排除Firepower威胁防御和ASA组播PIM故障

目录

简介

本文档介绍Firepower威胁防御(FTD)和自适应安全设备(ASA)如何实施协议无关组播(PIM)。

先决条件

要求

基本IP路由知识。

使用的组件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

本文档中的信息基于以下软件和硬件版本：

- 思科Firepower 4125威胁防御版本7.1.0。
- Firepower管理中心(FMC)版本7.1.0。
- 思科自适应安全设备软件版本9.17(1)9。

背景信息

组播路由基础知识

- 单播将数据包转发到目的地，而组播将数据包转发到远离源的位置。
- 组播网络设备（防火墙/路由器等）通过反向路径转发(RPF)转发数据包。请注意，RPF与单播中用于防止特定类型攻击的uRPF不同。RPF可以定义为一种机制，将组播数据包从源转发到通向组播接收器的接口。它的主要作用是防止流量环路和确保正确的流量路径。
- PIM等组播协议有3项主要功能：

1.查找上游接口（距离源最近的接口）。

2.查找与特定组播流（指向接收器的接口）关联的下游接口。

3.维护组播树（添加或删除树分支）。

- 组播树可通过以下两种方法之一构建和维护：隐式联合（泛洪和修剪）或显式联合（拉模型）。PIM密集模式(PIM-DM)使用隐式联合，而PIM稀疏模式(PIM-SM)使用显式联合。
- 组播树可以是共享，也可以是基于源的：
  - 共享树使用交汇点(RP)的概念，并记为(*, G)，其中G =组播组IP。
  - 基于源的树在源位置植根，不使用RP，并且标记为(S， G),其中S =组播源/服务器的IP。
- 组播转发模型：
  - 任意源组播(ASM)传输模式使用共享树(*, G)，其中任何源都可以发送组播流。
  - 源特定组播(SSM)使用基于源的树(S、G)和IP范围232/8。
  - 双向(BiDir)是一种共享树(*, G)，控制平面和数据平面流量均通过RP。
- 可以使用以下方法之一配置或选择交汇点：
  - 静态RP
  - 自动RP
  - Bootstrap路由器(BSR)

PIM模式摘要

PIM 模式	RP	共享树	记法	IGMP	支持ASA/FTD
PIM 稀疏模式	Yes	Yes	(*, G)和(S， G)	v1/v2/v3	Yes

PIM 密集模式	无	无	(S、G)	v1/v2/v3	否*
PIM双向模式	Yes	Yes	(*, G)	v1/v2/v3	Yes
PIM源特定组播(SSM)模式	无	无	(S、G)	v3	否**

*自动RP =自动RP流量可以通过

** ASA/FTD不能是最后一跳设备

RP配置摘要

交汇点配置	ASA/FTD
静态RP	Yes
自动RP	否，但自动RP控制平面流量可以通过
BSR	是，但不支持C-RP

注：在开始排除任何组播问题之前，必须清晰地了解组播拓扑。具体来说，您至少需要知道：
— 防火墙在组播拓扑中扮演什么角色？
-RP是谁？
— 组播流的发送者是谁（源IP和组播组IP）？
— 组播流的接收者是谁？
— 控制平面(IGMP/PIM)或数据平面（组播流）本身是否有问题？

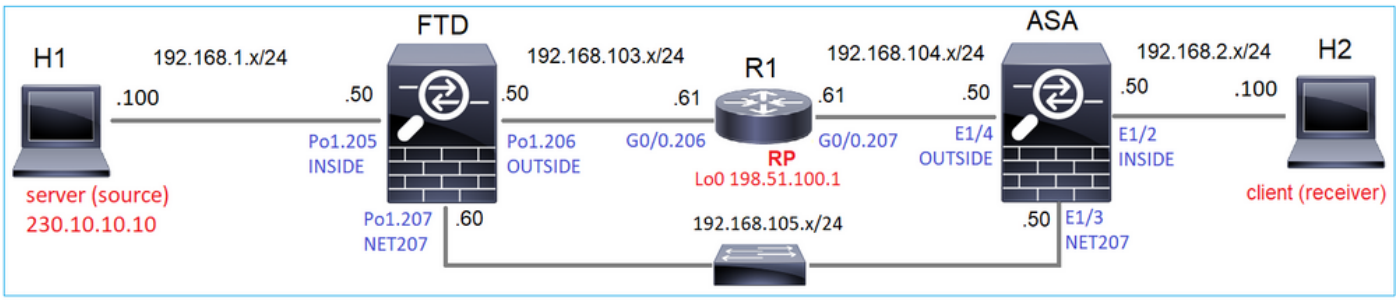
缩写/缩写

缩写词	说明
FHR	第一跳路由器 — 直接连接到组播流量源的一跳。
LHR	最后一跳路由器 — 直接连接到组播流量接收器的跳。

RP	交汇点
DR	指定路由器
SPT	最短路径树
RPT	交汇点(RP)树、共享树
RPF	反向路径转发
石油	传出接口列表
MRIB	组播路由信息库
MFIB	组播转发信息库
ASM	任意源组播
BSR	Bootstrap路由器
SSM	源特定组播
FP	快速路径
服务提供商	慢速路径
CP	控制点
PPS	每秒数据包速率

任务1 - PIM稀疏模式（静态RP）

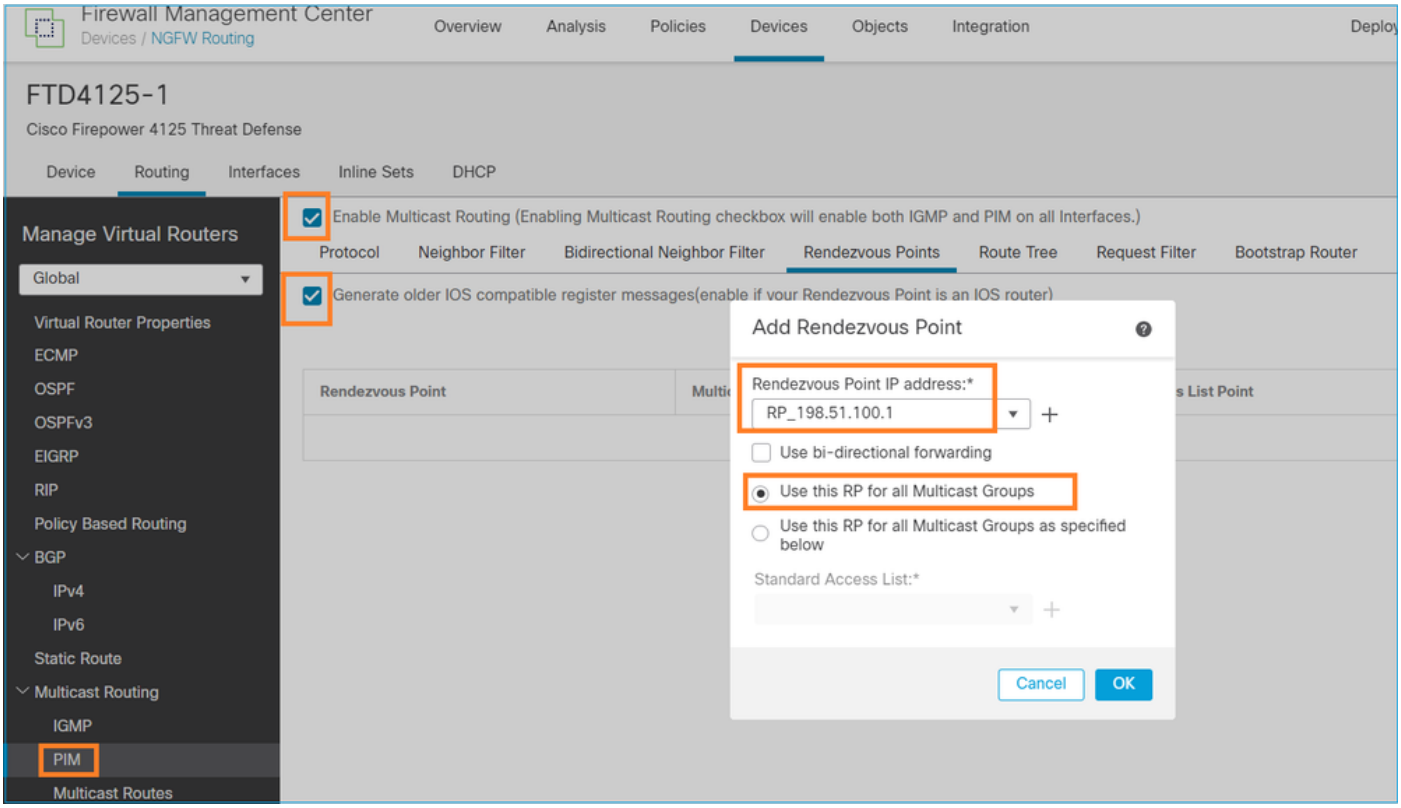
拓扑



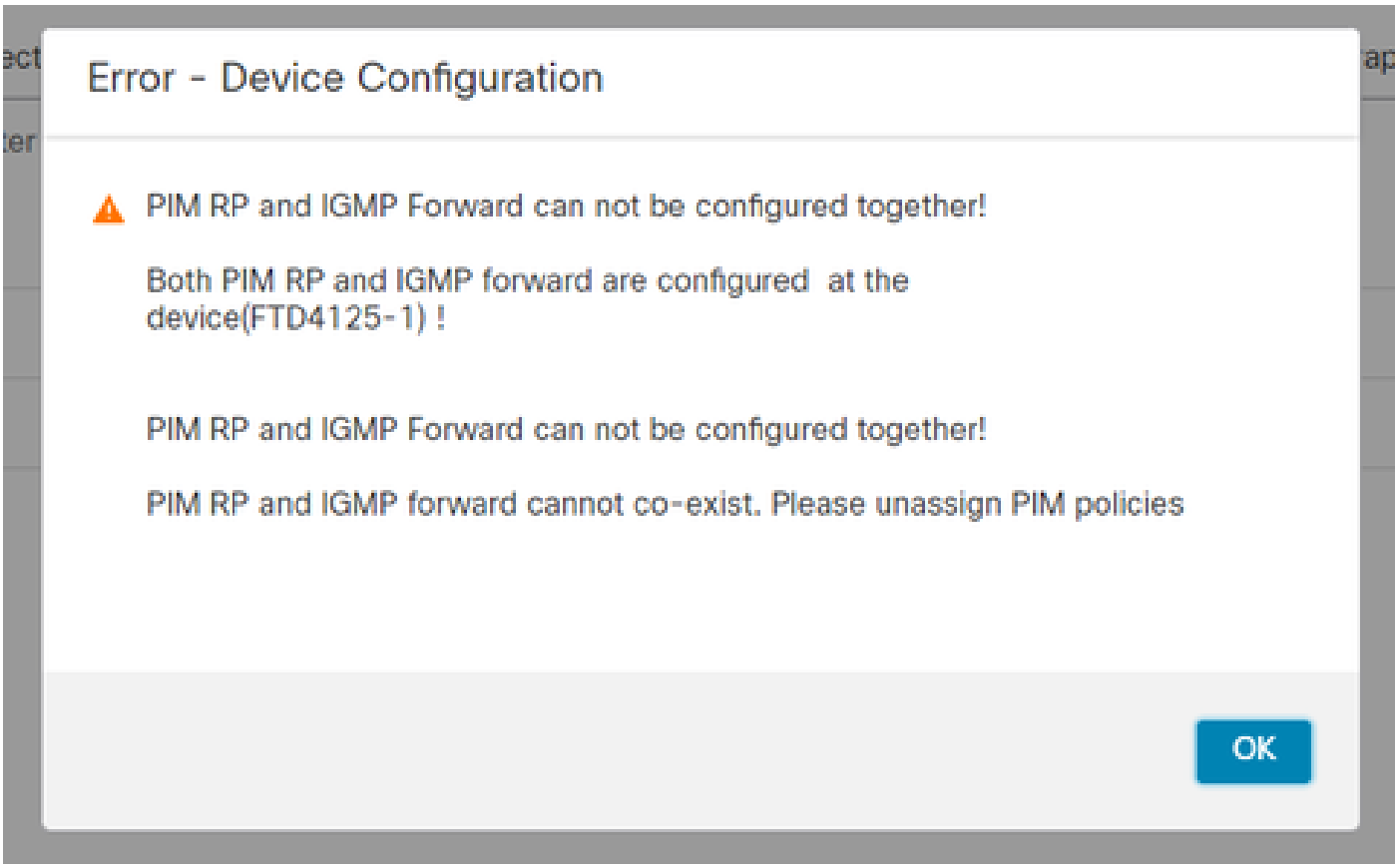
在拓扑中配置组播PIM稀疏模式，将R1(198.51.100.1)配置为RP。

解决方案

FTD配置：



无法同时为IGMP末节路由和PIM配置ASA/FTD:



FTD上的结果配置：

```
<#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
```

在ASA防火墙上有一个类似的配置：

```
<#root>

asa(config)#

multicast-routing


asa(config)#

pim rp-address 198.51.100.1
```

RP配置（思科路由器）：

```
<#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
```

确认

当没有组播流量（发送方或接收器）时，验证FTD上的组播控制平面：

```
<#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
```

验证PIM邻居：

```
<#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)
```

RP通告整个组播组范围：

```
<#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
```

防火墙mroute表包含一些不相关的条目(239.255.255.250是MAC OS和Microsoft Windows等供应商使用的简单服务发现协议(SSDP)):

