Dépannage des pertes de paquets multidiffusion sur le pare-feu avec configuration Bidir PIM

Table des matières

Problème

Ces symptômes sont observés sur Secure Firewall Threat Defense (FTD) qui participe en tant que saut intermédiaire dans le domaine de routage multicast avec le protocole bidirectionnel BIDIR-PIM (Bidirectional Protocol Independent Multicast), une variante de PIM Sparse-Mode (PIM-SM).

1. La mroute du groupe de multidiffusion spécifique 232.4.4.4 est absente :

<#root>

device#

show mroute 232.4.4.4

No mroute entries found.

2. Le compteur Other drops pour la plage de groupes 232.0.0.0/8 dans la sortie de la commande show mfib count augmente :

<#root>

device#

show mfib count

```
IP Multicast Statistics
6 routes, 3 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: 224.0.1.39
  RP-tree:
   Forwarding: 0/0/0/0, Other: 0/0/0
Group: 224.0.1.40
  RP-tree:
   Forwarding: 0/0/0/0, Other: 0/0/0

Group: 232.0.0.0/8

  RP-tree:
   Forwarding: 0/0/0/0,

Other: 2551

/0/

2551 <----

device#

show mfib count

IP Multicast Statistics
6 routes, 3 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: 224.0.1.39
  RP-tree:
   Forwarding: 0/0/0/0, Other: 0/0/0
Group: 224.0.1.40
  RP-tree:
   Forwarding: 0/0/0/0, Other: 0/0/0

Group: 232.0.0.0/8

```
  RP-tree:
   Forwarding: 0/0/0/0,

Other: 2864

/0/

2864

<----
```

3. Les paquets multidiffusion sont abandonnés avec la limite de débit Punt dépassée (punt-rate-limit) raison de l'abandon dans le chemin de sécurité accéléré (ASP). Le compteur de gouttes augmente continuellement :

<#root>

```
device#

cap capi trace interface inside match udp any host 232.4.4.4


device#

show cap capi trace


   2: 19:36:08.509205

192.168.1.2.12345 > 232.4.4.4.12345

:  udp 0
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 13056 ns
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 13056 ns
Config:
Implicit Rule
Additional Information:
MAC Access list
```

```
Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Elapsed time: 2560 ns
Config:
Additional Information:
Found flow with id 4876, using existing flow

Result:
input-interface: inside
input-status: up
input-line-status: up
Action: drop
Time Taken: 28672 ns

Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (NA



device#

show asp drop



Frame drop:

  Punt rate limit exceeded (punt-rate-limit)                                    142


  FP L2 rule drop (l2_acl)                                                        6

Last clearing: 19:38:00 UTC Apr 29 2026 by admin

Flow drop:

Last clearing: 19:38:00 UTC Apr 29 2026 by admin
…
device#

show asp drop



Frame drop:

  Punt rate limit exceeded (punt-rate-limit)                                    780


  FP L2 rule drop (l2_acl)                                                       37
```

4. Les captures de l’interface externe n’affichent aucun paquet de multidiffusion de sortie :

<#root>

device#

capture capo type raw-data interface outside match udp any host 232.4.4.4

device#

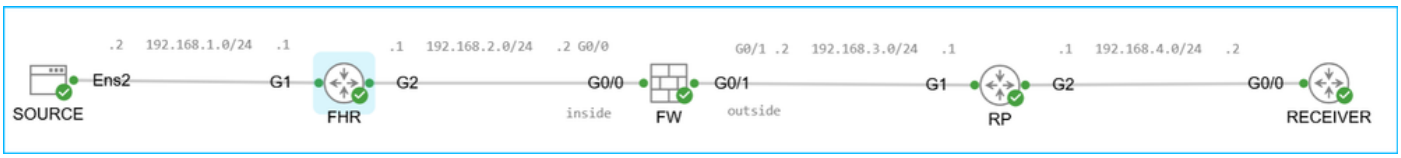
show cap capo

0 packet captured

0 packet shown

Environnement

Topologie



topologie.png

Points clés

- Les homologues du domaine de multidiffusion utilisent BIDIR-PIM.

- Le routeur de cet article fait référence à un routeur Cisco tel que CSR ou ASR.
- Rendezvous Point (RP) est ASR1001-X exécutant le logiciel Cisco IOS XE, version 17.09.08. D'autres plates-formes et versions logicielles peuvent également être affectées.
- Le routeur de premier saut (FHR) est C9200L-48T-4G exécutant le logiciel Cisco IOS XE, version 16.12.04. D'autres plates-formes et versions logicielles peuvent également être affectées.
- L'adresse de point de rendez-vous (RP) 10.4.4.4 sur l'interface de bouclage 0 pour la plage de multidiffusion entière 224.0.0.0/8 est propagée dynamiquement dans le domaine de multidiffusion à l'aide du routeur de démarrage PIM (BSR). Les déploiements avec la configuration d'adresse RP PIM statique peuvent également être affectés.

  Configuration PIM sur RP :

  <#root>

