Probleemoplossing voor Firepower Threat Defence en ASA Multicast PIM

Inhoud

Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Achtergrondinformatie
Multicast-routingbasics
Afkortingen/acroniemen
Taak 1 - PIM Sparse mode (statische RP)
Taak 2 - Configureer PIM bootstrap router (BSR)
Methodologie voor probleemoplossing
Opdrachten voor PIM-probleemoplossing (cheatsheet)
Bekende problemen
PIM wordt niet ondersteund op een vPC Nexus
Doelgebieden worden niet ondersteund
Firewall stuurt geen PIM-berichten naar upstream-routers vanwege HSRP
De firewall wordt niet als LHR beschouwd wanneer deze niet de methode voor noodherstel in het LAN-segment is
Firewall Drops Multicast Packets vanwege het doorsturen van pad naar omgekeerd pad Controleer de fout
Firewall genereert geen PIM-koppeling na PIM-switching naar bronstructuur
Firewall Drops Eerste paar pakketten vanwege punt rate Limit
Filter ICMP multicast verkeer
Bekende PIM-multicast defecten
Gerelateerde informatie

Inleiding

Dit document beschrijft hoe Firepower Threat Defence (FTD) en Adaptive Security Appliance (ASA) Protocol Independent Multicast (PIM) implementeren.

Voorwaarden

Vereisten

Basiskennis over IP-routing.

Gebruikte componenten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Firepower 4125 Threat Defence versie 7.1.0.
- Firepower Management Center (FMC) versie 7.1.0.
- Software voor Cisco adaptieve security applicatie versie 9.17(1)9.

Achtergrondinformatie

Multicast-routingbasics

- Unicast voorwaartse pakketten naar de bestemming terwijl **multicast voorwaartse pakketten weg van de bron.**
- Multicast-netwerkapparaten (firewalls/routers, enzovoort) sturen de pakketten door via **Reverse Path Forwarding (RPF).** Merk op dat RPF niet hetzelfde is als uRPF die wordt gebruikt in unicast om specifieke soorten aanvallen te voorkomen. RPF kan worden gedefinieerd als een mechanisme dat multicast-pakketten doorstuurt weg van de bron uit interfaces die naar multicast-ontvangers leiden. Zijn belangrijkste rol is om verkeerslussen te voorkomen en juiste verkeerspaden te verzekeren.
- Een multicast protocol zoals PIM heeft 3 hoofdfuncties:

1. Zoek de **upstream interface** (interface het dichtst bij de bron).

2. Vind de **stroomafwaartse interfaces** verbonden aan een specifieke multicast stroom (interfaces naar de ontvangers).

3. Onderhouden van de multicast-boom (toevoegen of verwijderen van de boomtakken).

- Een multicast boom kan worden gebouwd en onderhouden door een van de 2 methoden: **implicit joins (flood-and-prune)** of **expliciete joins (pull model).** PIM Dense Mode (PIM-DM) maakt gebruik van impliciete joins, terwijl PIM Sparse Mode (PIM-SM) expliciete joins gebruikt.
- Een multicast-structuur kan worden **gedeeld** of **op basis van bronnen:**
  - Gedeelde bomen gebruiken het concept van **rendez-vous point (RP)** en worden aangeduid als **(*, G)** waar G = multicast groep IP.
  - Op bronnen gebaseerde bomen zijn geworteld aan de bron, maken geen gebruik van een RP en worden aangeduid als **(S, G)** waar S = het IP van de multicast bron/server.
- Multicast-verzendmodellen:
  - **In de Any-Source Multicast (ASM)**-leveringsmodus worden gedeelde bomen (*, G) gebruikt, waar elke bron de multicast-stroom kan verzenden.
  - **Source Specific Multicast (SSM)** maakt gebruik van op bronnen gebaseerde bomen (S, G) en het IP-bereik 232/8.
  - **Bidirectioneel (BiDir)** is een type gedeelde boom (*, G) waar zowel besturings- als dataplaat verkeer door de RP gaat.
- Een rendez-vous point kan met een van de volgende methoden worden geconfigureerd of geselecteerd:
  - Statische RP
  - Auto-RP
  - Bootstrap router (BSR)

Samenvatting van PIM-modi

PIM-modus	RP	Gedeelde structuur	Notatie	IGMP	ASA/FTD ondersteund
PIM Sparse Mode	Ja	Ja	(*, G) en	v1/v2/v3	Ja

			(S, G)		
PIM Dense Mode	Nee	Nee	S, G)	v1/v2/v3	Nee*
PIM bidirectionele modus	Ja	Ja	(*, G)	v1/v2/v3	Ja
PIM Source-Specific-Multicast (SSM) modus	Nee	Nee	S, G)	v3	Nee**

*Auto-RP = Auto-RP verkeer kan doorlopen

** ASA/FTD kan geen laatste-hop apparaat zijn

Samenvatting van RP-configuratie

Rendez-vous point configuratie	**ASA/FTD**
Statische RP	Ja
Auto-RP	Nee, maar Auto-RP-besturingsplane verkeer kan door
BSR	Ja, maar niet voor C-RP-ondersteuning

Opmerking: voordat u een multicast probleem begint op te lossen, is het erg belangrijk om een duidelijk beeld van de multicast topologie te hebben. U moet op zijn minst weten:
- Wat is de rol van de firewall in de multicast topologie?
- Wie is de RP?
- Wie is de afzender van de multicast stream (IP van bron en IP van multicast groep)?
- Wie is de ontvanger van de multicast stream?
- Heeft u problemen met het besturingsplane (IGMP/PIM) of het dataplane (multicast stream) zelf?

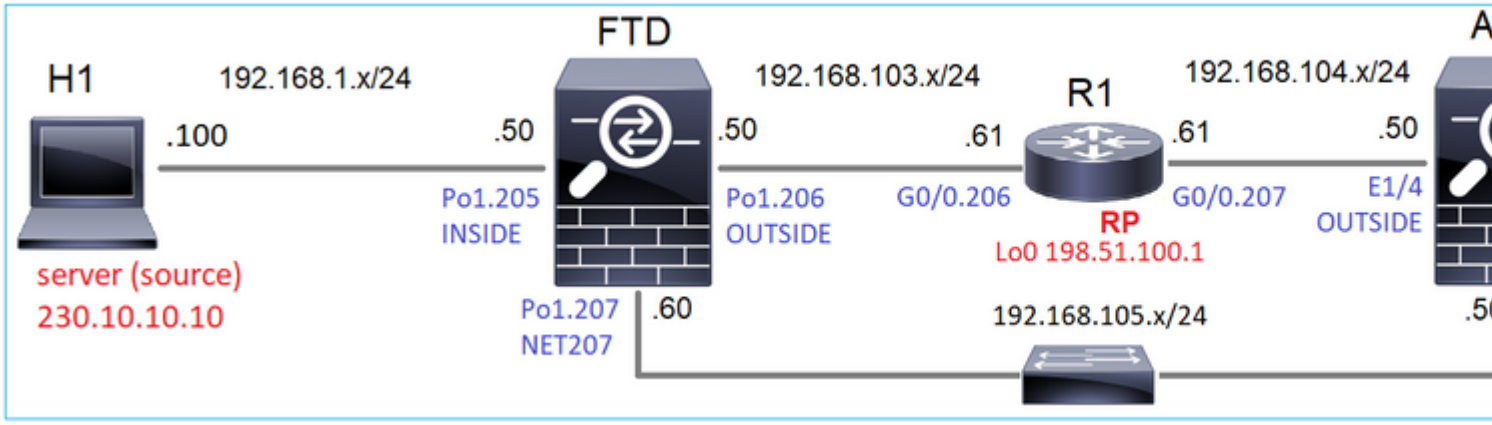
Afkortingen/acroniemen

Acroniemen	**Toelichting**
FHR	First-hop router - een hop die rechtstreeks is verbonden met de bron van het multicast verkeer.

LHR	Last-Hop Router - een hop die rechtstreeks is verbonden met de ontvangers van het multicast verkeer.
RP	rendez-point
DR	Aangewezen router
NBP	Shortest-Path boom
RPT	Rendezvous-Point (RP)-structuur, gedeelde structuur
RPF	Doorsturen van pad omkeren
OLIE	Uitgaande interfacelijst
MIRIB	Multicast-routing informatiebasis
MFIB	Multicast Forwarding Information Base
ASM	Any-bron multicast
BSR	Bootstrap router
SSM	Source-Specific Multicast
FP	Snel pad
SP	Langzaam pad
CP	Controlepunt
PS	Pakket per seconde

Taak 1 - PIM Sparse mode (statische RP)

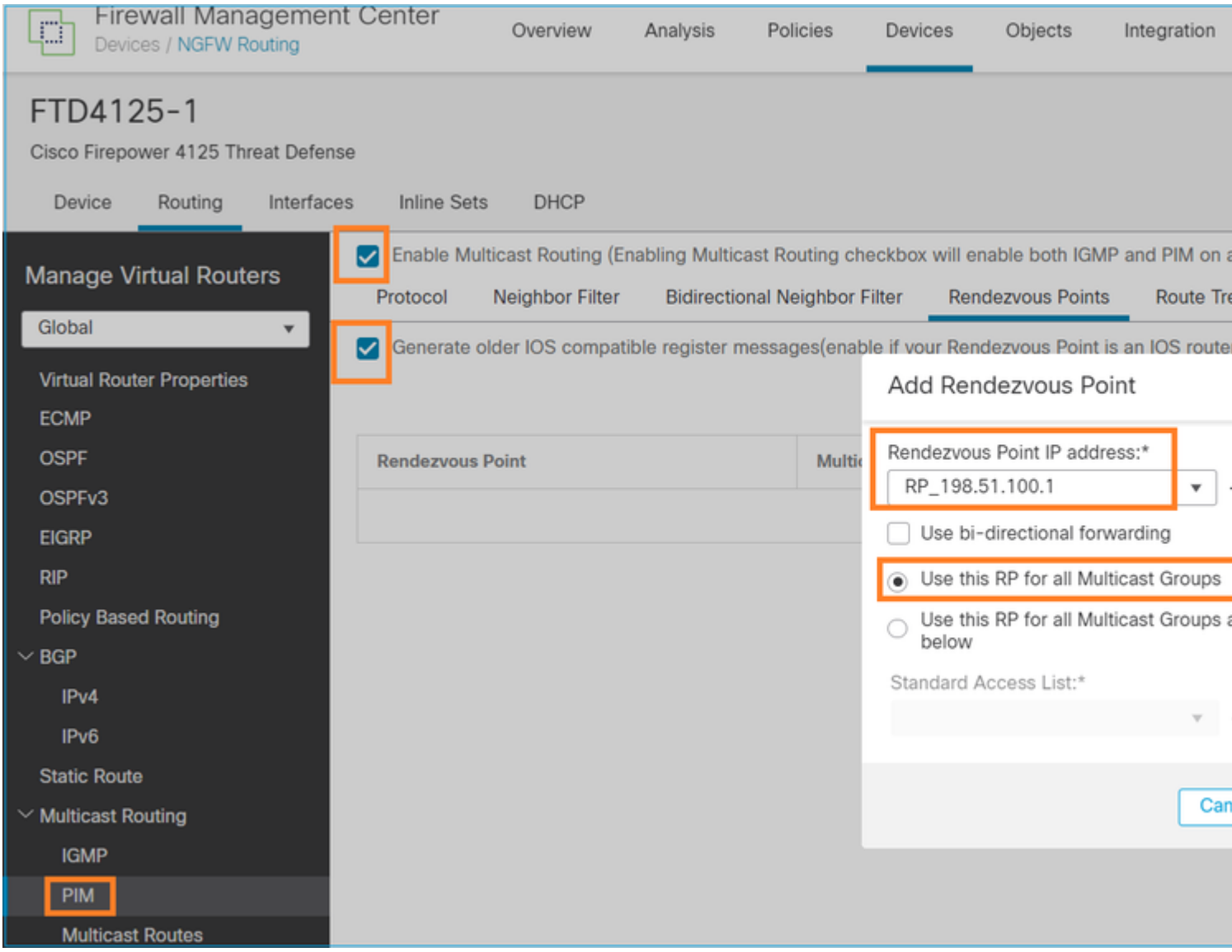
Topologie



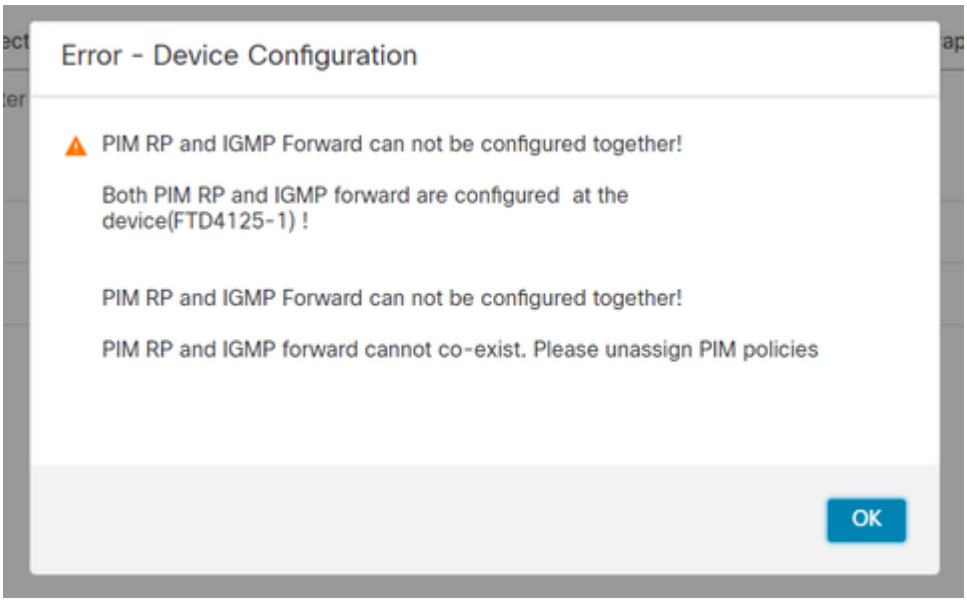
Configureer multicast PIM sparse-mode in de topologie met R1 (198.51.100.1) als RP.

