Risoluzione dei problemi di Firepower Threat Defense e ASA Multicast PIM

Sommario

Introduzione

In questo documento viene descritto come Firepower Threat Defense (FTD) e Adaptive Security Appliance (ASA) implementano il protocollo PIM (Protocol Independent Multicast).

Prerequisiti

Requisiti

Conoscenze base di routing IP.

Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Premesse

Nozioni di base sul routing multicast

- Unicast inoltra i pacchetti verso la destinazione, mentre **multicast inoltra i pacchetti lontano dall'origine.**
- I dispositivi di rete multicast (firewall/router e così via) inoltrano i pacchetti tramite **RPF (Reverse Path Forwarding).** Notare che RPF non è uguale a uRPF, che viene utilizzato in unicast per prevenire tipi specifici di attacchi. RPF può essere definito come un meccanismo che inoltra i pacchetti multicast allontanandoli dall'origine dalle interfacce che portano ai ricevitori multicast. Il suo ruolo principale è quello di prevenire i loop di traffico e garantire percorsi di traffico corretti.
- Un protocollo multicast come PIM ha tre funzioni principali:

1. Individuare l'**interfaccia a monte** (l'interfaccia più vicina alla sorgente).

2. Individuare le **interfacce a valle** associate a un flusso multicast specifico (interfacce verso i ricevitori).

3. Gestire la struttura multicast (aggiungere o rimuovere le diramazioni della struttura).

- Un albero multicast può essere costruito e gestito mediante uno dei due metodi seguenti: **join impliciti (flood-and-prune)** o **join espliciti (modello pull).** PIM-DM (PIM Dense Mode) utilizza join impliciti, mentre PIM-SM (PIM Sparse Mode) utilizza join espliciti.
- Una struttura multicast può essere **condivisa** o **basata sull'origine:**
  - Le strutture condivise utilizzano il concetto di **Rendezvous Point (RP)** e sono note come **(*, G)** dove G = multicast group IP.
  - Le strutture basate sull'origine hanno la radice all'origine, non utilizzano RP e sono indicate come **(S, G)** dove S = l'IP dell'origine/server multicast.
- Modelli di inoltro multicast:
  - **La** modalità di recapito **AnySource Multicast (ASM)** utilizza alberi condivisi (*, G) da cui qualsiasi origine può inviare il flusso multicast.
  - **SSM (Source-Specific Multicast)** utilizza alberi basati sull'origine (S, G) e l'intervallo IP 232/8.
  - **Bidirezionale (BiDir)** è un tipo di albero condiviso (*, G) in cui sia il traffico del piano di controllo che il traffico del piano dati attraversano l'RP.
- È possibile configurare o selezionare un punto di rendering con uno dei seguenti metodi:
  - RP statica
  - Auto-RP
  - BSR (Bootstrap Router)

Riepilogo modalità PIM

modalità PIM	RP	Albero condiviso	Notazione	IGMP	Supporto ASA/FTD
PIM Sparse Mode	Sì	Sì	(*, G) e (S, G)	v1/v2/v3	Sì

PIM Dense Mode	No	No	(S, G)	v1/v2/v3	No*
PIM Modalità bidirezionale	Sì	Sì	(*, G)	v1/v2/v3	Sì
PIM Source-Specific-Multicast (SSM) Mode	No	No	(S, G)	v3	No**

*Auto-RP = Il traffico Auto-RP può passare attraverso

** ASA/FTD non può essere un dispositivo dell'ultimo hop

Riepilogo configurazione RP

Configurazione di Rendezvous Point	**ASA/FTD**
RP statica	Sì
Auto-RP	No, ma il traffico del control plane Auto-RP può passare attraverso
BSR	Sì, ma non supporto C-RP

Nota: prima di iniziare a risolvere i problemi relativi al multicast, è molto importante avere una visione chiara della topologia multicast. In particolare, è necessario conoscere almeno:
- Qual è il ruolo del firewall nella topologia multicast?
- Chi è l'RP?
- Chi è il mittente del flusso multicast (IP di origine e IP gruppo multicast)?
- Chi riceve lo streaming multicast?
- Si verificano problemi con il Control Plane (IGMP/PIM) o con il Data Plane (multicast stream) stesso?

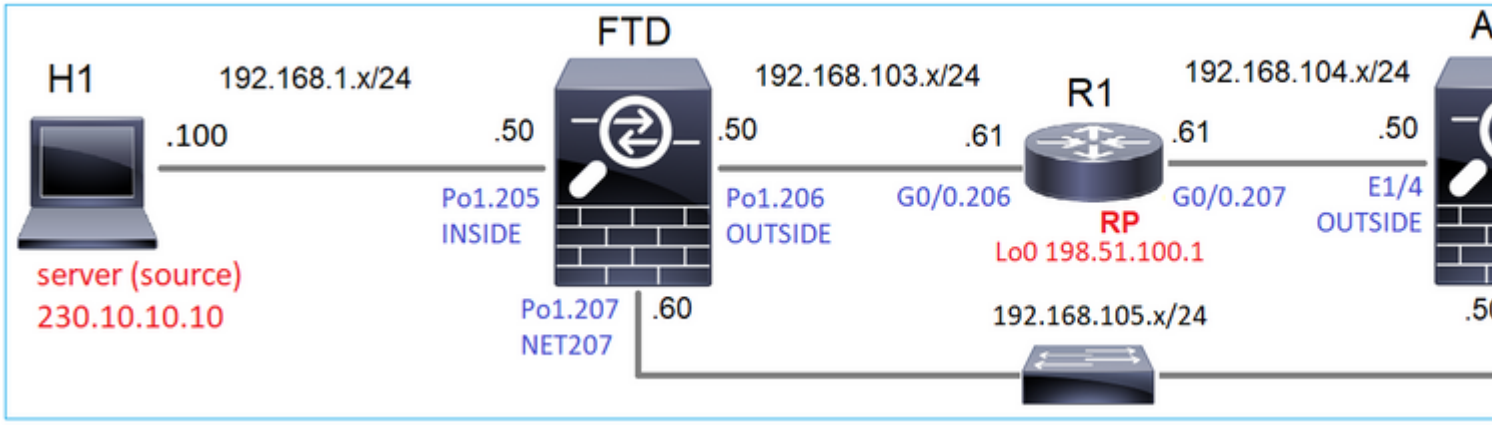
Abbreviazioni/Acronimi

Acronimi	**Spiegazione**
FHR	Router del primo hop: hop connesso direttamente all'origine del traffico multicast.

LHR	Router dell'ultimo hop: hop collegato direttamente ai destinatari del traffico multicast.
RP	Rendezvous-Point
DR.	Router designato
SPT	Albero del percorso più breve
RPT	Struttura ad albero di Rendezvous-Point (RP), albero condiviso
RPF	Inoltro percorso inverso
PETROLIO	Elenco interfacce in uscita
MRIB	Base informazioni routing multicast
MFIB	Base informazioni inoltro multicast
ASM	Multicast Any-Source
BSR	Bootstrap Router
SSM	Multicast specifico dell'origine
FP	Percorso rapido
SP	Percorso lento
PC	Punto di controllo
PPS	Frequenza pacchetti al secondo

Attività 1 - Modalità sparse PIM (RP statica)

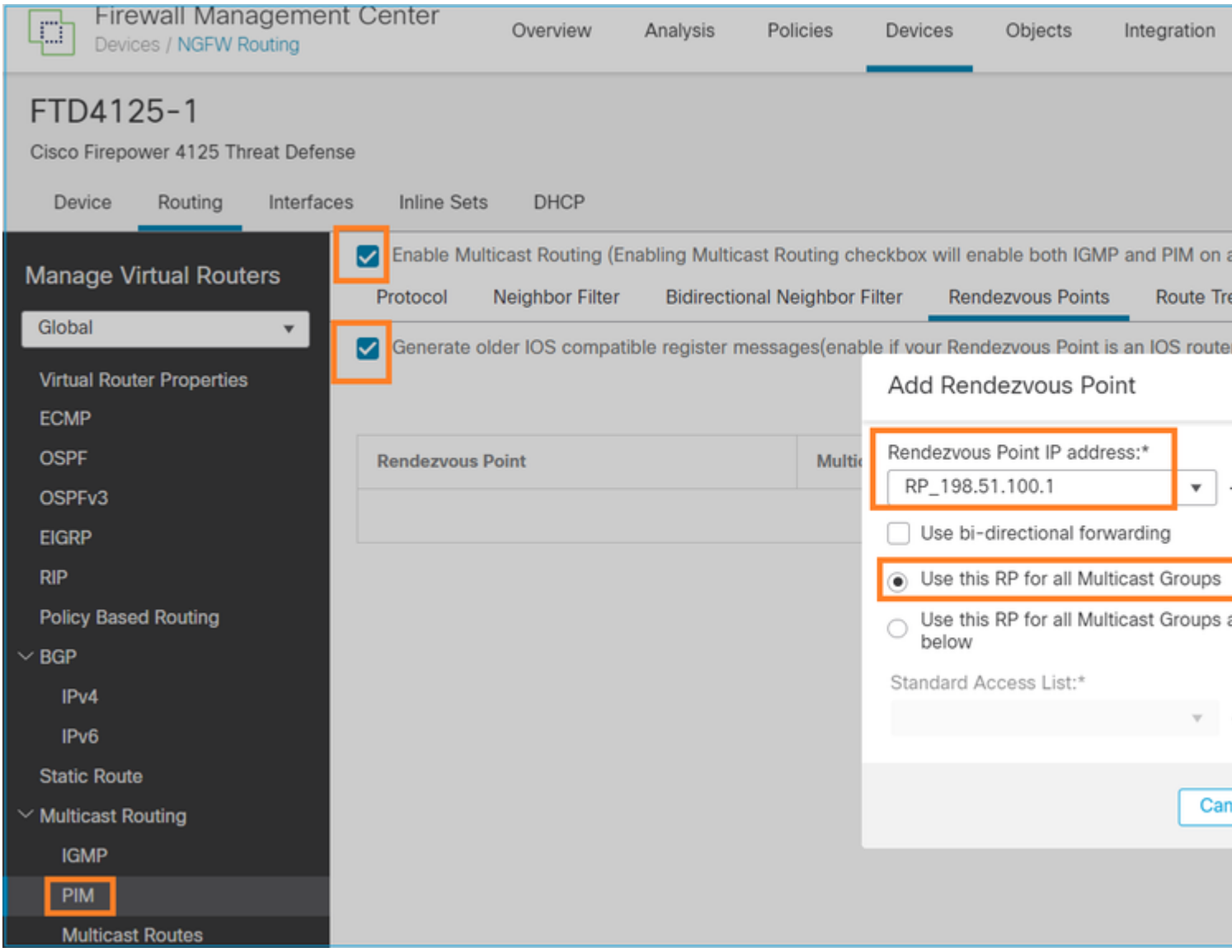
Topologia



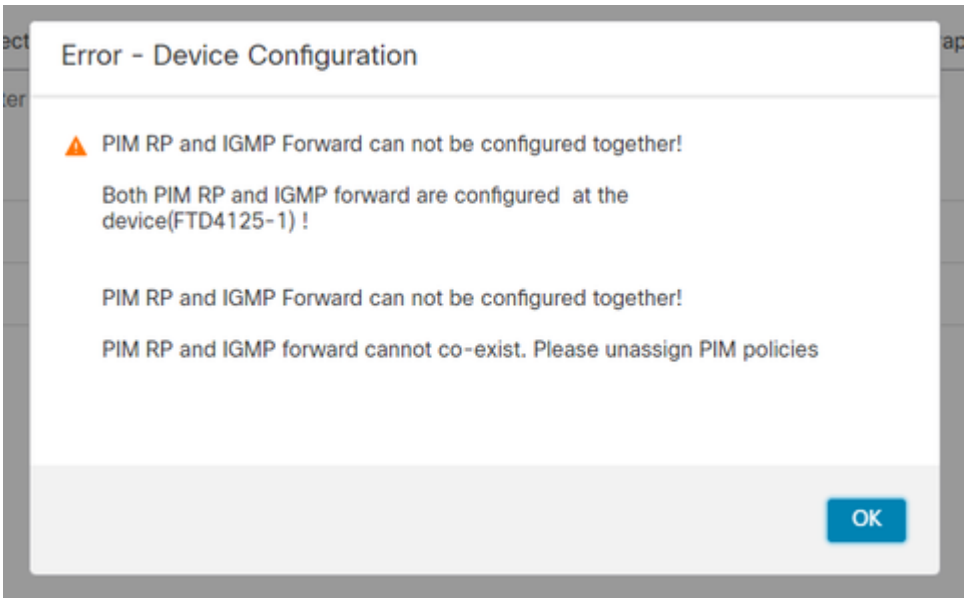
Configurare la modalità sparse PIM multicast nella topologia con R1 (198.51.100.1) come RP.

Soluzione

Configurazione FTD:



Non è possibile configurare l'ASA/FTD per il routing dello stub IGMP e il PIM contemporaneamente:



La configurazione risultante sull'FTD:

<#root>

firepower#

show running-config multicast-routing

multicast-routing

<-- Multicast routing is enabled globally on the device

firepower#

show running-config pim

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

firepower#

ping 198.51.100.1

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

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

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

Sul firewall ASA, la configurazione è simile:

```
<#root>

asa(config)#

multicast-routing


asa(config)#

pim rp-address 198.51.100.1
```

Configurazione RP (router Cisco):

```
<#root>

ip multicast-routing

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

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

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

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

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

 ip ospf 1 area 0
!
interface Loopback0


ip address 198.51.100.1 255.255.255.255

<-- The router is the RP


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

 ip ospf 1 area 0
```

Verifica

Verificare il control plane multicast su FTD quando non è presente traffico multicast (mittenti o destinatari):

```
<#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
```

Verificare i vicini PIM:

```
<#root>

firepower#
show pim neighbor

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

L'RP annuncia l'intera gamma di gruppi multicast:

```
<#root>

firepower#
show pim group-map

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

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

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

La tabella di route del firewall contiene alcune voci non rilevanti (239.255.255.250 è il protocollo SSDP (Simple Service Discovery Protocol) utilizzato da fornitori come MAC OS e Microsoft Windows):

```
<#root>

firepower#
show mroute
```

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

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

Tra i firewall e l'RP è stato costruito un tunnel PIM:

<#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

Il tunnel PIM può essere visualizzato anche nella tabella di connessione del firewall:

<#root>

firepower#

show conn all detail address 198.51.100.1

```
...
PIM OUTSIDE: 198.51.100.1/0 NP Identity Ifc: 192.168.103.50/0,


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

Verifica sul firewall ASA:

<#root>

asa#

show pim neighbor

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

<#root>

```
asa#
```

show pim tunnel

```
Interface          RP Address        Source Address
```

Tunnel0 198.51.100.1 192.168.104.50

<-- PIM tunnel between the ASA and the RP

Verifica RP (Cisco router). Esistono alcuni gruppi multicast per SSDP e Auto-RP:

<#root>

```
Router1#
```

show ip pim rp

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

Verifica quando un destinatario annuncia la propria presenza

> **Nota**: i comandi del firewall mostrati in questa sezione sono totalmente applicabili alle appliance ASA e FTD.

L'ASA riceve il messaggio IGMP Membership Report e crea le voci IGMP e mroute (*, G):

<#root>

```
asa#
```

show igmp group 230.10.10.10

```
IGMP Connected Group Membership
Group Address    Interface            Uptime    Expires   Last Reporter
```

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

Il firewall ASA crea una route per il gruppo multicast:

<#root>

```
asa#
show mroute 230.10.10.10


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


(*, 230.10.10.10)
, 00:00:17/never,
RP 198.51.100.1
, flags: SCJ
<-- The mroute for group 230.10.10.10


Incoming interface: OUTSIDE


<-- Expected interface for a multicast packet from the source. If the packet is not received on this int
  RPF nbr: 192.168.104.61


