Dépannage et problèmes courants de Multidiffusion ASA

Contenu

Introduction

Ce document explique des capacités multicasts de l'appliance de sécurité adaptable (ASA), aussi bien que des problèmes potentiels qui peuvent être produits en utilisant la caractéristique.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Multidiffusion ASA

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Les informations de caractéristique

Le guide de configuration de ligne de commande ASA trace les grandes lignes de la caractéristique de multicast-routing et comment la configurer :

http://www.cisco.com/en/US/docs/security/asa/asa90/configuration/guide/route_multicast.html

La Multidiffusion sur l'ASA peut être configurée dans un de deux modes :

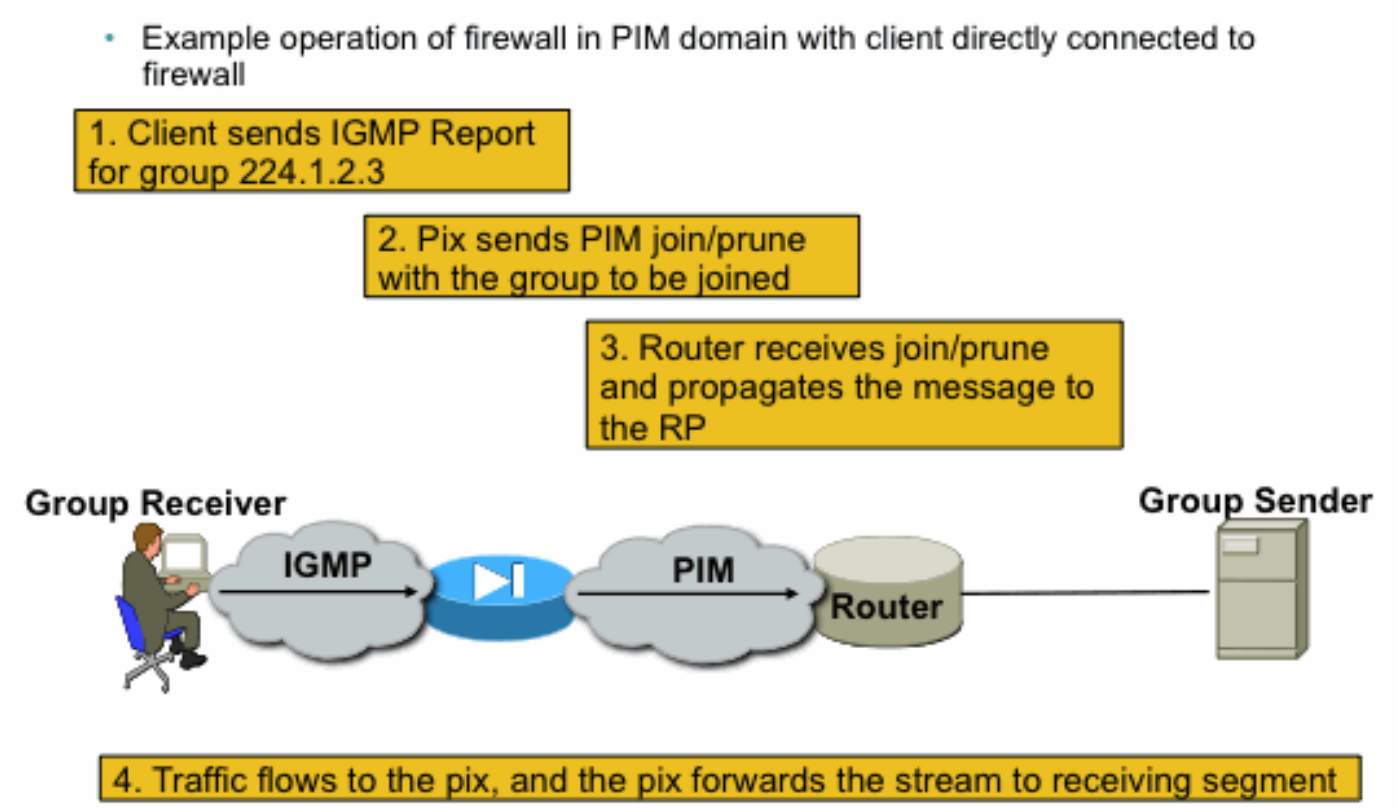
- Mode intermédiaire PIM (préféré)
- Stub-mode IGMP (protocole de gestion de groupes Internet (IGMP), RFC 2236 IGMPv2)

Le mode intermédiaire PIM est le choix préféré parce que l'ASA communique avec des voisins utilisant un véritable protocole de routage de Multidiffusion (PIM). Le Stub-mode IGMP était la seule option de configuration de Multidiffusion avant que la version 7.0 ASA ait été libérée, et actionnée en expédiant simplement des rapports IGMP reçus des clients vers les Routeurs ascendants.

