Dépannage de Firepower Threat Defense et ASA Multicast PIM

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
  - Notions de base sur le routage multidiffusion
  - Abréviations/Acronymes
  - Tâche 1 - Mode intermédiaire PIM (RP statique)
  - Tâche 2 : configuration du routeur d'amorçage PIM (BSR)
- Méthodologie de dépannage
- Commandes de dépannage PIM (Aide-mémoire)
- Problèmes connus
  - PIM n'est pas pris en charge sur un vPC Nexus
  - Zones de destination non prises en charge
  - Le pare-feu ne transmet pas de messages PIM aux routeurs en amont en raison de HSRP
  - Le pare-feu n'est pas considéré comme LHR lorsqu'il n'est pas le DR dans le segment LAN
  - Le pare-feu abandonne les paquets multidiffusion en raison d'un échec de vérification de transfert de chemin inverse
  - Le pare-feu ne génère pas de jointure PIM lors du basculement PIM vers l'arborescence source
  - Le pare-feu abandonne les premiers paquets en raison du taux de punt Limite
  - Filtrer le trafic multidiffusion ICMP
- Défauts de multidiffusion PIM connus
- Informations connexes

Introduction

Ce document décrit comment Firepower Threat Defense (FTD) et Adaptive Security Appliance (ASA) implémentent le protocole PIM (Protocol Independent Multicast).

Conditions préalables

Exigences

Connaissances de base du routage IP.

Composants utilisés

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

Informations générales

Notions de base sur le routage multidiffusion

- La monodiffusion transfère les paquets vers la destination tandis que la multidiffusion transfère les paquets loin de la source.
- Les périphériques réseau multidiffusion (pare-feu/routeurs, etc.) transfèrent les paquets via le protocole RPF (Reverse Path Forwarding). Notez que RPF n'est pas identique à uRPF qui est utilisé en monodiffusion pour empêcher des types spécifiques d'attaques. Le protocole RPF peut être défini comme un mécanisme qui transfère les paquets multidiffusion loin de la source à partir d’interfaces qui mènent vers des récepteurs multidiffusion. Son rôle principal est d'empêcher les boucles de trafic et de garantir des chemins de trafic corrects.
- Un protocole de multidiffusion comme PIM a 3 fonctions principales :

1. Recherchez l’interface en amont (l’interface la plus proche de la source).

2. Recherchez les interfaces en aval associées à un flux de multidiffusion spécifique (interfaces vers les récepteurs).

3. Maintenez l'arborescence de multidiffusion (ajoutez ou supprimez les branches de l'arborescence).

- Une arborescence de multidiffusion peut être créée et maintenue par l'une des 2 méthodes suivantes : jointures implicites (flood-and-prune) ou jointures explicites (modèle d'extraction). Le mode dense PIM (PIM-DM) utilise des jointures implicites tandis que le mode intermédiaire PIM (PIM-SM) utilise des jointures explicites.
- Une arborescence de multidiffusion peut être partagée ou basée sur la source :
    - Les arbres partagés utilisent le concept de Rendezvous Point (RP) et sont notés comme (*, G) où G = IP du groupe de multidiffusion.
    - Les arborescences basées sur la source sont enracinées à la source, n'utilisent pas de RP et sont notées comme (S, G) où S = l'IP de la source/serveur de multidiffusion.
- Modèles de transfert multidiffusion :
    - Le mode de livraison multidiffusion source (ASM) utilise des arborescences partagées (*, G) où n'importe quelle source peut envoyer le flux multidiffusion.
    - Le protocole SSM (Source-Specific Multicast) utilise des arborescences basées sur la source (S, G) et la plage IP 232/8.
    - Bidirectionnel (BiDir) est un type d'arborescence partagée (*, G) où le trafic du plan de contrôle et du plan de données passe par le RP.
- Vous pouvez configurer ou sélectionner un point de rendez-vous à l'aide de l'une des méthodes suivantes :
    - RP statique
    - Auto-RP
    - Routeur d'amorçage (BSR)

Résumé des modes PIM

mode PIM	RP	Arborescence partagée	Notation	IGMP	ASA/FTD pris en charge
Mode intermédiaire PIM	Oui	Oui	(*, G) et (S, G)	v1/v2/v3	Oui
Mode dense PIM	Non	Non	(S, G)	v1/v2/v3	Non*
Mode	Oui	Oui	(*, G)	v1/v2/v3	Oui

bidirectionnel PIM					
Mode PIM SSM (Source-Specific-Multicast)	Non	Non	(S, G)	v3	Non**

*Auto-RP = le trafic Auto-RP peut passer

** ASA/FTD ne peut pas être un périphérique de dernier saut

Résumé de la configuration RP

Configuration de Rendezvous Point	ASA/FTD
RP statique	Oui
Auto-RP	Non, mais le trafic du plan de contrôle Auto-RP peut passer
BSR	Oui, mais pas de prise en charge C-RP

Remarque : Avant de commencer à dépanner un problème de multidiffusion, il est très important d'avoir une vue claire de la topologie de multidiffusion. Plus précisément, au minimum, vous devez savoir :
- Quel est le rôle du pare-feu dans la topologie de multidiffusion ?
- Qui est le RP ?
- Qui est l'expéditeur du flux de multidiffusion (IP source et IP de groupe de multidiffusion) ?
- Qui est le destinataire du flux de multidiffusion ?
- Avez-vous des problèmes avec le plan de contrôle (IGMP/PIM) ou le plan de données (flux de multidiffusion) lui-même ?

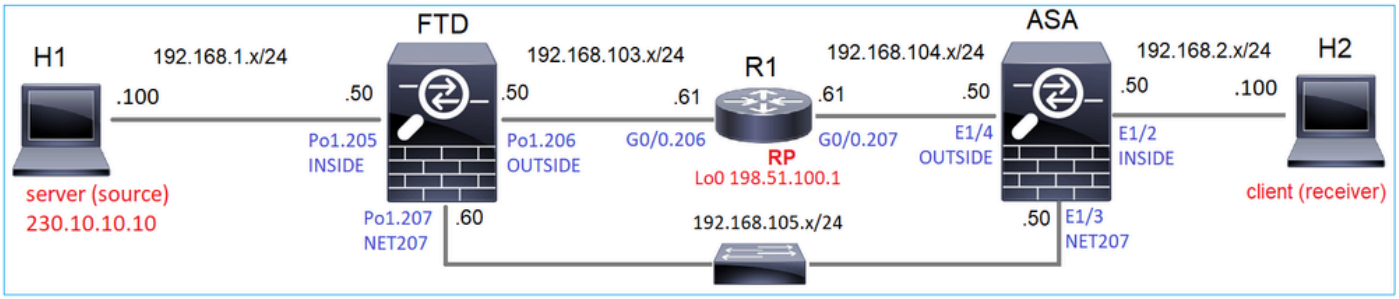
Abréviations/Acronymes

Acronymes	Explication
FHR	Routeur de premier saut : saut directement connecté à la source du trafic de multidiffusion.

LHR	Routeur de dernier saut : saut directement connecté aux récepteurs du trafic de multidiffusion.
RP	Point De Rendez-Vous
DR	Routeur désigné
SPT	Arborescence Du Chemin Le Plus Court
RPT	Arborescence de point de rendez-vous (RP), arborescence de partage
RPF	Transfert par chemin inverse
HUILE	Liste des interfaces sortantes
MRIB	Base d'informations de routage multidiffusion
MFIB	Base D'Informations De Transmission Multidiffusion
ASM	Multidiffusion à toutes les sources
BSR	Routeur Bootstrap
SSM	Multidiffusion spécifique à la source
FP	Chemin rapide
SP	Trajet Lent
CP	Point de contrôle
PPS	Taux de paquets par seconde

Tâche 1 - Mode intermédiaire PIM (RP statique)

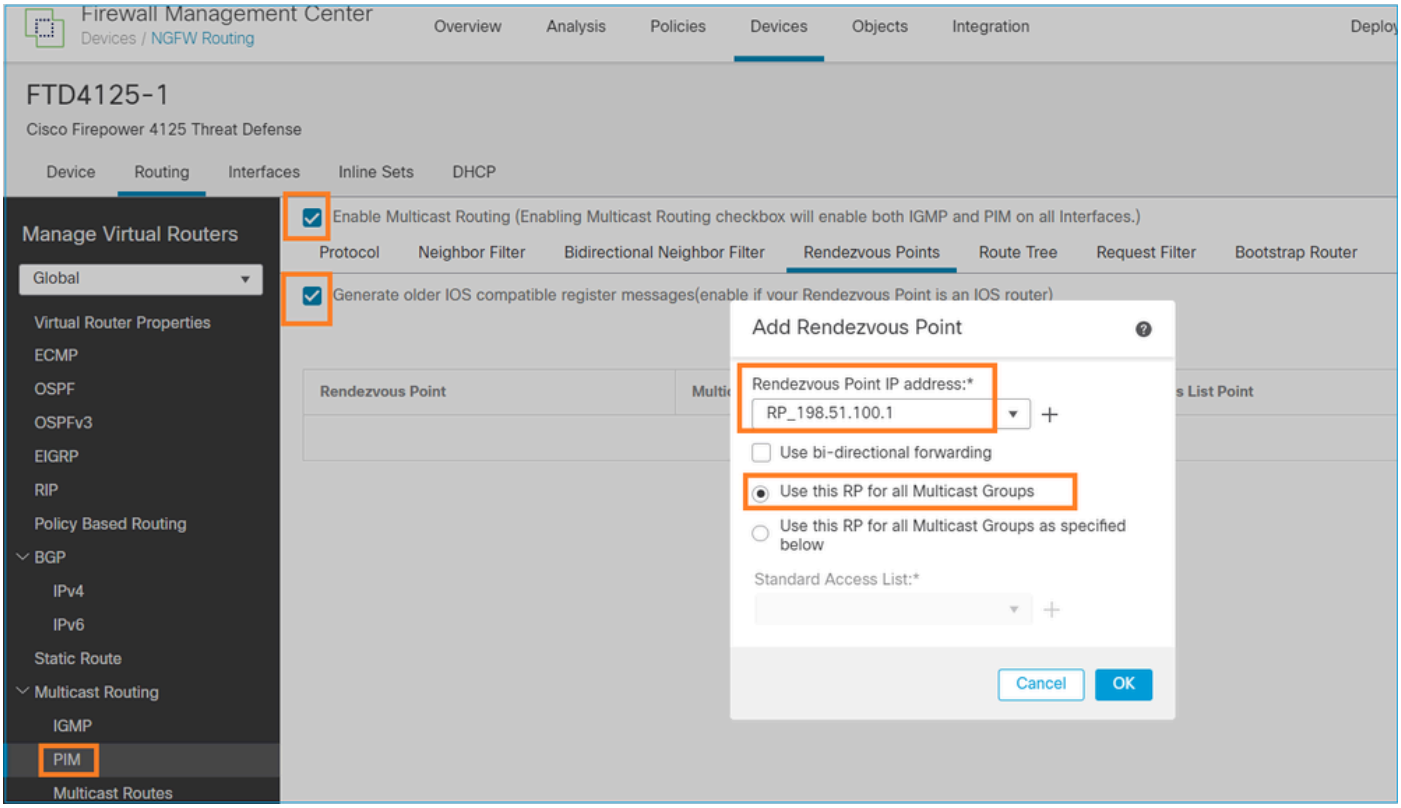
Topologie



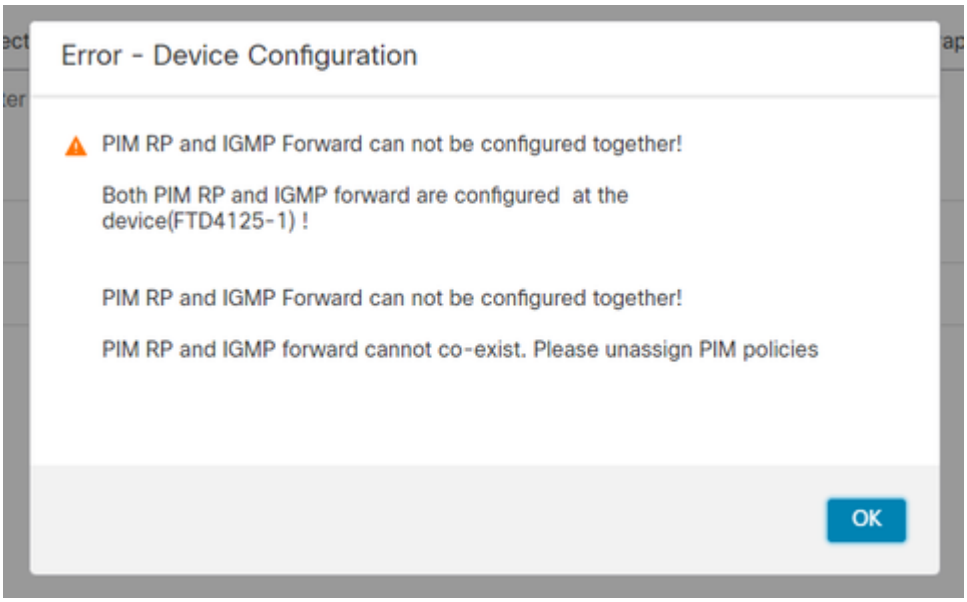
Configurez le mode intermédiaire PIM multicast dans la topologie avec R1 (198.51.100.1) comme RP.