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

Un'altra verifica del firewall è l'output della topologia PIM:

```
<#root>
asa#
show pim topology 230.10.10.10
...
(*,230.10.10.10) SM Up: 00:07:15 RP: 198.51.100.1                     <-- An entry for multicast group 23
JP: Join(00:00:33) RPF: OUTSIDE,192.168.104.61 Flags: LH
  INSIDE             00:03:15  fwd LI LH
```

> **Nota**: se il firewall non dispone di un percorso verso l'RP, l'output **del pim di debug** mostra un errore di ricerca RPF

Errore di ricerca RPF nell'output **pim di debug**:

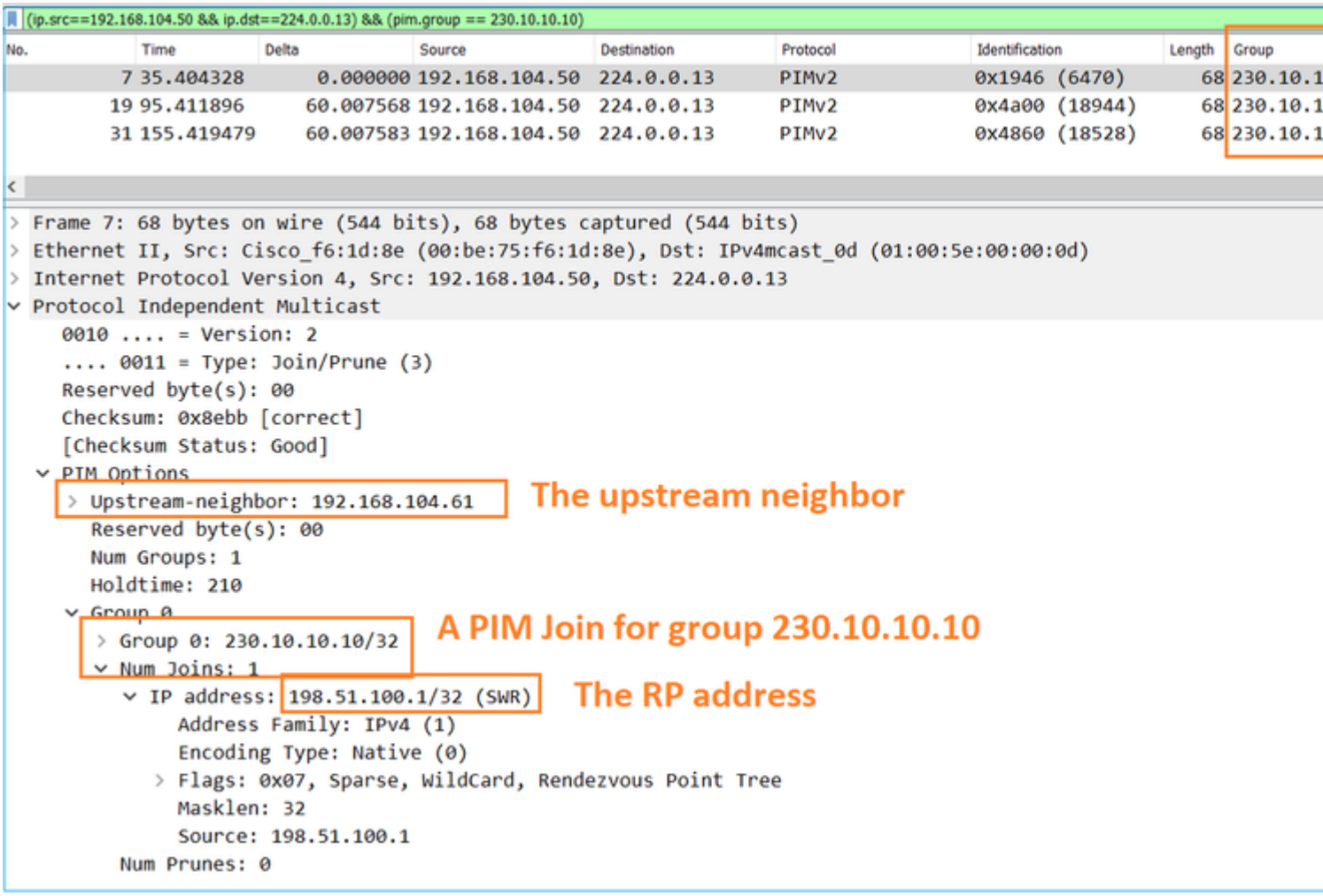
```
<#root>
```

```
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
```

Se tutto funziona correttamente, il firewall invia un messaggio PIM Join-Prune all'RP:

```
<#root>
asa#
debug pim group 230.10.10.10


IPv4 PIM group debugging is on
for group 230.10.10.10

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

L'acquisizione mostra che i messaggi di aggiunta PIM vengono inviati ogni 1 minuto e i messaggi di aggiunta PIM ogni 30 secondi. PIM utilizza il protocollo IP 224.0.0.13:



Suggerimento: filtro di visualizzazione Wireshark: (ip.src==192.168.104.50 && ip.dst==224.0.0.13) && (pim.group == 230.10.10.10)
- 192.168.104.50 è l'indirizzo IP del firewall dell'interfaccia di uscita (verso il vicino PIM a monte)
- 224.0.0.13 è il gruppo multicast PIM a cui vengono inviati i giunti PIM e le prugne
- 230.10.10.10 è il gruppo multicast a cui inviamo l'aggiunta/eliminazione PIM

L'RP crea una route (*, G). Poiché non sono ancora presenti server, l'interfaccia in ingresso è 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

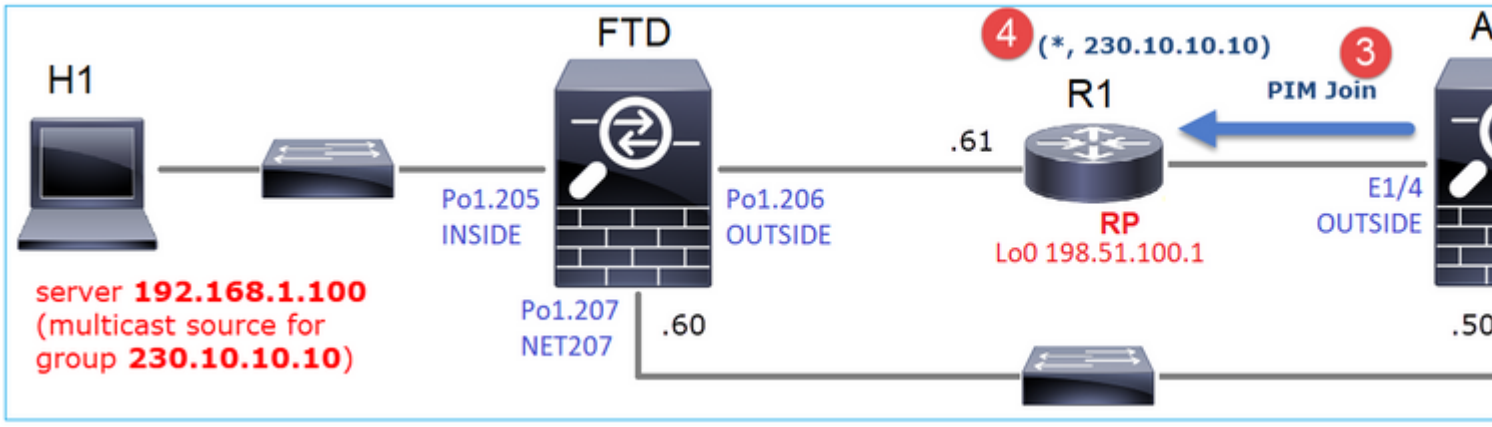
Incoming interface: Null

, 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
```

Ciò può essere visualizzato come:



1. Il report IGMP viene ricevuto sull'appliance ASA.
2. Viene aggiunto il percorso A (*, G).
3. L'ASA invia un messaggio di unione PIM all'RP (198.51.100.1).
4. L'RP riceve il messaggio Join e aggiunge un mroute (*, G).

Allo stesso tempo, sull'FTD non ci sono route poiché non è stato ricevuto alcun report IGMP né alcun join PIM:

```
<#root>

firepower#

show mroute 230.10.10.10

No mroute entries found.
```

Verifica quando il server invia un flusso multicast

L'FTD ottiene il flusso multicast da H1 e avvia il **processo di registrazione PIM** con l'RP. L'FTD invia un messaggio **unicast PIM Register** all'RP. L'RP invia un messaggio **PIM Join** al router First-Hop-Router (FHR), che in questo caso è l'FTD, per unirsi alla struttura multicast. Quindi invia un messaggio **Register-Stop**.

```
<#root>

firepower#

debug pim group 230.10.10.10

IPv4 PIM group debugging is on
```

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

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

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

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

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

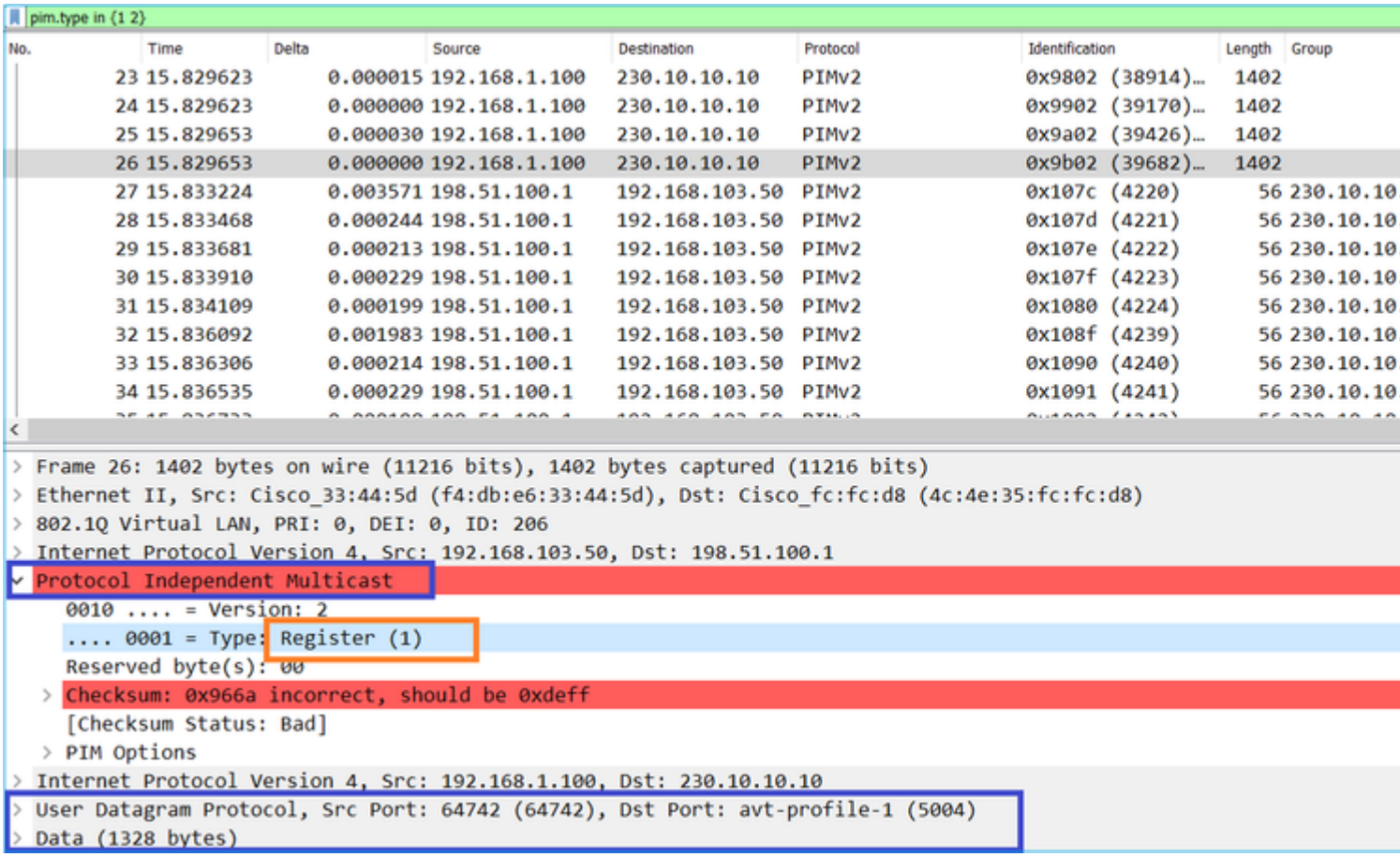
```
IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 J/P state changed from Null to Join
IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 FWD state change from Prune to Forward
IPv4 PIM: (192.168.1.100,230.10.10.10) Updating J/P status from Null to Join
IPv4 PIM: (192.168.1.100,230.10.10.10) J/P scheduled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

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

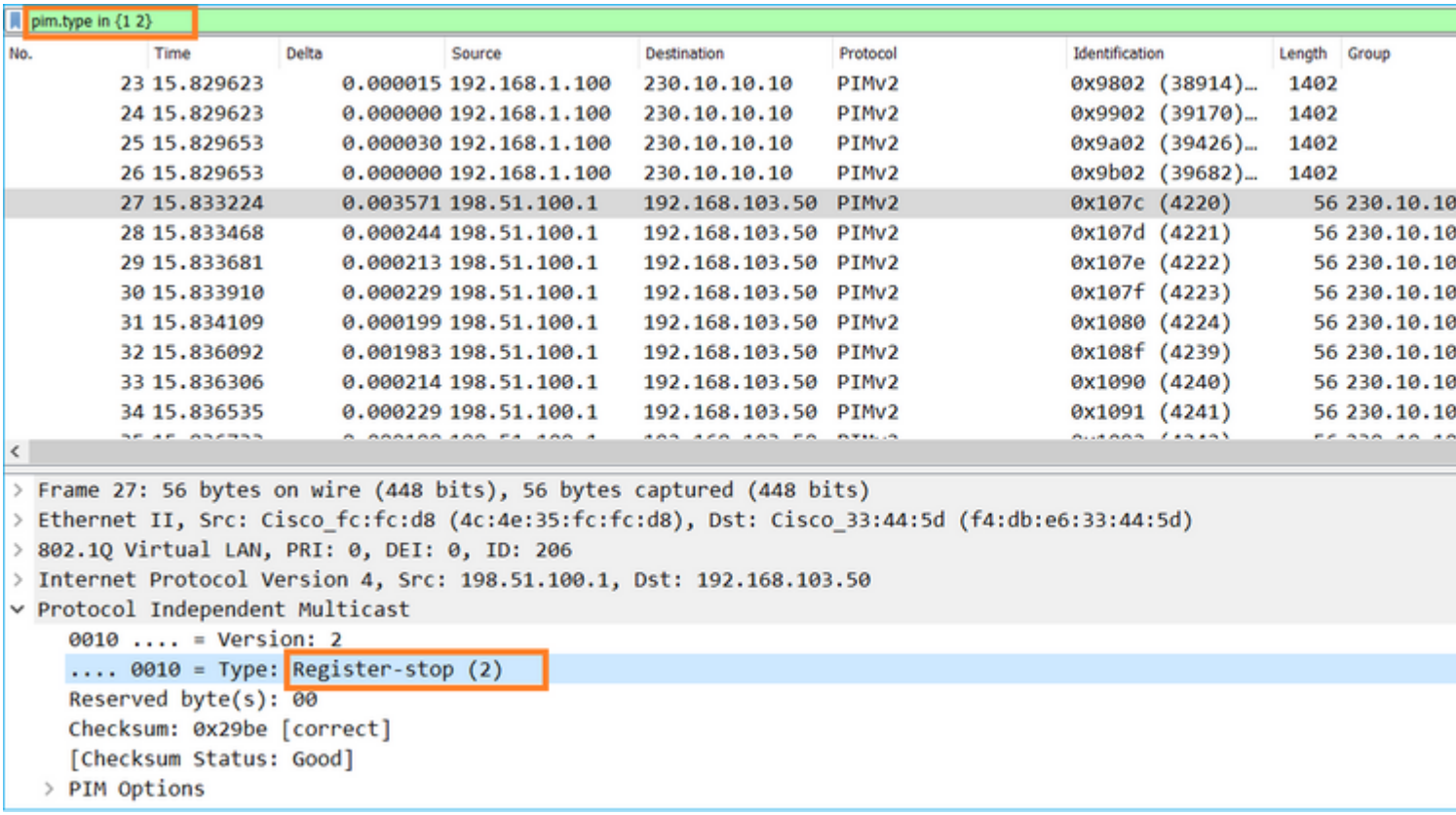
```
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE J/P state changed from Null to Join
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE FWD state change from Prune to Forward
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify F NS
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE Raise J/P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