Exécution de mode intermédiaire PIM

- L'ASA prend en charge le mode intermédiaire PIM et le mode bidirectionnel PIM.
- Des commandes de mode intermédiaire PIM et de stub-mode IGMP ne doivent pas être configurées simultanément.
- Avec le mode intermédiaire PIM que tout le trafic de multidiffusion au commencement circule au point de rendez-vous (RP), puis est expédié vers les récepteurs. Après que certains chronomètrent l'écoulement de Multidiffusion ira directement de la source aux récepteurs (sautant le RP).

L'image ci-dessous illustre un déploiement commun où l'ASA a des clients de Multidiffusion sur une interface, et des voisins PIM sur des autres :



Configuration d'échantillon de mode intermédiaire PIM

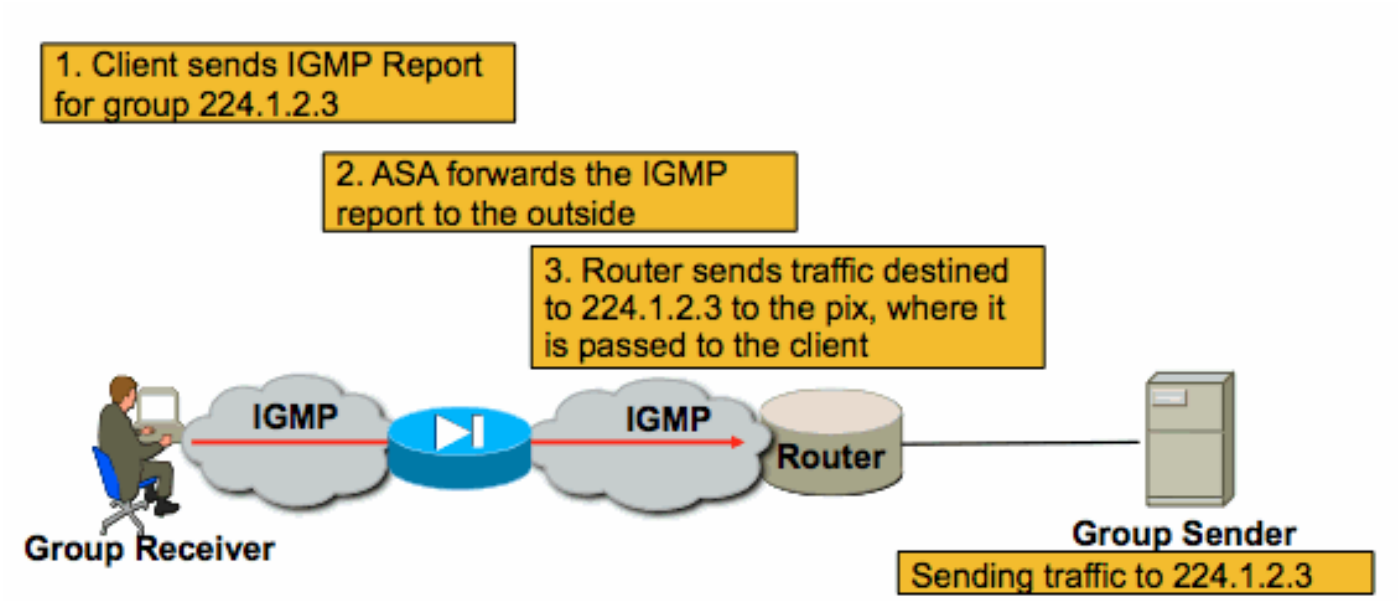
Procédez comme suit :

1. Routage de Multidiffusion d'enable (mode de configuration globale).`ASA(config)# multicast-routing`
2. Définissez l'adresse de point de rendez-vous PIM.`ASA(config)# pim rp-address 172.18.123.3`
3. Permettez les paquets de multidiffusion dedans sur l'interface appropriée (nécessaire seulement si la stratégie de sécurité de l'ASA bloque les paquets de multidiffusion d'arrivée).`access-list 105 extended permit ip any host 224.1.2.3`
`access-group 105 in interface outside`

Exécution de Stub-mode IGMP

- En Stub-mode IGMP l'ASA agit en tant que client de Multidiffusion en générant ou en expédiant des rapports IGMP (également connus sous le nom d'IGMP « se joint ») vers des routeurs contigus, pour déclencher la réception du trafic de multidiffusion
- Les Routeurs enverront périodiquement des requêtes aux hôtes pour voir si n'importe quel noeud sur le réseau veut continuer à recevoir le trafic de multidiffusion.
- Le Stub-mode IGMP n'est pas recommandé parce que le mode intermédiaire PIM offre beaucoup d'avantages au-dessus de Stub-mode (trafic de multidiffusion plus efficace y compris circule, capacité de participer à PIM, etc.).

