排除Firepower威脅防禦和ASA組播PIM故障

目錄

簡介

必要條件

- 需求
- 採用元件

背景資訊

- 組播路由基礎知識
- 縮寫/縮寫
- 任務1 - PIM稀疏模式（靜態RP）
- 任務2 — 配置PIM引導路由器(BSR)

故障排除方法

PIM故障排除命令（備忘單）

已知的問題

- vPC Nexus不支援PIM
- 不支援目標區域
- 由於HSRP，防火牆不會向上游路由器傳送PIM消息
- 當防火牆不是LAN網段中的DR時，不將其視為LHR
- 由於反向路徑轉發檢查失敗，防火牆丟棄組播資料包
- Firewall does not Generate PIM join when PIM Switchover to Source-tree（在PIM切換到源樹時，防火牆不會生成PIM加入）
- 防火牆由於轉發速率限制而丟棄前幾個資料包
- 篩選ICMP多點傳送流量

已知PIM組播缺陷

相關資訊

簡介

本檔案將說明Firepower威脅防禦(FTD)和調適型安全裝置(ASA)如何實施通訊協定無關多點傳送(PIM)。

必要條件

需求

基本IP路由知識。

採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

本文中的資訊係根據以下軟體和硬體版本：

- Cisco Firepower 4125威脅防禦版本7.1.0。
- Firepower管理中心(FMC)版本7.1.0。
- 思科調適型安全裝置軟體版本9.17(1)9。

背景資訊

組播路由基礎知識

- 單播將資料包轉發到目的地，而multicast將資料包轉發到遠離源的位置。
- 多點傳送網路裝置（防火牆/路由器等）透過反向路徑轉送(RPF)轉送封包。請注意，RPF與單播中用於防止特定型別攻擊的uRPF不同。RPF可以定義為一種將組播資料包從源轉發到通向組播接收器的介面之外的機制。它的主要作用是防止流量環路和確保正確的流量路徑。
- PIM等組播協定有3個主要功能：

1.查詢上游介面（距離源最近的介面）。

2.查詢與特定多點傳播流（通向接收器的介面）關聯的下游介面。

3.維護組播樹（新增或刪除樹分支）。

- 可以使用以下兩種方法之一來構建和維護組播樹：隱式聯合（泛洪和修剪）或顯式聯合（拉模型）。PIM密集模式(PIM-DM)使用隱式聯合，而PIM稀疏模式(PIM-SM)使用顯式聯合。
- 組播樹可以是共用樹也可以是基於源樹：
  - 共用樹使用Rendezvous Point(RP)的概念，並記為(*, G),其中G =組播組IP。
  - 基於源的樹在源位置紮根，不使用RP，並記作(S， G),其中S =組播源/伺服器的IP。
- 組播轉發模型：
  - 任意源組播(ASM)傳送模式使用共用樹(*, G)，其中任何源都可以傳送組播流。
  - 來源特定多點傳送(SSM)使用來源型樹狀目錄(S、G)和IP範圍232/8。
  - 雙向(BiDir)是一種共用樹(*, G)，控制平面和資料平面流量均通過RP。
- 可以使用以下方法之一配置或選擇交匯點：
  - 靜態RP
  - 自動RP
  - 啟動路由器(BSR)

PIM模式摘要

PIM模式	RP	共用樹	表示法	IGMP	支援的ASA/FTD
PIM稀疏模式	是	是	(*, G)和 (S， G)	v1/v2/v3	是

PIM密集模式	否	否	(S、G)	v1/v2/v3	否*
PIM雙向模式	是	是	(*, G)	v1/v2/v3	是
PIM來源特定多點傳送(SSM)模式	否	否	(S、G)	v3	否**

*自動RP =自動RP流量可以通過

** ASA/FTD不能是最後一跳裝置

RP配置摘要

交匯點配置	ASA/FTD
靜態RP	是
自動RP	否，但自動RP控制平面流量可以通過
BSR	是，但不支援C-RP

註：開始排除任何組播問題之前，必須清晰地檢視組播拓撲。具體來說，至少您需要知道：
— 防火牆在組播拓撲中扮演什麼角色？
-RP是誰？
— 組播流的傳送者是誰（源IP和組播組IP）？
— 組播流的接收者是誰？
— 控制平面(IGMP/PIM)或資料平面（組播流）本身是否有問題？

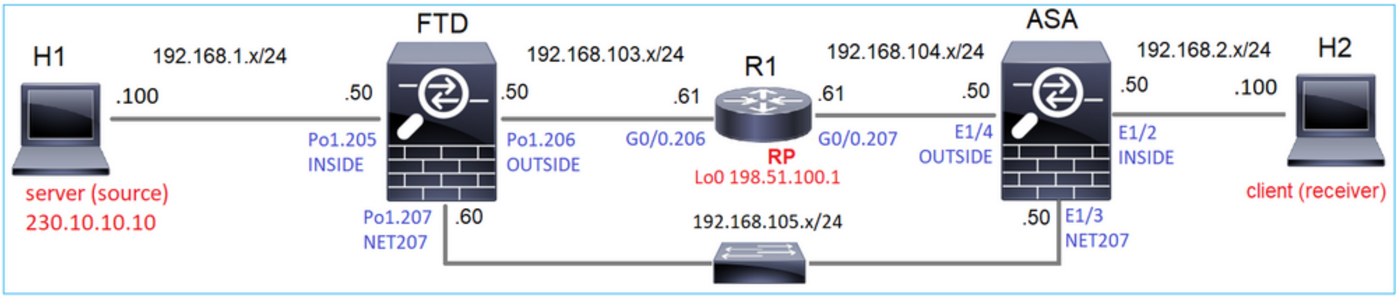
縮寫/縮寫

縮寫說明	說明
FHR	第一跳路由器 — 直接連線到組播流量源的一跳。
LHR	最後一跳路由器 — 直接連線到組播流量接收者的跳數。

RP	交匯點
DR	指定路由器
SPT	最短路徑樹
RPT	集結點(RP)樹，共用樹
RPF	反向路徑轉送
石油	傳出介面清單
MRIB	多點傳送路由資訊庫
MFIB	組播轉發資訊庫
ASM	任意來源多點傳送
BSR	啟動路由器
SSM	來源特定多點傳送
FP	快速路徑
SP	慢速路徑
CP	控制點
PPS	每秒資料包速率

任務1 - PIM稀疏模式（靜態RP）

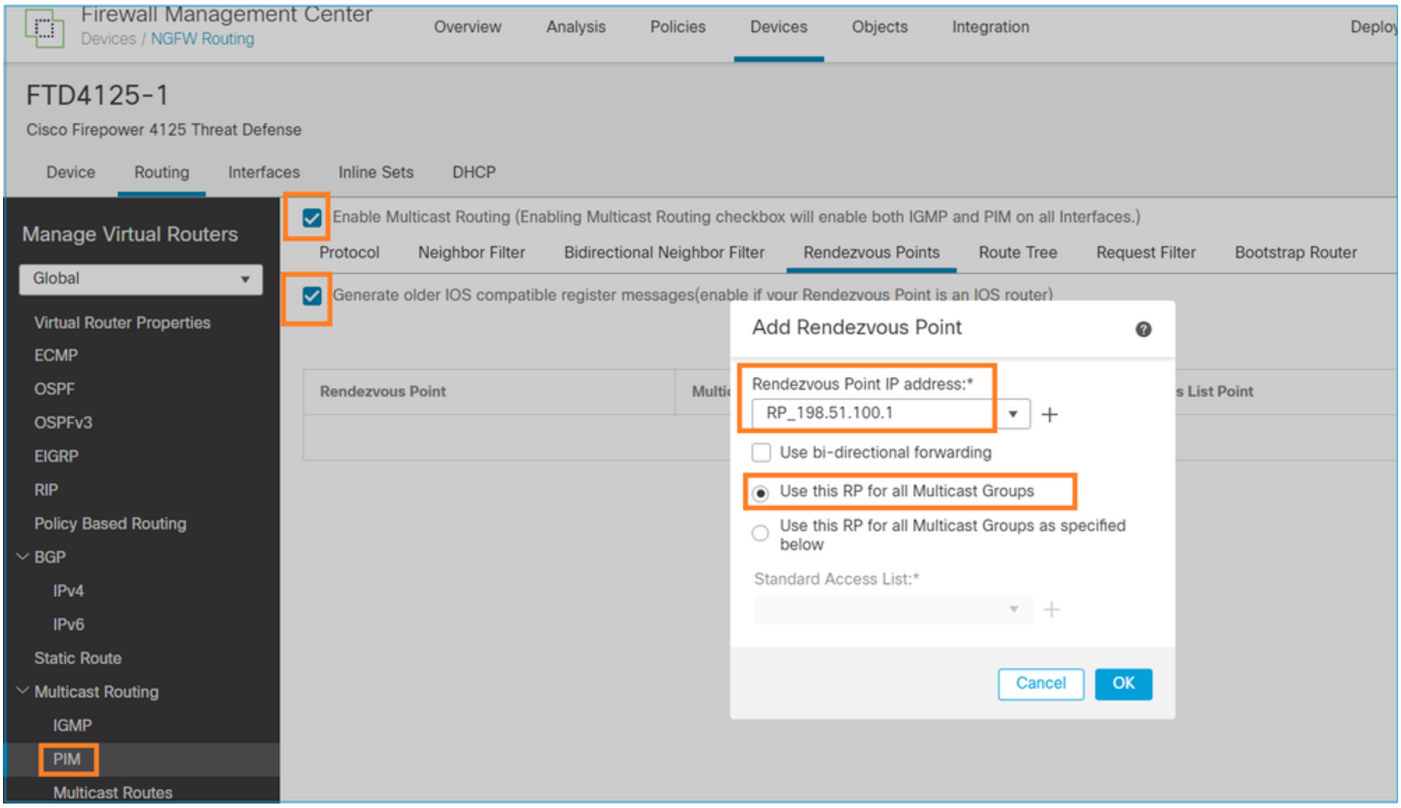
拓撲



在拓撲中配置組播PIM稀疏模式，將R1(198.51.100.1)配置為RP。

解決方案

FTD組態：



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

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

Add Rendezvous Point

Rendezvous Point IP address:* RP_198.51.100.1

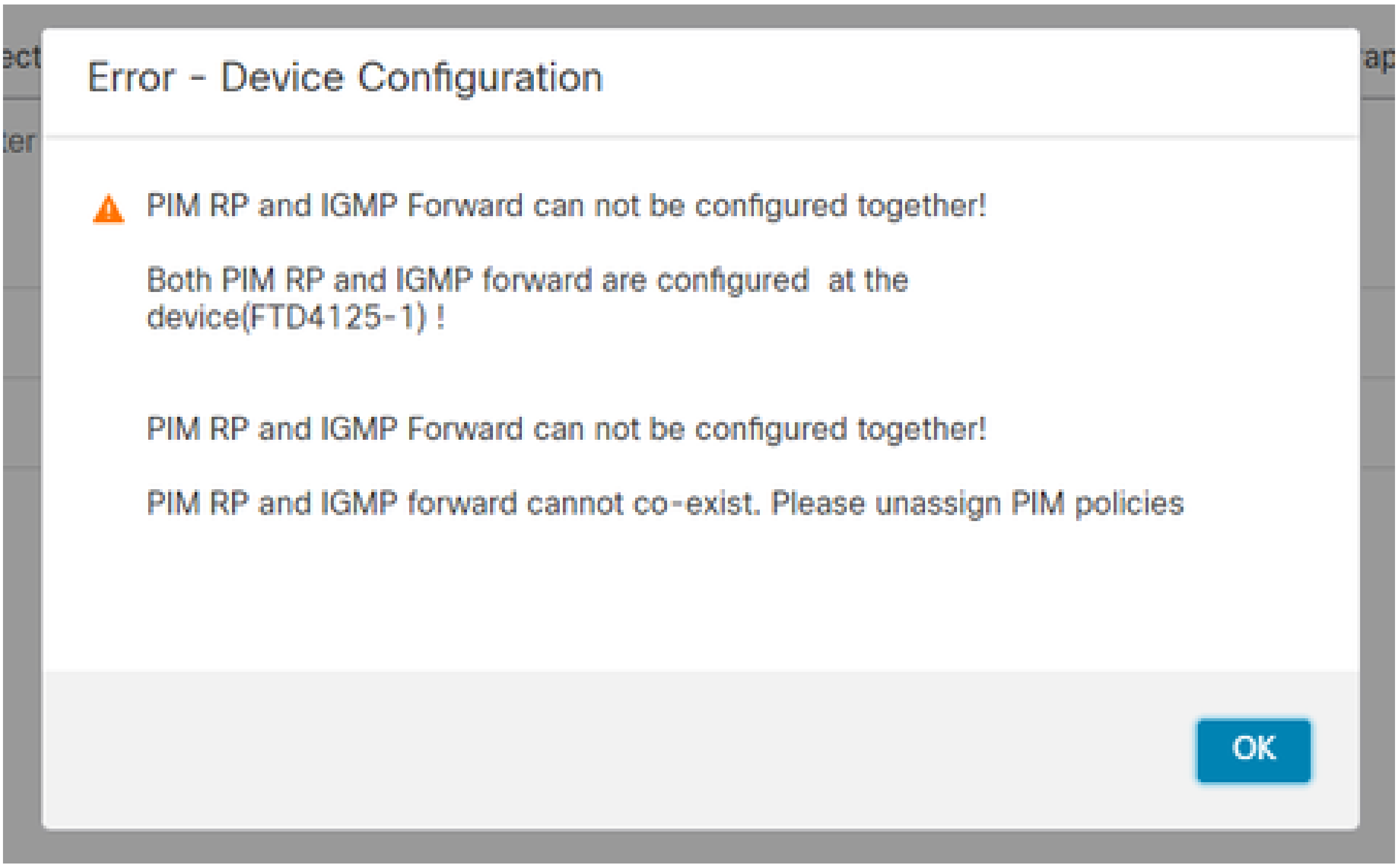
□ Use bi-directional forwarding

● Use this RP for all Multicast Groups

○ Use this RP for all Multicast Groups as specified below

Standard Access List:*

無法同時為IGMP Stub路由和PIM配置ASA/FTD:



Error - Device Configuration

PIM RP and IGMP Forward can not be configured together!

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

PIM RP and IGMP Forward can not be configured together!