<#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
```

防火墙和RP之间构建了一个PIM隧道：

<#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
```

PIM隧道也可以在防火墙连接表中看到：

<#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
```

ASA防火墙验证：

```
<#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（思科路由器）RP验证。SSDP和自动RP有一些组播组：

```
<#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
```

接收方宣布其存在时进行验证

注：本节中显示的防火墙命令完全适用于ASA和FTD。

ASA获取IGMP成员身份报告消息并创建IGMP和mroute(*, G)条目：

```
<#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
```

ASA防火墙为组播组创建mroute:

```
<#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
```

另一个防火墙验证是PIM拓扑输出：

```
<#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
```

注：如果防火墙没有指向RP的路由，则debug pim输出显示RPF查找失败

---

debug pim 输出中的RPF查找失败：

<#root>

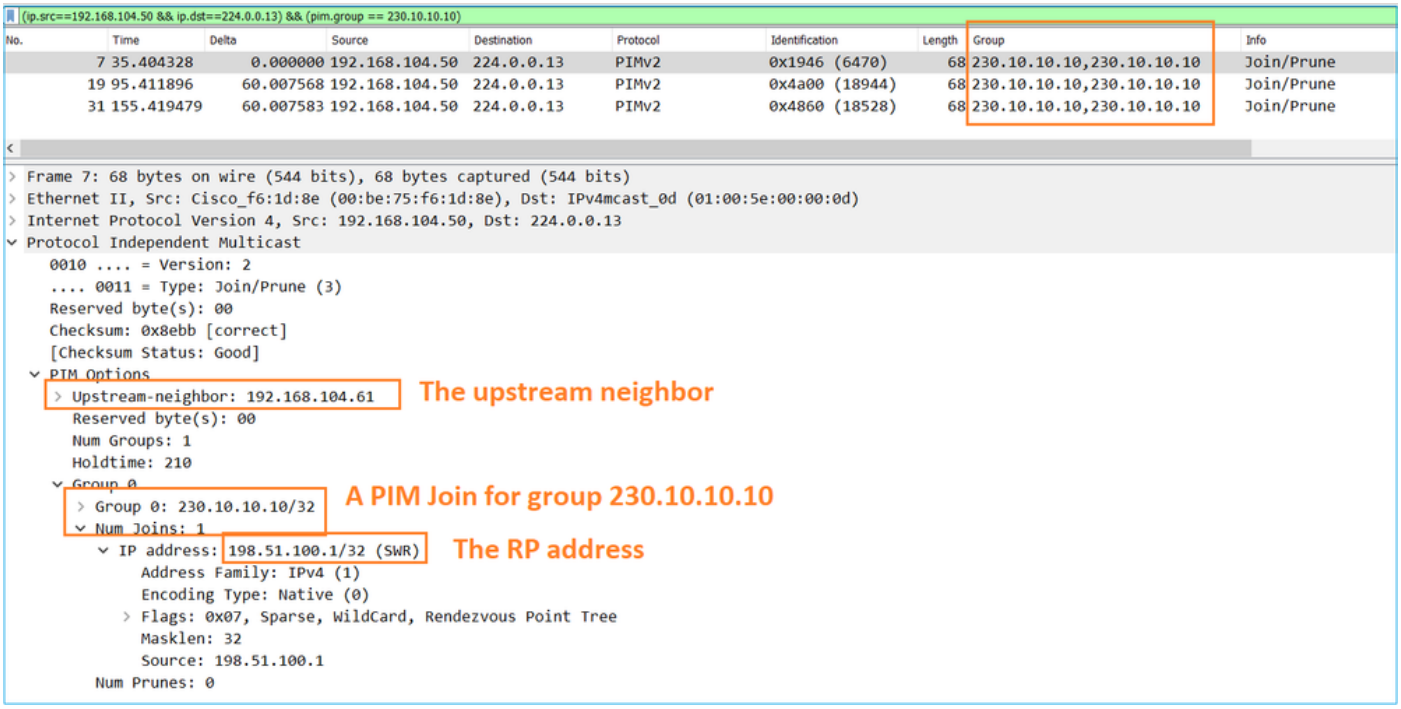
```
asa#

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
```

如果一切正常，防火墙会向RP发送PIM加入修剪消息：

<#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
```

捕获显示PIM加入消息每1分钟发送一次，PIM Hello每30秒发送一次。PIM使用IP 224.0.0.13:



提示：Wireshark显示过滤器：(ip.src==192.168.104.50 && ip.dst==224.0.0.13)&&(pim.group == 230.10.10.10)

- 192.168.104.50是出口接口（指向上游PIM邻居）的防火墙IP
- 224.0.0.13是发送PIM加入和修剪的PIM组播组
- 230.10.10.10是我们发送PIM加入/修剪的组播组

RP创建(*, G)mroute。请注意，由于尚未有任何服务器，因此传入接口为空：

<#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

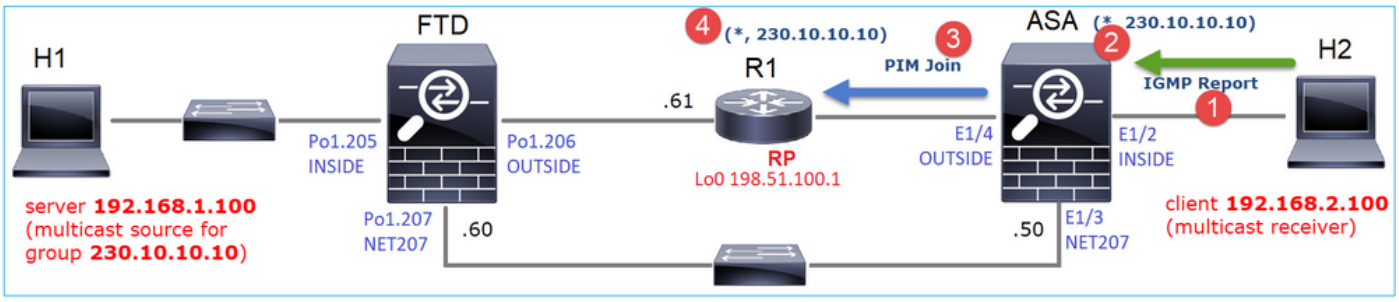
Outgoing interface list:

GigabitEthernet0/0.207

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

<-- There was a PIM Join on this interface

上述内容可以图形表示为：



1. 在ASA上收到IGMP报告。
2. 添加了(*, G)mroute。
3. ASA向RP(198.51.100.1)发送PIM加入消息。
4. RP收到加入消息并添加(*, G)mroute。

同时，在FTD上，由于未收到IGMP报告或PIM加入，因此没有任何mroutes:

```
<#root>

firepower#

show mroute 230.10.10.10

No mroute entries found.
```

服务器发送组播流时的验证

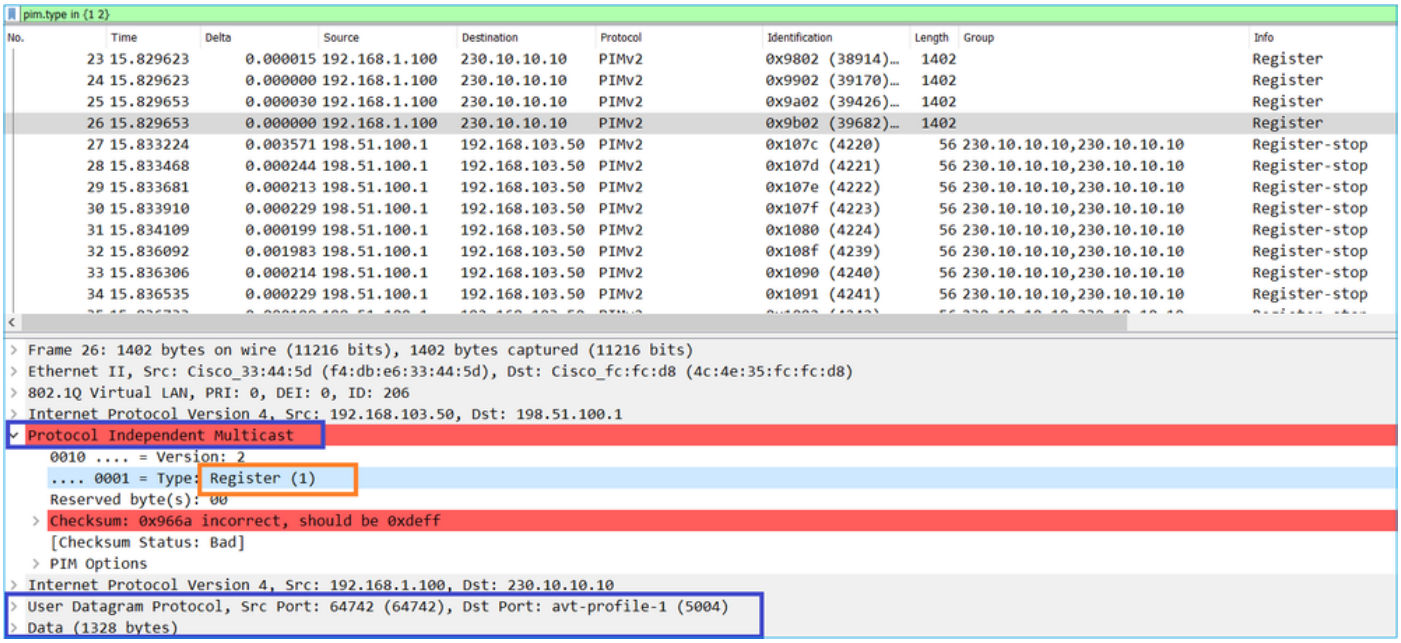
FTD从H1获取组播流，并启动RP的PIM注册过程。FTD向RP发送单播PIM注册消息。RP向第一跳路由器（在本例中为FTD）发送PIM Join消息以加入组播树。然后发送Register-Stop消息。

```
<#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
```

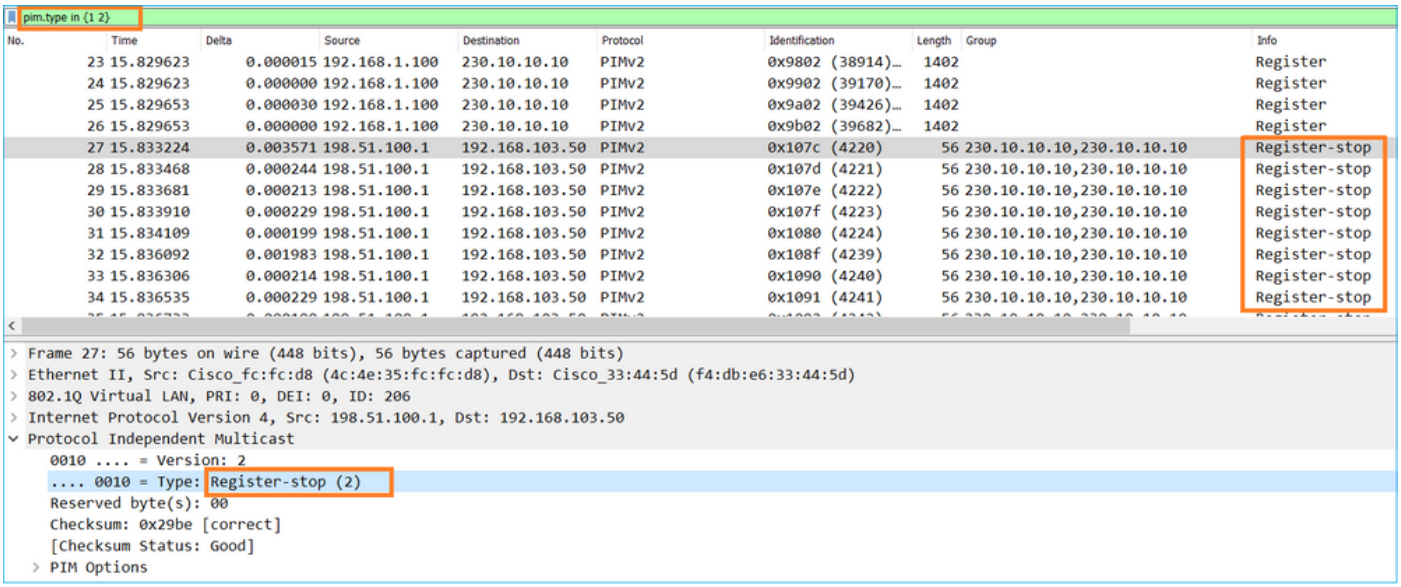
```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify NS
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) MRIB modify DC
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify A NS
IPv4 PIM: (192.168.1.100,230.10.10.10) Set alive timer to 210 sec
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) 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)
```

PIM Register消息是PIM消息，它将UDP数据与PIM Register信息一起传输：



PIM Register-Stop消息：



提示：要在Wireshark上仅显示PIM注册和PIM注册停止消息，可以使用显示筛选器：pim.type in {1 2}

防火墙（最后一跳路由器）获取接口OUTSIDE上的组播流，并启动到接口NET207的最短路径树(SPT)切换：

<#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)
```