L'image ci-dessous illustre le fonctionnement de base d'une ASA configurée pour le Stub-mode IGMP.



Configuration de Stub-mode IGMP

Procédez comme suit :

1. Routage de Multidiffusion d'enable (mode de configuration globale).`ASA(config)# multicast-routing`
2. Sur l'interface sur laquelle vous recevrez les états d'igmp, configurez la commande d'en avant-interface d'igmp. Expédiez aux paquets l'interface vers la source du flot. Dans

l'exemple ci-dessous, les récepteurs multicasts sont directement connectés à l'interface interne, et la source multicast est au delà de l'interface extérieure.!

```
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. Permettez les paquets de multidiffusion dedans sur l'interface appropriée (seulement nécessaire si la stratégie de sécurité de l'ASA refuse le trafic de multidiffusion d'arrivée).`access-list 105 extended permit ip any host 224.1.2.3` `access-group 105 in interface outside`Souvent il y a confusion autour des différentes commandes de **sous-modèle d'interface d'igmp**, et le diagramme au-dessous des tentatives de décrire quand utiliser chacun
:

igmp forward interface <interface>

```
!
Interface FastEthernet0/1
 nameif inside
 security-level 100
 ip address 10.0.0.1
255.255.255.0
 igmp forward interface outside
!
```

Causes the firewall to forward IGMP reports received on the inside interface out the outside interface. You would use this command if multicast receivers were on the inside interface and the multicast source was somewhere out the outside interface

igmp join-group <group name>

```
!
Interface FastEthernet0/1
 nameif inside
 security-level 100
 ip address 10.0.0.1
255.255.255.0
 igmp join-group 224.1.2.3
!
```

Tells the firewall that there are hosts behind the inside interface that might want to receive the traffic for the group. It will send IGMP reports out the interface telling the LAN segment that the firewall wishes to receive the stream. It will also add the inside interface to the OIL list for the group. This method is not recommended; If you need to cause the firewall to add an interface to the OIL for an mroute, use the static-group command below

igmp static-group <group name>

```
!
Interface FastEthernet0/1
 nameif inside
 security-level 100
 ip address 10.0.0.1
255.255.255.0
 igmp static-group 224.1.2.3
!
```

Tells the firewall that there are hosts behind the inside interface that might want to receive the traffic for the group. It will simply add the inside interface to the OIL list for the group. This is useful for simulating a multicast receiver behind the inside interface.

Dépannage de la méthodologie

Les informations pour collecter des problèmes multicasts de pour le dépannage

Afin de complètement comprendre et diagnostiquer un problème de Fonction Multicast Forwarding sur l'ASA, quelques ou tous ces informations pourraient être nécessaires :

- Une description de la topologie du réseau, y compris l'emplacement FO les expéditeurs de

Multidiffusion, des récepteurs, et du point de rendez-vous.
- L'adresse IP spécifique de groupe que le trafic utilise, aussi bien que les ports et les protocoles utilisés.
- Syslog générés par l'ASA lorsque le flot de Multidiffusion a le problème.
- Sortie de commande show spécifique de l'interface de ligne de commande ASA, incluant :`show mroute`
  `show mfib`
  `show pim neighbor`
  `show route`
  `show tech-support`
- Captures de paquet pour afficher si les données multicast arrivent à l'ASA, et si les paquets sont expédiés par l'ASA.
- Captures de paquet affichant des paquets IGMP et/ou PIM.
- Les informations des périphériques adjacents de Multidiffusion (Routeurs) comme le « mroute d'exposition » et le « mfib d'exposition ».
- Captures et/ou commandes show de paquet de déterminer si l'ASA relâche les paquets de multidiffusion. La commande « de baisse d'asp d'exposition » peut être utilisée pour déterminer si l'ASA relâche les paquets. Supplémentaire, des captures de paquet du type « asp-baisse » peuvent être utilisées pour capturer tous les paquets que l'ASA relâche, puis être examinées pour voir si les paquets de multidiffusion sont présents dans la capture de baisse.

Sortie de commande show utile

La sortie de commande de **mroute d'exposition** affiche les divers groupes et informations d'expédition, et est très semblable à la commande de **mroute d'exposition** IOS. La commande de **mfib d'exposition** affiche le statut d'expédition des divers groupes de multidiffusion. Il est particulièrement important d'observer le compteur de *transfert des paquets*, aussi bien qu'*autre* (qui indiquent des baisses) :

