Dépannage des problèmes courants de multidiffusion ASA

Table des matières

paquet supérieure à MTU

Introduction

Ce document décrit le routage de multidiffusion sur l'appliance de sécurité adaptatif (ASA) et les problèmes courants.

Informations sur les fonctionnalités

Remarque : pour obtenir un contenu mis à jour sur le routage multidiffusion sur l'appliance de sécurité adaptative (ASA), Firepower Threat Defense (FTD) ou Secure Firewall Threat Defense (FTD), reportez-vous aux articles suivants :
Dépannage de Firepower Threat Defense IGMP et des bases de la multidiffusion
Dépannage de Firepower Threat Defense et ASA Multicast PIM

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

La multidiffusion sur ASA peut être configurée dans l'un des deux modes suivants :

- PIM sparse-mode (Protocol Independent Multicast : RFC 4601)
- IGMP Stub-mode (Internet Group Management Protocol : RFC 2236)

Le mode intermédiaire PIM est le choix préféré, car l'ASA communique avec les voisins via un protocole de routage multicast (PIM). IGMP Stub-mode était la seule option de configuration de multidiffusion avant la publication de la version 7.0 d'ASA, et fonctionnait en transférant simplement les rapports IGMP reçus des clients vers les routeurs en amont.

Composants de la multidiffusion

En général, une infrastructure de multidiffusion se compose des éléments suivants :

Expéditeur => Hôte ou périphérique réseau à l'origine du flux de multidiffusion. Par exemple, un serveur qui envoie un flux vidéo et/ou audio et des périphériques réseau exécutant un protocole de routage tel que EIGRP ou OSPF.

Receiver => Hôte ou périphérique qui reçoit le flux de multidiffusion. Ce terme est plus fréquemment utilisé pour les hôtes activement intéressés par le trafic et qui utilisent le protocole

IGMP pour rejoindre ou quitter le groupe de multidiffusion en question.

Routeurs / ASA => Périphériques réseau chargés de traiter et de transférer le flux/trafic de multidiffusion vers d'autres segments du réseau, si nécessaire, de la source au(x) client(s).

Multicast Routing Protocol => Protocole chargé de transférer les paquets multidiffusion. Le plus courant est PIM (Protocol Independent Multicast), mais il y en a d'autres comme MOSPF par exemple.

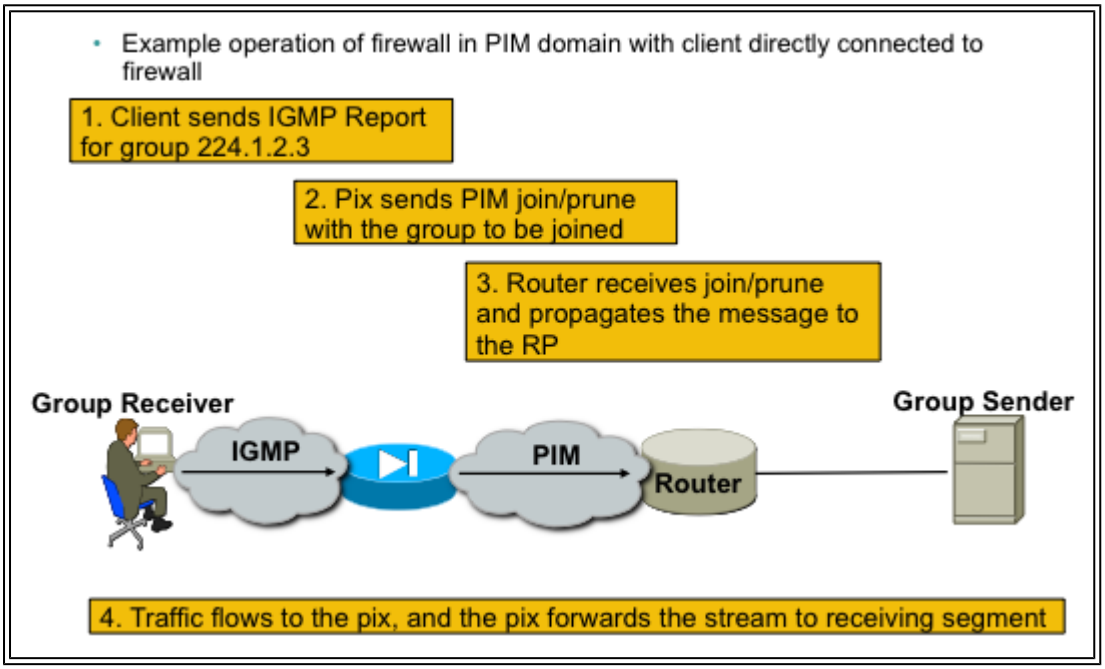
Protocole IGMP (Internet Group Management Protocol) => Processus utilisé par les clients pour recevoir un flux de multidiffusion d'un certain groupe.

Fonctionnement en mode intermédiaire de PIM

- L'ASA prend en charge le mode intermédiaire PIM et le mode bidirectionnel PIM.
- Les commandes PIM sparse-mode et IGMP stub-mode ne doivent pas être configurées simultanément.

- Avec le mode intermédiaire PIM, tout le trafic de multidiffusion circule d'abord vers le point de rendez-vous (RP), puis est transféré vers les récepteurs. Au bout d'un certain temps, le flux de multidiffusion passe directement de la source aux récepteurs (et contourne le RP).

Cette image illustre un déploiement commun où l'ASA a des clients de multidiffusion sur une interface et des voisins PIM sur une autre :