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

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


IPv4 PIM: (192.168.1.100,230.10.10.10) Stop registering


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

Il messaggio PIM Register è un messaggio PIM che trasporta i dati UDP insieme alle informazioni del registro PIM:



Viene visualizzato il messaggio PIM Register-Stop:



Suggerimento: per visualizzare solo i messaggi PIM Register e PIM Register-Stop su Wireshark, è possibile utilizzare il filtro di visualizzazione pim.type in {1}

Il firewall (router dell'ultimo hop) ottiene il flusso multicast sull'interfaccia OUTSIDE e avvia il switchover Shortest Path Tree (SPT) sull'interfaccia NET207:

<#root>

asa#

debug pim group 230.10.10.10

IPv4 PIM group debugging is on
for group 230.10.10.10

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

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

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

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

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

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

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

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

Set SPT bit <-- The SPT bit is set

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

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

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


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


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

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


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


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

Il debug PIM sull'FTD quando si verifica il passaggio:

<#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
```

Il percorso FTD una volta avviato il cambio SPT:

<#root>

```
firepower#
```

show mroute 230.10.10.10

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

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

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

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

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

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

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

Alla fine del passaggio a SPT, solo l'interfaccia NET207 è mostrata in OIL di FTD:

<#root>

```
firepower#
```

show mroute 230.10.10.10

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

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

NET207, Forward

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

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

Anche sul router dell'ultimo hop (ASA), il bit SPT è impostato:

<#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

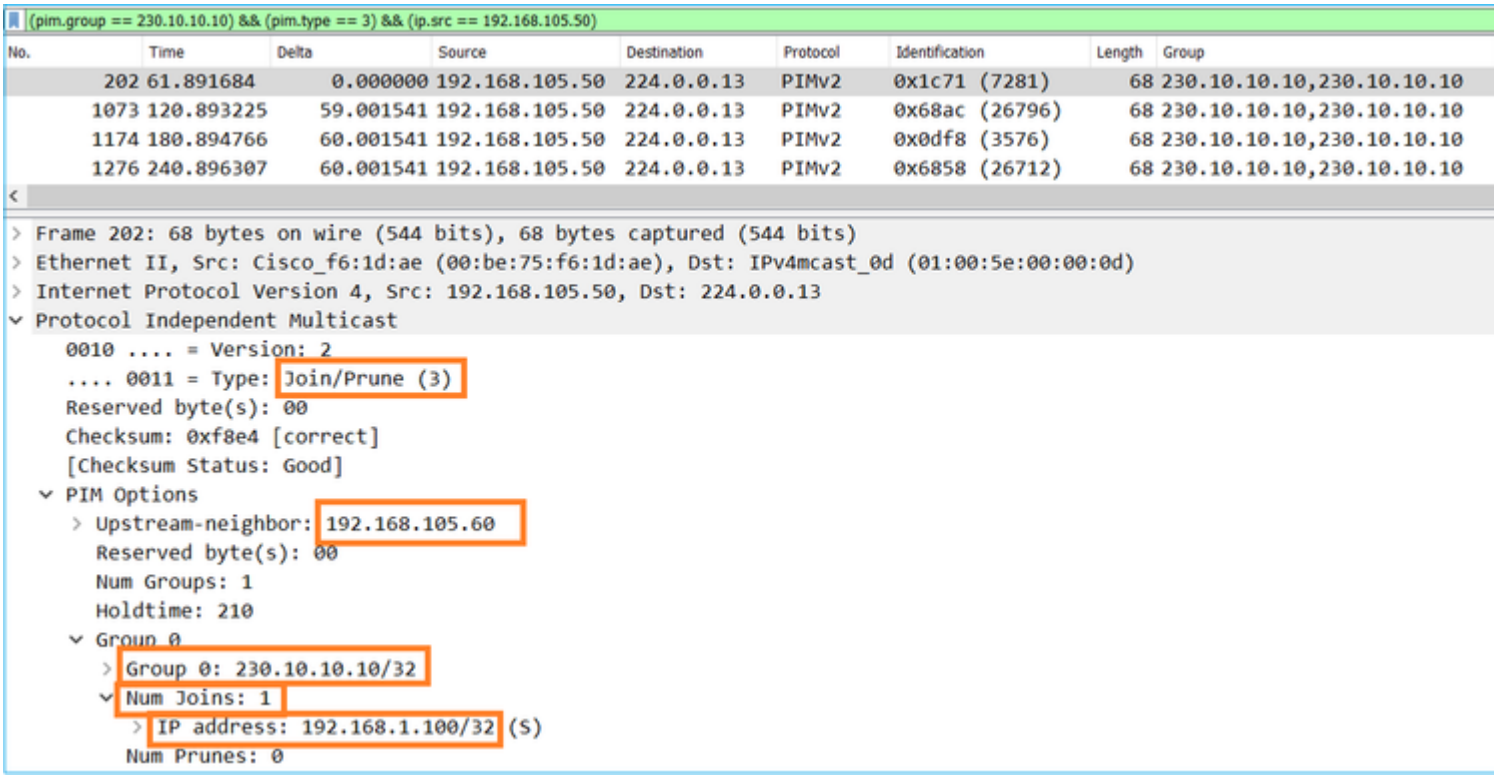
T   <-- SPT switchover for group 230.10.10.10

Incoming interface:

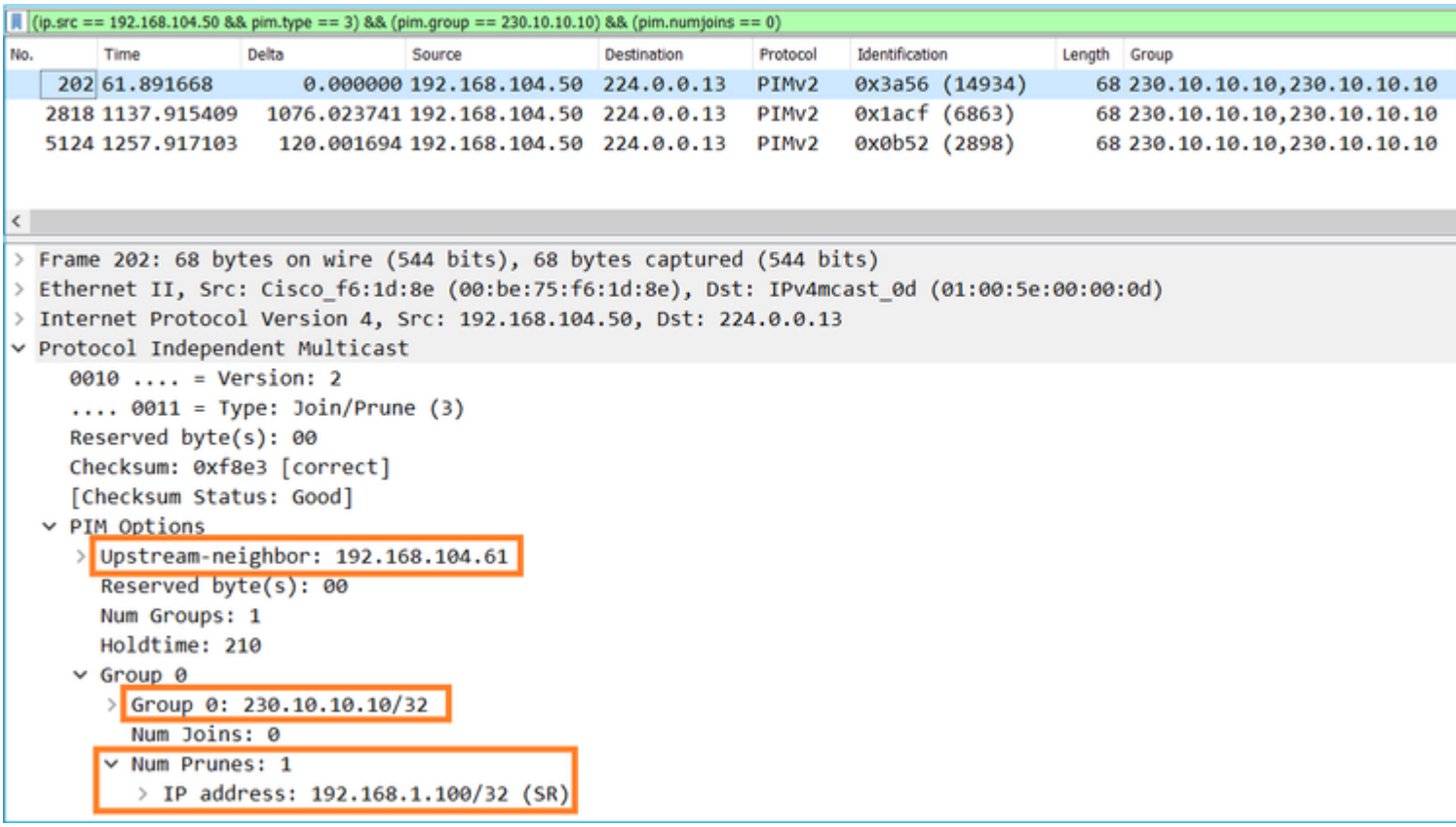
NET207   <-- The multicast packets arrive on interface NET207

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

Lo switchover dall'interfaccia ASA NET207 (il router del primo hop che ha eseguito lo switchover). Viene inviato un messaggio di unione PIM al dispositivo upstream (FTD):



Sull'interfaccia OUTSIDE viene inviato un messaggio PIM Prune all'RP per interrompere il flusso multicast:



Verifica del traffico PIM:

<#root>

```
firepower#
```

show pim traffic

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

                           Received     Sent
Valid PIM Packets          53934        63983
Hello                      36905        77023
Join-Prune                 6495         494          <-- PIM Join/Prune messages
Register                   0            2052         <-- PIM Register messages
Register Stop              1501         0            <-- PIM Register Stop messages
Assert                     289          362
Bidir DF Election          0            0

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

Per verificare il numero di pacchetti gestiti in Percorso lento rispetto a Percorso rapido rispetto a Control Point:

<#root>

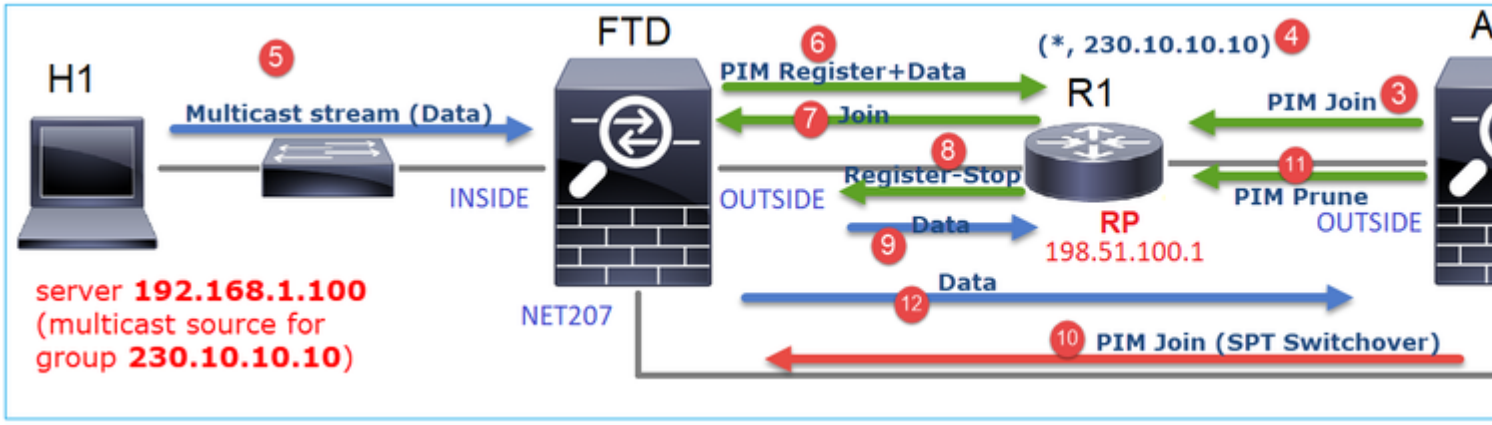
firepower#

show asp cluster counter

```
Global dp-counters:

Context specific dp-counters:
MCAST_FP_FROM_PUNT                    2712    Number of multicast packets punted from CP to FP
MCAST_FP_FORWARDED                    94901   Number of multicast packets forwarded in FP
MCAST_FP_TO_SP                        1105138 Number of multicast packets punted from FP to SP
MCAST_SP_TOTAL                        1107850 Number of total multicast packets processed in SP
MCAST_SP_FROM_PUNT                    2712    Number of multicast packets punted from CP to SP
MCAST_SP_FROM_PUNT_FORWARD            2712    Number of multicast packets coming from CP that are forw
MCAST_SP_PKTS                         537562  Number of multicast packets that require slow-path atter
MCAST_SP_PKTS_TO_FP_FWD               109     Number of multicast packets that skip over punt rule and
MCAST_SP_PKTS_TO_CP                   166981  Number of multicast packets punted to CP from SP
MCAST_FP_CHK_FAIL_NO_HANDLE           567576  Number of multicast packets failed with no flow mcast_ha
MCAST_FP_CHK_FAIL_NO_ACCEPT_IFC       223847  Number of multicast packets failed with no accept interf
MCAST_FP_CHK_FAIL_NO_SEQ_NO_MATCH     131     Number of multicast packets failed with no matched seque
```