Solution

Configuration FTD :



L'ASA/FTD ne peut pas être configuré pour le routage de stub IGMP et le PIM en même temps :



La configuration résultante sur 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
```

Sur le pare-feu ASA, il existe une configuration similaire :

```
<#root>
asa(config)#

multicast-routing


asa(config)#

pim rp-address 198.51.100.1
```

Configuration RP (routeur Cisco) :

```
<#root>
ip multicast-routing

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

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

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

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

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

 ip ospf 1 area 0
!
interface Loopback0


ip address 198.51.100.1 255.255.255.255
```

```
<-- The router is the RP

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

 ip ospf 1 area 0
```

Vérification

Vérifiez le plan de contrôle de multidiffusion sur FTD lorsqu'il n'y a pas de trafic de multidiffusion (expéditeurs ou récepteurs) :

<#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
```

Vérifiez les voisins PIM :

<#root>

```
firepower#

show pim neighbor

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

Le RP annonce toute la plage de groupes de multidiffusion :

<#root>

```
firepower#

show pim group-map

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

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

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

La table mroute du pare-feu comporte des entrées non pertinentes (239.255.255.250 est le protocole SSDP (Simple Service Discovery Protocol) utilisé par des fournisseurs tels que MAC OS et 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
```

Il y a un tunnel PIM construit entre les pare-feu et le 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
```

Le tunnel PIM peut également être vu sur la table de connexion du pare-feu :

```
<#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
```

Vérification sur le pare-feu ASA :

```
<#root>

asa#

show pim neighbor


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


<#root>

asa#

show pim tunnel
```

```
Interface          RP Address       Source Address

Tunnel0            198.51.100.1     192.168.104.50



<-- PIM tunnel between the ASA and the RP
```

Vérification RP (routeur Cisco) RP. Il existe des groupes de multidiffusion pour SSDP et 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
```

Vérification dès qu'un destinataire annonce sa présence

Remarque : Les commandes de pare-feu présentées dans cette section sont entièrement applicables à ASA et FTD.

L'ASA obtient le message IGMP Membership Report et crée les entrées IGMP et mroute (*, G) :

```
<#root>

asa#

show igmp group 230.10.10.10

IGMP Connected Group Membership
Group Address    Interface            Uptime    Expires   Last Reporter

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

Le pare-feu ASA crée une mroute pour le groupe de multidiffusion :

```
<#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
```

Une autre vérification du pare-feu est le résultat de la topologie PIM :

```
<#root>

asa#

show pim topology 230.10.10.10

...

(*,230.10.10.10) SM Up: 00:07:15 RP: 198.51.100.1                    <-- An entry for multicast group 23
```

```
JP: Join(00:00:33) RPF: OUTSIDE,192.168.104.61 Flags: LH
  INSIDE             00:03:15  fwd LI LH
```

Remarque : si le pare-feu n'a pas de route vers le RP, la sortie debug pim montre un échec de recherche RPF

L'échec de recherche RPF dans la sortie debug pim :

<#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
```

Si tout est OK, le pare-feu envoie un message PIM Join-Prune au RP :

<#root>

```
asa#

debug pim group 230.10.10.10

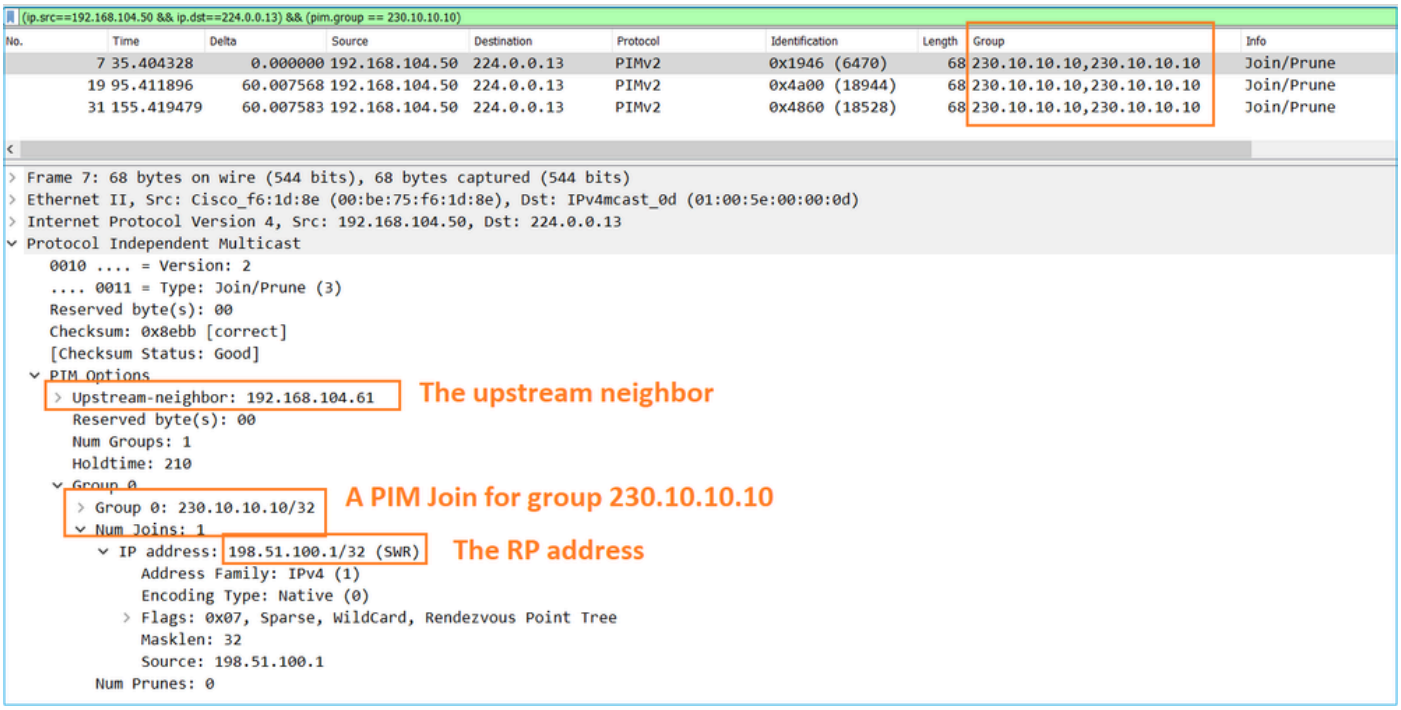


IPv4 PIM group debugging is on
for group 230.10.10.10

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
```

La capture montre que les messages PIM Join sont envoyés toutes les 1 min et les messages PIM Hello toutes les 30 secondes. PIM utilise l'adresse IP 224.0.0.13 :



Conseil : Filtre d'affichage Wireshark : (ip.src==192.168.104.50 && ip.dst==224.0.0.13) && (pim.group == 230.10.10.10)
- 192.168.104.50 est l'adresse IP du pare-feu de l'interface de sortie (vers le voisin PIM en amont)
- 224.0.0.13 est le groupe de multidiffusion PIM où les jonctions et les pruneaux PIM sont envoyés
- 230.10.10.10 est le groupe de multidiffusion pour lequel nous envoyons le PIM Join/Prune

---

Le RP crée une mroute (*, G). Notez que puisqu'il n'y a pas encore de serveurs, l'interface entrante est nulle :

<#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

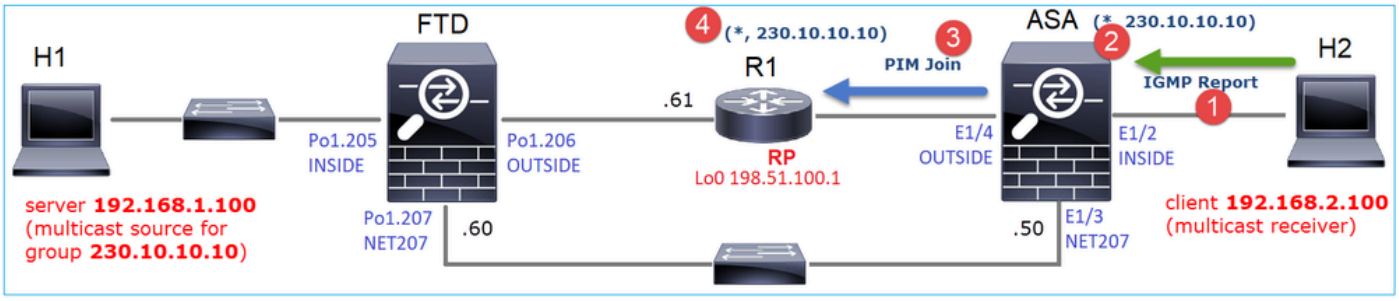
Outgoing interface list:

GigabitEthernet0/0.207

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

<-- There was a PIM Join on this interface

Cela peut être visualisé comme suit :



1. Le rapport IGMP est reçu sur ASA.
2. Une mroute (*, G) est ajoutée.
3. L'ASA envoie un message PIM Join au RP (198.51.100.1).
4. Le RP reçoit le message Join et ajoute un mroute (*, G).

En même temps, sur FTD, il n'y a pas de mroutes car il n'y a pas de rapport IGMP ni de jointure PIM reçue :

<#root>

firepower#

show mroute 230.10.10.10

No mroute entries found.

Vérification lorsque le serveur envoie un flux de multidiffusion

Le FTD obtient le flux de multidiffusion de H1 et démarre le processus d'enregistrement PIM avec le RP. Le FTD envoie un message d'enregistrement PIM monodiffusion au RP. Le RP envoie un message PIM Join au First-Hop-Router (FHR), qui est le FTD dans ce cas, pour rejoindre l'arbre de multidiffusion. Il envoie ensuite un message Register-Stop.

<#root>

```
firepower#

debug pim group 230.10.10.10


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

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



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


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

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


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

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


IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE J/P state changed from Null to Join
```

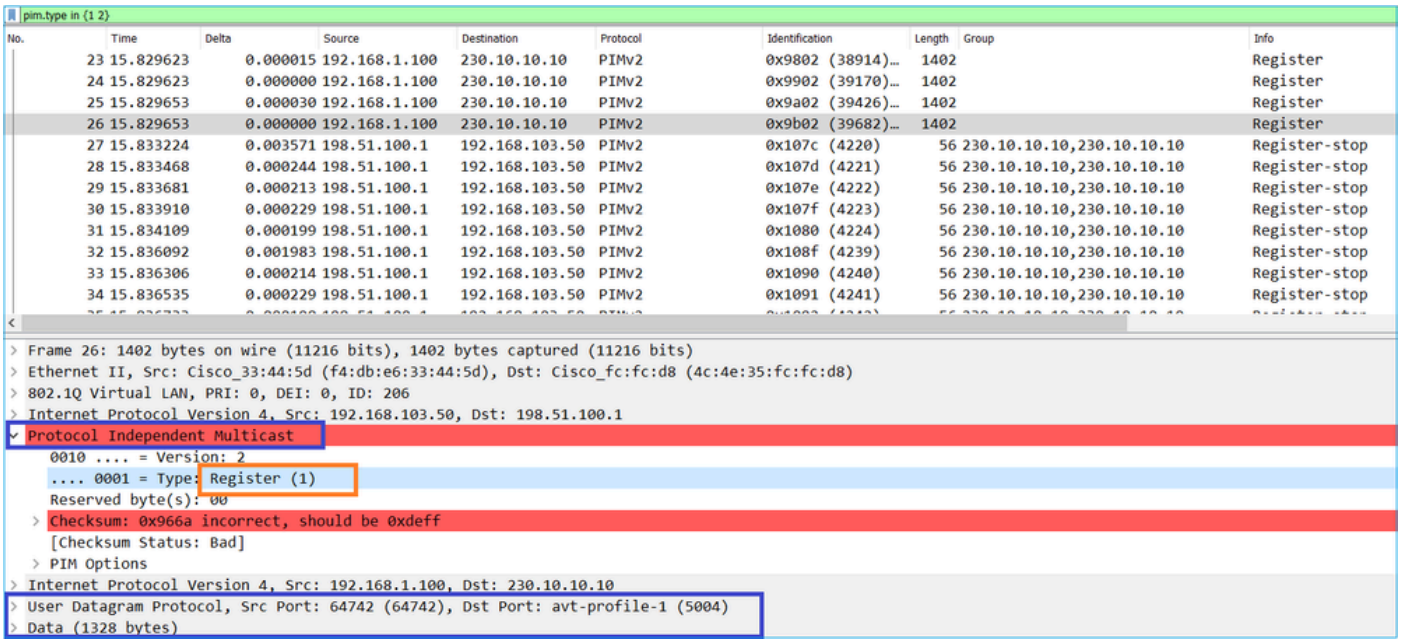
```
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE FWD state change from Prune to Forward
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify F NS
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE Raise J/P expiration timer to 210 seconds
IPv4 PIM: J/P entry: Join root: 192.168.1.100 group: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

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

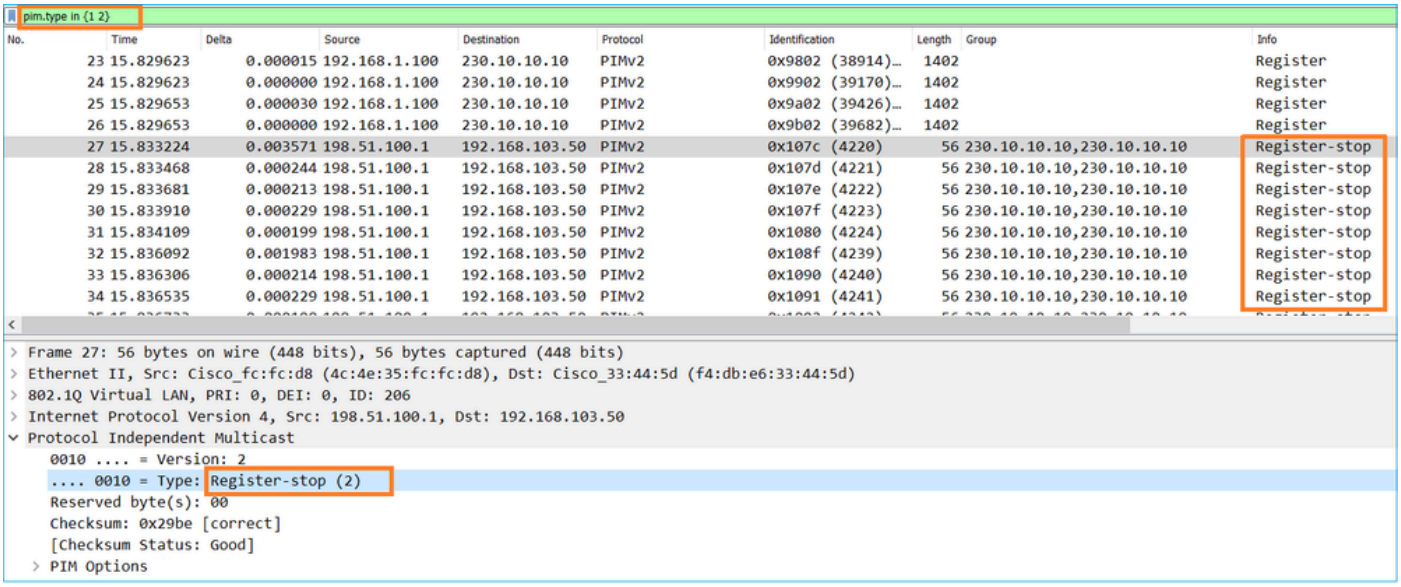

IPv4 PIM: (192.168.1.100,230.10.10.10) Stop registering


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

Le message PIM Register est un message PIM qui transporte des données UDP avec les informations du registre PIM :



