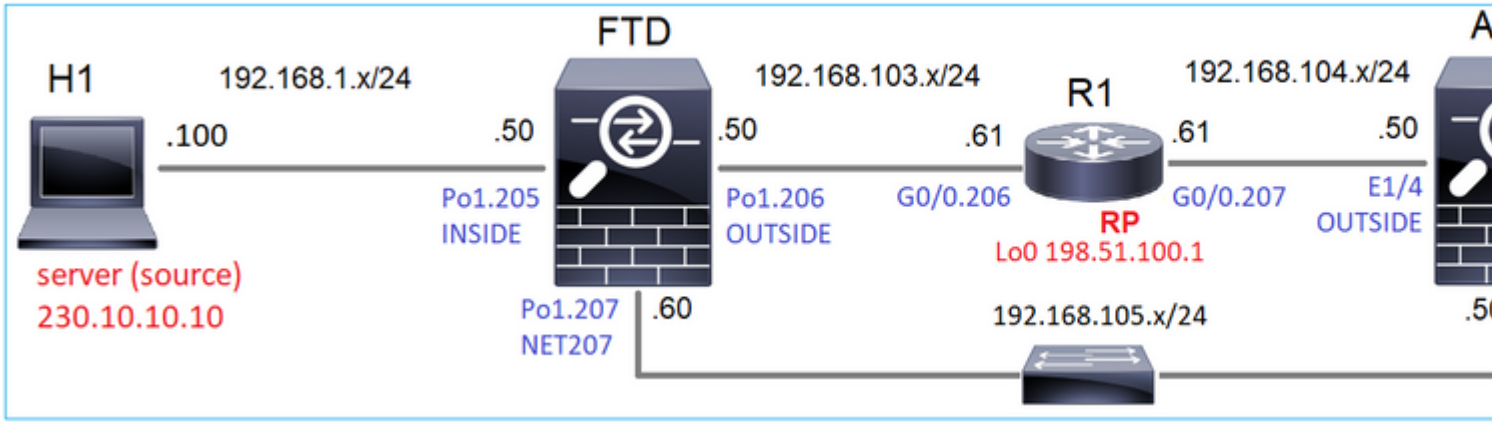
Abbreviations/Acronyms

Acronyms	**Explanation**
FHR	First-Hop Router â€“ a hop directly connected to the source of the multicast traffic.
LHR	Last-Hop Router â€“ a hop directly connected to the receivers of the

	multicast traffic.
RP	Rendezvous-Point
DR	Designated Router
SPT	Shortest-Path Tree
RPT	Rendezvous-Point (RP) Tree, share tree
RPF	Reverse Path Forwarding
OIL	Outgoing Interface List
MRIB	Multicast Routing Information Base
MFIB	Multicast Forwarding Information Base
ASM	Any-Source Multicast
BSR	Bootstrap Router
SSM	Source-Specific Multicast
FP	Fast Path
SP	Slow Path
CP	Control Point
PPS	Packet Per Second rate

Task 1 â€“ PIM Sparse mode (Static RP)

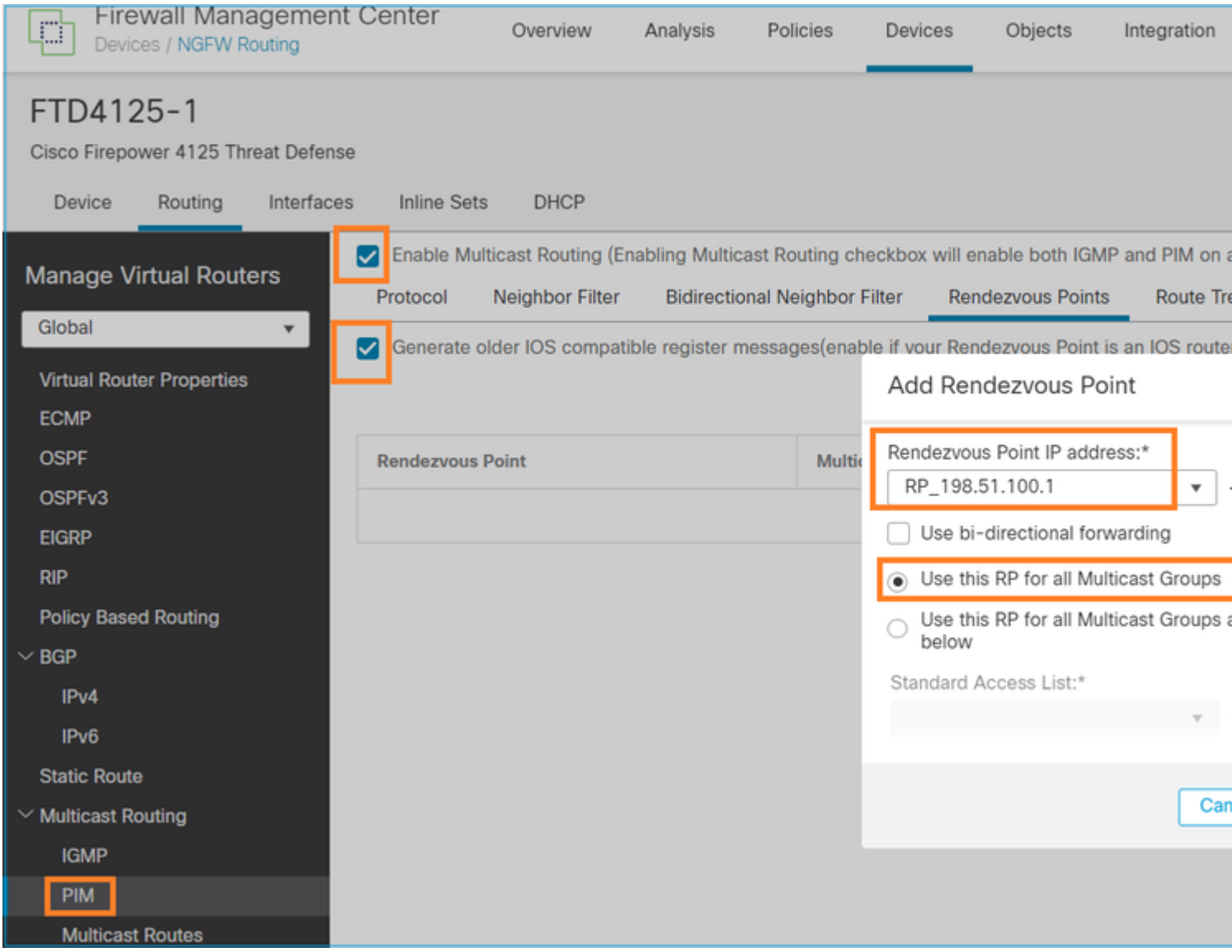
Topology



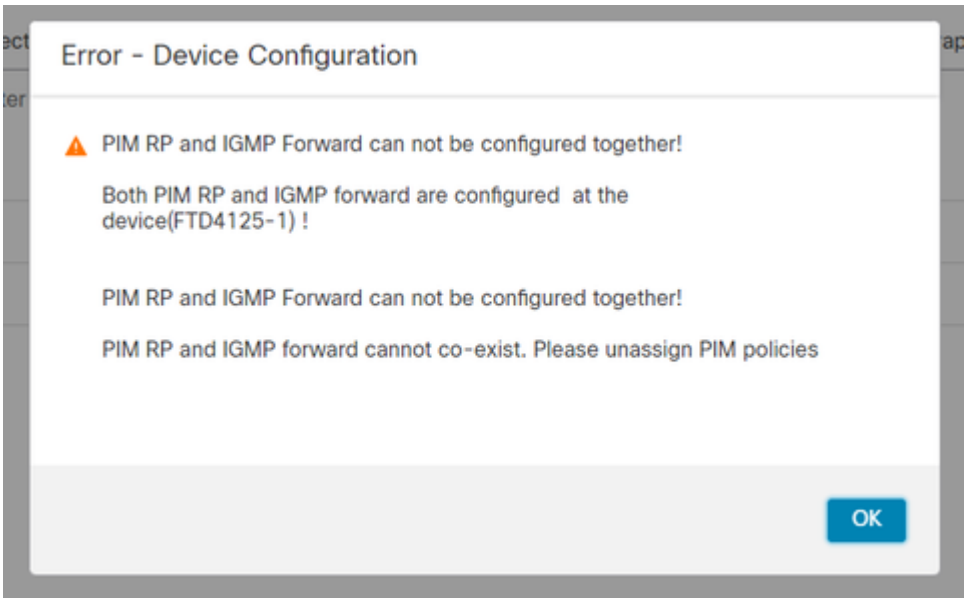
Configure multicast PIM sparse-mode in the topology with R1 (198.51.100.1) as RP.

Solution

FTD configuration:



The ASA/FTD cannot be configured for IGMP Stub Routing and PIM at the same time:



The resulted configuration on 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

On ASA firewall there is a similar configuration:

```
<#root>

asa(config)#

multicast-routing


asa(config)#

pim rp-address 198.51.100.1
```

RP configuration (Cisco router):

```
<#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
```

Verification

Verify the multicast control plane on FTD when there is no multicast traffic (senders or receivers):

```
<#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
```

Verify the PIM neighbors:

<#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)
```

The RP advertises the whole multicast group range:

<#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
```

The firewall mroute table has some non-relevant entries (239.255.255.250 is Simple Service Discovery Protocol (SSDP) used by vendors like MAC OS and 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
```

There is a PIM tunnel built between the firewalls and the 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

The PIM tunnel can be also seen on the firewall connection table:

<#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
```

Verification on the ASA firewall:

<#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

RP (Cisco router) RP verification. There are some multicast groups for SSDP and 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
```

Verification once a receiver announces its presence

Note: The firewall commands shown in this section are fully applicable to ASA and FTD.

The ASA gets the IGMP Membership Report message and creates the IGMP and mroute (*, G) entries:

<#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

The ASA firewall creates an mroute for the multicast group:

<#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
```

Another firewall verification is the PIM topology output:

```
<#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
```

> **Note**: If the firewall does not have a route towards the RP then the **debug pim** output shows an RPF lookup failure