发生切换时FTD上的PIM调试：

<#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

SPT切换开始后，FTD将路由：

<#root>

```
firepower#
```

show mroute 230.10.10.10

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

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

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

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

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

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

Tunnel0, Forward, 00:00:06/never

在SPT切换结束时，FTD的OIL中仅显示NET207接口：

<#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

在最后一跳路由器(ASA)上，还设置SPT位：

<#root>

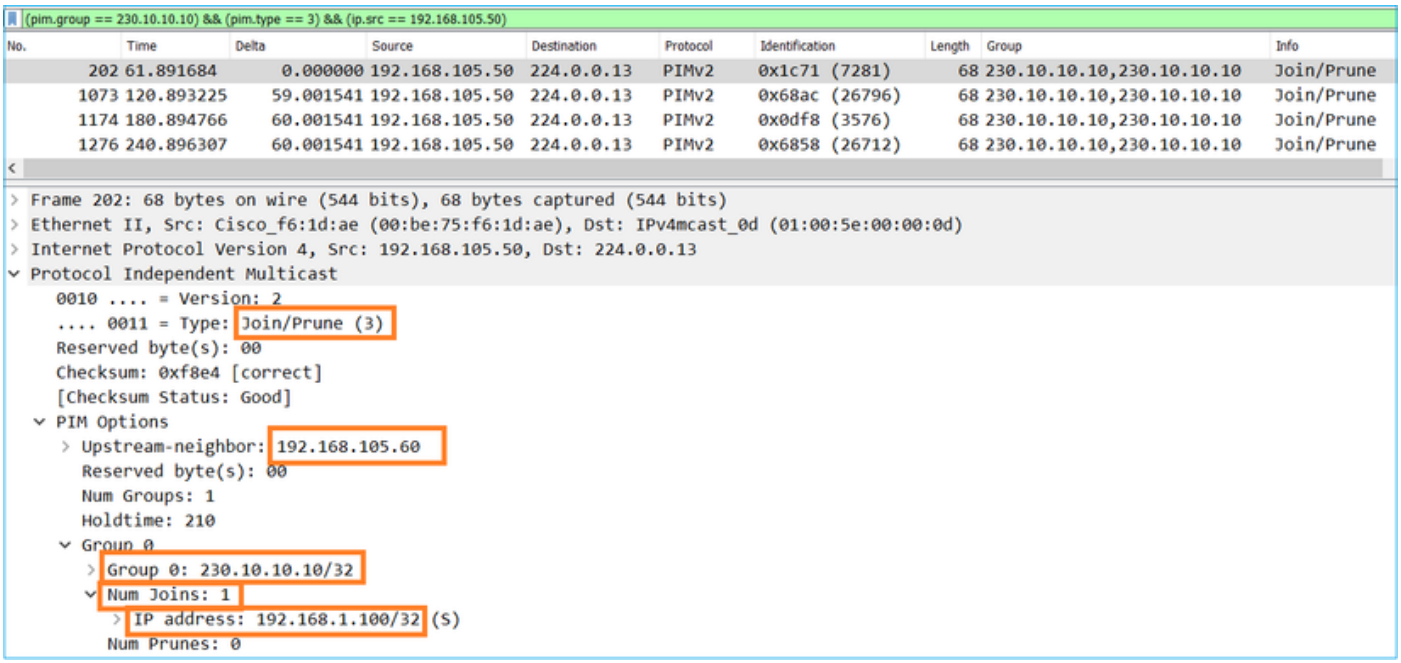
asa#

show mroute 230.10.10.10

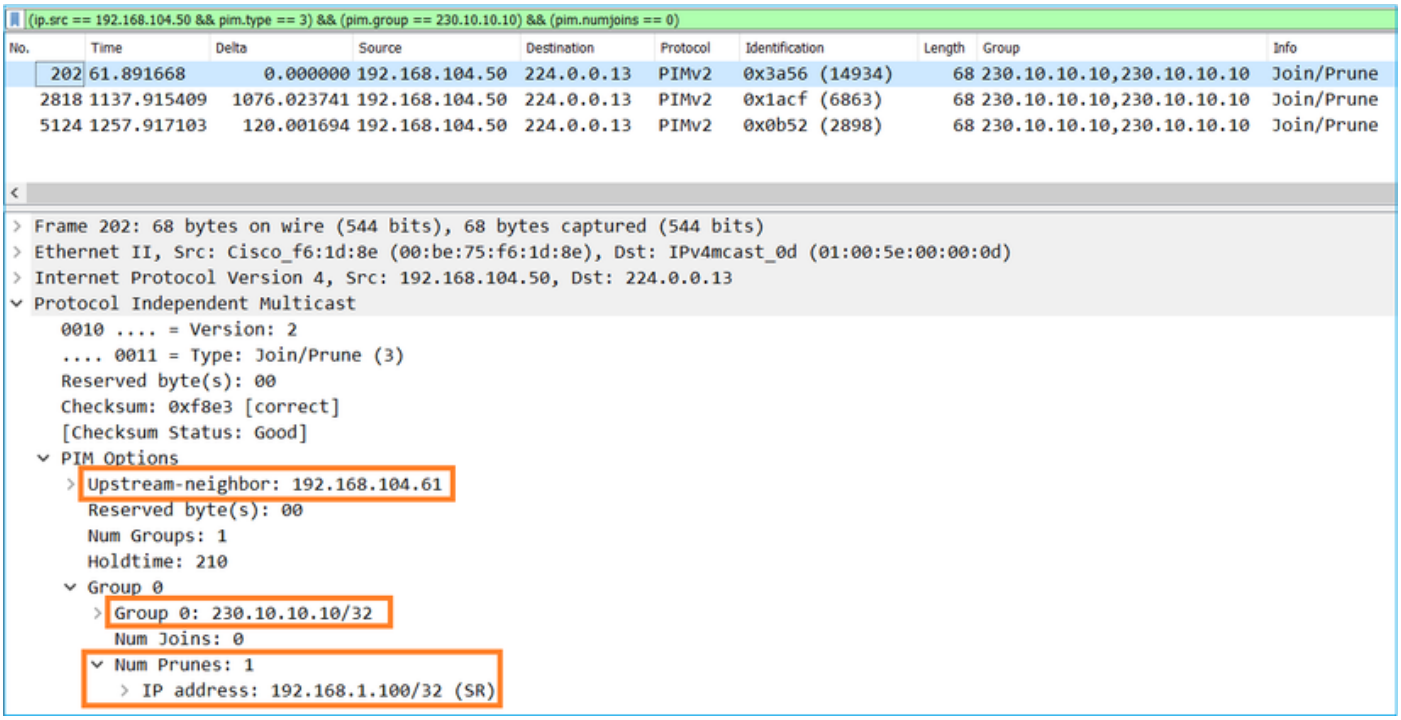
```
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface,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

从ASA NET207接口（执行切换的第一跳路由器）进行切换。PIM加入消息发送到上游设备(FTD):



在OUTSIDE接口上，会向RP发送PIM修剪消息以停止组播流：



验证PIM流量：

<#root>

firepower#

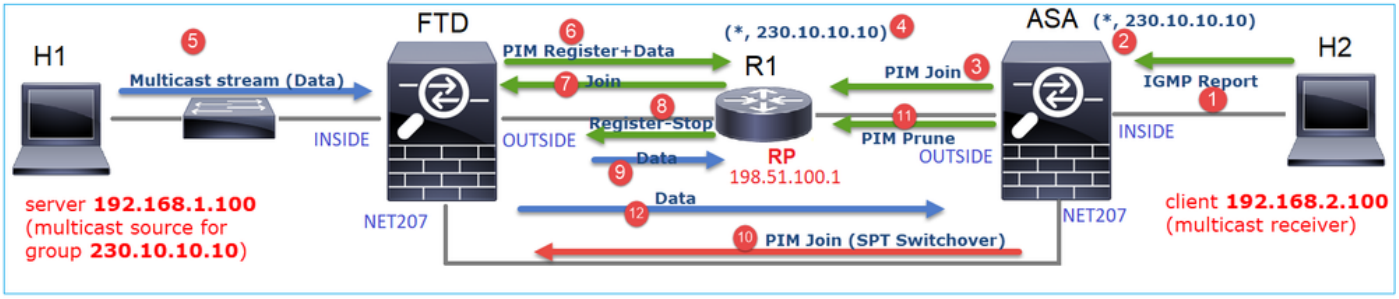
show pim traffic

```
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
```

要验证在慢速路径与快速路径与控制点中处理的数据包数量，请执行以下操作：