Le message Register-Stop PIM :



Conseil : Pour afficher uniquement les messages PIM Register et PIM Register-Stop sur Wireshark, vous pouvez utiliser le filtre d'affichage : pim.type dans {1}2}

Le pare-feu (routeur de dernier saut) obtient le flux de multidiffusion sur l'interface OUTSIDE et initie le basculement SPT (Shortest Path Tree) vers l'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)

Le débogage PIM sur le FTD lorsque le basculement se produit :

<#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
```

Le mroute FTD une fois que la commutation SPT démarre :

<#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
```

À la fin de la commutation SPT, seule l'interface NET207 est affichée dans l'OIL de FTD :

<#root>

```
firepower#

show mroute 230.10.10.10



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

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


NET207, Forward


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

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

Sur le routeur de dernier saut (ASA), le bit SPT est également défini :

<#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
```

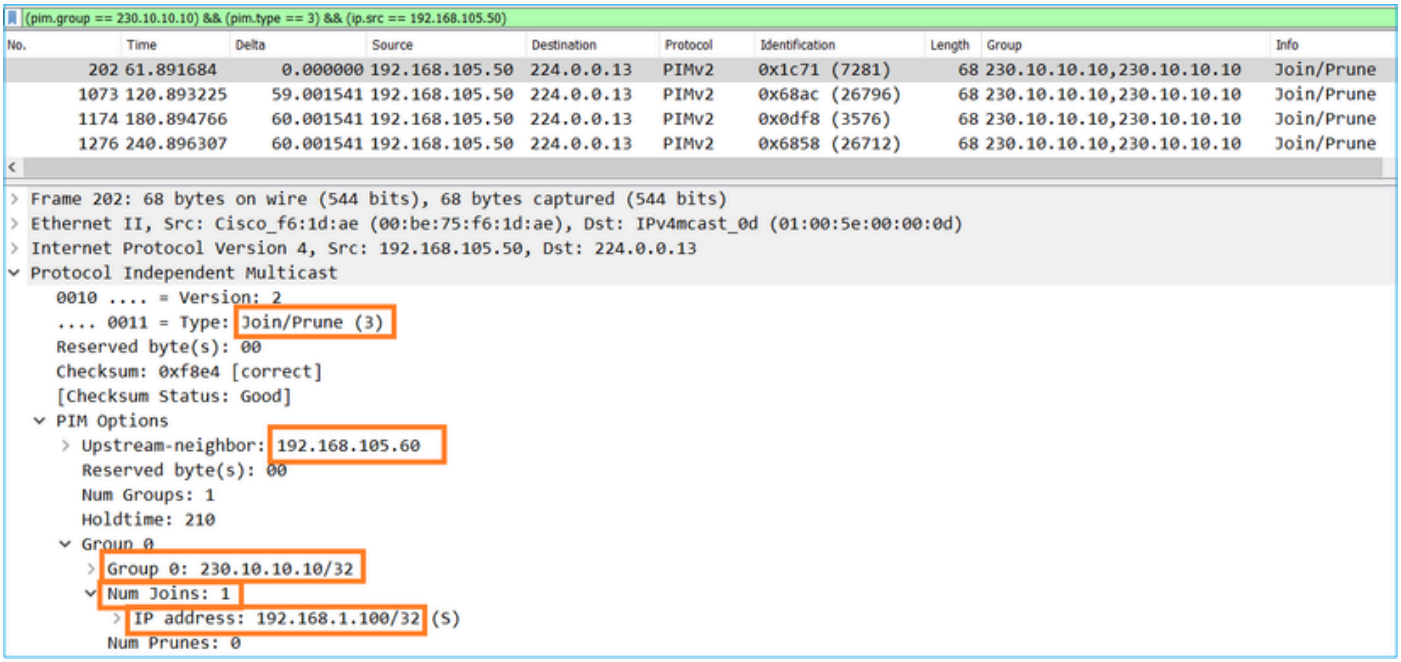
T   <-- SPT switchover for group 230.10.10.10

Incoming interface:

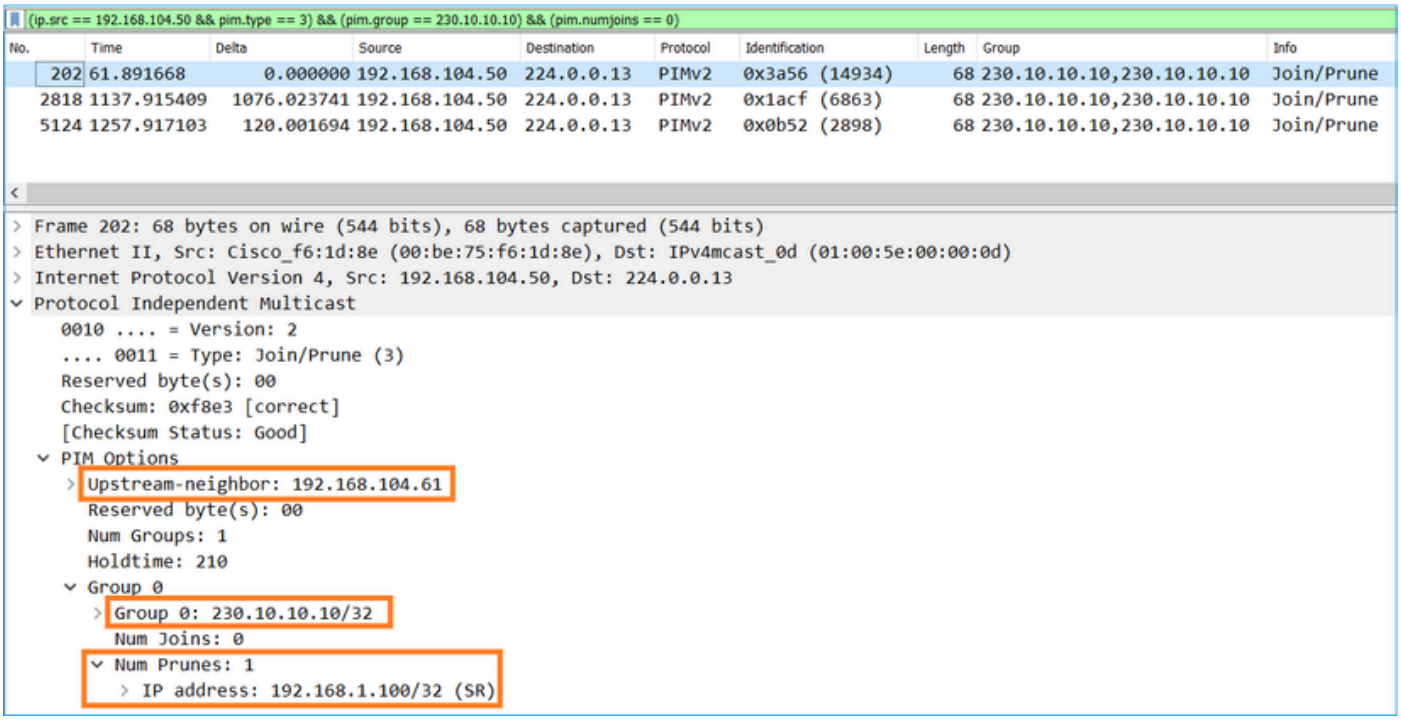
NET207   <-- The multicast packets arrive on interface NET207

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

La commutation à partir de l'interface ASA NET207 (le routeur de premier saut qui a effectué la commutation). Un message PIM Join est envoyé au périphérique en amont (FTD) :



Sur l'interface OUTSIDE, un message PIM Prune est envoyé au RP pour arrêter le flux de multidiffusion :



Vérification du trafic PIM :

<#root>

```
firepower#

show pim traffic



PIM Traffic Counters
Elapsed time since counters cleared: 1w2d

                              Received     Sent
Valid PIM Packets             53934        63983
Hello                         36905        77023

Join-Prune                    6495         494          <-- PIM Join/Prune messages



Register                      0            2052         <-- PIM Register messages



Register Stop                 1501         0            <-- PIM Register Stop messages



Assert                        289          362
Bidir DF Election             0            0

Errors:
```

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

Pour vérifier le nombre de paquets traités dans le rapport Slow Path vs Fast Path vs Control Point :

<#root>

```
firepower#

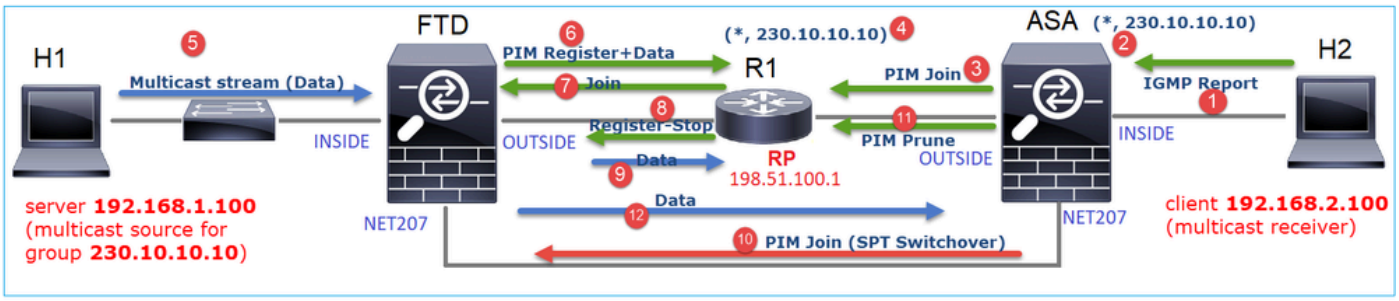
show asp cluster counter



Global dp-counters:


Context specific dp-counters:
MCAST_FP_FROM_PUNT                      2712    Number of multicast packets punted from CP to FP
MCAST_FP_FORWARDED                      94901   Number of multicast packets forwarded in FP
MCAST_FP_TO_SP                          1105138 Number of multicast packets punted from FP to SP
MCAST_SP_TOTAL                          1107850 Number of total multicast packets processed in SP
MCAST_SP_FROM_PUNT                      2712    Number of multicast packets punted from CP to SP
MCAST_SP_FROM_PUNT_FORWARD              2712    Number of multicast packets coming from CP that are for
MCAST_SP_PKTS                           537562  Number of multicast packets that require slow-path atte
MCAST_SP_PKTS_TO_FP_FWD                 109     Number of multicast packets that skip over punt rule an
MCAST_SP_PKTS_TO_CP                     166981  Number of multicast packets punted to CP from SP
MCAST_FP_CHK_FAIL_NO_HANDLE             567576  Number of multicast packets failed with no flow mcast_h
MCAST_FP_CHK_FAIL_NO_ACCEPT_IFC         223847  Number of multicast packets failed with no accept inter
MCAST_FP_CHK_FAIL_NO_SEQ_NO_MATCH       131     Number of multicast packets failed with no matched sequ
MCAST_FP_CHK_FAIL_NO_FP_FWD             313584  Number of multicast packets that cannot be fast-path fo
MCAST_FP_UPD_FOR_UNMATCH_IFC            91      Number of times that multicast flow's ifc_out  cannot b
```

Diagramme montrant ce qui se passe étape par étape :



1. L'hôte d'extrémité (H2) envoie un rapport IGMP pour joindre le flux de multidiffusion

230.10.10.10.
2. Le routeur de dernier saut (ASA) qui est le DR PIM crée une entrée (*, 230.10.10.10).
3. L'ASA envoie un message PIM Join vers RP pour le groupe 230.10.10.10.
4. Le RP crée l'entrée (*, 230.10.10.10).
5. Le serveur envoie les données du flux de multidiffusion.
6. Le FTD encapsule les paquets de multidiffusion dans les messages du registre PIM et les envoie (monodiffusion) au RP. À ce stade, le RP voit qu'il a un récepteur actif, décapsule les paquets de multidiffusion et les envoie au récepteur.
7. Le RP envoie un message PIM Join au FTD pour rejoindre l'arborescence de multidiffusion.
8. Le RP envoie un message d'arrêt du registre PIM au FTD.
9. Le FTD envoie un flux multicast natif (pas d'encapsulation PIM) vers le RP.
10. Le routeur de dernier saut (ASA) constate que la source (192.168.1.100) a un meilleur chemin à partir de l'interface NET207 et démarre une commutation. Il envoie un message PIM Join au périphérique en amont (FTD).
11. Le routeur de dernier saut envoie un message d'élagage PIM au RP.
12. Le FTD achemine le flux de multidiffusion vers l'interface NET207. L'ASA passe de l'arborescence partagée (arborescence RP) à l'arborescence source (SPT).