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

FTD上的結果組態：

<#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防火牆上有一個類似的配置：

<#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
```

驗證

當沒有多點傳播流量（傳送者或接收器）時，驗證FTD上的多點傳播控制平面：

```
<#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
```

檢驗PIM鄰居：

```
<#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通告整個組播組範圍：

```
<#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
```

防火牆路由表包含一些不相關的條目(239.255.255.250是MAC OS和Microsoft Windows等供應商使用的簡單服務發現協定(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
```

在防火牆和RP之間構建了一個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
```

也可以在防火牆連線表中看到PIM隧道：

<#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
```

在ASA防火牆上進行驗證：

<#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驗證。SSDP和自動RP有一些組播組：

<#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
```

接收方宣佈其存在時進行驗證

注意：本節顯示的防火牆命令完全適用於ASA和FTD。

ASA獲取IGMP成員身份報告消息並建立IGMP和mroute(*, G)條目：

<#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防火牆為組播組建立路由：

<#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
```

另一個防火牆驗證是PIM拓撲輸出：

<#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
```

註：如果防火牆沒有通向RP的路由，則debug pim 輸出顯示RPF查詢失敗

debug pim 輸出中的RPF查詢失敗：

<#root>

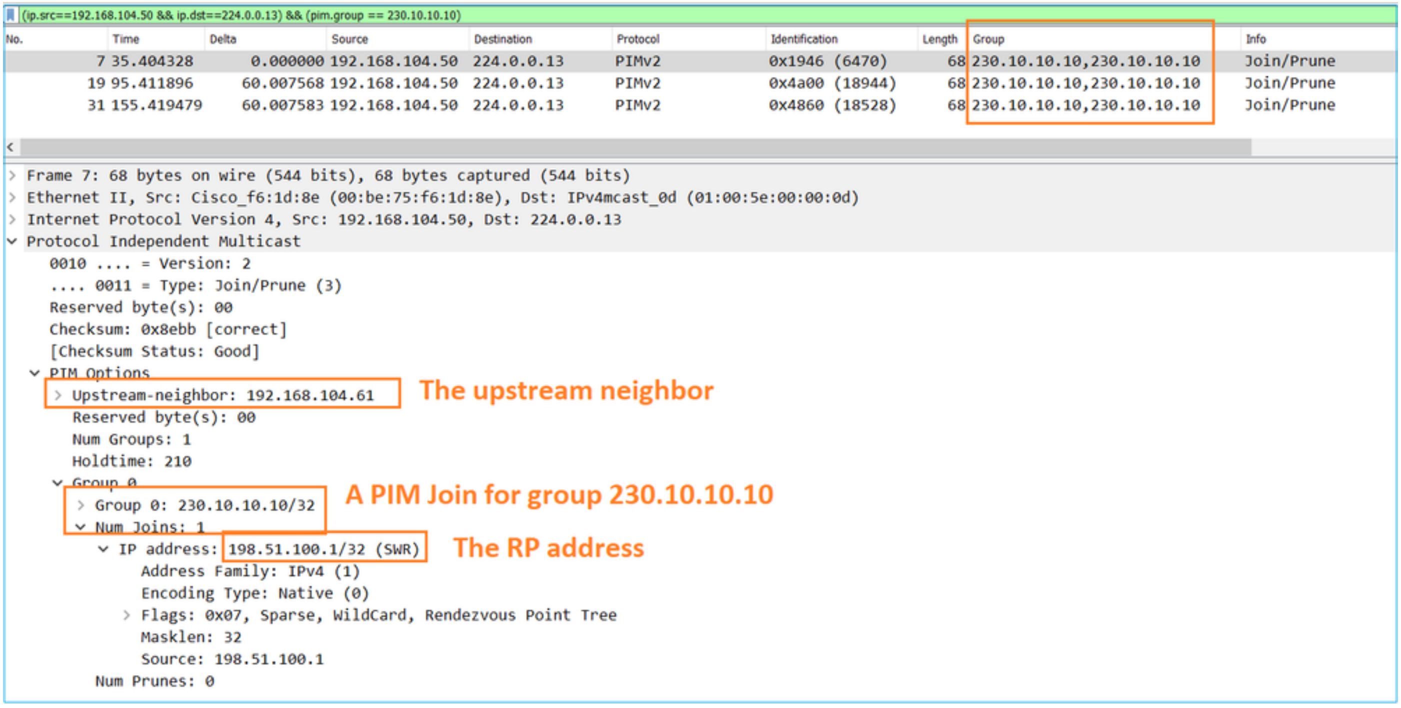
```
asa#

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，防火牆會向RP傳送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
```

捕獲顯示，PIM加入消息每1分鐘傳送一次，PIM Hello每30秒傳送一次。PIM使用IP 224.0.0.13:



```
(ip.src==192.168.104.50 && ip.dst==224.0.0.13) && (pim.group == 230.10.10.10)
No.   Time        Delta      Source          Destination  Protocol  Identification  Length  Group                        Info
    7 35.404328    0.000000  192.168.104.50  224.0.0.13   PIMv2     0x1946 (6470)       68  230.10.10.10,230.10.10.10    Join/Prune
   19 95.411896   60.007568  192.168.104.50  224.0.0.13   PIMv2     0x4a00 (18944)      68  230.10.10.10,230.10.10.10    Join/Prune
   31 155.419479  60.007583  192.168.104.50  224.0.0.13   PIMv2     0x4860 (18528)      68  230.10.10.10,230.10.10.10    Join/Prune

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

The upstream neighbor

A PIM Join for group 230.10.10.10

The RP address

提示：Wireshark顯示過濾器：(ip.src==192.168.104.50 && ip.dst==224.0.0.13)和&(pim.group == 230.10.10.10)

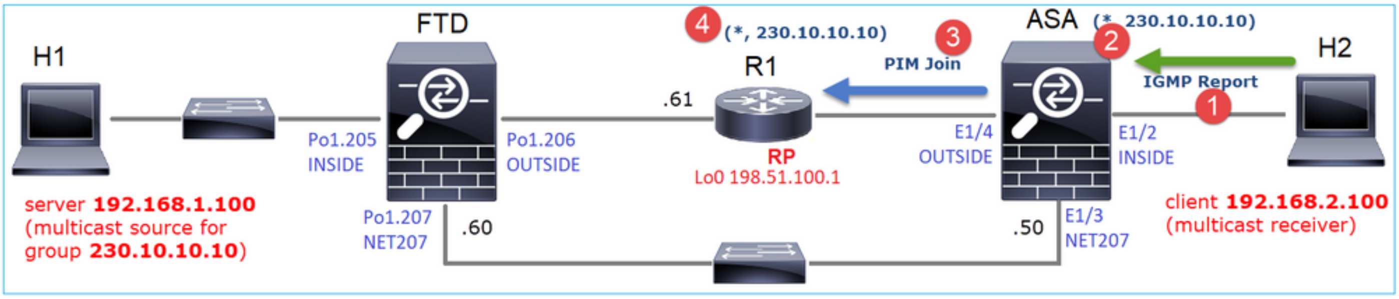
- 192.168.104.50是輸出介面（通向上游PIM鄰居）的防火牆IP
- 224.0.0.13是傳送PIM加入和修剪的PIM組播組
- 230.10.10.10是我們傳送PIM加入/修剪的組播組

RP建立(*, G)mroute。請注意，由於尚未有任何伺服器，因此傳入介面為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
```

其視覺化結果為：



1. 在ASA上收到IGMP報告。
2. 新增了(*, G)mroute。
3. ASA向RP(198.51.100.1)傳送PIM加入消息。
4. RP收到Join消息並新增(*, G)mroute。

同時，由於未收到IGMP報告或PIM加入，FTD上沒有路由：

<#root>

```
firepower#

show mroute 230.10.10.10

No mroute entries found.
```

驗證伺服器何時傳送組播流

FTD從H1取得多點傳送流，並使用RP啟動PIM註冊流程。FTD將單點傳送PIM註冊器訊息傳送到RP。RP向第一躍點路由器(FHR)（在本例中為FTD）傳送PIM加入消息以加入組播樹。然後傳送Register-Stop消息。

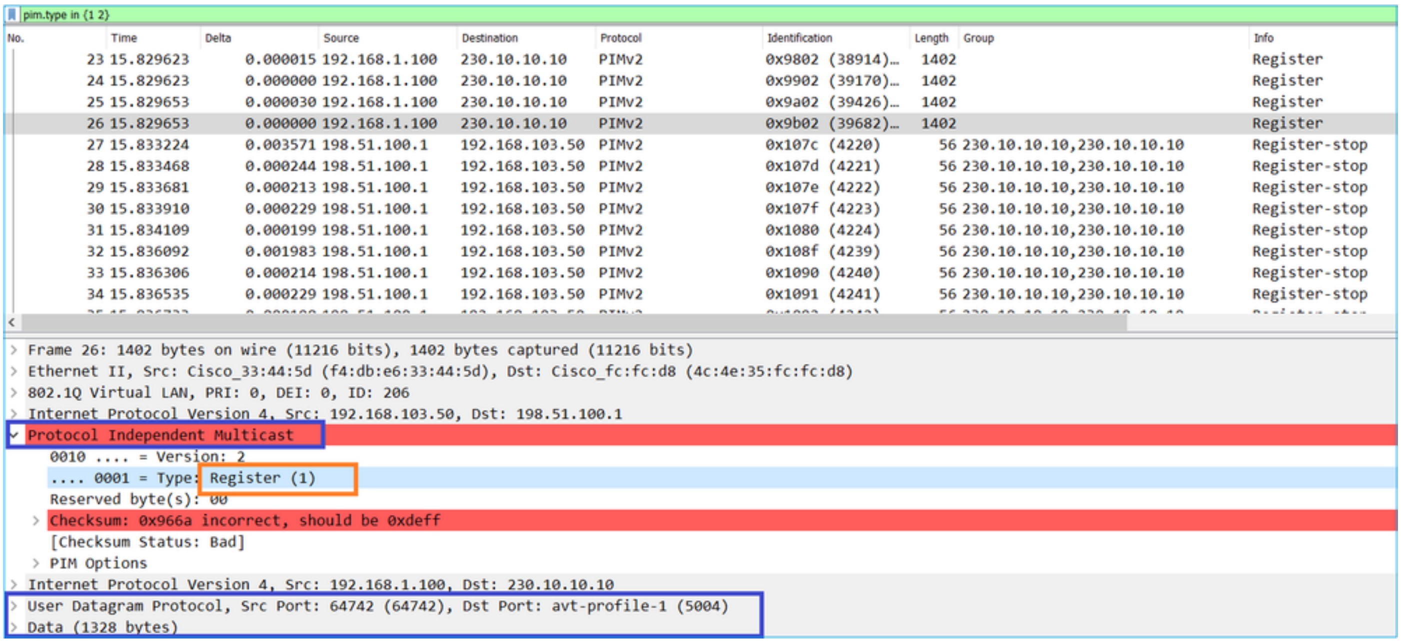
<#root>

```
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註冊消息是PIM消息，它攜帶UDP資料以及PIM註冊資訊：

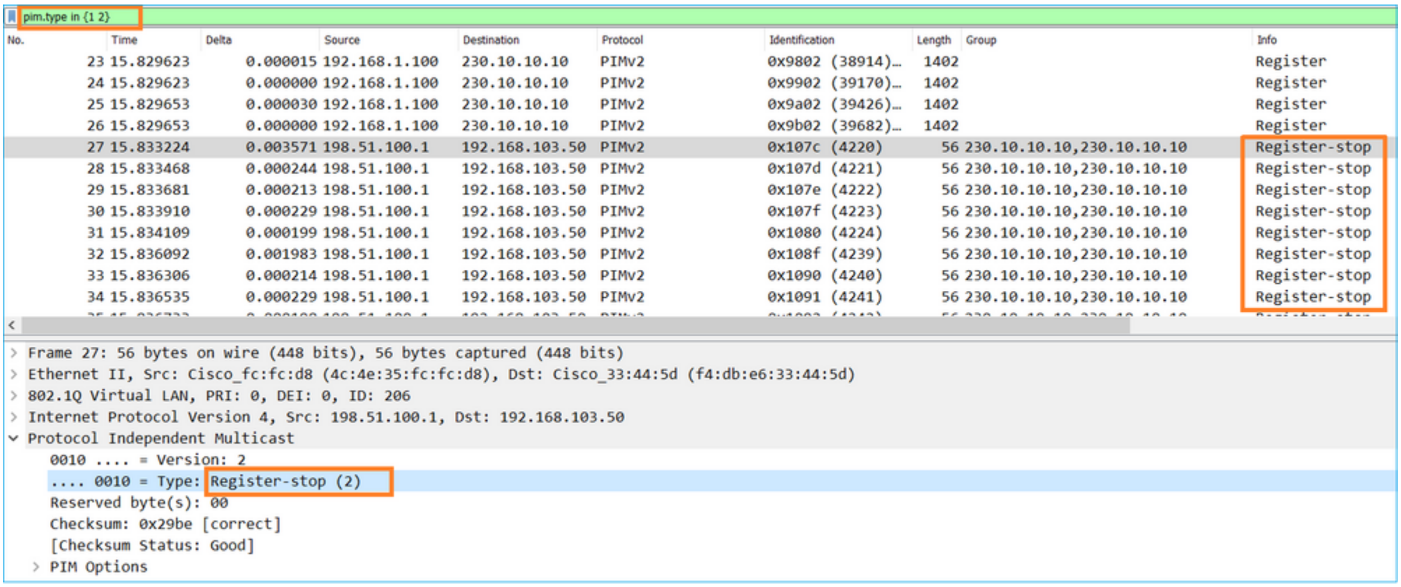


pim.type in {1 2}

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

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

PIM註冊停止消息：



pim.type in {1 2}

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

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

提示：要在Wireshark上僅顯示PIM註冊和PIM註冊停止消息，可以使用顯示篩選器：pim.type in {1 2}

防火牆（最後一跳路由器）獲取介面OUTSIDE上的組播流，並發起到介面NET207的最短路徑樹(SPT)切換：

<#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)
```

