Dépannage du trafic multidiffusion ne passant pas par le pare-feu FTD avec configuration Bidir PIM

Table des matières

Problème

Tous ces symptômes sont visibles :

- Le trafic multidiffusion ne fonctionne plus sur Firewall Threat Defense (FTD) pour un groupe de multidiffusion spécifique.
- Il n'existe aucune route de multidiffusion (mroutes) sur le FTD pour le groupe (224.2.2.2 dans cet exemple).

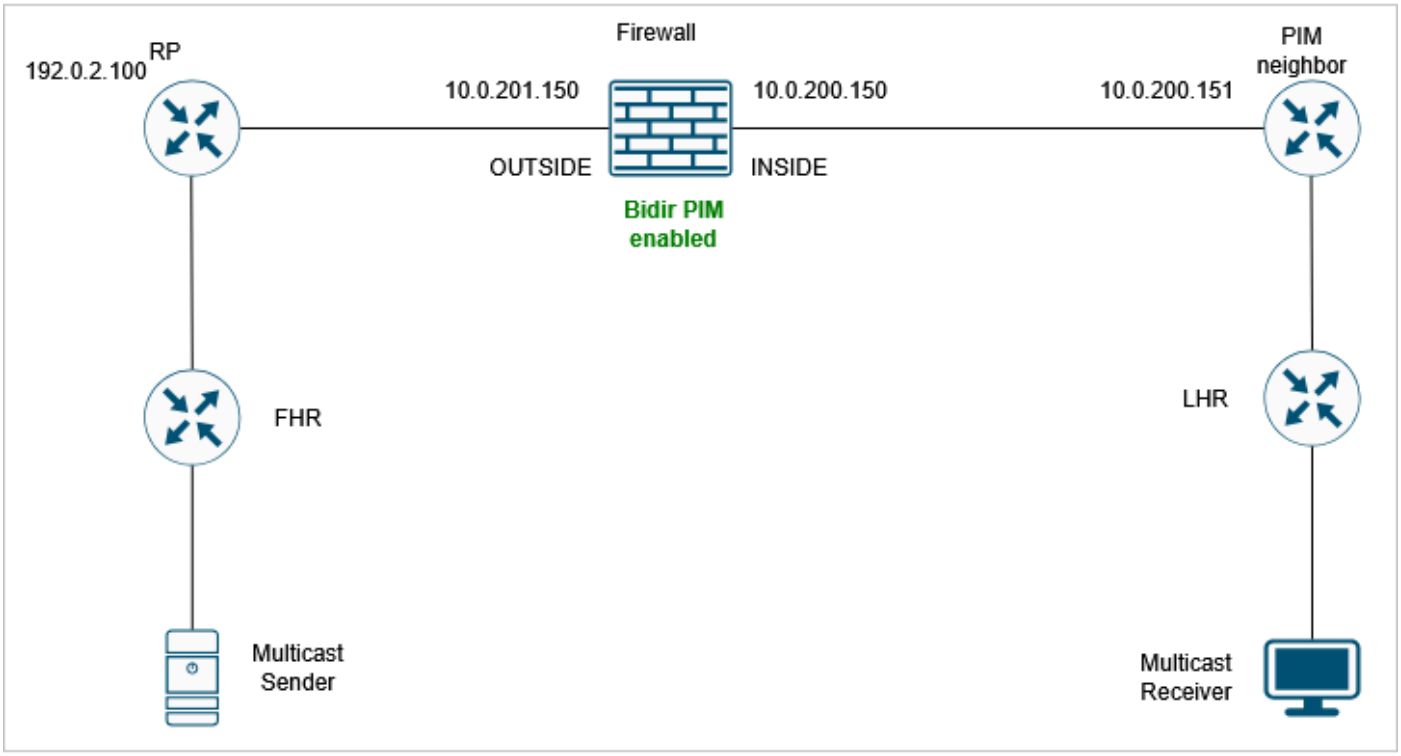
<#root>

```
device#

show mroute 224.2.2.2


No mroute entries found.
device#
```

Environnement

- D'abord vu dans la version FTD 7.4. D'autres versions logicielles, y compris ASA (Adaptive Security Appliance), peuvent également être affectées.
- Le protocole PIM (Bidirectional Protocol Independent Multicast) est activé sur le pare-feu.