Tâche 2 : configuration du routeur d'amorçage PIM (BSR)

Notions de base sur BSR

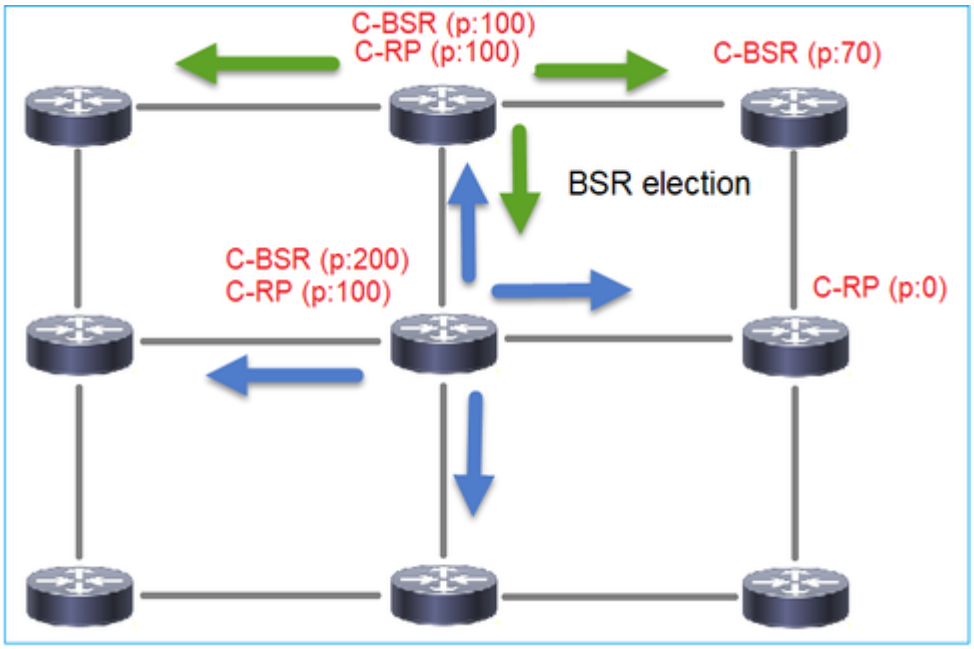
- BSR (RFC 5059) est un mécanisme de multidiffusion de plan de contrôle qui utilise le protocole PIM et permet aux périphériques d'apprendre les informations RP de manière dynamique.
- Définitions BSR :
  - Candidat RP (C-RP) : Périphérique qui veut être un RP.
  - Candidat BSR (C-BSR) : Périphérique qui veut être un BSR et qui annonce des RP-sets à d'autres périphériques.
  - BSR : Périphérique qui est sélectionné comme BSR parmi de nombreux C-BSR. La priorité BSR la plus élevée remporte l'élection.
  - RP-set : Une liste de tous les C-RP et de leurs priorités.
  - RP : Le périphérique dont la priorité RP est la plus faible remporte la sélection.
  - Message BSR PIM (vide) : Message PIM utilisé dans la sélection BSR.
  - Message BSR PIM (normal) : Un message PIM envoyé à l'adresse IP 224.0.0.13 contient un RP-set et des informations BSR.

Fonctionnement de BSR

1. Mécanisme d'élection du BSR.

Chaque C-BSR envoie des messages PIM BSR vides qui contiennent une priorité. Le périphérique ayant la priorité la plus élevée (le fallback est l'IP la plus élevée) remporte la

sélection et devient le BSR. Les autres périphériques n'envoient plus de messages BSR vides.



Un message BSR utilisé dans le processus de sélection contient uniquement des informations de priorité C-BSR :

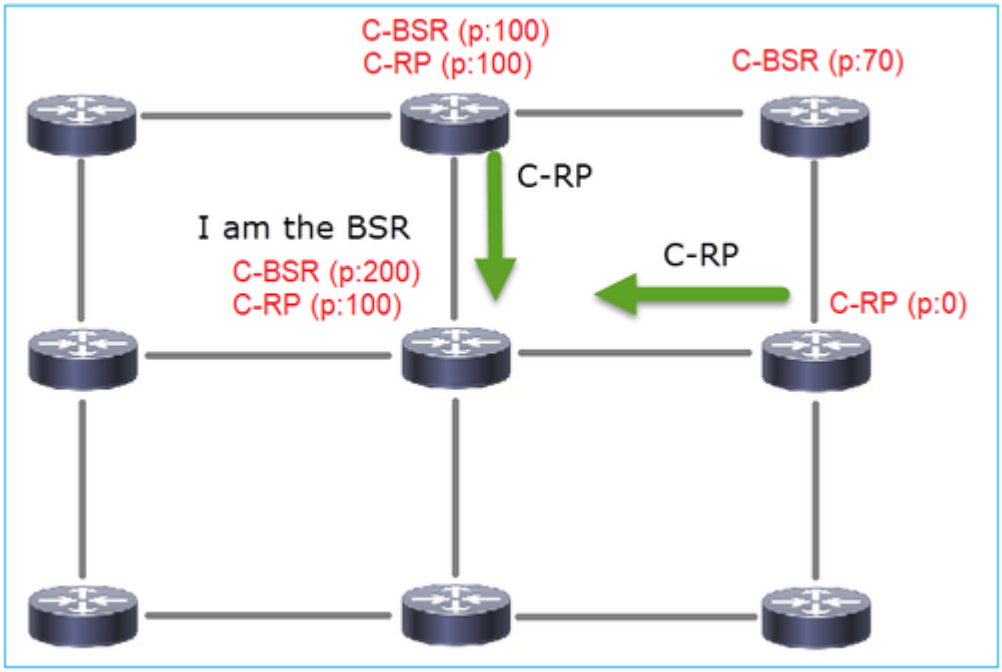
pim.type == 4

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

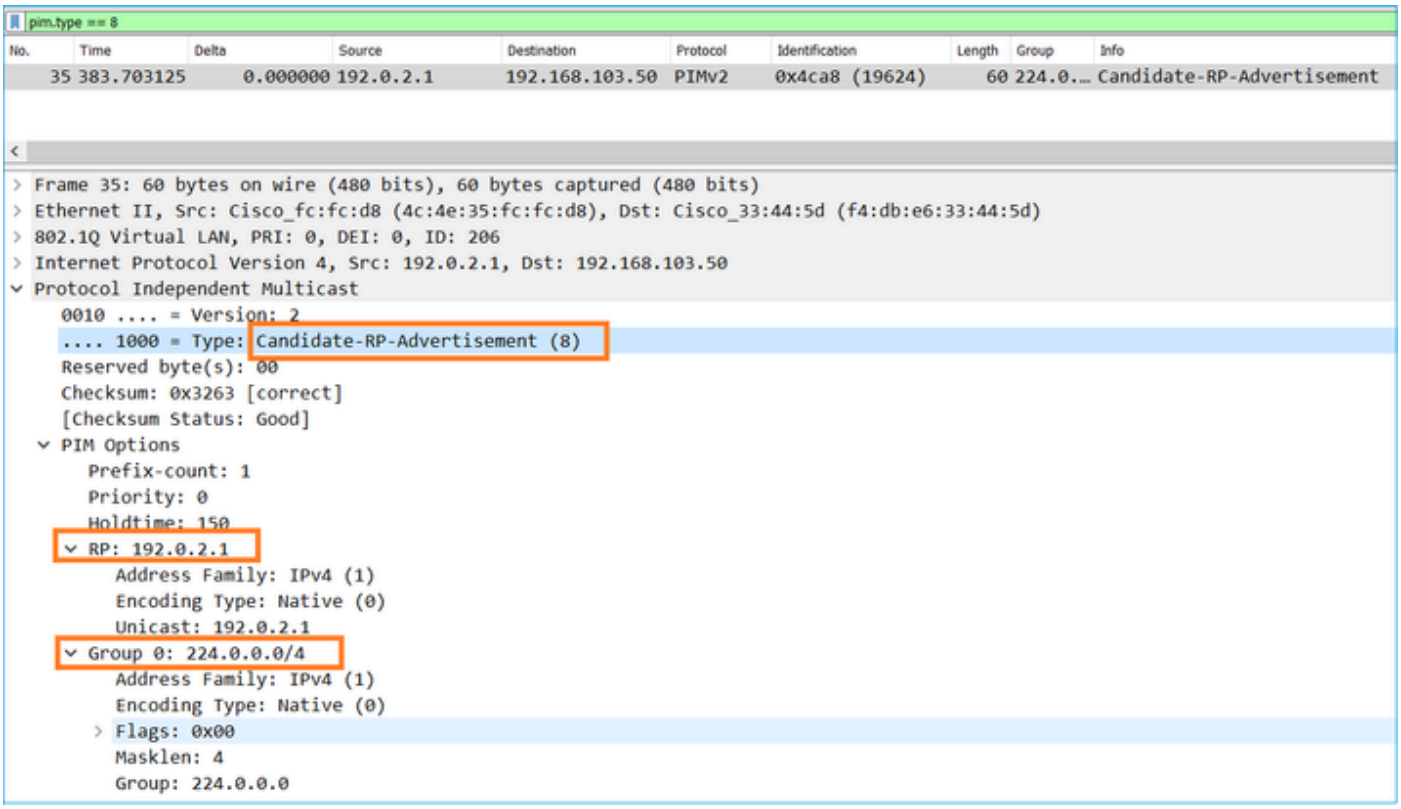
```
> Frame 2: 52 bytes on wire (416 bits), 52 bytes captured (416 bits)
> Ethernet II, Src: Cisco_33:44:5d (f4:db:e6:33:44:5d), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 206
> Internet Protocol Version 4, Src: 192.168.103.50, Dst: 224.0.0.13
v Protocol Independent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

Pour afficher les messages BSR dans Wireshark, utilisez ce filtre d'affichage : pim.type == 4

2. Les C-RP envoient des messages BSR de monodiffusion au BSR qui contiennent leur priorité C-RP :

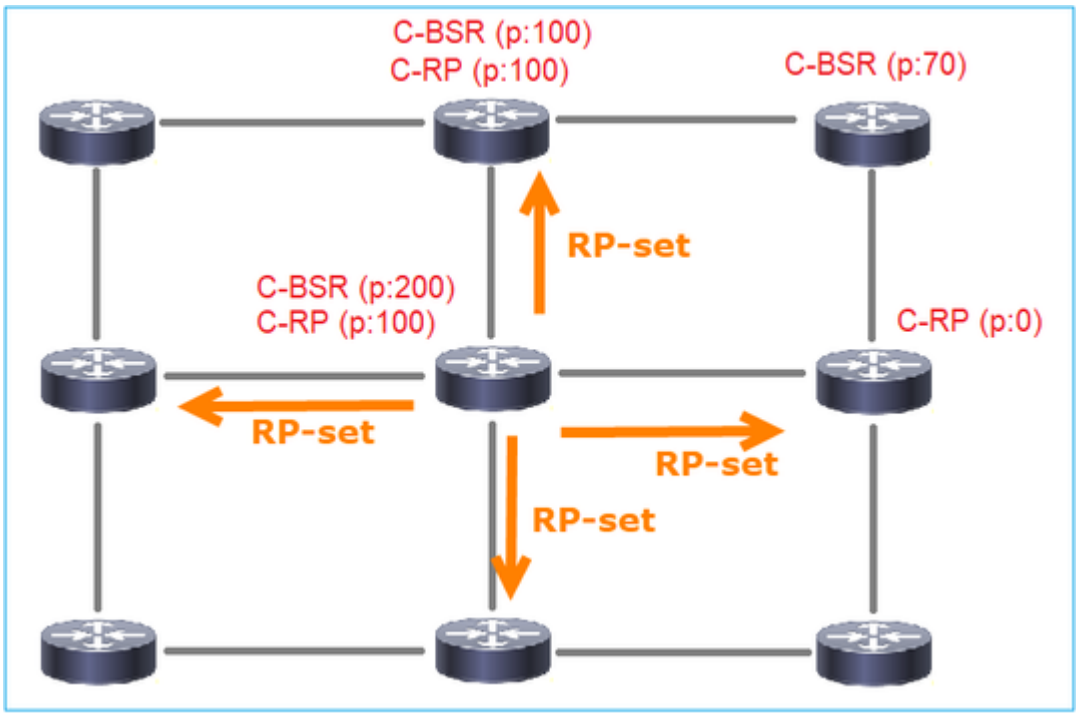


Un message RP candidat :



Pour afficher les messages BSR dans Wireshark, utilisez ce filtre d'affichage : pim.type == 8

3. Le BSR compose le RP-set et l'annonce à tous les voisins PIM :

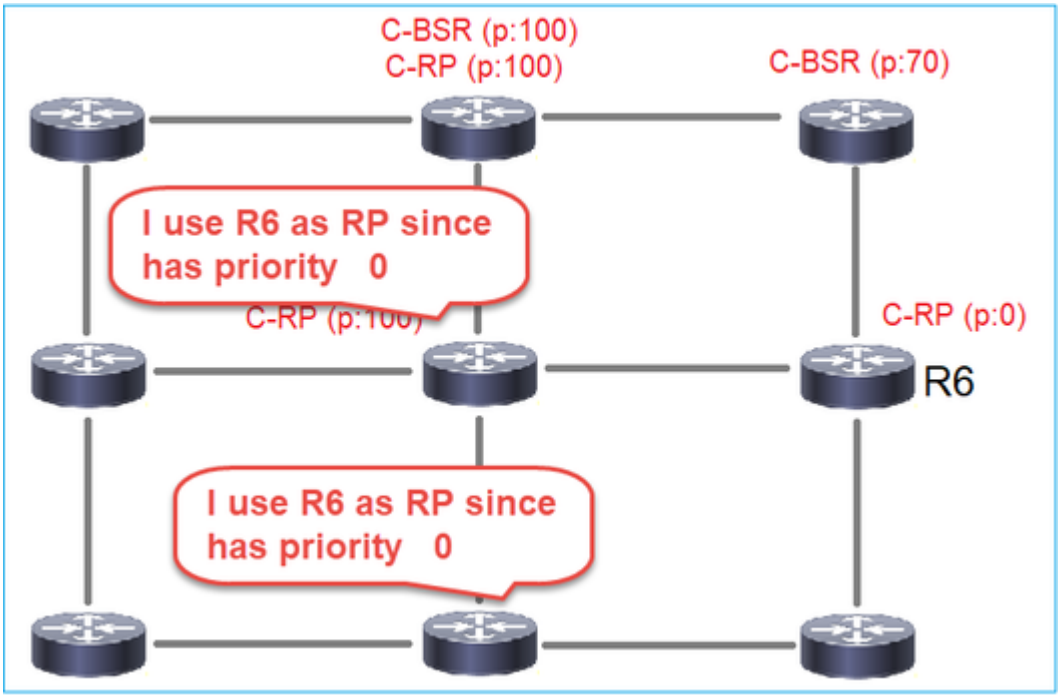


(ip.src == 192.168.105.60) && (pim.type == 4)

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

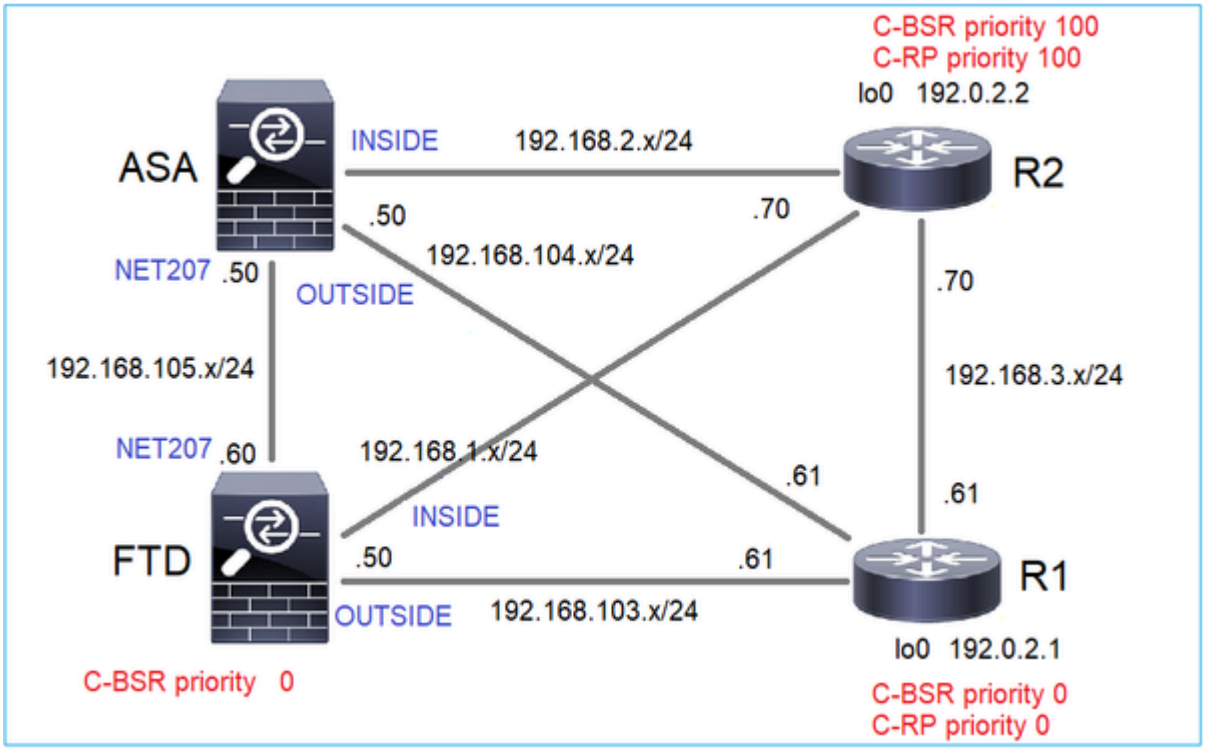
```
> Frame 152: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
> Ethernet II, Src: Cisco_33:44:5d (f4:db:e6:33:44:5d), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
> 802.1Q Virtual LAN, PRI: 6, DEI: 0, ID: 207
> Internet Protocol Version 4, Src: 192.168.105.60, Dst: 224.0.0.13
v Protocol Independent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