```
MCAST_FP_CHK_FAIL_NO_FP_FWD             313584  Number of multicast packets that cannot be fast-path for
MCAST_FP_UPD_FOR_UNMATCH_IFC            91      Number of times that multicast flow's ifc_out  cannot be
```

Diagramma che illustra in modo dettagliato l'operazione eseguita:



1. L'host finale (H2) invia un report IGMP per unirsi al flusso multicast 230.10.10.10.
2. Il router dell'ultimo hop (ASA), ossia il DR PIM, crea una voce (*, 230.10.10.10).
3. L'ASA invia un messaggio di unione PIM all'RP per il gruppo 230.10.10.10.
4. L'RP crea la voce (*, 230.10.10.10).
5. Il server invia i dati del flusso multicast.
6. L'FTD incapsula i pacchetti multicast nei messaggi PIM Register e li invia (unicast) all'RP. A questo punto, l'RP si accorge di avere un destinatario attivo, decapsula i pacchetti multicast e li invia al destinatario.
7. L'RP invia un messaggio di unione PIM all'FTD per unirsi all'albero multicast.
8. L'RP invia un messaggio PIM Register-Stop all'FTD.
9. L'FTD invia un flusso multicast nativo (senza incapsulamento PIM) all'RP.
10. Il router dell'ultimo hop (ASA) rileva che l'origine (192.168.1.100) ha un percorso migliore dall'interfaccia NET207 e avvia la commutazione. Invia un messaggio di unione PIM al dispositivo upstream (FTD).
11. Il router dell'ultimo hop invia un messaggio PIM Prune all'RP.
12. L'FTD inoltra il flusso multicast verso l'interfaccia NET207. L'ASA si sposta dalla struttura ad albero condivisa (struttura ad albero RP) alla struttura ad albero origine (SPT).

Attività 2 - Configurazione del router di bootstrap PIM (BSR)

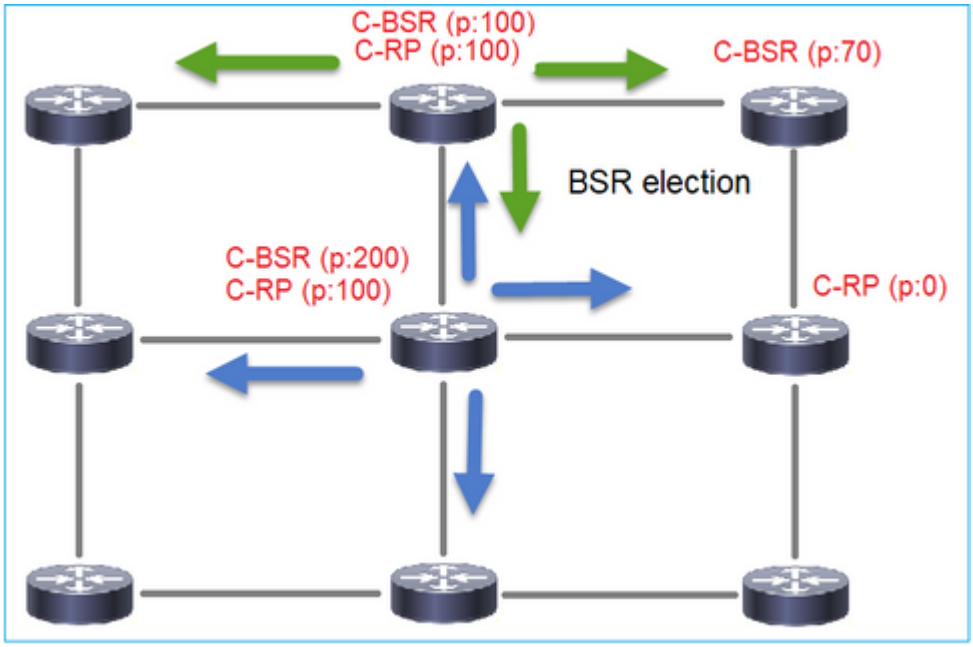
Nozioni di base sulla tecnologia BSR

- BSR (RFC 5059) è un meccanismo multicast basato su un piano di controllo che utilizza il protocollo PIM e consente ai dispositivi di imparare dinamicamente le informazioni RP.
- Definizioni BSR:
  - RP candidato (C-RP): un dispositivo che desidera essere un RP.
  - BSR candidato (C-BSR): un dispositivo che desidera essere un BSR e pubblicizza gli RP-set ad altri dispositivi.
  - BSR: dispositivo selezionato come BSR tra molti C-BSR. La **priorità più alta del BSR vince** le elezioni.
  - RP-set: un elenco di tutti i C-RP e delle loro priorità.
  - RP: il dispositivo con la **priorità RP più bassa vince** la scelta.
  - Messaggio PIM BSR (vuoto): messaggio PIM utilizzato nella selezione BSR.
  - Messaggio PIM BSR (normale): un messaggio PIM inviato a 24.0.0.13 IP e contenente un set RP e informazioni BSR.

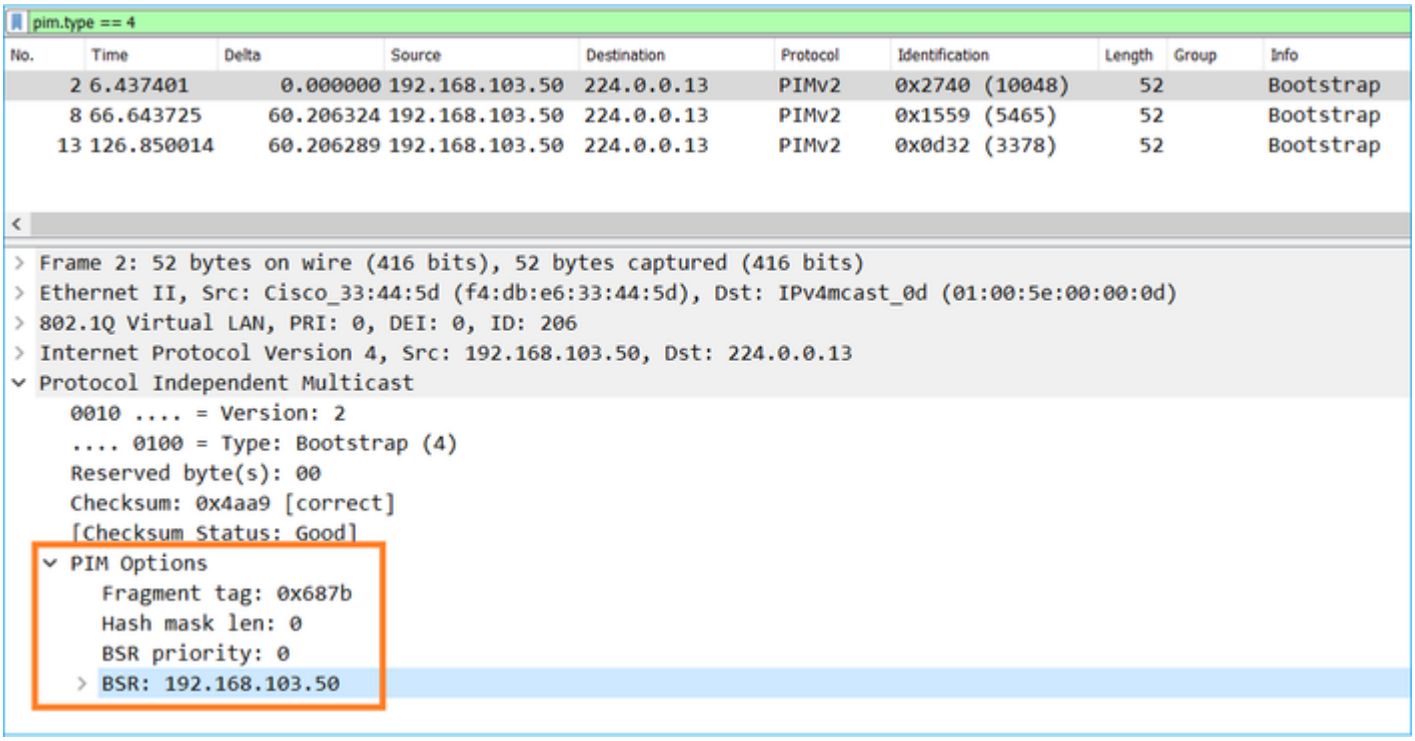
Funzionamento di BSR

1. Meccanismo di selezione della BSR.

Ogni C-BSR invia messaggi PIM BSR vuoti che contengono una priorità. Il dispositivo con la priorità più alta (il fallback è l'IP più alto) vince la scelta e diventa il BSR. Gli altri dispositivi non inviano più messaggi BSR vuoti.

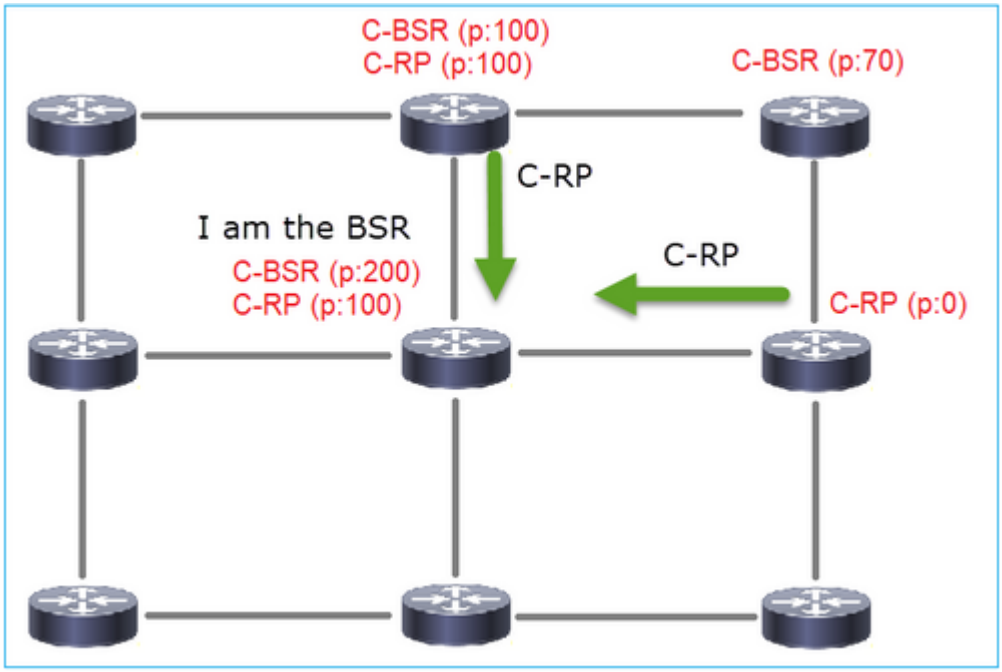


Un messaggio BSR utilizzato nel processo di elezione contiene solo informazioni sulla priorità C-BSR:

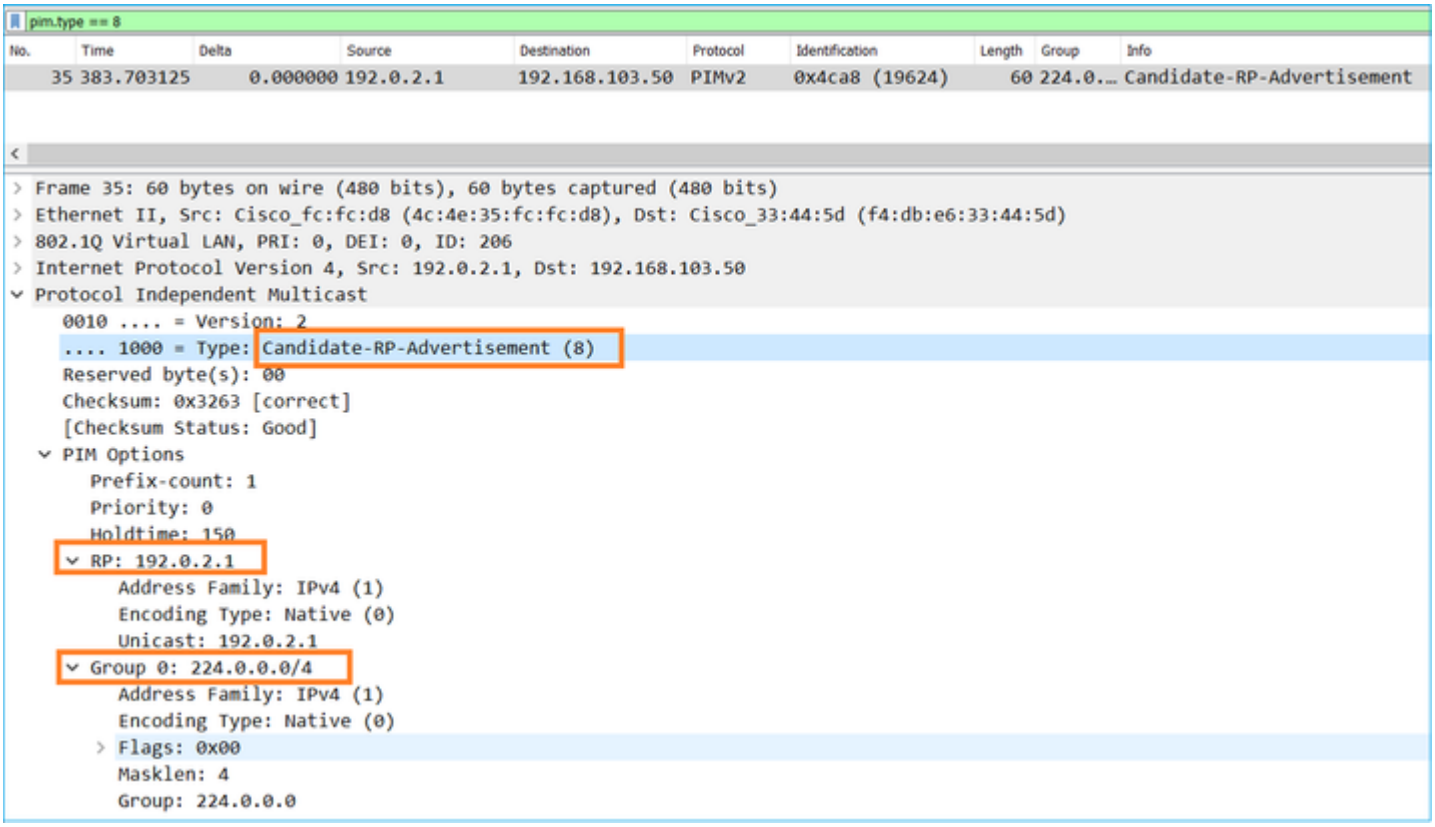


Per visualizzare i messaggi BSR in Wireshark, utilizzare il seguente filtro di visualizzazione: pim.type == 4

2. I C-RP inviano messaggi BSR **unicast** al BSR che contengono la loro priorità C-RP:

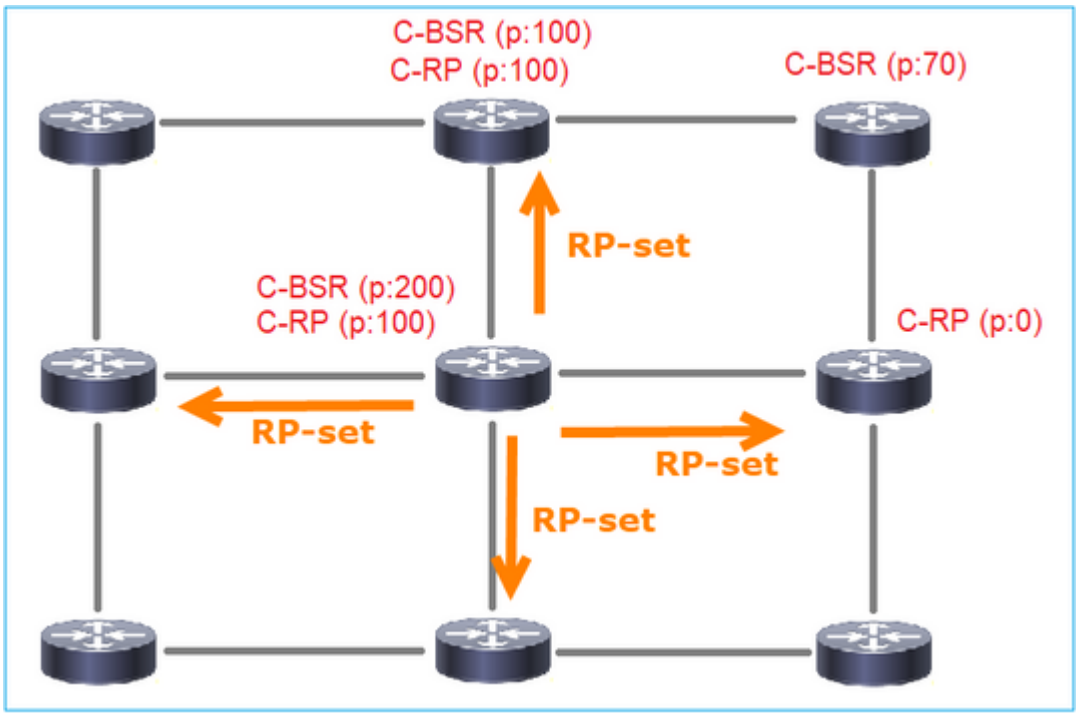


Un messaggio RP candidato:



Per visualizzare i messaggi BSR in Wireshark, utilizzare il seguente filtro di visualizzazione: pim.type == 8

3. Il BSR compone l'RP-set e lo pubblicizza a tutti i vicini PIM:

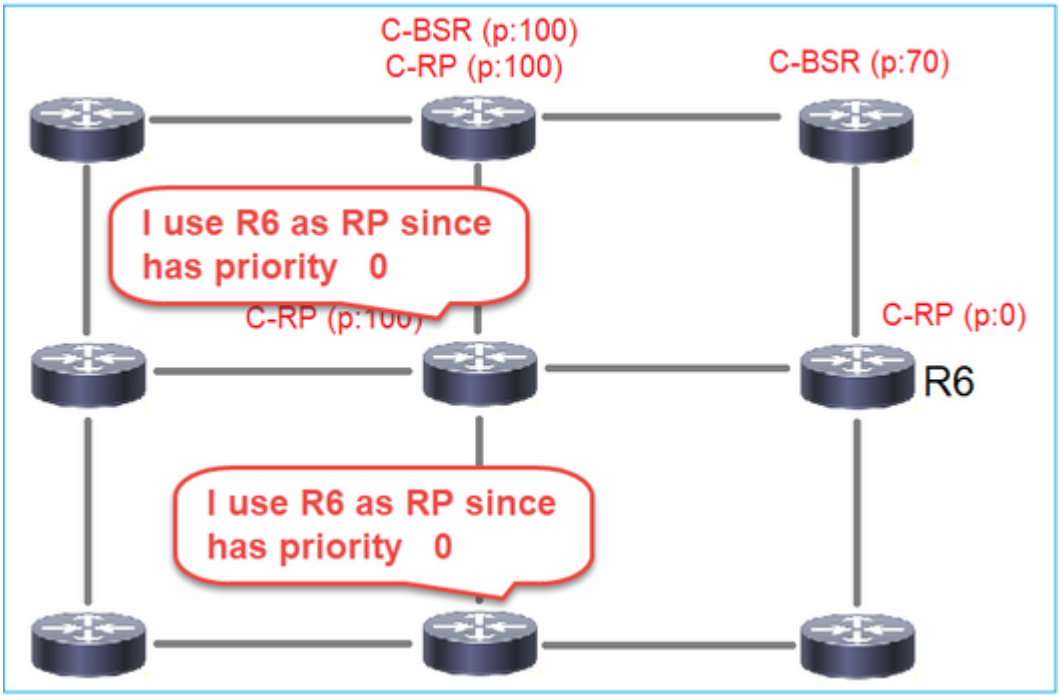


(ip.src == 192.168.105.60) && (pim.type == 4)

No.	Time	Delta	Source	Destination	Protocol	Identification	Length	Group	Info
152	747.108256	1.001297	192.168.105.60	224.0.0.13	PIMv2	0x0bec (3052)	84	224.0.0.0,224.0.0.0	Boo

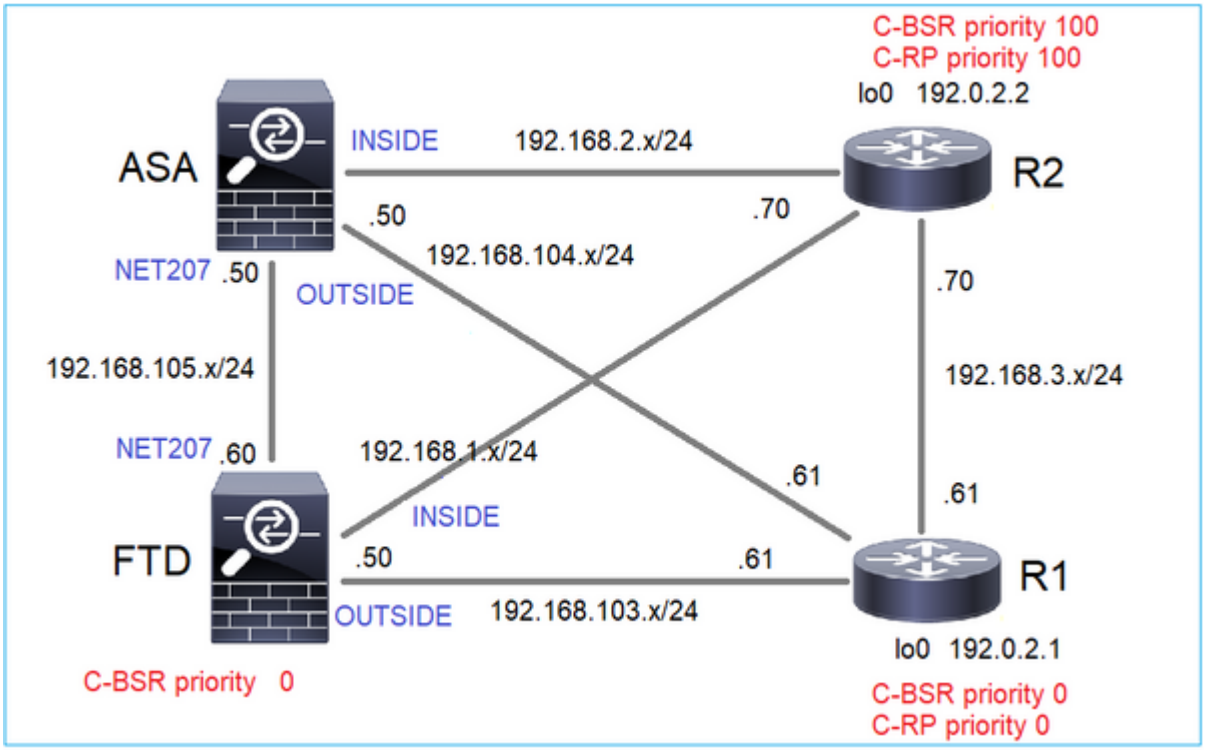
```
> Frame 152: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
> Ethernet II, Src: Cisco_33:44:5d (f4:db:e6:33:44:5d), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
> 802.1Q Virtual LAN, PRI: 6, DEI: 0, ID: 207
> Internet Protocol Version 4, Src: 192.168.105.60, Dst: 224.0.0.13
v Protocol Independent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