進行轉接時，FTD上的PIM偵錯：

<#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切換啟動後FTD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 i
```

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

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

在SPT切換結束時，僅NET207介面顯示在FTD的OIL中：

<#root>

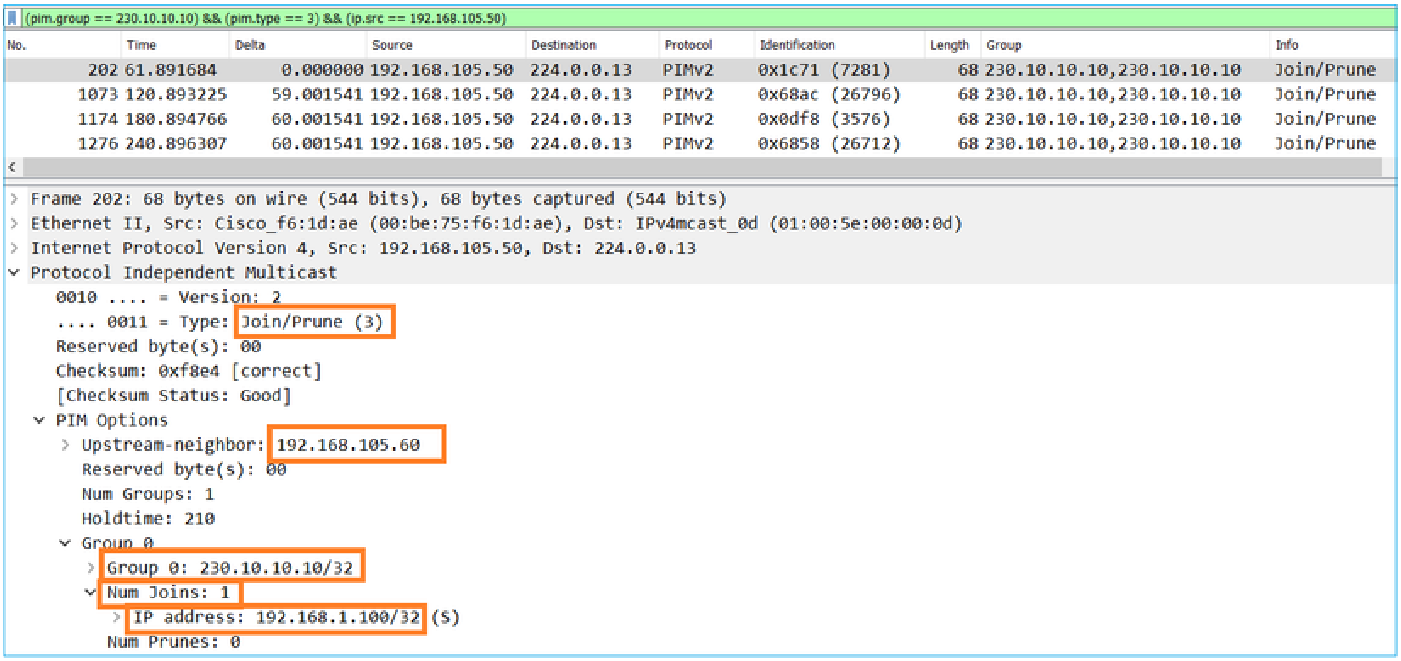
```
firepower#

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
```

在最後一跳路由器(ASA)上還設定了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
```

從ASA NET207介面（執行切換的第一跳路由器）進行切換。PIM加入消息傳送到上游裝置(FTD):

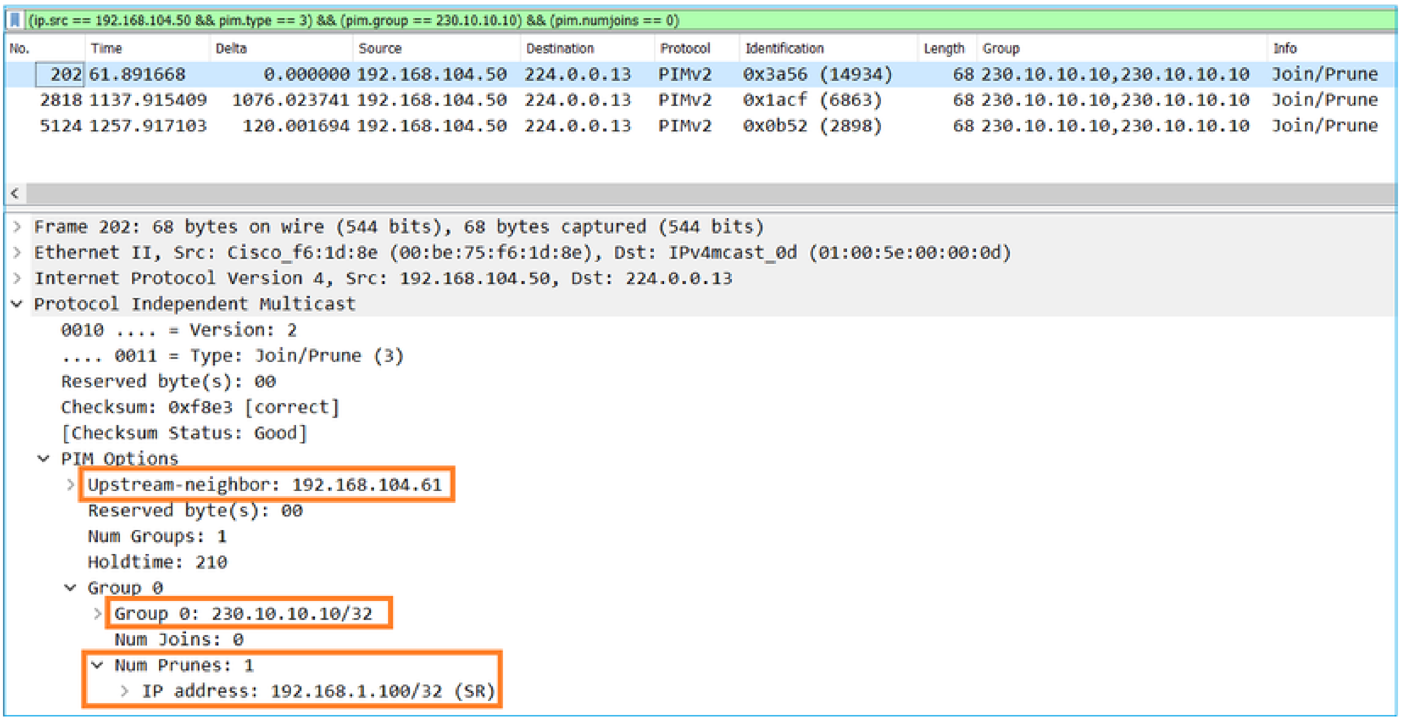


(pim.group == 230.10.10.10) && (pim.type == 3) && (ip.src == 192.168.105.50)

No.	Time	Delta	Source	Destination	Protocol	Identification	Length	Group	Info
202	61.891684	0.000000	192.168.105.50	224.0.0.13	PIMv2	0x1c71 (7281)	68	230.10.10.10,230.10.10.10	Join/Prune
1073	120.893225	59.001541	192.168.105.50	224.0.0.13	PIMv2	0x68ac (26796)	68	230.10.10.10,230.10.10.10	Join/Prune
1174	180.894766	60.001541	192.168.105.50	224.0.0.13	PIMv2	0x0df8 (3576)	68	230.10.10.10,230.10.10.10	Join/Prune
1276	240.896307	60.001541	192.168.105.50	224.0.0.13	PIMv2	0x6858 (26712)	68	230.10.10.10,230.10.10.10	Join/Prune

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

在OUTSIDE介面上，PIM修整消息被傳送到RP以停止組播流：



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

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

驗證PIM流量：

<#root>

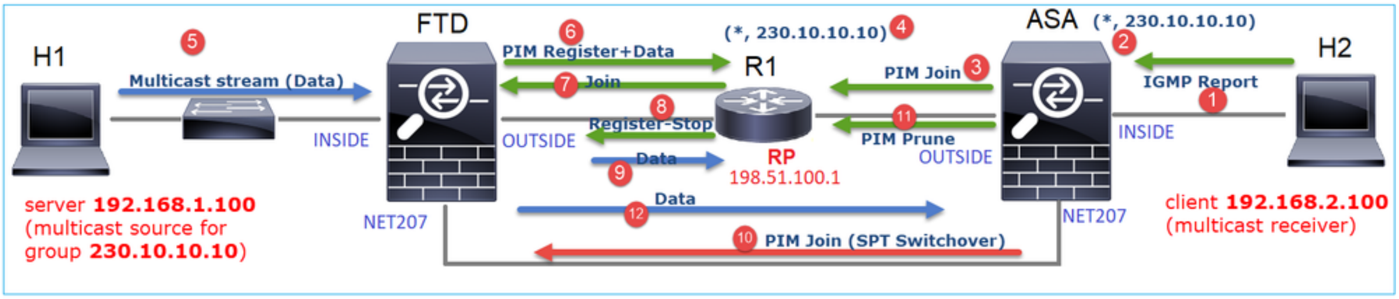
```
firepower#

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
```