4. Les routeurs/pare-feu obtiennent le RP-set et sélectionnent le RP en fonction de la priorité la plus basse :



Exigence de la tâche

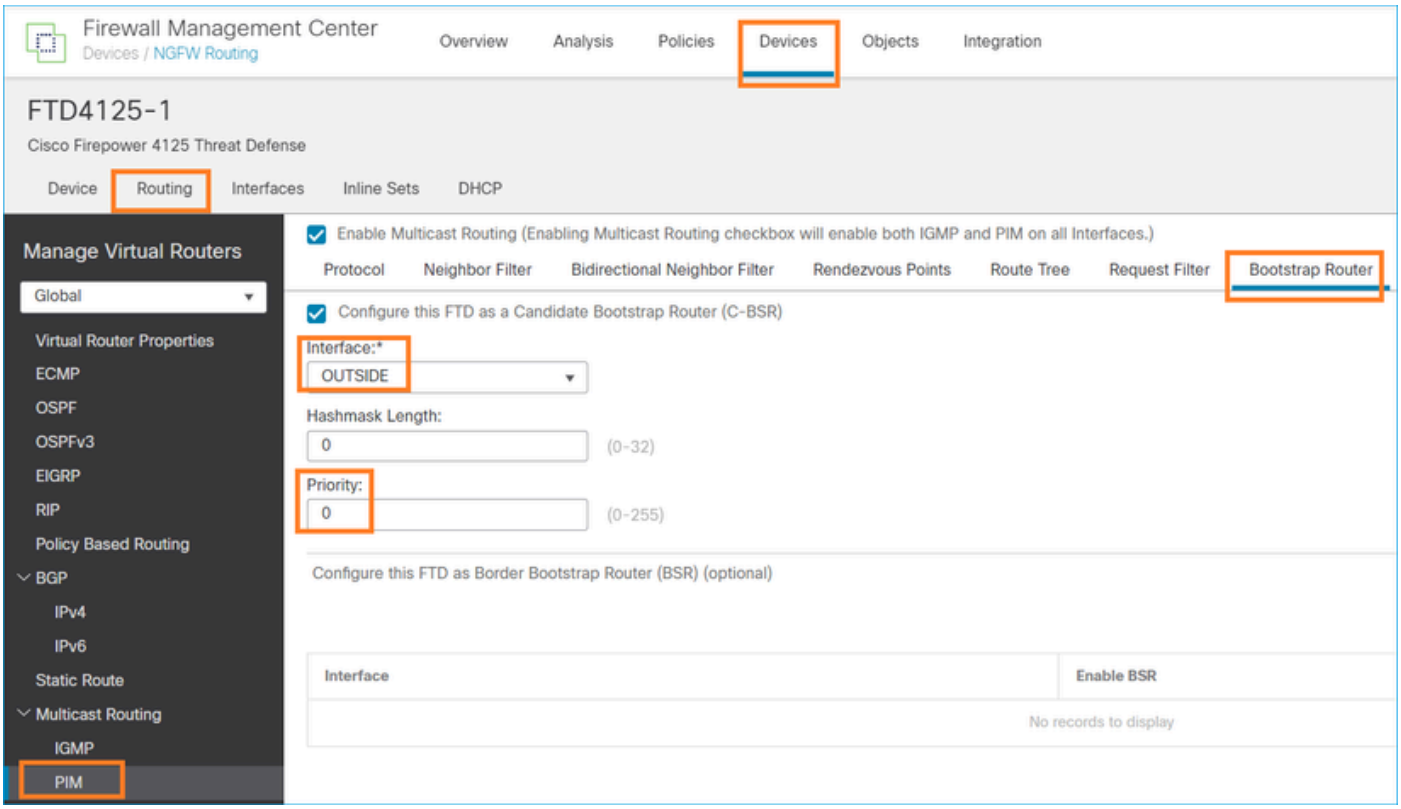
Configurez les C-BSR et les C-RP conformément à cette topologie :



pour cette tâche, le FTD doit s'annoncer comme C-BSR sur l'interface OUTSIDE avec la priorité BSR 0.

Solution

Configuration FMC pour FTD :



La configuration déployée :

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

Configuration sur les autres périphériques :

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)
```

Identique sur R2, mais avec des priorités C-BSR et C-RP différentes

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

Sur ASA, la multidiffusion est uniquement activée globalement. Cela active le protocole PIM sur toutes les interfaces :

```
multicast-routing
```

Vérification

R2 est le BSR élu en raison de la priorité la plus élevée :

<#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 est sélectionné comme RP en raison de la priorité la plus faible :

```
<#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
```

Les messages BSR sont soumis à un contrôle RPF. Vous pouvez activer debug pim bsr pour vérifier ceci :

```
<#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/
```

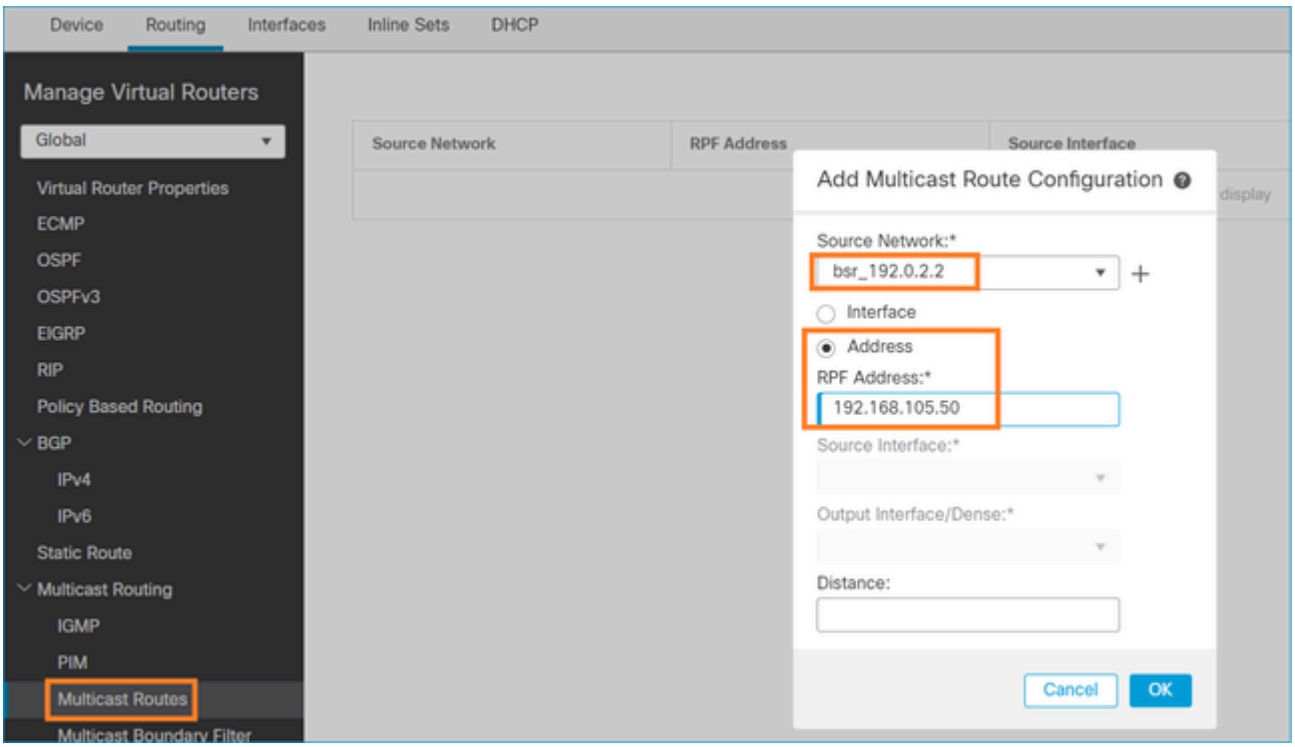
NET207

for 192.0.2.2

RPF failed, dropped

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

Si vous souhaitez modifier l'interface RPF, vous pouvez configurer une mroute statique. Dans cet exemple, le pare-feu accepte les messages BSR de l'adresse 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
```

Maintenant, les messages BSR sur l'interface NET207 sont acceptés, mais sur INSIDE sont abandonnés :

<#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
```

Activez la capture avec trace sur le pare-feu et vérifiez le traitement des messages BSR :

<#root>

```
firepower#

show capture


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

Les connexions PIM sont terminées sur le pare-feu, donc pour que la trace affiche des informations utiles, il est nécessaire d'effacer les connexions vers la boîte :

<#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
```

Si le paquet PIM est abandonné en raison d'une défaillance RPF, la trace indique :

<#root>

```
firepower#

show capture NET207 packet-number 4 trace
```

85 packets captured

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

192.168.104.61 > 224.0.0.13 ip-proto-103

, length 38

<-- Ingress PIM packet

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

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

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

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

Result:
input-interface: NET207(vrfid:0)
input-status: up
input-line-status: up
output-interface: OUTSIDE(vrfid:0)
output-status: up
output-line-status: up
Action: drop
Time Taken: 25376 ns

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

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

La table ASP supprime et capture les paquets show RPF-failed :

<#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

Pour capturer des paquets abandonnés en raison d'une défaillance RPF :

<#root>

firepower#

capture ASP type asp-drop rpf-violated

<#root>

firepower#

show capture ASP | include 224.0.0.13

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

Méthodologie de dépannage

La méthodologie de dépannage du pare-feu dépend principalement du rôle du pare-feu dans la topologie de multidiffusion. Voici la liste des étapes recommandées pour le dépannage :

1. Clarifier les détails de la description du problème et des symptômes. Essayez de réduire la portée aux problèmes du plan de contrôle (IGMP/PIM) ou du plan de données (flux de multidiffusion).
2. La condition préalable obligatoire pour le dépannage des problèmes de multidiffusion sur le pare-feu est de clarifier la topologie de multidiffusion. Vous devez au minimum identifier les éléments suivants :
    - rôle du pare-feu dans la topologie de multidiffusion : FHR, LHR, RP ou un autre rôle intermédiaire.
    - interfaces d'entrée et de sortie de multidiffusion attendues sur le pare-feu.
    - RP.
    - les adresses IP source de l'expéditeur.
    - groupes de multidiffusion adresses IP et ports de destination.
    - récepteurs du flux de multidiffusion.

3. Identifiez le type de routage de multidiffusion - Routage de multidiffusion Stub ou PIM :

- Routage multidiffusion d'extrémité : il permet l'enregistrement dynamique des hôtes et facilite le routage multidiffusion. Lorsqu'il est configuré pour le routage de multidiffusion d'extrémité, l'ASA agit comme un agent proxy IGMP. Au lieu de participer pleinement au routage de multidiffusion, l'ASA transfère les messages IGMP à un routeur de multidiffusion en amont, qui configure la livraison des données de multidiffusion. Pour identifier le routage en mode stub, utilisez la commande show igmp interface et vérifiez la configuration IGMP forward :

<#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 est activé sur les interfaces ; cependant, le voisinage n'est pas établi :

<#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.

Le transfert PIM-SM/Bidir et IGMP ne sont pas pris en charge simultanément.

Vous ne pouvez pas configurer d'options telles que l'adresse RP :

<#root>

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

- Routage de multidiffusion PIM - Le routage de multidiffusion PIM est le déploiement le plus courant. Le pare-feu prend en charge à la fois le PIM-SM et le PIM bidirectionnel. PIM-SM

est un protocole de routage multidiffusion qui utilise la base d'informations de routage monodiffusion sous-jacente ou une base d'informations de routage multidiffusion distincte. Il construit une arborescence partagée unidirectionnelle enracinée à un point de rendez-vous unique (RP) par groupe de multidiffusion et crée éventuellement des arborescences de plus court chemin par source de multidiffusion. Dans ce mode de déploiement, contrairement au mode stub, les utilisateurs configurent généralement la configuration d'adresse RP, et le pare-feu établit des contiguïtés PIM avec les homologues :

```
<#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. Vérifiez que l'adresse IP RP est configurée et qu'elle est accessible :

```
<#root>

firepower#

show run pim
```

```
pim rp-address 10.10.10.1

firepower#

show pim group-map



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

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


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

<#root>

```
firepower#

show pim group-map



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

224.0.0.0/4*        SM      config   1      192.168.2.2     RPF: Tunnel0,192.168.2.2 (us) <--- “us” mean


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

Avertissement : Le pare-feu ne peut pas être simultanément un RP et un FHR (sauf FTD version 10.1.0 et ultérieure, ASA 9.24.10 et ultérieure).