Topologie



image_en_ligne_0.png

Résolution

Étape 1: Vérifiez la configuration de multidiffusion actuelle.

Examinez la configuration de routage de multidiffusion existante sur tous les périphériques du chemin réseau pour identifier les erreurs de configuration ou les paramètres manquants qui pourraient empêcher le trafic de multidiffusion de traverser le pare-feu.

Sur le pare-feu, il y a une configuration PIM bidirectionnelle :

<#root>

```
device#
```

show run pim

```
pim rp-address 192.0.2.100 bidir
```

Étape 2: Vérifiez les voisins PIM.

Vérifiez que les voisins de multidiffusion sont correctement affichés sur le pare-feu :

<#root>

```
device#

show pim neighbor


Neighbor Address  Interface          Uptime    Expires DR pri Bidir
10.0.200.151      INSIDE             19:13:30  00:01:24 1 (DR)
10.0.201.200      OUTSIDE            00:01:31  00:01:42 1 (DR)

B
```

Dans la sortie, notez que le voisin 10.0.201.200 a l'indicateur Bidir B, alors que le voisin 10.0.200.151 ne l'a pas.

Étape 3: Activez le débogage PIM pour le groupe de multidiffusion 224.2.2.2 :

<#root>

```
FPR3100-14#

debug pim group 224.2.2.2


IPv4 PIM group debugging is on
 for group 224.2.2.2
```

Le débogage montre qu'il y a un paquet PIM Join/Prune qui est rejeté en raison de 'no bidir df election' :

<#root>

```
IPv4 PIM: J/P entry: Join root: 192.0.2.100 group: 224.2.2.2 flags:  RPT WC S
IPv4 PIM: (*,224.2.2.2) J/P with RP 192.0.2.100 on INSIDE

discarded, no bidir df election-state on this intf
```

Étape 4: Activez les captures PIM vers le voisin PIM 10.0.200.151. L'objectif est d'obtenir une meilleure visibilité sur le contenu des paquets :

<#root>

```
device#

capture CAPI interface INSIDE trace match pim host 10.0.200.151 any
```

Étape 5: Collectez la capture du pare-feu à partir du périphérique FTD :

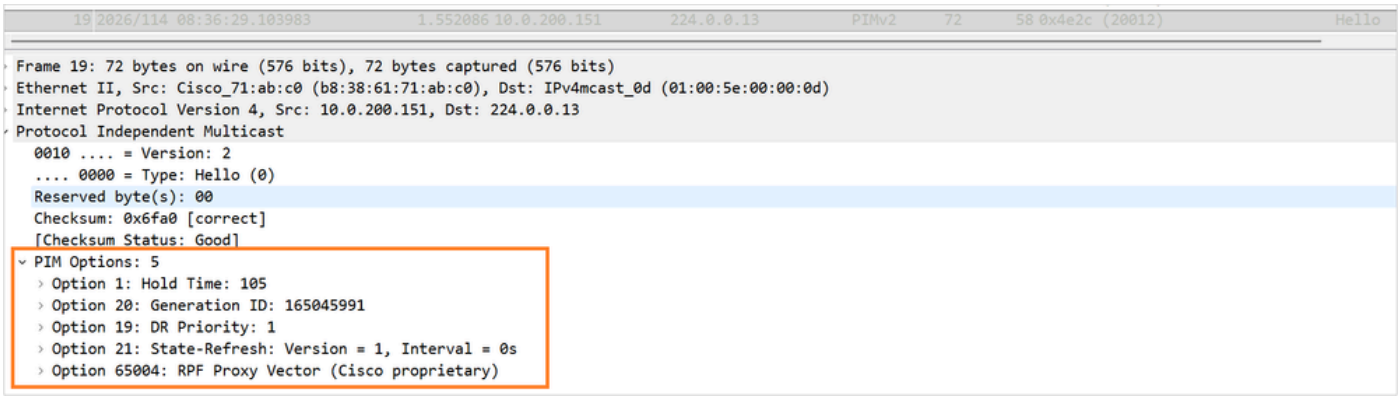
<#root>

```
device#

copy /pcap capture:CAPI CAPI.pcap


Source capture name [CAPI]?
Destination filename [CAPI.pcap]?
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
!
28 packets copied in 0.0 secs
```

Collectez le fichier pcap à partir de FMC en suivant la procédure décrite à l'adresse https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html

Étape 6: Capturer l'analyse.