```
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 de **clears mfib counters** peut être utilisée pour effacer les compteurs, qui est très utile pendant le test :

```
ciscoasa# clear mfib counters
```

```
ciscoasa#
```

Utilisant des captures de paquet pour capturer le trafic de multidiffusion

L'utilitaire à bord de capture du paquet de l'ASA est très utile pour dépanner des problèmes multicasts. Dans l'exemple ci-dessous, tous les paquets arrivant au DMZ de l'ASA relient, ont destiné à 239.17.17.17 seront capturés :

```
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
....
```

Les captures de paquet sont également utiles pour capturer le trafic PIM et IGMP. La capture ci-dessous affiche que l'interface interne a reçu un paquet IGMP (protocole IP 2) originaire de 10.0.0.2 :

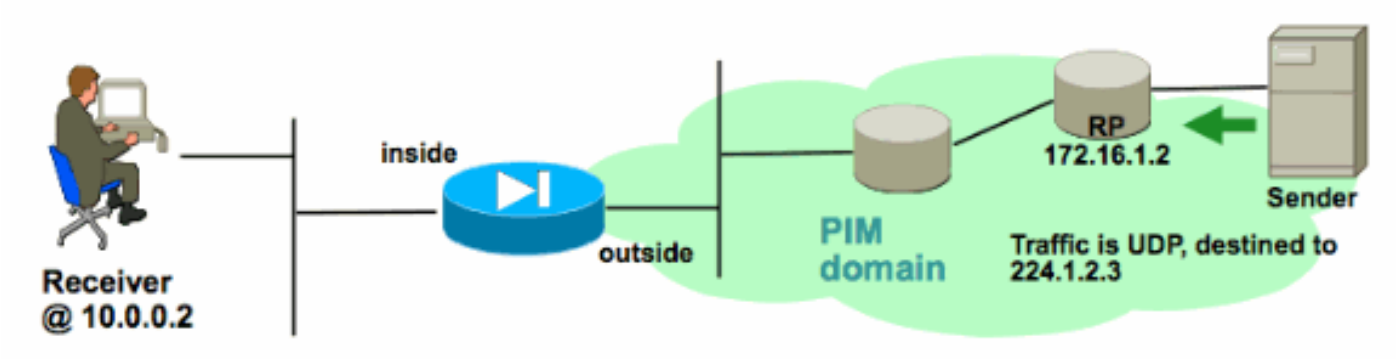
```
ciscoasa# capture capin interface inside
ciscoasa# capture capin match igmp any any
ciscoasa# show cap capin
1 packets captured
1: 10:47:53.540346 802.1Q vlan#15 P0 10.0.0.2 > 224.1.2.3:
  ip-proto-2, length 8
ciscoasa#
```

Déploiement de Multidiffusion de mode intermédiaire PIM de l'exemple ASA

Les diagrammes ci-dessous montrent comment l'ASA interagit avec les périphériques voisins pour obtenir le trafic de multidiffusion circulant avec le mode intermédiaire PIM. Dans cet exemple spécifique, l'ASA reçoit.

Compréhension de la topologie du réseau

Déterminez exactement où l'expéditeur et le récepteur du flot spécifique de Multidiffusion vous testent résident. En outre, déterminez l'adresse IP de groupe de multidiffusion étant utilisée, aussi bien que l'emplacement du point de rendez-vous.



Dans ce cas, les données devraient être reçues à l'interface extérieure de l'ASA, et être expédiées au récepteur multicast sur l'interface interne. Puisque le récepteur est dans le même IP de sous-réseau que l'interface interne de l'ASA, comptez voir un rapport IGMP reçu à l'interface interne de l'ASA quand les demandes de client de recevoir le flot. L'adresse IP de l'expéditeur est 192.168.1.50.

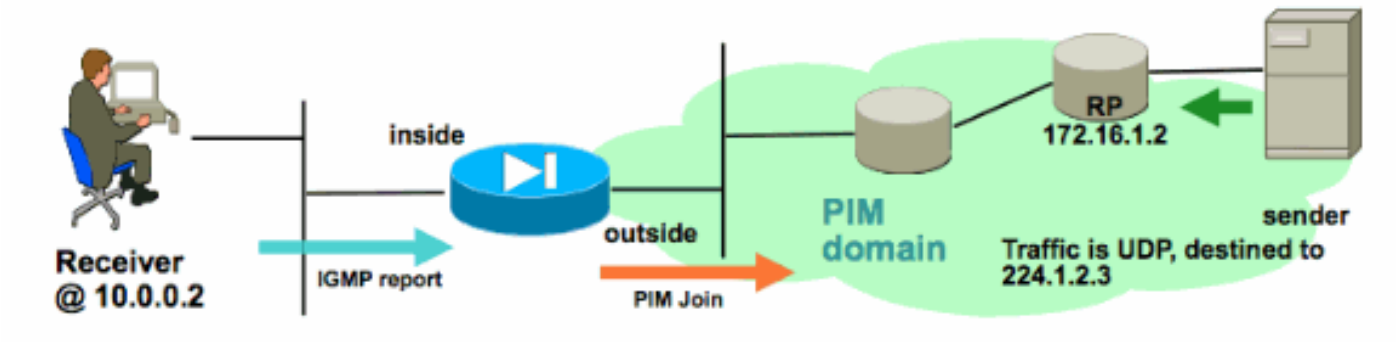
Vérifier l'ASA reçoit le rapport IGMP du récepteur