5. Vérifiez les résultats supplémentaires en fonction du rôle du pare-feu dans la topologie de multidiffusion et des symptômes du problème.

FHR

- Vérifiez l’état de l’interface Tunnel0. Cette interface est utilisée pour encapsuler le trafic

multicast brut à l'intérieur de la charge utile PIM et envoyer le paquet unicast au RP pour avec le bit de registre PIM défini :

<#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
```

- Vérifiez mroutes :

<#root>

```
firepower#

show mroute



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

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

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

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

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

Lorsque le pare-feu reçoit un paquet PIM avec un bit Register-Stop, Tunnel0 est supprimé de l'OIL. Le pare-feu arrête ensuite l'encapsulation et envoie le trafic multicast brut via l'interface de sortie :

<#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
```

- Vérifier les compteurs de registre PIM :

<#root>

```
firepower#

show pim traffic



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

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

Register                    0            8  <--- Sent to the RP



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



Assert                      0            0
Bidir DF Election           0            0

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

- Vérifiez les captures de paquets PIM de monodiffusion entre le pare-feu et le 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
```

- Collecter des sorties supplémentaires (x.x.x.x est le groupe de multidiffusion, y.y.y.y est l'IP RP). Il est recommandé de collecter les sorties quelques fois :

<#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
```

- Collecter le paquet d'interface multicast brut et les captures d'abandon ASP.

<#root>

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

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

- Messages Syslog : les ID courants sont 302015, 302016 et 710005.

RP

- Vérifiez l'état de l'interface Tunnel0. Cette interface est utilisée pour encapsuler le trafic multicast brut à l'intérieur de la charge utile PIM et envoyer un paquet unicast à FHR pour avec le bit d'arrêt PIM défini :

<#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        -
```

- Vérifiez mroutes :

<#root>

```
firepower#

show mroute



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


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




Incoming interface: Tunnel0


  RPF nbr: 192.168.2.2
  Immediate Outgoing interface list:


outside

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


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


  Incoming interface:

inside
```

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


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

- Vérifier les compteurs PIM :

<#root>

```
firepower #

show pim traffic


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

                              Received     Sent

Valid PIM Packets             948          755




Hello                         467          584




Join-Prune                    125          32




Register                      344          16




Register Stop                 12           129



Assert                        0            0
Bidir DF Election             0            0

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

- Collecter des sorties supplémentaires (x.x.x.x est le groupe de multidiffusion, y.y.y.y est l'IP RP). Il est recommandé de collecter les sorties quelques fois :

<#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

- Collecter le paquet d'interface multicast brut et les captures d'abandon ASP :

<#root>

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

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

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

- Syslog : les ID courants sont 302015, 302016 et 710005.

LHR

Examinez les étapes mentionnées dans la section pour le RP et les vérifications supplémentaires suivantes :

- Mroutes :

<#root>

firepower#

show mroute

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

Timers: Uptime/Expires
Interface state: Interface, State

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

  Incoming interface:

inside

  RPF nbr: 192.168.2.1
  Immediate Outgoing interface list:

outside

, Forward, 00:23:30/never

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

  Incoming interface:

inside

  RPF nbr: 192.168.2.1
  Inherited Outgoing interface list:

outside

, Forward, 00:23:30/never

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

  Incoming interface:

inside

  RPF nbr: 192.168.2.1
  Immediate Outgoing interface list:

outside

, Forward, 00:01:50/never

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

  Incoming interface:

inside

  RPF nbr: 192.168.2.1
  Inherited Outgoing interface list:

outside

, Forward, 00:01:50/never

- Groupes IGMP :

<#root>

firepower#

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

Interface: outside

Group: 230.1.1.1

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

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

Source list is empty
Interface: outside

Group: 230.1.1.2

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

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

```
Source list is empty
```

- Statistiques de trafic IGMP :

<#root>

```
firepower#

show igmp traffic
```

```
IGMP Traffic Counters
Elapsed time since counters cleared: 1d04h

                            Received     Sent
Valid IGMP Packets          2468         856
Queries                     2448         856
Reports                     20           0
Leaves                      0            0
Mtrace packets              0            0
DVMRP packets               0            0
PIM packets                 0            0

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

Commandes de dépannage PIM (Aide-mémoire)

Commande	Description
show running-config multicast-routing	Pour voir si le routage de multidiffusion est activé sur le pare-feu
show run mroute	Pour afficher les mroutes statiques configurées sur le pare-feu
show running-config pim	Pour afficher la configuration PIM sur le pare-feu

show pim interface	Pour voir quelles interfaces de pare-feu ont PIM activé et les voisins PIM.
show pim neighbor	Pour afficher les voisins PIM
show pim group-map	Pour afficher les groupes de multidiffusion mappés au RP
show mroute	Pour afficher la table de routage multidiffusion complète
show mroute 230.10.10.10	Pour afficher la table de multidiffusion d'un groupe de multidiffusion spécifique
show pim tunnel	Pour voir si un tunnel PIM est construit entre le pare-feu et le RP
show conn adresse détaillée RP_IP_ADDRESS	Pour voir si une connexion (tunnel PIM) est établie entre le pare-feu et le RP
show pim topology	Pour afficher le résultat de la topologie PIM du pare-feu
debug pim	Ce débogage affiche tous les messages PIM provenant et vers le pare-feu
debug pim group 230.10.10.10	Ce débogage affiche tous les messages PIM en provenance et à destination du pare-feu pour le groupe de multidiffusion spécifique
show pim traffic	Pour afficher des statistiques sur les messages PIM reçus et

	envoyés
show asp cluster counter	Vérifier le nombre de paquets traités dans le chemin lent ou le chemin rapide ou le point de contrôle
show asp drop	Pour afficher toutes les pertes de niveau logiciel sur le pare-feu
capture CAP interface INSIDE trace match pim any any	Pour capturer et suivre les paquets de multidiffusion PIM entrants sur le pare-feu
capture CAP interface INSIDE trace match udp host 224.1.2.3 any	Pour capturer et suivre le flux de multidiffusion entrant
show pim bsr-router	Pour vérifier qui est le routeur BSR sélectionné
show conn all address 24.1.2.3	Pour afficher la connexion de multidiffusion parente
show local-host 24.1.2.3	Pour afficher les connexions de multidiffusion enfant/stub

Pour plus d'informations sur les captures de pare-feu, vérifiez : Utiliser les captures Firepower Threat Defense et Packet Tracer

Problèmes connus

Limitations de multidiffusion Firepower :

- Ne prend pas en charge IPv6.
- La multidiffusion PIM/IGMP n'est pas prise en charge sur les interfaces d'une zone de trafic (EMCP).
- Le pare-feu ne peut pas être simultanément un RP et un FHR (sauf FTD version 10.1.0 et ultérieure, ASA 9.24.10 et ultérieure).

- La commande show conn all affiche uniquement les connexions de multidiffusion d'identité. Pour afficher la connexion de multidiffusion stub/secondaire, utilisez la commande show local-host <group IP>.

PIM n'est pas pris en charge sur un vPC Nexus

Si vous essayez de déployer une contiguïté PIM entre un vPC Nexus et le pare-feu, il y a une limitation Nexus comme décrit ici :

Topologies prises en charge pour le routage sur canal de port virtuel sur les plateformes Nexus

Du point de vue du pare-feu de nouvelle génération, vous voyez dans la capture avec trace ce drop :

<#root>

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

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

Le pare-feu ne peut pas terminer l'enregistrement RP :

<#root>

```
firepower#

show mroute 224.1.2.3


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

(*, 224.1.2.3), 01:05:21/never, RP 10.1.0.209, flags: SCJ
  Incoming interface: OUTSIDE
  RPF nbr: 10.1.104.10
```

```
  Immediate Outgoing interface list:
    Server_102, Forward, 01:05:21/never

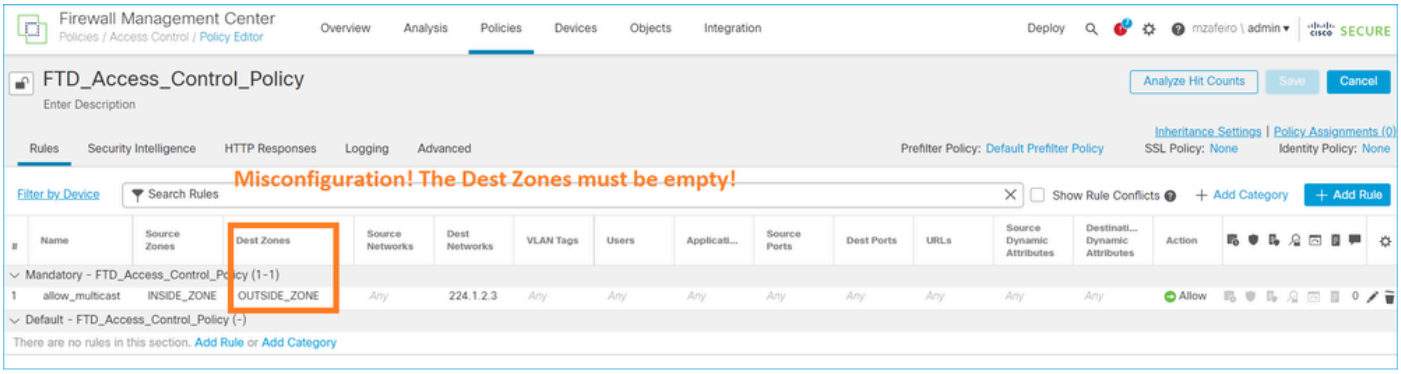
(10.1.1.48, 224.1.2.3), 00:39:15/00:00:04, flags: SFJT
  Incoming interface: NET102

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

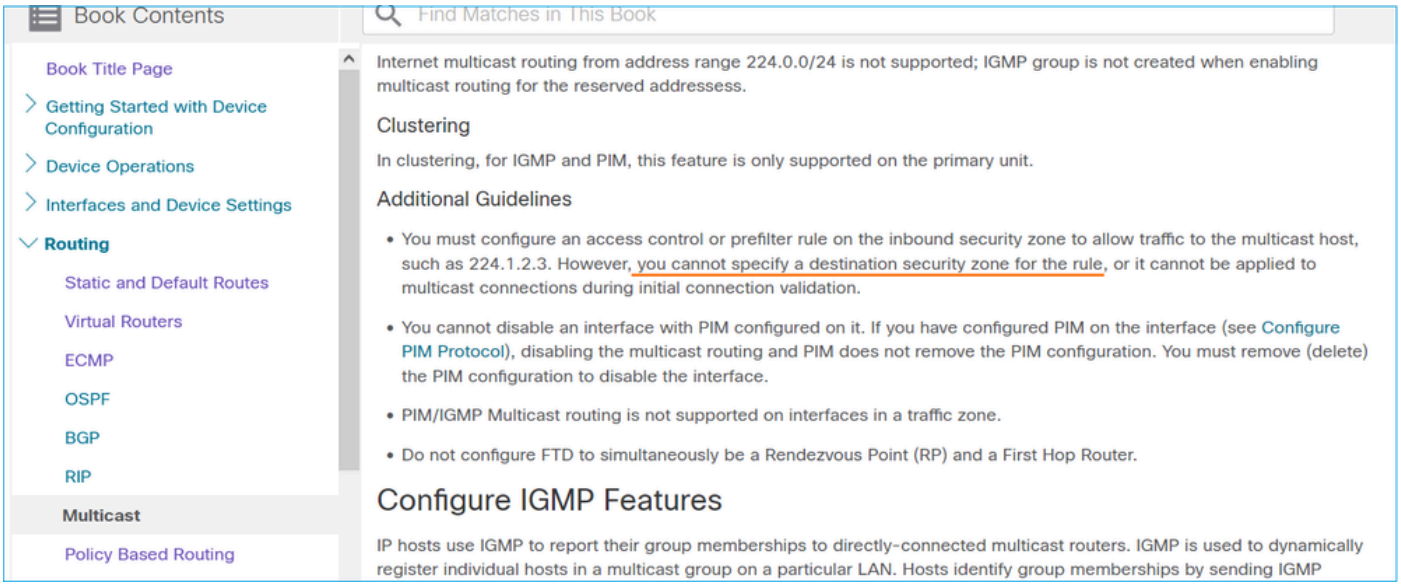
  Immediate Outgoing interface list:
    Tunnel0, Forward, 00:39:15/never
```

Zones de destination non prises en charge

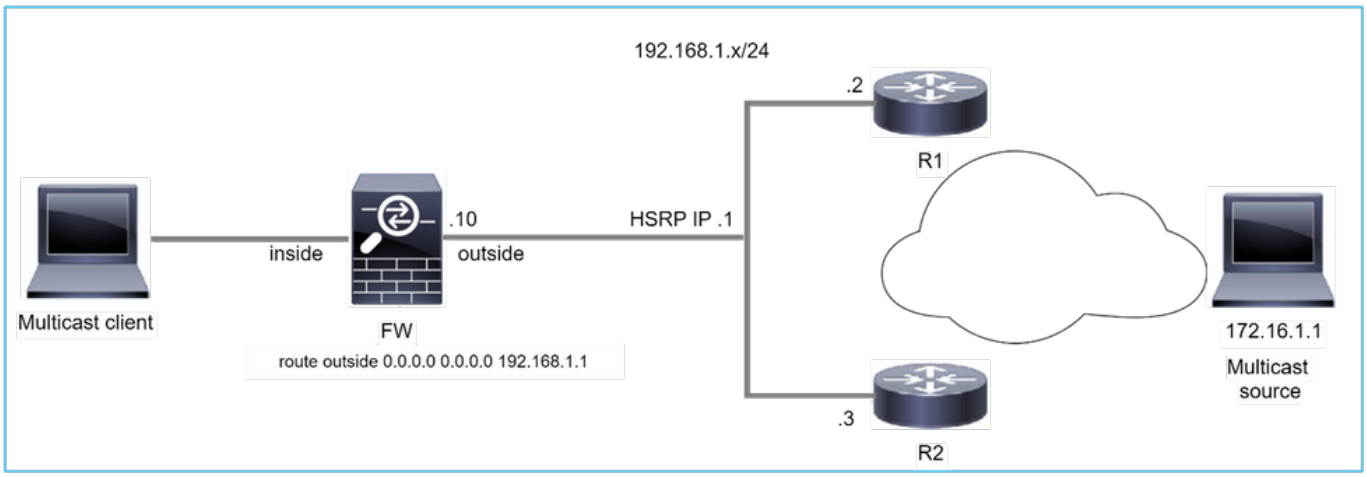
Vous ne pouvez pas spécifier une zone de sécurité de destination pour la règle de stratégie de contrôle d'accès qui correspond au trafic de multidiffusion :



Ceci est également documenté dans le guide de l'utilisateur FMC :



Le pare-feu ne transmet pas de messages PIM aux routeurs en amont en raison de HSRP



Dans ce cas, le pare-feu a une route par défaut via l'IP 192.168.1.1 du protocole HSRP (Hot Standby Redundancy Protocol) et le voisinage PIM avec les routeurs R1 et R2 :

<#root>