要驗證在慢速路徑與快速路徑與控制點中處理的資料包數，請執行以下操作：

<#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 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 inter
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 fo
MCAST_FP_UPD_FOR_UNMATCH_IFC        91      Number of times that multicast flow's ifc_out  cannot be
```

顯示逐步發生情況的圖表：



1. 終端主機(H2)傳送IGMP報告以加入組播流230.10.10.10。
2. 最後跳路由器(ASA)（即PIM DR）建立一個(*, 230.10.10.10)條目。
3. ASA向組230.10.10.10的RP傳送PIM加入消息。
4. RP會建立(*, 230.10.10.10)條目。
5. 伺服器傳送組播流資料。
6. FTD將多點傳播封包封裝在PIM暫存器訊息中，並將其傳送（單點傳播）到RP。此時，RP看到他有一個活動接收器，解除封裝組播資料包，並將它們傳送到接收器。
7. RP向FTD傳送PIM加入訊息以加入多點傳送樹。
8. RP向FTD傳送PIM註冊停止訊息。
9. FTD將本機多點傳送流（無PIM封裝）傳送到RP。
10. 最後一跳路由器(ASA)發現源(192.168.1.100)具有來自NET207介面的更好路徑並開始切換。

它向上游裝置(FTD)傳送PIM加入消息。

11. 最後一跳路由器向RP傳送PIM修剪消息。
12. FTD將多點傳播流轉送到NET207介面。ASA從共用樹（RP樹）移動到源樹(SPT)。

任務2 — 配置PIM引導路由器(BSR)

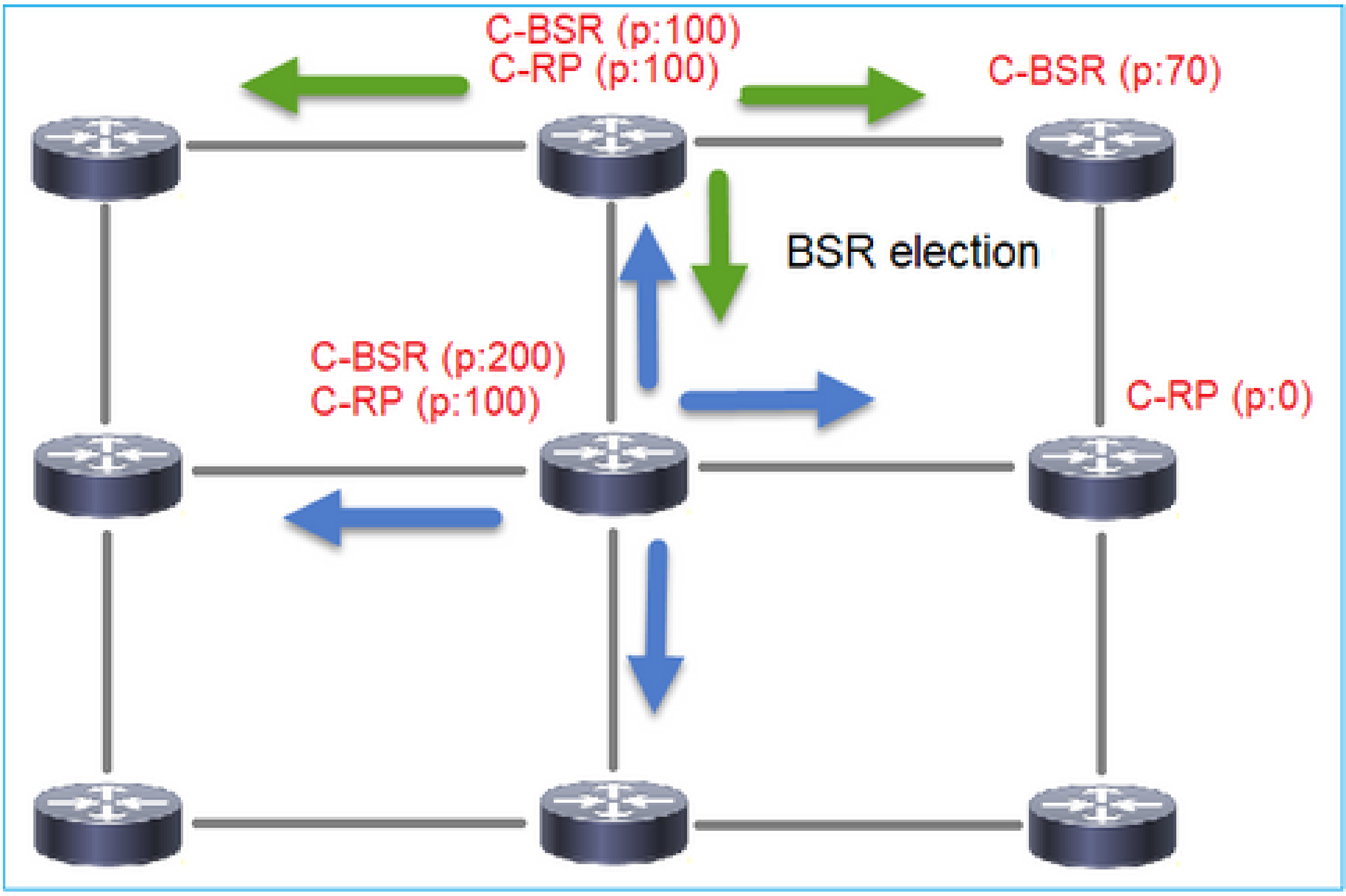
BSR基礎知識

- BSR(RFC 5059)是一種使用PIM協定並允許裝置動態瞭解RP資訊的控制平面組播機制。
- BSR定義：
  - 候選RP(C-RP)：希望成為RP的裝置。
  - 候選BSR(C-BSR)：想要成為BSR並向其他裝置通告RP集的裝置。
  - BSR：在許多C-BSR中選擇了BSR的裝置。最高的BSR優先順序會贏得選舉。
  - RP-set：所有C-RP及其優先順序的清單。
  - RP：具有最低RP優先級的裝置將獲得選擇。
  - BSR PIM消息（空）：用於BSR選擇的PIM消息。
  - BSR PIM消息（正常）：傳送到224.0.0.13 IP並包含RP集和BSR資訊的PIM消息。

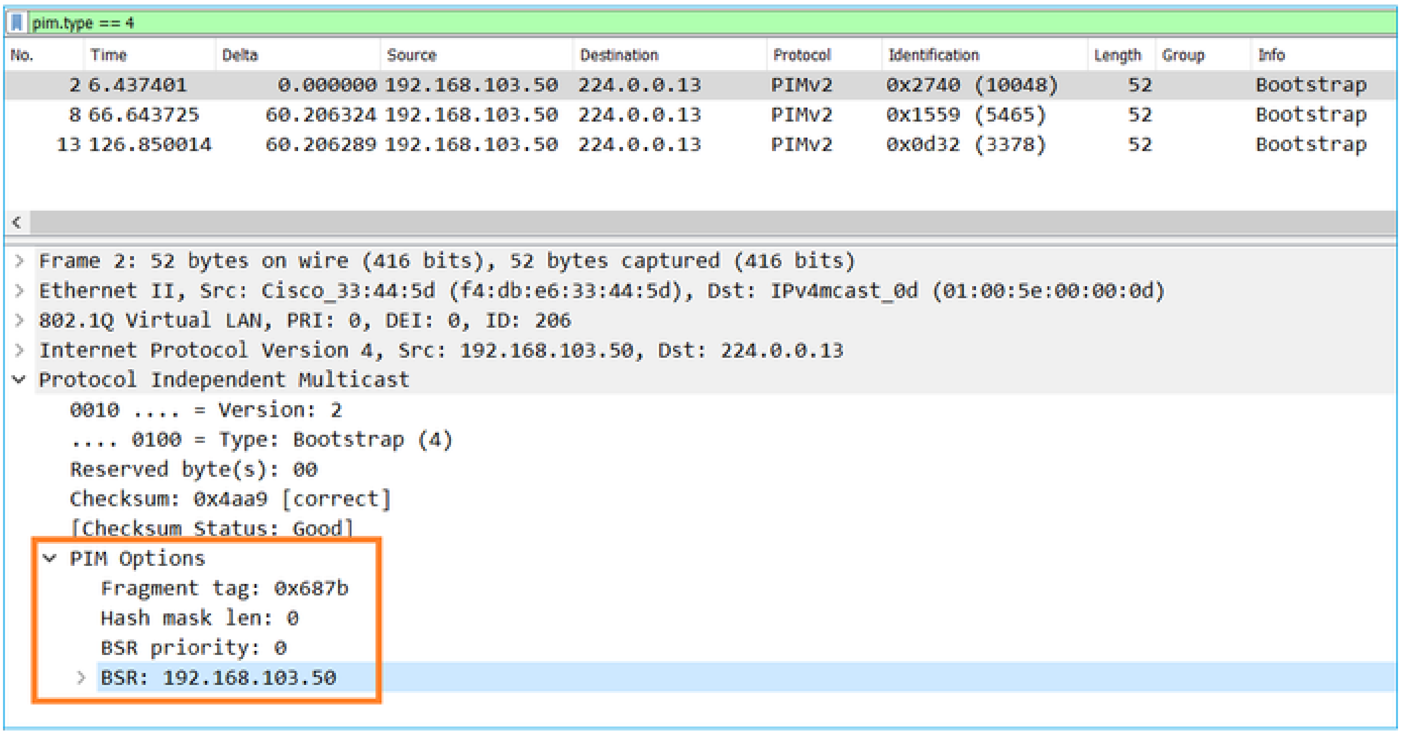
BSR的工作原理

1. BSR選舉機制。

每個C-BSR傳送包含優先順序的PIM BSR空消息。具有最高優先順序的裝置（回退是最高的IP）將贏得選舉並成為BSR。其餘裝置不再傳送任何空BSR消息。



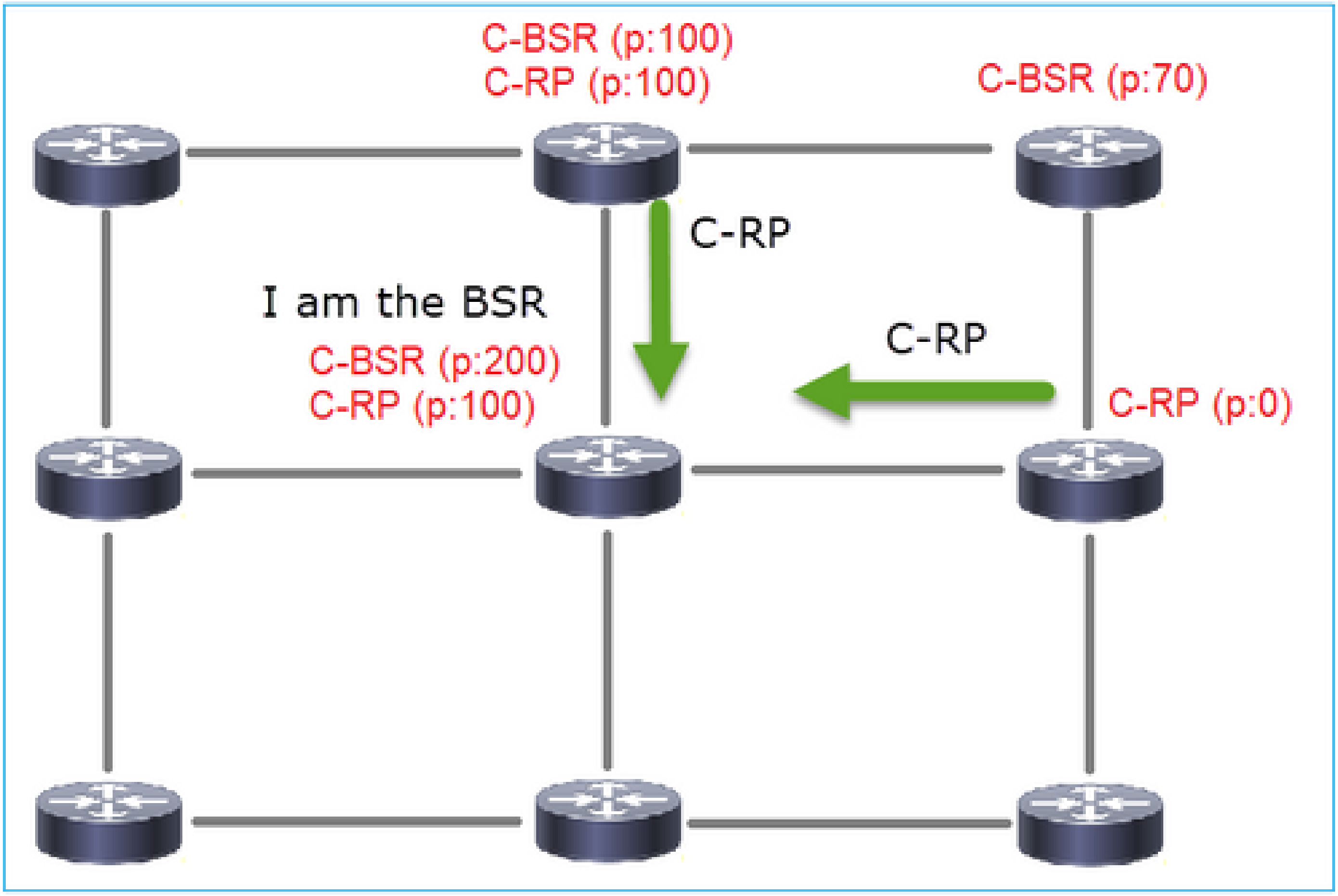
選舉過程中使用的BSR消息僅包含C-BSR優先順序資訊：



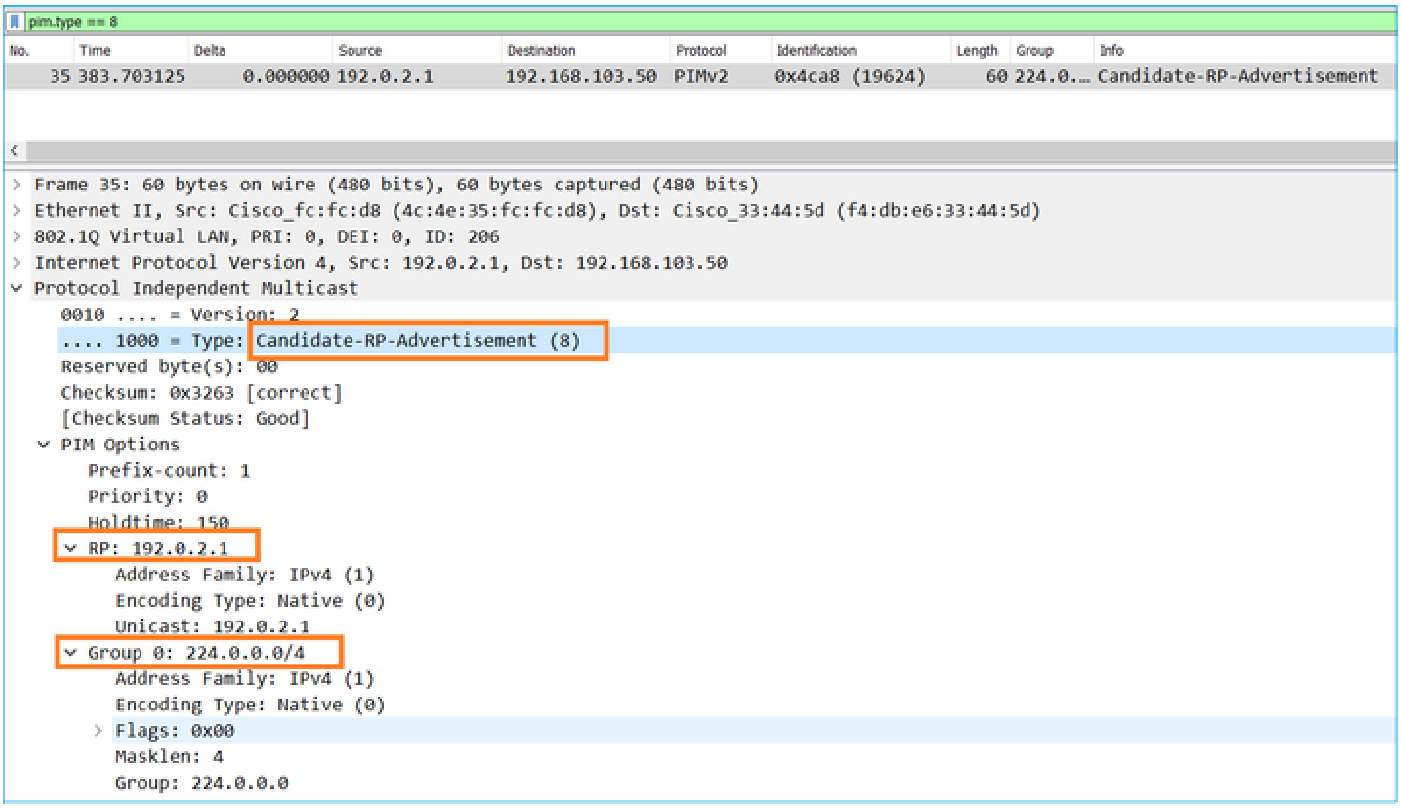
```
pim.type == 4