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

Les captures de paquet et la sortie de mettent au point l'igmp peuvent être utilisées pour vérifier que l'ASA reçue, et avec succès traitée le message IGMP.

Vérifier l'ASA envoie un PIM joignent le message vers le point de rendez-vous

L'ASA interprète le rapport IGMP et génère un PIM joignent le message, puis lui envoient l'interface vers le RP.

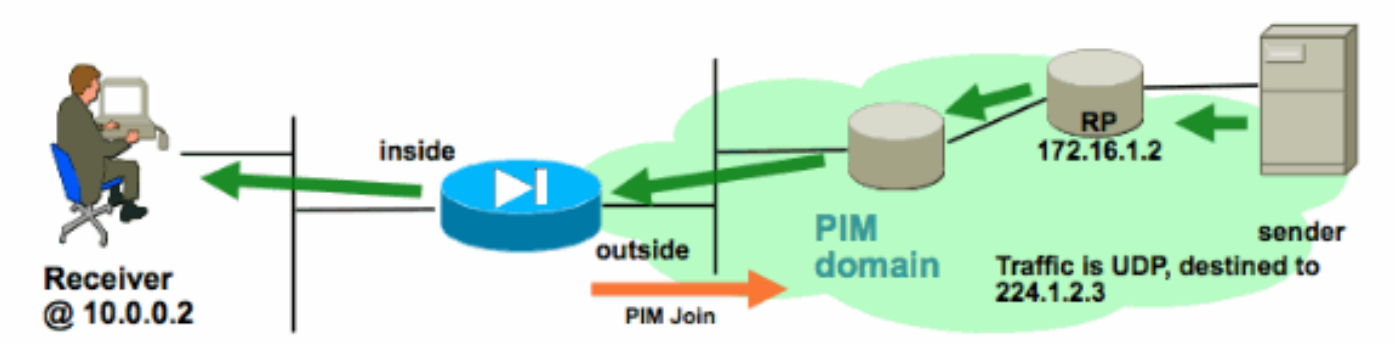


La sortie ci-dessous est de mettent au point le groupe 224.1.2.3 de pim et affichent que l'ASA envoyant avec succès le PIM joignent le message. L'expéditeur du flot de Multidiffusion est 192.168.1.50

```
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 192.168.1.5
```

Vérifier l'ASA reçoit et en avant le flot de Multidiffusion

L'ASA commence recevant le trafic de multidiffusion sur l'interface extérieure (illustrée par les flèches vertes), et l'expédiant aux récepteurs sur l'intérieur.



Le mroute d'exposition et les commandes de **mfib d'exposition**, aussi bien que des captures de paquet, peuvent être utilisés pour vérifier l'ASA reçoit et en avant les paquets de multidiffusion.

Une connexion sera établie dans la table de la connexion de l'ASA pour représenter le flot de Multidiffusion :

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

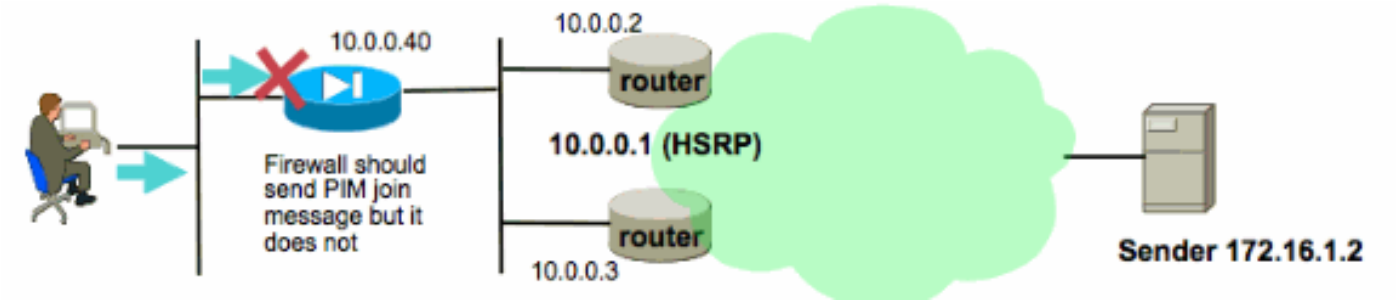
Analyse de données

Problèmes courants

Cette section fournit une gamme de problèmes associés par Multidiffusion du monde réel ASA que les administrateurs réseau ont rencontrés dans le passé.