---

The RPF lookup failure in the **debug pim** output:

```
<#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

In case everything is OK the firewall sends a PIM Join-Prune message to the RP:

<#root>

asa#

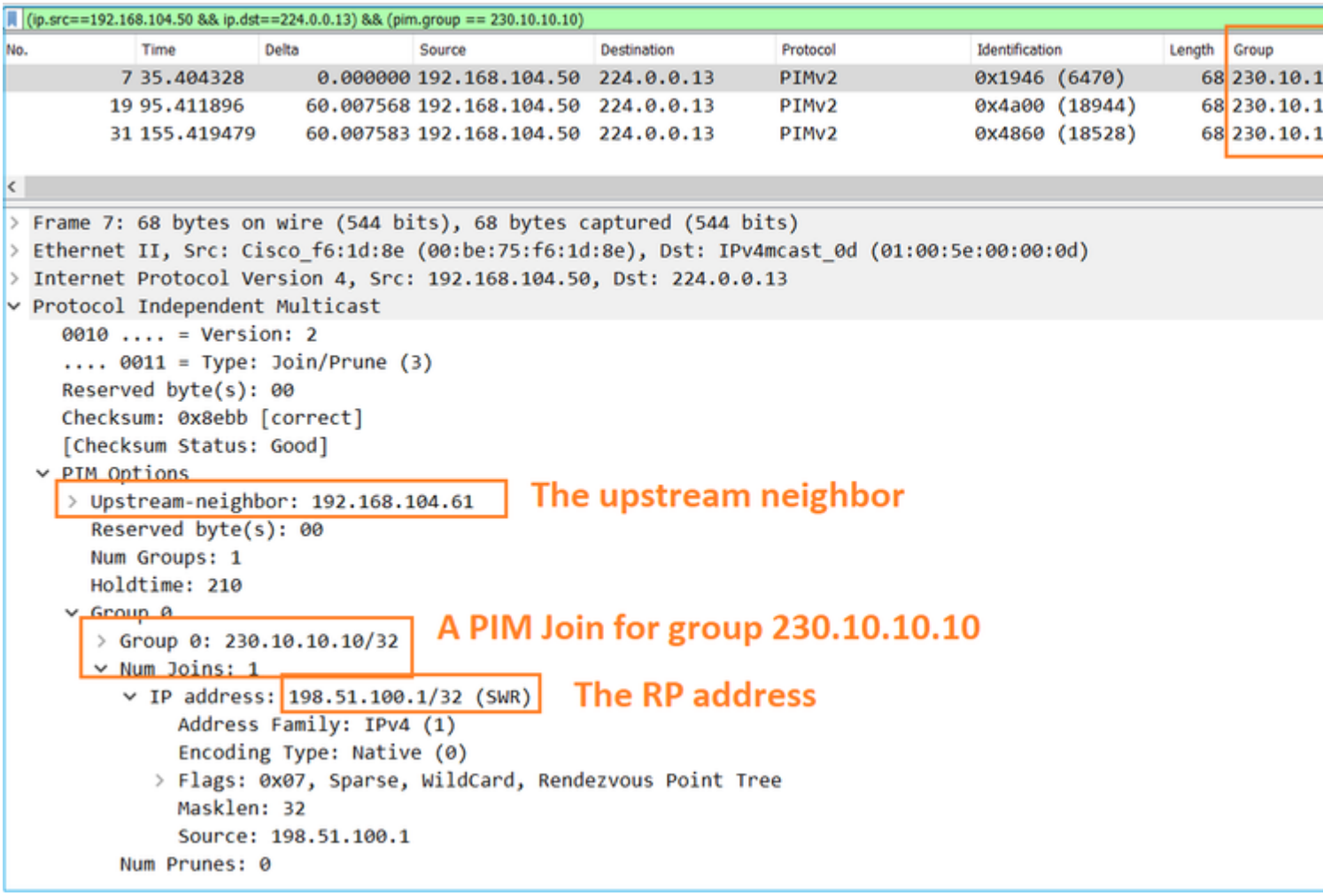
debug pim group 230.10.10.10

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

The capture shows that the PIM Join messages are sent every 1 min and PIM Hellos every 30 seconds. PIM uses the IP 224.0.0.13:



Tip: Wireshark display filter: (ip.src==192.168.104.50 && ip.dst==224.0.0.13) && (pim.group == 230.10.10.10)
- 192.168.104.50 is the firewall IP of the egress interface (towards the upstream PIM neighbor)
- 224.0.0.13 is the PIM multicast group where the PIM Joins and Prunes are sent
- 230.10.10.10 is the multicast group that we send the PIM Join/Prune for

---

The RP creates a (*, G) mroute. Note that since there are not yet any servers the Incoming Interface is Null:

<#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

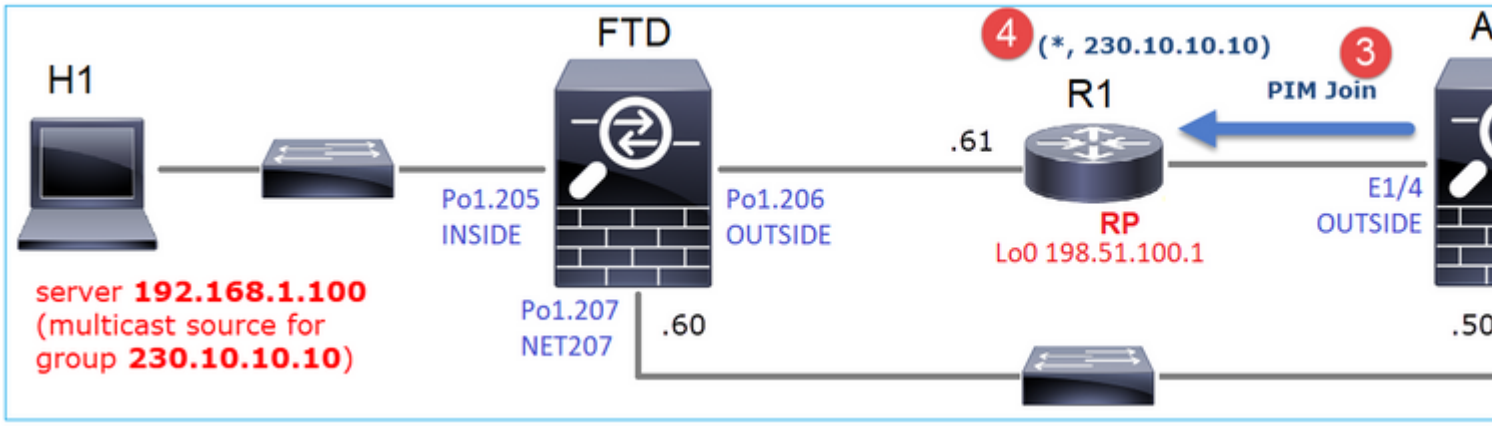
Incoming interface: Null

, 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
```

This can be visualized as:



1. IGMP Report is received on ASA.
2. A (*, G) mroute is added.
3. The ASA sends a PIM Join message to the RP (198.51.100.1).
4. The RP receives the Join message and adds a (*, G) mroute.

At the same time, on FTD there are no mroutes since there was no IGMP Report nor PIM Join received:

```
<#root>

firepower#

show mroute 230.10.10.10

No mroute entries found.
```

Verification when the server sends a multicast stream

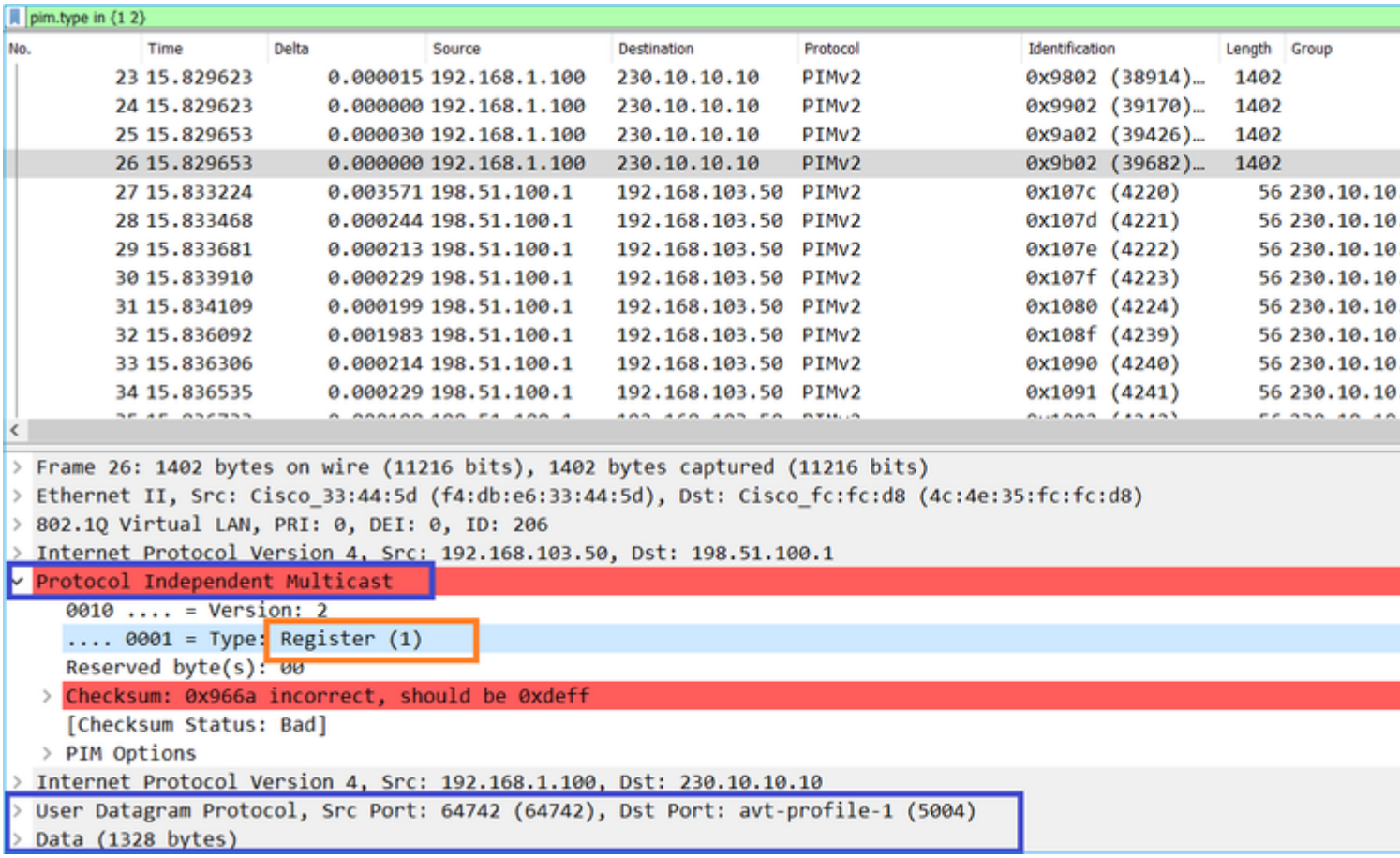
The FTD gets the multicast stream from H1 and starts the **PIM Registration process** with the RP. The FTD sends a **unicast PIM Register** message to the RP. The RP sends a **PIM Join** message to the First-Hop-Router (FHR), which is the FTD in this case, to join the multicast tree. Then it sends a **Register-Stop** message.

```
<#root>

firepower#

debug pim group 230.10.10.10


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

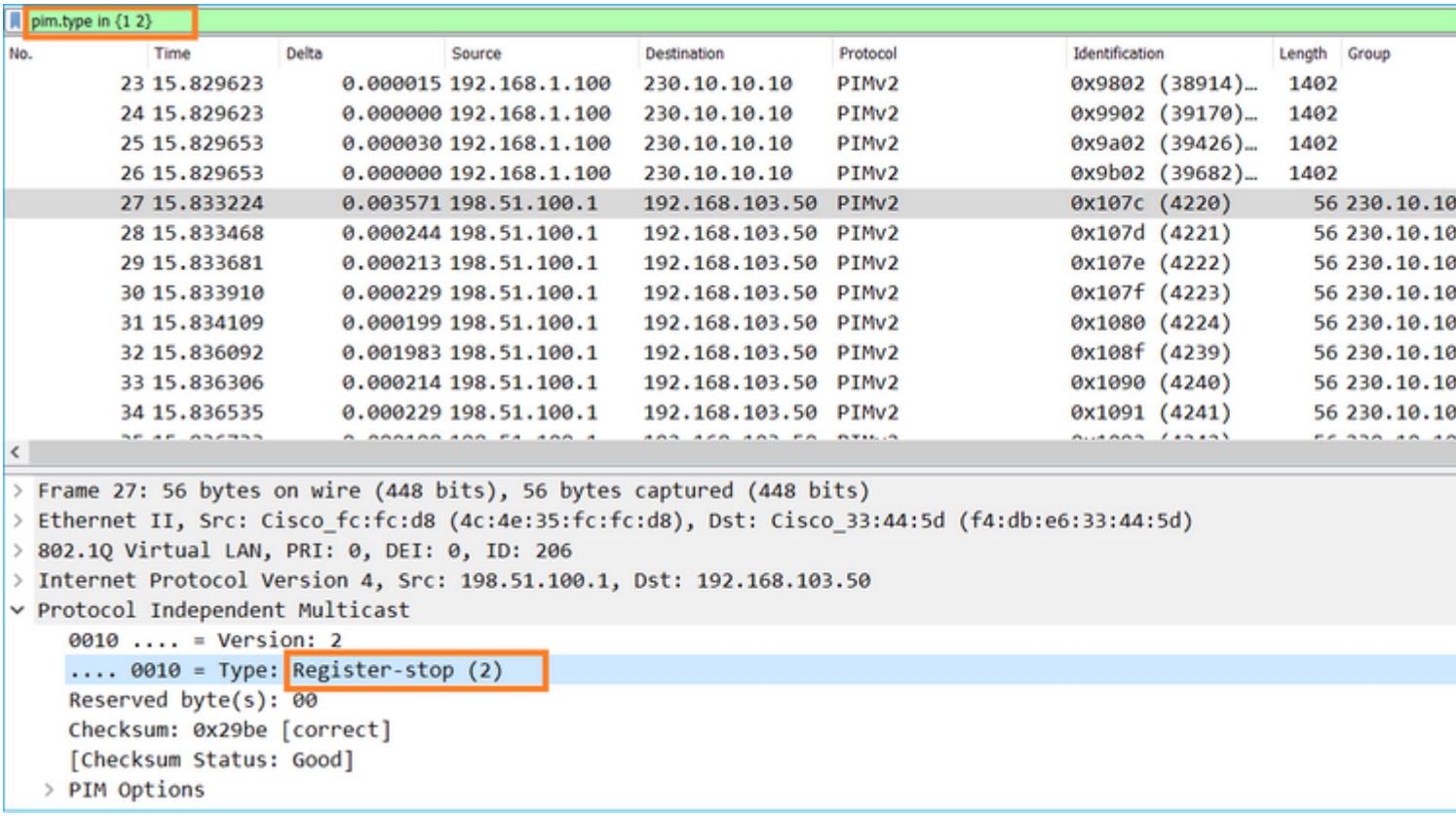
```
firepower#
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB update (f=20,c=20)
IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on INSIDE
IPv4 PIM: (192.168.1.100,230.10.10.10) Create entry
IPv4 PIM: (192.168.1.100,230.10.10.10) RPF changed from 0.0.0.0/- to 192.168.1.100/INSIDE