Exemple de configuration en mode dispersé PIM

1. Activez le routage multidiffusion (mode de configuration globale).

<#root>

ASA(config)#

multicast-routing

2. Définissez l'adresse du point de rendez-vous PIM.

<#root>

ASA(config)#

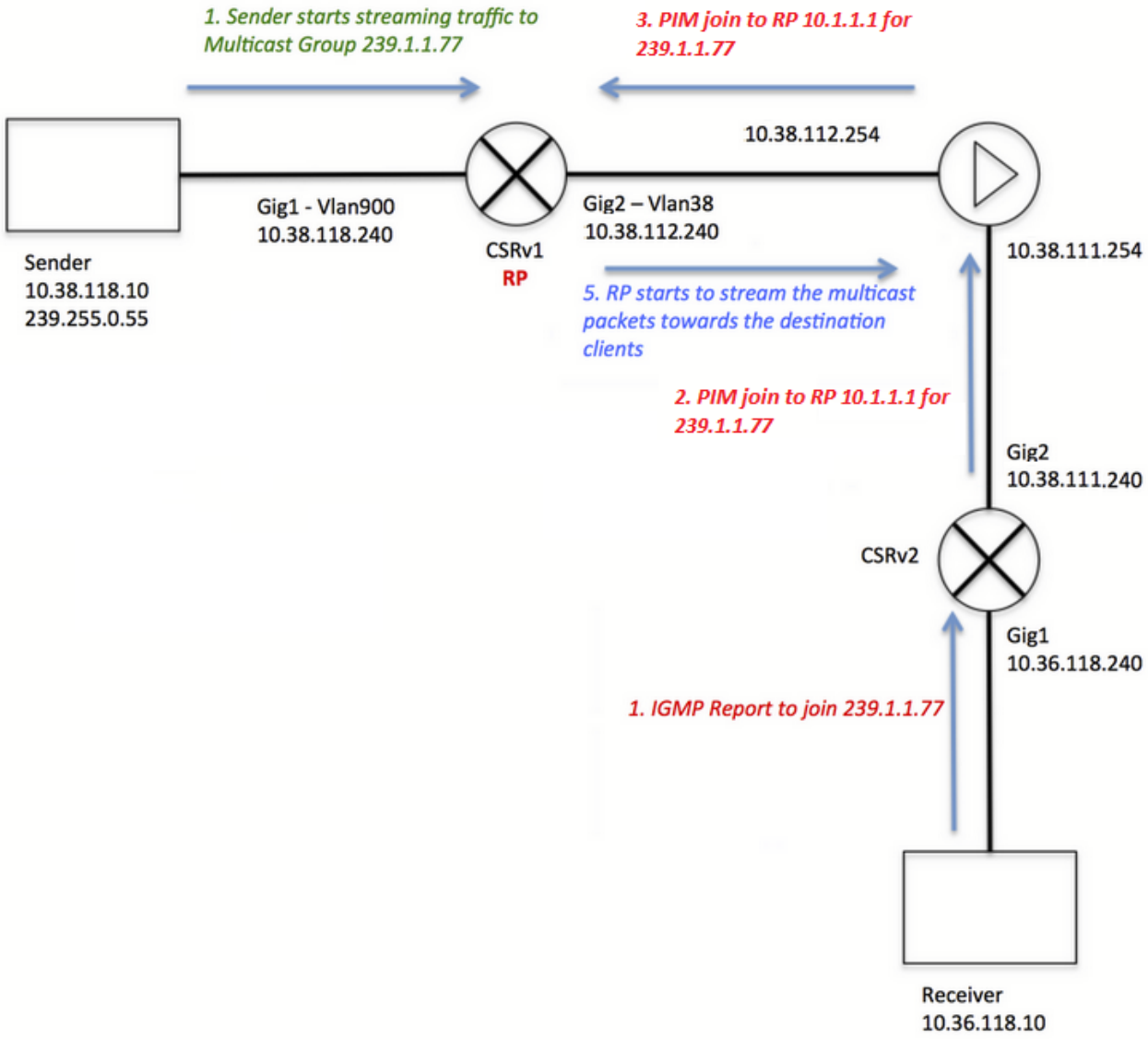
pim rp-address 172.18.123.3

3. Autorisez les paquets de multidiffusion sur l'interface appropriée (nécessaire uniquement si la stratégie de sécurité de l'ASA bloque les paquets de multidiffusion entrants).

<#root>

access-list 105 extended permit ip any host 224.1.2.3
access-group 105 in interface outside

Exemple de mode intermédiaire PIM :



Notez que l'enregistrement IGMP du client (étapes en rouge) et le flux reçu par le serveur (étapes en vert) ont été colorés différemment, et ceci a été fait de cette façon pour prouver que les deux processus peuvent se produire indépendamment.

Étapes d'enregistrement du client (étapes rouges) :

1. Le client envoie un rapport IGMP pour le groupe 239.1.1.7

2. Le routeur envoie un message PIM Join au RP statique configuré (10.1.1.1) pour le groupe 239.1.1.7.

3. ASA envoie au RP un message PIM Join pour le groupe 239.1.1.7.

ASA affiche l'entrée PIM *,G sur la sortie de la commande show mroute :

<#root>

ciscoasa#

show mroute 239.1.1.77

```
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

(*, 239.1.1.77), 00:03:43/00:02:41, RP 10.1.1.1, flags: S
  Incoming interface: outside
  RPF nbr: 10.38.111.240
  Immediate Outgoing interface list:
    inside, Forward, 00:03:43/00:02:41
```

Mais comme le serveur source n'a pas démarré de flux, le résultat « show mfib » sur l'ASA n'affiche aucun paquet reçu :

```
<#root>

ciscoasa#

show mfib 239.1.1.77


Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, K - Keepalive
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count

(*,239.1.1.77) Flags: C K
   Forwarding: 0/0/0/0, Other: 0/0/0
   outside Flags: A
   inside Flags: F NS
     Pkts: 0/0
```

Avant que le serveur ne commence à envoyer du trafic au groupe de multidiffusion, le RP affiche uniquement une entrée « *.G » sans interface entrante dans la liste, comme par exemple :

```
<#root>

CRSv#

show ip mroute 239.1.1.77

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
```

```
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector, p - PIM Joins on route,
       x - VxLAN group
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.1.1.77), 00:00:02/00:03:27, RP 10.1.1.1, flags: S
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet2, Forward/Sparse-Dense, 00:00:02/00:03:27
```

Une fois que le serveur commence le flux vers le groupe de multidiffusion, le RP crée une entrée « S, G » et place l'interface face à l'expéditeur sur la liste d'interfaces entrantes et commence à envoyer le trafic en aval vers l'ASA :

<#root>

```
CRSv#
```

show ip mroute 239.1.1.77

```
...

(*, 239.1.1.77), 00:03:29/stopped, RP 10.1.1.1, flags: SF
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet2, Forward/Sparse-Dense, 00:03:29/00:02:58

(10.38.118.10, 239.1.1.77), 00:00:07/00:02:52, flags: FT
  Incoming interface: GigabitEthernet1, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet2, Forward/Sparse-Dense, 00:00:07/00:03:22
```

Utilisez ces commandes pour les vérifications :

- La commande show mroute affiche une entrée « S, G »

- show mfib affiche les compteurs de paquets de transfert

- la commande show conn affiche la connexion associée au groupe de multidiffusion ip

<#root>

```
ciscoasa#
```

show mroute 239.1.1.77

```
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

(*, 239.1.1.77), 00:06:22/00:02:50, RP 10.1.1.1, flags: S
  Incoming interface: outside
  RPF nbr: 10.38.111.240
  Immediate Outgoing interface list:
    inside, Forward, 00:06:22/00:02:50

(10.38.118.10, 239.1.1.77), 00:03:00/00:03:28, flags: ST
  Incoming interface: outside
  RPF nbr: 10.38.111.240
  Immediate Outgoing interface list:
    inside, Forward, 00:03:00/00:03:26

ciscoasa#
```

show mfib 239.1.1.77

```
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, K - Keepalive
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count

(*,239.1.1.77) Flags: C K
   Forwarding: 15/0/1271/0, Other: 0/0/0
   outside Flags: A
   inside Flags: F NS
     Pkts: 0/15
(10.38.118.10,239.1.1.77) Flags: K
   Forwarding: 7159/34/1349/360, Other: 0/0/0
   outside Flags: A
   inside Flags: F NS
     Pkts: 7159/5

ciscoasa#
```

show conn all | i 239.1.1.77

```
UDP outside  10.38.118.10:58944 inside  239.1.1.77:5004, idle 0:00:00, bytes 10732896, flags -
UDP outside  10.38.118.10:58945 inside  239.1.1.77:5005, idle 0:00:01, bytes 2752, flags -
UDP outside  10.38.118.10:58944 NP Identity Ifc  239.1.1.77:5004, idle 0:00:00, bytes 0, flags -
UDP outside  10.38.118.10:58945 NP Identity Ifc  239.1.1.77:5005, idle 0:00:01, bytes 0, flags -
```

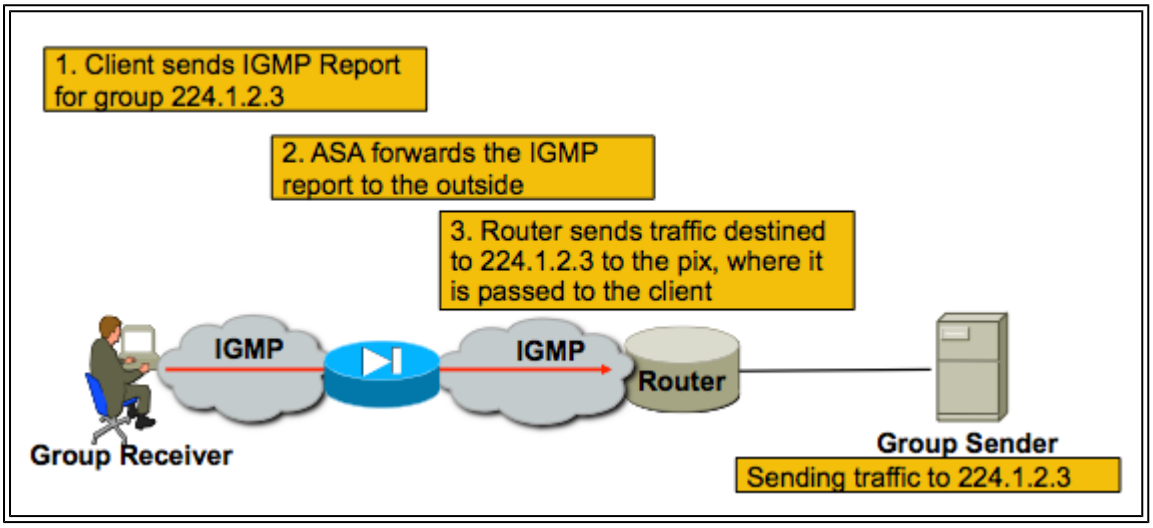
Remarque : une fois que le client ferme l'application cliente de multidiffusion, l'hôte envoie un message de requête IGMP.