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

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

要在Wireshark中顯示BSR消息，請使用此顯示過濾器：pim.type == 4

2. C-RP向包含其C-RP優先順序的BSR傳送單播BSR消息：



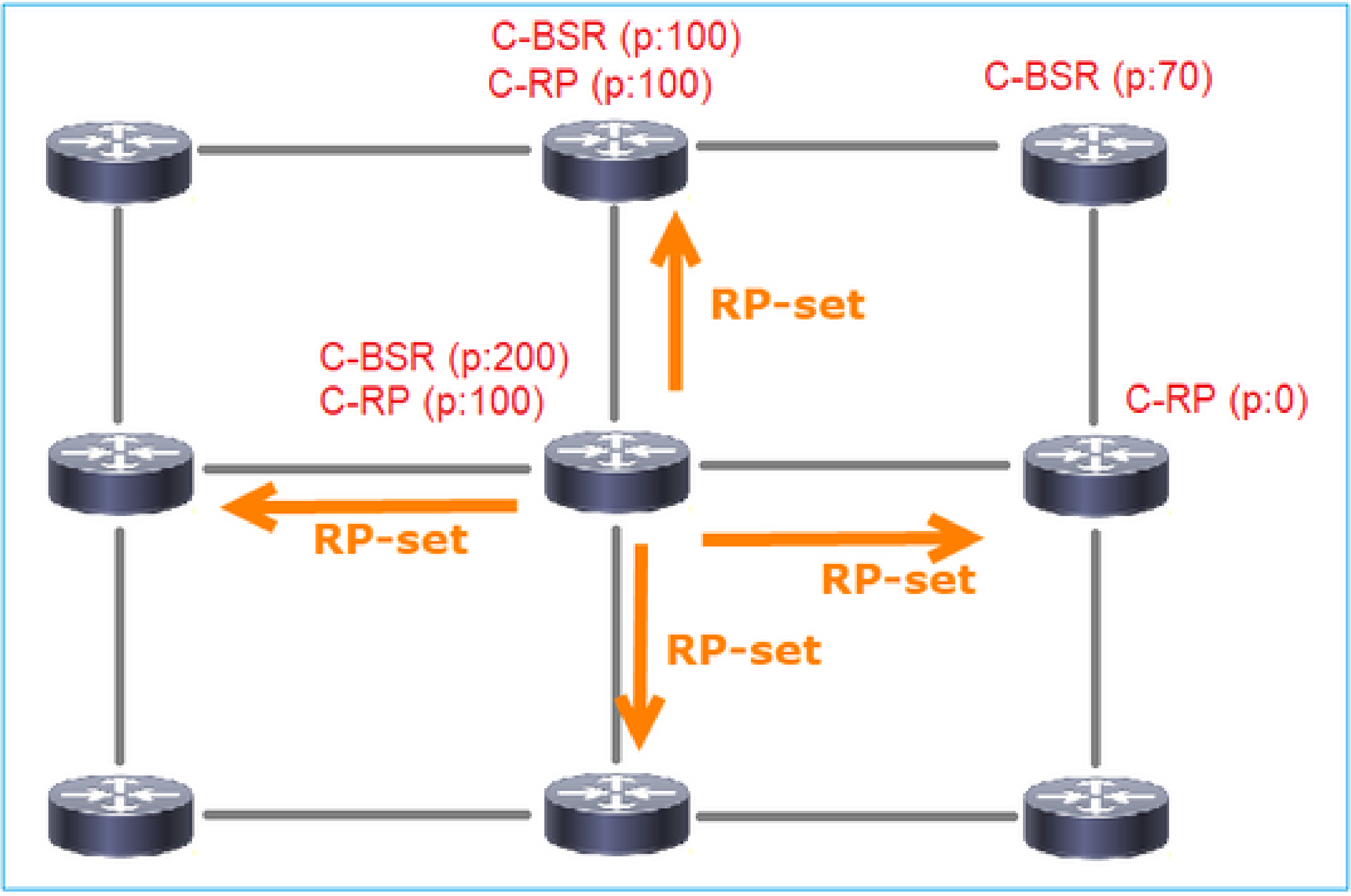
候選RP消息：

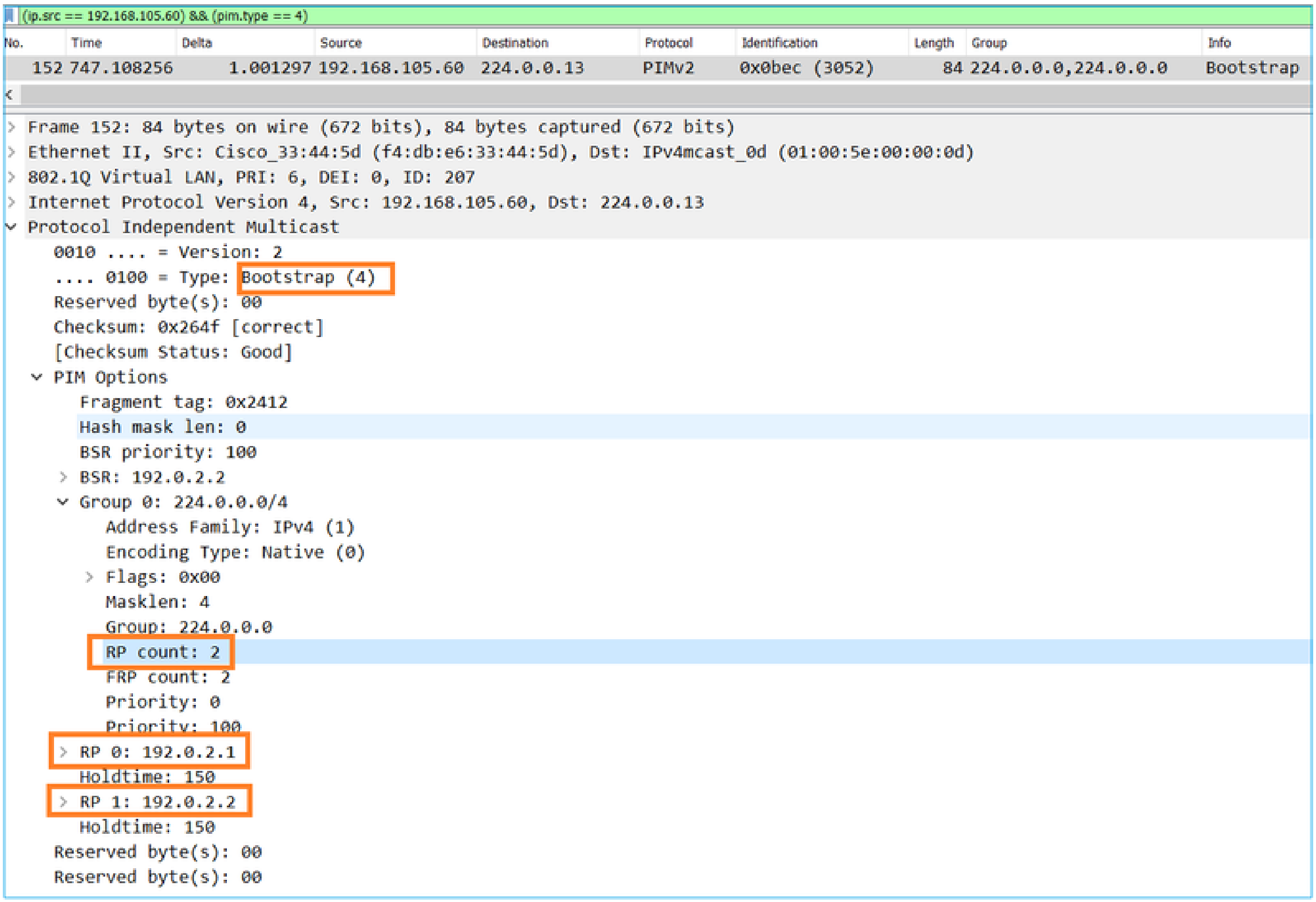


```
pim.type == 8
No.  Time        Delta     Source      Destination     Protocol Identification  Length Group    Info
  35 383.703125  0.000000  192.0.2.1   192.168.103.50  PIMv2    0x4ca8 (19624)      60 224.0.… Candidate-RP-Advertisement

> 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
```

要在Wireshark中顯示BSR消息，請使用此顯示過濾器：pim.type == 8

3. BSR構成RP集並將其通告給所有PIM鄰居：

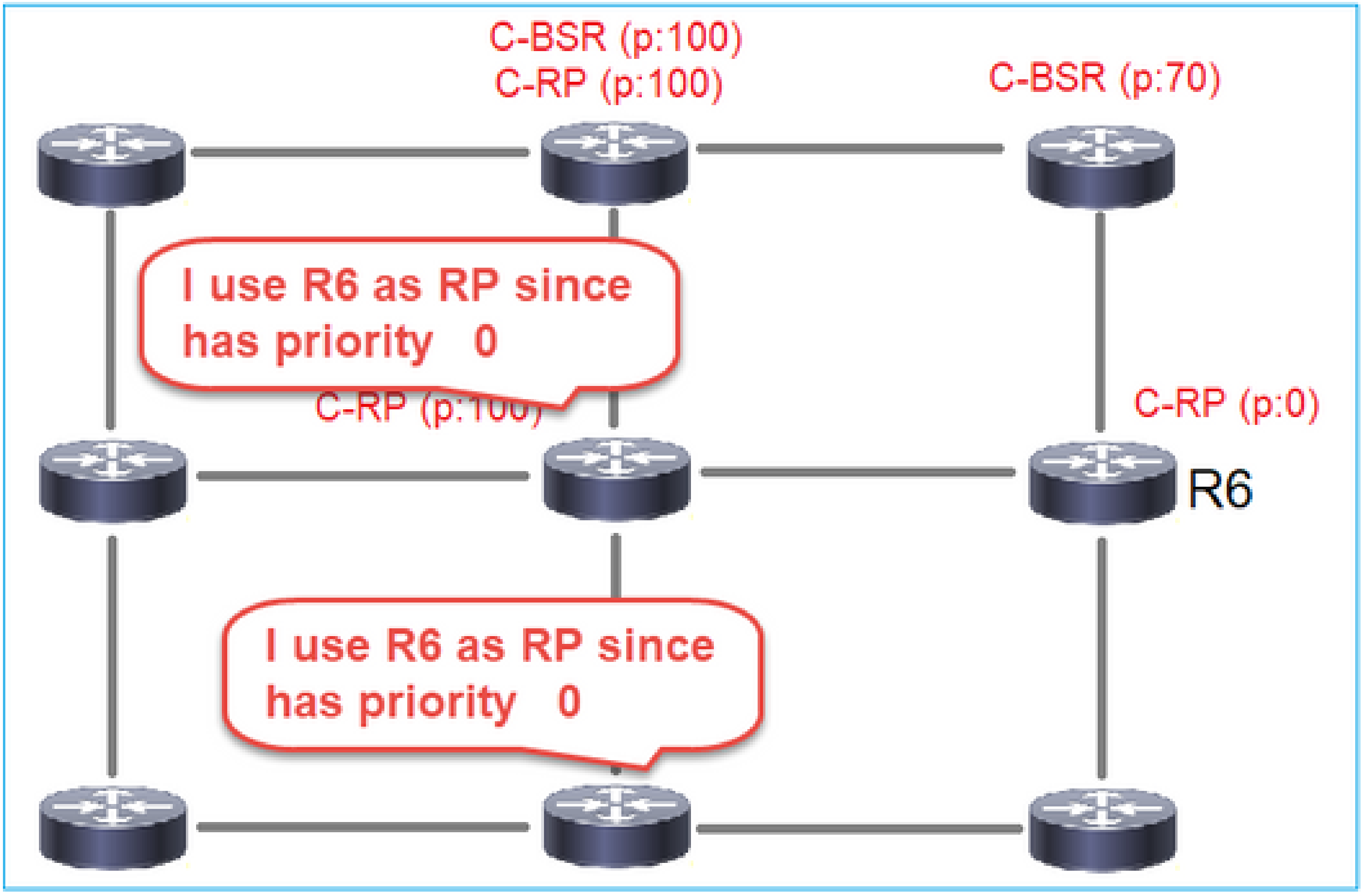




```
(ip.src == 192.168.105.60) && (pim.type == 4)
No.  Time        Delta     Source          Destination  Protocol  Identification  Length  Group                Info
 152 747.108256  1.001297  192.168.105.60  224.0.0.13   PIMv2     0x0bec (3052)       84  224.0.0.0,224.0.0.0  Bootstrap
```

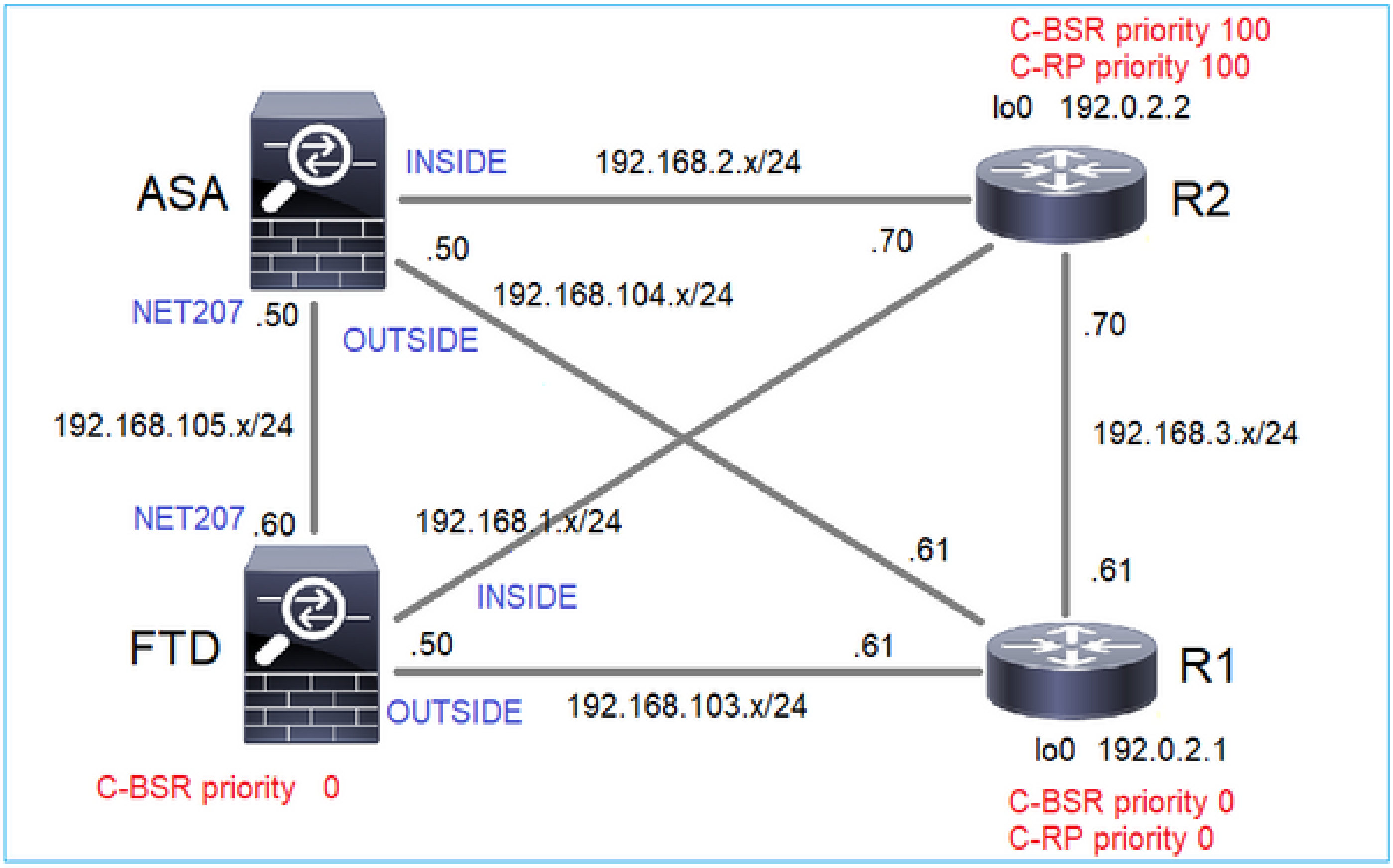
```
> Frame 152: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
> Ethernet II, Src: Cisco_33:44:5d (f4:db:e6:33:44:5d), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
> 802.1Q Virtual LAN, PRI: 6, DEI: 0, ID: 207
> Internet Protocol Version 4, Src: 192.168.105.60, Dst: 224.0.0.13
v Protocol Independent 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/防火牆獲取RP集並根據最低優先順序選擇RP:


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

任務需求

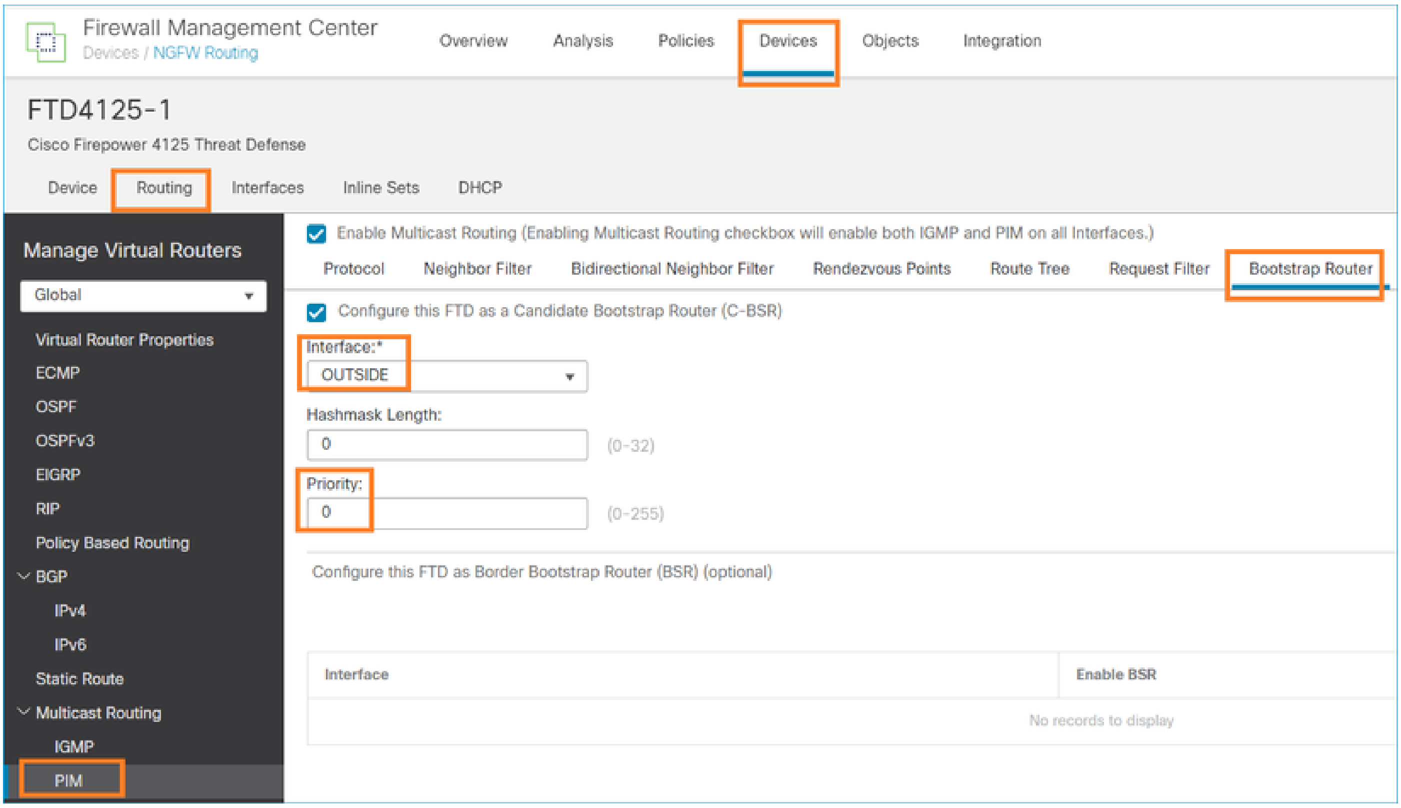
根據以下拓撲配置C-BSR和C-RP:



對於此任務，FTD必須在OUTSIDE介面上以C-BSR的身份通告，且BSR優先順序為0。

解決方案

FTD的FMC組態：



FTD4125-1

Cisco Firepower 4125 Threat Defense

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

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

Interface:* OUTSIDE

Hashmask Length: 0 (0-32)

Priority: 0 (0-255)

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

Interface	Enable BSR
No records to display	

部署的配置：

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

其他裝置上的組態：

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)
```