<-- 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)
```

The PIM Register message is a PIM message that carries UDP data along with the PIM Register info:



The PIM Register-Stop message:



Tip: To display only PIM Register and PIM Register-Stop messages on Wireshark, you can use the display filter: pim.type in {1 2}

The firewall (last-hop router) gets the multicast stream on interface OUTSIDE, and initiates the Shortest Path Tree (SPT) switchover to interface NET207:

<#root>

asa#

debug pim group 230.10.10.10

IPv4 PIM group debugging is on
for group 230.10.10.10

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

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

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

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

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

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

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

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

Set SPT bit **<-- The SPT bit is set**

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

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

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

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

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

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

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

The PIM debug on the FTD when the switchover occurs:

<#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
```

The FTD mroute once the SPT switchover starts:

<#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 ir

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

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

At the end of the SPT switchover, only the NET207 interface is shown in the OIL of 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

On the last-hop router (ASA), the SPT bit is also set:

<#root>

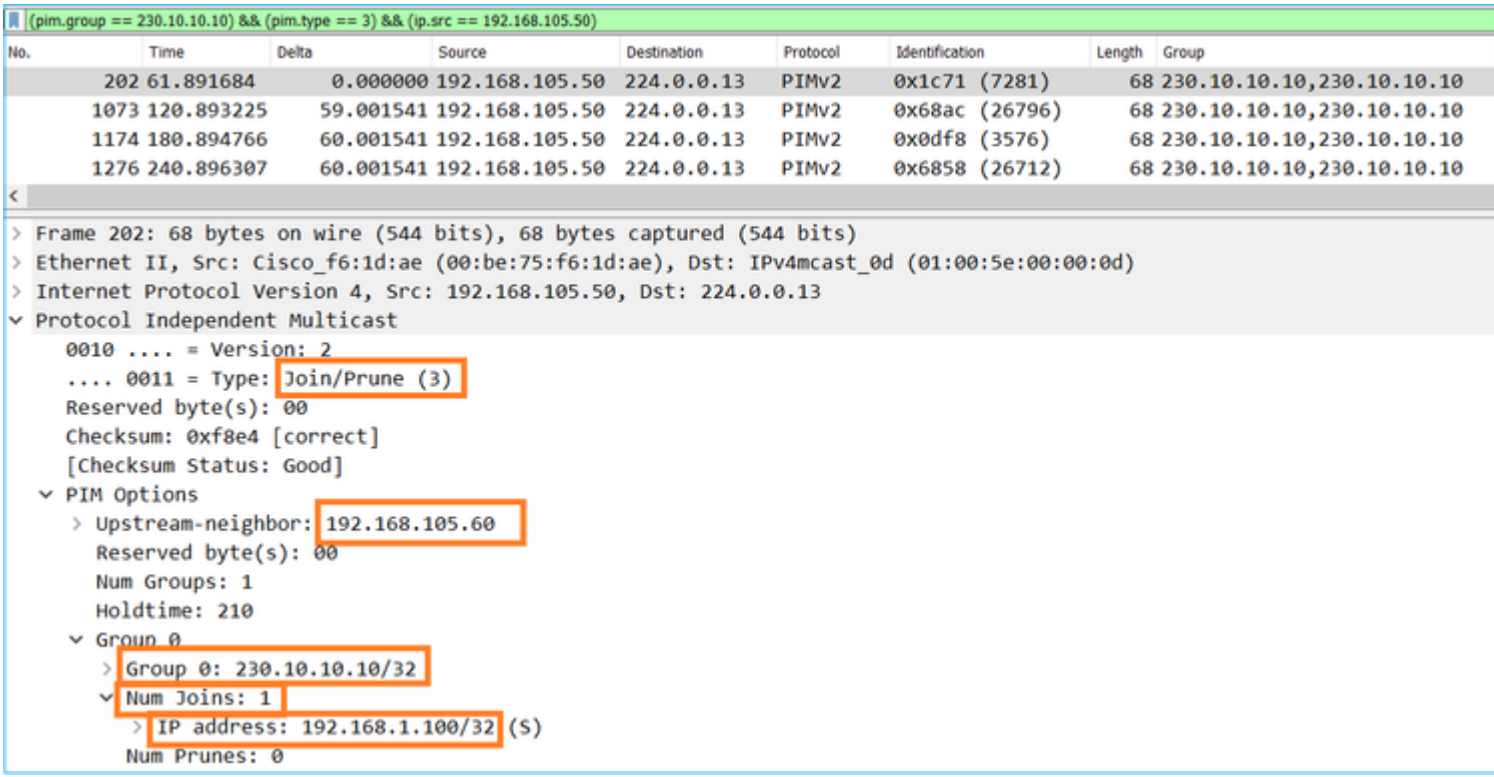
asa#

show mroute 230.10.10.10

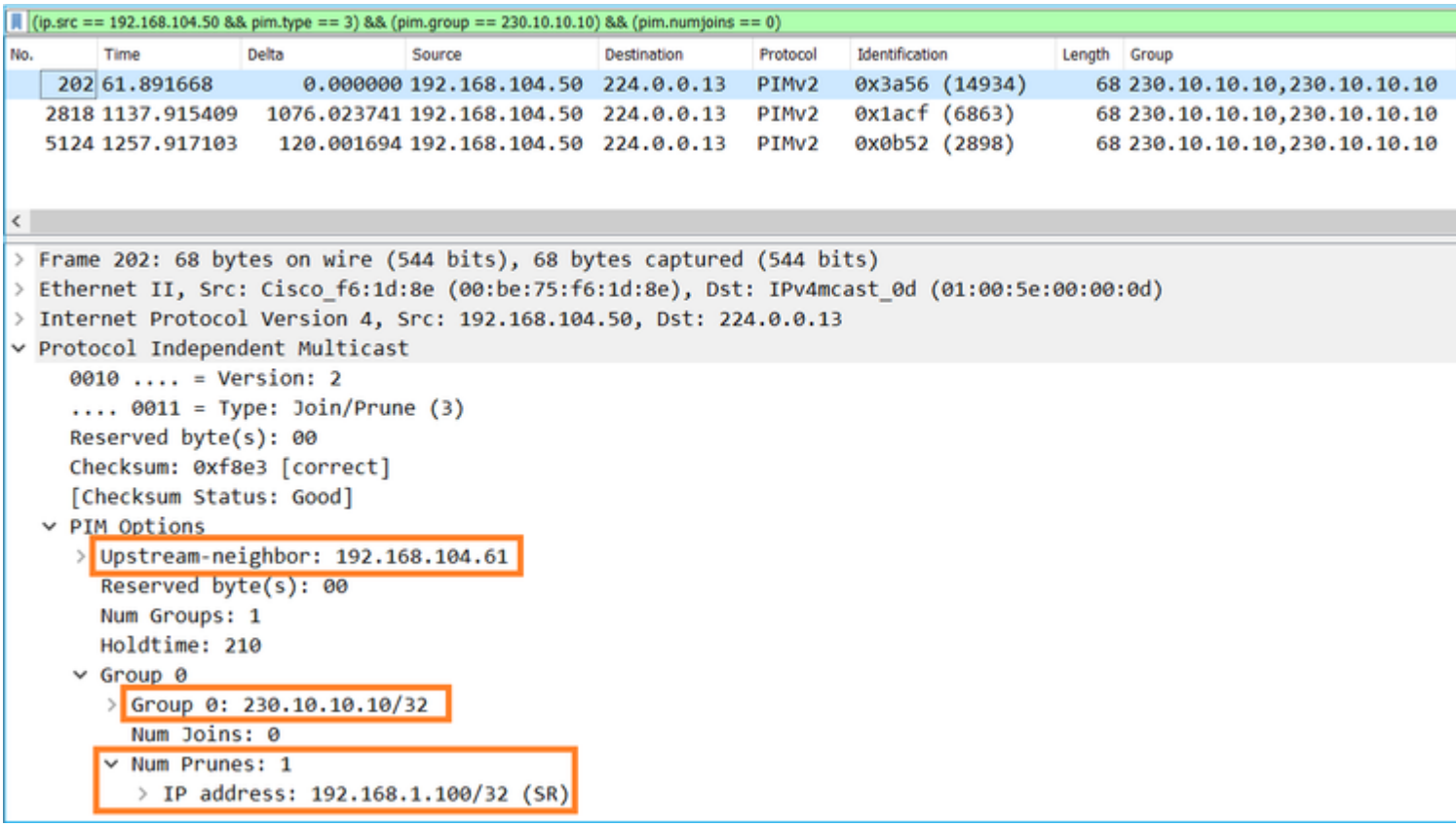
```
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
```

```
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
```

The switchover from the ASA NET207 interface (the first-hop router that did the switchover). A PIM Join message is sent to the upstream device (FTD):



On the OUTSIDE interface a PIM Prune message is sent to the RP to stop the multicast stream:



Verification of the PIM traffic:

<#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
```

To verify the number of packets handled in the Slow Path vs Fast Path vs Control Point:

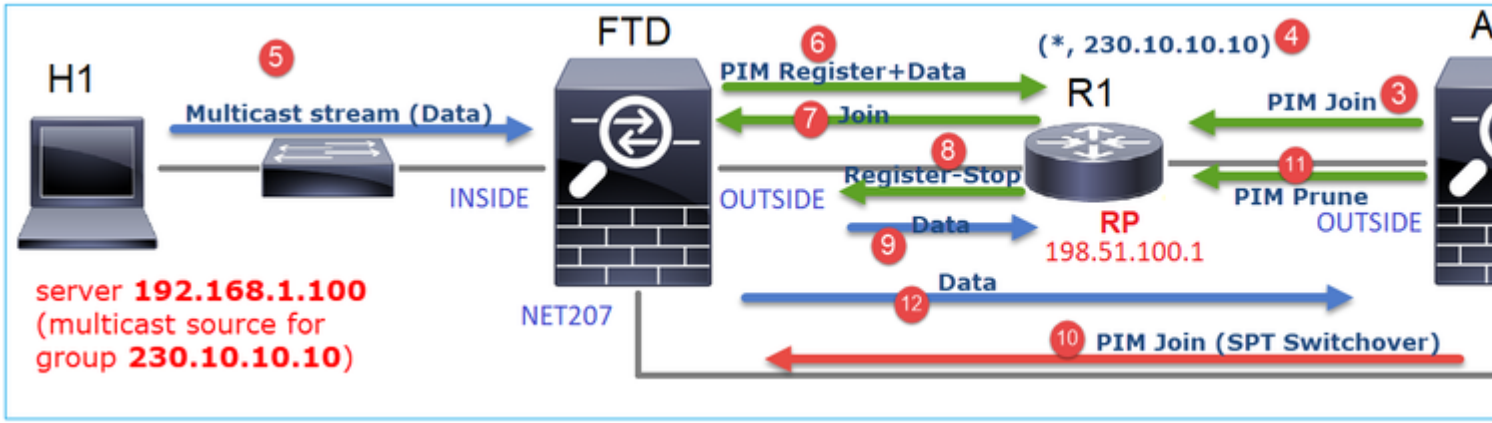
<#root>