S'il s'agit du seul hôte connu par le routeur comme un client veut recevoir le flux, le routeur envoie un message d'élagage IGMP au RP.

Fonctionnement en mode stub IGMP

- En mode STUB IGMP, l'ASA agit comme un client de multidiffusion, et génère ou transfère des rapports IGMP (également appelés « jonctions » IGMP) vers des routeurs adjacents, pour déclencher la réception du trafic de multidiffusion
- Les routeurs envoient régulièrement des requêtes aux hôtes pour voir si un noeud du réseau souhaite continuer à recevoir le trafic de multidiffusion.
- Le mode de stub IGMP n'est pas recommandé car le mode intermédiaire PIM offre de nombreux avantages par rapport au mode de stub (avec des flux de trafic multicast plus efficaces, la possibilité de participer au PIM, etc.).

Cette image illustre le fonctionnement de base d'un ASA configuré pour le mode d'extrémité IGMP :



Configuration du mode stub IGMP

1. Activez le routage multidiffusion (mode de configuration globale).

<#root>

```
ASA(config)#
```

multicast-routing

2. Sur l'interface sur laquelle le pare-feu reçoit les rapports igmp, configurez la commande igmp forward-interface. Transférez les paquets de l'interface vers la source du flux. Dans cet exemple, les récepteurs de multidiffusion sont directement connectés à l'interface interne et la source de multidiffusion se trouve au-delà de l'interface externe.

<#root>

```
!
interface Ethernet0
 nameif outside
```

```
 security-level 0
 ip address 172.16.1.1 255.255.255.0
 no pim
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.0.0.1 255.255.255.0
 no pim
```

igmp forward interface outside

!

3. Autorisez les paquets de multidiffusion sur l'interface appropriée (uniquement nécessaire si la stratégie de sécurité de l'ASA refuse le trafic de multidiffusion entrant).

<#root>

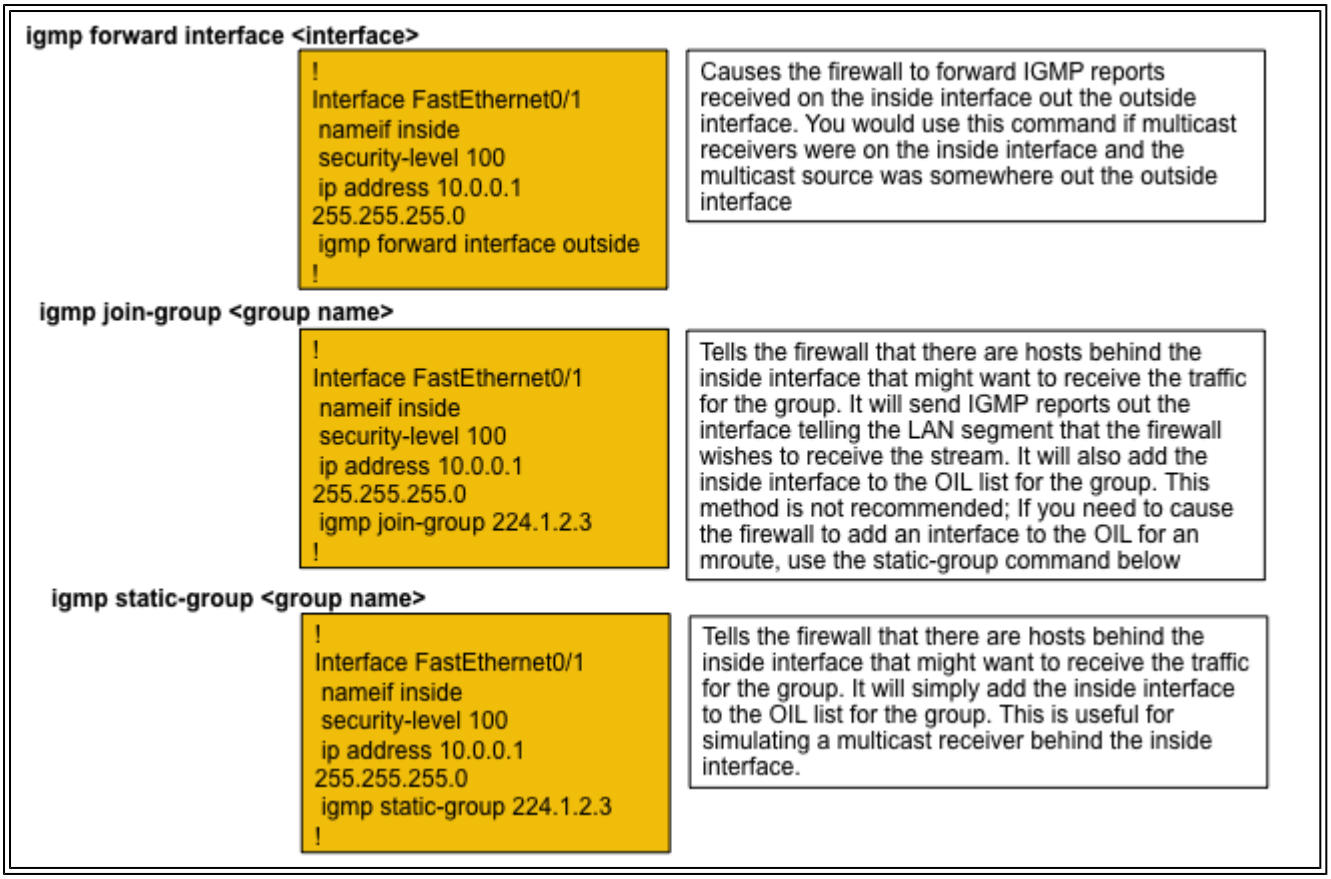
ASA(config)#

access-list 105 extended permit ip any host 224.1.2.3

ASA(config)#

access-group 105 in interface outside

Souvent, il y a confusion autour des différentes commandes de sous-mode d'interface igmp, et ce diagramme décrit quand utiliser chacune :



Bidir PIM

Dans le PIM bidirectionnel, il n'y a pas d'arborescence partagée (SPT). Cela signifie trois choses :

1. Le routeur du premier saut (connecté à l'expéditeur) n'envoie pas de paquets PIM Register au RP.

2. Le RP n'envoie pas de messages PIM JOIN pour rejoindre l'arborescence source.

3. Les routeurs sur le chemin vers le récepteur envoient des messages de jonction PIM vers le RP pour rejoindre le RPT.

Cela signifie que l'ASA ne génère pas de (S, G) car les périphériques ne rejoignent pas le SPT. Tout le trafic de multidiffusion passe par le RP. L'ASA transfère tout le trafic de multidiffusion tant qu'il y a un (*, G). S'il n'y a pas de (*, G), cela signifie que l'ASA n'a jamais reçu de paquet de jonction PIM. Si tel est le cas, l'ASA ne doit pas transférer de paquets de multidiffusion.

Configuration Bidir PIM

1. Activez le routage multidiffusion (mode de configuration globale).

<#root>

```
ASA(config)#
```

multicast-routing

2. Définissez l'adresse du point de rendez-vous PIM.

<#root>

```
ASA(config)#
pim rp-address 172.18.123.3 bidir
```

3. Autorisez les paquets de multidiffusion sur l'interface appropriée (nécessaire uniquement si la stratégie de sécurité de l'ASA bloque les paquets de multidiffusion entrants).