```
device#
show run interface loopback0


interface Loopback0
 description LOO
 ip address 10.4.4.4 255.255.255.255
 ip pim sparse-mode

device(config)#
ip pim bidir-enable


device(config)#
ip pim bsr-candidate Loopback0 0 1


device(config)#
ip pim rp-candidate Loopback0 interval 10 priority 1 bidir
```

- Par souci de simplicité, dans ce cas, le RP est représenté comme connecté au récepteur, c'est-à-dire qu'il est également le routeur de dernier saut (LHR). Ceci est facultatif.
- Le pare-feu est le pare-feu Secure Firewall 3110 exécutant la version 7.6.4. D'autres plates-formes de pare-feu, versions logicielles et logiciels ASA (Adaptive Security Appliance) peuvent également être affectés.
- Sur le pare-feu, le routage multicast est activé et il y a une contiguïté PIM avec le routeur de premier saut (FHR) et le RP avec la capacité PIM BIDIR :

```
<#root>

device#

show run multicast-routing


multicast-routing


device#

show pim neighbor


Neighbor Address  Interface          Uptime    Expires DR pri Bidir

192.168.2.1       inside             1d12h     00:01:40 1

B


192.168.3.1       outside            1d12h     00:01:35 1

B
```

- Sur le pare-feu, malgré l'utilisation de PIM BSR, l'adresse PIM RP 10.4.4.4 est configurée manuellement. Il s'agit d'une configuration redondante. Par conséquent, il existe 2 mappages RP-à-groupe entre le groupe 224.0.0.0/4 et l'adresse RP 10.4.4.4 :

```
<#root>

device#

show run pim


pim rp-address 10.4.4.4 bidir


device#

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*        BD      BSR      0      10.4.4.4   RPF: outside,192.168.3.1 <-- * means the ma
```

```
224.0.0.0/4         BD      config   0      10.4.4.4   RPF: outside,192.168.3.1

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

Résolution

Avant de continuer, vérifiez la section Cause suivante.

Les abandons de paquets sur le pare-feu sont attendus en raison d'une incompatibilité entre la configuration prévue (BIDIR-PIM) et le trafic qui doit être géré à l'aide de PIM SSM.

Si la configuration prévue est BIDIR-PIM, considérez ces options :

- Utilisez uniquement des groupes SSM non-PIM.
- Si des groupes PIM SSM doivent être utilisés, assurez-vous que le pare-feu gère les groupes de multidiffusion de la plage PIM SSM comme des adresses de groupe non-SSM. Reportez-vous à la section Questions/Réponses pour plus d'informations.
- Prenons l'ID de bogue Cisco CSCwt9960.

Motif

L'adresse 232.4.4.4 appartient à la plage de groupes SSM (Source Specific Multicast) réservée par l'IANA (Internet Assigned Numbers Authority). Le pare-feu réserve automatiquement la plage 232.0.0.0/8 pour PIM SSM :

<#root>

```
device#

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*        BD      BSR      0      10.4.4.4   RPF: outside,192.168.3.1
224.0.0.0/4         BD      config   0      10.4.4.4   RPF: outside,192.168.3.1
224.0.0.0/4         SM      static   0      0.0.0.0         RPF: ,0.0.0.0
```

Principaux aspects de PIM SSM :

- Il construit des arborescences basées sur la source et utilise (S, G) mroutes.
- L'infrastructure d'arborescence partagée basée sur RP du protocole PIM-SM n'est pas requise. En d'autres termes, RP ou (*, G) mroutes ne sont pas utilisés.
- Les récepteurs rejoignent généralement l'arborescence de multidiffusion en utilisant le protocole IGMPv3 (Internet Group Management Protocol Version 3) avec « filtrage de source », c'est-à-dire la capacité d'un système à signaler un intérêt pour la réception de paquets uniquement à partir d'adresses source spécifiques, ou à partir de toutes les adresses source sauf des adresses source spécifiques, envoyées à une adresse de multidiffusion particulière.

Principaux aspects du BIDIR-PIM :

- Il construit des arborescences partagées bidirectionnelles connectant des sources et des récepteurs multidiffusion.
- Les arborescences bidirectionnelles sont construites à l'aide d'un mécanisme de sélection DF (Designated Forwarder) à sécurité intégrée fonctionnant sur chaque liaison d'une topologie de multidiffusion.
- Avec l'aide du DF, les données de multidiffusion sont transmises nativement des sources au RP et donc le long de l'arborescence partagée aux récepteurs sans nécessiter d'état spécifique à la source.
- BIDIR-PIM n'utilise pas les entrées SPT (Shortest Path Trees) et (S, G).
- Les homologues BIDIR-PIM créent des arbres partagés à l'aide d'entrées (*, G). Cette entrée pour un groupe de multidiffusion particulier doit exister dans la table mroute.