```
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
```

A diagram that shows what happens step-by-step:



1. The end-host (H2) sends an IGMP Report to join the multicast stream 230.10.10.10.
2. The last-hop router (ASA) which is the PIM DR creates a (*, 230.10.10.10) entry.
3. The ASA sends a PIM Join message towards RP for group 230.10.10.10.
4. The RP creates the (*, 230.10.10.10) entry.
5. The server sends the multicast stream data.
6. The FTD encapsulates the multicast packets in PIM Register messages and sends them (unicast) to

RP. At this point, the RP sees that he has an active receiver, decapsulates the multicast packets, and sends them to the receiver.
7. The RP sends a PIM Join message to the FTD to join the multicast tree.
8. The RP sends a PIM Register-Stop message to the FTD.
9. The FTD sends a native multicast stream (no PIM encapsulation) towards the RP.
10. The last-hop router (ASA) sees that the source (192.168.1.100) has a better path from the NET207 interface and starts a switchover. It sends a PIM Join message to the upstream device (FTD).
11. The last-hop router sends a PIM Prune message to the RP.
12. The FTD forwards the multicast stream towards the NET207 interface. The ASA moves from the shared tree (RP tree) to the source tree (SPT).

Task 2 â€“ Configure PIM Bootstrap Router (BSR)

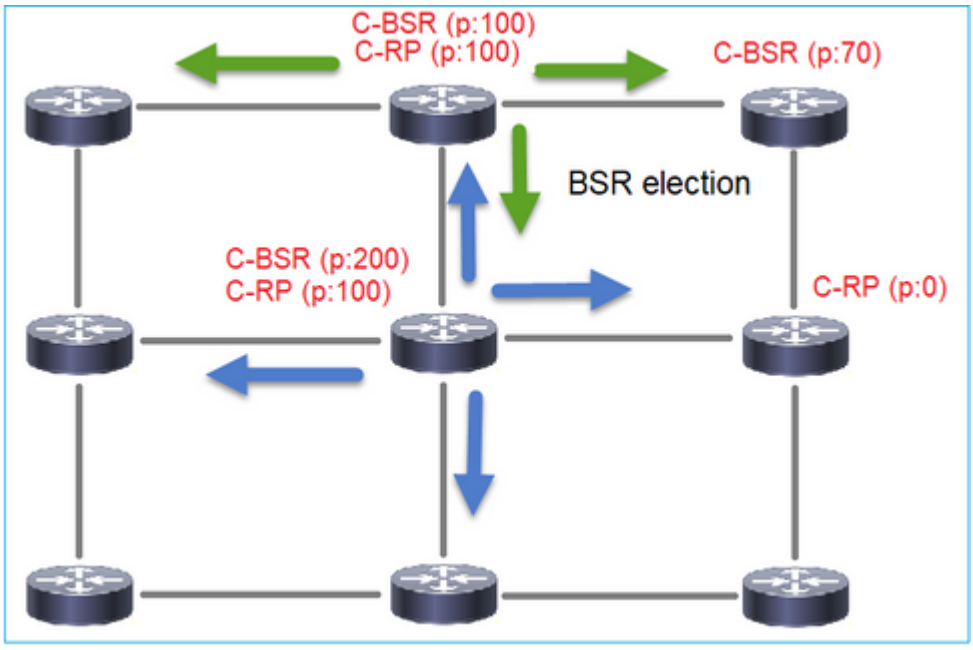
BSR basics

- BSR (RFC 5059) is a control-plane multicast mechanism that uses the PIM protocol and allows devices to learn the RP information dynamically.
- BSR definitions:
  - Candidate RP (C-RP): A device that wants to be an RP.
  - Candidate BSR (C-BSR): A device that wants to be a BSR and advertises RP-sets to other devices.
  - BSR: A device that is elected a BSR among many C-BSRs. The **highest BSR priority wins** the election.
  - RP-set: A list of all C-RPs and their priorities.
  - RP: The device with the **lowest RP priority wins** the election.
  - BSR PIM message (empty): A PIM message used in the BSR election.
  - BSR PIM message (normal): A PIM message sent to 224.0.0.13 IP and contains an RP-set and BSR info.

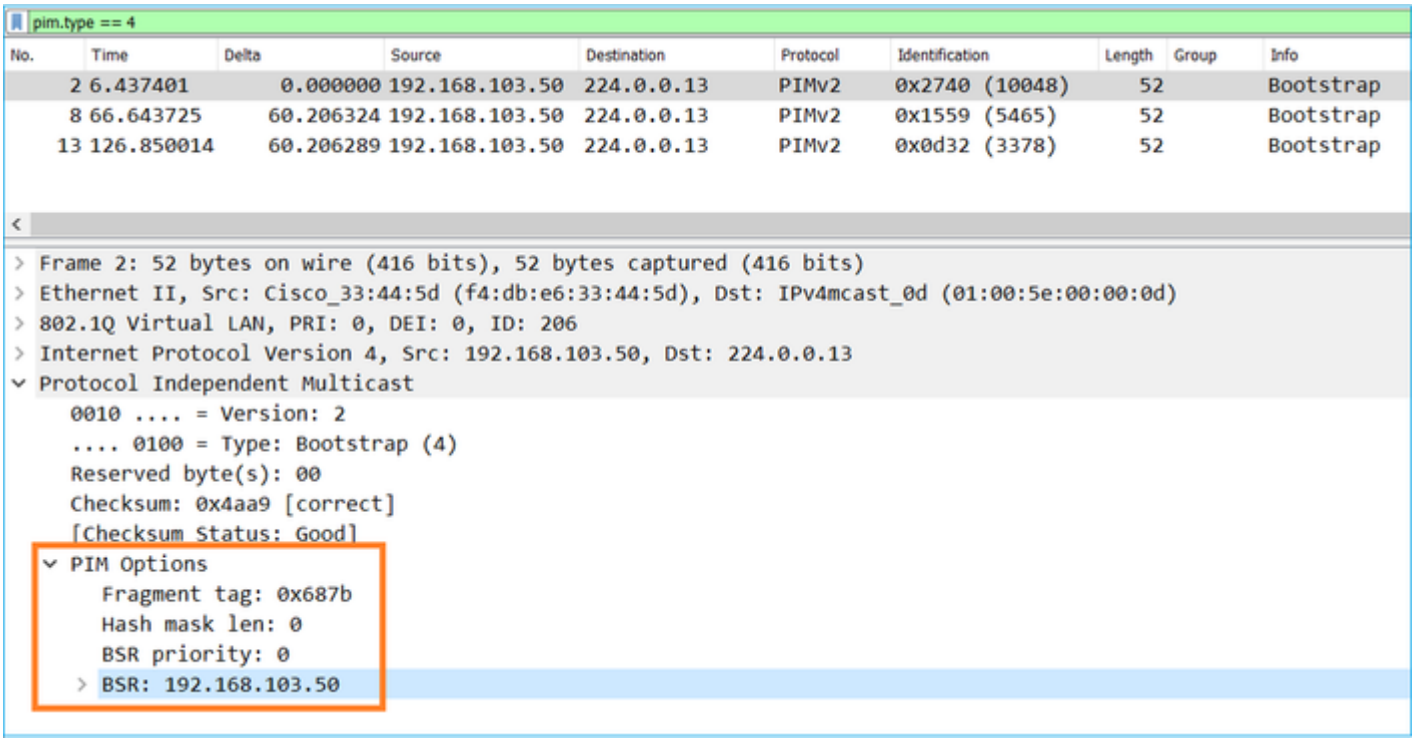
How BSR works

1. BSR election mechanism.

Each C-BSR sends PIM BSR empty messages that contain a priority. The device with the highest priority (fallback is the highest IP) wins the election and becomes the BSR. The rest of the devices do not send any more empty BSR messages.

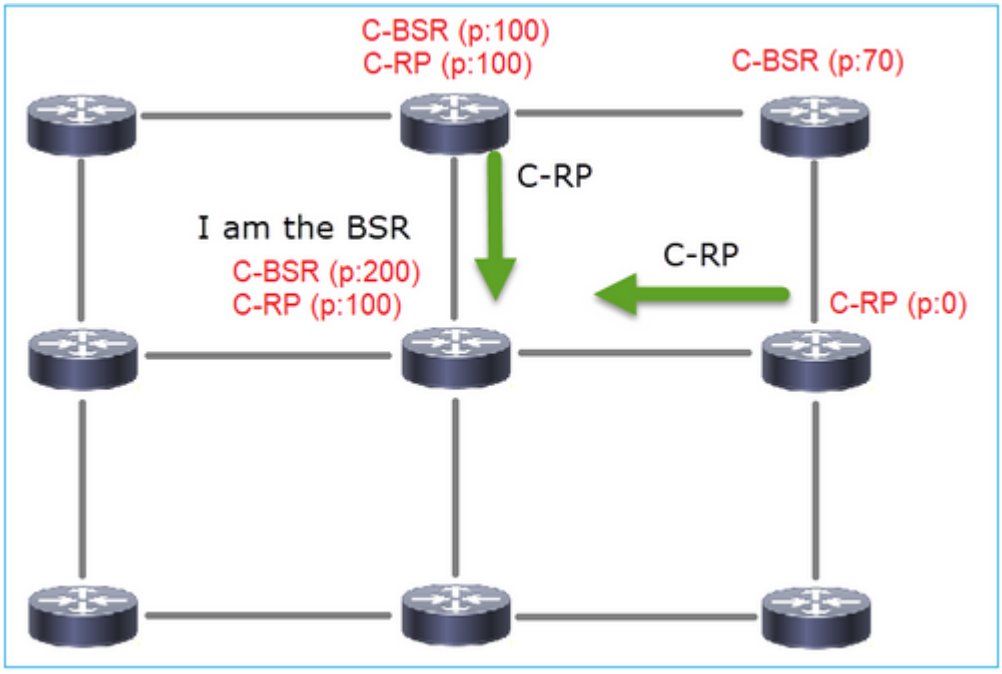


A BSR message used in the election process contains only C-BSR priority info:



To display BSR messages in Wireshark, use this display filter: pim.type == 4

2. The C-RPs send **unicast** BSR messages to the BSR that contain their C-RP priority:



A candidate RP message:

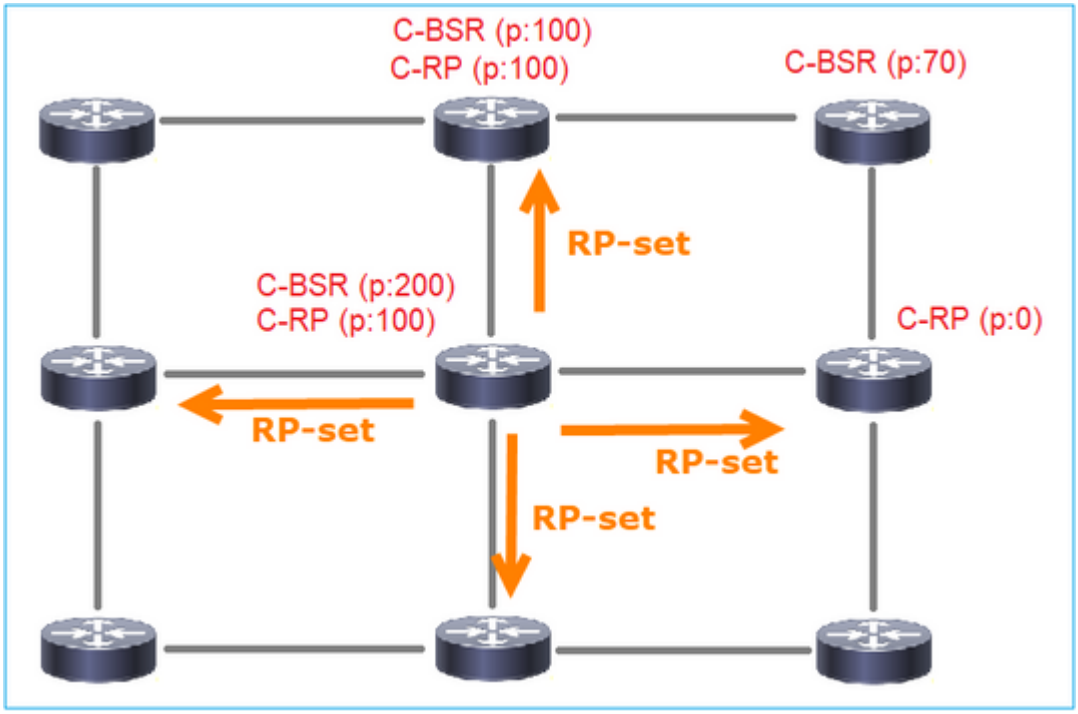
pim.type == 8

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
```

To display BSR messages in Wireshark, use this display filter: pim.type == 8

3. The BSR composes the RP-set and advertises it to all PIM neighbors:

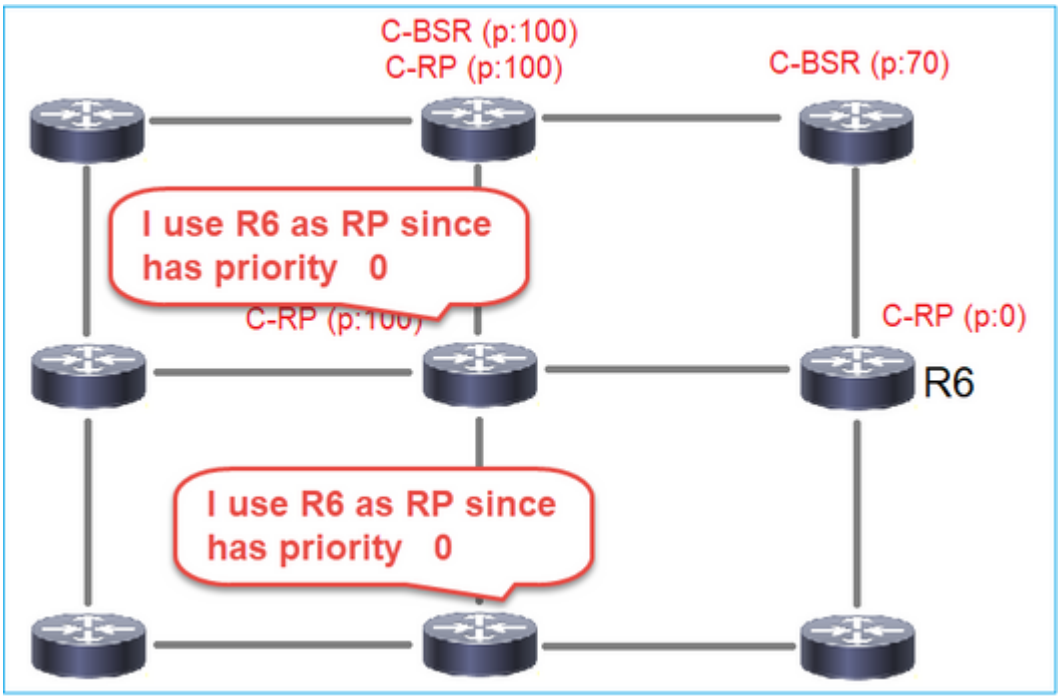


(ip.src == 192.168.105.60) && (pim.type == 4)