<#root>

```
access-list 105 extended permit ip any host 224.1.2.3
access-group 105 in interface outside
```

Méthodologie de dépannage

Informations À Collecter Lors Du Dépannage De Problèmes De Multidiffusion

Afin de comprendre et de diagnostiquer complètement un problème de transfert multidiffusion sur l'ASA, une partie ou la totalité de ces informations sont nécessaires :

· Une description de la topologie du réseau, l'emplacement des expéditeurs de multidiffusion, des récepteurs et du point de rendez-vous.
· L'adresse IP du groupe spécifique, ainsi que les ports et les protocoles utilisés.
· Syslogs générés par l'ASA au moment où le flux de multidiffusion rencontre des problèmes.
· Sortie spécifique de la commande show de l'interface de ligne de commande ASA :

<#root>

```
show mroute
show mfib
show pim neighbor
show route
show tech-support
```

· Captures de paquets pour indiquer si les données de multidiffusion arrivent à l'ASA et si les paquets sont transférés via l'ASA (prenez note de la durée de vie IP (TTL) du paquet. Ceci peut être vu avec la commande « show capture x detail »)
· Capture de paquets pour les paquets IGMP et/ou PIM. Exemple :

<#root>

```
capture cap1 interface outside match ip any host 239.1.1.77

  >>> This captures the multicast traffic itself

capture cappim1 interface inside match pim any any

         >>> This captures PIM Join/Prune messages

capture capigmp interface inside match igmp any any

          >>> This captures IGMP Report/Query messages
```

· Informations provenant de périphériques de multidiffusion adjacents (routeurs) tels que « show mroute » et « show mfib ».
· Capture de paquets et/ou commandes show pour déterminer si l'ASA abandonne les paquets de multidiffusion. La commande « show asp drop » peut être utilisée pour déterminer si l'ASA abandonne les paquets. En outre, les captures de paquets de type « asp-drop » peuvent être utilisées pour capturer tous les paquets abandonnés par l'ASA, puis examinées pour voir si les paquets de multidiffusion sont présents dans la capture d'abandon.

Résultat utile de la commande show

Le résultat de la commande show mroute montre les différents groupes et les informations de transfert, et est très similaire à la commande IOS show mroute. La commande show mfib affiche l'état de transmission des différents groupes de multidiffusion. Il est particulièrement important d'observer le compteur de paquets Forwarding, ainsi que Other (qui indique des abandons) :

```
<#root>

ciscoasa#

show mfib

Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, K - Keepalive
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.1.2.3) Flags: S K
   Forwarding: 0/0/0/0, Other: 0/0/0
   inside Flags: F
     Pkts: 0/0
(192.168.1.100,224.1.2.3) Flags: K
   Forwarding: 6749/18/1300/182, Other: 690/0/690
   outside Flags: A
   inside Flags: F
     Pkts: 6619/8
(*,232.0.0.0/8) Flags: K
   Forwarding: 0/0/0/0, Other: 0/0/0
ciscoasa#
```

La commande clear mfib counters peut être utilisée pour effacer les compteurs, ce qui est très utile pendant le test :

<#root>

```
ciscoasa#
clear mfib counters
```

Captures de paquets

L'utilitaire de capture de paquets intégré est très utile pour résoudre les problèmes de multidiffusion. Dans cet exemple, tous les paquets entrants sur l'interface DMZ, destinés à 239.17.17.17, sont capturés :

<#root>

```
ciscoasa#
capture dmzcap interface dmz

ciscoasa#
capture dmzcap match ip any host 239.17.17.17
ciscoasa#
show cap dmzcap

324 packets captured
   1: 17:13:30.976618       802.1Q vlan#301 P0 10.1.123.129.2000 > 239.17.17.17.16384:  udp 172
   2: 17:13:30.976679       802.1Q vlan#301 P0 10.1.123.129.2000 > 239.17.17.17.16384:  udp 172
   3: 17:13:30.996606       802.1Q vlan#301 P0 10.1.123.129.2000 > 239.17.17.17.16384:  udp 172
   4: 17:13:30.996652       802.1Q vlan#301 P0 10.1.123.129.2000 > 239.17.17.17.16384:  udp 172
   5: 17:13:31.016676       802.1Q vlan#301 P0 10.1.123.129.2000 > 239.17.17.17.16384:  udp 172
   6: 17:13:31.016722       802.1Q vlan#301 P0 10.1.123.129.2000 > 239.17.17.17.16384:  udp 172
....
```

Le résultat de la commande show capture x detail montre la durée de vie des paquets, ce qui est très utile. Dans ce résultat, la durée de vie du paquet est 1 (et l'ASA passe ce paquet car il ne décrémente pas la durée de vie des paquets IP par défaut) mais un routeur en aval abandonnerait les paquets :

<#root>

```
ASA#
```

```
show cap capout detail

453 packets captured
...
   1: 14:40:39.427147 c062.6baf.8dc3 0100.5e7f.02c3 0x8100 Length: 1362
      802.1Q vlan#1007 P0 10.4.2.95.1806 > 239.255.2.195.5000:  [udp sum ok] udp 1316 (DF) [ttl 1] (id
```

Les captures de paquets sont également utiles pour capturer le trafic PIM et IGMP. Cette capture montre que l'interface interne a reçu un paquet IGMP (protocole IP 2) provenant de 10.0.0.2 :

```
<#root>

ciscoasa#

capture capin interface inside

ciscoasa#

capture capin match igmp any any

ciscoasa#

show cap capin

1 packets captured
1: 10:47:53.540346 802.1Q vlan#15 P0 10.0.0.2 > 224.1.2.3:  ip-proto-2, length 8
ciscoasa#
```

Notez que la durée de vie des paquets peut être affichée avec la commande « show capture x detail ».

Ici, nous pouvons voir les captures d'abandon ASP prises qui montrent les paquets de multidiffusion abandonnés et la raison des abandons (punt-rate-limit) :

```
<#root>

ASA#

show cap capasp det

 12: 14:37:26.538332 c062.6baf.8dc3 0100.5e7f.02c3 0x8100 Length: 1362
      802.1Q vlan#1007 P0 10.76.4.95.1806 > 239.255.2.195.5000:  [udp sum ok] udp 1316 (DF) [ttl 1] (id
  13: 14:37:26.538439 c062.6baf.8dc3 0100.5e7f.02c3 0x8100 Length: 1362
      802.1Q vlan#1007 P0 10.76.4.95.1806 > 239.255.2.195.5000:  [udp sum ok] udp 1316 (DF) [ttl 1] (id
```

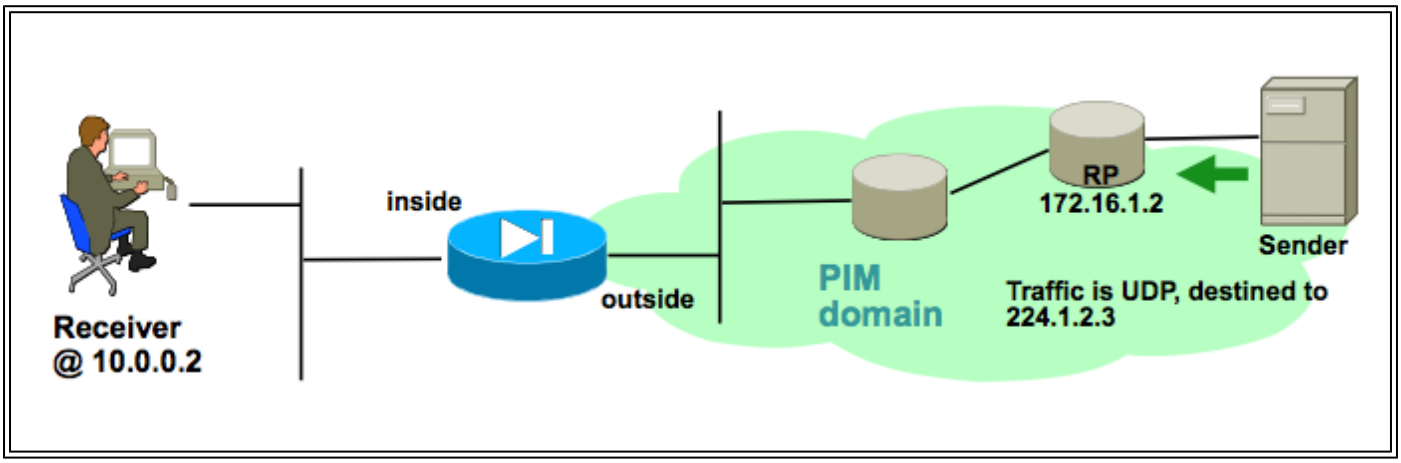
Exemple de déploiement de multidiffusion en mode dispersé ASA PIM

Ce schéma illustre comment l'ASA interagit avec les périphériques voisins en mode intermédiaire

PIM.