Oplossing

FTD-configuratie:



ASA/FTD kan niet tegelijkertijd worden geconfigureerd voor IGMP Stub Routing en PIM:



De resulterende configuratie van 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

Op ASA firewall is er een vergelijkbare configuratie:

<#root>

```
asa(config)#
multicast-routing

asa(config)#
pim rp-address 198.51.100.1
```

RP-configuratie (Cisco router):

<#root>

```
ip multicast-routing
ip pim rp-address 198.51.100.1           <-- The router is the RP
!
interface GigabitEthernet0/0.206
 encapsulation dot1Q 206
 ip address 192.168.103.61 255.255.255.0
 ip pim sparse-dense-mode                <-- The interface participates in multicast routing
 ip ospf 1 area 0
!
interface GigabitEthernet0/0.207
 encapsulation dot1Q 207
 ip address 192.168.104.61 255.255.255.0
 ip pim sparse-dense-mode                <-- The interface participates in multicast routing
 ip ospf 1 area 0
!
interface Loopback0

ip address 198.51.100.1 255.255.255.255
<-- The router is the RP

ip pim sparse-dense-mode                <-- The interface participates in multicast routing
 ip ospf 1 area 0
```

Verificatie

Controleer het multicast-besturingsplane op FTD wanneer er geen multicast-verkeer is (afzenders of ontvangers):

<#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
```

Controleer de PIM-buren:

```
<#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)
```

De RP adverteert voor het gehele multicast groepsbereik:

```
<#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
```

De firewallroutetabel bevat een aantal niet-relevante vermeldingen (239.255.255.250 is Simple Service Discovery Protocol (SSDP) dat wordt gebruikt door leveranciers als MAC OS en 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
```

Er is een PIM-tunnel gebouwd tussen de firewalls en de RP:

<#root>

firepower#

show pim tunnel

Interface	RP Address	Source Address
Tunnel0	**198.51.100.1**	**192.168.103.50**

<-- PIM tunnel between the FTD and the RP

De PIM-tunnel is ook te zien op de tabel met firewallverbindingen:

<#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
```

Verificatie op de ASA firewall:

<#root>

asa#

show pim neighbor

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

<#root>

```
asa#
```

show pim tunnel

```
Interface          RP Address        Source Address
```

Tunnel0 198.51.100.1 192.168.104.50

<-- PIM tunnel between the ASA and the RP

RP (Cisco router) RP-verificatie. Er zijn enkele multicastgroepen voor SSDP en 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
```

Verificatie zodra een ontvanger zijn aanwezigheid aankondigt

Opmerking: de firewallopdrachten in deze sectie zijn volledig van toepassing op ASA en FTD.

ASA krijgt het IGMP-ledenrapportbericht en maakt de IGMP- en routegegevens (*, G) aan:

<#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

De ASA firewall maakt een route voor de multicast groep:

<#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

Een andere firewallcontrole is de PIM topologieoutput:

<#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

> **Opmerking**: Als de firewall geen route naar de RP heeft, toont de **debug**-pim-uitvoer een RPF-lookup-fout

---

De RPF-zoekfout in de **debug**-output:

<#root>

asa#

debug pim

IPv4 PIM: RPF lookup failed for root 198.51.100.1 <-- The RPF look fails because ther

IPv4 PIM: RPF lookup failed for root 198.51.100.1

IPv4 PIM: (*,230.10.10.10) Processing Periodic Join-Prune timer
IPv4 PIM: (*,230.10.10.10) J/P processing
IPv4 PIM: (*,230.10.10.10) Periodic J/P scheduled in 50 secs
IPv4 PIM: (*,230.10.10.10) No RPF neighbor to send J/P

In het geval dat alles OK is, stuurt de firewall een PIM Join-Prune bericht naar de RP:

<#root>

asa#

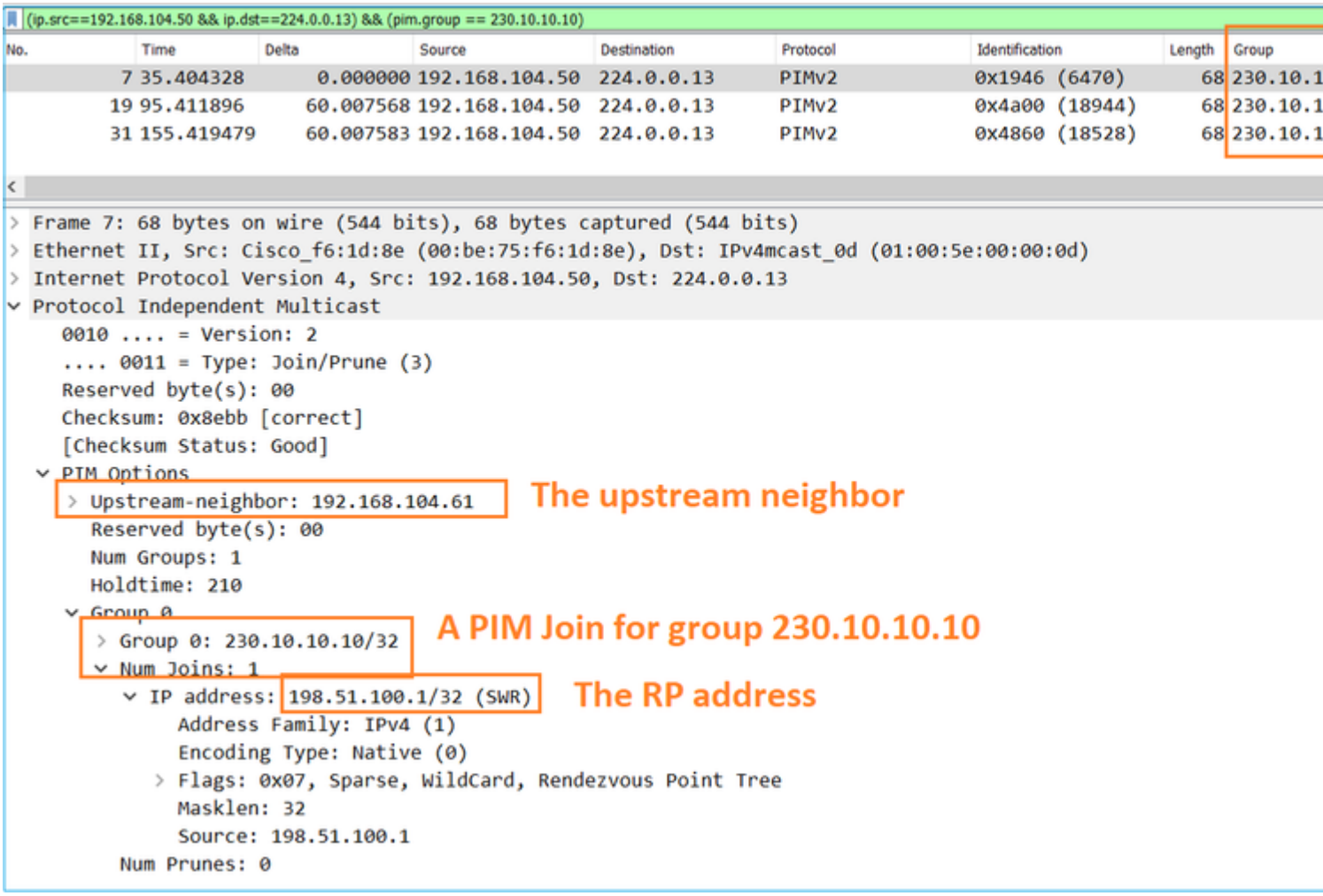
debug pim group 230.10.10.10

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

De opname laat zien dat de PIM Join-berichten elke 1 min en PIM Hellos elke 30 seconden worden verzonden. PIM gebruikt IP 24.0.0.13:



Tip: Wireshark display filter: (ip.src==192.168.104.50 & ip.dst==224.0.0.13) & & (pim.group == 230.10.10.10)
- 192.168.104.50 is de firewall IP van de uitgaande interface (naar de upstream PIM-buur)
- 224.0.0.13 is de multicastgroep van PIM waarin de PIM-verbindingen en -prunes worden verzonden
- 230.10.10.10 is de multicastgroep waarvoor we de PIM Join/Prune verzenden

---

De RP creëert een (*, G) route. Merk op dat aangezien er nog geen servers zijn de Inkomende Interface leeg is:

<#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

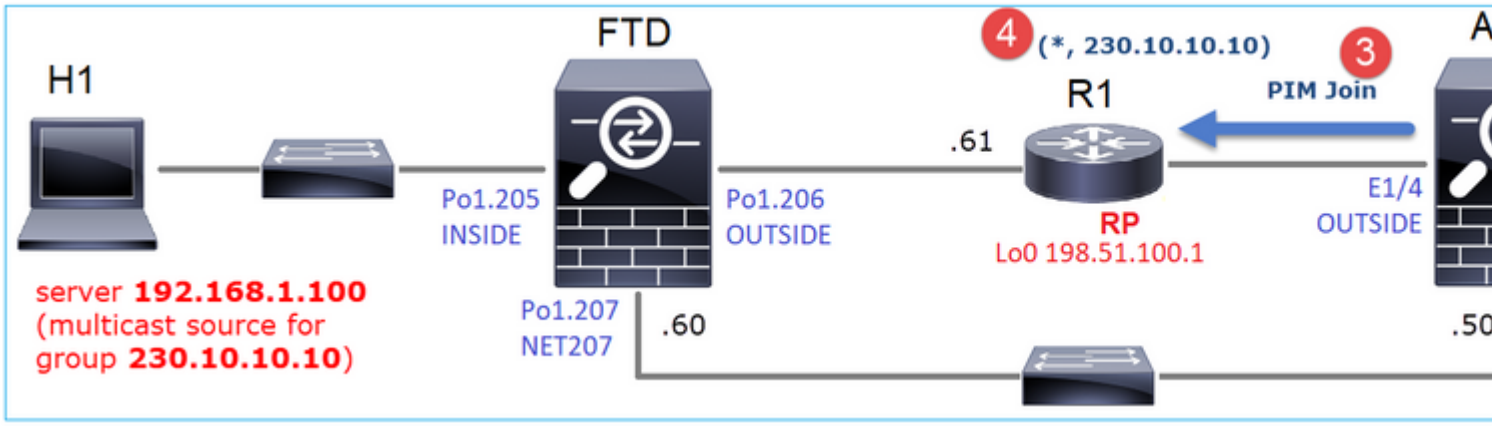
Incoming interface: Null

, 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
```

Dit kan worden gevisualiseerd als:



1. IGMP-rapport wordt ontvangen op ASA.
2. A (*, G) route wordt toegevoegd.
3. ASA stuurt een PIM Join-bericht naar de RP (198.51.100.1).
4. De RP ontvangt het Join bericht en voegt een (*, G) route toe.

Tegelijkertijd zijn er op FTD geen routes sinds er geen IGMP-rapport was en geen PIM Join ontving:

```
<#root>

firepower#

show mroute 230.10.10.10

No mroute entries found.
```

Verificatie wanneer de server een multicast-stroom verstuurt

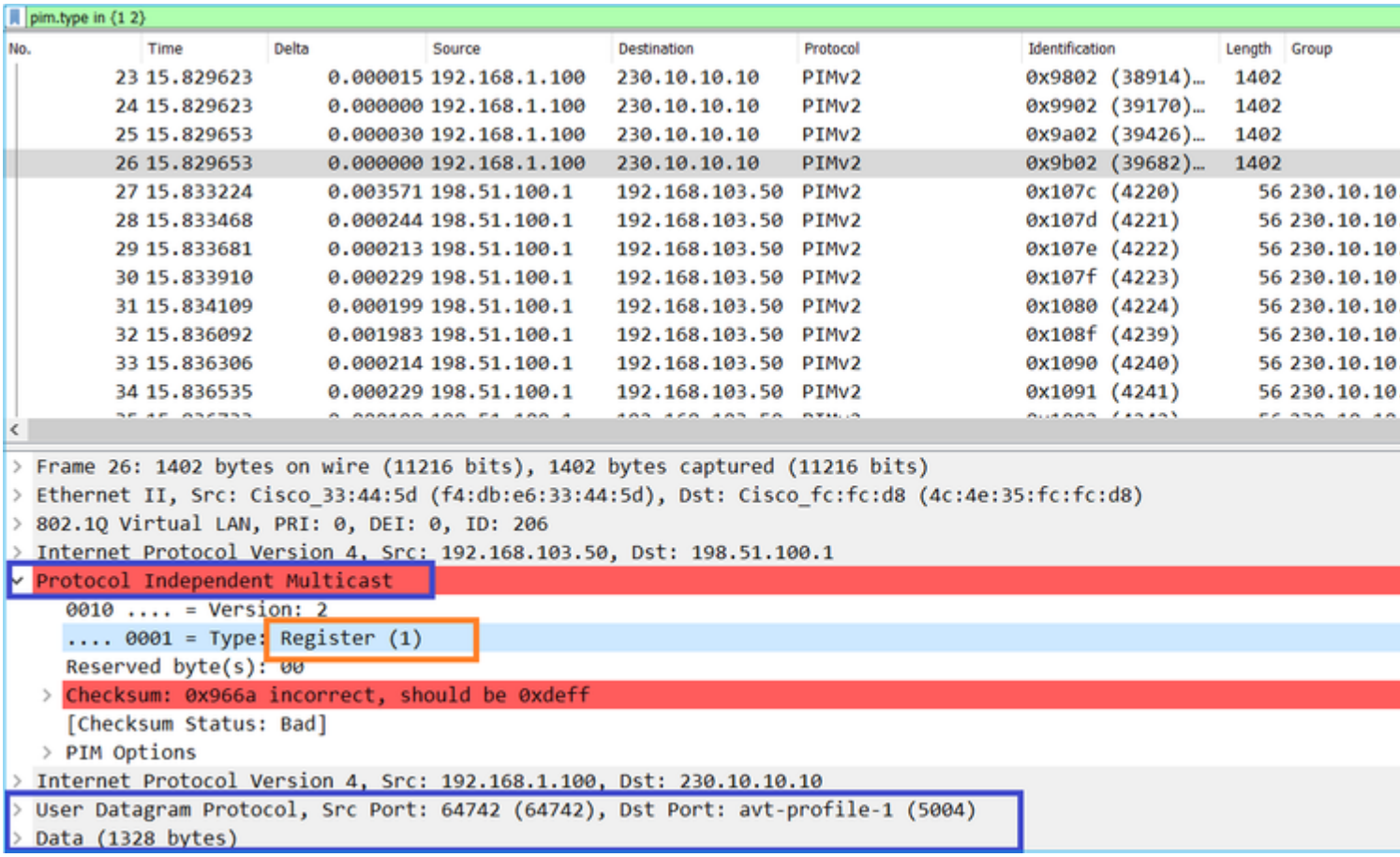
De FTD krijgt de multicast stream van H1 en start het **PIM-registratieproces** met de RP. Het FTD stuurt een **unicast PIM Register**-bericht naar de RP. De RP stuurt een **PIM Join** bericht naar de First-Hop-Router (FHR), in dit geval de FTD, om zich aan te sluiten bij de multicast boom. Dan stuurt het een **Register-Stop** bericht.