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

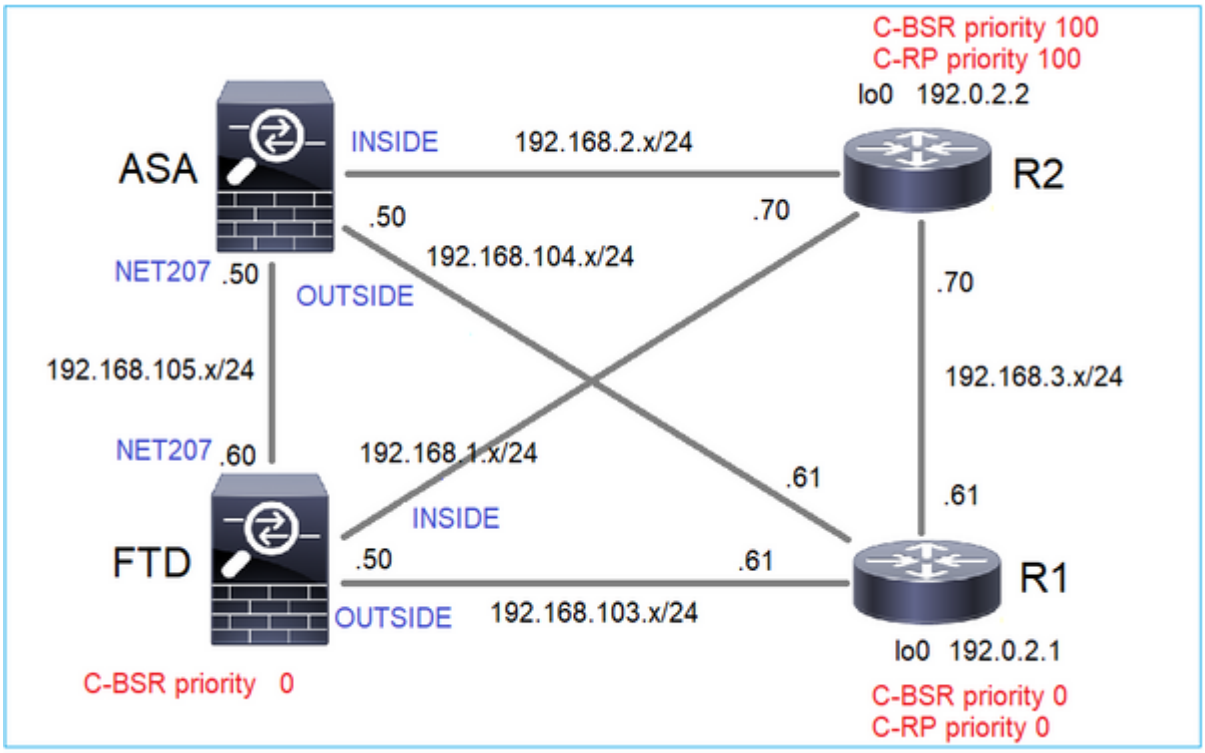
```
> Frame 152: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
> Ethernet II, Src: Cisco_33:44:5d (f4:db:e6:33:44:5d), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
> 802.1Q Virtual LAN, PRI: 6, DEI: 0, ID: 207
> Internet Protocol Version 4, Src: 192.168.105.60, Dst: 224.0.0.13
v Protocol Independent 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. The routers/firewalls get the RP-set and elect the RP based on the lowest priority:



Task requirement

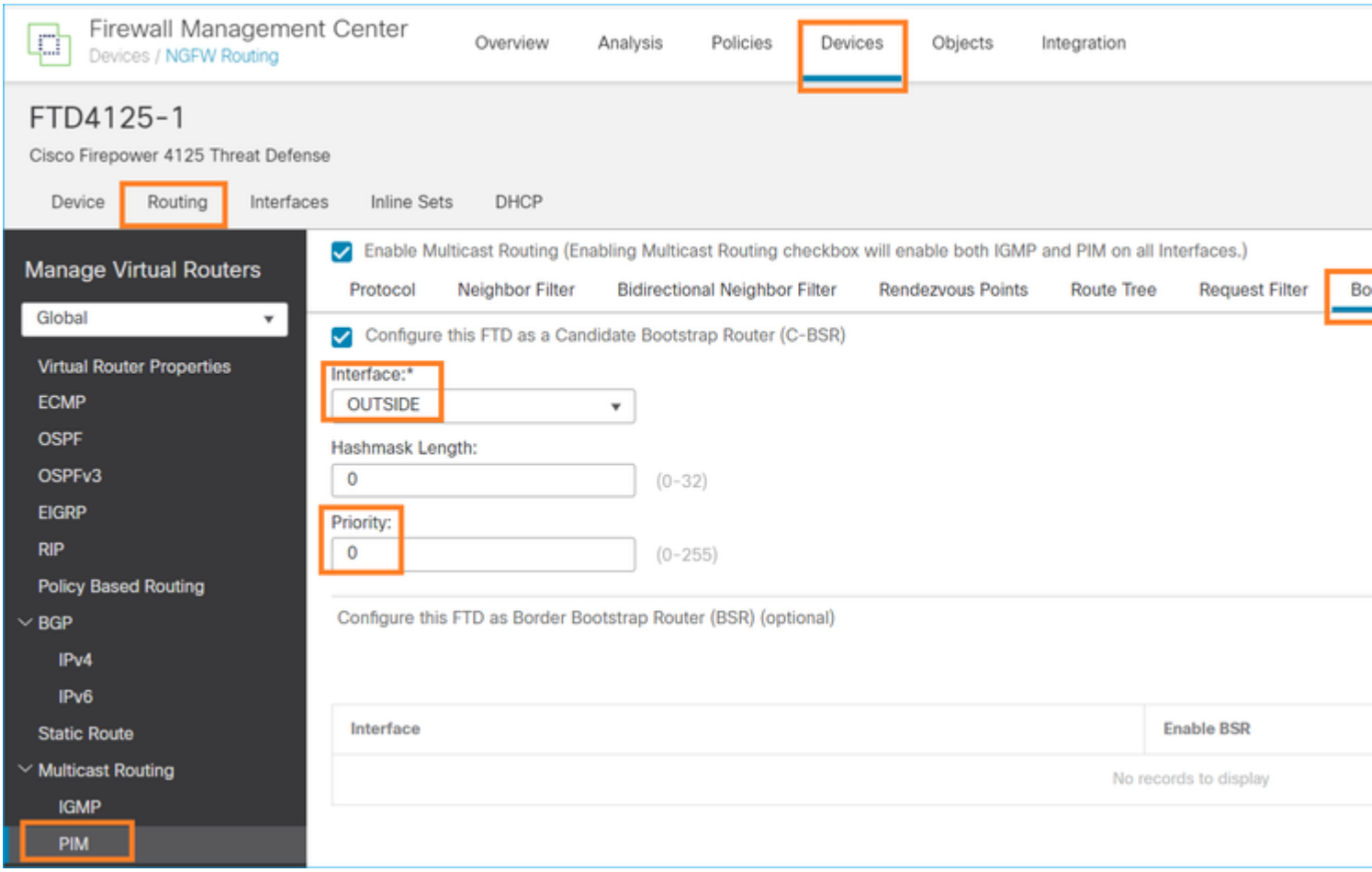
Configure the C-BSRs and C-RPs per this topology:



for this task, the FTD must announce itself as C-BSR on the OUTSIDE interface with BSR priority 0.

Solution

FMC configuration for FTD:



The deployed configuration:

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

Configuration on the other devices:

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)
```

Same on R2, but with different C-BSR and C-RP priorities

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

On ASA there is just multicast globally enabled. This enables PIM on all interfaces:

```
multicast-routing
```

Verification

R2 is the elected BSR due to the highest priority:

```
<#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 is elected as RP due to the lowest priority:

```
<#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

The BSR messages **are subject to RPF check**. You can enable **debug pim bsr** to verify this:

<#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/

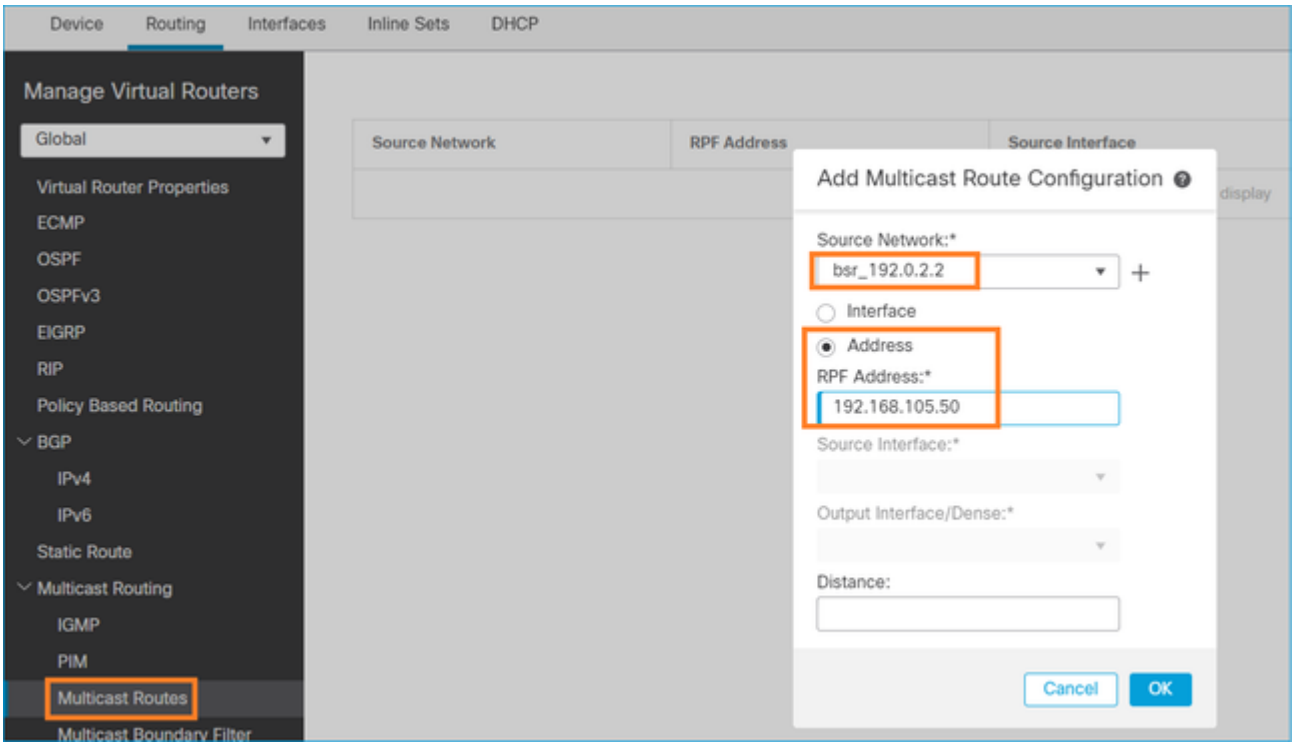
NET207

for 192.0.2.2

RPF failed, dropped

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

If you want to change the RPF interface you can configure a static mroute. In this example, the firewall accepts BSR messages from 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

Now BSR messages on NET207 interface are accepted, but on INSIDE are dropped:

<#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

Enable capture with trace on the firewall and check how the BSR messages are processed:

<#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
```

The PIM connections are terminated on the firewall so in order for the trace to show useful information there is a need to clear the connections to the box:

<#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
```

If the PIM packet is dropped due to RPF failure, the trace shows:

<#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

The ASP table drops and captures show RPF-failed packets:

<#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

To capture packets that are dropped due to RPF failure:

<#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
```

Troubleshooting Methodology

The troubleshooting methodology for the firewall mainly depends on the on the role of the firewall in the multicast topology. This is the list of recommended steps for troubleshooting:

1. Clarify the details of problem description and symptoms. Try to narrow down the scope to the **Control Plane (IGMP/PIM)** or the **Data Plane (multicast stream)** issues.
2. The mandatory prerequisite for troubleshooting multicast issues on the firewall is to clarify the multicast topology. At minimum, you need to identify:
    - role of the firewall in the multicast topology - FHR, LHR, RP, or another intermediary role.
    - expected multicast ingress and egress interfaces on the firewall.
    - RP.
    - sender source IP addresses.
    - multicast groups IP addresses and destination ports.
    - receivers of the multicast stream.

3. Identify the type of multicast routing **- Stub** or **PIM multicast routing:**

- **Stub multicast routing -** it provides dynamic host registration and facilitates multicast routing. When configured for stub multicast routing, the ASA acts as an IGMP proxy agent. Instead of fully participating in multicast routing, the ASA forwards IGMP messages to an upstream multicast router, which sets up delivery of the multicast data. To identify the stub mode routing, use the **show igmp interface** command and check IGMP forward configuration:

```
<#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 is enabled on the interfaces; however, neighborship is not established:

```
<#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.
```

PIM-SM/Bidir and IGMP forwarding are **not** supported concurrently.