Comprendre la topologie du réseau

Déterminez exactement l'emplacement des expéditeurs et des récepteurs du flux de multidiffusion spécifique. Déterminez également l'adresse IP du groupe de multidiffusion, ainsi que l'emplacement du point de rendez-vous.



Dans ce cas, les données peuvent être reçues au niveau de l'interface externe de l'ASA, et transmises au récepteur de multidiffusion sur l'interface interne. Étant donné que le récepteur se trouve dans le même sous-réseau IP que l'interface interne de l'ASA, attendez-vous à voir un rapport IGMP reçu à l'interface interne lorsque le client demande à recevoir le flux. L'adresse IP de l'expéditeur est 192.168.1.50.

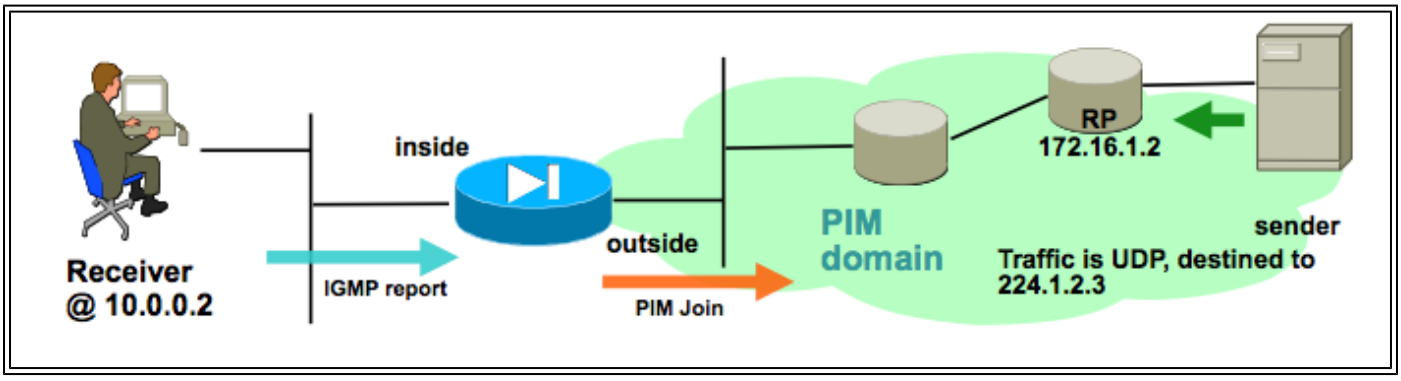
Vérifiez que l'ASA reçoit le rapport IGMP du destinataire

Dans cet exemple, le rapport IGMP est généré par le récepteur et traité par l'ASA.

Les captures de paquets et la sortie de debug igmp peuvent être utilisées pour vérifier que l'ASA a reçu et traité avec succès le message IGMP.

Vérifiez que l'ASA envoie un message de jointure PIM vers le point de rendez-vous

L'ASA interprète le rapport IGMP et génère un message de jonction PIM, puis l'envoie par l'interface vers le RP.

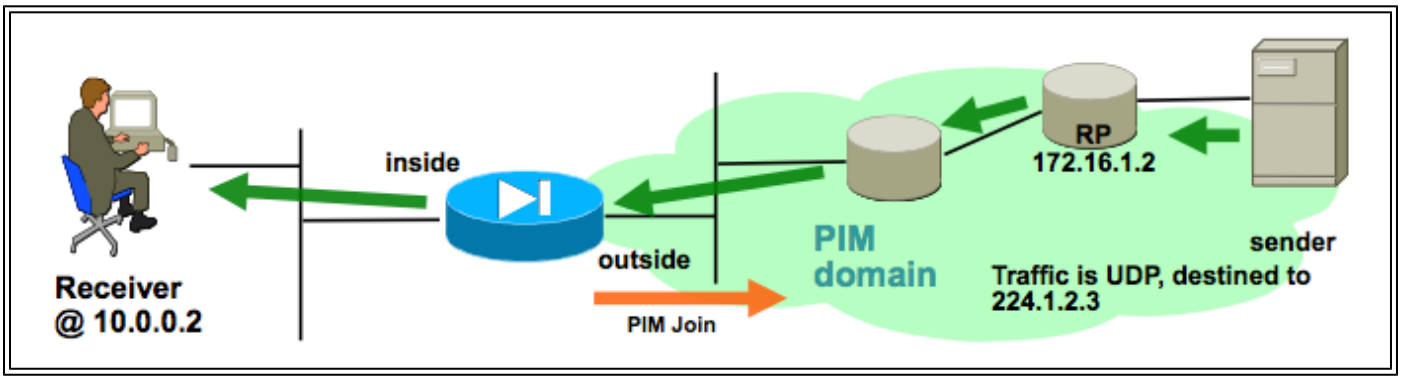


Cette sortie provient du groupe debug pim 224.1.2.3 et montre que l'ASA envoie avec succès le message de jointure PIM. L'expéditeur du flux de multidiffusion est 192.168.1.50.

```
IPv4 PIM: (*,224.1.2.3) J/P processing
IPv4 PIM: (*,224.1.2.3) Periodic J/P scheduled in 50 secs
IPv4 PIM: (*,224.1.2.3) J/P adding Join on outside
IPv4 PIM: (*,224.1.2.3) inside Processing timers
IPv4 PIM: Sending J/P message for neighbor 10.2.3.2 on outside for 1 groups
IPv4 PIM: [0] (192.168.1.50,224.1.2.3/32) MRIB update (a=0,f=0,t=1)
IPv4 PIM: [0] (192.168.1.50,224.1.2.3/32) outside MRIB update (f=20,c=20)
IPv4 PIM: [0] (192.168.1.50,224.1.2.3) Signal present on outside
IPv4 PIM: (192.168.1.50,224.1.2.3) Create entry
IPv4 PIM: [0] (192.168.1.50,224.1.2.3/32) outside MRIB modify NS
IPv4 PIM: Adding monitor for 192.168.1.50
```

Vérifiez que l'ASA reçoit et transfère le flux de multidiffusion

L'ASA commence à recevoir le trafic de multidiffusion sur l'interface externe (illustré par les flèches vertes) et à le transférer aux récepteurs internes.



Les commandes show mroute et show mfib, ainsi que les captures de paquets, peuvent être utilisées pour vérifier que l'ASA reçoit et transfère les paquets de multidiffusion.