```
firepower#
```

show run route

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

Le pare-feu dispose d'une contiguïté PIM entre l'interface IP externe et l'interface physique sur R1 et 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)
```

Le pare-feu n'envoie pas de message PIM Join au réseau en amont. La commande de débogage PIM debug pim affiche ce résultat :

<#root>

```
firepower#
```

debug pim

```
...
```

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

Le document RFC 2362 indique qu'« un routeur envoie un message périodique de jonction/élagage à chaque voisin RPF distinct associé à chaque entrée (S, G), (*, G) et (*,*, RP). Les messages Join/Prune sont envoyés uniquement si le voisin RPF est un voisin PIM."

Pour atténuer le problème, l'utilisateur peut ajouter une entrée mroute statique sur le pare-feu. Le routeur doit pointer vers l'une des deux adresses IP d'interface du routeur, 192.168.1.2 ou 192.168.1.3, généralement l'adresse IP active du routeur HSRP.

Exemple :

<#root>

```
firepower#
```

show run mroute

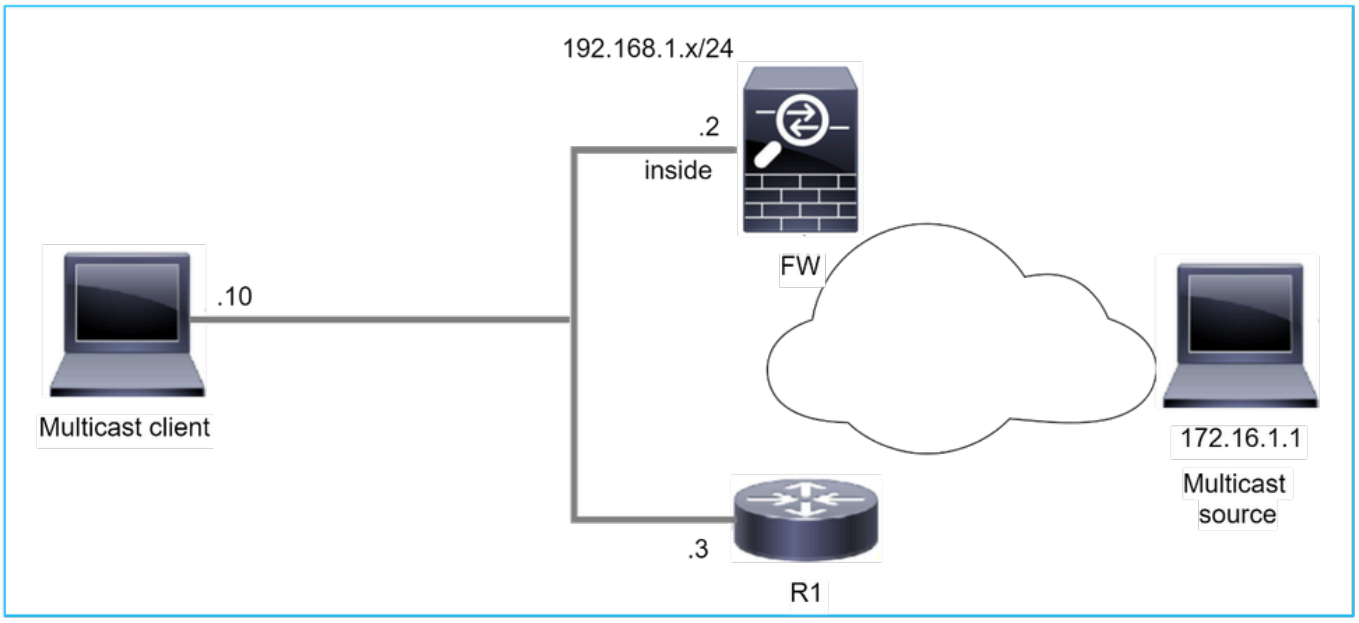
```
firepower#
```

mroute 172.16.1.1 255.255.255.255 192.168.1.2

Une fois la configuration de mroute statique en place, pour la recherche RPF, le pare-feu donne la préférence à la table de routage de multidiffusion au lieu de la table de routage de monodiffusion de l'ASA et envoie les messages PIM directement au voisin 192.168.1.2.

Remarque : Le mroute statique est, dans une certaine mesure, inutile la redondance HSRP, car le mroute accepte seulement 1 saut suivant par combinaison adresse/masque de réseau. Si le saut suivant spécifié dans la commande mroute échoue ou devient inaccessible, le pare-feu ne revient pas à l'autre routeur.

Le pare-feu n'est pas considéré comme LHR lorsqu'il n'est pas le DR dans le segment LAN



Le pare-feu a R1 comme voisins PIM dans le segment LAN. R1 est le DR PIM :

<#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)
```

Si une demande de jonction IGMP du client est reçue, le pare-feu ne devient pas le LHR.

Le mroute montre un Null supplémentaire comme l'OIL et a le drapeau Pruned :

<#root>

```
firepower#

show mroute


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

```
Timers: Uptime/Expires
Interface state: Interface, State


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

flags

: S

P

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


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

Pour faire du pare-feu le LHR, la priorité DR de l'interface peut être augmentée.

<#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
```

La commande de débogage PIM debug pim affiche ce résultat :

<#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

L'indicateur Pruned et la valeur Null sont supprimés de la mroute :

<#root>

firepower#

show mroute

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

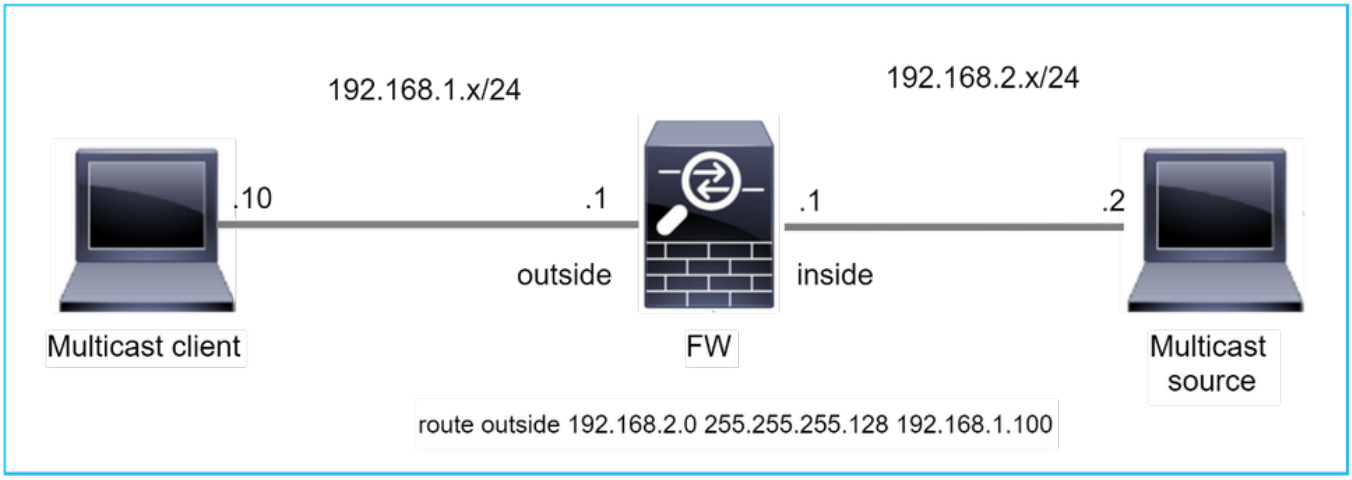
(*, 230.1.1.1), 16:48:23/never, RP 0.0.0.0, flags:

SCJ

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

```
    inside, Forward, 16:48:23/never
```

Le pare-feu abandonne les paquets multidiffusion en raison d'un échec de vérification de transfert de chemin inverse



Dans ce cas, les paquets UDP de multidiffusion sont abandonnés en raison d'une défaillance RPF, car le pare-feu a une route plus spécifique avec le masque 255.255.255.128 via l'interface externe.

<#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

Les captures d'abandon ASP indiquent la raison de l'abandon rpf violé :

```
<#root>

firepower#

show capture asp



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

21 packets captured



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


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

Les compteurs en échec RPF dans la sortie MFIB augmentent :

```
<#root>

firepower#

show mfib 230.1.1.1 count



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

Group: 230.1.1.1


  RP-tree:

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



...
```

```
firepower#

show mfib 230.1.1.1 count


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


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

La solution consiste à corriger l'échec du contrôle RPF. Une option consiste à supprimer la route statique.

S'il n'y a plus d'échec de contrôle RPF, les paquets sont transférés et le compteur de transfert dans la sortie MFIB augmente :

<#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,



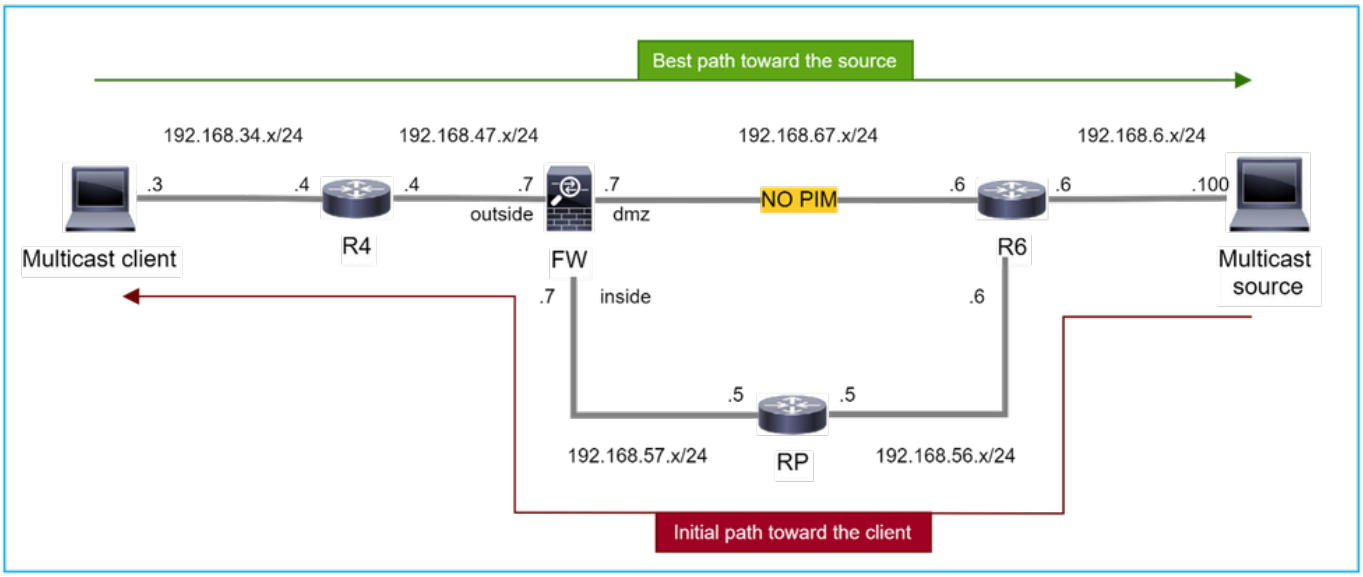
   Forwarding: 1044/10/528/41

, Other: 0/0/0

<--- Forward counter increased


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

Le pare-feu ne génère pas de jointure PIM lors du basculement PIM vers l'arborescence source



Dans ce cas, le pare-feu apprend le chemin vers la source de multidiffusion via l'interface dmz R4 > FW > R6, alors que le chemin de trafic initial de la source au client est R6 > RP > DW > R4 :

<#root>

```
firepower#
```

show route 192.168.6.100

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

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

```
  Routing Descriptor Blocks:
```