L'ASA n'envoie pas des messages PIM vers les Routeurs en amont dus au HSRP

Quand ce problème est produit, l'ASA n'envoie pas à tous les messages PIM une interface. Le diagramme ci-dessous prouve que l'ASA ne peut pas envoyer des messages PIM vers l'expéditeur, mais le même problème peut être vu quand l'ASA doit envoyer un message PIM vers le RP.



La sortie de **mettent au point le pim** prouve que l'ASA ne peut pas envoyer le message PIM au routeur du prochain saut en amont :

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

Cette question n'est pas spécifique à l'ASA, et affecte également des Routeurs. Le problème est

déclenché par la combinaison de la configuration de table de routage de l'ASA et de la configuration de HSRP utilisées par les voisins PIM.

La table de routage de l'ASA indique l'IP 10.0.0.1 de HSRP comme périphérique de prochain-saut :

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

Cependant, les relations voisines PIM ne sont formées entre les adresses IP d'interface physique des Routeurs, et pas l'IP de HSRP :

```
ciscoasa# sh 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 ne fait pas le travail de mode intermédiaire PIM avec une artère statique à une adresse de HSRP ? pour plus d'informations.

Un extrait du document :

« Pourquoi le routeur n'envoie-t-il pas le message de joindre/pruneau ? RFC 2362 déclare que « un routeur envoie un périodique se joignent/message de pruneau à chaque voisin distinct RPF associé avec le chaque (S, G), (, G) et (*, *, RP) entrée. Des messages joignez/pruneau sont envoyés seulement si le voisin RPF est un voisin PIM. »*

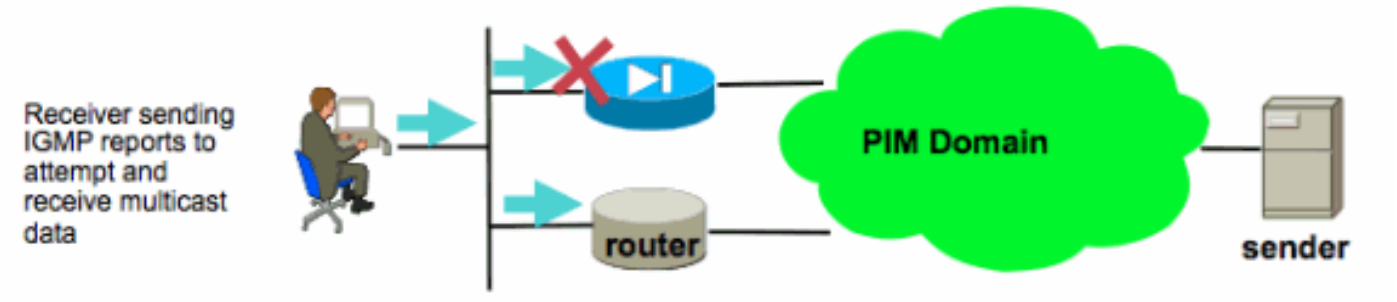
Afin d'atténuer le problème, ajoutez une entrée statique de mroute sur l'ASA pour le trafic en question. Assurez-vous qu'il indique une de deux adresses IP de l'interface du routeur (10.0.0.2 ou 10.0.0.3 dans l'exemple ci-dessus). Dans ce cas, la commande suivante permet à l'ASA pour envoyer des messages PIM orientés sur l'expéditeur de Multidiffusion chez 172.16.1.2 :

```
ciscoasa(config)# mroute 172.16.1.2 255.255.255.255 10.0.0.3
```

Une fois que ceci est fait la table de routage de Multidiffusion ignorera la table de routage d'unicast de l'ASA, et l'ASA enverra les messages PIM directement au voisin de 10.0.0.3.

L'ASA ignore des rapports IGMP puisque ce n'est pas le routeur indiqué sur le segment de RÉSEAU LOCAL

Pour ce problème, l'ASA reçoit un rapport IGMP d'un récepteur multicast directement connecté, pourtant elle l'ignore. Aucune sortie de débogage ne sera générée et le paquet est simplement lâché, et la réception de flot échoue.



Pour ce problème, l'ASA ignore le paquet parce que ce n'est pas le PIM routeur indiqué élu sur le segment de RÉSEAU LOCAL où les clients résident.

La sortie ASA CLI ci-dessous prouve qu'un différent périphérique est le routeur indiqué (dénoté par le « DR ») sur le réseau d'interface interne :