Une connexion est créée dans la table de connexion pour représenter le flux de multidiffusion :

<#root>

```
ciscoasa#
```

show conn

```
59 in use, 29089 most used
...
UDP outside:192.168.1.50/52075 inside:224.1.2.3/1234 flags -
...
```

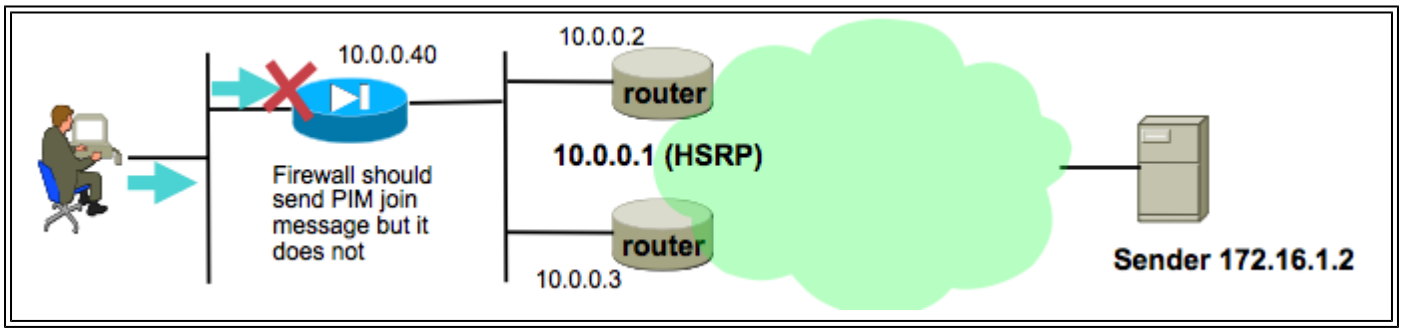
Analyse des données

Problèmes courants

Cette section présente une série de problèmes réels liés à la multidiffusion ASA

L'ASA ne parvient pas à envoyer des messages PIM vers les routeurs en amont en raison de HSRP

Lorsque ce problème est rencontré, l'ASA ne parvient pas à envoyer des messages PIM à partir d'une interface. Ce diagramme montre que l'ASA ne peut pas envoyer de messages PIM vers l'expéditeur, mais le même problème peut être vu quand l'ASA doit envoyer un message PIM vers le RP.



Le résultat de la commande debug pim montre que l'ASA ne peut pas envoyer le message PIM au routeur de tronçon suivant en amont :

```
IPv4 PIM: Sending J/P to an invalid neighbor: outside 10.0.0.1
```

Ce problème n'est pas spécifique à l'ASA et affecte également les routeurs. Le problème est déclenché par la combinaison de la configuration de la table de routage et de la configuration HSRP utilisée par les voisins PIM.

La table de routage pointe vers l'IP 10.0.0.1 de HSRP comme périphérique de tronçon suivant :

<#root>

```
ciscoasa#
show run route
route outside 0.0.0.0 0.0.0.0 10.0.0.1 1
```

Cependant, la relation de voisinage PIM est formée entre les adresses IP d'interface physique des routeurs, et non l'IP HSRP :

<#root>

```
ciscoasa#
show pim neighbor
Neighbor Address  Interface          Uptime    Expires DR pri Bidir
```

```
10.0.0.2          outside            01:18:27  00:01:25 1
10.0.0.3          outside            01:18:03  00:01:29 1 (DR)
```

Référez-vous à "Pourquoi le mode intermédiaire PIM ne fonctionne-t-il pas avec une route statique vers une adresse HSRP ?" pour plus d'informations.

Un extrait du document :

Pourquoi le routeur n'envoie-t-il pas le message Joindre/Élaguer ? 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."

Afin d'atténuer le problème, ajoutez une entrée mroute statique sur l'ASA pour le trafic en question. Assurez-vous qu'elle pointe vers l'une des deux adresses IP d'interface de routeur (10.0.0.2 ou 10.0.0.3). Dans ce cas, cette commande permet à l'ASA d'envoyer des messages PIM dirigés vers l'expéditeur de multidiffusion à l'adresse 172.16.1.2 :

<#root>

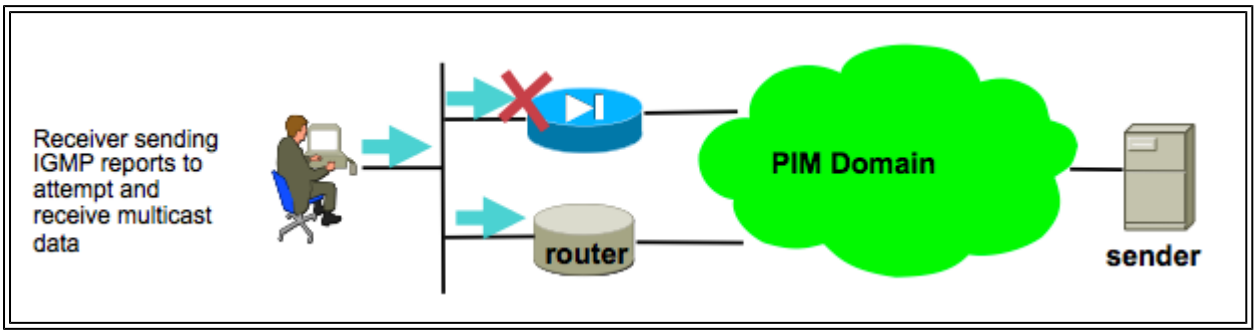
```
ciscoasa(config)#
```

mroute 172.16.1.2 255.255.255.255 10.0.0.3

Une fois que cela est fait, la table de routage de multidiffusion remplace la table de routage de monodiffusion de l'ASA, et l'ASA envoie les messages PIM directement au voisin 10.0.0.3.

L'ASA Ignore Les Rapports IGMP Car Il Ne S'Agit Pas Du Routeur Désigné Sur Le Segment LAN

Pour ce problème, l'ASA reçoit un rapport IGMP d'un récepteur de multidiffusion connecté directement, mais il l'ignore. Aucune sortie de débogage n'est générée et le paquet est simplement abandonné, et la réception du flux échoue.



Pour ce problème, l'ASA ignore le paquet parce qu'il n'est pas le routeur désigné sélectionné par

PIM sur le segment LAN où résident les clients.

Cette sortie CLI ASA montre qu'un périphérique différent est le routeur désigné (désigné par « DR ») sur le réseau d'interface interne :

```
<#root>

ciscoasa#

show pim neighbor


 Neighbor Address  Interface          Uptime    Expires DR pri Bidir
 192.168.1.2       outside             01:18:27  00:01:25 N/A>
 10.0.0.2          inside              01:18:03  00:01:29 1

(DR)
```

Par défaut, PIM est activé sur toutes les interfaces ASA quand la commande multicast-routing est ajoutée à la configuration. S'il y a d'autres voisins PIM (d'autres routeurs ou ASA) sur l'interface interne de l'ASA (où résident les clients) et que l'un de ces voisins a été sélectionné parce que le DR pour ce segment, alors les autres routeurs non-DR abandonnent les rapports IGMP. La solution est de désactiver PIM sur l'interface (avec la commande no pim sur l'interface impliquée), ou de faire de l'ASA le DR pour le segment via la commande d'interface pim dr-priority.

Les rapports IGMP sont refusés par le pare-feu lorsque la limite d'interface IGMP est dépassée

Par défaut, l'ASA autorise 500 jointures actives (rapports) suivies sur une interface. Il s'agit de la valeur maximale configurable. Si un grand nombre de flux de multidiffusion sont demandés par les clients à partir d'une interface, le maximum de 500 jointures actives peut être rencontré, et l'ASA peut ignorer les rapports IGMP entrants supplémentaires des récepteurs de multidiffusion.

Pour confirmer si ceci est la cause d'un échec de multidiffusion, émettez la commande « show igmp interface interfacename » et recherchez les informations « IGMP limit » pour l'interface.

```
<#root>

ASA#

show igmp interface inside

Hosting-DMZ is up, line protocol is up
  Internet address is 10.11.27.13/24
  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: 500

  Cumulative IGMP activity: 7018 joins, 6219 leaves
  IGMP querying router is 10.11.27.13 (this system)
```

```
DEBUG - IGMP: Group x.x.x.x limit denied on outside
```

L'ASA ne parvient pas à transférer le trafic multidiffusion dans la plage 232.x.x.x/8

Cette plage d'adresses est destinée à être utilisée avec un SSM (Source Specific Multicast) que l'ASA ne prend pas actuellement en charge.