在R2上相同，但具有不同的C-BSR和C-RP優先順序

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

在ASA上，僅全域性啟用組播。這將在所有介面上啟用PIM:

```
multicast-routing
```

驗證

R2是選擇的BSR，因為具有最高優先順序：

<#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
```

由於優先順序最低，R1被選為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
```

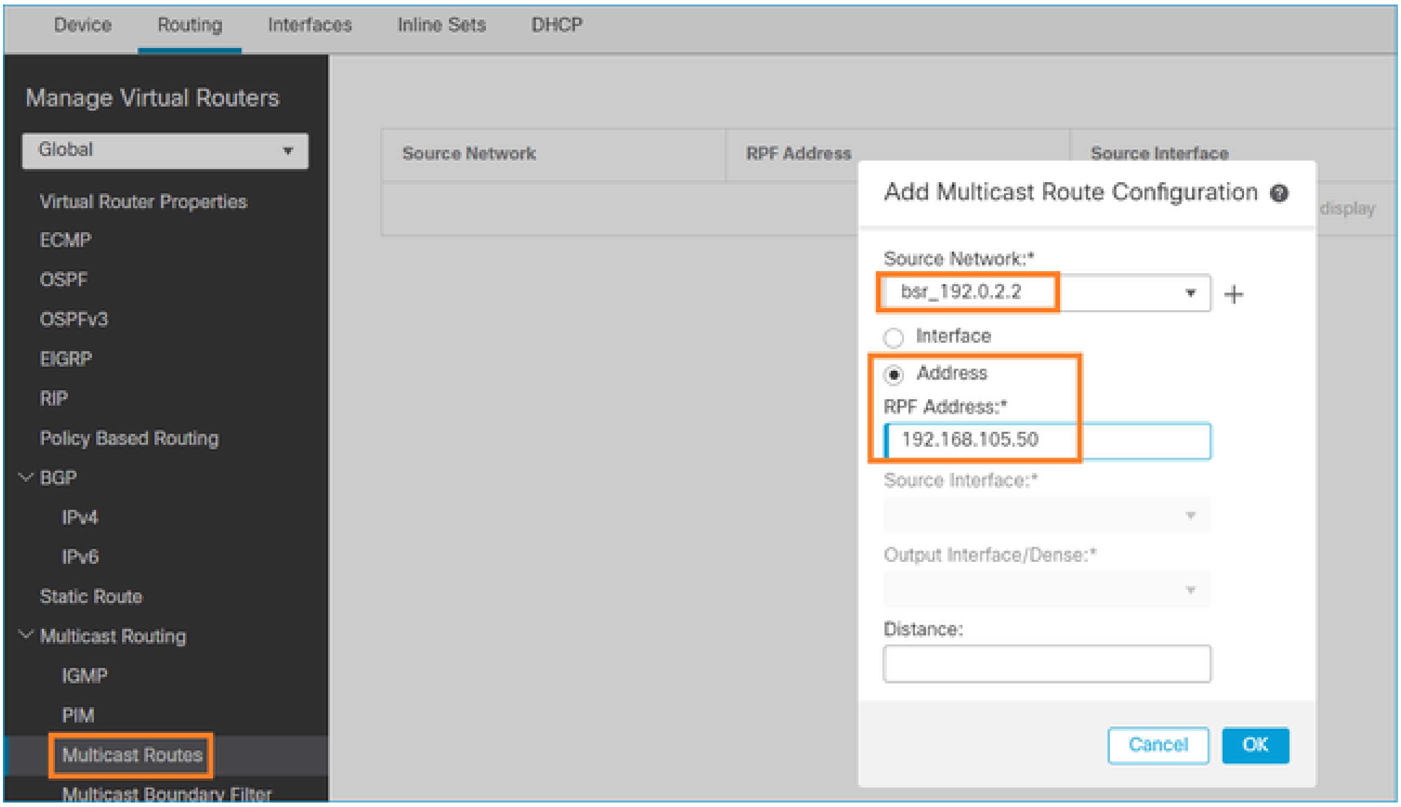
```
*

       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消息需進行RPF檢查。您可以啟用debug pim bsr以驗證這點：

<#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介面，可以配置靜態路由。在本示例中，防火牆接受來自IP 192.168.105.50的BSR消息：



Add Multicast Route Configuration

Source Network:* bsr_192.0.2.2

○ Interface

● Address

RPF Address:* 192.168.105.50

Source Interface:*

Output Interface/Dense:*

Distance:

<#root>

```
firepower#

show run mroute

mroute 192.0.2.2 255.255.255.255 192.168.105.50
```

<#root>

```
firepower#

show pim bsr-router


PIMv2 BSR information

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


RPF: 192.168.105.50,NET207

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

現在，NET207介面上的BSR消息被接受，但INSIDE上的消息被丟棄：

<#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
```

在防火牆上啟用含有追蹤軌跡的擷取，並檢查BSR訊息的處理方式：

<#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連線將在防火牆上終止，因此為使跟蹤顯示有用資訊，需要清除與框的連線：

<#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
```

如果由於RPF故障而丟棄PIM資料包，跟蹤將顯示：

<#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表丟棄並捕獲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
```

捕獲由於RPF故障而丟棄的資料包：

<#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

防火牆的故障排除方法主要取決於防火牆在組播拓撲中的作用。以下是疑難排解的建議步驟清單：

1. 明確問題說明和症狀的詳情。嘗試將範圍縮小到控制平面(IGMP/PIM)或資料平面（組播流）問題。
2. 對防火牆上的組播問題進行故障排除的強制性前提是澄清組播拓撲。 您至少需要確定：
   - 組播拓撲中防火牆的角色 — FHR、LHR、RP或其他中間角色。
   - 防火牆上的預期組播入口和出口介面。
   - RP。
   - 發件人源IP地址。
   - 組播組IP地址和目標埠。
   - 組播流的接收器。

3.確定組播路由的型別- Stub或PIM組播路由：

- 末節組播路由 — 它提供動態主機註冊，並方便組播路由。當配置為末節組播路由時，ASA將充當IGMP代理。ASA不是完全參與組播路由，而是將IGMP消息轉發到上游組播路由器，後者設定組播資料的傳送。要識別末節模式路由，請使用show igmp interface命令並檢查IGMP轉發配置：

<#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)
```

介面上啟用了PIM；但是未建立鄰居關係：

<#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轉發不同時支援。

您無法配置諸如RP地址之類的選項：

<#root>

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

- PIM組播路由 - PIM組播路由是最常見的部署。防火牆同時支援PIM-SM和雙向PIM。PIM-SM是一種組播路由協定，它使用底層單播路由資訊庫或獨立的支援組播的路由資訊庫。它為每個組播組建立根於單個集結點(RP)的單向共用樹，並根據需要為每個組播源建立最短路徑樹。在此部署模式下，與末節模式不同，使用者通常配置RP地址配置，防火牆與對等體建立PIM鄰接關係：

<#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.檢查RP IP地址是否已配置和可訪問性：

<#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：防火牆不能同時為RP和FHR。

5.根據防火牆在組播拓撲中的角色和問題症狀，檢查其他輸出。

FHR

- 檢查接口Tunnel0狀態。此介面用於封裝PIM負載內的原始組播流量，並將單播資料包傳送到RP，RP設定了PIM暫存器位：

<#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
```

- 檢查路由：

<#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.
```

當防火牆收到具有註冊停止位的PIM資料包時，會從OIL中刪除Tunnel0。接著，防火牆會停止封裝，並透過輸出介面傳送原始多點傳播流量：

<#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
```

- 檢查PIM暫存器計數器：

<#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
```

- 檢查防火牆和RP之間的單播PIM資料包捕獲：

<#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
```

- 收集其他輸出（x.x.x.x是組播組，y.y.y.y是RP IP）。建議收集輸出幾次:

<#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
```

- 收集原始組播介面資料包和ASP丟棄捕獲。

<#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
```

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

- 系統日誌消息 — 常見ID是302015、302016和710005。

RP

- 檢查介面Tunnel0狀態。此介面用於封裝PIM負載內的原始多點傳播流量，並將單點傳播封包傳送到FHR，以進行設定PIM-stop位元：

<#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         -
```

- 檢查路由：

<#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
```

- 檢查PIM計數器：

<#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
```

- 收集其他輸出（x.x.x.x是組播組，y.y.y.y是RP IP）。建議收集輸出幾次:

<#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
```

- 收集原始組播介面資料包和ASP丟棄捕獲：

<#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 — 公共ID是302015、302016和710005。

LHR

請考慮有關RP和這些附加檢查一節中提到的步驟：

- 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組：

<#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流量統計資訊：

<#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（備忘單）

指令	說明
show running-config multicast-routing	檢視防火牆上是否已啟用多點傳送路由
show run mroute	檢視防火牆上配置的靜態路由
show running-config pim	檢視防火牆上的PIM配置
show pim interface	檢視哪些防火牆介面啟用了PIM和PIM鄰居。
show pim neighbor	檢視PIM鄰居

show pim group-map	檢視對映到RP的組播組
show mroute	檢視完整的組播路由表
show mroute 230.10.10.10	檢視特定組播組的組播表
show pim tunnel	檢視防火牆和RP之間是否構建了PIM隧道
show conn all detail address RP_IP_ADDRESS	檢視防火牆和RP之間是否已建立連線（PIM隧道）
show pim topology	檢視防火牆PIM拓撲輸出
debug pim	此調試顯示進出防火牆的所有PIM消息
debug pim group 230.10.10.10	此調試顯示特定組播組的防火牆和防火牆之間的所有PIM消息
show pim traffic	檢視有關已接收和已傳送PIM消息的統計資訊
show asp cluster counter	驗證慢速路徑與快速路徑與控制點中處理的資料包數
show asp drop	檢視防火牆上的所有軟體級丟棄
capture CAP interface INSIDE trace match pim any any	在防火牆上捕獲和跟蹤輸入PIM組播資料包
capture CAP interface INSIDE trace match udp host 224.1.2.3 any	捕獲和跟蹤入口組播流
show pim bsr-router	驗證誰是被選擇的BSR路由器
show conn all address 224.1.2.3	顯示父組播連線

show local-host 224.1.2.3	顯示子/末節組播連線

有關防火牆捕獲檢查的詳細資訊：使用Firepower威脅防禦捕獲和Packet Tracer

已知的問題

Firepower組播限制：

- 不支援IPv6。
- 流量區域(EMCP)中的介面不支援PIM/IGMP組播。
- 防火牆不能同時是RP和FHR。
- show conn all命令僅顯示身份組播連線。要顯示末節/輔助組播連線，請使用show local-host <group IP>命令。

vPC Nexus不支援PIM

如果您嘗試在Nexus vPC和防火牆之間部署PIM鄰接關係，則存在Nexus限制，如下所述：

在 Nexus 平台上透過虛擬連接埠通道進行路由時所支援的拓撲

從NGFW的角度來看，您在使用跟蹤的捕獲中看到此丟棄:

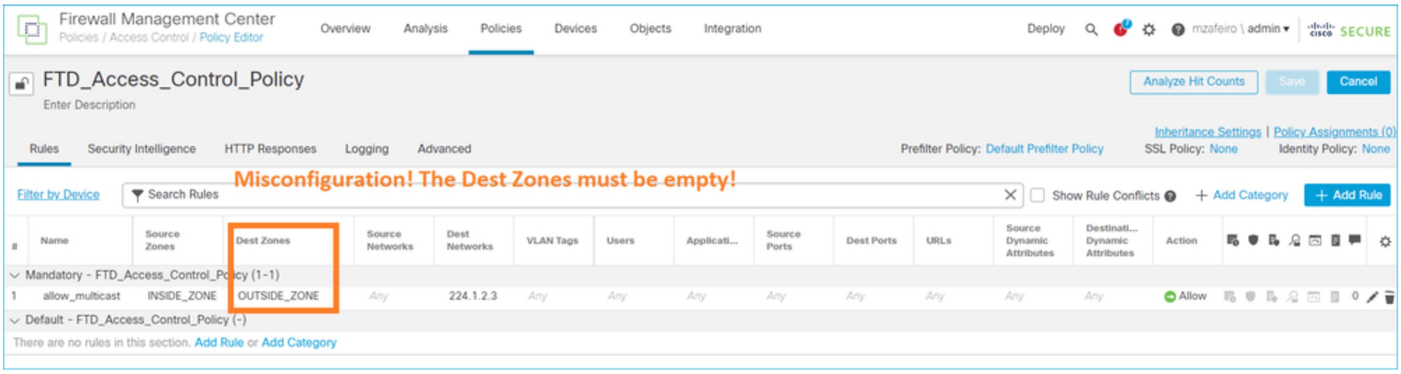
```
<#root>