```
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 de **multicast-routing** est ajoutée à la configuration de l'ASA. S'il y a d'autres voisins PIM (d'autres Routeurs ou ASA) sur l'interface interne de l'ASA (où les clients résident) et un de ces voisins ont été élus parce que le DR pour ce segment, alors autre, les Routeurs non-DR relâchera des rapports IGMP. La solution est de désactiver PIM sur l'interface de l'ASA (avec l'**aucune** commande de **pim** sur l'interface impliquée), ou de faire à l'ASA le DR pour le segment utilisant la **commande d'interface de dr-priority de pim**.

L'ASA n'expédie pas le trafic de multidiffusion dans la plage 232.x.x.x/8

Cette plage d'adresses sert avec le Fonction Source Specific Multicast (SSM) que l'ASA ne prend en charge pas actuellement.

La sortie de **mettent au point l'igmp** affichera cette erreur :

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

Les paquets de multidiffusion de baisses ASA dus au contrôle de Reverse Path Forwarding

Dans ce cas, l'ASA reçoit le trafic de multidiffusion sur une interface, mais elle n'est pas expédiée en fonction au récepteur. Des paquets sont lâchés par l'ASA parce qu'ils échouent le contrôle de Sécurité du Reverse Path Forwarding (RPF). Le RPF est activé sur toutes les interfaces pour le trafic de multidiffusion et ne peut pas être désactivé (pour des paquets monodiffusions le contrôle n'est pas allumé par défaut, et est activé avec l'**IP vérifient la commande d'interface de chemin inverse**).

En raison du contrôle RPF, quand le trafic de multidiffusion est reçu à une interface, l'ASA vérifie pour voir qu'elle a une route de retour vers la source de trafic du trafic de multidiffusion (elle vérifie la table de routage d'unicast et de Multidiffusion) sur cette interface. S'il n'a pas une artère à l'expéditeur, il relâche le paquet. Ces baisses peuvent être vues comme compteur dans la sortie de la **baisse d'asp d'exposition** :

```
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
```

Ce problème peut être atténué en ajoutant une entrée de table spécifique de routage de Multidiffusion à l'ASA pour l'expéditeur du trafic. Dans l'exemple ci-dessous, la commande de mroute est utilisée de satisfaire le RPF vérifient le trafic de multidiffusion originaire de 172.16.1.2 a reçu sur l'interface extérieure :

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

L'ASA ne génère pas le PIM Join sur le basculement PIM à la Source-arborescence

Au commencement, les paquets de multidiffusion de mode intermédiaire PIM découleront de l'expéditeur de Multidiffusion au RP, puis du RP au récepteur par l'intermédiaire d'un arbre de multicast partagé. Cependant, une fois que le débit binaire d'agrégat atteint un certain seuil, le routeur le plus proche du récepteur multicast tentera de recevoir le trafic le long de l'arborescence de source-particularité. Ce routeur génèrera un nouveau PIM se joignent pour le groupe et l'envoient vers l'expéditeur du flot de Multidiffusion (et pas vers le RP, en tant qu'avant).

Selon la topologie du réseau, l'expéditeur du trafic de multidiffusion pourrait résider sur une interface différente ASA que le RP. Quand l'ASA reçoit les PIM se joignent pour commuter à l'arborescence spécifique de source, l'ASA doivent avoir une artère à l'adresse IP de l'expéditeur. Si cette artère n'est pas trouvée, les PIM joignent le paquet seront relâchés et le message suivant sera vu dans la sortie de **mettent au point le pim** :

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

La solution pour ce problème est d'ajouter une entrée statique de mroute pour l'expéditeur du flot, précisant l'interface ASA hors fonction dont l'expéditeur réside.

L'ASA relâche des paquets de multidiffusion dus au Time to Live (TTL) dépassé

Dans ce cas, le trafic de multidiffusion manque parce que le TTL des paquets est si bas. Ceci fait pour les relâcher l'ASA, ou un autre périphérique dans le réseau.

Souvent les paquets de multidiffusion ont la valeur d'IP TTL réglée très basse par l'application qui les a envoyés. Parfois ceci est fait par défaut pour aider à s'assurer que le trafic de multidiffusion ne voyage pas trop loin cependant le réseau. Par exemple, par défaut l'application cliente visuelle de RÉSEAU LOCAL (un outil populaire d'émetteur et de test de Multidiffusion) place le TTL dans le paquet IP au par défaut de 1par.