Le résultat de la commande debug igmp montre cette erreur :

```
IGMP: Exclude report on inside ignored for SSM group 232.179.89.253
```

L'ASA abandonne les paquets de multidiffusion en raison de la vérification du transfert de chemin inverse

Dans ce cas, l'ASA reçoit le trafic de multidiffusion sur une interface, mais il n'est pas transféré au récepteur. Les paquets sont abandonnés par l'ASA parce qu'ils échouent au contrôle de sécurité RPF (Reverse Path Forwarding). Le RPF est activé sur toutes les interfaces pour le trafic de multidiffusion et ne peut pas être désactivé (pour les paquets de monodiffusion, la vérification n'est pas activée par défaut et est activée avec la commande ip verify reverse-path interface).

En raison de la vérification RPF, lorsque le trafic de multidiffusion est reçu au niveau d'une interface, l'ASA vérifie qu'il a une route vers la source du trafic de multidiffusion (il vérifie la table de routage de monodiffusion et de multidiffusion) sur cette interface. S'il n'a pas de route vers l'expéditeur, il abandonne le paquet. Ces abandons peuvent être vus comme un compteur dans la sortie de show asp drop :

<#root>

```
ciscoasa(config)#
```

```
show asp drop
```

```
Frame drop:
  Invalid UDP Length                                     2
  No valid adjacency                                    36
  No route to host                                    4469
  Reverse-path verify failed                        121012
```

Une option consiste à ajouter une mroute pour l'expéditeur du trafic. Dans cet exemple, la commande mroute est utilisée pour satisfaire le contrôle RPF pour le trafic de multidiffusion provenant de 172.16.1.2 reçu sur l'interface externe :

<#root>

```
ciscoasa(config)#
mroute 172.16.1.2 255.255.255.255 outside
```

L'ASA ne génère pas de jonction PIM lors du basculement PIM vers l'arborescence source

Initialement, les paquets de multidiffusion PIM en mode clairsemé circulent de l'expéditeur de multidiffusion au RP, puis du RP au récepteur via une arborescence de multidiffusion partagée. Cependant, une fois que le débit binaire total atteint un certain seuil, le routeur le plus proche du récepteur de multidiffusion tente de recevoir le trafic le long de l'arborescence spécifique à la source. Ce routeur génère une nouvelle jointure PIM pour le groupe et l'envoie vers l'expéditeur du flux de multidiffusion (et non vers le RP, comme précédemment).

L'expéditeur du trafic de multidiffusion peut résider sur une interface ASA différente de celle du RP. Lorsque l'ASA reçoit la jonction PIM pour commuter vers l'arborescence spécifique à la source, l'ASA doit avoir une route vers l'adresse IP de l'expéditeur. Si cette route est introuvable, les paquets de jonction PIM sont abandonnés et ce message est vu dans le résultat de debug pim

```
NO RPF Neighbor to send J/P
```

La solution à ce problème est d'ajouter une entrée mroute statique pour l'expéditeur du flux, qui pointe vers l'interface ASA à partir de laquelle l'expéditeur réside.

L'ASA abandonne les paquets de multidiffusion en raison du dépassement de la durée de vie (TTL)

Dans ce cas, le trafic de multidiffusion échoue parce que la durée de vie des paquets est trop faible. Cela entraîne l'abandon de l'ASA ou d'un autre périphérique du réseau.

Souvent, la valeur de durée de vie IP des paquets multidiffusion est très faible pour l'application qui les a envoyés. Cette opération est parfois effectuée par défaut pour garantir que le trafic de multidiffusion ne traverse pas trop le réseau. Par exemple, par défaut, la vidéo LAN L'application cliente (un émetteur multidiffusion et un outil de test très répandus) définit la durée de vie dans le paquet IP sur 1 par défaut.

L'ASA Subit Une Utilisation CPU Élevée Et Des Paquets Abandonnés En Raison

D'Une Topologie De Multidiffusion Spécifique

L'ASA peut faire l'expérience d'un CPU élevé et le flux de multidiffusion peut faire l'expérience de pertes de paquets si toutes ces choses sont vraies à propos de la topologie de multidiffusion :

1. L'ASA agit en tant que RP.
2. L'ASA est le premier récepteur de saut du flux de multidiffusion. Cela signifie que l'expéditeur de multidiffusion se trouve dans le même sous-réseau IP qu'une interface ASA.
3. L'ASA est le dernier routeur de saut du flux de multidiffusion. Cela signifie qu'un récepteur de multidiffusion se trouve dans le même sous-réseau IP qu'une interface ASA.

Si tous les symptômes mentionnés sont rencontrés, alors En raison d'une limitation de conception, l'ASA est forcé de traiter le trafic multicast du commutateur. Il en résulte des flux de multidiffusion à haut débit de données qui subissent des pertes de paquets. Le compteur show asp drop qui s'incrémente lorsque ces paquets sont abandonnés est punt-rate-limit.

Afin de déterminer si un ASA a ce problème, complétez ces étapes :

Étape 1 : vérifiez si l'ASA est le RP :

<#root>

show run pim
show pim tunnel

Étape 2 : vérifiez si l'ASA est le dernier routeur de saut :

<#root>

show igmp group

<mcast_group_IP>

Étape 3 : vérifiez si l'ASA est le routeur du premier saut :

<#root>

show mroute

<mcast_group_IP>

Les mesures suivantes peuvent être prises pour atténuer ce problème :

- Modifiez la topologie de sorte que l'ASA ne soit pas le RP. Vous pouvez également empêcher l'expéditeur ou le destinataire d'être directement connecté à l'ASA

- Au lieu de PIM, utilisez le mode d'extrémité IGMP pour le transfert multidiffusion.

L'ASA supprime les premiers paquets lors du premier démarrage d'un flux de multidiffusion

Lorsque les premiers paquets d'un flux de multidiffusion arrivent à l'ASA, l'ASA doit construire cette connexion de multidiffusion particulière et l'entrée mroute associée pour transférer les paquets. Pendant que l'entrée est en cours de création, certains paquets de multidiffusion peuvent être abandonnés jusqu'à ce que la mroute et les connexions aient été établies (cela prend généralement moins d'une seconde). Une fois la configuration du flux de multidiffusion terminée, les paquets ne sont plus limités en débit.

Les paquets abandonnés pour cette raison ont la raison d'abandon ASP de « (punt-rate-limit) Punt rate limit beyond ». Voici le résultat de « show capture asp » (où asp est une capture d'abandon ASP configurée sur l'ASA pour capturer les paquets abandonnés) et vous pouvez voir les paquets de multidiffusion qui ont été abandonnés pour cette raison :

<#root>

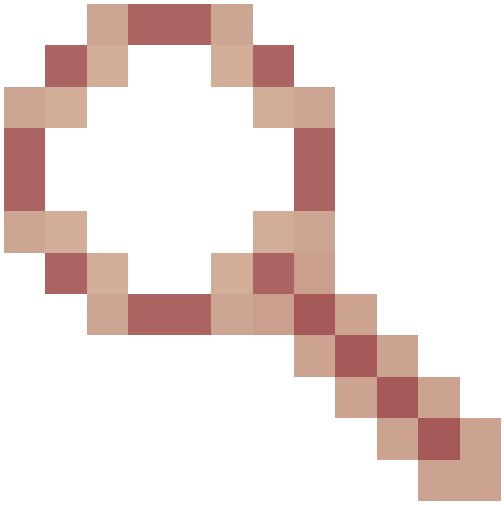
```
ASA #

show capture asp

2 packets captured
   1: 16:14:49.419091 10.23.2.2.810 > 239.255.123.123.890:  udp 32 Drop-reason: (punt-rate-limit) Punt
   2: 16:14:49.919172 10.23.2.2.810 > 239.255.123.123.890:  udp 32 Drop-reason: (punt-rate-limit) Punt
2 packets shown
```

Un Récepteur De Multidiffusion Déconnecté Interrompt La Réception De Groupe De Multidiffusion Sur D'Autres Interfaces

Seuls les ASA qui fonctionnent en mode Stub IGMP rencontrent ce problème. Les ASA qui participent au routage de multidiffusion PIM ne sont pas affectés.