You cannot configure options such as the RP address:

<#root>

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

- **PIM multicast routing** - **The PIM multicast routing is the most common deployment.** The firewall supports both PIM-SM and bidirectional PIM. PIM-SM is a multicast routing protocol that uses the underlying unicast routing information base or a separate multicast-capable routing information base. It builds unidirectional shared tree rooted at a single Rendezvous Point (RP) per multicast group and optionally creates shortest-path trees per multicast source. In this deployment mode, unlike the stub mode, the users usually configure the RP address configuration, and the firewall establishes PIM adjacencies with the peers:

<#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. Check RP IP address is configured and reacheability:

<#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
```

Warning: The firewall cannot be simultaneously an **RP** and a **FHR**.

---

5. Check additional outputs depending on the role of the firewall in the multicast topology and the problem symptoms.

FHR

- Check interface **Tunnel0** status. This interface is used to encapsulate raw multicast traffic inside PIM payload and send unicast packet to RP for with PIM-register bit set:

```
<#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
```

- Check mroutes:

```
<#root>

firepower#

show mroute


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

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

  RPF nbr: 192.168.2.1, Registering <--- Registering state


  Immediate Outgoing interface list:
    outside, Forward, 00:00:07/00:03:26

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

When the firewall receives PIM packet with Register-Stop bit, Tunnel0 is removed from the OIL. The firewall then stops encapsulation and sends raw multicast traffic via the egress interface:

<#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

- Check PIM register counters:

<#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
```

- Check unicast PIM packet captures between the firewall and the 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
```

- Collect additional outputs (x.x.x.x is the multicast group, y.y.y.y is the RP IP). It is recommended to collect the outputs **few times**:

<#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
```

- Collect raw multicast interface packet and ASP drop captures.

<#root>

```
capture capi interface <ingress intf> buffer 32000000 match udp host X host Z <--- (ingress capture for
```

```
capture capo interface <egress intf> buffer 32000000 match udp host X host Z <--- (egress capture for mu
capture asp type asp-drop buffer 32000000 match udp host X host Z <--- (ASP drop capture for multicast U
```

- Syslog messages - common IDs are 302015, 302016 and 710005.

RP

- Check interface Tunnel0 status. This interface is used to encapsulate raw multicast traffic inside PIM payload and send unicast packet to FHR for with PIM-stop bit set:

<#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        -
```

- Check mroutes:

<#root>

```
firepower#

show mroute



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


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



Incoming interface: Tunnel0


  RPF nbr: 192.168.2.2
  Immediate Outgoing interface list:


outside

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


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


  Incoming interface:

inside


  RPF nbr: 192.168.2.1
  Immediate Outgoing interface list:


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

- Check PIM counters:

<#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
```

- Collect additional outputs (x.x.x.x is the multicast group, y.y.y.y is the RP IP). It is recommended to collect the outputs **few times**:

<#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
```

- Collect raw multicast interface packet and ASP drop captures:

<#root>

```
capture capi interface <ingress intf> buffer 32000000 match udp host X host Z <--- (ingress capture for

capture capo interface <egress intf> buffer 32000000 match udp host X host Z <--- (egress capture for mu

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

- Syslog - common IDs are 302015, 302016 and 710005.

LHR

Consider the steps mentioned in the section for the RP and these additional checks:

- 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
```

- IGMP groups:

<#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
```

- IGMP traffic statistics:

<#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
```

PIM Troubleshooting Commands (Cheat Sheet)

Command	Description
show running-config multicast-routing	To see if multicast routing is enabled on the firewall
show run mroute	To see the static mroutes configured on the firewall
show running-config pim	To see the PIM configuration on the firewall
show pim interface	To see which firewall interfaces have PIM enabled and the PIM neighbors.
show pim neighbor	To see the PIM neighbors
show pim group-map	To see the multicast groups mapped to the RP
show mroute	To see the full multicast routing table
show mroute 230.10.10.10	To see the multicast table for a specific multicast group
show pim tunnel	To see if there is a PIM tunnel built between the firewall and the RP
show conn all detail address RP_IP_ADDRESS	To see if there is a connection (PIM tunnel) established between the firewall and the RP

show pim topology	To see the firewall PIM topology output
debug pim	This debug shows all PIM messages from and to the firewall
debug pim group 230.10.10.10	This debug shows all PIM messages from and to the firewall for the specific multicast group
show pim traffic	To see statistics about received and sent PIM messages
show asp cluster counter	To verify the number of packets handled in the Slow Path vs Fast Path vs Control Point
show asp drop	To see all software-level drops on the firewall
capture CAP interface INSIDE trace match pim any any	To capture and trace ingress PIM multicast packets on the firewall
capture CAP interface INSIDE trace match udp host 224.1.2.3 any	To capture and trace the ingress multicast stream
show pim bsr-router	To verify who is the elected BSR router
show conn all address 224.1.2.3	To show the parent multicast connection
show local-host 224.1.2.3	To show the child/stub multicast connections

For more info about firewall captures check: Work with Firepower Threat Defense Captures and Packet Tracer

Known Issues

Firepower multicast limitations:

- Does not support IPv6.
- PIM/IGMP multicast is not supported on interfaces in a traffic zone (EMCP).
- The firewall cannot be simultanouesly an RP and a FHR.
- The **show conn all** command shows only the identity multicast connections. To show the stub/secondary multicast connection use the **show local-host <*group IP*>** command.

PIM is not Supported on a vPC Nexus

If you try to deploy a PIM adjacency between a Nexus vPC and the Firewall there is a Nexus limitation as described here:

Supported Topologies for Routing over Virtual Port Channel on Nexus Platforms

From the NGFW point of view, you see in capture with trace this drop:

<#root>

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

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

The firewall cannot complete the RP Registration:

<#root>

```
firepower#
```

show mroute 224.1.2.3

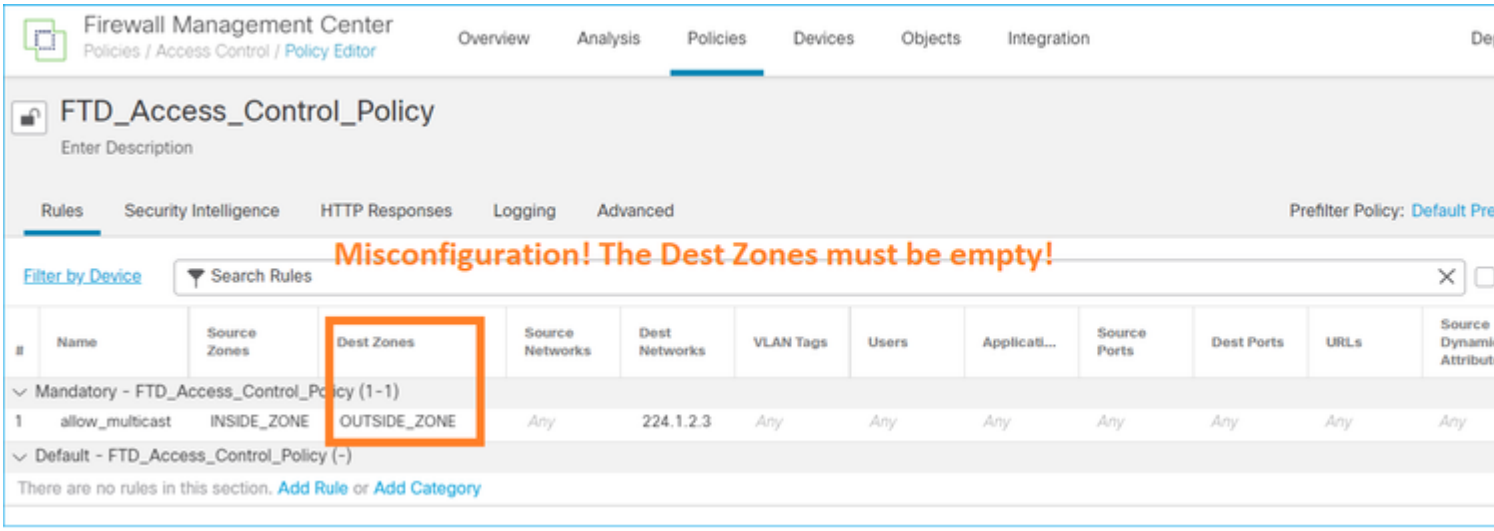
```
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface,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

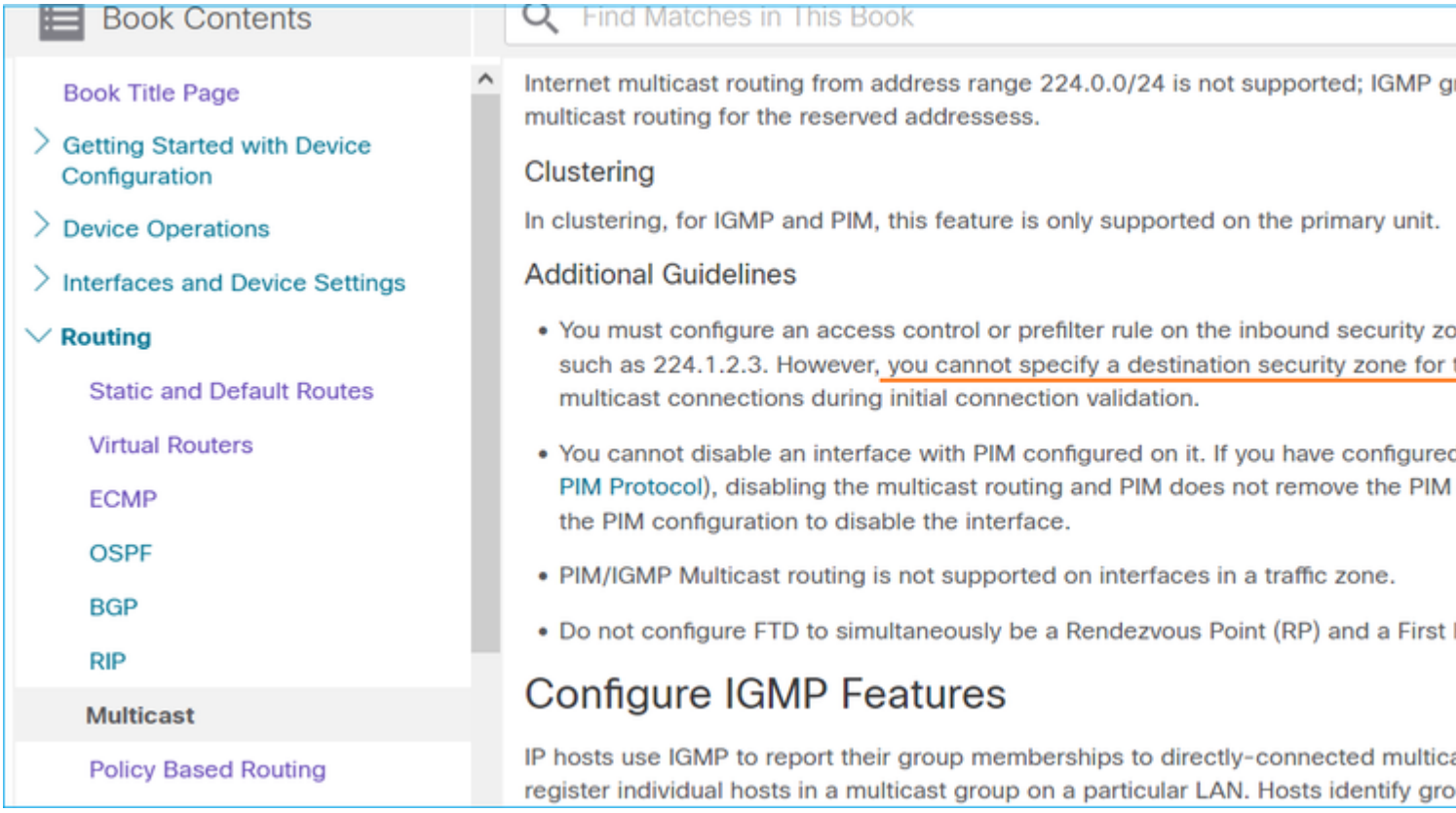
```
  Immediate Outgoing interface list:
    Tunnel0, Forward, 00:39:15/never
```