```
<#root>

firepower#

debug pim group 230.10.10.10


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

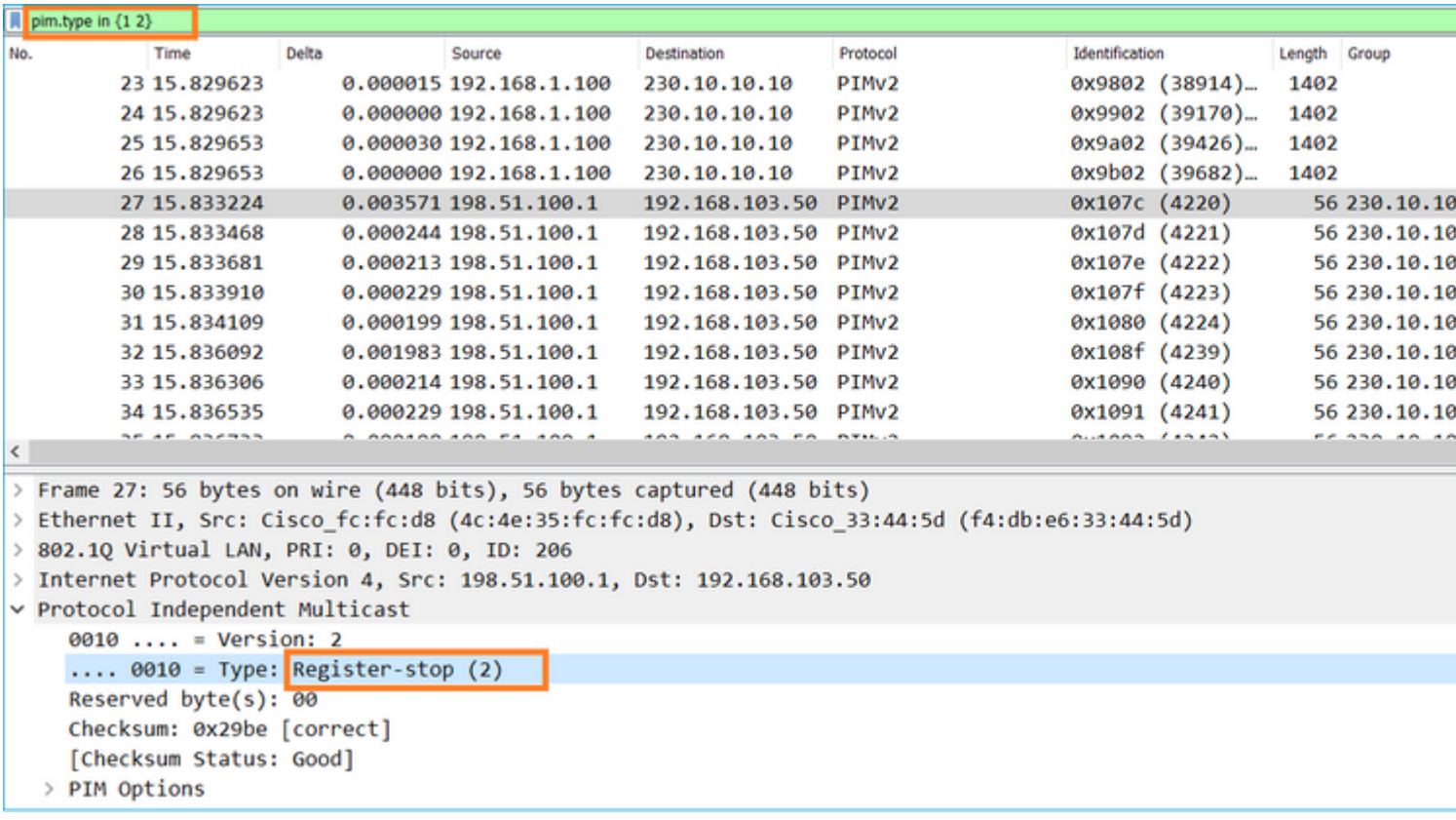
```
firepower#
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB update (f=20,c=20)
IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on INSIDE
IPv4 PIM: (192.168.1.100,230.10.10.10) Create entry
IPv4 PIM: (192.168.1.100,230.10.10.10) RPF changed from 0.0.0.0/- to 192.168.1.100/INSIDE


<-- 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)
```

Het PIM Register-bericht is een PIM-bericht dat UDP-gegevens draagt samen met de PIM Register-informatie:



Het PIM Register-Stop bericht:



Tip: Om alleen PIM Register en PIM Register-Stop berichten op Wireshark weer te geven, kunt u het weergavefilter gebruiken: pim.type in {1} 2}

De firewall (last-hop router) krijgt de multicast stream op de interface BUITEN, en initieert de overgang Shortest Path Tree (SPT) naar de interface NET207:

<#root>

asa#

debug pim group 230.10.10.10

IPv4 PIM group debugging is on
for group 230.10.10.10

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

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

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

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

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

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

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

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

Set SPT bit <-- The SPT bit is set

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

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

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


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


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

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


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


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

De PIM debug op de FTD wanneer de overschakeling plaatsvindt:

<#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
```

De FTD-route zodra de NBP-overschakeling begint:

```
<#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
```

Aan het einde van de NBP-overschakeling wordt alleen de NET207-interface in de OIL van FTD getoond:

```
<#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

Op de laatste-hop router (ASA), wordt het SPT-bit ook ingesteld:

<#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
```

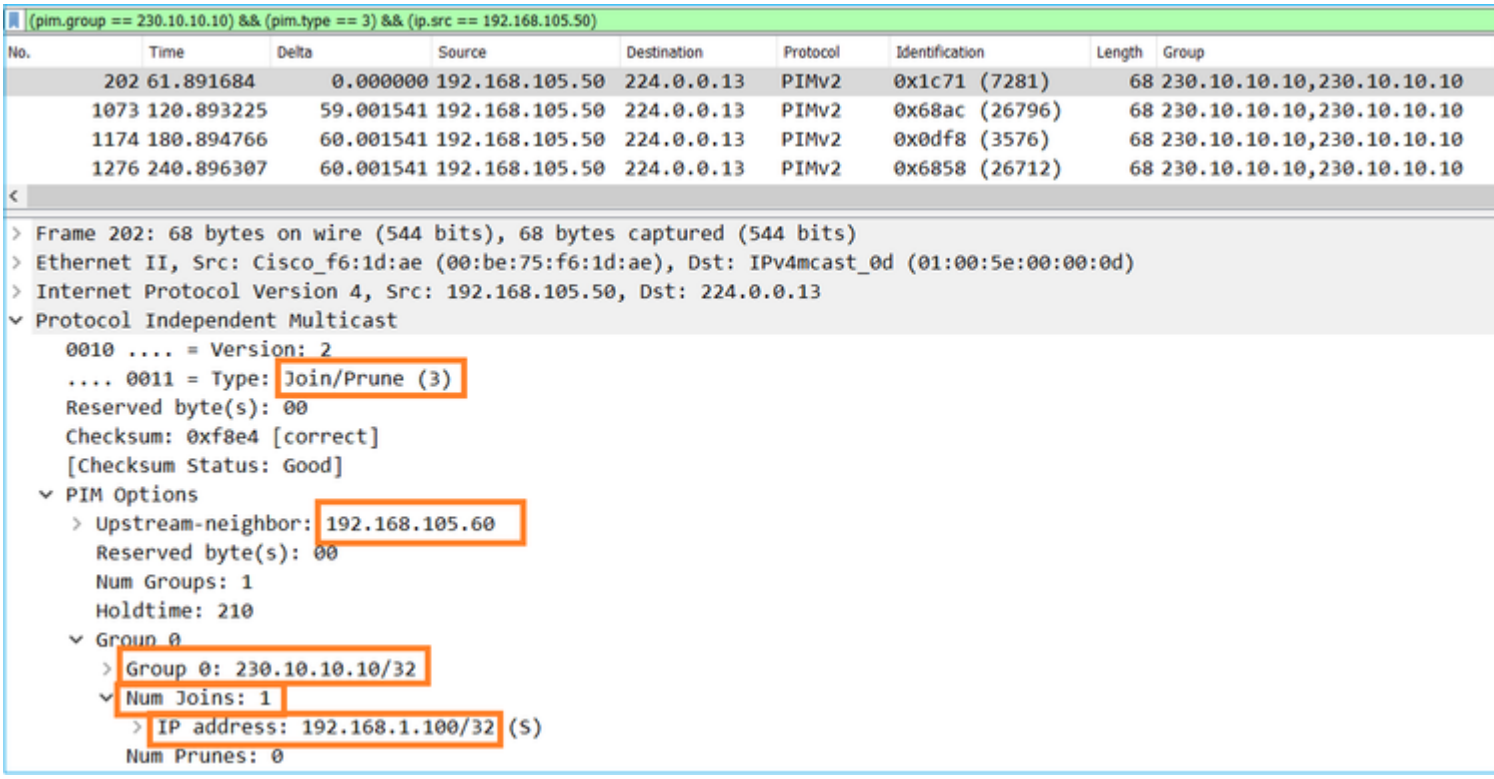
T   <-- SPT switchover for group 230.10.10.10

Incoming interface:

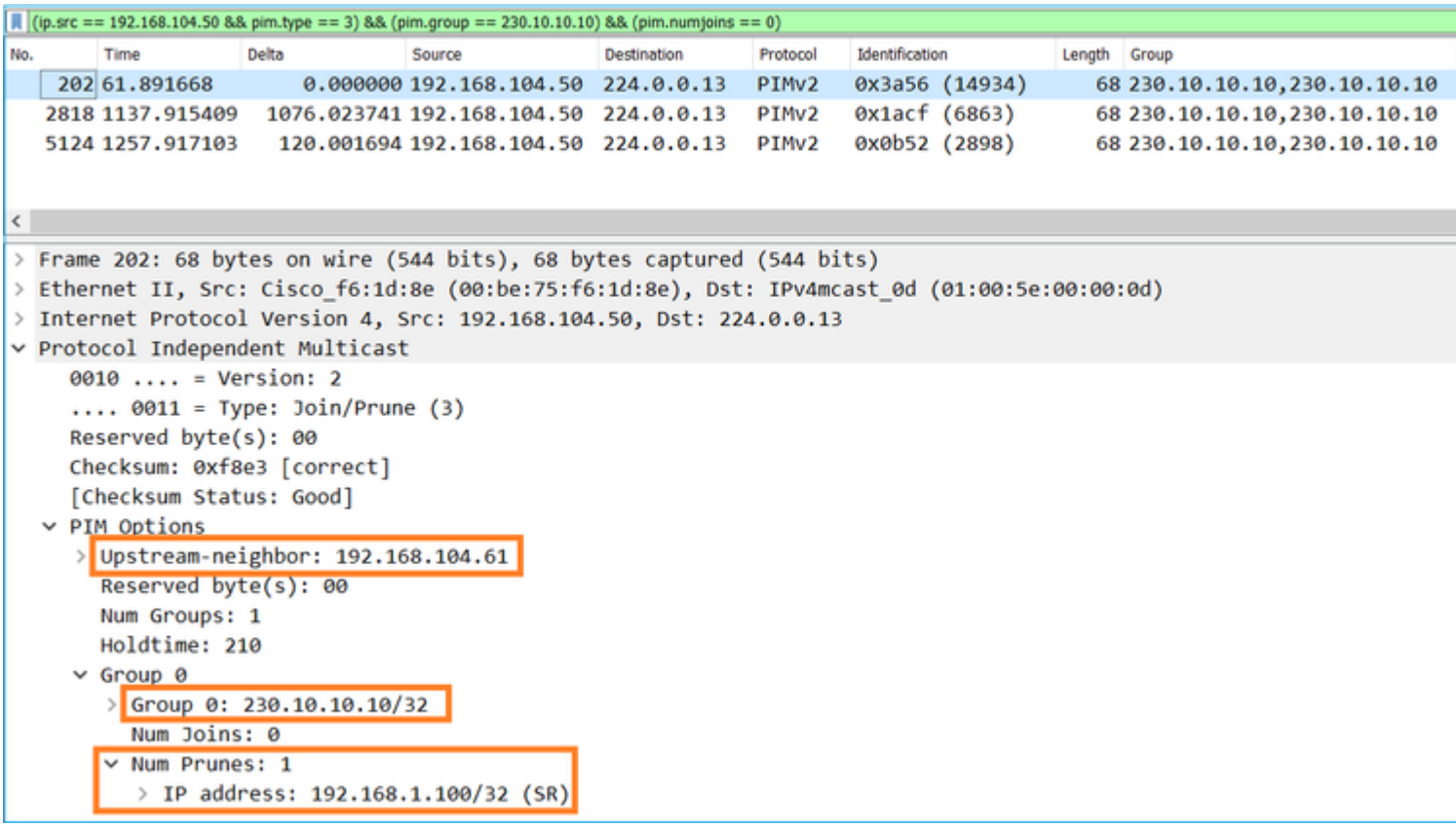
NET207   <-- The multicast packets arrive on interface NET207

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

De overschakeling van de ASA NET207 interface (de router met de eerste hop die de overschakeling heeft uitgevoerd). Een PIM Join bericht wordt verzonden naar het stroomopwaartse apparaat (FTD):



Op de BUITENinterface wordt een PIM Prune-bericht naar de RP gestuurd om de multicast stream te stoppen:



Verificatie van het PIM-verkeer:

```
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
```

Zo verifieert u het aantal pakketten dat in het langzame pad versus het snelle pad versus het controlepunt is verwerkt:

<#root>

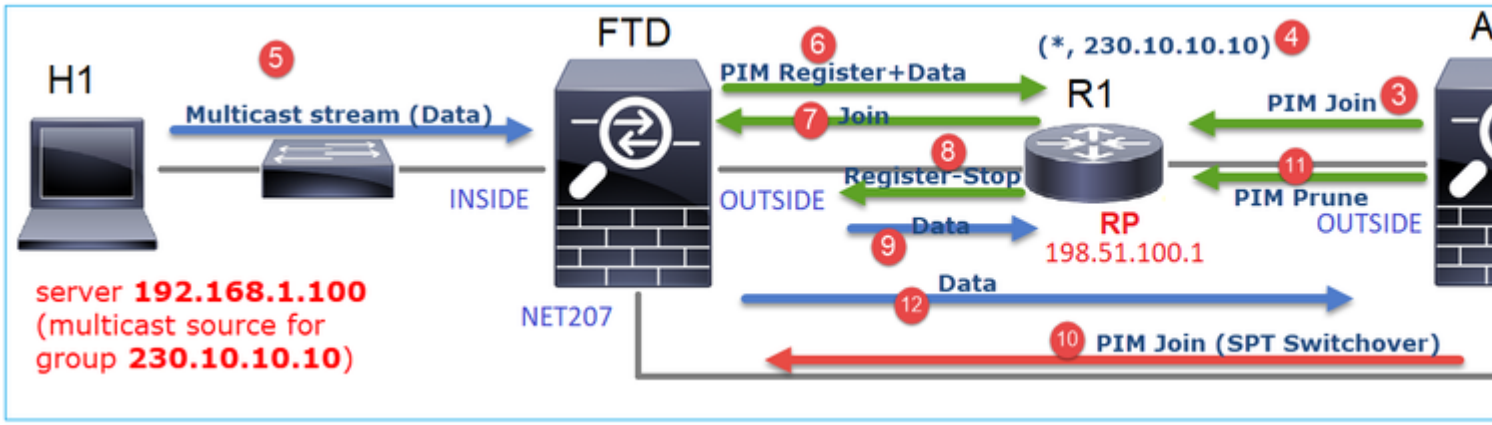
```
firepower#
```

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
```

Een diagram dat laat zien wat er stap voor stap gebeurt:



1. De end-host (H2) verstuurt een IGMP-rapport om zich aan te sluiten bij de multicast stream 230.10.10.10.
2. De laatste-hop router (ASA) die de PIM DR is, maakt een (*, 230.10.10.10) ingang.
3. De ASA stuurt een PIM Join-bericht naar RP voor groep 230.10.10.10.
4. Met de referentieprijs wordt het (*, 230.10.10.10) item gemaakt.
5. De server verstuurt de multicast stream gegevens.
6. Het FTD kapselt de multicastpakketten in PIM Register-berichten in en stuurt ze (unicast) naar RP. Op dit punt ziet de RP dat hij een actieve ontvanger heeft, decapsuleert de multicastpakketten en stuurt ze naar de ontvanger.
7. De RP stuurt een PIM Join bericht naar de FTD om zich aan te sluiten bij de multicast boom.
8. De RP stuurt een PIM Register-Stop bericht naar de FTD.
9. De FTD stuurt een native multicast stream (geen PIM-inkapseling) naar de RP.
10. De last-hop router (ASA) ziet dat de bron (192.168.1.100) een beter pad heeft van de NET207 interface en een overschakeling start. Het verzendt een PIM Join bericht naar het stroomopwaartse apparaat (FTD).
11. De laatste-hop router stuurt een PIM Prune bericht naar de RP.
12. De FTD verstuurt de multicast stream naar de NET207-interface. De ASA beweegt zich van de gedeelde boom (RP-boom) naar de bronboom (SPT).