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
```

防火牆無法完成RP註冊：

```
<#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
```

不支援目標區域

您不能為匹配組播流量的訪問控制策略規則指定目標安全區域：



Firewall Management Center
Policies / Access Control / Policy Editor

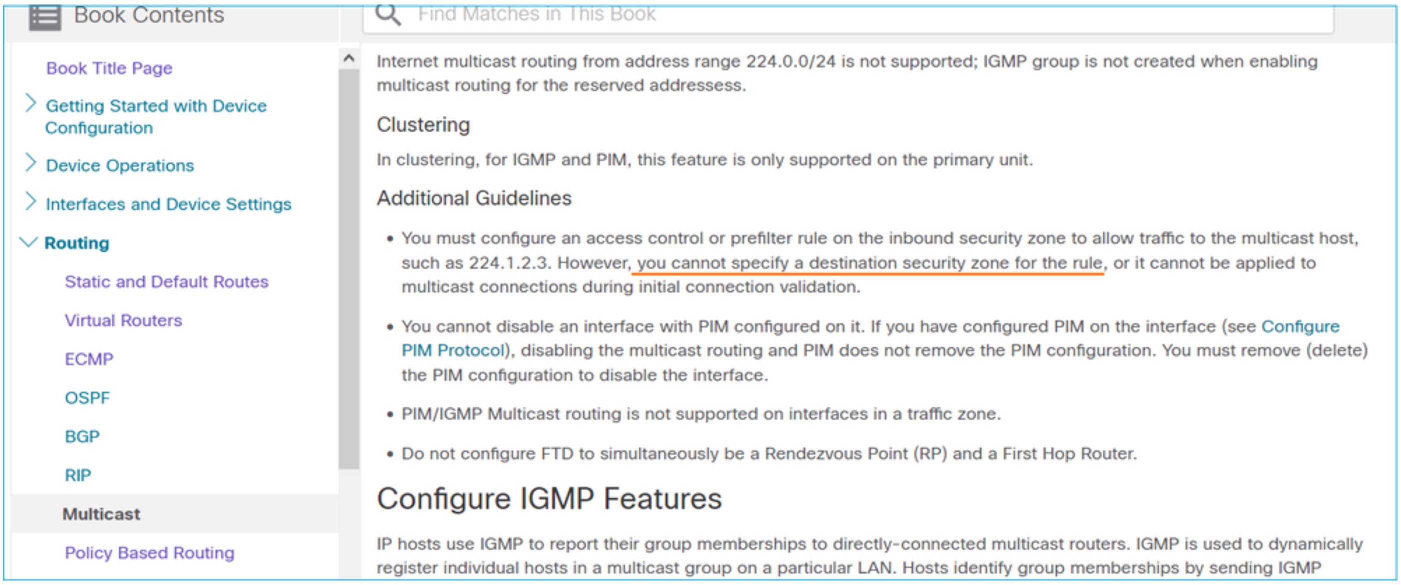
FTD_Access_Control_Policy
Enter Description

Prefilter Policy: Default Prefilter Policy   SSL Policy: None   Identity Policy: None

Misconfiguration! The Dest Zones must be empty!

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destinati... Dynamic Attributes	Action
Mandatory - FTD_Access_Control_Policy (1-1)														
1	allow_multicast	INSIDE_ZONE	OUTSIDE_ZONE	Any	224.1.2.3	Any	Any	Any	Any	Any	Any	Any	Any	Allow
Default - FTD_Access_Control_Policy (-)														
There are no rules in this section. Add Rule or Add Category														

FMC使用手冊中也有相關說明：



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

Internet multicast routing from address range 224.0.0/24 is not supported; IGMP group is not created when enabling multicast routing for the reserved addressess.

Clustering

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

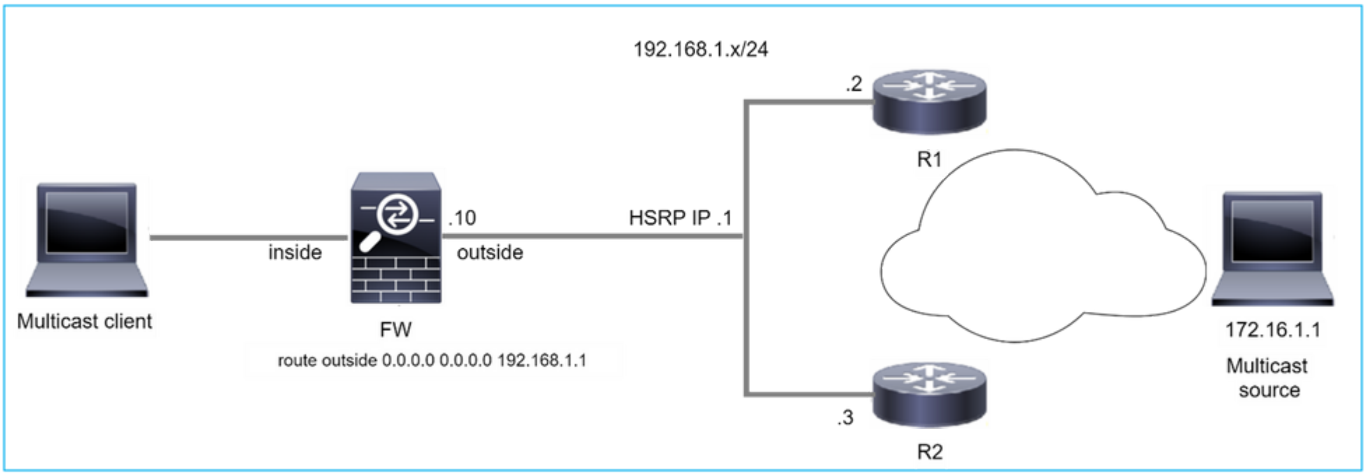
Additional Guidelines

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

Configure IGMP Features

IP hosts use IGMP to report their group memberships to directly-connected multicast routers. IGMP is used to dynamically register individual hosts in a multicast group on a particular LAN. Hosts identify group memberships by sending IGMP

由於HSRP，防火牆不會向上游路由器傳送PIM消息



在這種情況下，防火牆具有經由熱待命備援通訊協定(HSRP)IP 192.168.1.1和路由器R1和R2的PIM鄰居關係的預設路由：

<#root>

```
firepower#

show run route

route outside 0.0.0.0 0.0.0.0 192.168.1.1 1
```

防火牆在R1和R2的外部和物理介面IP之間具有PIM鄰接關係：

<#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)
```

防火牆不會將PIM加入消息傳送到上游網路。PIM debug指令debug pim 顯示以下輸出：

<#root>

```
firepower#

debug pim
...

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

RFC 2362指出「路由器定期向與每個(S，G)、(*,G)和(*,*,RP)條目關聯的每個不同RPF鄰居傳送加入/修剪消息。只有當RPF鄰居是PIM鄰居時，才會傳送加入/修整消息。

為緩解此問題，使用者可在防火牆上新增靜態mroute條目。路由器必須指向兩個路由器介面IP地址之一192.168.1.2或192.168.1.3，通常是HSRP活動路由器IP。

範例：

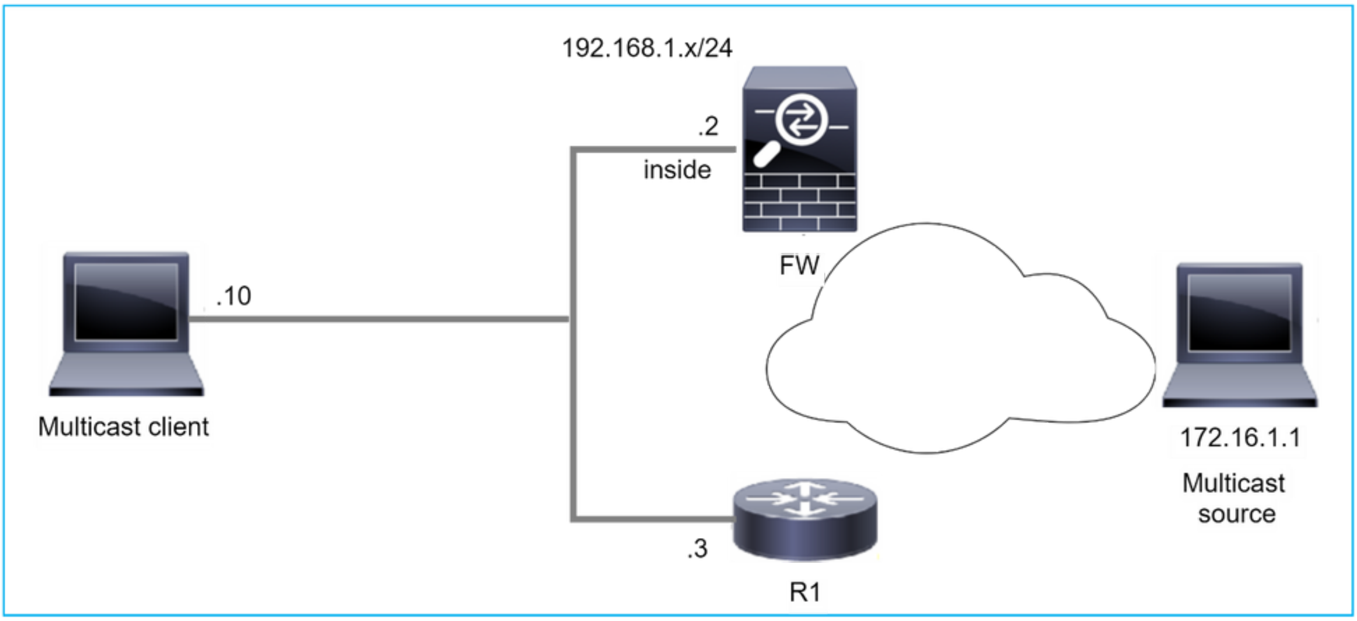
<#root>

```
firepower#

show run mroute


firepower#

mroute 172.16.1.1 255.255.255.255 192.168.1.2
```

在靜態mroute配置到位後，對於RPF查詢，防火牆將優先使用組播路由表而不是ASA的單播路由表，並將PIM消息直接傳送到鄰居192.168.1.2。

注意：靜態mroute在某些方面削弱了HSRP冗餘的實用性，因為mroute僅接受每個地址/網路掩碼組合的1個下一跳。如果mroute命令中指定的下一個躍點失敗或無法訪問，防火牆不會回退到另一個路由器。

當防火牆不是LAN網段中的DR時，不將其視為LHR



防火牆將R1作為LAN網段中的PIM鄰居。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)
```

如果收到來自客戶端的IGMP加入請求，則防火牆不會成為LHR。

mroute顯示其他Null作為OIL，並具有Pruned標誌：

```
<#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
```

要使防火牆成為LHR，可以增加介面DR優先順序。

```
<#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指令debug pim 顯示以下輸出：

<#root>

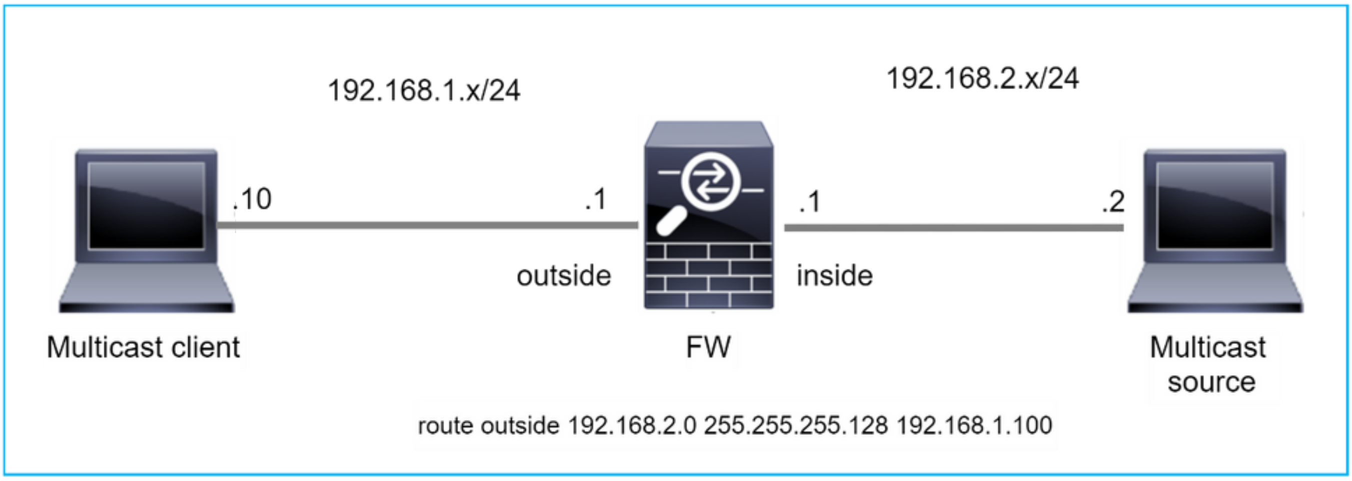
```
firepower#

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標誌和Null從mroute中刪除：

<#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
```

由於反向路徑轉發檢查失敗，防火牆丟棄組播資料包



在這種情況下，由於RPF故障，組播UDP資料包將被丟棄，因為防火牆通過外部介面具有掩碼為255.255.255.128的更具體的路由。

<#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丟棄捕獲顯示違反rpf的丟棄原因：

<#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
```