Le paquet Hello PIM contient les options suivantes :



PIM_Hello_Options_no-bidir-capable.png

Notez l'absence de l'indicateur Bidir.

Étape 7: Activez le protocole PIM bidirectionnel sur le voisin 10.0.200.151.

Maintenant, l'indicateur Bidir B PIM est affiché pour les deux voisins :

<#root>

device#

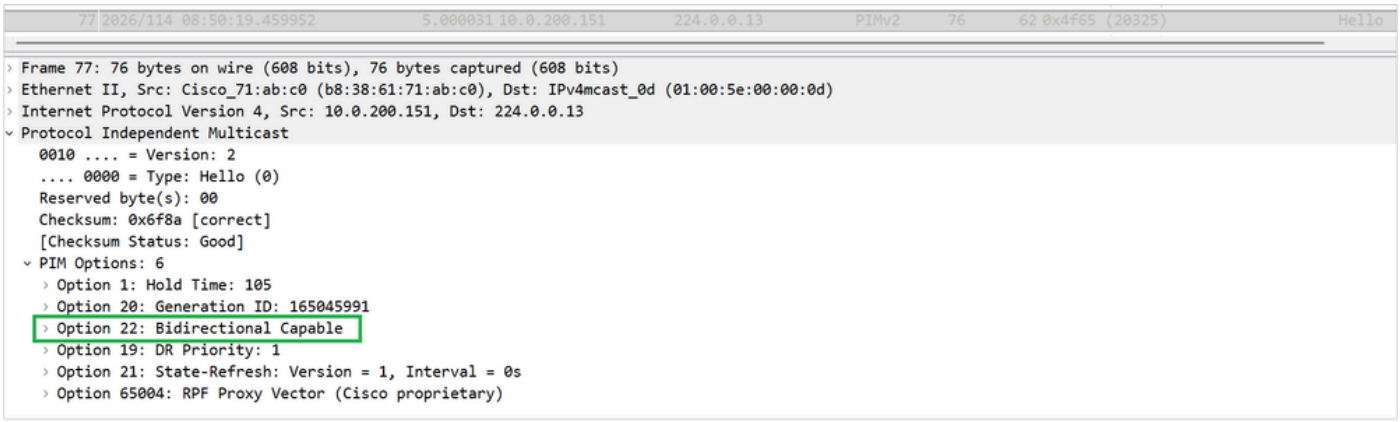
show pim neighbor

Neighbor Address Interface Uptime Expires DR pri Bidir
10.0.200.151 INSIDE 19:34:26 00:01:38 1 (DR)

B

10.0.201.200 OUTSIDE 00:22:27 00:01:23 1 (DR) B

Étape 8: Collectez une nouvelle capture et vérifiez les options Hello PIM pour le voisin 10.0.200.151. L'option PIM 22 (Bidirectional Capable) s'affiche :



PIM_Hello_Options_option2.png

Étape 9: Vérifiez que la mroute du groupe de multidiffusion 224.2.2.2 est maintenant affichée :