Taak 2 - Configureer PIM bootstrap router (BSR)

BSR-basiskennis

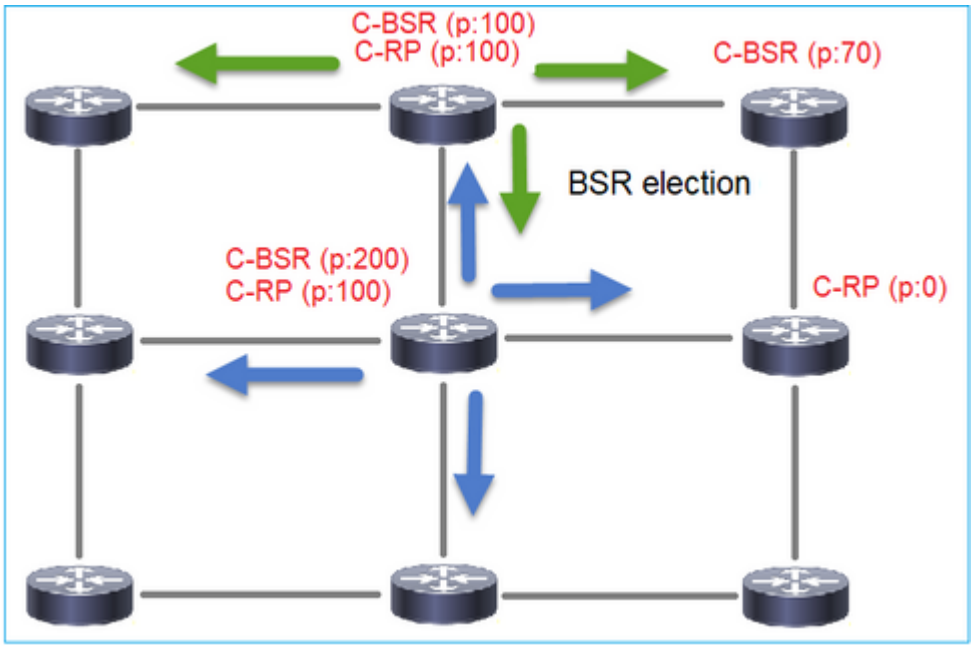
- BSR (RFC 5059) is een control-plane multicast-mechanisme dat het PIM-protocol gebruikt en apparaten in staat stelt de RP-informatie dynamisch te leren.
- BSR-definities:
  - Kandidaat RP (C-RP): Een apparaat dat een RP wil zijn.
  - Kandidaat-BSR (C-BSR): Een apparaat dat een BSR wil zijn en RP-sets adverteert naar andere apparaten.
  - BSR: Een apparaat dat wordt gekozen als BSR tussen veel C-BSR's. De **hoogste BSR-prioriteit wint** de verkiezingen.
  - RP-set: een lijst van alle C-RP's en hun prioriteiten.
  - RP: Het apparaat met de **laagste RP-prioriteit wint** de verkiezing.

- BSR PIM bericht (leeg): Een PIM bericht gebruikt in de BSR verkiezing.
- BSR PIM bericht (normaal): Een PIM bericht verzonden naar 224.0.0.13 IP en bevat een RP-set en BSR info.

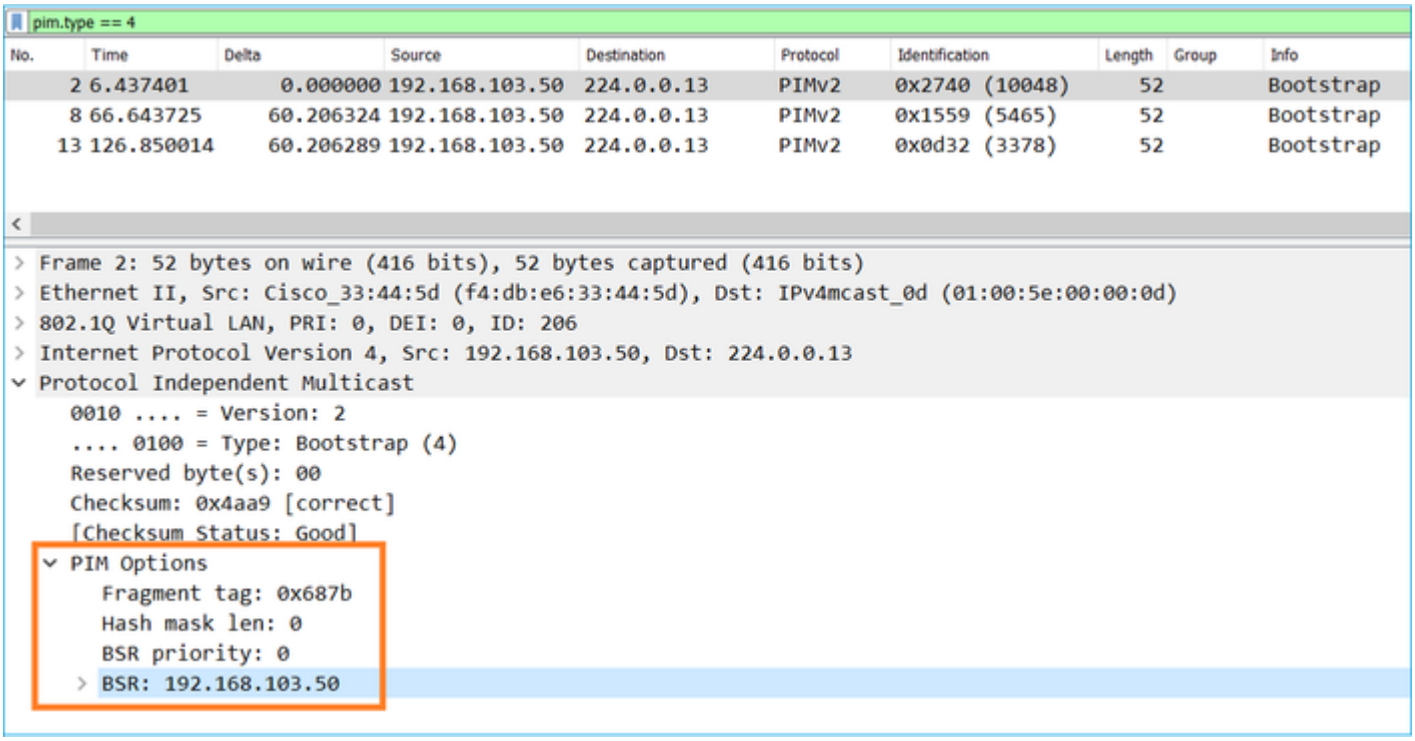
Hoe BSR werkt

1. BSR-verkiezingsmechanisme.

Elke C-BSR verstuurt lege PIM BSR berichten die een prioriteit bevatten. Het apparaat met de hoogste prioriteit (de reserve is de hoogste IP) wint de verkiezing en wordt BSR. De rest van de apparaten verstuurt geen lege BSR-berichten meer.

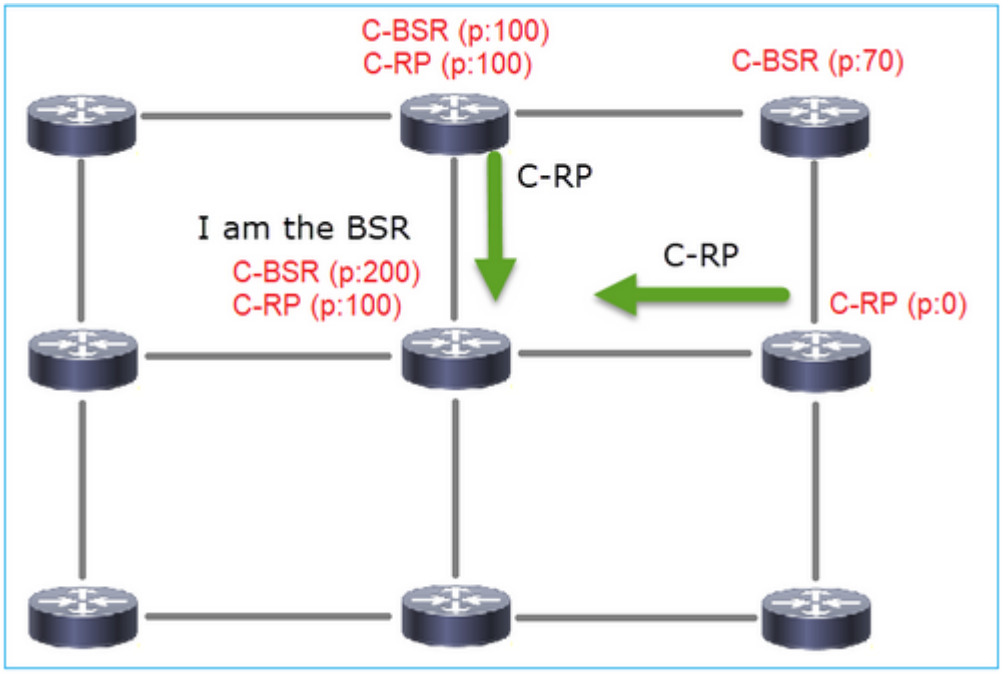


Een BSR-bericht dat in het verkiezingsproces wordt gebruikt, bevat alleen C-BSR-prioriteitsinformatie:

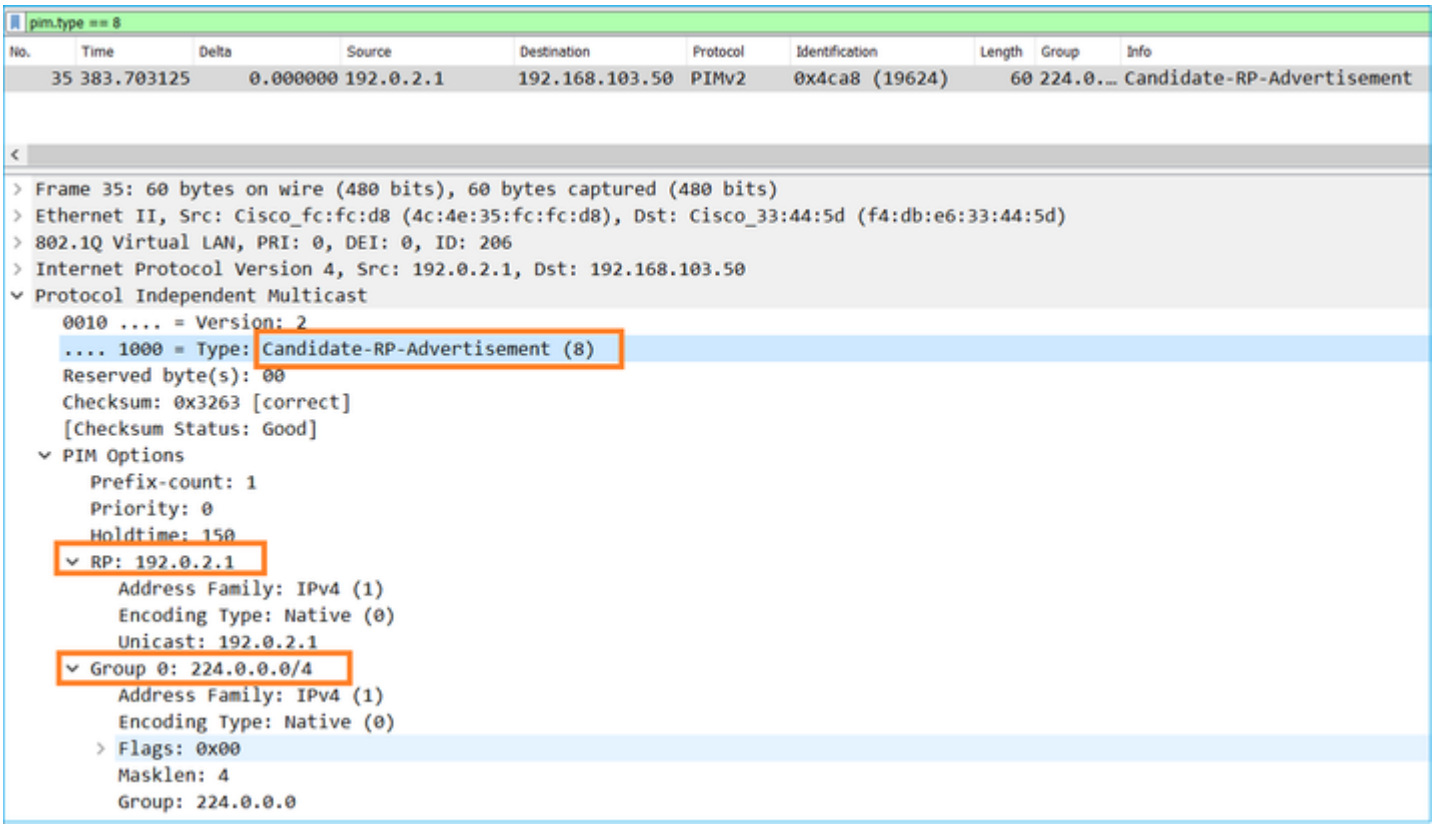


Om BSR-berichten in Wireshark weer te geven, gebruikt u dit weergavefilter: pim.type == 4

2. De C-RPâ€™s sturen **unicast** BSR-berichten naar de BSR die hun C-RP-prioriteit bevatten:

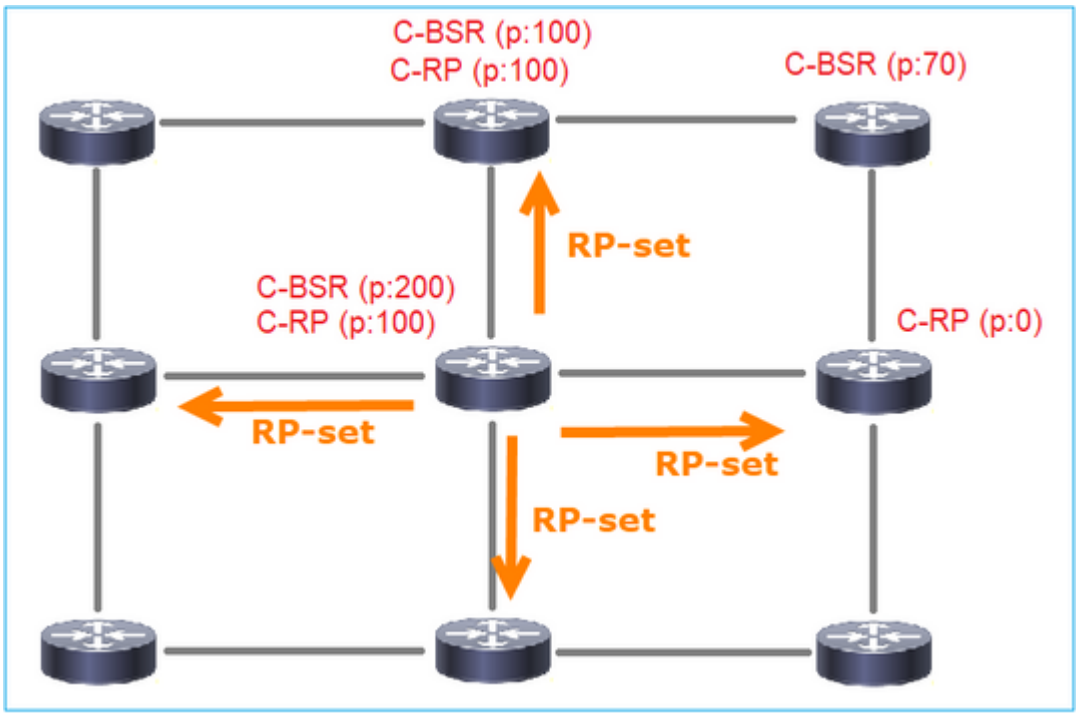


Een kandidaat-RP-bericht:



Om BSR-berichten in Wireshark weer te geven, gebruikt u dit weergavefilter: pim.type == 8

3. De BSR stelt de RP-set samen en adverteert deze naar alle PIM-buren:

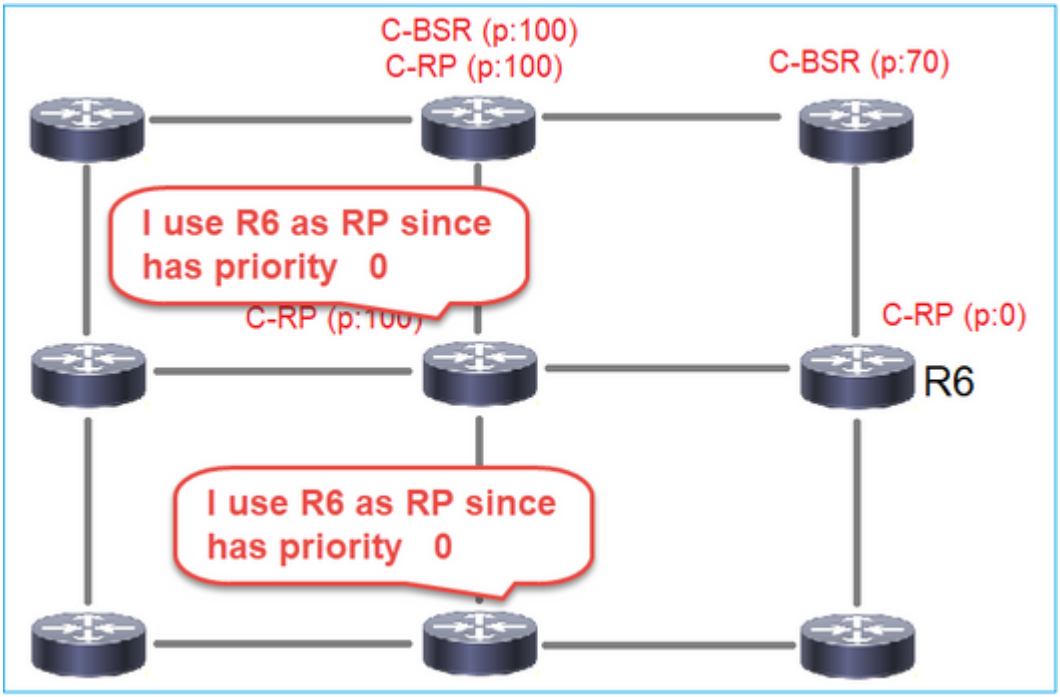


(ip.src == 192.168.105.60) && (pim.type == 4)

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

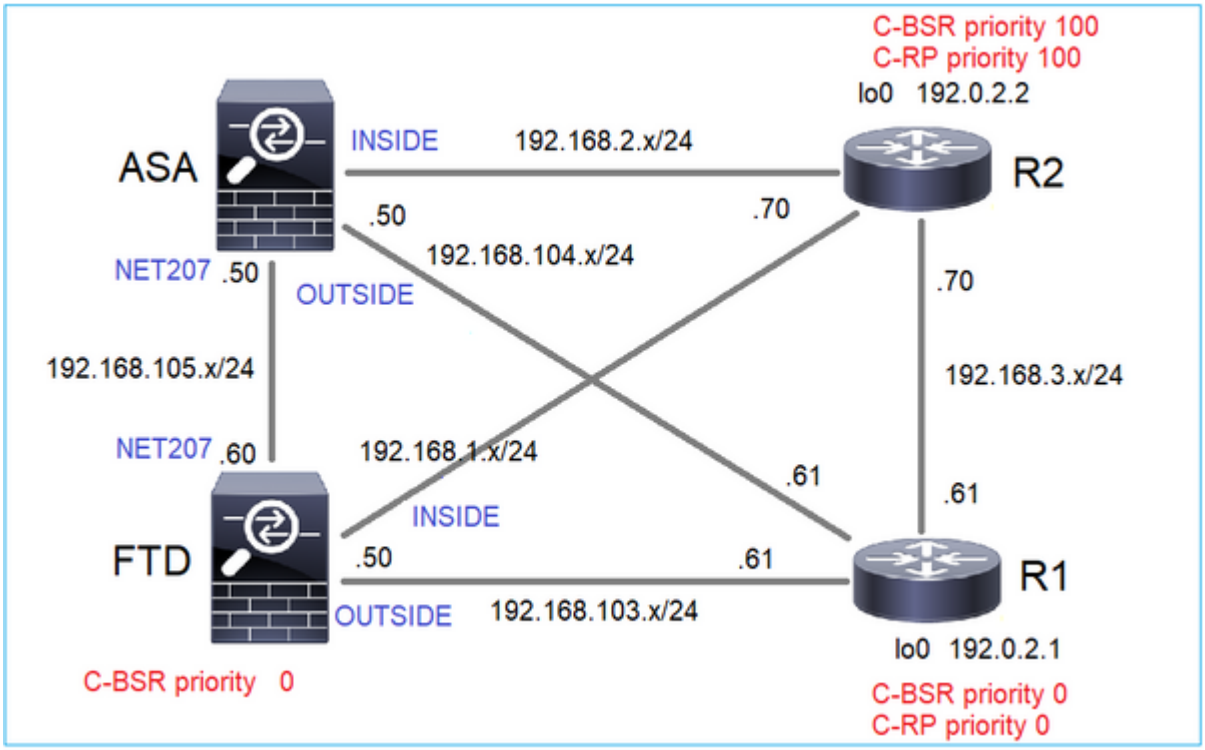
```
> Frame 152: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
> Ethernet II, Src: Cisco_33:44:5d (f4:db:e6:33:44:5d), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
> 802.1Q Virtual LAN, PRI: 6, DEI: 0, ID: 207
> Internet Protocol Version 4, Src: 192.168.105.60, Dst: 224.0.0.13
v Protocol Independent 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. De routers/firewalls krijgen de RP-set en kiezen de RP op basis van de laagste prioriteit:



Taakvereiste

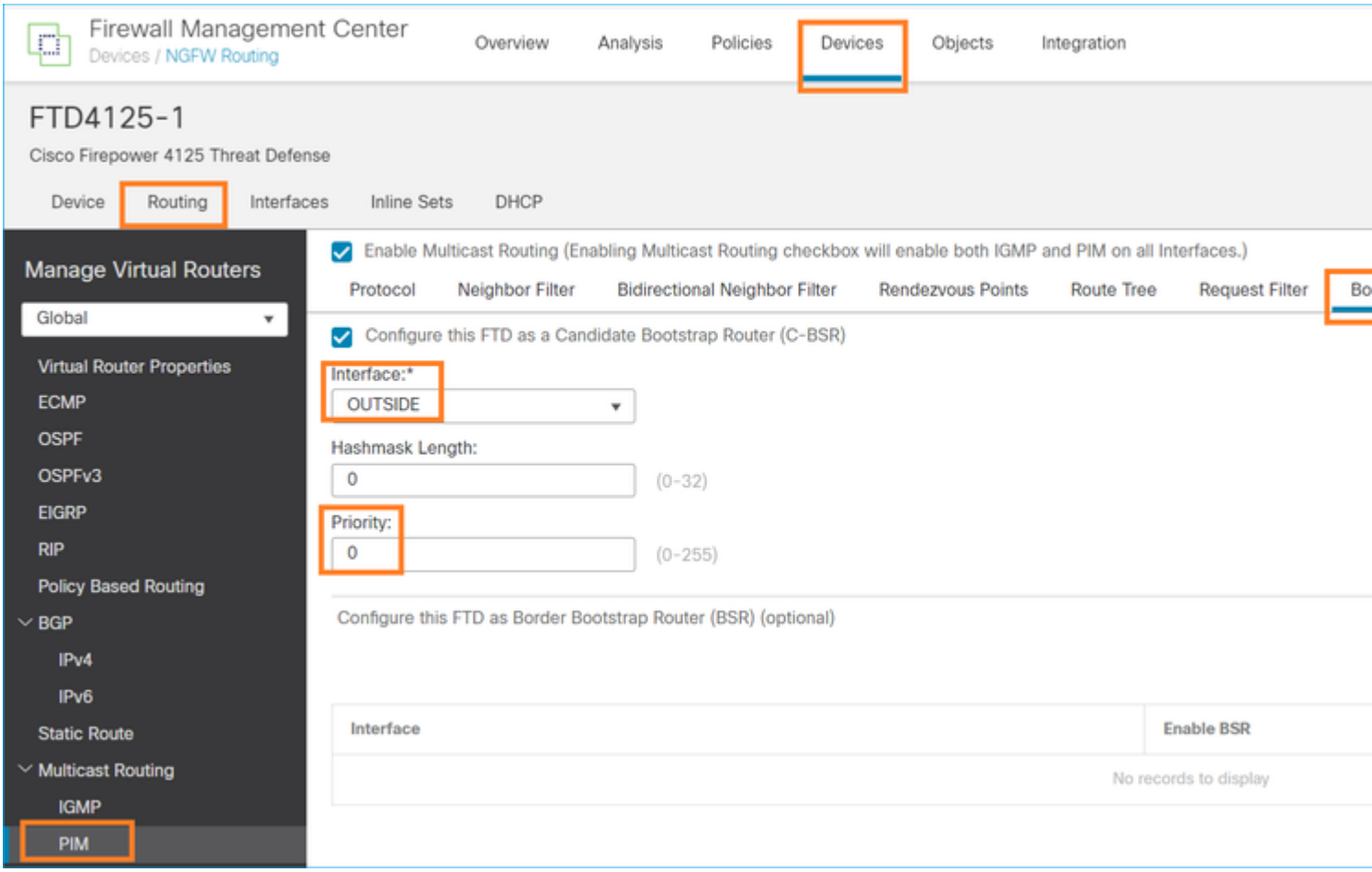
Configureer de C-BSRâ€™s en C-RPâ€™s volgens deze topologie:



Voor deze taak moet de FTD zichzelf aankondigen als C-BSR op de buiteninterface met BSR-prioriteit 0.

Oplossing

FMC-configuratie voor FTD:



De geïmplementeerde configuratie:

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

Configuratie op de andere apparaten:

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)
```

Hetzelfde voor R2, maar met verschillende C-BSR en C-RP prioriteiten

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

Op ASA is er wereldwijd slechts multicast ingeschakeld. Dit laat PIM op alle interfaces toe:

```
multicast-routing
```

Verificatie

R2 is de gekozen BSR vanwege de hoogste prioriteit:

```
<#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 wordt gekozen als RP vanwege de laagste prioriteit:

```
<#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
```

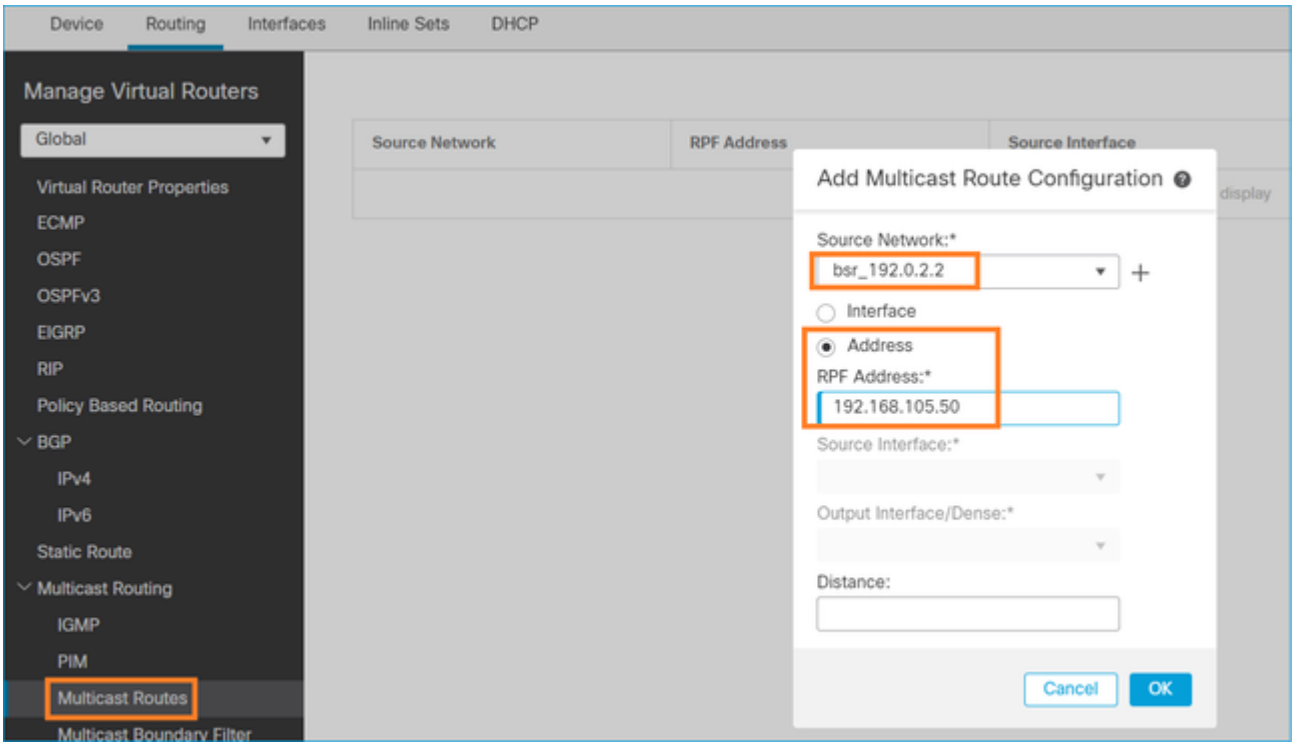
```
224.0.0.0/4

*

       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
```

De BSR-berichten **worden gecontroleerd**. U kunt **debug pim bsr** inschakelen om dit te verifiëren:

<#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
```

Als u de RPF-interface wilt wijzigen, kunt u een statische route configureren. In dit voorbeeld accepteert de firewall BSR-berichten van 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

Nu worden BSR-berichten op de NET207-interface geaccepteerd, maar op INSIDE worden verwijderd:

<#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

Schakel opname met overtrekken op de firewall in en controleer hoe de BSR-berichten worden verwerkt:

<#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
```

De PIM-verbindingen worden op de firewall beëindigd, zodat de overtrek nuttige informatie kan tonen als de verbindingen met de box moeten worden gewist:

<#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
```

Als het PIM-pakket vanwege een RPF-fout wordt gedropt, ziet u het volgende:

<#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

De ASP-tabel laat vallen en vangt met RPF-mislukte pakketten:

<#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

Om pakketten op te nemen die vanwege een RPF-fout zijn gevallen:

<#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
```

Methodologie voor probleemoplossing

De methodologie voor probleemoplossing voor de firewall is voornamelijk afhankelijk van de rol van de firewall in de multicast topologie. Dit is de lijst met aanbevolen stappen voor probleemoplossing:

1. Verklaar de details van probleembeschrijving en symptomen. Probeer het bereik te beperken tot de problemen met **het besturingsplane (IGMP/PIM)** of het **dataplane (multicast-stream)**.
2. De verplichte voorwaarde voor probleemoplossing bij multicast-problemen op de firewall is dat de multicast-topologie wordt verduidelijkt. U moet minimaal het volgende identificeren:
    - rol van de firewall in de multicast topologie - FHR, LHR, RP of een andere intermediaire rol.
    - verwachte multicast in- en uitgangen op de firewall.
    - RP
    - IP-adressen van afzenderbron.
    - multicast-groepen IP-adressen en doelpoorten.
    - ontvangers van de multicast-stroom.

3. Identificeer het type multicast routing **- Stub** of **PIM multicast routing:**

- **Stub multicast routing -** deze biedt dynamische hostregistratie en vergemakkelijkt multicast routing. Wanneer geconfigureerd voor stub multicast routing, fungeert de ASA als IGMP proxy-agent. In plaats van volledig deel te nemen aan multicast routing, stuurt de ASA IGMP-berichten door naar een upstream multicast router, die de levering van de multicast gegevens instelt. Om de stub mode routing te identificeren, gebruik de **show igmp interface** commando en controleer IGMP voorwaartse configuratie:

<#root>

```
firepower#
```

```
show igmp interface
```

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

```
IGMP forwarding on interface inside
```

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

PIM is ingeschakeld op de interfaces; buren zijn echter niet tot stand gebracht:

<#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.
```

Doorsturen van PIM-SM/Bidir en IGMP worden **niet** tegelijkertijd ondersteund.