4. I router/firewall ottengono l'RP-set e selezionano l'RP in base alla priorità più bassa:



Attività richiesta

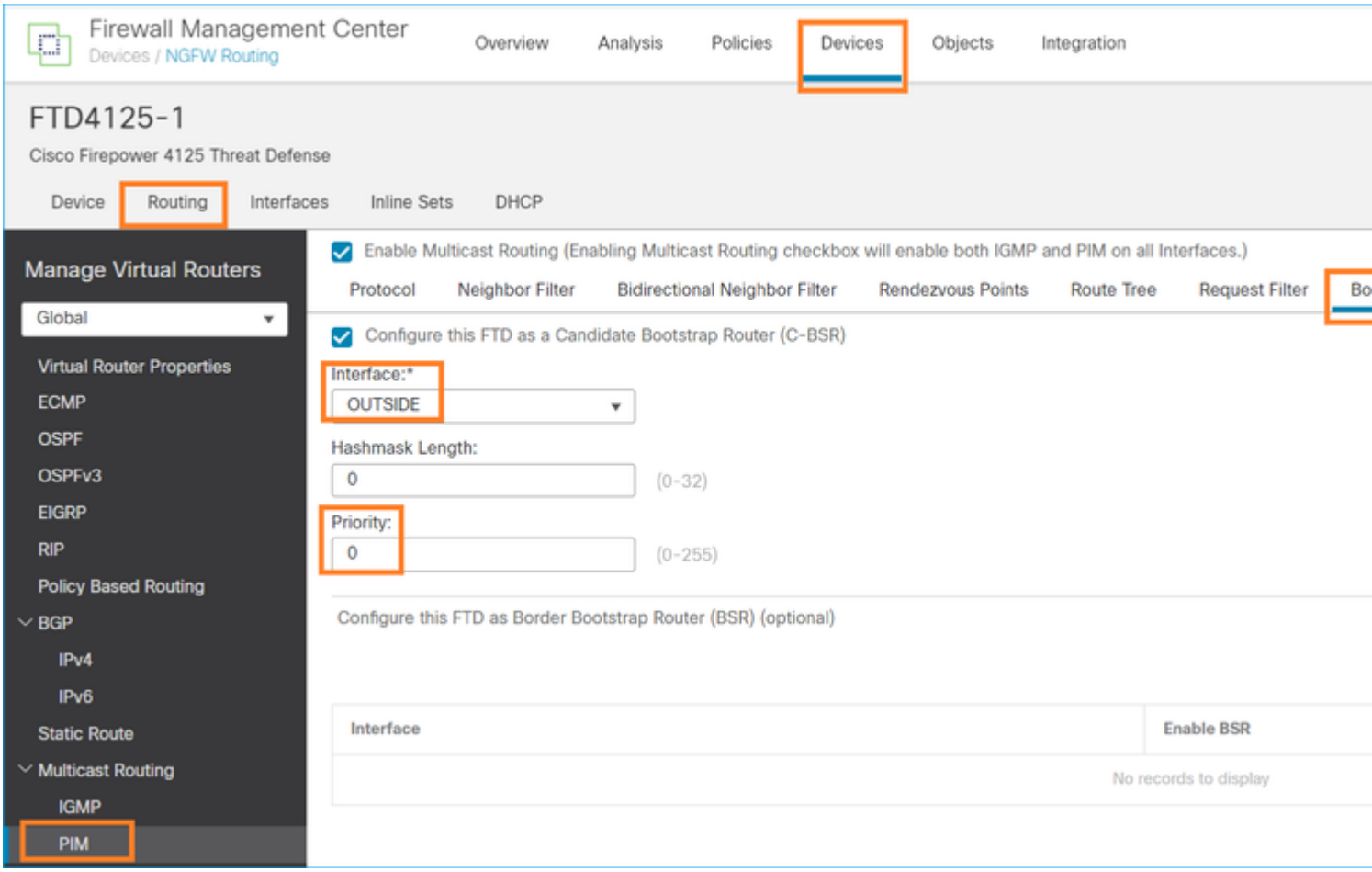
Configurare i C-BSR e i C-RP in base alla seguente topologia:



per questa operazione, l'FTD deve annunciarsi come C-BSR sull'interfaccia ESTERNA con priorità BSR 0.

Soluzione

Configurazione FMC per FTD:



La configurazione distribuita:

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

Configurazione sugli altri dispositivi:

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)
```

Stesso per R2, ma con priorità C-BSR e C-RP diverse

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

Sull'appliance ASA il multicast è abilitato a livello globale. Ciò abilita PIM su tutte le interfacce:

```
multicast-routing
```

Verifica

R2 è il BSR scelto in base alla priorità più alta:

```
<#root>

firepower#

show pim bsr-router


PIMv2 BSR information

BSR Election Information


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

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

,

Hash mask length: 0
     RPF: 192.168.1.70,INSIDE

<-- The interface to the BSR

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

R1 è selezionato come RP a causa della priorità più bassa:

```
<#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
```

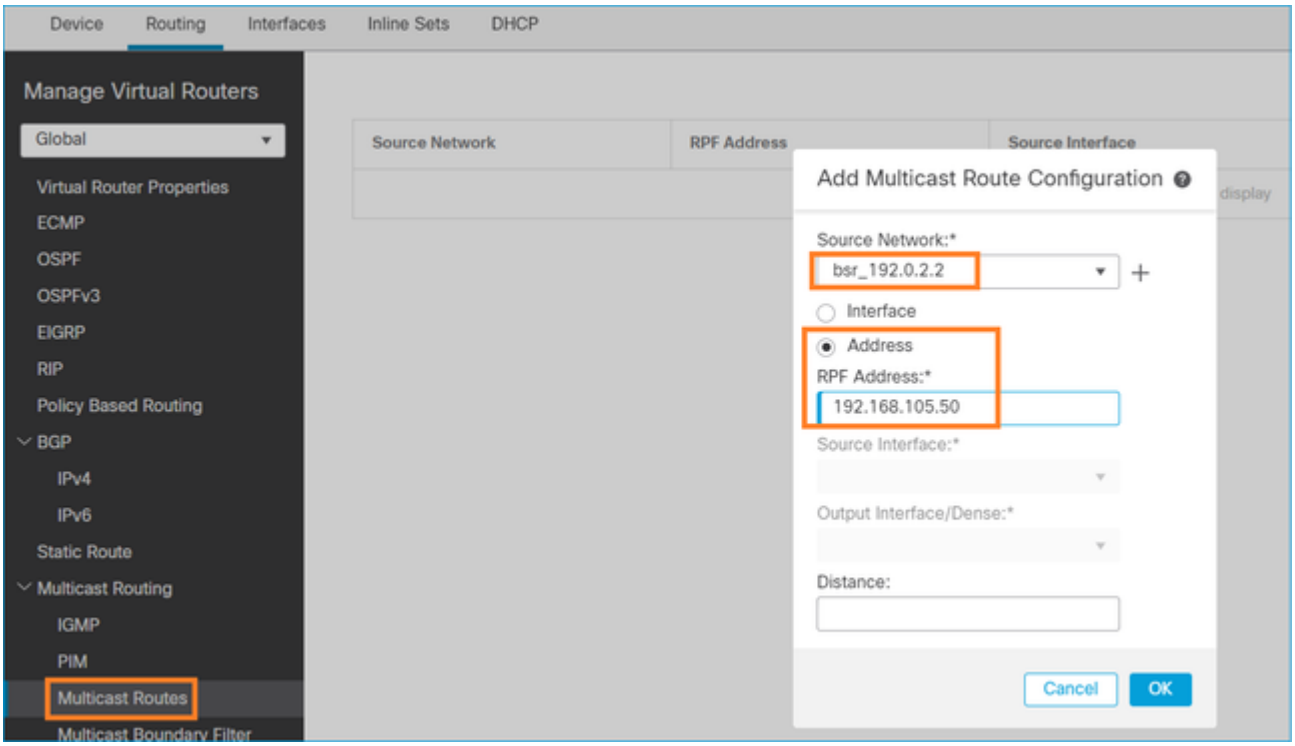
```
224.0.0.0/4

*

       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
```

I messaggi BSR **sono soggetti al controllo RPF**. Per verificare questa condizione, è possibile abilitare il comando **debug pim bsr**:

<#root>

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

BSR message

 from 192.168.105.50/

NET207

 for 192.0.2.2

RPF failed, dropped


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

Se si desidera modificare l'interfaccia RPF, è possibile configurare una route statica. Nell'esempio, il firewall accetta messaggi BSR da IP 192.168.105.50:



<#root>

firepower#

show run mroute

mroute 192.0.2.2 255.255.255.255 192.168.105.50

<#root>

firepower#

show pim bsr-router

PIMv2 BSR information

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

RPF: 192.168.105.50,NET207

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

Ora i messaggi BSR sull'interfaccia NET207 sono accettati, ma su INSIDE sono scartati:

<#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

Abilitare l'acquisizione con traccia sul firewall e controllare come vengono elaborati i messaggi BSR:

<#root>

firepower#

show capture

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

Le connessioni PIM sono terminate sul firewall, quindi per consentire la visualizzazione di informazioni utili sulla traccia è necessario deselezionare le connessioni alla casella:

<#root>

firepower#

show conn all | i PIM

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

firepower#

clear conn all addr 224.0.0.13

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

clear cap /all

<#root>

```
firepower#
```

show capture CAPI packet-number 2 trace

```
6 packets captured

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

192.168.1.70 > 224.0.0.13

```
 ip-proto-103, length 38
```

<-- Ingress PIM packet

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

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

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

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

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

Phase: 6
Type: NAT
```

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

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

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

Phase: 9

Type: MULTICAST <-- The multicast process

Subtype: pim

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

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

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

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

Action: allow

```
Time Taken: 76616 ns
```

Se il pacchetto PIM viene scartato a causa di un errore di RPF, la traccia mostra:

<#root>

```
firepower#
```

show capture NET207 packet-number 4 trace

```
85 packets captured

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

192.168.104.61 > 224.0.0.13 ip-proto-103

```
, length 38
```

<-- Ingress PIM packet

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

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

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

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

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

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

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

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

La tabella ASP scarta e acquisisce i pacchetti con errori RPF:

<#root>

firepower#

show asp drop

Frame drop:

Reverse-path verify failed (rpf-violated) 122

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

Per acquisire i pacchetti scartati a causa di un errore RPF:

<#root>

firepower#

capture ASP type asp-drop rpf-violated

<#root>

firepower#

show capture ASP | include 224.0.0.13

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

Metodologia di risoluzione dei problemi

La metodologia di risoluzione dei problemi per il firewall dipende principalmente dal ruolo del firewall nella topologia multicast. Di seguito sono elencati i passaggi consigliati per la risoluzione dei problemi:

1. Chiarire i dettagli della descrizione del problema e dei sintomi. Provare a restringere l'ambito ai problemi **del Control Plane (IGMP/PIM)** o del **Data Plane (flusso multicast)**.
2. Il prerequisito obbligatorio per la risoluzione dei problemi relativi al multicast sul firewall è quello di chiarire la topologia multicast. È necessario identificare almeno:
    - ruolo del firewall nella topologia multicast, ovvero FHR, LHR, RP o un altro ruolo intermedio.
    - interfacce multicast in entrata e in uscita previste sul firewall.
    - RP.
    - indirizzi IP origine mittente.
    - multicast raggruppa indirizzi IP e porte di destinazione.
    - ricevitori del flusso multicast.

3. Identificare il tipo di routing multicast - **Stub** o **PIM multicast routing:**

- **Stub multicast routing**: fornisce una registrazione host dinamica e facilita il routing multicast. Quando configurata per il routing multicast di stub, l'ASA agisce come agente proxy IGMP. Anziché partecipare completamente al routing multicast, l'ASA inoltra i messaggi IGMP a un router multicast upstream, che configura il recapito dei dati multicast. Per identificare il routing in modalità stub, usare il comando **show igmp interface** e controllare la configurazione di inoltro IGMP:

<#root>

```
firepower#
```

```
show igmp interface
```

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

```
IGMP forwarding on interface inside
```

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

PIM è abilitato sulle interfacce; tuttavia, il vicinato non è stabilito:

<#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.
```

L'inoltro PIM-SM/Bidir e IGMP **non** sono supportati contemporaneamente.