```
<#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 atte
MCAST_SP_PKTS_TO_FP_FWD                 109      Number of multicast packets that skip over punt rule an
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_h
MCAST_FP_CHK_FAIL_NO_ACCEPT_IFC         223847   Number of multicast packets failed with no accept inter
MCAST_FP_CHK_FAIL_NO_SEQ_NO_MATCH       131      Number of multicast packets failed with no matched sequ
MCAST_FP_CHK_FAIL_NO_FP_FWD             313584   Number of multicast packets that cannot be fast-path fo
MCAST_FP_UPD_FOR_UNMATCH_IFC            91       Number of times that multicast flow's ifc_out  cannot b
```

显示分步执行的操作的图：



1. 终端主机(H2)发送IGMP报告以加入组播流230.10.10.10。
2. 作为PIM DR的最后一跳路由器(ASA)创建一个(*, 230.10.10.10)条目。
3. ASA向RP发送组230.10.10.10的PIM加入消息。
4. RP会创建(*, 230.10.10.10)条目。
5. 服务器发送组播流数据。
6. FTD将组播数据包封装在PIM注册消息中，然后将其发送（单播）到RP。此时，RP发现自己有一个活动接收器，解封组播数据包，然后将其发送到接收器。
7. RP向FTD发送PIM加入消息以加入组播树。
8. RP向FTD发送PIM注册 — 停止消息。
9. FTD向RP发送本地组播流（无PIM封装）。
10. 最后一跳路由器(ASA)发现源(192.168.1.100)具有来自NET207接口的更好路径并开始切换。

它向上游设备(FTD)发送PIM加入消息。

11. 最后一跳路由器向RP发送PIM修剪消息。
12. FTD将组播流转发到NET207接口。ASA从共享树（RP树）移至源树(SPT)。

任务2 — 配置PIM引导路由器(BSR)

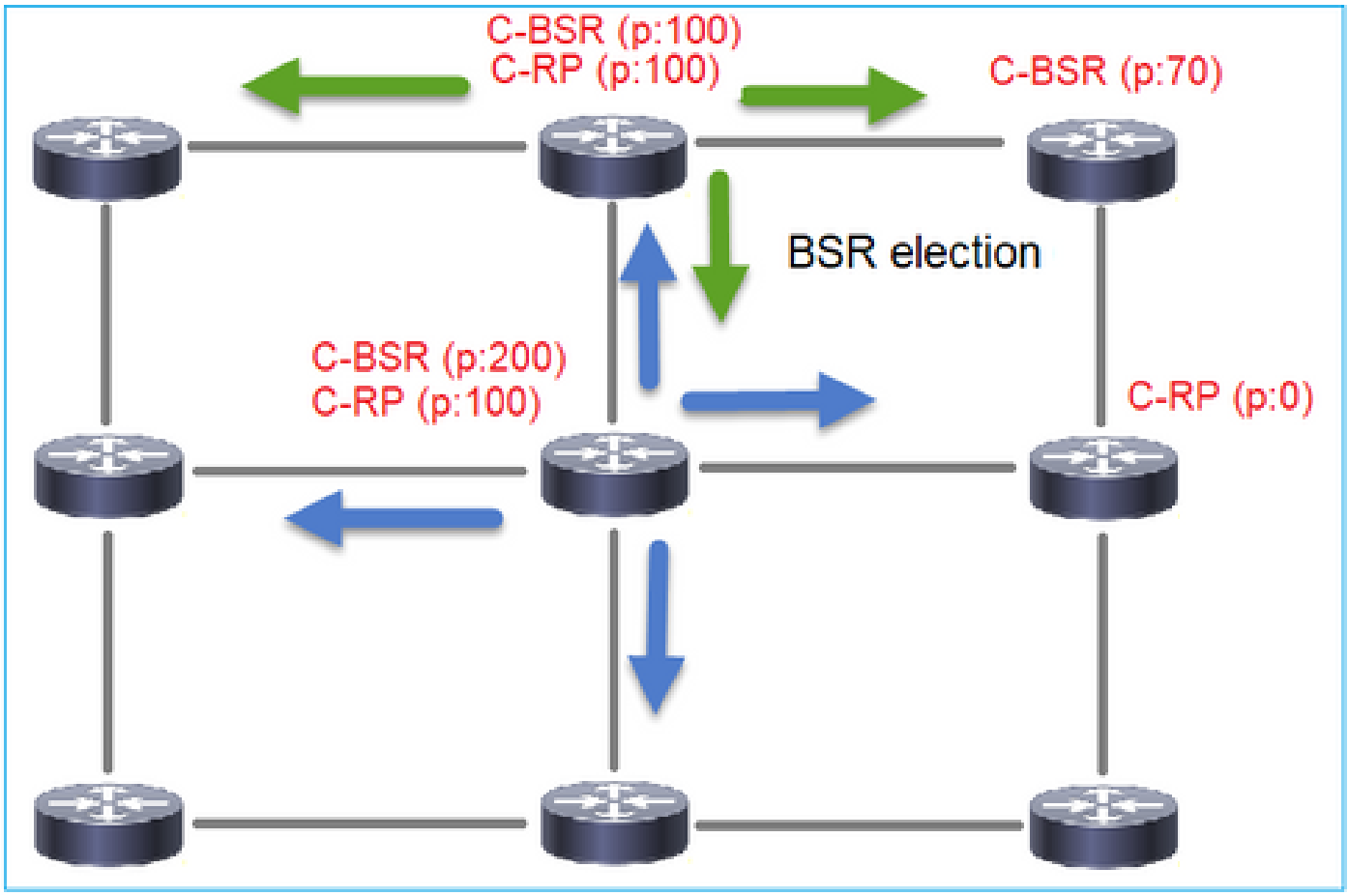
BSR基础知识

- BSR(RFC 5059)是使用PIM协议并允许设备动态获取RP信息的控制平面组播机制。
- BSR定义：
  - 候选RP(C-RP)：想要成为RP的设备。
  - 候选BSR(C-BSR)：想要成为BSR并向其他设备通告RP集的设备。
  - BSR：在许多C-BSR中选择了BSR的设备。最高的BSR优先级会赢得选举。
  - RP-set：所有C-RP及其优先级的列表。
  - RP：具有最低RP优先级的设备会赢得选举。
  - BSR PIM消息（空）：用于BSR选举的PIM消息。
  - BSR PIM消息（正常）：发送到224.0.0.13 IP并包含RP集和BSR信息的PIM消息。

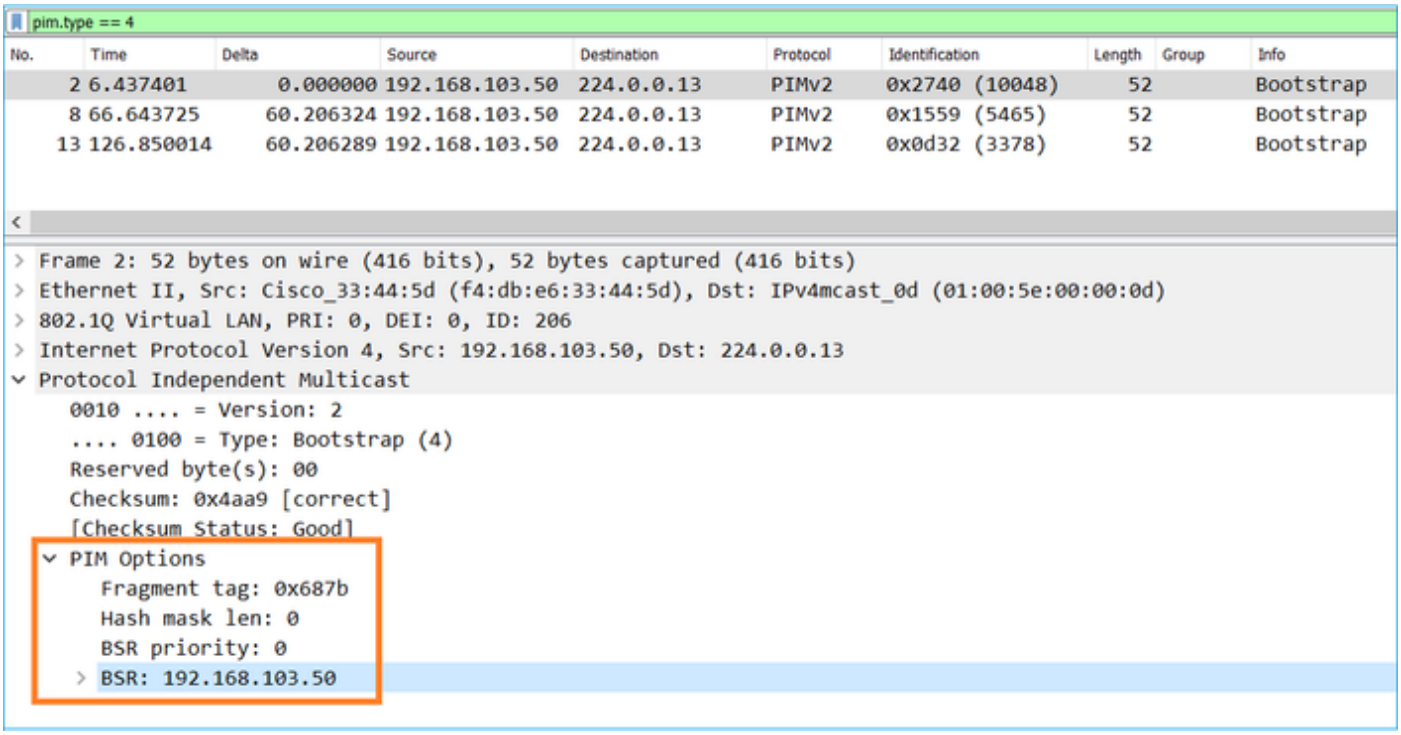
BSR的工作原理

1. BSR选举机制。

每个C-BSR发送包含优先级的PIM BSR空消息。具有最高优先级（回退为最高IP）的设备将赢得选举并成为BSR。其余设备不再发送任何空BSR消息。

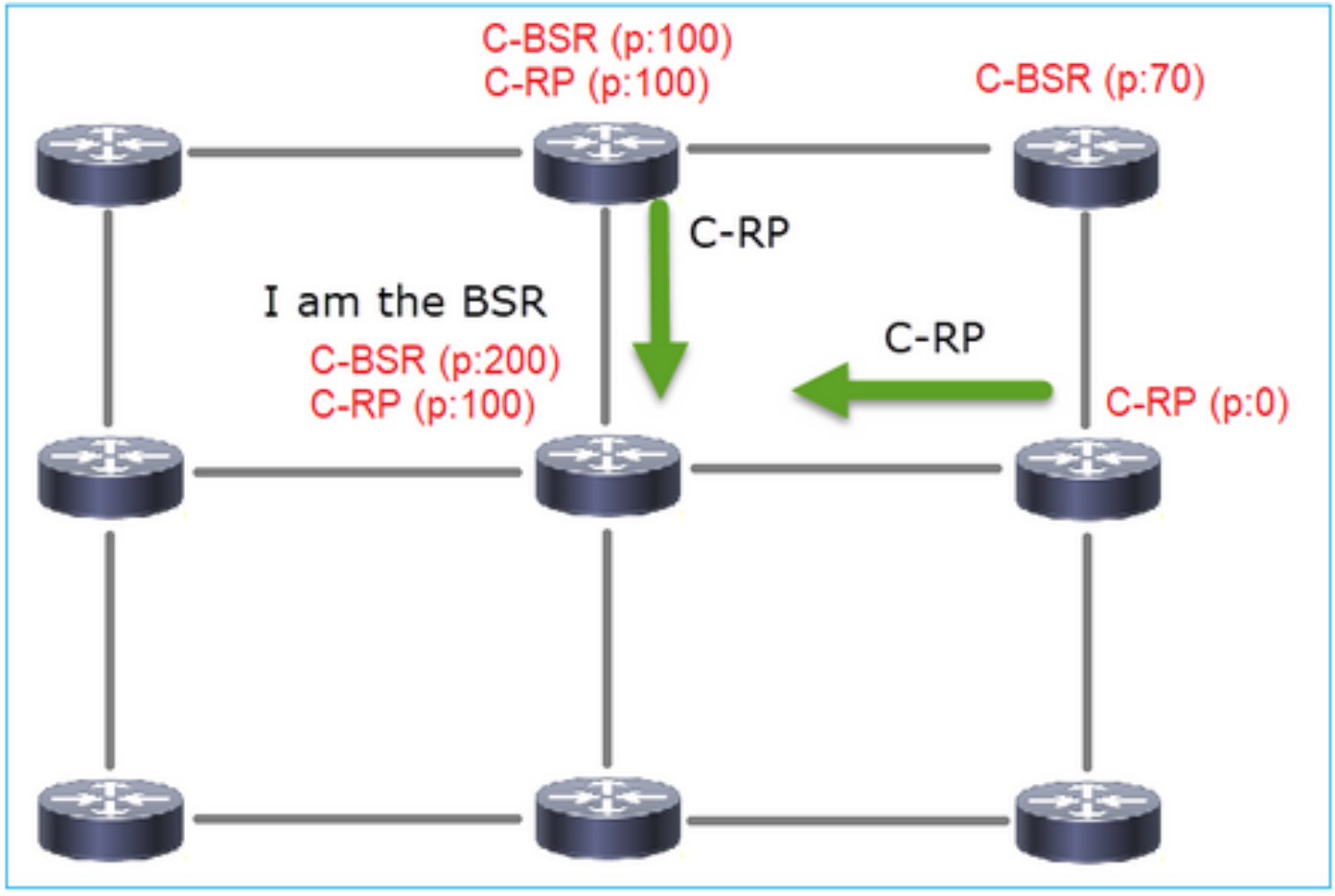


选举过程中使用的BSR消息仅包含C-BSR优先级信息：

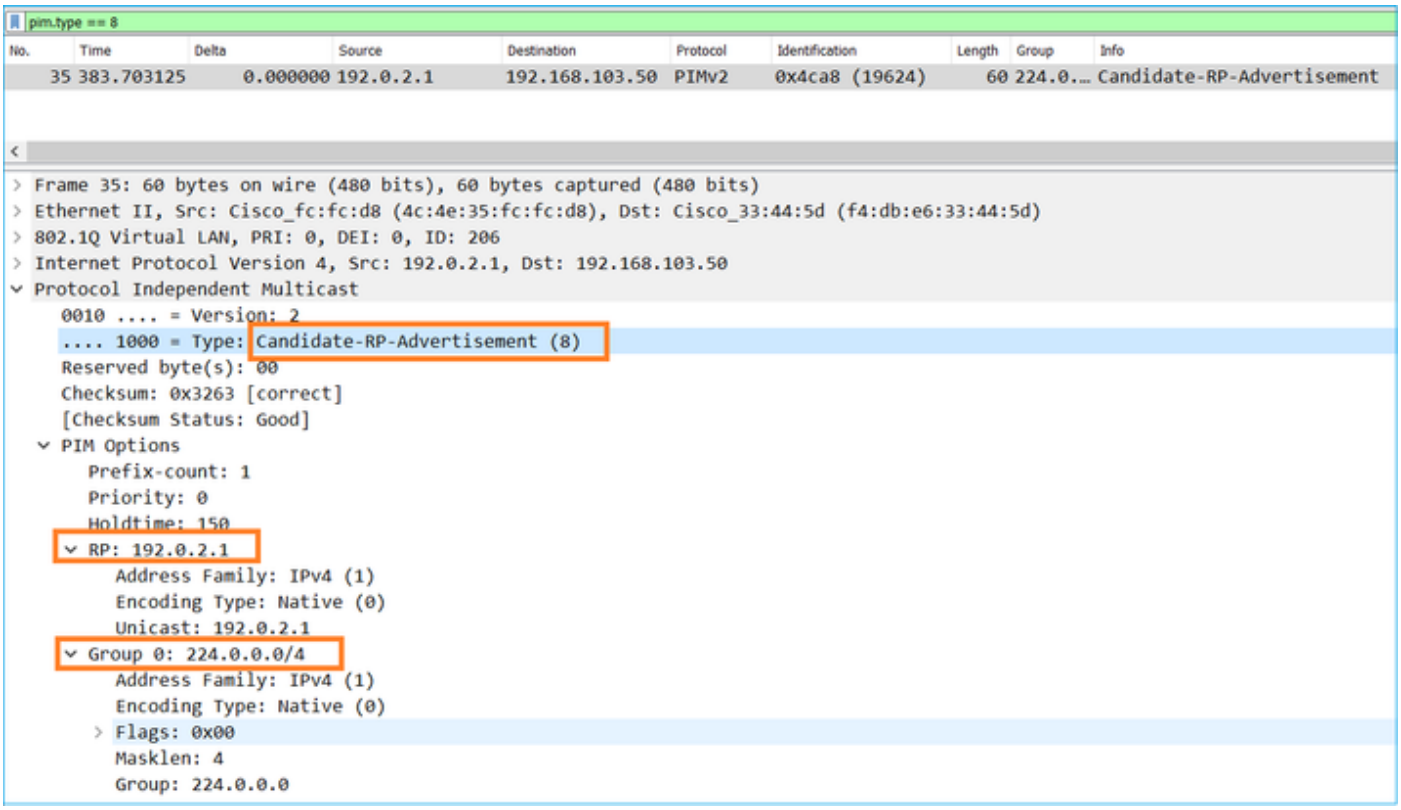


要在Wireshark中显示BSR消息，请使用此显示过滤器：pim.type == 4

2. C-RP向包含其C-RP优先级的BSR发送单播BSR消息：

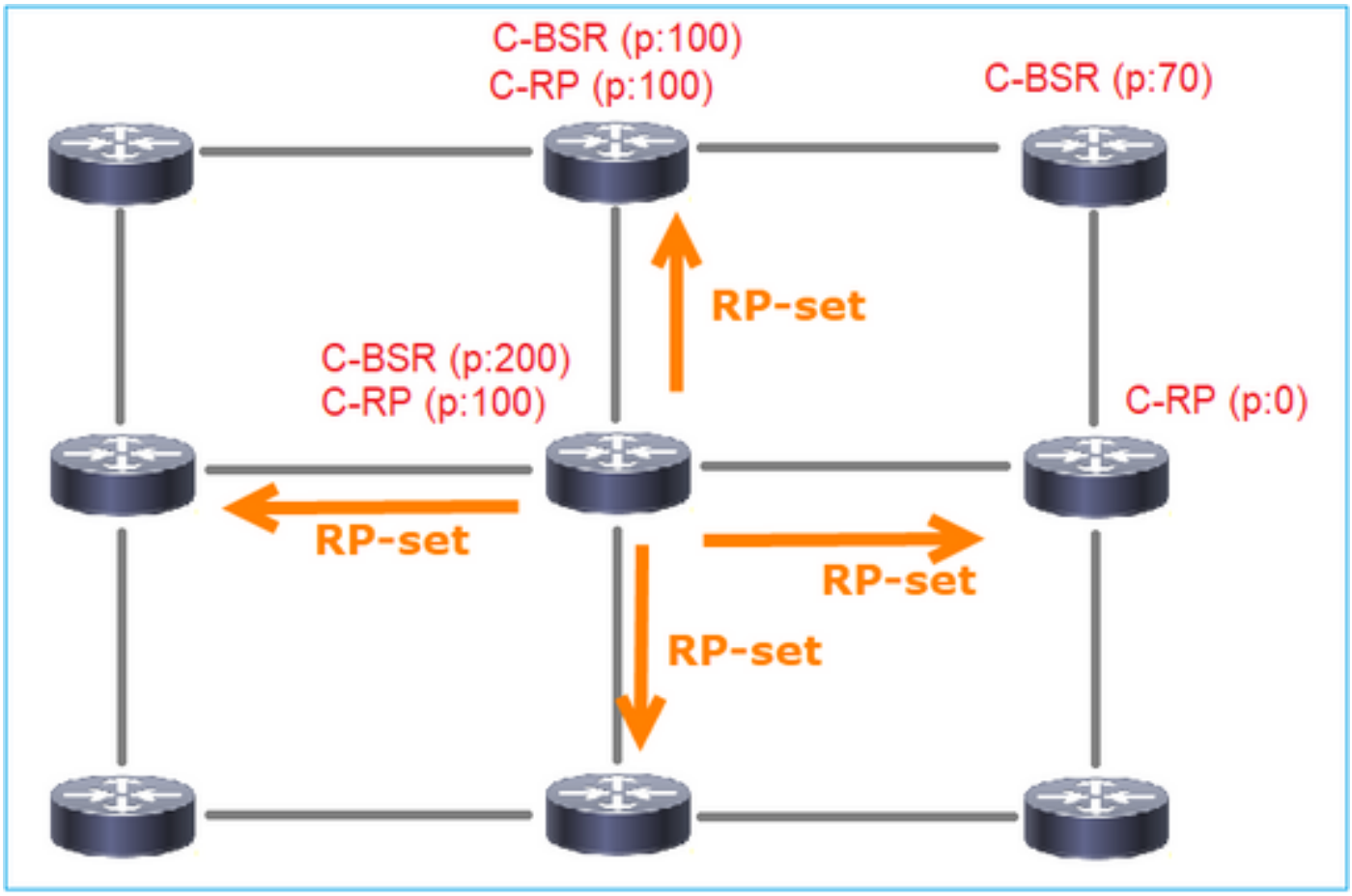


候选RP消息：



要在Wireshark中显示BSR消息，请使用此显示过滤器：pim.type == 8

3. BSR构成RP集并将其通告给所有PIM邻居：

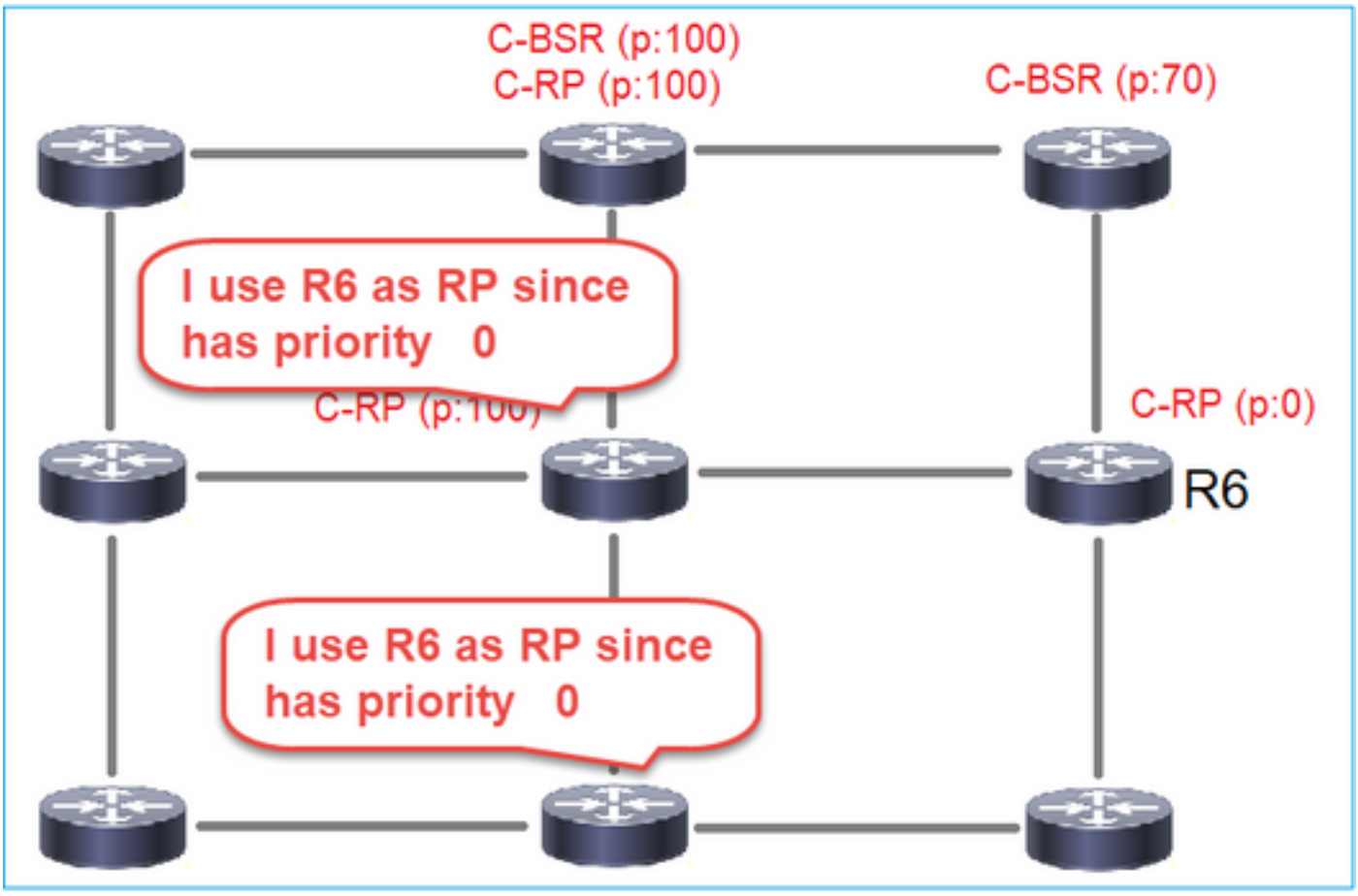


(ip.src == 192.168.105.60) && (pim.type == 4)

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	Bootstrap

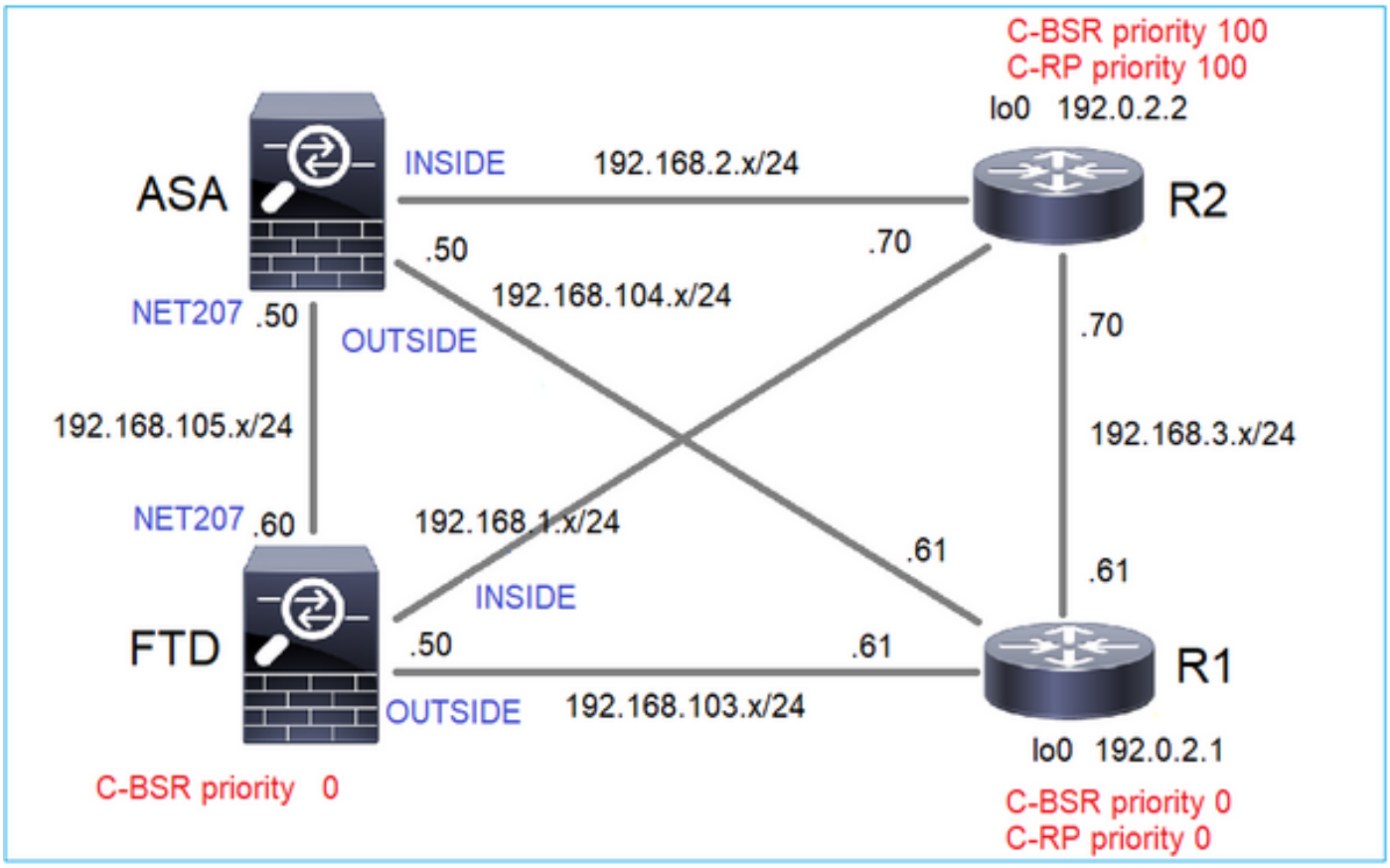
```
> Frame 152: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
> Ethernet II, Src: Cisco_33:44:5d (f4:db:e6:33:44:5d), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
> 802.1Q Virtual LAN, PRI: 6, DEI: 0, ID: 207
> Internet Protocol Version 4, Src: 192.168.105.60, Dst: 224.0.0.13
v Protocol Independent 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.路由器/防火墙获取RP集并根据最低优先级选择RP:



任务要求

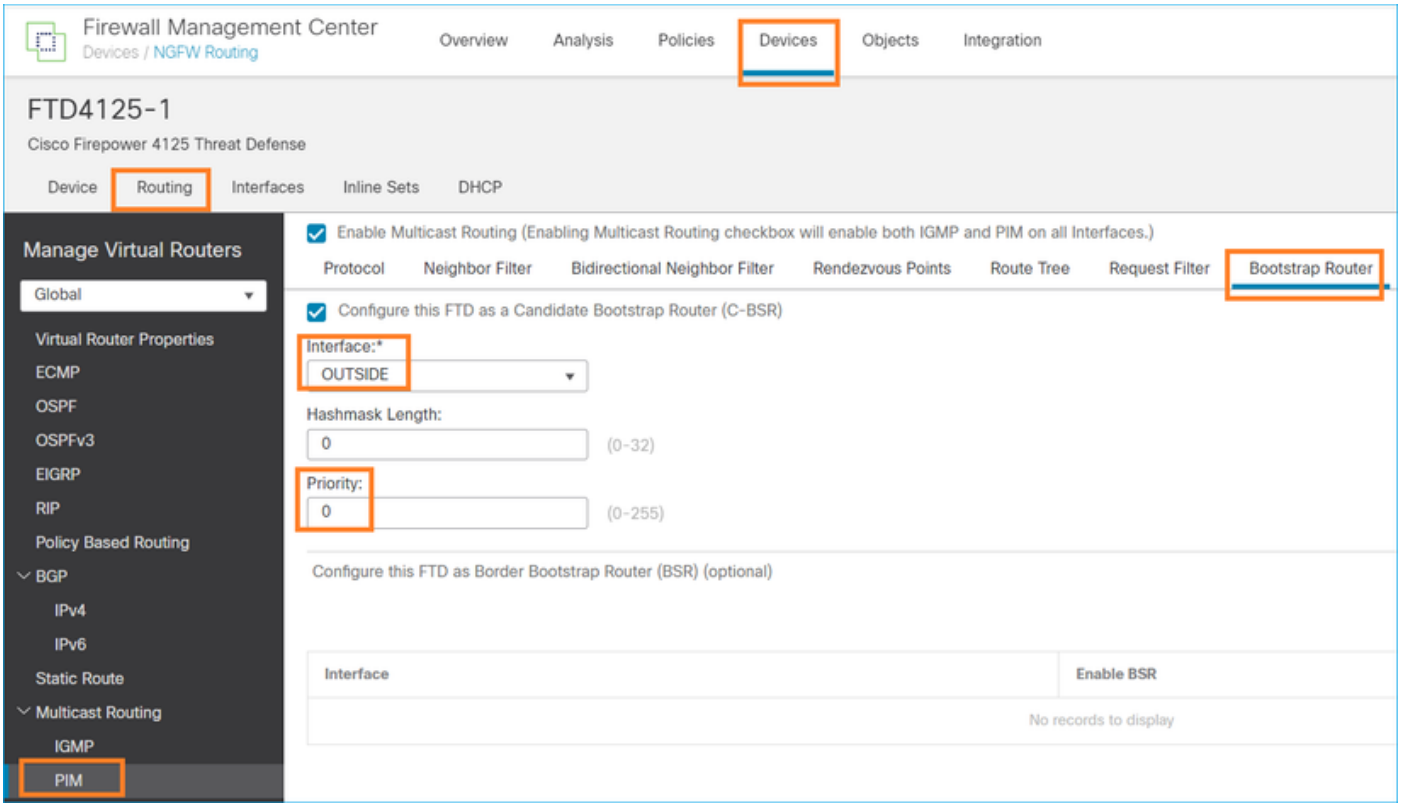
根据此拓扑配置C-BSR和C-RP:



对于此任务，FTD必须在具有BSR优先级0的外部接口上将其自身通告为C-BSR。

解决方案

FTD的FMC配置：



已部署的配置：

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

其他设备上的配置：

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)
```

R2上相同，但具有不同的C-BSR和C-RP优先级

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

在ASA上，仅全局启用组播。这将在所有接口上启用PIM:

```
multicast-routing
```

确认

由于具有最高优先级，因此R2是选定的BSR:

```
<#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
```

由于优先级最低，R1被选为RP:

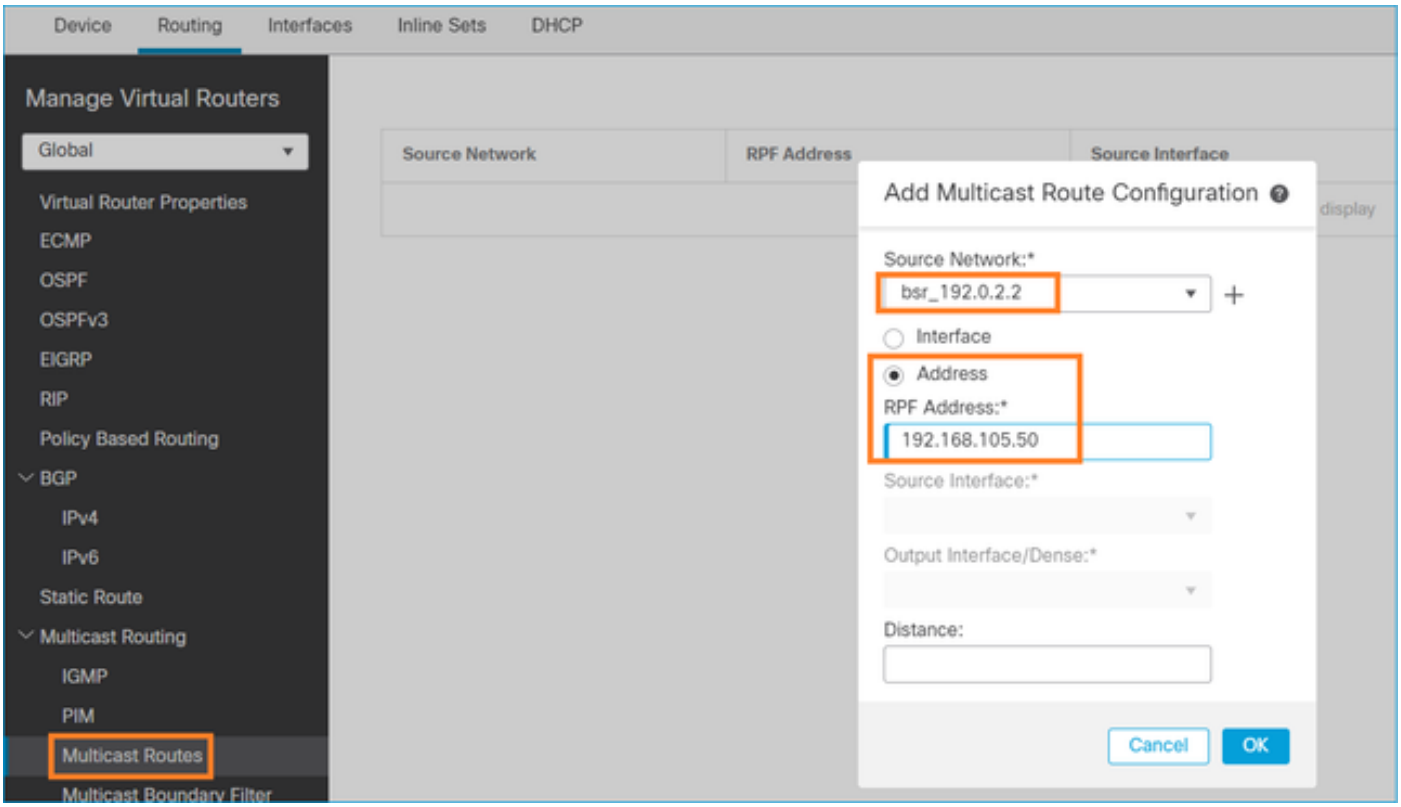
```
<#root>

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
```

BSR消息需要进行RPF检查。您可以启用debug pim bsr以验证这一点：

```
<#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
```

如果要更改RPF接口，可以配置静态路由。在本示例中，防火墙接受来自IP 192.168.105.50的BSR消息：



<#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
```

现在，NET207接口上的BSR消息被接受，但INSIDE上的消息被丢弃：

<#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

在防火墙上启用带跟踪的捕获，并检查BSR消息的处理方式：

<#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

PIM连接会在防火墙上终止，因此为使跟踪显示有用信息，需要清除与设备的连接：

<#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

如果由于RPF故障而丢弃PIM数据包，跟踪将显示：

<#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
```

ASP表丢弃并捕获show RPF-failed数据包：

```
<#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
```

要捕获由于RPF故障而丢弃的数据包，请执行以下操作：

```
<#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
```

故障排除方法

防火墙的故障排除方法主要取决于防火墙在组播拓扑中的作用。以下是故障排除的建议步骤列表：

1. 阐明问题描述和症状的细节。尝试将范围缩小到控制平面(IGMP/PIM)或数据平面（组播流）问题。
2. 排除防火墙上组播问题的必备条件是澄清组播拓扑。 您至少需要确定：
    - 组播拓扑中防火墙的角色 — FHR、LHR、RP或其他中间角色。
    - 防火墙上的预期组播入口和出口接口。
    - RP。
    - 发件人源IP地址。
    - 组播组IP地址和目标端口。
    - 组播流的接收器。

3.确定组播路由的类型- Stub或PIM组播路由：

- 末节组播路由 — 它提供动态主机注册并便于组播路由。为末节组播路由配置时，ASA充当IGMP代理。ASA不是完全参与组播路由，而是将IGMP消息转发到上游组播路由器，后者设置组播数据的传输。要识别末节模式路由，请使用show igmp interface命令并检查IGMP转发配置：

<#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)
```

接口上启用了PIM；但是，未建立邻居关系：

<#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和IGMP转发不同时支持。

您无法配置诸如RP地址之类的选项：

<#root>

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

- PIM组播路由 - PIM组播路由是最常见的部署。防火墙支持PIM-SM和双向PIM。PIM-SM是一种组播路由协议，使用底层单播路由信息库或独立的支持组播的路由信息库。它为每个组播组建立根于单个交汇点(RP)的单向共享树，并且可选择为每个组播源创建最短路径树。在此部署模式下，与末节模式不同，用户通常配置RP地址配置，防火墙与对等体建立PIM邻接关系：

<#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.检查RP IP地址是否已配置以及可达性：

<#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) <--- “us” mean

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

警告：防火墙不能同时为RP和FHR。

5.根据防火墙在组播拓扑中的角色和问题症状检查其他输出。

FHR

- 检查接口Tunnel0状态。此接口用于封装PIM负载内的原始组播流量并将单播数据包发送到RP，以设置PIM寄存器位：

<#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
```

- 检查路由：

<#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.
```

当防火墙收到具有注册停止位的PIM数据包时，会从OIL中删除Tunnel0。然后，防火墙停止封装，并通过出口接口发送原始组播流量：

<#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
```

- 检查PIM寄存器计数器：

<#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
```

- 检查防火墙和RP之间的单播PIM数据包捕获：

<#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
```

- 收集其他输出（x.x.x.x是组播组，y.y.y.y是RP IP）。建议收集输出几次:

<#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
```

- 收集原始组播接口数据包和ASP丢弃捕获。

<#root>

```
capture capi interface
```

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

```
capture capo interface
```

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

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

- 系统日志消息 — 通用ID为302015、302016和710005。

RP

- 检查接口Tunnel0状态。此接口用于封装PIM负载内的原始组播流量并将单播数据包发送到FHR，以设置PIM-stop位：

<#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        -
```

- 检查路由：

<#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
```

- 检查PIM计数器：

```
<#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
```

- 收集其他输出（x.x.x.x是组播组，y.y.y.y是RP IP）。建议收集输出几次:

<#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
```

- 收集原始组播接口数据包和ASP丢弃捕获：

<#root>

```
capture capi interface
```

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

```
capture capo interface
```

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

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

- Syslog — 公用ID是302015、302016和710005。

LHR

请考虑有关RP和这些附加检查的部分中提到的步骤：

- 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组：

<#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流量统计信息：

<#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故障排除命令（备忘单）

命令	描述
show running-config multicast-routing	查看防火墙上是否启用了组播路由
show run mroute	查看防火墙上配置的静态路由
show running-config pim	查看防火墙上的PIM配置
show pim interface	查看哪些防火墙接口启用了PIM和PIM邻居。
show pim neighbor	查看PIM邻居
show pim group-map	查看映射到RP的组播组
show mroute	查看完整的组播路由表
show mroute 230.10.10.10	查看特定组播组的组播表

show pim tunnel	查看防火墙和RP之间是否构建了PIM隧道
show conn all detail address RP_IP_ADDRESS	查看防火墙和RP之间是否已建立连接（PIM隧道）
show pim topology	查看防火墙PIM拓扑输出
debug pim	此调试显示进出防火墙的所有PIM消息
debug pim group 230.10.10.10	此调试显示特定组播组进出防火墙的所有PIM消息
show pim traffic	查看有关已接收和已发送PIM消息的统计信息
show asp cluster counter	验证在慢速路径与快速路径与控制点中处理的数据包数量
show asp drop	要查看防火墙上的所有软件级丢弃，请执行以下操作
capture CAP interface INSIDE trace match pim any any	在防火墙上捕获和跟踪入口PIM组播数据包
capture CAP interface INSIDE trace match udp host 224.1.2.3 any	捕获和跟踪入口组播流
show pim bsr-router	验证谁当选的BSR路由器
show conn all address 224.1.2.3	显示父组播连接
show local-host 224.1.2.3	显示子/末节组播连接

有关防火墙捕获检查的详细信息：使用Firepower威胁防御捕获和Packet Tracer

已知问题

Firepower组播限制：

- 不支持IPv6。
- 流量区域(EMCP)中的接口不支持PIM/IGMP组播。
- 防火墙不能同时是RP和FHR。
- show conn all命令仅显示身份组播连接。要显示末节/辅助组播连接，请使用show local-host <group IP>命令。

vPC Nexus不支持PIM

如果您尝试在Nexus vPC和防火墙之间部署PIM邻接关系，则存在Nexus限制，如下所述：

[Nexus 平台上通过虚拟端口通道进行路由所支持的拓扑]

从NGFW的角度来看，您将在跟踪此丢弃的捕获中看到:

<#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
```

防火墙无法完成RP注册：

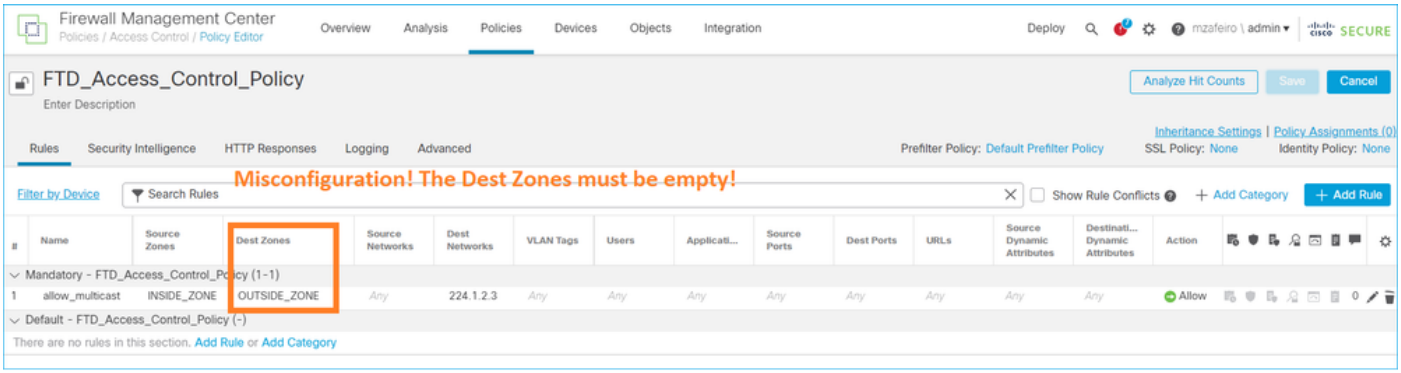
<#root>

```
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
```