U kunt geen opties zoals het RP-adres configureren:

<#root>

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

- **PIM multicast routing - De PIM multicast routing is de meest gebruikelijke implementatie.** De firewall ondersteunt zowel PIM-SM als bidirectionele PIM. PIM-SM is een multicast routeringsprotocol dat de onderliggende unicast routinginformatiebasis of een afzonderlijke multicast-geschikte routinginformatiebasis gebruikt. Het bouwt eenrichtings gedeelde boom die bij één enkel rendez-vous punt (RP) per multicast groep wordt geworteld en leidt naar keuze tot kort-weg bomen per multicast bron. In deze implementatiemodus, in tegenstelling tot de stub-modus, configureren de gebruikers meestal de RP-adresconfiguratie en de firewall zorgt ervoor dat er een PIM-nabijheid is met de peers:

<#root>

```
firepower#

show run pim


pim rp-address 10.10.10.1

firepower#

show pim group-map


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

224.0.0.0/4*        SM      config   1      10.10.10.1     RPF: inside,192.168.2.1 <--- RP address is 10


224.0.0.0/4         SM      static   0      0.0.0.0         RPF: ,0.0.0.0

firepower#
```

show pim neighbor

```
Neighbor Address  Interface          Uptime    Expires DR pri Bidir
192.168.2.1       inside             00:02:52  00:01:19 1
192.168.3.100     outside            00:03:03  00:01:39 1 (DR)
```

4. Controleer RP IP-adres is ingesteld en bereikbaarheid:

<#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
```

Waarschuwing: de firewall kan niet tegelijkertijd een **RP** en een **FHR zijn**.

---

5. Controleer extra uitgangen afhankelijk van de rol van de firewall in de multicast topologie en de probleemsymptomen.

FHR

- Controleer de status **van de** interface **Tunnel0**. Deze interface wordt gebruikt om rauw multicast verkeer in te kapselen binnen de payload van PIM en unicast-pakket naar RP te verzenden voor met PIM-register bitset:

<#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
```

- Controleer de routes:

<#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.
```

Wanneer de firewall een PIM-pakket ontvangt met het Register-Stop-bit, wordt Tunnel0 uit de OIL verwijderd. De firewall stopt vervolgens de insluiting en verstuurt rauw multicast-verkeer via de uitgangsinterface:

<#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
```

- Controleer de tellers van het PIM-register:

<#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
```

- Controleer unicast PIM-pakketopname tussen de firewall en de 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
```

- Verzamel extra uitgangen (x.x.x.x is de multicastgroep, y.y.y is de RP IP). Aanbevolen wordt de output **enkele malen** te verzamelen:

<#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
```

- Verzamel onbewerkte multicast interfacepakket en ASP-drop-opnamen.

<#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-berichten - veelvoorkomende ID's zijn 302015, 302016 en 710005.

RP

- Controleer de status van de interface Tunnel0. Deze interface wordt gebruikt om rauw multicast verkeer in te kapselen binnen de payload van PIM en om unicast-pakket naar FHR te verzenden voor met PIM-stop-bitset:

<#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        -
```

- Controleer de routes:

<#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
```

- Controleer PIM-tellers:

<#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
```

- Verzamel extra uitgangen (x.x.x.x is de multicastgroep, y.y.y is de RP IP). Aanbevolen wordt de output **enkele malen** te verzamelen:

<#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
```

- Verzamel onbewerkte multicast interfacepakket en ASP-drop-opnamen:

<#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 - de gemeenschappelijke IDs zijn 302015, 302016 en 710005.

LHR

Neem de in het hoofdstuk over het herstructureringsplan genoemde stappen en deze aanvullende controles:

- routes:

<#root>

```
firepower#
show mroute

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

(*, 230.1.1.1), 00:23:30/never, RP 10.10.10.1, flags: SCJ <--- C flag means connected receiver

  Incoming interface:
inside

  RPF nbr: 192.168.2.1
  Immediate Outgoing interface list:

outside
, Forward, 00:23:30/never

(192.168.1.100, 230.1.1.1), 00:00:36/00:03:04, flags: SJT <--- J flag indicates switchover to SPT, T fla

  Incoming interface:
inside

  RPF nbr: 192.168.2.1
  Inherited Outgoing interface list:

outside
, Forward, 00:23:30/never

(*, 230.1.1.2), 00:01:50/never, RP 10.10.10.1, flags: SCJ <--- C flag means connected receiver

  Incoming interface:
inside

  RPF nbr: 192.168.2.1
  Immediate Outgoing interface list:

outside
, Forward, 00:01:50/never

(192.168.1.100, 230.1.1.2), 00:00:10/00:03:29, flags: SJT <--- <--- J flag indicates switchover to SPT,
```

```
  Incoming interface:
```

inside

```
  RPF nbr: 192.168.2.1
  Inherited Outgoing interface list:
```

outside

```
, Forward, 00:01:50/never
```

- IGMP-groepen:

<#root>

```
firepower#
```

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

```
Interface:      outside
```

Group: 230.1.1.1

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

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

```
Source list is empty
Interface:      outside
```

Group: 230.1.1.2

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

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

```
Source list is empty
```

- IGMP-verkeersstatistieken:

<#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
```

Opdrachten voor PIM-probleemoplossing (cheatsheet)

Opdracht	**Beschrijving**
toon in werking stelt-Config multicast-routing	Om te zien of multicast routing is ingeschakeld op de firewall
show run mroute	Om de statische routes te zien die op de firewall zijn geconfigureerd
toon in werking stelt -in werking stellen-Config	De PIM-configuratie op de firewall bekijken
PIM-interface tonen	Om te zien welke firewallinterfaces PIM en de buren PIM hebben toegelaten.
naburig wezen tonen	De PIM-buren bekijken
pim group-map weergeven	Om de multicastgroepen te zien die aan de RP zijn toegewezen
toon route	Om de volledige multicast routeringstabel te zien
toon 230.10.10.10	De multicast tabel bekijken voor een specifieke multicast groep
Toon pittunnel	Om te zien of er een PIM-tunnel is gebouwd tussen de firewall en

	de RP
toon conn alle details adres RP_IP_ADDRESS	Om te zien of er een verbinding (PIM-tunnel) tot stand is gebracht tussen de firewall en de RP
Toon PIM topologie	De output van de firewall PIM-topologie bekijken
debugpomp	Dit debug toont alle PIM-berichten van en naar de firewall
debug pim groep 230.10.10.10	Dit debug toont alle PIM-berichten van en naar de firewall voor de specifieke multicast groep
verkeer weergeven	Om statistieken over ontvangen en verzonden PIM-berichten te zien
IP-clusterteller tonen	Het aantal pakketten dat in het langzame pad versus het snelle pad versus het controlepunt wordt verwerkt, verifiëren
druppel tonen	Om alle softwareniveaudalingen op de firewall te zien
Capture CAP interface INSIDE trace match pim elke willekeurige	Om toegang PIM multicast-pakketten op de firewall vast te leggen en te traceren
Capture CAP-interface INSIDE-sporenmatch udp-host 24.1.2.3 willekeurige	Om de toegangsmulticast-stroom op te nemen en te traceren
bsr-router tonen	Om te verifiëren wie de geselecteerde BSR-router is
toon conn alle adres 224.1.2.3	De parent-multicast-verbinding tonen
toon local-host 24.1.2.3	De kind/stub multicast-verbindingen tonen

Voor meer informatie over firewall-opnamecontrole: Werken met Firepower Threat Defense Captures en Packet Tracer

Bekende problemen

Firepower multicast beperkingen:

- Ondersteunt IPv6 niet.
- PIM/IGMP-multicast wordt niet ondersteund op interfaces in een verkeerszone (EMCP).
- De firewall kan niet tegelijkertijd een RP en een FHR zijn.
- De **show conn al** bevel toont slechts de identiteit multicast verbindingen. Om de stub/de secundaire multicast verbinding te tonen, gebruik de **show local-host <*group IP*>** opdracht.

PIM wordt niet ondersteund op een vPC Nexus

Als u probeert een PIM-nabijheid tussen een Nexus vPC en de firewall te implementeren, geldt er een Nexus-beperking zoals hier wordt beschreven:

Ondersteunde technologieën voor routing via Virtual Port Channel op Nexus-platforms

Vanuit het NGFW-standpunt ziet u deze druppel in Opname met spoor:

<#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

De firewall kan de registratie van de referentieprijs niet voltooien:

<#root>

```
firepower#
```

show mroute 224.1.2.3

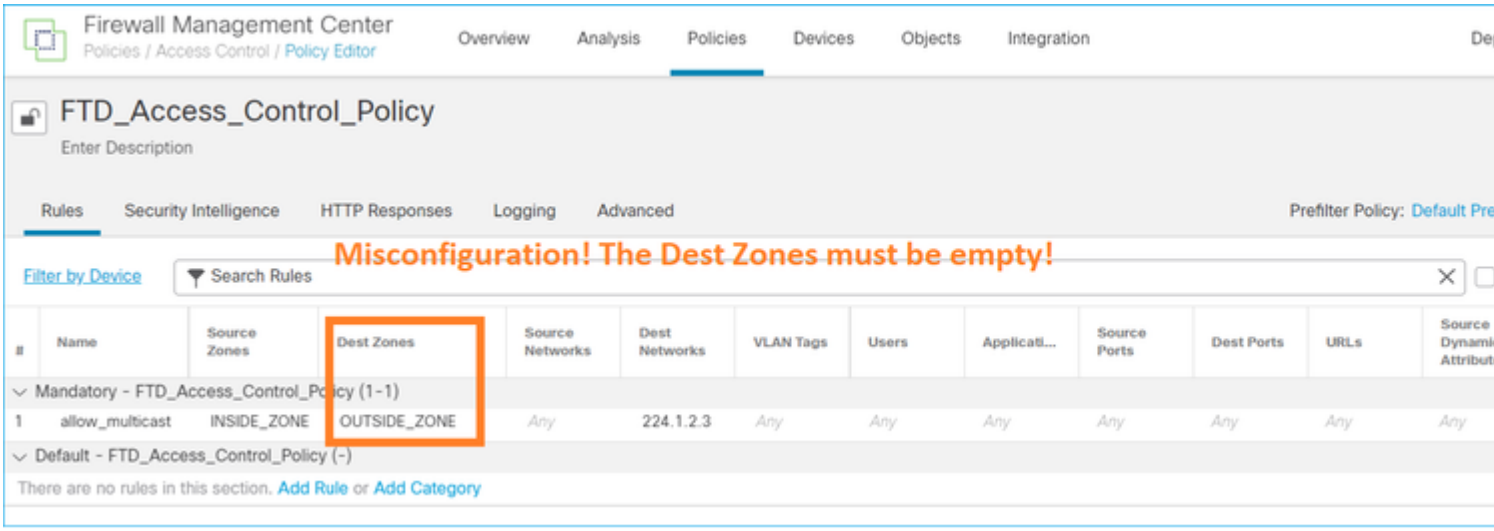
```
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface,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

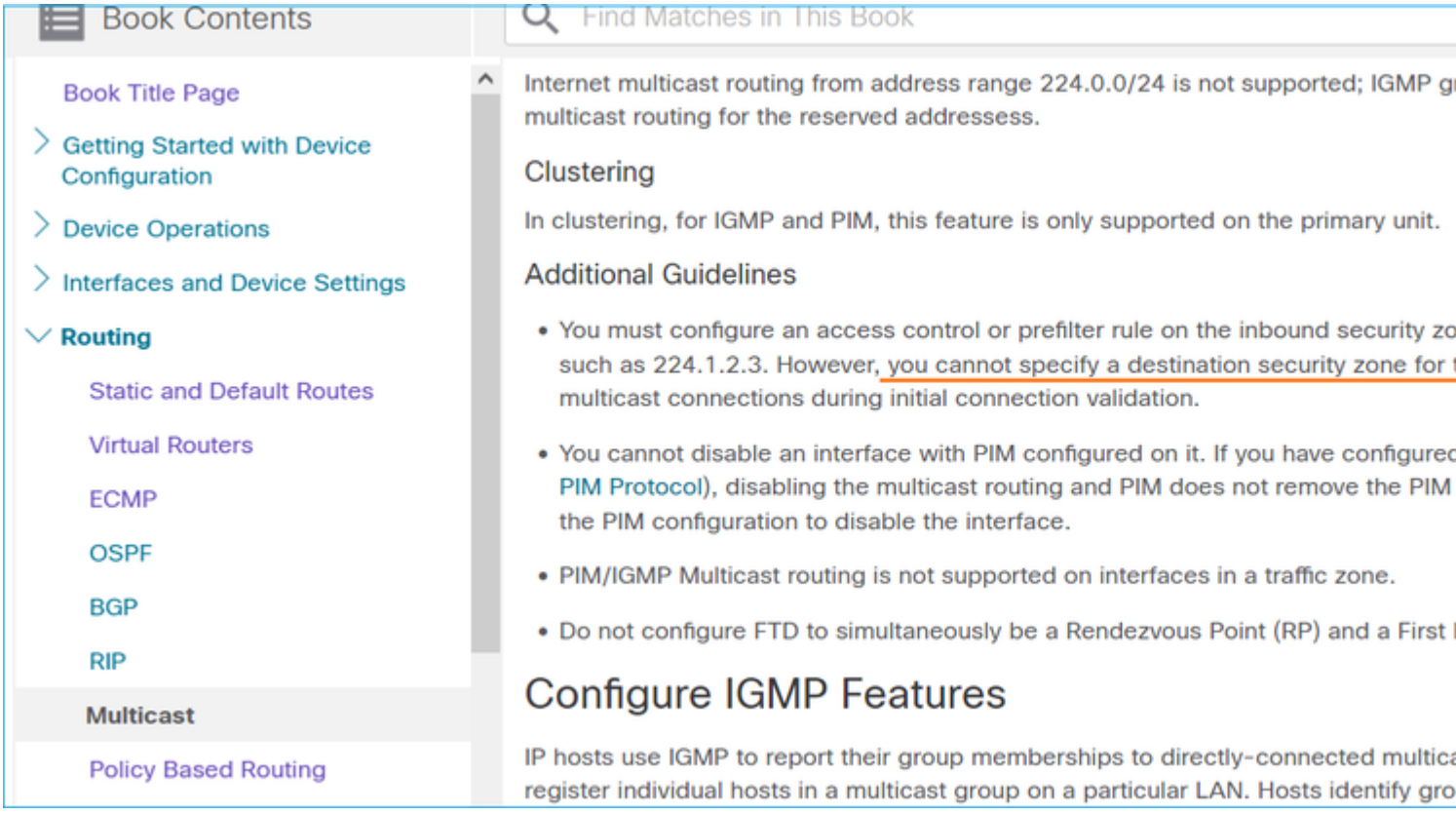
```
Immediate Outgoing interface list:
  Tunnel0, Forward, 00:39:15/never
```

Doelgebieden worden niet ondersteund

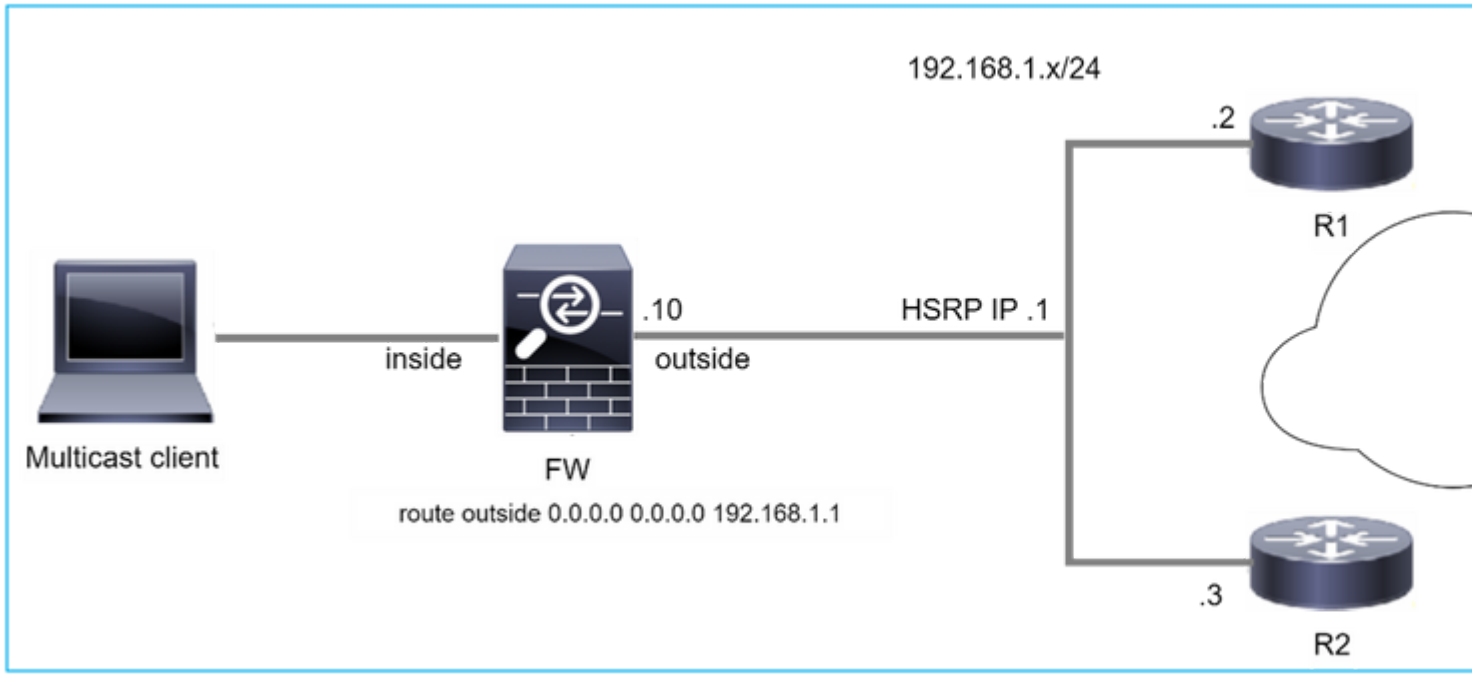
U kunt geen doelbeveiligingszone opgeven voor de regel Toegangsbeheer die overeenkomt met multicastverkeer:



Dit wordt ook gedocumenteerd in de FMC-gebruikershandleiding:



Firewall stuurt geen PIM-berichten naar upstream-routers vanwege HSRP



In dit geval heeft de firewall een standaardroute via het Hot Standby Redundancy Protocol (HSRP), IP-telefoon 192.168.1.1 en PIM-nabuurschap met routers R1 en R2:

```
<#root>

firepower#

show run route

route outside 0.0.0.0 0.0.0.0 192.168.1.1 1
```

De firewall heeft nabijheid PIM tussen de buitenkant en de fysieke interface IP op R1 en 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)
```

De firewall verzendt geen PIM Join-bericht naar een upstream-netwerk. De PIM debug opdracht **debug pim** toont deze output:

```
<#root>

firepower#

debug pim
```

```
...

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

RFC 2362 verklaart dat *"een router een periodiek Join/Prune bericht naar elke verschillende RPF buur verbonden aan elke (S,G), (*,G) en (*,*,RP) ingang verzendt. Berichten worden alleen verstuurd als de RPF-buur een PIM-buur is."*

Om het probleem te verlichten, kan de gebruiker een statische routeingang op de firewall toevoegen. De router moet verwijzen naar een van de twee IP-adressen van de routerinterface, 192.168.1.2 of 192.168.1.3, doorgaans de actieve HSRP-router IP.

Voorbeeld:

<#root>

```
firepower#
```

show run mroute

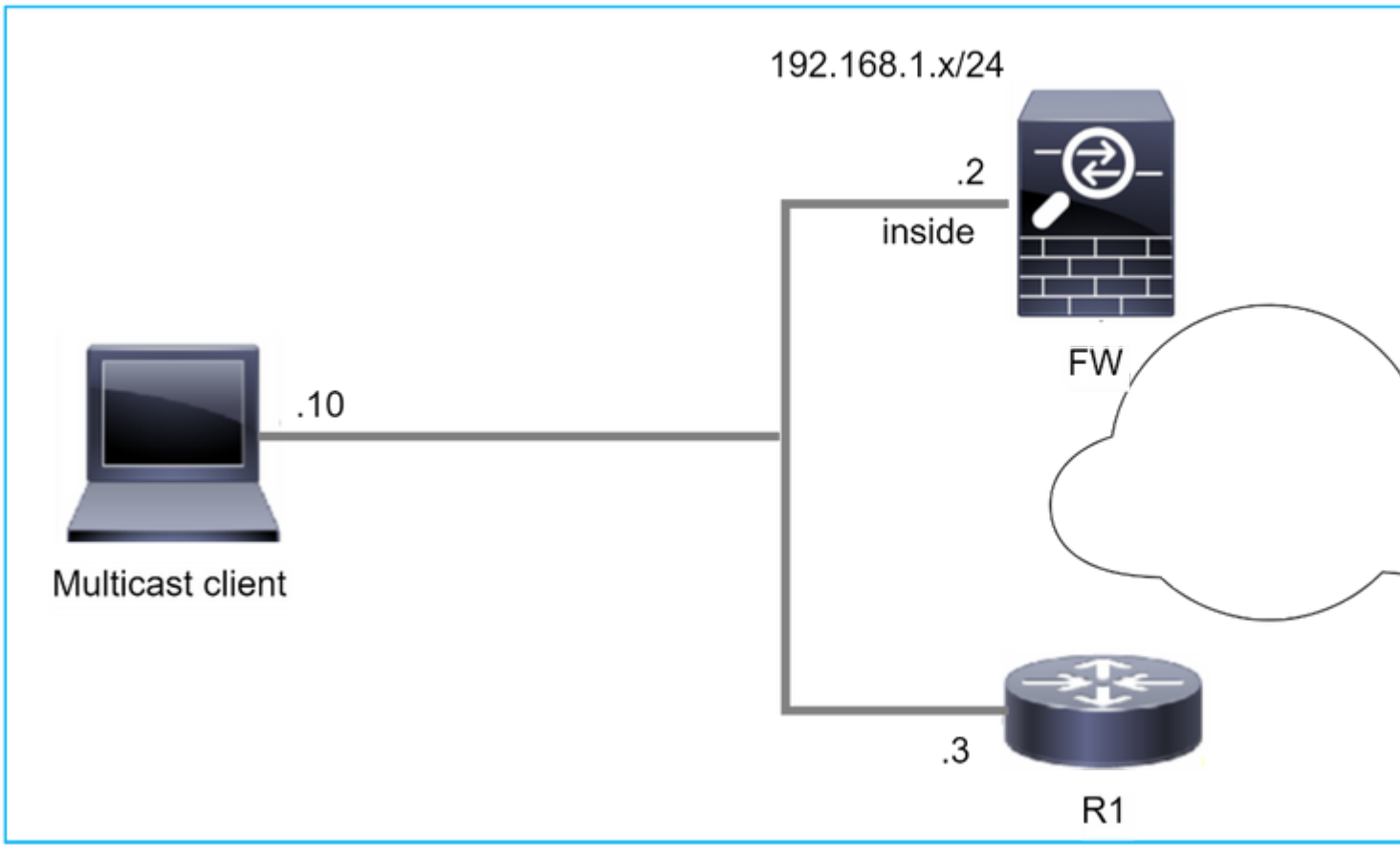
```
firepower#
```

mroute 172.16.1.1 255.255.255.255 192.168.1.2

Zodra de statische routeconfiguratie, voor de RPF-raadpleging, is geïnstalleerd, geeft de firewall voorkeur aan de multicast routeringstabel in plaats van de unicast-routeringstabel van de ASA en verstuurt de PIM-berichten rechtstreeks naar buur 192.168.1.2.

> **Opmerking:** de statische route is op sommige punten uitgebreid verslaat de bruikbaarheid van HSRP-redundantie, omdat de route slechts 1 volgende-hop per adres/netmasker combinatie accepteert. Als de volgende hop die in het routebevel wordt gespecificeerd ontbreekt of onbereikbaar wordt, valt de firewall niet terug naar de andere router.

De firewall wordt niet als LHR beschouwd wanneer deze niet de methode voor noodherstel in het LAN-segment is



De firewall heeft R1 als PIM-buren in het LAN-segment. R1 = 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)
```

Als IGMP zich aansluit bij een verzoek van de client wordt ontvangen, wordt de firewall niet de LHR.

De route toont extra **leeg** als de OLIE en heeft de **gesnoeide** vlag:

```
<#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

Om van de firewall de LHR te maken, kan de interface DR prioriteit worden verhoogd.

<#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

De PIM debug opdracht **debug pim** toont deze 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
```

De gesnoeide vlag en de Null worden verwijderd van de route:

<#root>

firepower#

show mroute

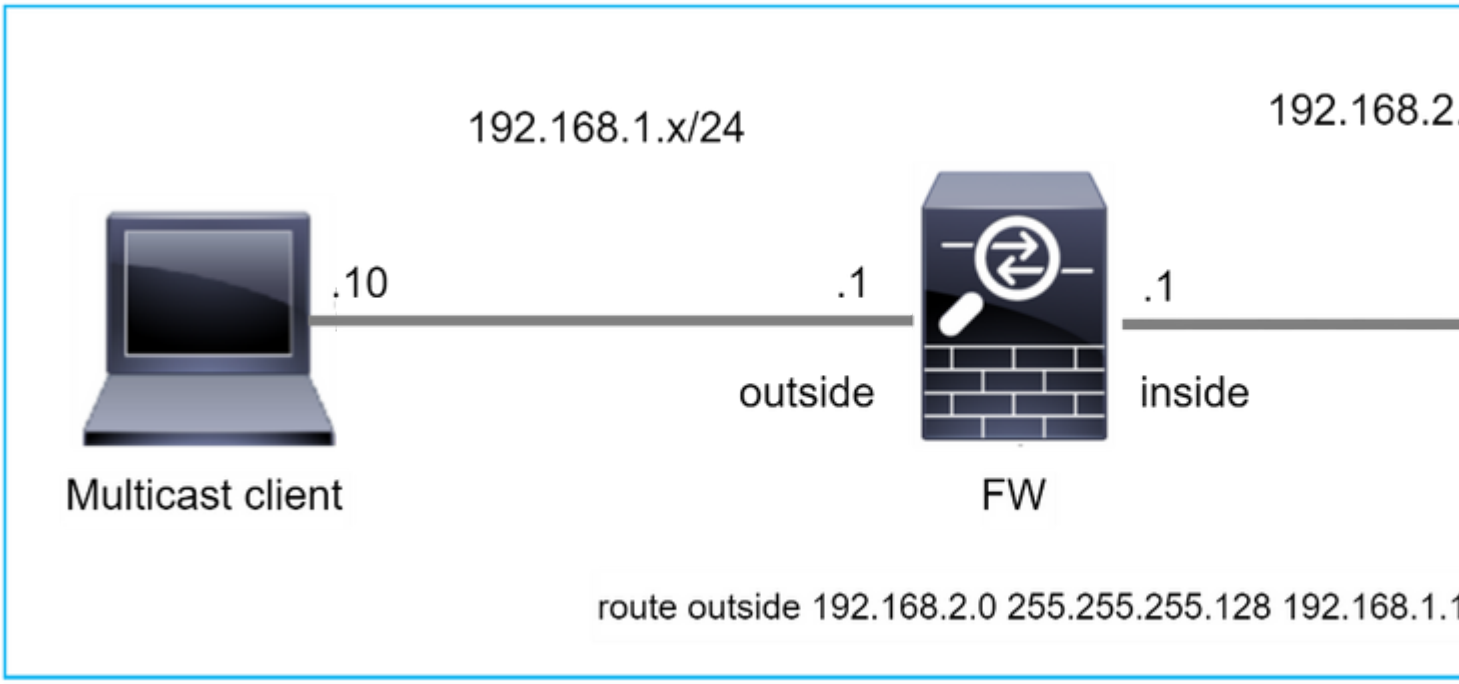
```
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface,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

Firewall Drops Multicast Packets vanwege het doorsturen van pad naar omgekeerd pad Controleer de fout



In dit geval worden de multicast UDP-pakketten verloren als gevolg van RPF-fout, omdat de firewall een specifiekere route heeft met het masker 255.255.255.128 via de buiteninterface.

<#root>

```
firepower#
```

capture capi type raw-data trace interface inside match udp any any

```
firepower#
```

show captureture capi packet-number 1 trace

```
106 packets captured
   1: 08:57:18.867234       192.168.2.2.12345 > 230.1.1.1.12354:  udp 500
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 2684 ns
Config:
Additional Information:
MAC Access list


Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 2684 ns
Config:
Implicit Rule
Additional Information:
MAC Access list
```

```
Phase: 3
Type: INPUT-ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Elapsed time: 13664 ns
Config:
Additional Information:
Found next-hop 192.168.1.100 using egress ifc  outside