Non è possibile configurare opzioni quali l'indirizzo RP:

<#root>

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

- **PIM multicast routing** - **Il PIM multicast routing è la distribuzione più comune.** Il firewall supporta sia PIM-SM che PIM bidirezionale. PIM-SM è un protocollo di routing multicast che utilizza la base di informazioni di routing unicast sottostante o una base di informazioni di routing multicast separata. Crea una struttura ad albero condivisa unidirezionale basata su un singolo punto di rendering (RP, Rendezvous Point) per gruppo multicast e, facoltativamente, crea alberi con il percorso più breve per origine multicast. In questa modalità di distribuzione, a differenza della modalità stub, gli utenti in genere configurano la configurazione dell'indirizzo RP e il firewall stabilisce le adiacenze PIM con i peer:

<#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. Verificare che l'indirizzo IP RP sia configurato e raggiungibile:

<#root>

firepower#

show run pim

pim rp-address 10.10.10.1

firepower#

show pim group-map

```
Group Range         Proto   Client   Groups RP address      Info
224.0.1.39/32*      DM      static   0      0.0.0.0
224.0.1.40/32*      DM      static   0      0.0.0.0
224.0.0.0/24*       L-Local static   1      0.0.0.0
232.0.0.0/8*        SSM     config   0      0.0.0.0
224.0.0.0/4*        SM      config   1      10.10.10.1     RPF: inside,192.168.2.1 <--- RP is 10.10.10.1

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

<#root>

firepower#

show pim group-map

```
Group Range         Proto   Client   Groups RP address      Info
224.0.1.39/32*      DM      static   0      0.0.0.0
224.0.1.40/32*      DM      static   0      0.0.0.0
224.0.0.0/24*       L-Local static   1      0.0.0.0
232.0.0.0/8*        SSM     config   0      0.0.0.0
224.0.0.0/4*        SM      config   1      192.168.2.2     RPF: Tunnel0,192.168.2.2 (us) <--- â€œusâ€

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

Avviso: il firewall non può essere contemporaneamente un **RP** e un **FHR**.

---

5. Controllare gli output aggiuntivi a seconda del ruolo del firewall nella topologia multicast e dei sintomi del problema.

FHR

- Controllare lo stato dell'interfaccia **Tunnel0**. Questa interfaccia viene utilizzata per incapsulare il traffico multicast raw all'interno del payload PIM e inviare il pacchetto unicast all'RP per con bit del registro PIM impostato:

<#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
```

- Verifica route:

<#root>

```
firepower#
```

`show mroute`

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

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

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

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

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

Quando il firewall riceve il pacchetto PIM con bit Register-Stop, il tunnel 0 viene rimosso da OIL. Il firewall interrompe quindi l'incapsulamento e invia il traffico multicast raw tramite l'interfaccia in uscita:

```
<#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
```

- Controllare i contatori del registro PIM:

```
<#root>

firepower#

show pim traffic



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

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

Register                    0            8  <--- Sent to the RP



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


Assert                      0            0
Bidir DF Election           0            0

Errors:
Malformed Packets                         0
Bad Checksums                             0
Send Errors                               0
Packet Sent on Loopback Errors            0
```

```
Packets Received on PIM-disabled Interface  0
Packets Received with Unknown PIM Version   0
Packets Received with Incorrect Addressing  0
```

- Controllare le acquisizioni di pacchetti PIM unicast tra il firewall e l'RP:

<#root>

```
firepower#
```

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

```
firepower#
```

show capture capi

```
4 packets captured
```

```
  1: 09:53:28.097559       192.168.3.1 > 10.10.10.1  ip-proto-103, length 50     <--- Unicast to RP
  2: 09:53:32.089167       192.168.3.1 > 10.10.10.1  ip-proto-103, length 50
  3: 09:53:37.092890       192.168.3.1 > 10.10.10.1  ip-proto-103, length 50
  4: 09:53:37.095850       10.10.10.1 > 192.168.3.1  ip-proto-103, length 18     <--- Unicast from RP
```

- Raccogli output aggiuntivi (x.x.x.x è il gruppo multicast, y.y.y è l'indirizzo IP RP). Si consiglia di raccogliere gli output **poche volte**:

<#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
```

- Raccogli pacchetti di interfaccia multicast non elaborati e acquisizioni drop ASP.

<#root>

```
capture capi interface
```

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

```
capture capo interface
```

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

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

- Messaggi syslog: gli ID comuni sono 302015, 302016 e 710005.

RP

- Controllare lo stato dell'interfaccia Tunnel0. Questa interfaccia viene utilizzata per incapsulare il traffico multicast raw all'interno del payload PIM e inviare il pacchetto unicast a FHR per con bit di stop PIM impostato:

<#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        -
```

- Verifica route:

<#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

- Controllare i contatori PIM:

<#root>

firepower #

show pim traffic

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

	Received	Sent
Valid PIM Packets	**948**	**755**
Hello	**467**	**584**
Join-Prune	**125**	**32**
Register	**344**	**16**
Register Stop	**12**	**129**
Assert	0	0
Bidir DF Election	0	0

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

- Raccogli output aggiuntivi (x.x.x.x è il gruppo multicast, y.y.y è l'indirizzo IP RP). Si consiglia di raccogliere gli output **poche volte**:

<#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

- Raccogli pacchetti di interfaccia multicast non elaborati e acquisizioni di rilascio ASP:

<#root>

capture capi interface

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

capture capo interface

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

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

- Syslog: gli ID comuni sono 302015, 302016 e 710005.

LHR

Prendere in considerazione i passi descritti nella sezione per l'RP e i seguenti controlli aggiuntivi:

- Route:

<#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

- Gruppi IGMP:

<#root>

firepower#

show igmp groups detail <--- The list of IGMP groups

Interface: outside

Group: 230.1.1.1

Uptime: 00:21:42
Router mode: EXCLUDE (Expires: 00:03:17)
Host mode: INCLUDE

Last reporter: 192.168.3.100 <--- Host joined group 230.1.1.1

Source list is empty
Interface: outside

Group: 230.1.1.2

Uptime: 00:00:02
Router mode: EXCLUDE (Expires: 00:04:17)
Host mode: INCLUDE

Last reporter: 192.168.3.101 <--- Host joined group 230.1.1.2

Source list is empty

- Statistiche traffico IGMP:

<#root>

firepower#

show igmp traffic

IGMP Traffic Counters
Elapsed time since counters cleared: 1d04h

	Received	Sent
Valid IGMP Packets	2468	856
Queries	2448	856
Reports	20	0
Leaves	0	0

```
Mtrace packets                0            0
DVMRP packets                 0            0
PIM packets                   0            0

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

Comandi per la risoluzione dei problemi PIM (scheda Cheat)

Comando	**Descrizione**
show running-config multicast-routing	Per verificare se il routing multicast è abilitato sul firewall
mostra route	Per visualizzare le route statiche configurate sul firewall
show running-config pim	Per visualizzare la configurazione PIM sul firewall
mostra interfaccia pim	Per verificare quali interfacce firewall hanno attivato PIM e i router adiacenti PIM.
mostra router adiacente pim	Per vedere i vicini PIM
show pim group-map	Per visualizzare i gruppi multicast mappati all'RP
mostra route	Per visualizzare la tabella di routing multicast completa
show route 230.10.10.10	Per visualizzare la tabella multicast per un gruppo multicast specifico
mostra tunnel pim	Per verificare se tra il firewall e l'RP è stato creato un tunnel PIM
show conn all detail address RP_IP_ADDRESS	Per verificare se è stata stabilita una connessione (tunnel PIM) tra il firewall e l'RP
mostra topologia pim	Per visualizzare l'output della topologia PIM del firewall

pim di debug	Questo debug visualizza tutti i messaggi PIM da e verso il firewall
debug pim group 230.10.10.10	Questo debug visualizza tutti i messaggi PIM da e verso il firewall per il gruppo multicast specifico
mostra traffico pim	Per visualizzare le statistiche sui messaggi PIM ricevuti e inviati
mostra contatore cluster asp	Per verificare il numero di pacchetti gestiti in Percorso lento rispetto a Percorso rapido rispetto a Control Point
show asp drop	Per visualizzare tutte le perdite a livello di software sul firewall
acquisizione interfaccia CAP INSIDE traccia corrispondenza pim any	Per acquisire e tracciare i pacchetti multicast PIM in entrata sul firewall
capture CAP interface INSIDE trace match udp host 24.1.2.3 any	Per acquisire e tracciare il flusso multicast in entrata
show pim bsr-router	Per verificare chi è il router BSR scelto
show conn all address 24.1.2.3	Per visualizzare la connessione multicast padre
show local-host 24.1.2.3	Per visualizzare le connessioni multicast figlio/stub

Per ulteriori informazioni sulle acquisizioni del firewall, controllare: Uso di Firepower Threat Defense Capture e Packet Tracer

Problemi noti

Limitazioni di Firepower multicast:

- IPv6 non supportato.
- Il multicast PIM/IGMP non è supportato sulle interfacce in una zona di traffico (EMCP).
- Il firewall non può essere contemporaneamente RP e FHR.
- Il comando **show conn all** mostra solo le connessioni multicast di identità. Per visualizzare la connessione multicast stub/secondaria, usare il comando **show local-host <*group IP*>**.

PIM non supportato su un Nexus vPC

Se si tenta di distribuire un'adiacenza PIM tra un Nexus vPC e il firewall, è presente una limitazione Nexus come descritto di seguito:

Topologie supportate per il routing su vPC (Virtual Port Channel) sulle piattaforme Nexus

Dal punto di vista di NGFW, è possibile vedere in capture with trace this drop:

<#root>

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

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

Il firewall non è in grado di completare la registrazione dell'RP:

<#root>

```
firepower#
```

show mroute 224.1.2.3

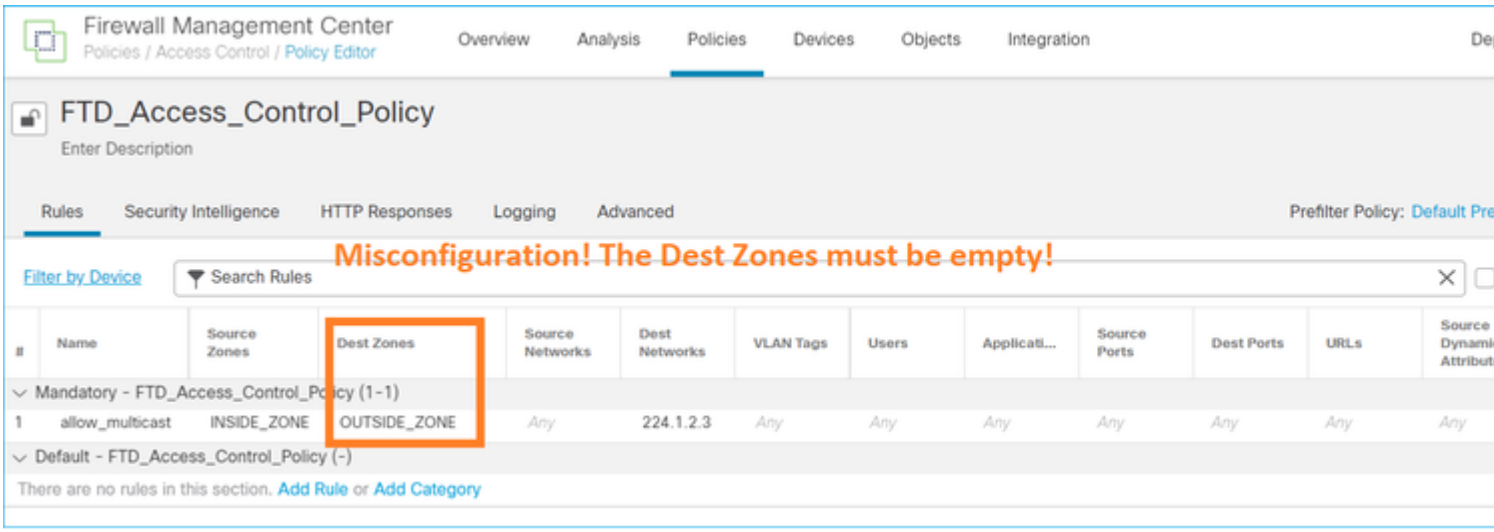
```
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface,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

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

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

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

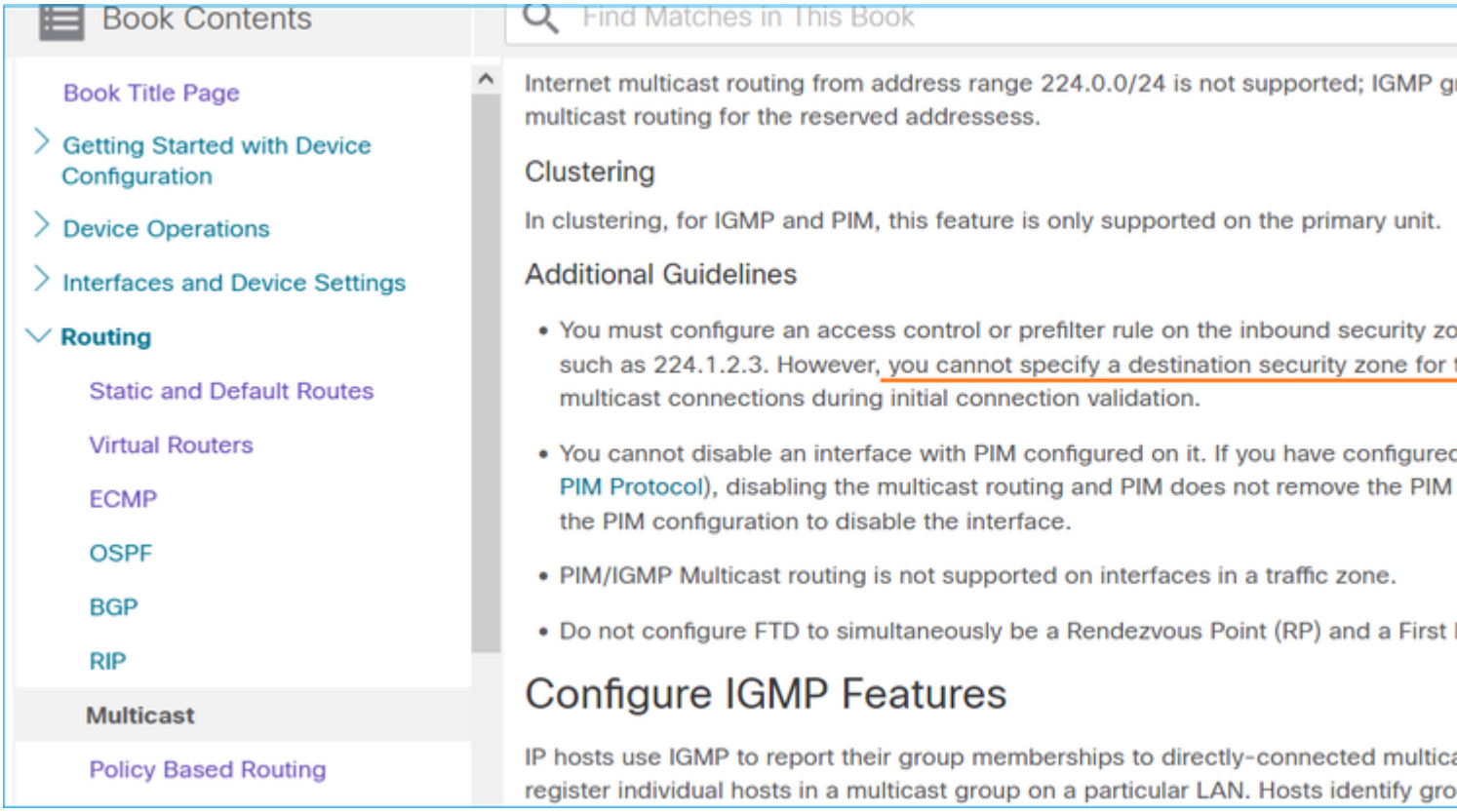
```
  Immediate Outgoing interface list:
    Tunnel0, Forward, 00:39:15/never
```

Zone di destinazione non supportate

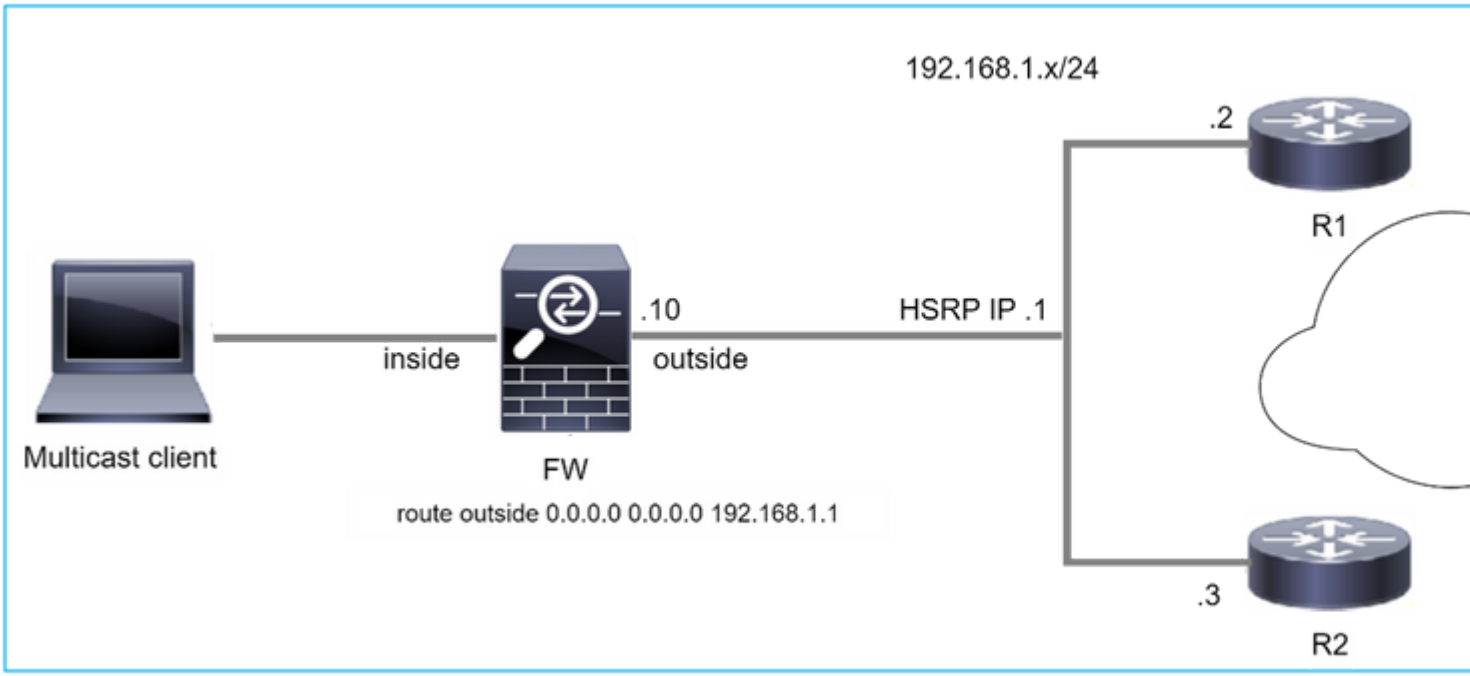
Non è possibile specificare un'area di sicurezza di destinazione per la regola dei criteri di controllo di accesso corrispondente al traffico multicast:



Questo è documentato anche nel manuale per l'utente del CCP:



Il firewall non supporta messaggi PIM verso router upstream a causa di HSRP



In questo caso, il firewall dispone di un percorso predefinito tramite il protocollo HSRP (Hot Standby Redundancy Protocol) IP 192.168.1.1 e la connessione PIM con i router R1 e R2:

<#root>

```
firepower#
```

`show run route`

```
route outside 0.0.0.0 0.0.0.0 192.168.1.1 1
```

Il firewall dispone di un'adiacenza PIM tra l'esterno e l'interfaccia fisica IP su R1 e R2:

<#root>

```
firepower#
```

`show pim neighbor`

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

Il firewall non invia il messaggio di aggiunta PIM alla rete upstream. Il comando PIM debug **pim** visualizza questo output:

<#root>

```
firepower#
```

`debug pim`

```
...

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

La RFC 2362 afferma che *"un router invia un messaggio di join/eliminazione periodico a ogni singolo router adiacente RPF associato a ciascuna voce (S,G), (*,G) e (*,*,RP). I messaggi di unione/eliminazione vengono inviati solo se il router adiacente RPF è un router adiacente PIM."*

Per ridurre il problema, l'utente può aggiungere una voce di route statica sul firewall. Il router deve puntare a uno dei due indirizzi IP dell'interfaccia del router, 192.168.1.2 o 192.168.1.3, in genere l'indirizzo IP del router attivo HSRP.

Esempio:

<#root>

```
firepower#
```

show run mroute

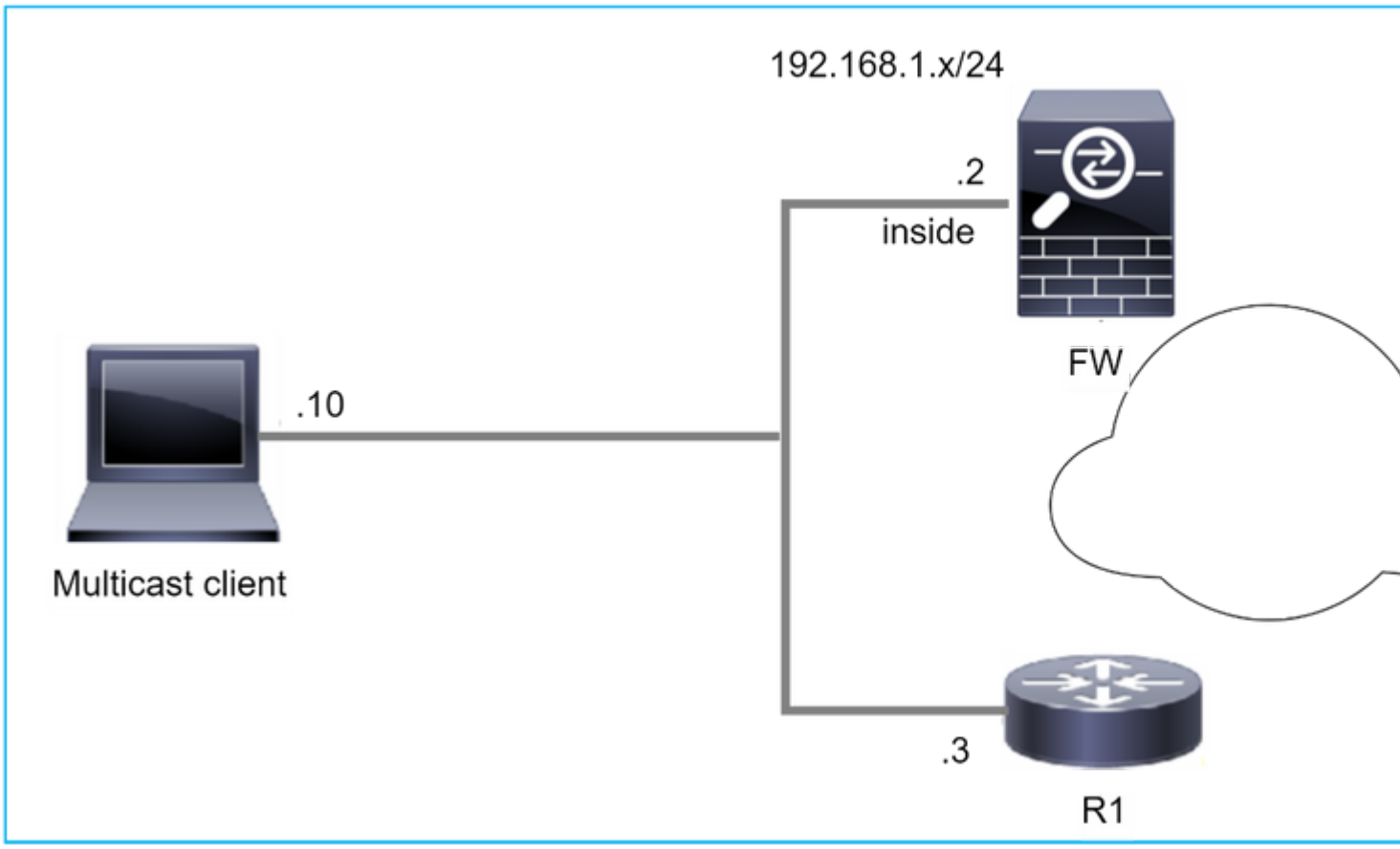
```
firepower#
```

mroute 172.16.1.1 255.255.255.255 192.168.1.2

Dopo aver configurato la route statica, per la ricerca RPF il firewall assegna la preferenza alla tabella di routing multicast anziché alla tabella di routing unicast dell'appliance ASA e invia i messaggi PIM direttamente alla porta adiacente 192.168.1.2.

> **Nota:** la route statica in alcuni casi annulla l'utilità della ridondanza HSRP, in quanto accetta solo 1 hop successivo per combinazione di indirizzo/maschera di rete. Se l'hop successivo specificato nel comando mroute ha esito negativo o non è più raggiungibile, il firewall non esegue il fallback sull'altro router.

Il firewall non è considerato LHR quando non è il DR nel segmento LAN



Il firewall ha R1 come router PIM adiacenti nel segmento LAN. R1 è il PIM DR:

```
<#root>

firepower#

show pim neighbor

Neighbor Address  Interface          Uptime    Expires DR pri Bidir

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

Se viene ricevuta una richiesta di aggiunta IGMP dal client, il firewall non diventa il LHR.

Il percorso mostra **Null** aggiuntivo come OIL e ha il flag **Pruned**:

```
<#root>

firepower#

show mroute

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

```
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State


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

flags

```
: S
```

P

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

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

Per rendere il firewall l'LHR, la priorità DR dell'interfaccia può essere aumentata.

<#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

Il comando PIM debug **pim** visualizza questo output:

<#root>

```
firepower#
```

debug pim

```
firepower#
```

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

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

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

Il flag Eliminato e il valore Null vengono rimossi dalla route:

<#root>

firepower#

show mroute

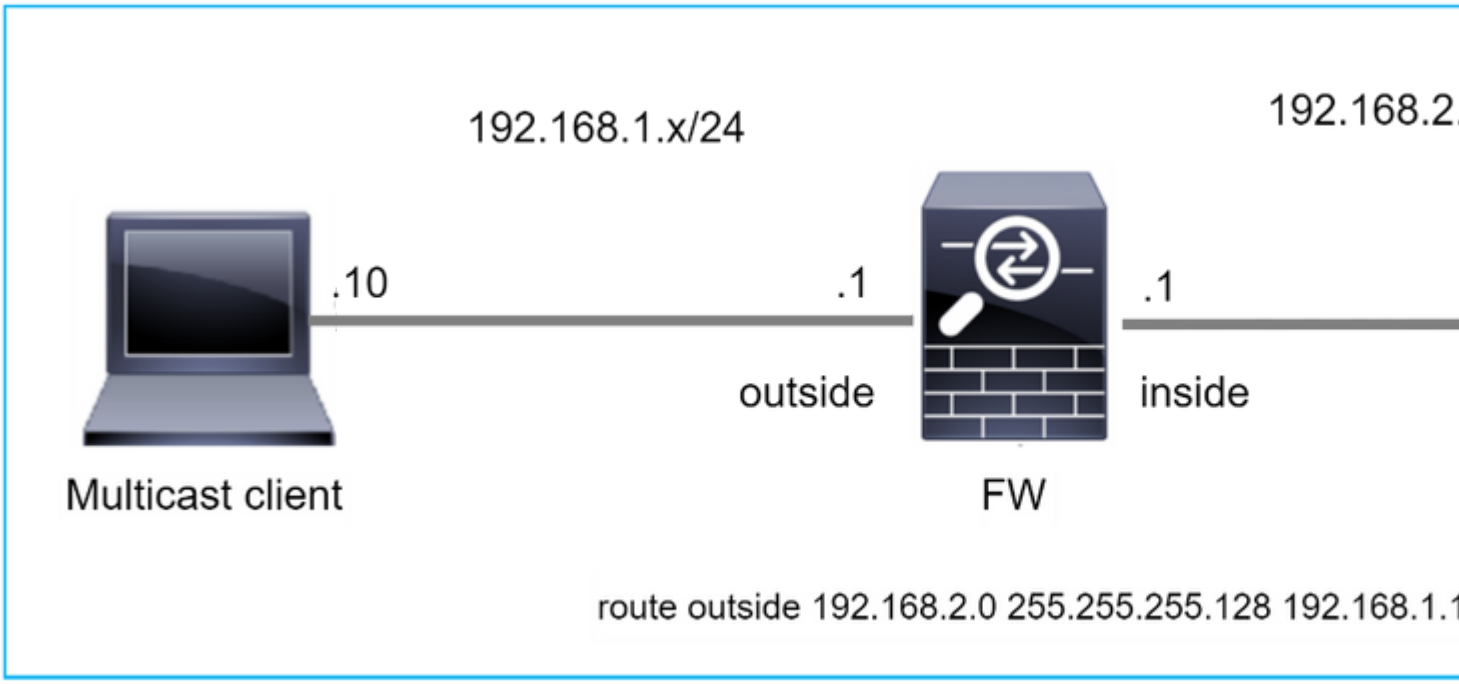
```
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface,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

Il firewall rifiuta i pacchetti multicast a causa di un errore di controllo inoltro percorso inverso



In questo caso, i pacchetti UDP multicast vengono scartati a causa di un errore RPF, in quanto il firewall ha un percorso più specifico con maschera 255.255.255.128 tramite l'interfaccia esterna.