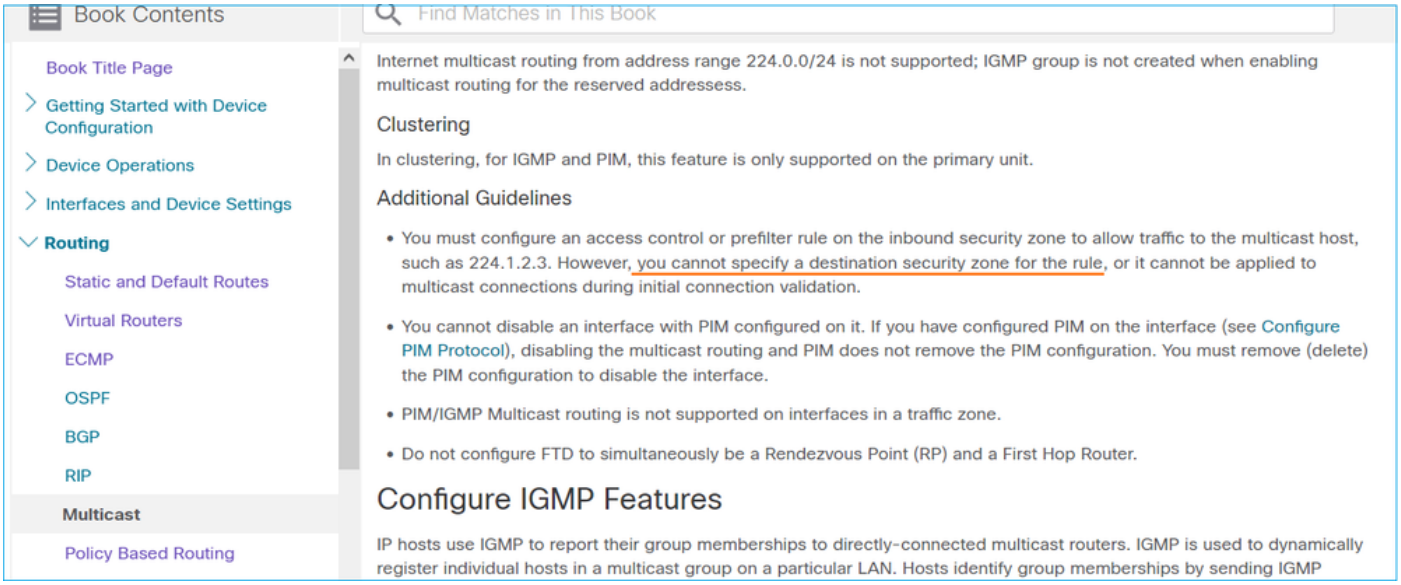
```
  Immediate Outgoing interface list:
    Tunnel0, Forward, 00:39:15/never
```

不支持目标区域

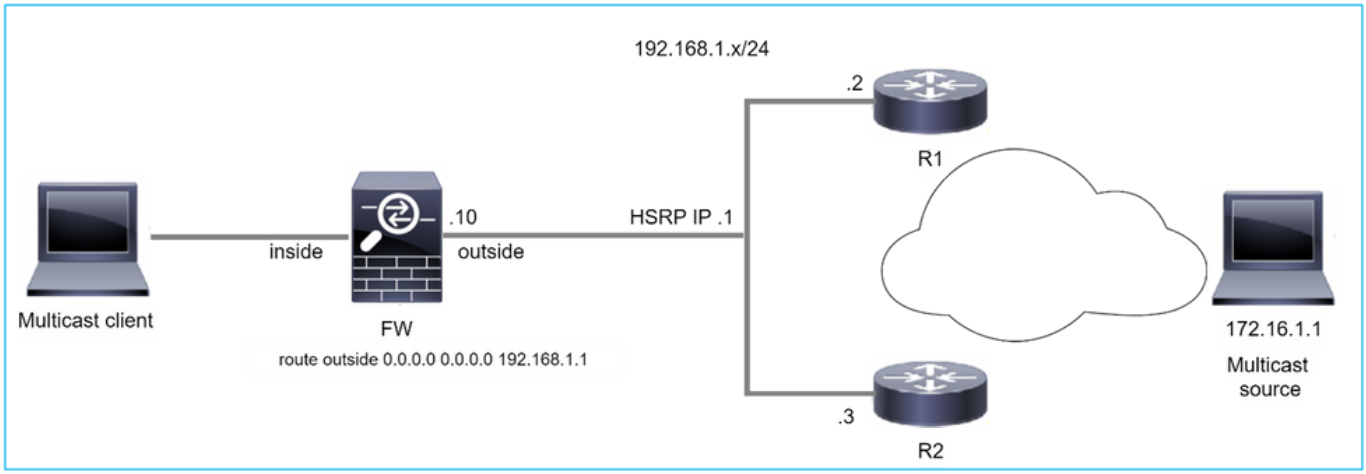
您不能为匹配组播流量的访问控制策略规则指定目标安全区域：



FMC用户指南中也介绍了以下内容：



由于HSRP，防火墙不会向上游路由器发送PIM消息



在这种情况下，防火墙通过热备份冗余协议(HSRP)IP 192.168.1.1以及与路由器R1和R2的PIM邻居关系拥有默认路由：

```
<#root>

firepower#

show run route

route outside 0.0.0.0 0.0.0.0 192.168.1.1 1
```

防火墙在R1和R2的外部和物理接口IP之间具有PIM邻接关系：

```
<#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)
```

防火墙不会将PIM加入消息发送到上游网络。PIM debug命令debug pim显示以下输出：

```
<#root>

firepower#

debug pim
...


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

RFC 2362指出，“路由器定期向每个(S，G)、(*,G)和(*,*,RP)条目关联的每个不同RPF邻居发送加入/修剪消息。只有当RPF邻居是PIM邻居时，才会发送加入/修剪消息。"

为缓解此问题，用户可在防火墙上添加一个静态mroute条目。路由器必须指向两个路由器接口的IP地址之一192.168.1.2或192.168.1.3，通常是HSRP活动路由器IP。

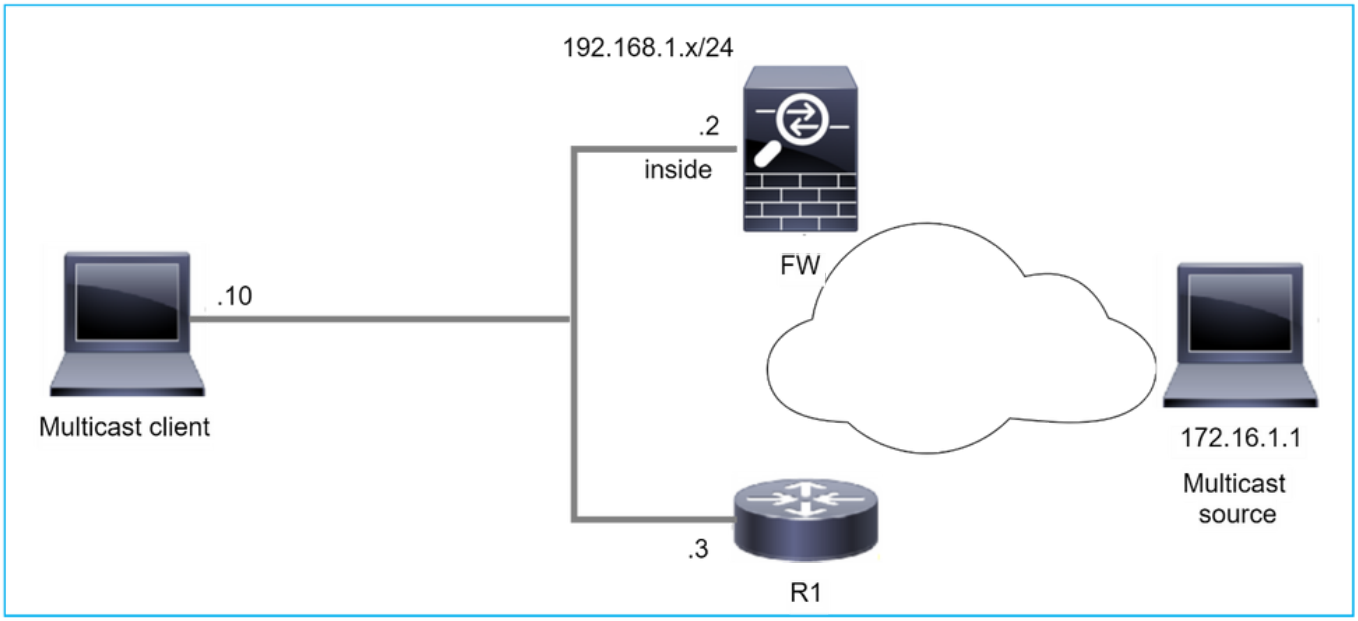
示例：

```
<#root>

firepower#

show run mroute


firepower#

mroute 172.16.1.1 255.255.255.255 192.168.1.2
```

静态路由配置到位后，对于RPF查找，防火墙会优先选择组播路由表而不是ASA的单播路由表，并将PIM消息直接发送到邻居192.168.1.2。

注意：静态mroute在某些方面削弱了HSRP冗余的实用性，因为mroute仅接受每个地址/网络掩码组合的1个下一跳。如果mroute命令中指定的下一跳发生故障或无法到达，防火墙不会回退到其他路由器。

当防火墙不是LAN网段中的DR时，不将其视为LHR



防火墙将R1作为LAN网段中的PIM邻居。R1是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)

如果收到来自客户端的IGMP加入请求，防火墙不会成为LHR。

mroute将其他Null显示为OIL，并具有Pruned标志：

<#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

要使防火墙成为LHR，可以增加接口DR优先级。

<#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
```

PIM debug命令debug pim显示以下输出：

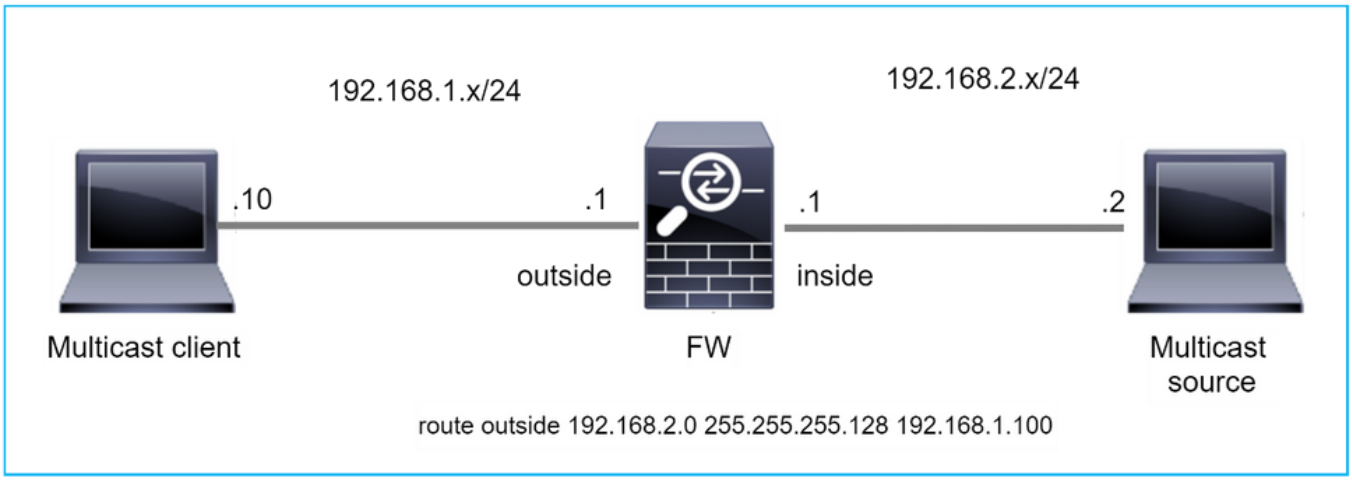
```
<#root>

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
```

Pruned标志和Null将从mroute中删除：

```
<#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
```

防火墙由于反向路径转发检查失败而丢弃组播数据包



在这种情况下，由于RPF故障，组播UDP数据包将被丢弃，因为防火墙通过外部接口具有掩码为255.255.255.128的更具体的路由。

<#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丢弃捕获显示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) R
   3: 09:00:53.812152       192.168.2.2.12345 > 230.1.1.1.12354:  udp 500 Drop-reason: (rpf-violated) R
   4: 09:00:53.908613       192.168.2.2.12345 > 230.1.1.1.12354:  udp 500 Drop-reason: (rpf-violated) R
```

MFIB输出中的RPF失败计数器增加：

<#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)
```