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

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

R4 lance la commutation SPT et envoie un message de jonction PIM spécifique à la source une fois que le seuil de commutation SPT est atteint. Dans le pare-feu, la commutation SPT n'a pas lieu, le mroute (S, G) n'a pas l'indicateur T :

<#root>

```
firepower#
```

show mroute

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

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

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

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

La commande debug debug pim du PIM affiche 2 requêtes PIM Join reçues de l'homologue R4 - pour (*, G) et (S, G). Le pare-feu a envoyé une demande de jointure PIM pour (*,G) en amont et n'a pas pu envoyer de demande spécifique à la source en raison d'un voisin non valide 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
```

La sortie des commandes show pim neighbor manque 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 est activé sur l'interface de pare-feu 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 est désactivé sur l'interface R6 :

<#root>

```
R6#

show ip interface brief


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

GigabitEthernet0/3         192.168.67.6    YES manual up                    up


Tunnel0                    192.168.56.6    YES unset  up                    up

R6#

show ip pim interface GigabitEthernet0/3 detail


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


PIM: disabled <--- PIM is disabled


  Multicast Tagswitching: disabled
```

La solution consiste à activer le protocole PIM sur l'interface GigabitEthernet0/3 sur R6 :

<#root>

```
R6(config-if)#

interface GigabitEthernet0/3


R6(config-if)#

ip pim sparse-mode
```

```
R6(config-if)#
*Apr 21 13:17:14.575: %PIM-5-NBRCHG: neighbor 192.168.67.7 UP on interface GigabitEthernet0/3

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

Le pare-feu installe l'indicateur T, qui indique la commutation SPT:

<#root>

```
firepower#

show mroute



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

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


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


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

Le pare-feu abandonne les premiers paquets en raison du taux de punt Limite

Lorsque le pare-feu reçoit les premiers paquets d'un nouveau flux de multidiffusion dans FP, un traitement supplémentaire par le PC peut être requis. Dans ce cas, le FP envoie les paquets au CP via SP (FP > SP > CP) pour des opérations supplémentaires :

- Création d'une connexion parent dans FP entre les interfaces d'entrée et les interfaces d'identité.
- Contrôles supplémentaires spécifiques à la multidiffusion, tels que la validation RPF, l'encapsulation PIM (dans le cas où le pare-feu est le FHR), le contrôle OIL, etc.
- Création d'une entrée (S, G) avec les interfaces entrantes et sortantes dans la table mroute.
- Création d'une connexion enfant/stub dans FP entre les interfaces entrantes et sortantes.

Dans le cadre de la protection du plan de contrôle, le pare-feu limite en interne le débit des paquets acheminés vers le PC.

Les paquets qui dépassent le débit sont abandonnés dans le avec la raison punt-rate-limit drop :

<#root>

```
firepower#

show asp drop


Frame drop:


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

Utilisez la commande show asp cluster counter pour vérifier le nombre de paquets de multidiffusion envoyés au point de connexion à partir du SP :

<#root>

```
firepower#

show asp cluster counter


Global dp-counters:

Context specific dp-counters:

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

```
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
```

Utilisez la commande show asp event dp-cp punt pour vérifier le nombre de paquets dans la file d'attente FP > CP, et le débit de 15 secondes :

<#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
```

Lorsque la mroute est remplie et que les connexions parent/enfant sont établies dans le FP, les paquets sont transférés dans le FP dans le cadre des connexions existantes. Dans ce cas, FP n'envoie pas les paquets au PC.

Comment le pare-feu traite-t-il les premiers paquets d'un nouveau flux multicast ?

Lorsque le pare-feu reçoit les premiers paquets d'un nouveau flux de multidiffusion dans le chemin de données, il effectue les actions suivantes :

1. Vérifie si la stratégie de sécurité autorise les paquets.
2. Transmet les paquets au PC via le chemin FP.
3. Crée une connexion parent entre les interfaces d'entrée et les interfaces d'identité :

<#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
```

SYSLOG:

<#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
```

Cette connexion est visible dans le résultat de la commande show conn all :

<#root>

```
firepower#

show conn all protocol udp


13 in use, 17 most used


UDP inside  192.168.1.100:12345 NP Identity Ifc  230.1.1.1:12345, idle 0:00:02, bytes 0, flags –
```

4. Le protocole CP engage le processus de multidiffusion pour des vérifications supplémentaires spécifiques à la multidiffusion, telles que la validation RPF, l'encapsulation PIM (dans le cas où le pare-feu est le FHR), la vérification OIL, etc.
5. Le PC crée une entrée (S, G) avec les interfaces entrantes et sortantes dans la mroute :

<#root>

```
firepower#

show mroute



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

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

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

Incoming interface: inside

RPF nbr: 192.168.2.1
Immediate Outgoing interface list:

outside, Forward, 00:00:32/00:02:57

6. Le point d'accès demande au point d'accès FP via CP > SP > chemin FP de créer une connexion enfant/stub entre les interfaces entrantes et sortantes :

Cette connexion n'est visible que dans le résultat de la commande 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
```

Dans les versions logicielles avec le correctif de l'ID de bogue Cisco CSCwe21280, le message syslog 302015 pour la connexion enfant/stub est également généré :

<#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
```

Lorsque les connexions parent et enfant/stub sont établies, les paquets entrants correspondent à la connexion existante et sont transférés dans 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
```

Filtrer le trafic multidiffusion ICMP

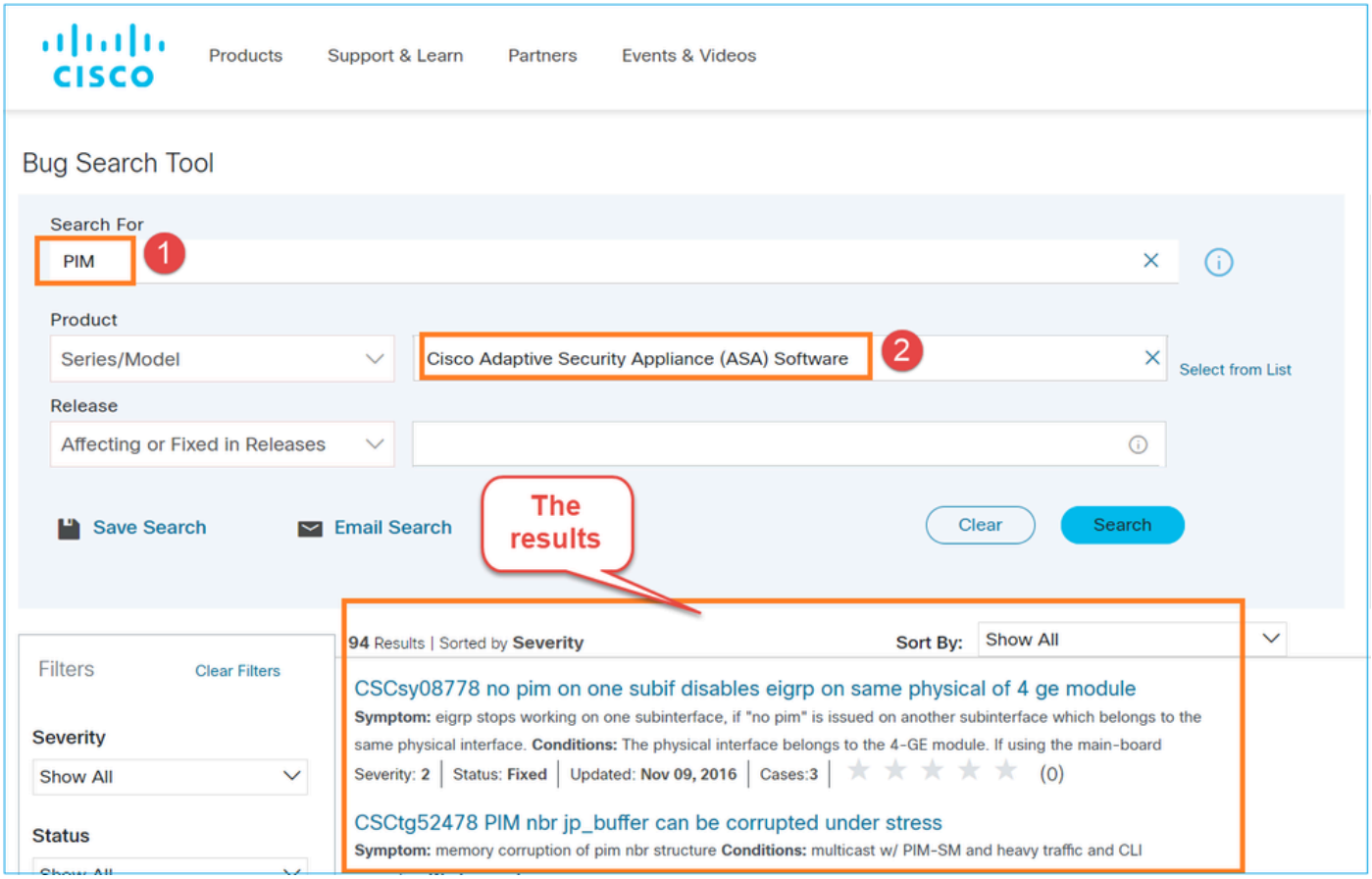
Vous ne pouvez pas filtrer le trafic multidiffusion ICMP avec une liste de contrôle d'accès. Vous devez utiliser la stratégie du plan de contrôle (ICMP) :

L'ID de bogue Cisco CSCsl26860 ASA ne filtre pas les paquets ICMP de multidiffusion

Défauts de multidiffusion PIM connus

Vous pouvez utiliser l'outil de recherche de bogues pour les défauts connus : https://bst.cloudapps.cisco.com/bugsearch

La plupart des défauts ASA et FTD sont répertoriés sous le produit « Logiciel Cisco Adaptive Security Appliance (ASA) » :



CSCwt99960 Le pare-feu en mode Bidir PIM limite le trafic de multidiffusion et supprime les paquets dépassant la limite de débit avec une raison de suppression ASP

CSCwu19440 Le résultat de la commande « show pim topology » doit être lisible

CSCwu18794 "Le trafic de multidiffusion est limité en débit et abandonné avec punt-rate-limit si aucune jonction spécifique à la source n'est reçue ou si aucune commutation LHR SPT n'est effectuée"

CSCwu18733 "Joindre/élaguer pour PIM SSM ne sont pas envoyés vers la source de multidiffusion"

CSCwu18098 "Paquets PIM non générés après la désactivation du transfert IGMP sur les interfaces participantes"

CSCwu17380 "Le paquet d'enregistrement PIM est envoyé à 0.0.0.0 si la route par défaut est configurée"

CSCwh76458 ASA/FTD supprime le trafic de multidiffusion lorsqu'il n'y a aucune entrée mroute lors de l'utilisation de Bidir PIM

CSCwq86288 ENH : Amélioration des débogages/syslogs pour le flux de messages du registre PIM

CSCvy36751 : L'indicateur de registre S, G mroute F n'est pas effacé lorsque le paquet d'arrêt

de registre PIM est reçu
CSCvy18138: Le compteur d'envoi de registre PIM n'augmente pas lorsque des paquets encapsulés avec indicateur de registre sont envoyés au RP

CSCv16723 ENH : Permet de supprimer manuellement les entrées mroute et mfib
CSCvy51227 ENH : Renommez « show pim traffic » en « show pim counters »
CSCvy51232 ENH : Ajouter la prise en charge de plusieurs groupes de multidiffusion dans des conditions de débogage
CSCvy60096 ENH : Afficher l'indicateur d'interface sortante du gagnant Assert dans 'show mroute'
CSCvy67176 ENH : Prise en charge du filtrage des tables mroute/mrib/mfib en fonction des entrées des arborescences partagées ou source
CSCvy73891 ENH : Générer un message syslog lorsque Rendezvous Point (RP) n'est pas configuré ou est inaccessible
CSCvy67187 ENH : Prise en charge du filtrage des tables mroute/mfib en fonction de l'interface sortante

CSCwe21280 Les messages syslog générés ou désactivés par la connexion multidiffusion ne sont pas toujours générés

CSCwd41553 Les paquets du registre PIM ne sont pas envoyés au point de rendez-vous (RP) en raison de l'état d'interruption de l'interface du tunnel PIM

CSCwe21187 ASA/FTD peut abandonner des paquets de multidiffusion en raison de la raison d'abandon d'ASP no-mcast-intrf jusqu'à expiration du délai d'attente UDP

CSCwf07767 ASA/FTD peut générer des messages syslog d'interruption de connexion de multidiffusion en double

CSCvu68826 Entrées de connexion de données multidiffusion introuvables sur ASA après le démarrage du trafic multidiffusion

CSCv14440 DOC : Connexions de données multidiffusion à afficher sous « show local-host »

CSCvx54396 Échec de déploiement de stratégie intermittent lorsque le routage multidiffusion est activé
CSCvy24859 Les paquets multidiffusion peuvent être abandonnés avec une raison d'abandon ASP punt-rate-limit

CSCwe21280 Les messages syslog générés ou désactivés de connexion multidiffusion ne sont pas toujours générés

CSCwe21280 ASA/FTD peut abandonner des paquets de multidiffusion en raison d'une raison d'abandon non mcast-intrf ASP jusqu'à expiration du délai d'attente UDP

CSCwd4153 Les paquets du registre PIM ne sont pas envoyés au point de rendez-vous (RP) en raison de l'état d'interruption de l'interface du tunnel PIM

CSCwb94431 MFIB RPF a échoué au compteur au lieu d'autres abandons incréments lorsque la liste d'interfaces sortantes est Null

CSCwf07767 ASA/FTD peut générer des messages syslog d'interruption de connexion de multidiffusion en double

CSCwe61928 Les paquets du registre PIM ne sont pas envoyés au RP après un rechargement si FTD utilise une passerelle par défaut pour atteindre le RP

CSCwj56862 ASA/FTD n'envoie pas de paquets PIM Null-Register lorsque la route par défaut est utilisée pour atteindre RP

CSCwf52220 ENH : Prise en charge du délai de propagation et de l'intervalle de remplacement configurables pour PIM

Informations connexes

- Dépannage de la multidiffusion ASA et problèmes courants
- Multidiffusion Firepower Management Center
- Résumé des indicateurs de multidiffusion Firepower

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.