MFIB輸出中的RPF失敗計數器增加：

<#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
```

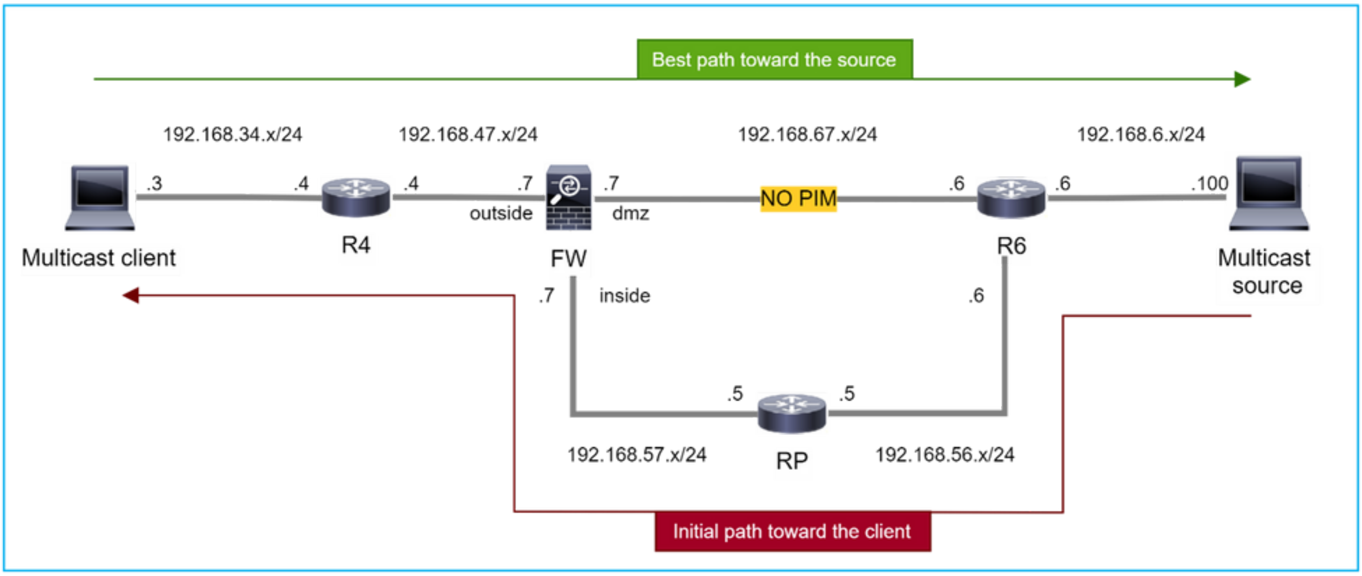
解決方案是修復RPF檢查失敗。一個選擇是刪除靜態路由。

如果沒有其他RPF檢查失敗，則會轉發資料包，且MFIB輸出中的Forwarding計數器會增加：

<#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
```

Firewall does not Generate PIM join when PIM Switchover to Source-tree（在PIM切換到源樹時，防火牆不會生成PIM加入）



在本例中，防火牆通過dmz介面R4 > FW > R6獲知通向組播源的路徑，而從源到客戶端的初始流量路徑為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
```

一旦達到SPT切換閾值，R4會啟動SPT切換並傳送源特定的PIM加入消息。在防火牆中不會發生SPT切換，(S，G)mroute沒有T標志：

<#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 debug命令debug pim 顯示從對等體R4接收的2個PIM加入請求 — 針對(*,G)和(S，G)。防火牆向(*,G)上游傳送了PIM加入請求，並且由於鄰居192.168.67.6無效而無法傳送源特定請求：

<#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命令輸出缺少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
```

在防火牆介面dmz上啟用PIM:

<#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介面上禁用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
```

解決方案是在R6的GigabitEthernet0/3介面上啟用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
```

防火牆安裝T標誌，表示SPT切換:

<#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
```

防火牆由於轉發速率限制而丟棄前幾個資料包

當防火牆在FP中收到新組播流的第一個資料包時，可能需要由CP進行額外處理。在這種情況下，FP通過SP(FP > SP > CP)將資料包轉發到CP以進行其他操作：

- 在FP中輸入介面和身份介面之間建立父連線。
- 其他特定於組播的檢查，例如RPF驗證、PIM封裝（如果防火牆是FHR）、OIL檢查等。
- 在mroute表中建立具有傳入和傳出介面的(S，G)條目。
- 在傳入和傳出介面之間在FP中建立子/存根連線。

作為控制平面保護的一部分，防火牆在內部限制向CP傳送資料包的速率。

超出速率的資料包會在中丟棄，並顯示punt-rate-limit drop reason:

<#root>

```
firepower#

show asp drop


Frame drop:


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

使用show asp cluster counter命令驗證從SP傳送到CP的組播資料包數：

<#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 命令驗證FP > CP隊列中的資料包數以及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
```

當填充mroute並在FP中建立父/子連線時，資料包將作為現有連線的一部分在FP中轉發。在這種情況下，FP不會將資料包轉發到CP。

防火牆如何處理新組播流的第一個資料包？

當防火牆在資料路徑中收到新組播流的第一個封包時，防火牆會採取以下動作：

1. 檢查安全策略是否允許資料包。
2. 通過路徑FP將資料包轉發到CP。
3. 在入口介面和標識介面之間建立父連線:

<#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
```

系統日誌：

<#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
```

此連線在show conn all 命令的輸出中可見：

<#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通過組播過程執行額外的組播特定檢查，例如RPF驗證、PIM封裝（如果防火牆是FHR）、OIL檢查等。
5. CP建立一個(S，G)條目，該條目中的傳入和傳出介面位於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
```

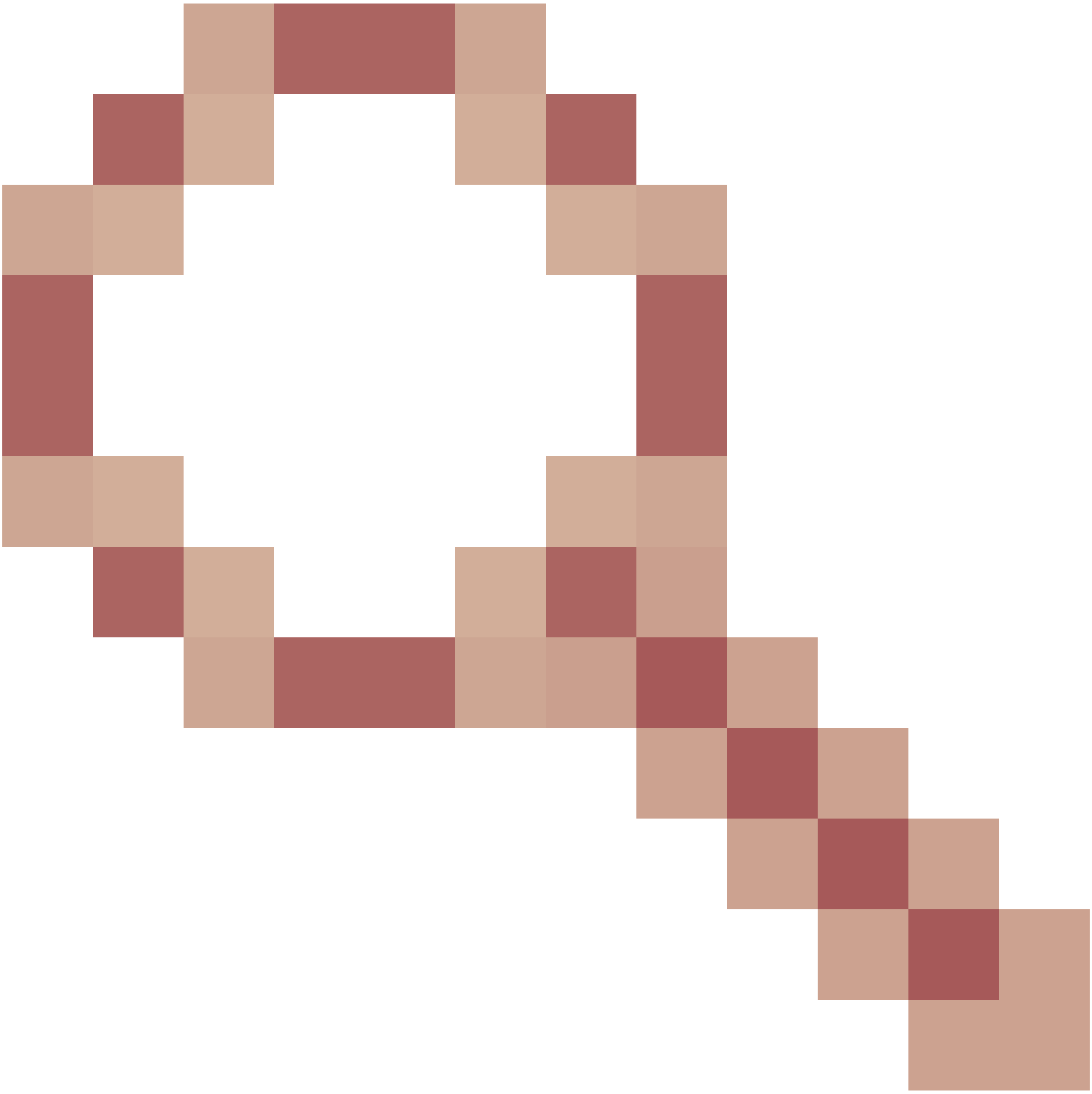
6. CP通過CP > SP > FP路徑指示FP在傳入和傳出介面之間建立子/末節連線：

此連線僅在show local-host命令的輸出中可見：

<#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
```

在修正了思科錯誤ID CSCwe21280的軟體版本中



，還會生成子302015/末節連線的系統日誌消息：

<#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
```

當父連線和子/末節連線都建立時，入口資料包與現有連線匹配，並在FP中轉發：

<#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
```

篩選ICMP多點傳送流量

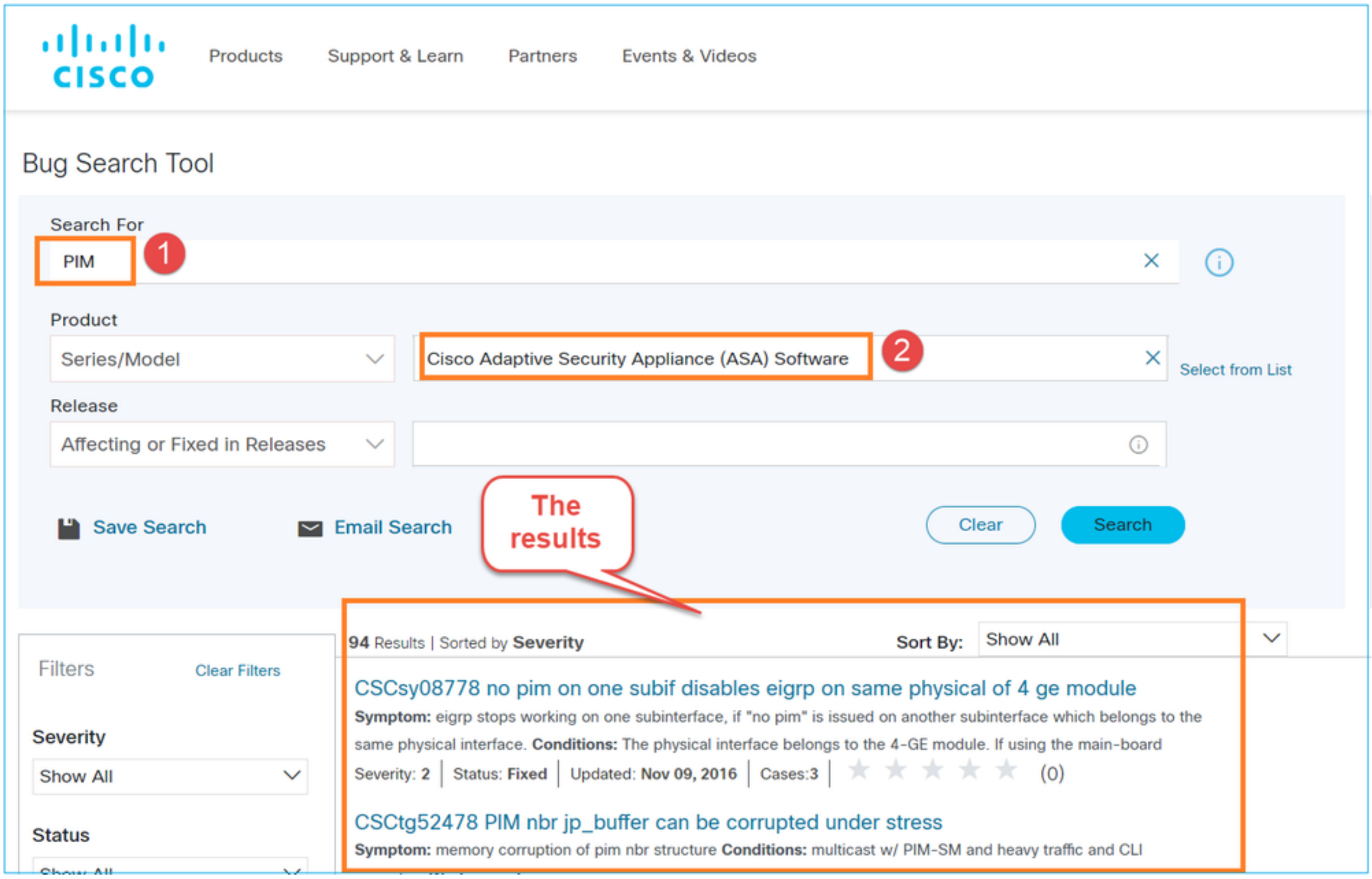
無法使用ACL過濾ICMP多點傳送流量。必須使用控制平面策略(ICMP):

Cisco錯誤ID CSCsl26860 ASA不過濾組播ICMP資料包

已知PIM組播缺陷

您可以使用Bug Search Tool尋找已知缺陷：https://bst.cloudapps.cisco.com/bugsearch

大多數ASA和FTD缺陷列在「Cisco Adaptive Security Appliance(ASA)Software」產品下：



94 Results | Sorted by **Severity**

CSCsy08778 no pim on one subif disables eigrp on same physical of 4 ge module

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

Severity: **2** | Status: **Fixed** | Updated: **Nov 09, 2016** | Cases:**3** | (0)

CSCtg52478 PIM nbr jp_buffer can be corrupted under stress

Symptom: memory corruption of pim nbr structure **Conditions:** multicast w/ PIM-SM and heavy traffic and CLI

相關資訊

- ASA組播故障排除和常見問題
- Firepower管理中心多點傳送
- Firepower組播標誌摘要

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。