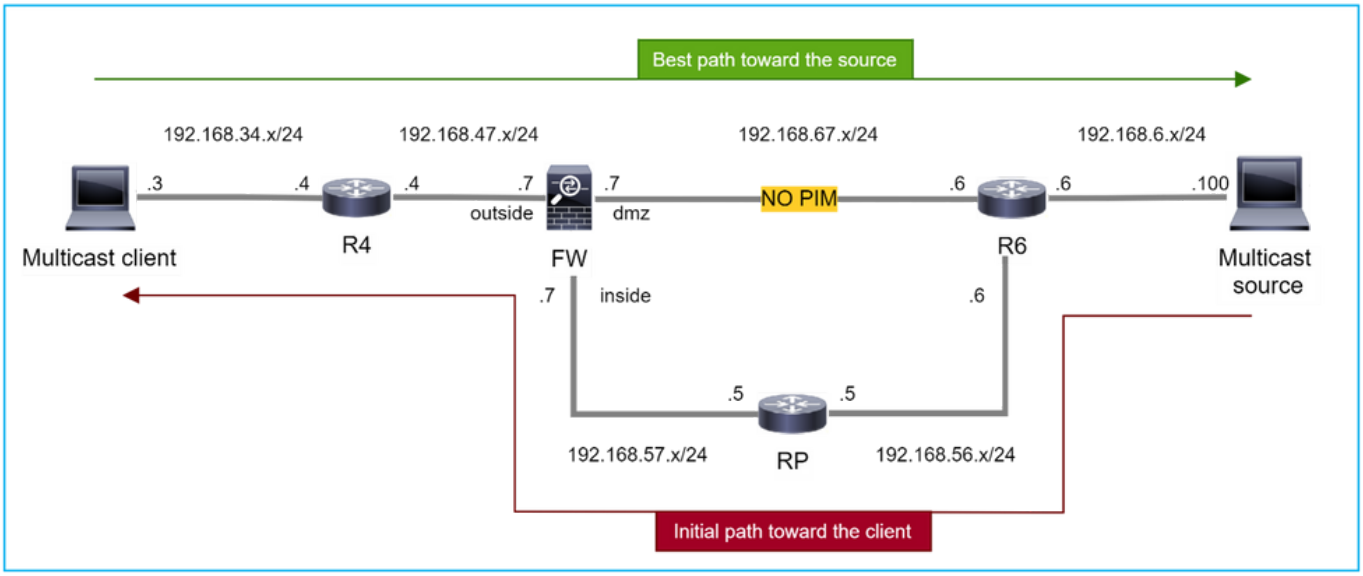
```
Group: 230.1.1.1
  RP-tree:

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

解决方案是修复RPF检查失败。一个选项是删除静态路由。

如果没有其他RPF检查故障，则会转发数据包，且MFIB输出中的Forwarding计数器会增加：

```
<#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
```

在PIM切换到源树时，防火墙不会生成PIM加入



在本例中，防火墙通过dmz接口R4 > FW > R6获取通向组播源的路径，而从源到客户端的初始流量路径为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
```

一旦达到SPT切换阈值，R4会启动SPT切换并发送源特定的PIM加入消息。在防火墙中，不会发生SPT切换，(S，G)mroute没有T标志：

<#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
```

PIM调试命令debug pim显示从对等体R4收到的2个PIM加入请求 — 针对(*,G)和(S，G)。防火墙为(*,G)上游发送了PIM加入请求，并且由于无效邻居192.168.67.6，未能发送源特定请求：

```
<#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

show pim neigbour命令输出缺少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在防火墙接口dmz上启用：

<#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
```

在R6接口上禁用PIM:

```
<#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
```

解决方案是在R6的接口GigabitEthernet0/3上启用PIM:

```
<#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
```

防火墙安装T标志，指示SPT切换:

```
<#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
```

防火墙因传送速率限制而丢弃前几个数据包

当防火墙在FP中收到新组播流的第一个数据包时，可能需要CP进行额外处理。在这种情况下，FP通过SP(FP > SP > CP)将数据包传送到CP以执行其他操作：

- 在FP中入口接口和身份接口之间创建父连接。
- 其他组播特定检查，例如RPF验证、PIM封装（如果防火墙是FHR）、OIL检查等。
- 在mroute表中创建具有传入和传出接口的(S，G)条目。
- 在传入和传出接口之间创建子/末节连接。

作为控制平面保护的一部分，防火墙在内部限制传送到CP的数据包的速率。

超过该速率的数据包会在中丢弃，并带有punt-rate-limit丢弃原因：

```
<#root>

firepower#
```

show asp drop

Frame drop:

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

使用show asp cluster counter命令验证从SP传送到CP的组播数据包的数量：

<#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

使用show asp event dp-cp punt命令验证FP > CP队列中的数据包数以及15秒的速率：

<#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
```

当填充mroute并在FP中建立父/子连接时，数据包将作为现有连接的一部分在FP中转发。在这种情况下，FP不会将数据包传送到CP。

防火墙如何处理新组播流的第一个数据包？

当防火墙在数据路径中收到新组播流的第一个数据包时，防火墙将执行以下操作：

1. 检查安全策略是否允许数据包。
2. 通过路径FP将数据包传送到CP。
3. 在入口接口和身份接口之间创建父连接:

<#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

系统日志：

<#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
```

此连接在show conn all命令的输出中可见：

<#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 –
```

4. CP通过组播进程进行其他组播特定检查，例如RPF验证、PIM封装（如果防火墙是FHR）、OIL检查等。
5. CP在mroute中创建一个(S，G)条目，其中包含传入和传出接口：

<#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
```

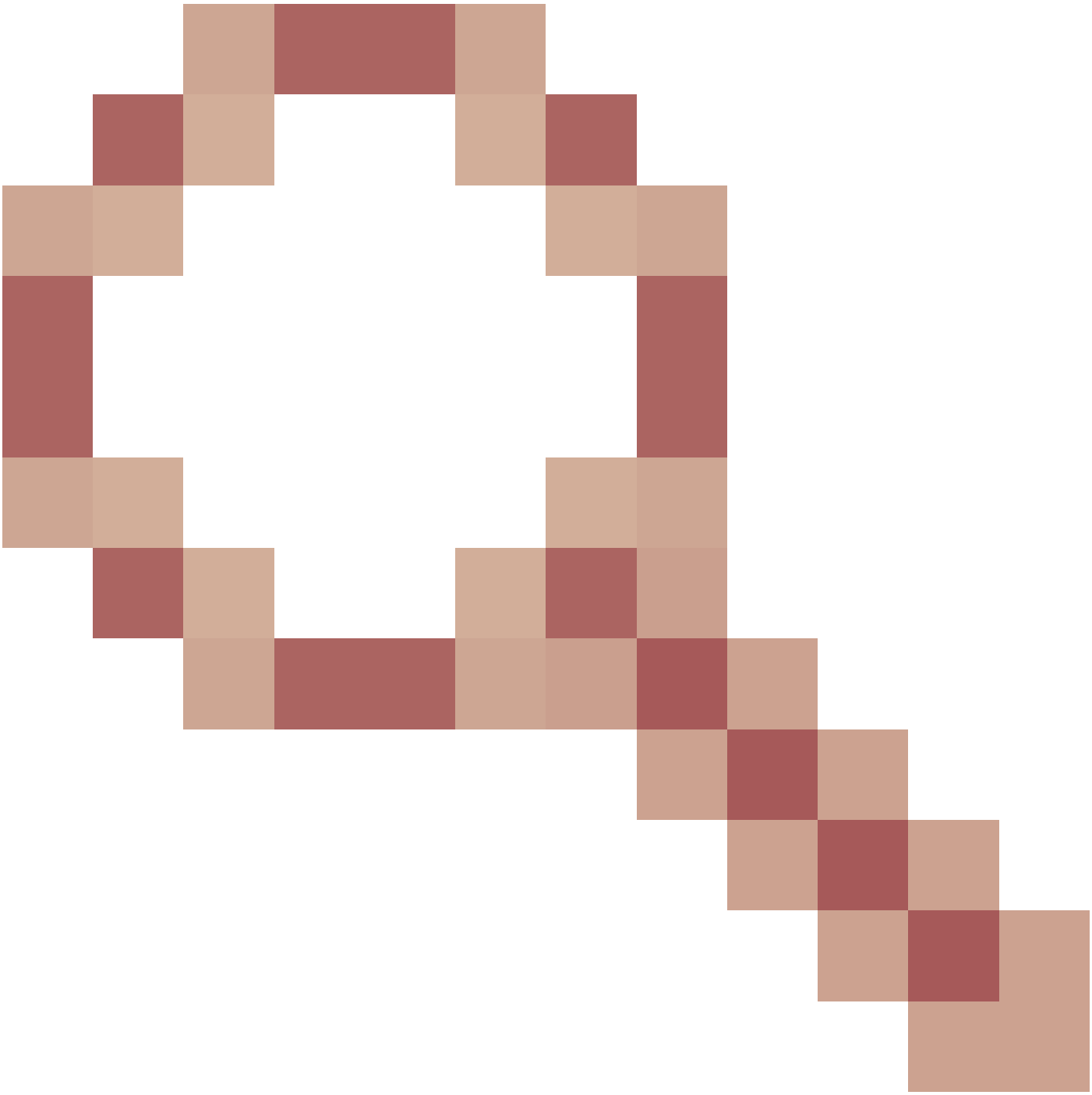
```
  Incoming interface: inside


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

6. CP通过CP > SP > FP路径指示FP在传入和传出接口之间创建子/末节连接：

此连接仅在show local-host命令的输出中可见：

```
<#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
```

在软件版本中修复Cisco Bug ID CSCwe21280



，还会生成用于子/末节连接的系统日志消息302015:

<#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

当父连接和子/末节连接都建立时，入口数据包将匹配现有连接并在FP中转发：

<#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
```

过滤ICMP组播流量

您不能使用ACL过滤ICMP组播流量。您必须使用控制平面策略(ICMP):

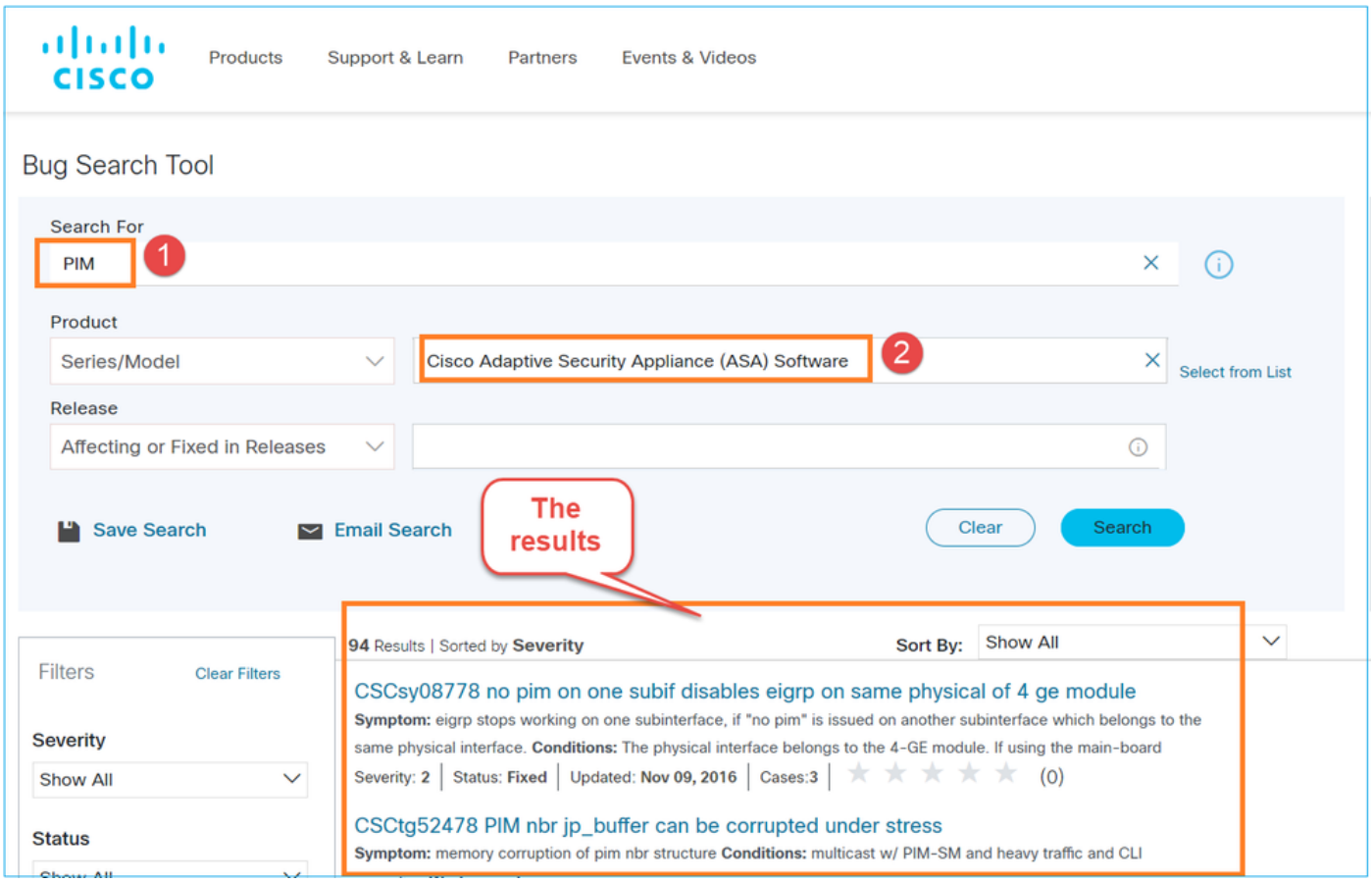
Cisco Bug ID CSCsl26860 ASA不过滤组播ICMP数据包

已知PIM组播缺陷

您可以使用漏洞搜索工具查找已知缺陷：https://bst.cloudapps.cisco.com/bugsearch

大多数ASA和FTD缺陷列在“Cisco Adaptive Security Appliance(ASA)Software”(思科自适应安全设

备(ASA)软件)产品下：



相关信息

- ASA组播故障排除和常见问题
- Firepower管理中心组播
- Firepower组播标志摘要

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。