<#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
```

Le acquisizioni ASP mostrano il motivo **della** rimozione **violata da rpf**:

```
<#root>

firepower#

show capture asp


Target:     OTHER
```

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

21 packets captured



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


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

I contatori RPF non riusciti nell'output MFIB aumentano:

<#root>

```
firepower#
```

show mfib 230.1.1.1 count

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

Group: 230.1.1.1

```
  RP-tree:
```

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

```
...
firepower#
```

show mfib 230.1.1.1 count

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

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

La soluzione consiste nel correggere l'errore di controllo RPF. Un'opzione consiste nel rimuovere la route statica.

Se non si verificano altri errori di controllo RPF, i pacchetti vengono inoltrati e il contatore **Forwarding** nell'output MFIB aumenta:

<#root>

```
firepower#
```

show mfib 230.1.1.1 count

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

Source: 192.168.2.2,

Forwarding: 1033/9/528/39

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

show mfib 230.1.1.1 count

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

Source: 192.168.2.2,

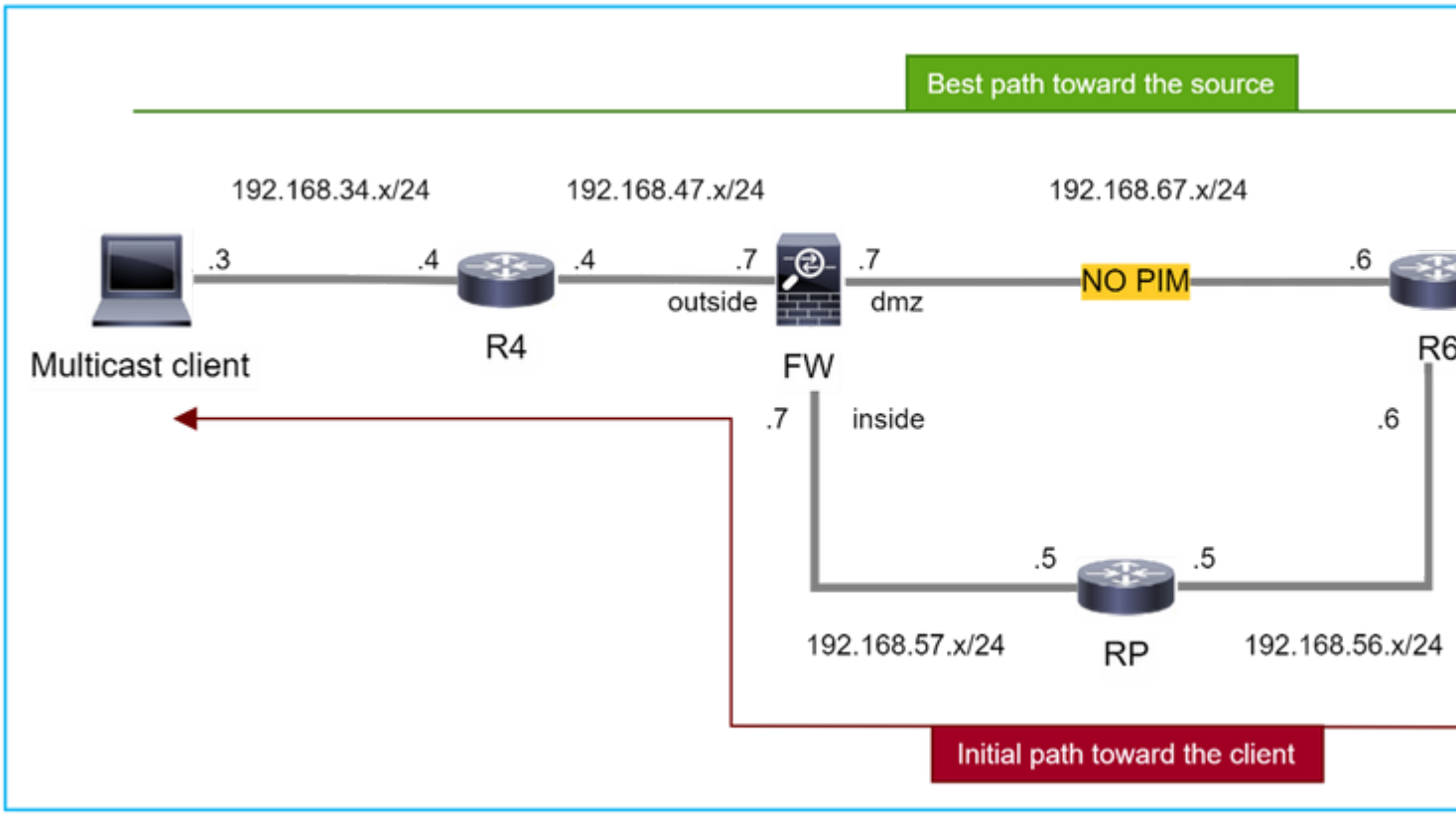
Forwarding: 1044/10/528/41

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

<--- Forward counter increased

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

Il firewall non genera l'unione PIM in caso di passaggio PIM all'albero di origine



In questo caso, il firewall apprende il percorso verso l'origine multicast tramite l'interfaccia **dmz R4 > FW > R6**, mentre il percorso iniziale del traffico dall'origine al client è **R6 > RP > DW > R4:**

<#root>

```
firepower#
```

```
show route 192.168.6.100
```

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

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

```
  Routing Descriptor Blocks:
```

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

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

R4 avvia lo switchover SPT e invia un messaggio di join PIM specifico dell'origine una volta raggiunta la soglia di switchover SPT. Nel firewall lo switchover SPT non ha luogo, il percorso (S,G) non ha il flag **T**:

<#root>

```
firepower#
```

show mroute

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

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

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

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

Il comando PIM debug **pim** visualizza 2 richieste di unione PIM ricevute dal peer R4 - per **(*,G) e (S,G).** Il firewall ha inviato una richiesta di aggiunta PIM per (*,G) a monte e non è stato in grado di inviare una richiesta specifica dell'origine a causa di un router adiacente non valido 192.168.67.6:

<#root>

```
firepower#
```

debug pim

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

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

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

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

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

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

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

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

<--- Invalid neighbor

L'output del comando **show pim neigbour** è privo di R6:

<#root>

firepower#

show pim neighbor

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

PIM è abilitato sul dmz dell'interfaccia del firewall:

<#root>

firepower#

show pim interface

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

```
192.168.47.7     outside            on   1     30     1          this system
192.168.67.7     dmz                on   0     30     1          this system
192.168.57.7     inside             on   1     30     1          this system
```

PIM disattivato sull'interfaccia R6:

<#root>

```
R6#
show ip interface brief

Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         192.168.6.1     YES manual up                    up
GigabitEthernet0/1         192.168.56.6    YES manual up                    up
GigabitEthernet0/2         unassigned      YES unset  administratively down down
GigabitEthernet0/3         192.168.67.6    YES manual up                    up

Tunnel0                    192.168.56.6    YES unset  up                    up

R6#
show ip pim interface GigabitEthernet0/3 detail

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

PIM: disabled <--- PIM is disabled

  Multicast Tagswitching: disabled
```

La soluzione consiste nell'abilitare PIM sull'interfaccia Gigabit Ethernet0/3 su R6:

<#root>

```
R6(config-if)#
interface GigabitEthernet0/3

R6(config-if)#
ip pim sparse-mode

R6(config-if)#
```

```
*Apr 21 13:17:14.575: %PIM-5-NBRCHG: neighbor 192.168.67.7 UP on interface GigabitEthernet0/3
```

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

Il firewall installa il flag T, che indica lo switchover SPT**:**

<#root>

```
firepower#
```

```
show mroute
```

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

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

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

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

Il firewall rifiuta i primi pacchetti a causa del limite della velocità massima

Quando il firewall riceve i primi pacchetti di un **nuovo** flusso multicast in FP, può essere necessaria un'ulteriore elaborazione da parte del CP. In questo caso, FP punta i pacchetti al CP tramite SP (FP > SP > CP) per operazioni aggiuntive:

- Creazione di una connessione **padre** in FP tra le interfacce in entrata e le interfacce di identità.
- Controlli aggiuntivi specifici per il multicast, come la convalida RPF, l'incapsulamento PIM (nel caso in cui il firewall sia FHR), il controllo OIL e così via.
- Creazione di una voce (S,G) con le interfacce in entrata e in uscita nella tabella mroute.
- Creazione di una connessione **figlio/stub** in FP tra le interfacce in ingresso e in uscita.

Come parte della protezione del control plane, il firewall limita internamente la velocità del pacchetto inviato al PC.

I pacchetti che superano la velocità vengono scartati nel router con il motivo della perdita del **limite di velocità di punt**:

<#root>

firepower#

show asp drop

Frame drop:

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

Utilizzare il comando **show asp cluster counter** per verificare il numero di pacchetti multicast puntati a TCP dall'SP:

<#root>

firepower#

show asp cluster counter

Global dp-counters:

Context specific dp-counters:

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

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

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

Usare il comando **show asp event dp-cp punt** per verificare il numero di pacchetti nella coda FP > CP e la frequenza di 15 secondi:

<#root>

firepower#

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

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

multicast

23800 0

23800

0 10200

```
1402

  pim                 652          0      652        0      652          0
```

Quando la route viene popolata e le connessioni padre/figlio vengono stabilite nell'FP, i pacchetti vengono inoltrati nell'FP come parte delle connessioni esistenti. In questo caso, FP non reindirizza i pacchetti al CP.

In che modo il firewall elabora i primi pacchetti di un nuovo flusso multicast?

Quando il firewall riceve i primi pacchetti di un **nuovo** flusso multicast nel datapath, esegue le seguenti azioni:

1. Controlla se il criterio di protezione consente i pacchetti.
2. Perfora i pacchetti verso il PC tramite il percorso FP.
3. Crea una connessione **padre** tra le interfacce in entrata e le interfacce di identità:

```
<#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

Registri di sistema:

<#root>

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

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

Questa connessione è visibile nell'output del comando **show conn all**:

<#root>

```
firepower#
```

show conn all protocol udp

```
13 in use, 17 most used
```

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

4. Il CP avvia il processo multicast per ulteriori controlli specifici del multicast, come la convalida RPF, l'incapsulamento PIM (nel caso in cui il firewall sia il FHR), il controllo OIL, e così via.
5. Il CP crea una voce (S,G) con le interfacce in entrata e in uscita nel router:

<#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. Il PC indica al FP tramite CP > SP > FP path di creare una connessione **figlio/stub** tra le interfacce in entrata e in uscita:

Questa connessione è visibile solo nell'output del comando **show local-host**:

<#root>

```
firepower#
show local-host



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


    UDP outside  230.1.1.1:12345 inside  192.168.1.100:12345, idle
 0:00:04, bytes 4000, flags -
local host: <224.0.0.5>,
local host: <224.0.0.1>,
Interface inside: 4 active, 5 maximum active
local host: <192.168.1.100>,


  Conn:


    UDP outside  230.1.1.1:12345 inside  192.168.1.100:12345, idle
 0:00:04, bytes 4000, flags -
local host: <224.0.0.13>,
local host: <192.168.2.1>,
local host: <224.0.0.5>,
Interface nlp_int_tap: 0 active, 2 maximum active
Interface any: 0 active, 0 maximum active
```

Nelle versioni software con la correzione del bug Cisco con ID CSCwe21280 , viene generato anche il messaggio syslog 302015 per la connessione figlio/stub:

<#root>

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

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

Quando vengono stabilite connessioni padre e figlio/stub, i pacchetti in entrata corrispondono alla connessione esistente e vengono inoltrati in FP:

<#root>

```
firepower#
show capture capi trace packet-number 2


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

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


Phase: 3


Type: FLOW-LOOKUP


Subtype:
Result: ALLOW
Config:
Additional Information:
Found flow with id 19, using existing flow <--- Existing flow




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

Filtra traffico multicast ICMP

Non è possibile filtrare il traffico multicast ICMP con un ACL. È necessario utilizzare la policy Control

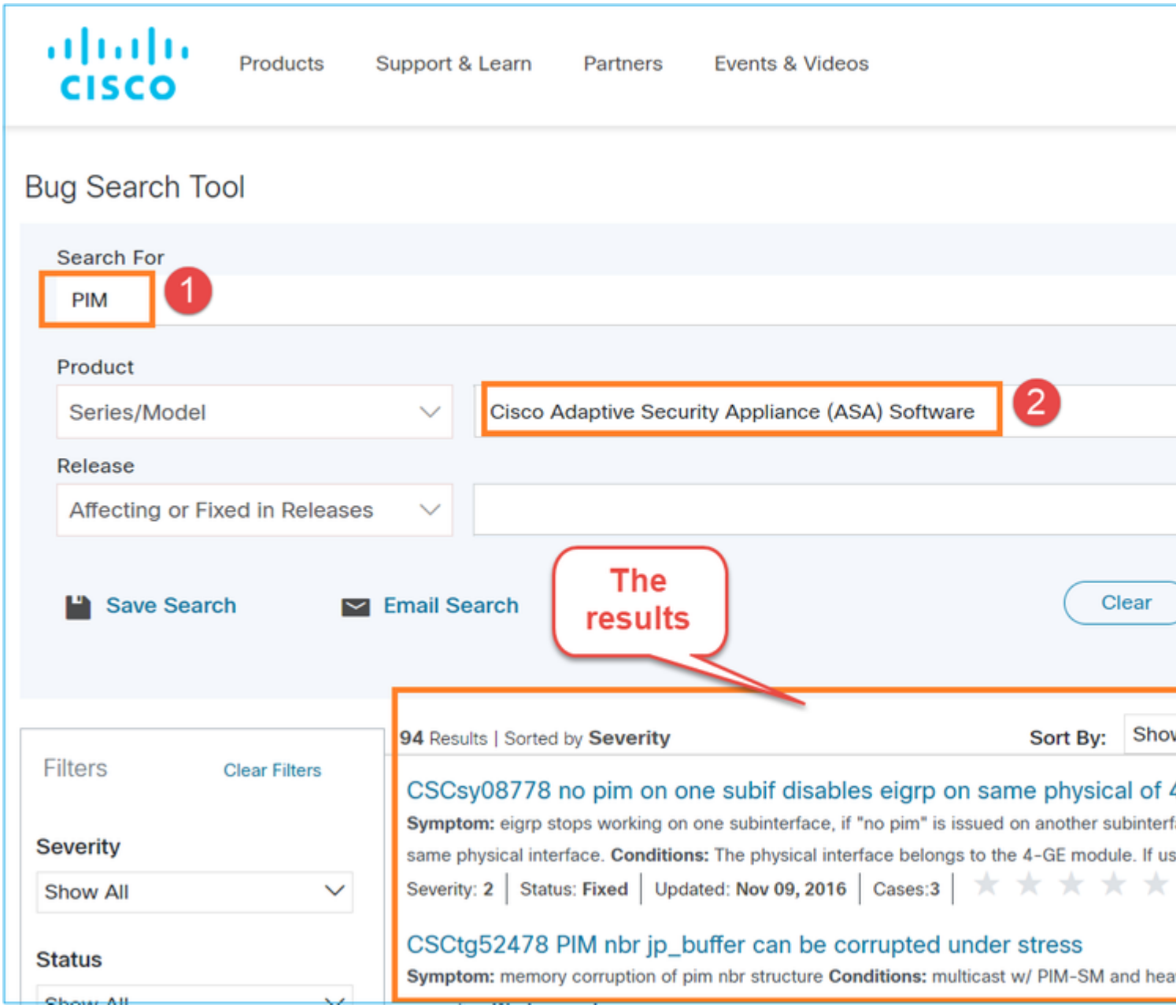
Plane (ICMP):

Cisco bug ID CSCsl26860 ASA non filtra i pacchetti ICMP multicast

Difetti noti del multicast PIM

Per individuare i difetti noti, è possibile usare Bug Search Tool: https://bst.cloudapps.cisco.com/bugsearch

La maggior parte dei difetti di ASA e FTD è elencata nel prodotto 'Software Cisco Adaptive Security Appliance (ASA)':



Informazioni correlate

- Risoluzione dei problemi comuni e multicast ASA
- Multicast di Firepower Management Center
- Riepilogo dei flag Firepower Multicast

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).