Comparer les aspects clés de PIM SSM et BIDIR-PIM montre que PIM SSM et BIDIR-PIM ont des

fonctionnalités mutuellement exclusives.

Dans ce cas, le domaine de multidiffusion est configuré pour utiliser BIDIR-PIM, tandis que le groupe de multidiffusion appartient à la plage réservée par l'IANA et le pare-feu pour PIM SSM. Puisque le domaine de multidiffusion utilise BIDIR-PIM, (S, G) mroutes requises pour PIM SSM ne sont pas disponibles sur le pare-feu. En raison du manque de mroutes, l'interface de sortie/sortie pour le trafic de multidiffusion n'est pas disponible. L'absence d'interface de sortie/de sortie entraîne des abandons de paquets dans la base d'informations de transfert multidiffusion (MFIB). Les abandons peuvent être vérifiés à l'aide des commandes show mfib ou show mfib count :

<#root>

```
device#

show mfib count



IP Multicast Statistics
6 routes, 3 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: 224.0.1.39
  RP-tree:
   Forwarding: 0/0/0/0, Other: 0/0/0
Group: 224.0.1.40
  RP-tree:
   Forwarding: 0/0/0/0, Other: 0/0/0

Group: 232.0.0.0/8



  RP-tree:
   Forwarding: 0/0/0/0, Other:

333797

/0/

333797
```

Le pare-feu tente de résoudre l'interface de sortie/sortie en engageant le point de contrôle (CP). Il

s'agit du composant essentiel du pare-feu, principalement responsable des fonctions de gestion et de plan de contrôle, telles que les protocoles de routage, l'accès à la gestion, la gestion du basculement/cluster, la gestion des paquets destinés à l'interface du pare-feu, les adresses IP de multidiffusion ou de diffusion, etc.

Pour éviter de surcharger le point de contrôle, le pare-feu dispose de mécanismes de protection intégrés. Par exemple, le pare-feu limite le débit des paquets envoyés du plan de données (DP) au point de contrôle. Les paquets dépassant le débit sont abandonnés avec la limite de débit punt dépassée (punt-rate-limit) raison de l'abandon ASP. La fréquence de points peut être vérifiée dans la sortie de la commande show asp event dp-cp punt | begin EVENT-TYPE, commande :

```
<#root>
device#

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


EVENT-TYPE          ALLOC ALLOC-FAIL ENQUEUED ENQ-FAIL  RETIRED 15SEC-RATE

punt              1264746          0  1264746        0  1264746         44

<-- 15-second punt rate

  multicast       1250020          0  1250020        0  1250020         44



  pim               14726          0    14726        0    14726          0
```

En résumé, la conclusion est que les abandons de paquets sur le pare-feu sont attendus en raison d'une incompatibilité entre la configuration prévue (BIDIR-PIM) et le trafic qui doit être géré à l'aide de PIM SSM.

Q&R

Dans cette section, le terme « routeur » fait référence à un routeur Cisco tel que CSR et le terme « pare-feu » fait référence aux pare-feu Cisco exécutant ASA ou FTD.

Q : Le pare-feu réserve-t-il automatiquement 232.0.0.0/8 pour PIM SSM ?

A : Oui. Contrairement, par exemple, aux routeurs comme CSR, aucune configuration spécifique n'est requise. Sur les routeurs, la plage PIM SSM nécessite une configuration explicite :

<#root>

```
device(config)#

ip pim ssm ?


  default  Use 232/8 group range for SSM


  range    ACL for group range to be used for SSM
```

Q : Le compteur MFIB Other Drops est-il spécifique au pare-feu ?

A : Non. Un compteur similaire existe sur les routeurs Cisco avec routage multidiffusion.

Q : Un autre périphérique, comme un routeur à la place d'un pare-feu, abandonnerait-il également les paquets envoyés au groupe 232.4.4.4 ?

A : Cela dépend de la façon dont le routeur traite l'adresse 232.4.4.4. Contrairement aux pare-feu, les routeurs par défaut ne réservent pas la plage 232.0.0.0/8 pour PIM SSM. Cependant, si les deux modules PIM SSM et BIDIR-PIM sont activés, et que le routeur est un RP compatible BIDIR-PIM ou reçoit un mappage RP-à-groupe avec l'indicateur Bidir et reçoit des paquets de multidiffusion envoyés à la plage PIM SSM, les paquets sont abandonnés et le compteur MFIB « Autre » augmente :