Destination Zones are not Supported

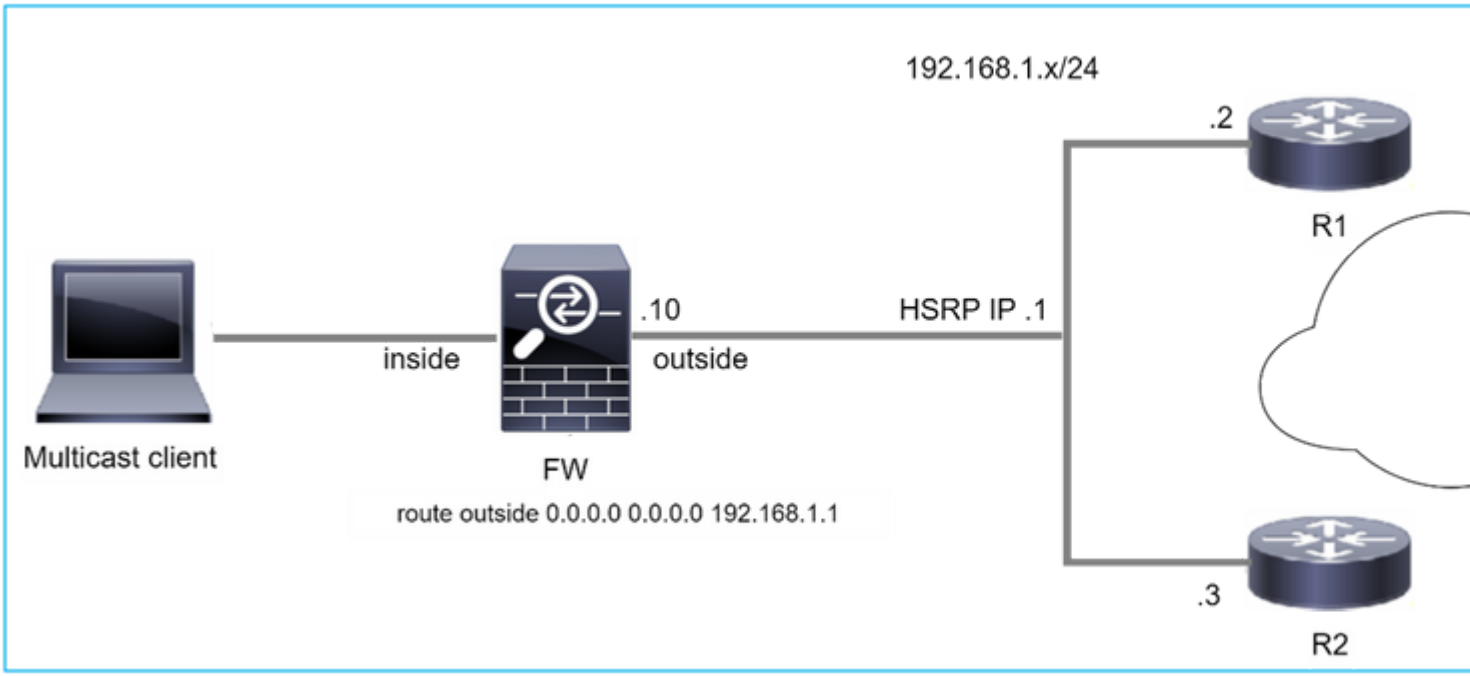
You cannot specify a destination security zone for the Access Control Policy rule that matches multicast traffic:



This is also documented in the FMC user guide:



Firewall does not PIM Messages Toward Upstream Routers Due To HSRP



In this case, the firewall has a default route via the Hot Standby Redundancy Protocol (HSRP) IP 192.168.1.1 and PIM neighborship with routers R1 and R2:

```
<#root>

firepower#

show run route

route outside 0.0.0.0 0.0.0.0 192.168.1.1 1
```

The firewall has PIM adjacency between the outside and the physical interface IP on R1 and 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)
```

The firewall does not send PIM Join message to upstream network. The PIM debug command **debug pim** shows this output:

```
<#root>

firepower#

debug pim
```

```
...

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

RFC 2362 states that *"a router sends a periodic Join/Prune message to each distinct RPF neighbor associated with each (S,G), (*,G) and (*,*,RP) entry. Join/Prune messages are sent only if the RPF neighbor is a PIM neighbor."*

To mitigate the problem, the user can add a static mroute entry on the firewall. The router must point to one of the two router interface IP addresses, 192.168.1.2 or 192.168.1.3, typically the HSRP active router IP.

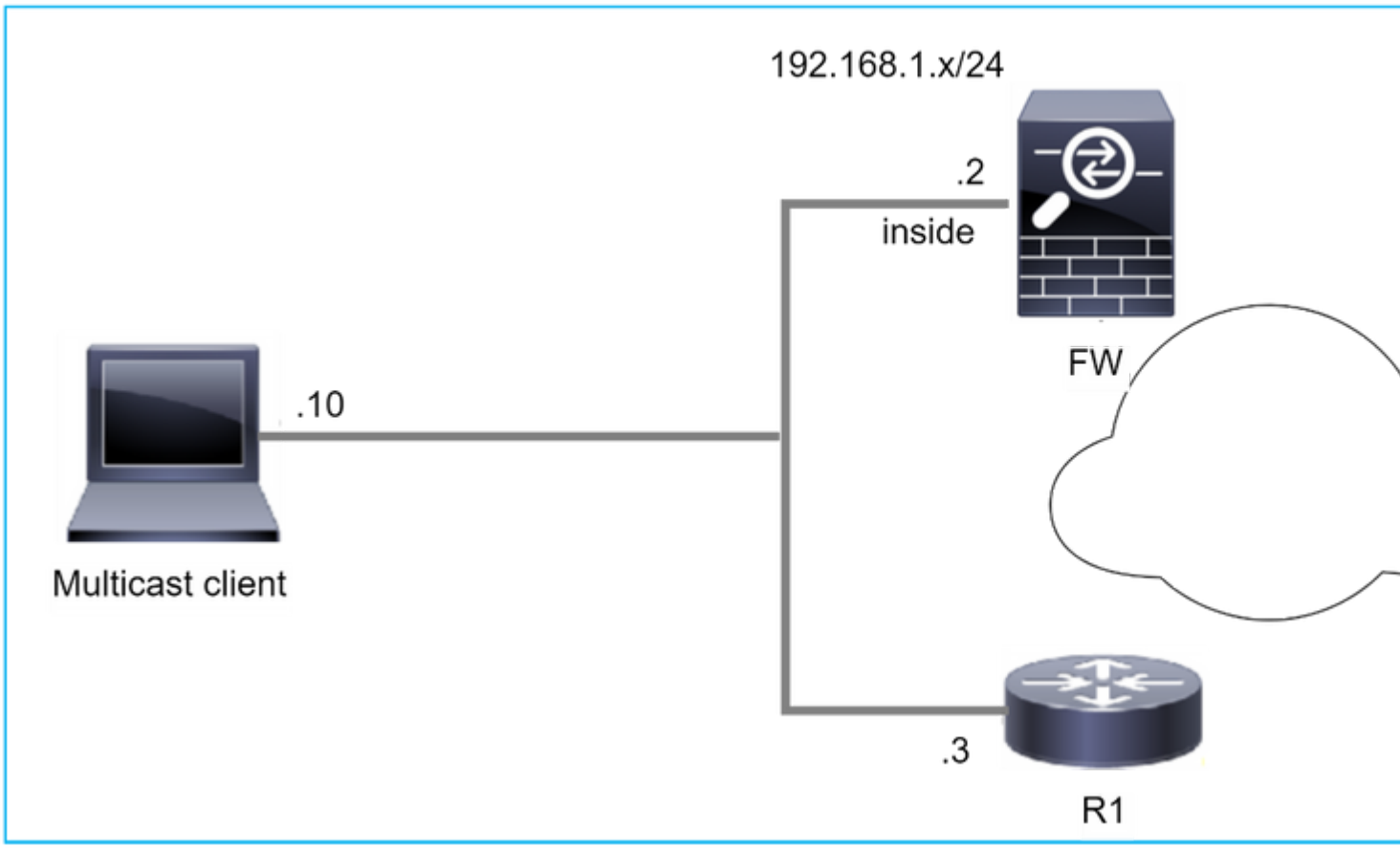
Example:

```
<#root>

firepower#

show run mroute


firepower#

mroute 172.16.1.1 255.255.255.255 192.168.1.2
```

Once the static mroute configuration is in place, for the RPF lookup, the firewall gives preference to the multicast routing table instead of unicast routing table of the ASA and send the PIM messages directly to neighbor 192.168.1.2.

> **Note:** The static mroute is to some extend defeats the usefulness of HSRP redundancy, since the mroute accepts only 1 next-hop per address/netmask combination. If the next hop specified in the mroute command fails or becomes unreachable, the firewall does not fall back to the other router.

Firewall is not Considered as LHR when it is not the DR in the LAN Segment



The firewall has R1 as the PIM neighbors in the LAN segment. R1 is the PIM DR:

```
<#root>

firepower#

show pim neighbor

Neighbor Address  Interface          Uptime    Expires DR pri Bidir

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

If IGMP join request from the client is received, the firewall does not become the LHR.

The mroute shows additional **Null** as the OIL and has the **Pruned** flag:

```
<#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

To make the firewall the LHR, the interface DR priority can be increased.

<#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

The PIM debug command **debug pim** shows this output:

<#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
```

The Pruned flag and the Null are removed from the mroute:

<#root>

firepower#

show mroute

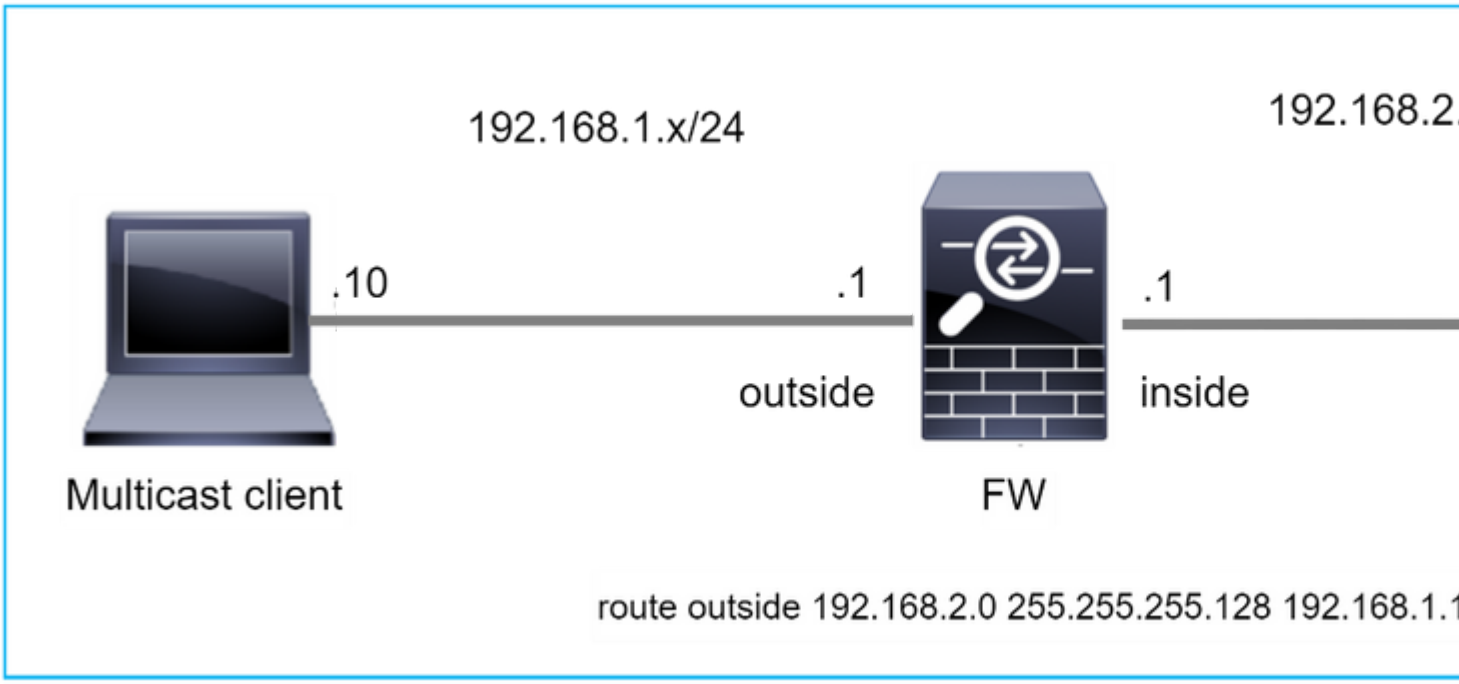
```
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface,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

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

SCJ

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

inside, Forward, 16:48:23/never

Firewall Drops Multicast Packets due to Reverse path Forwarding Check Failure



In this case, the multicast UDP packets are dropped due to RPF failure, as the firewall has more specific route with the mask 255.255.255.128 via the outside interface.