Le problème est identifié par l'ID de bogue Cisco CSCeg48235
IGMP Leave sur une interface interrompt le trafic de multidiffusion sur les autres interfaces.

Voici la note de version du bogue, qui explique le problème :

```
Symptom:
When a PIX or ASA firewall is configured for IGMP stub mode multicast reception and traffic from a mult

The problem is triggered when the firewall forwards the IGMP leave for the group towards the upstream d

Conditions:
The PIX or ASA must be configured for IGMP stub mode multicast. IGMP stub mode is a legacy multicast fo

Workarounds:
1) Use PIM multicast routing instead of IGMP stub mode.
2) Decrease multicast IGMP query timers so that the receivers are queried more frequently, so their IGM
```

L'ASA abandonne les paquets de multidiffusion en raison de la stratégie de sécurité de la liste d'accès sortante

Avec ce problème spécifique, l'ASA abandonne les paquets de multidiffusion (conformément à la stratégie de sécurité configurée). Cependant, il est difficile pour l'administrateur réseau d'identifier la raison des abandons de paquets. Dans ce cas, l'ASA abandonne les paquets en raison de la liste d'accès sortante configurée pour une interface. La solution de contournement consiste à autoriser le flux de multidiffusion dans la liste de contrôle d'accès sortante.

Dans ce cas, les paquets de multidiffusion sont abandonnés avec le compteur d'abandon ASP « FP no mcast output intrf (no-mcast-intrf) ».

L'ASA abandonne continuellement certains paquets (mais pas tous) dans un flux de multidiffusion en raison de la limitation du débit du point de contrôle

Le trafic est très probablement limité en débit par le point de contrôle en raison de punt-rate-limit. Examinez le résultat de l'extraction asp et les captures pour confirmer :

```
<#root>

ASA#

show asp drop


Frame drop:
  Punt rate limit exceeded (punt-rate-limit)                              1492520
```

```
ASA#  show cap capasp det
 12: 14:37:26.538332 c062.6baf.8dc3 0100.5e7f.02c3 0x8100 Length: 1362
      802.1Q vlan#1007 P0 10.76.4.95.1806 > 239.255.2.195.5000:  [udp sum ok] udp 1316 (DF) [ttl 1] (id
```

L'entrée mfib indique que tout le trafic est commuté par processus :

<#root>

```
ASA(config)#

show mfib  239.255.2.1195

Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, K - Keepalive
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count

(*,239.255.2.195) Flags: C K
   Forwarding: 4278/50/1341/521, Other: 0/0/0
   Outside-1007 Flags: A
   RDEQ-to-Corporate Flags: F NS
     Pkts: 0/4278                                <---- HERE
```

La table de routage de multidiffusion affiche un (*, G) mais aucun (S, G).

<#root>

```
ASA(config)#

show mroute  239.255.2.1195

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

(*, 239.255.2.195), 00:44:03/00:02:44, RP 10.1.135.10, flags: S
  Incoming interface: Outside-1007
  RPF nbr: 10.100.254.18
  Immediate Outgoing interface list:
    RDEQ-to-Corporate, Forward, 00:44:03/00:02:44
```

Le problème ici est que le TTL des paquets de données multidiffusion qui arrivent à l'ASA est de 1. L'ASA transfère ces paquets au périphérique en aval (car il ne décrémente pas la durée de vie), mais le routeur en aval abandonne les paquets. Par conséquent, le routeur en aval n'envoie pas de jointure PIM (S, G) (une jointure spécifique à la source) à l'ASA vers l'expéditeur. L'ASA ne crée pas d'entrée (S, G) tant qu'il ne reçoit pas cette jointure PIM. Étant donné que (S, G) n'est pas construit, tout le trafic de multidiffusion est commuté par processus, ce qui entraîne une limite de débit.

La solution à ce problème est de s'assurer que la durée de vie des paquets n'est pas 1, ce qui permet au périphérique en aval d'envoyer la jointure spécifique à la source vers l'expéditeur ; cela amène l'ASA à installer une mroute spécifique à la source dans la table, puis tous les paquets sont commutés rapidement (au lieu d'être traités comme commutés) et le trafic doit passer par l'ASA sans problème.

Le flux de multidiffusion est arrêté en raison d'un message PIM ASSERT

Si deux périphériques réseau transfèrent les mêmes paquets de multidiffusion sur le même sous-réseau, l'un d'eux doit alors, dans l'idéal, arrêter de transférer les paquets (car dupliquer le flux est un gaspillage). Si les routeurs exécutant PIM détectent qu'ils reçoivent les mêmes paquets qu'ils génèrent également sur cette même interface, ils génèrent des messages ASSERT sur ce LAN pour sélectionner le périphérique réseau qui arrête de transférer le flux.

Vous trouverez plus d'informations sur ce message dans une section de la RFC 4601 relative au processus ASSERT.

Les débogages montrent que l'ASA reçoit un rapport IGMP pour le groupe 239.1.1.227, mais il ignore le rapport en raison du message d'affirmation qu'il reçoit d'un routeur voisin :

```
IPv4 PIM: (*,239.1.1.227) Periodic J/P scheduled in 50 secs
IPv4 PIM: (*,239.1.1.227) J/P adding Join on outside
IPv4 PIM: (10.99.41.205,239.1.1.227)RPT J/P adding Prune on outside
IPv4 PIM: (10.99.41.253,239.1.1.227)RPT J/P adding Prune on outside
IGMP: Received v2 Report on inside from 10.20.213.204 for 239.1.1.227
IGMP: Updating EXCLUDE group timer for 239.1.1.227
IPv4 PIM: (10.99.41.253,239.1.1.227) Received [15/110] Assert from 10.20.13.2 on inside
IPv4 PIM: (10.99.41.253,239.1.1.227) Assert processing message wins
IPv4 PIM: (10.99.41.253,239.1.1.227) inside Update assert timer (winner 10.20.13.2)
```

Ce problème a été observé dans un réseau de production où deux sites ont été accidentellement pontés au niveau de la couche 2, de sorte que le réseau local sur lequel se trouvaient les récepteurs de multidiffusion avait deux périphériques qui acheminaient le trafic de multidiffusion vers eux. En raison d'un autre problème réseau, l'ASA et un autre périphérique n'ont pas pu se détecter via les HELLO PIM, et par conséquent ils ont tous deux assumé le rôle de routeur désigné pour le LAN. Le trafic de multidiffusion a ainsi fonctionné pendant un certain temps, puis a échoué lorsque les messages ASSERT ont été envoyés par les périphériques. Pour résoudre le problème, la connexion incorrecte qui a ponté les périphériques au niveau de la couche 2 a été désactivée, puis le problème a été résolu.

ASA envoie une jointure PIM, mais elle n'est pas traitée par le voisin en raison de la taille du paquet supérieure à MTU

Ceci a été observé en 629575899. L'ASA a été configuré pour les trames Jumbo et le 4900 ne l'a pas été. Lorsque le client a demandé plus de 73 flux de multidiffusion, certains flux de multidiffusion ne fonctionnaient pas. 73 SG créent un message PIM Join de taille 1494, qui se

trouve toujours dans la MTU. 74 SG créent un message PIM Join supérieur à 1500, ce qui entraîne l'abandon du paquet entrant par le 4900M.

Le correctif pour ce problème était :

1. Assurez-vous que les trames Jumbo sont activées globalement sur le 4900M

2. Configurez l'interface physique et l'interface SVI avec un MTU de 9216

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.