<#root>

```
device#

show run | i pim
```

ip pim bidir-enable

no ip pim autorp

ip pim ssm default

device#

show ip pim rp mapping

Auto-RP is not enabled
PIM Group-to-RP Mappings

Group(s) 224.0.0.0/4
  RP 10.4.4.4 (?), v2,

bidir <-- mapping has the bidir flag

    Info source: 10.4.4.4 (?), via bootstrap, priority 1, holdtime 150
         Uptime: 17:32:39, expires: 00:02:05

device#

show ip mfib count

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)
Default
 9 routes, 6 (*,G)s, 3 (*,G/m)s
Group: 224.0.0.0/4
  RP-tree,
   SW Forwarding: 1/0/28/0, Other: 41037/41037/0
   HW Forwarding: 3428217/0/64/0, Other: 0/0/0

Group: 232.0.0.0/8

  RP-tree,

   SW Forwarding: 0/0/0/0, Other: 97/97

/0 <----
   HW Forwarding: 0/0/0/0, Other: 0/0/0

```
device#
```

show ip mfib count

```
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)
Default
 9 routes, 6 (*,G)s, 3 (*,G/m)s
Group: 224.0.0.0/4
  RP-tree,
   SW Forwarding: 1/0/28/0, Other: 41037/41037/0
   HW Forwarding:   3428217/0/64/0, Other: 0/0/0
```

Group: 232.0.0.0/8

```
  RP-tree,
SW Forwarding: 0/0/0/0,
```

Other: 106/106

```
/0 <----
   HW Forwarding:   0/0/0/0, Other: 0/0/0
```

Notez que contrairement au pare-feu avec le compteur croissant « Other drops » sur le routeur, le compteur croissant est « RPF failed ».

Q : Comment forcer les pare-feu à gérer un groupe de la plage PIM SSM comme une adresse de groupe non-SSM ?

A : Assurez-vous que RP annonce le mappage RP-à-groupe pour les groupes qui sont plus spécifiques que 232.0.0.0/8 (préfixe plus long) ou sur le pare-feu configurez manuellement l'adresse RP pour des groupes spécifiques.

Option 1. Configuration sur RP :

<#root>

```
device(config)#
```

access-list 1 permit host 232.4.4.4

```
device(config)#

ip pim rp-candidate Loopback0 group 1 interval 10 priority 1 bidir

<-- group refers to the access-list
```

Vérification sur le pare-feu :

```
<#root>
device#

show pim group-map 232.4.4.4

Group Range         Proto   Client   Groups RP address      Info

232.4.4.4/32*       BD

    BSR      0      10.4.4.4   RPF: outside,192.168.3.1 <-- Proto is BD, not SSM
```

Option 2. Configuration sur le pare-feu :

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

access-list mcast standard permit 232.4.4.4 255.255.255.254

device(config)#

pim rp-address 10.4.4.4 mcast bidir

device(config)#

show pim group-map 232.4.4.4

Group Range         Proto   Client   Groups RP address      Info

232.4.4.4/31*
```

```
BD

      config   0      10.4.4.4   RPF: outside,192.168.3.1 <-- Proto is BD, not SSM
```

Notez que la liste de contrôle d'accès ne doit pas utiliser d'entrées d'hôte ou d'entrées avec le masque 255.255.255.255.

Q : Que se passe-t-il si le pare-feu traite un groupe de la plage PIM SSM comme une adresse de groupe non-SSM ?

A : Supposez que le groupe 232.4.4.4 est traité comme une adresse non-SSM (reportez-vous à la question 4) :

```
<#root>

device#

show pim group-map 232.4.4.4


Group Range         Proto   Client   Groups RP address      Info

232.4.4.4/32*       BD

      BSR      0      10.4.4.4   RPF: outside,192.168.3.1
```

Si la version du logiciel est affectée par l'ID de bogue Cisco CSCwt9960, la mroute (*, G) est manquante et le flux de multidiffusion est limité en débit à environ 50 paquets par seconde. Les paquets excessifs sont abandonnés lorsque la limite de débit est dépassée (punt-rate-limit) Raison de l'abandon ASP :

```
<#root>

device#

show mroute 232.4.4.4
```

No mroute entries found.

device#

show mfib 232.4.4.4 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: 232.4.4.4
  RP-tree:
   Forwarding: 23317/

50

/28/10, Other: 0/0/0

device#

show mfib 232.4.4.4 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: 232.4.4.4
  RP-tree:
   Forwarding: 23540/

49

/28/10, Other: 0/0/0

device#

```
capture capi interface inside trace match udp any host 232.4.4.4


device#

show capture capi trace | i Drop-reason


Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (NA
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (NA
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (NA
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (NA
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (NA
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (NA
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (NA
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (NA
…
```

Pour plus d'informations, référez-vous à l'ID de bogue Cisco CSCwt9960.

Autres informations utiles

- Bloc de multidiffusion spécifique à la source
- ID de bogue Cisco CSCwt99960

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.