<#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

ASP drop captures show the **rpf-violated** drop reason:

<#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
```

The RPF failed counters in the MFIB output increases:

```
<#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
```

The solution is to fix the RPF check failure. One option is to remove the static route.

If there is no more RPF check failure, the packets are forwarded and the **Forwarding** counter in the MFIB output increases:

<#root>

```
firepower#
```

show mfib 230.1.1.1 count

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

Source: 192.168.2.2,

Forwarding: 1033/9/528/39

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

show mfib 230.1.1.1 count

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

Source: 192.168.2.2,

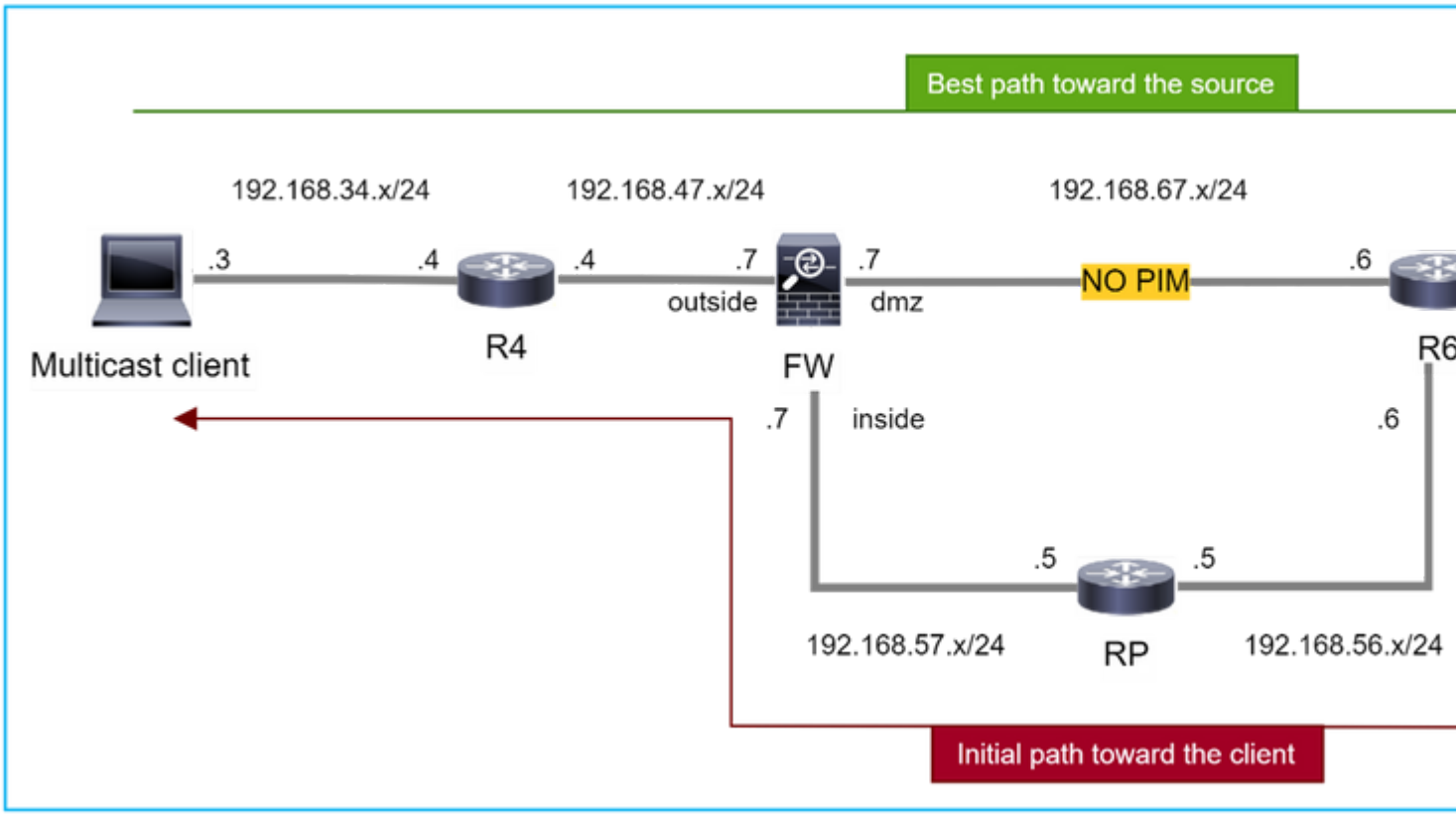
Forwarding: 1044/10/528/41

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

<--- Forward counter increased

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

Firewall does not Generate PIM join upon PIM Switchover to Source-tree



In this case, the firewall learns the path toward the multicast source via the **dmz** interface **R4 > FW > R6**, whereas the initial traffic path from the source to the client is **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 initiates SPT switchover and sends source specific PIM join message once the SPT switchover threshold is reached. In the firewall the SPT switchover does not take place, the (S,G) mroute does not have the **T** flag:

<#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
```

The PIM debug command **debug pim** shows 2 received PIM Join request from the peer R4 â€“ for **(*,G) and (S,G).** The firewall sent PIM Join request for (*,G) upstream, and failed to send source-specific request due to invalid neighbor 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

The **show pim neigbour** commands output lacks 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 is enabled on the firewall interface 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
```

PIM is disabled on the R6 interface:

<#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
```

The solution is to enable PIM on interface GigabitEthernet0/3 on 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**

The firewall installs the T flag, that indicates SPT switchover**:**

<#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 Drops First few Packets due punt rate Limit

When the firewall receives the first packets of a **new** multicast stream in FP, additional processing by the CP can be required. In this case, the FP punts the packets to the CP via SP (FP > SP > CP) for additional operations:

- Creation of a **parent** connection in FP between the ingress interfaces and the identity interfaces.
- Additional multicast-specific checks, such as the RPF validation, PIM encapsulation (in the case if the firewall is the FHR), OIL check, and so on.
- Creation of a (S,G) entry with the incoming and outgoing interfaces in the mroute table.
- Creation of a **child/stub** connection in FP between the incoming and outgoing interfaces.

As part of the control plane protection, the firewall internally limits the rate of packet punted to the CP.

The packets that exceed the rate are dropped in the with the **punt-rate-limit** drop reason:

<#root>

```
firepower#
show asp drop

Frame drop:

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

Use the **show asp cluster counter** command to verify the number of multicast packets punted to CP from SP:

```
<#root>

firepower#
show asp cluster counter

Global dp-counters:

Context specific dp-counters:

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

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

Use **show asp event dp-cp punt** command to verify the number of packets in the FP > CP queue, and the 15-second rate:

```
<#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
```

When the mroute is populated and the parent/child connections are established in the FP, the packets are forwarded in the FP as part of the existing connections. In this case, FP does not punt the packets to the CP.

How the firewall processes the first packets of a new multicast stream?

When the firewall receives the first packets of a **new** multicast stream in datapath, the firewall takes these actions:

1. Checks if the security policy allows packets.
2. Punts the packets to the CP via path FP.
3. Creates a **parent** connection between the ingress interfaces and the identity interfaces:

<#root>

```
firepower#
```

```
show capture capi packet-number 1 trace
```

```
10 packets captured
```

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

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

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

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


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

Config:
Implicit Rule
Additional Information:

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

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

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

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

Phase: 9

Type: MULTICAST

Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 10

Type: FLOW-CREATION

Subtype:
Result: ALLOW
Config:
Additional Information:

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

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

Action: allow

Syslogs:

<#root>

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

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

This connection is visible in the output of the **show conn all** command:

<#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. The CP engages the multicast process for additional multicast-specific checks, such as the RPF validation, PIM encapsulation (in the case if the firewall is the FHR), OIL check, and so on.
5. The CP creates an (S,G) entry with the incoming and outgoing interfaces in the mroute:

<#root>

```
firepower#
```

show mroute

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

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

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

```
  Incoming interface: inside


  RPF nbr: 192.168.2.1
  Immediate Outgoing interface list:
    outside, Forward, 00:00:32/00:02:57
```

6. The CP instructs the FP via CP > SP > FP path to create a **child/stub** connection between the incoming and outgoing interfaces:

This connection is visible only in the output of the **show local-host** command:

<#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
```

In the software versions with the fix of the Cisco bug ID CSCwe21280 , the syslog message 302015 for the child/stub connection is also generated:

<#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
```

When both parent and child/stub connections are established, the ingress packets match the existing connection and forwarded in 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
```

Filter ICMP Multicast Traffic

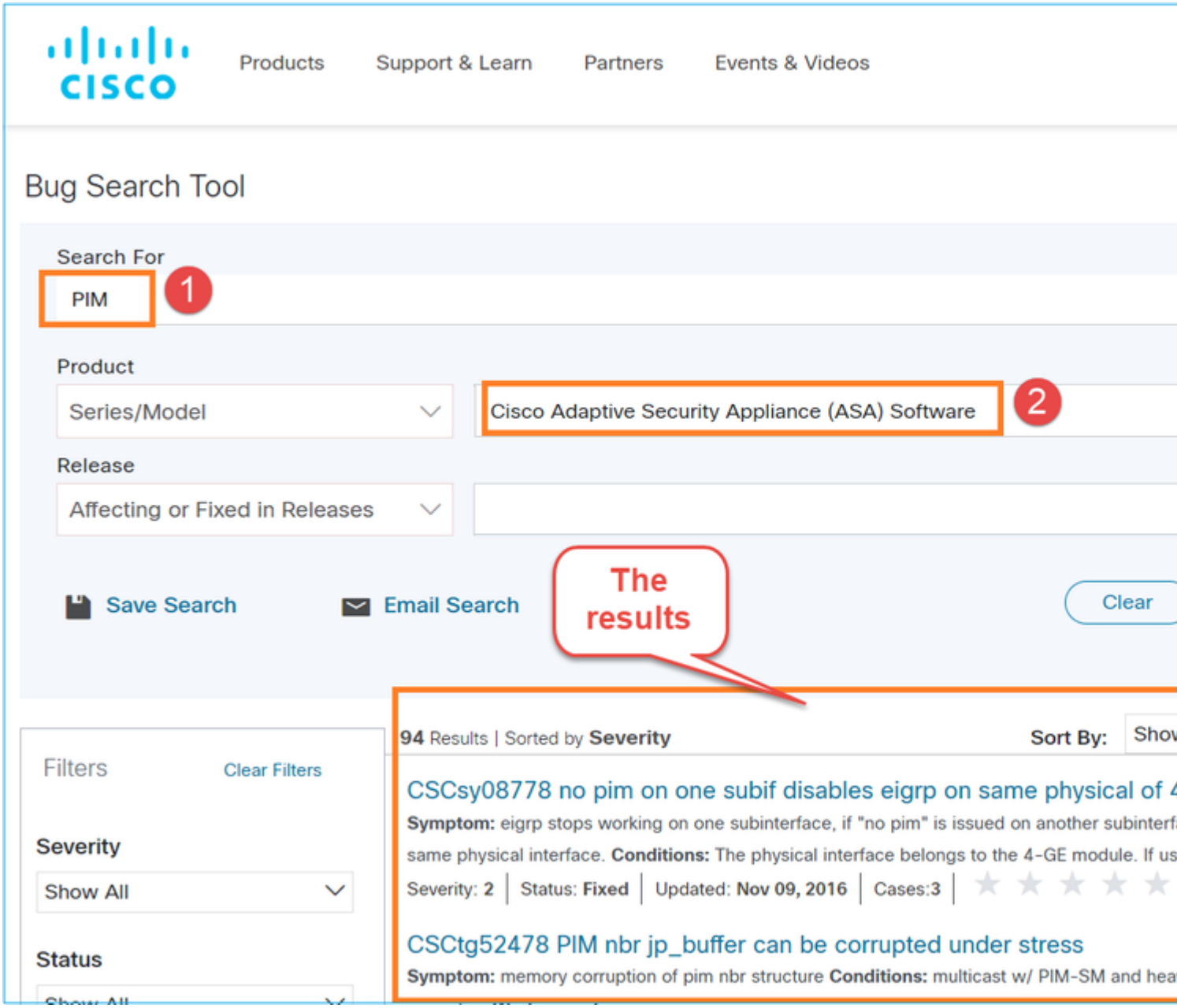
You cannot filter ICMP Multicast traffic with an ACL. You have to use Control Plane policy (ICMP):

Cisco bug ID CSCsl26860 ASA does not filter multicast ICMP packets

Known PIM Multicast Defects

You can use the Bug Search Tool for known defects: https://bst.cloudapps.cisco.com/bugsearch

Most ASA and FTD defects are listed under the 'Cisco Adaptive Security Appliance (ASA) Software' Product:



Related Information

- ASA Multicast Troubleshooting and Common Problems
- Firepower Management Center Multicast
- Summary of the Firepower Multicast Flags