Phase: 4
Type: INPUT-ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Elapsed time: 8296 ns
Config:
Additional Information:
Found next-hop 192.168.1.100 using egress ifc  outside

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: drop
Time Taken: 27328 ns


Drop-reason: (rpf-violated) Reverse-path verify failed, Drop-location: frame 0x0000556bcb1069dd flow

(NA)/NA

firepower#
```

show route static

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is not set
```

S   192.168.2.0 255.255.255.128 [1/0] via 192.168.1.100, outside

ASP drop Captures tonen de **rpf-geschonden** drop reden:

```
<#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
```

De RPF-mislukte tellers in de MFIB-uitvoerverhogingen:

<#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
```

De oplossing is om de RPF controle fout te herstellen. Eén optie is het verwijderen van de statische route.

Als er geen RPF-controlefout meer is, worden de pakketten doorgestuurd en wordt de **Forwarding**-teller in de MFIB-uitvoer verhoogd:

<#root>

```
firepower#
```

show mfib 230.1.1.1 count

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

Source: 192.168.2.2,

Forwarding: 1033/9/528/39

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

show mfib 230.1.1.1 count

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

Source: 192.168.2.2,

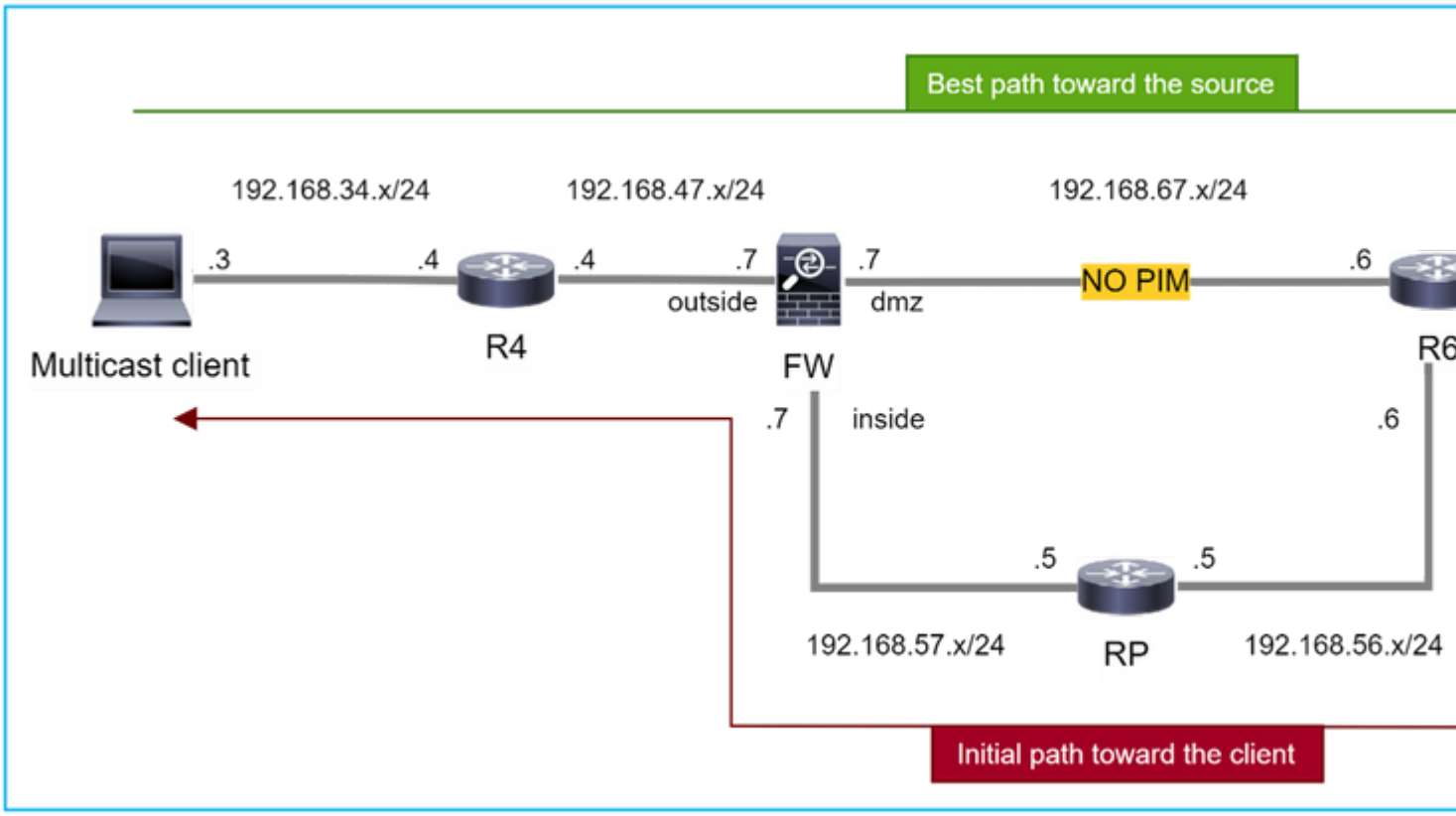
Forwarding: 1044/10/528/41

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

<--- Forward counter increased

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

Firewall genereert geen PIM-koppeling na PIM-switching naar bronstructuur



In dit geval leert de firewall het pad naar de multicastbron via de **dmz**-interface **R4** > **FW** > **R6**, terwijl het oorspronkelijke verkeerspad van de bron naar de client **R6** > **RP** > **DW** > **R4** is**:**

<#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 initieert SPT switchover en verstuurt een bronspecifieke PIM-vervoegingsbericht zodra de SPT-switchover-drempel is bereikt. In de firewall vindt de NBP-overschakeling niet plaats, de (S,G) route heeft niet de **T**-vlag:

<#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
```

De PIM debug opdracht **debug pim** toont 2 ontvangen PIM Join request van de peer R4 - voor **(*,G) en (S,G).** De firewall stuurde PIM Join request for (*,G) upstream, en slaagde er niet in een bronspecifieke aanvraag te verzenden vanwege een ongeldige buurman 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

In de **show pim neigbour** commando's output ontbreekt R6:

<#root>

firepower#

show pim neighbor

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

PIM is ingeschakeld op de firewall-interface dmz:

<#root>

firepower#

show pim interface

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

192.168.47.7     outside            on   1     30     1          this system

192.168.67.7     dmz                on   0     30     1          this system


192.168.57.7     inside             on   1     30     1          this system
```

PIM is uitgeschakeld in de R6-interface:

<#root>

```
R6#

show ip interface brief


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

GigabitEthernet0/3         192.168.67.6    YES manual up                    up


Tunnel0                    192.168.56.6    YES unset  up                    up

R6#

show ip pim interface GigabitEthernet0/3 detail


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


PIM: disabled <--- PIM is disabled


  Multicast Tagswitching: disabled
```

De oplossing is om PIM op interface Gigabit Ethernet0/3 op R6 in te schakelen:

<#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**

De firewall installeert de T-vlag, die aangeeft dat de overschakeling naar NBP plaatsvindt**:**

<#root>

```
firepower#
```

show mroute

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

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

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

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

Firewall Drops Eerste paar pakketten vanwege punt rate Limit

Wanneer de firewall de eerste pakketten van een **nieuwe** multicast stroom in FP ontvangt, kan extra verwerking door de CP worden vereist. In dit geval, de FP punts de pakketten aan de CP via SP (FP > SP > CP) voor extra verrichtingen:

- Creatie van een **ouder** verbinding in FP tussen de ingangsinterfaces en de identiteits interfaces.
- Aanvullende multicast-specifieke controles, zoals de RPF-validatie, PIM-insluiting (als de firewall de FHR is), Oil-controle, enzovoort.
- Creatie van een (S, G) ingang met de inkomende en uitgaande interfaces in de routetabel.
- Creatie van een **kind/stub-**verbinding in FP tussen de inkomende en uitgaande interfaces.

Als deel van de bescherming van het controlevliegtuig, beperkt de firewall intern het tarief van pakket dat aan CP wordt gestraft.

De pakketten die de snelheid overschrijden worden in het veld gedropt met de reden voor **puntkoers-limiet** val:

<#root>

firepower#

show asp drop

Frame drop:

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

Gebruik de opdracht **show asp cluster teller** om het aantal multicast pakketten te verifiëren dat vanuit SP aan CP wordt doorgestuurd:

<#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
```

Gebruik **tonen asp event dp-cp punt** commando om het aantal pakketten in de FP > CP wachtrij te verifiëren, en de 15-seconden tarief:

<#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
```

Wanneer de route wordt bevolkt en de ouder/kind verbindingen in FP worden gevestigd, door:sturen de pakketten in FP als deel van de bestaande verbindingen. In dit geval geeft FP de pakketten niet af aan de CP.

Hoe de firewall de eerste pakketten van een nieuwe multicast stream verwerkt?

Wanneer de firewall de eerste pakketten van een **nieuwe** multicast stroom in datapath ontvangt, onderneemt de firewall deze acties:

1. Controleert als het veiligheidsbeleid pakketten toestaat.
2. Punts de pakketten aan CP via weg FP.
3. Maakt een **parent**-verbinding tussen de ingangsinterfaces en de identiteitsinterfaces:

<#root>

```
firepower#
```

show capture capi packet-number 1 trace

```
10 packets captured
```

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

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

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

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


Phase: 4
Type: ACCESS-LIST
```

Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:

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

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

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

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

Phase: 9

Type: MULTICAST

Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 10

Type: FLOW-CREATION

Subtype:
Result: ALLOW
Config:
Additional Information:

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

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

```
output-status: up
output-line-status: up
```

Action: allow

Syslogs:

<#root>

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

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

Deze verbinding is zichtbaar in de output van de **show conn all** commando:

<#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. De CP voert het multicastproces uit voor extra multicast-specifieke controles, zoals de RPF-validatie, PIM-inkapseling (als de firewall de FHR is), Oil-controle, enzovoort.
5. De CP maakt een (S,G) ingang met de inkomende en uitgaande interfaces in de 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), 00:19:28/00:03:13, 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. De CP instrueert de FP via CP > SP > FP pad om een **kind/stub** verbinding tussen de inkomende en uitgaande interfaces te maken:

Deze verbinding is alleen zichtbaar in de uitvoer van de opdracht **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
```

In de softwareversies met de fix van Cisco bug ID CSCwe21280 , wordt het syslogbericht 302015 voor de kinder/stub-verbinding ook gegenereerd:

```
<#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

Wanneer zowel ouder- als kind/stub-verbindingen tot stand worden gebracht, komen de ingangspakketten overeen met de bestaande verbinding en worden deze doorgestuurd in FP:

<#root>

```
firepower#
```

show capture capi trace packet-number 2

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

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

Phase: 3

Type: FLOW-LOOKUP

```
Subtype:
Result: ALLOW
Config:
Additional Information:
```

Found flow with id 19, using existing flow <--- Existing flow

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

Filter ICMP multicast verkeer

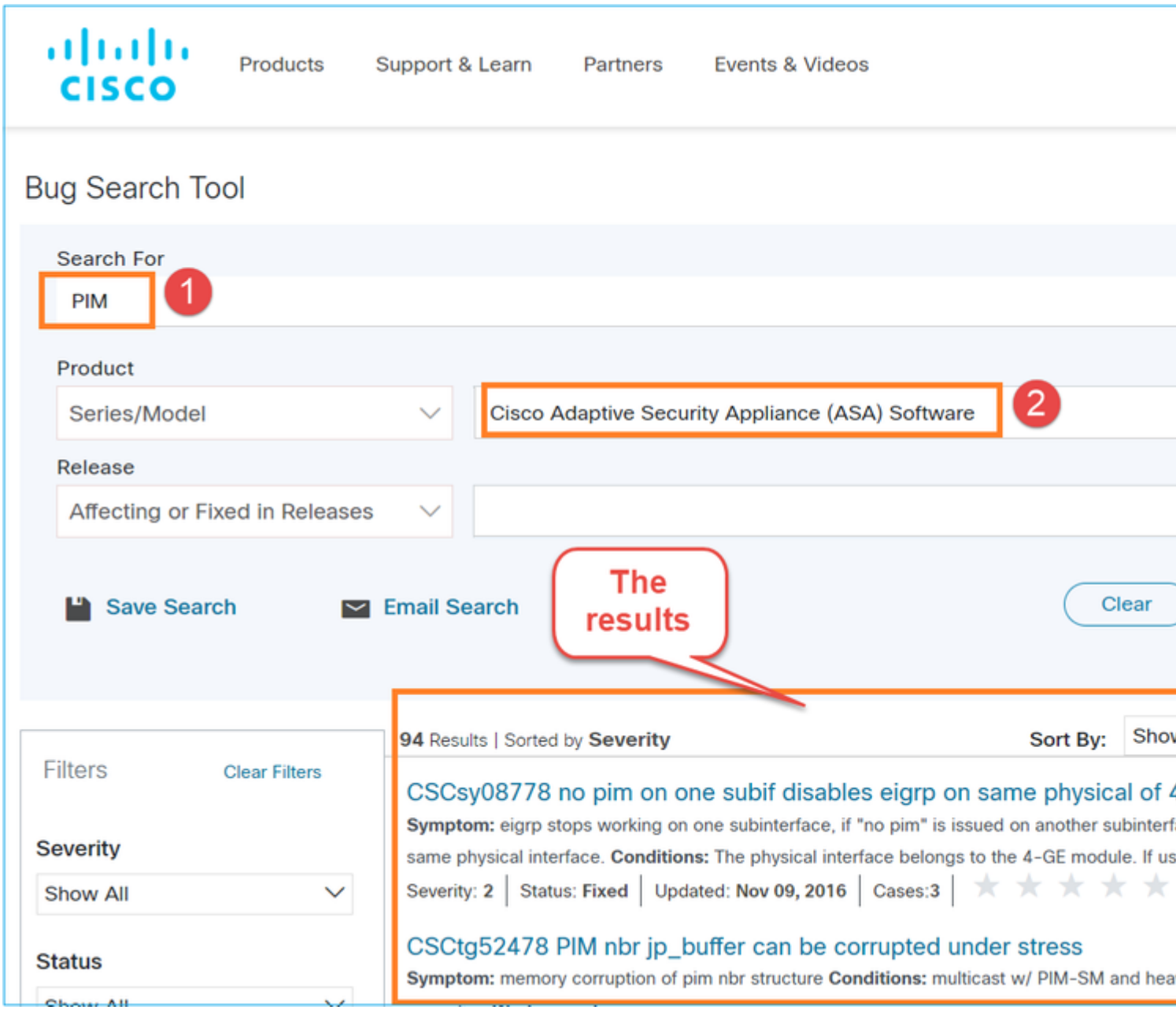
U kunt geen ICMP-multicast verkeer met een ACL filteren. U moet het Control Plane-beleid (ICMP) gebruiken:

Cisco bug-id CSCsl26860 ASA filtert multicast ICMP-pakketten niet

Bekende PIM-multicast defecten

U kunt de Bug Search Tool gebruiken voor bekende defects: https://bst.cloudapps.cisco.com/bugsearch

De meeste ASA- en FTD-defecten worden vermeld onder het product 'Cisco adaptieve security applicatie (ASA)':



Gerelateerde informatie

- ASA multicast probleemoplossing en algemene problemen
- Firepower Management Center multicast

- Samenvatting van de Firepower Multicast Vlaggen

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.