<#root>

device#

show mroute

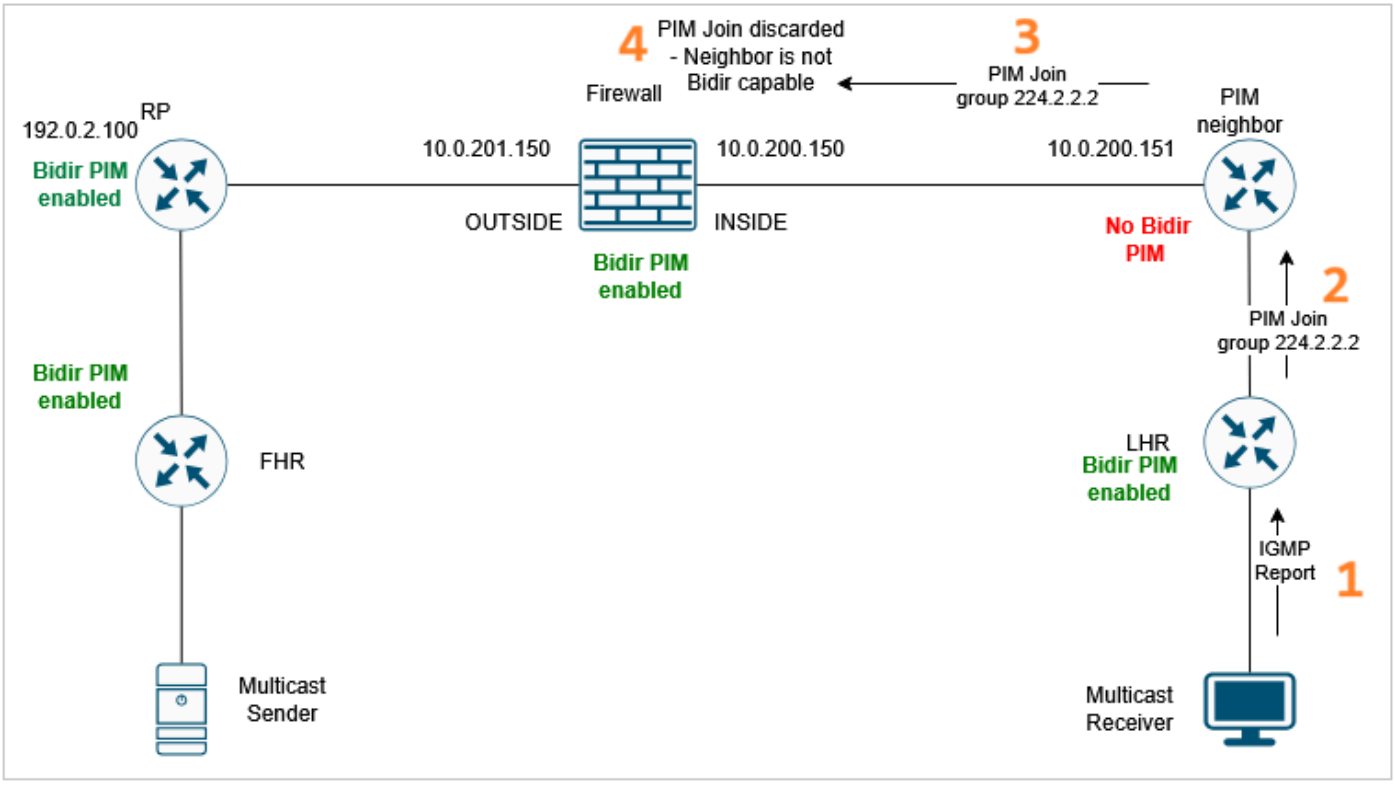
```
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State
(*, 224.0.1.40), 19:41:44/never, RP 0.0.0.0, flags: DPC
  Incoming interface: Null
  RPF nbr: 0.0.0.0
  Immediate Outgoing interface list:
    INSIDE, Null, 19:41:44/never
```

(*, 224.2.2.2)

```
, 00:06:29/00:02:53, RP 192.0.2.100, flags: B
  Bidir-Upstream: OUTSIDE
  RPF nbr: 10.0.201.200
  Immediate Outgoing interface list:
    INSIDE, Forward, 00:06:29/00:02:53
```

Motif

La défaillance du trafic de multidiffusion est due à une configuration PIM bidirectionnelle et de multidiffusion incorrecte ou incomplète sur le périphérique réseau adjacent. Le problème de configuration spécifique a entraîné l'abandon par FTD du message PIM Join/Prune pour le groupe de multidiffusion spécifique. Par conséquent, le pare-feu n'a pas pu créer la mroute pour le trafic de multidiffusion. Pour que le trafic de données de multidiffusion passe par le plan de données du pare-feu, le plan de contrôle (PIM) doit établir la mroute appropriée.



Cause.png

Autres informations utiles

- https://datatracker.ietf.org/doc/html/rfc5015#section-3.7.4

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.