L'ASA éprouve l'utilisation du CPU élevée et les paquets relâchés dus à la topologie spécifique de Multidiffusion

L'ASA pourrait éprouver la CPU de haute et le flot de Multidiffusion pourrait éprouver des pertes de paquets si tout les suivre sont vrai au sujet de la topologie de Multidiffusion :

1. L'ASA agit en tant que RP.
2. L'ASA est le premier récepteur de saut du flot de Multidiffusion. Ceci signifie que l'expéditeur de Multidiffusion est dans le même IP de sous-réseau une interface ASA.
3. L'ASA est le dernier routeur de saut du flot de Multidiffusion. Ceci signifie qu'un récepteur multicast est dans le même IP de sous-réseau comme interface ASA.

Si tous les ci-dessus sont vrais, alors le dû font une limite de calcul que l'ASA sera forcée pour traiter le commutateur le trafic de multidiffusion. Ceci a comme conséquence les flots élevés de Multidiffusion de débit de données pour éprouver des pertes de paquets. Le compteur de baisse d'asp d'exposition qu'incréments quand ces paquets sont lâchés est la coup de volée-débit-limite.

Afin de déterminer si une ASA rencontre ce problème, terminez-vous ces étapes :

Étape 1 : Vérifiez si l'ASA est le RP à l'aide des deux commandes :

```
show run pim
show pim tunnel
```

Étape 2 : Vérifiez si l'ASA est le dernier routeur de saut à l'aide de cette commande :

```
show igmp group <mcast_group_IP>
```

Étape 3 : Vérifiez si l'ASA est le premier routeur de saut à l'aide de cette commande :

```
show mroute <mcast_group_IP>
```

Un récepteur multicast déconnectant interrompt la réception de groupe de multidiffusion sur d'autres interfaces

Seulement les ASA fonctionnant en Stub-mode IGMP rencontrent ce problème. Les ASA qui participent au routage de Multidiffusion PIM ne sont pas affectées.

La question est identifiée par la bogue CSCeg48235 - IGMP : Arrêter le rcvr de groupe interrompt la réception de groupe sur d'autres interfaces

C'est la note de mise à jour de la bogue, qui explique le problème :

```
Symptom:
When a PIX or ASA firewall is configured for IGMP stub mode multicast reception and
traffic from a multicast group is forwarded to more than one interface, if a host
behind a receiving interface sends an IGMP Leave message for the group, it could
temporarily interrupt the reception for that group on other interfaces of the firewall.

The problem is triggered when the firewall forwards the IGMP leave for the group
towards the upstream device; that device then sends a IGMP query to determine if any
other receivers exist out that interface towards the firewall, but the firewall does
not report that it still has valid receivers.

Conditions:
The PIX or ASA must be configured for IGMP stub mode multicast. IGMP stub mode is a
legacy multicast forwarding technique, whereby IGMP packets from receivers are forwarded
through the firewall towards the source of the stream. It is recommended to use PIM
multicast routing instead of stub igmp forwarding.

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,
causing their IGMP reports to be forwarded towards the sender more frequently, thus
restarting the stream quicker.
```

L'ASA relâche des paquets de multidiffusion dus à la stratégie de sécurité de la liste d'accès sortante

Avec cette problématique spécifique l'ASA relâche correctement des paquets de multidiffusion (par stratégie de sécurité configurée). Cependant, il est difficile que l'administrateur réseau identifie la raison pour les pertes de paquets. Dans ce cas, l'ASA relâche des paquets dus à la liste d'accès sortante configurée pour une interface. Le contournement est de permettre le flot de Multidiffusion dans la liste d'accès sortante.

Quand ceci se produit, des paquets de multidiffusion seront lâchés et le compteur de baisse d'ASP sera « point de gel aucun intrf de sortie de mcast (NO--mcast-intrf) ».

L'ASA relâche les paquets premiers quand un flot de Multidiffusion est d'abord commencé

Quand les premiers paquets d'un flot de Multidiffusion arrivent à l'ASA, l'ASA doit établir cette connexion particulière de Multidiffusion et l'entrée associée de mroute pour expédier les paquets. Tandis que l'entrée est créée quelques paquets de multidiffusion pourraient être lâchés jusqu'au mroute et des connexions ont été établies (habituellement ceci prend moins qu'une seconde). Une

fois que l'installation de flot de Multidiffusion est complète, les paquets ne seront plus débit limité.

Les paquets lâchés pour cette raison auront la raison de baisse d'ASP « du raté limit de coup de volée (de coup de volée-débit-limite) dépassé ». Est ci-dessous la sortie de l'**asp de show capture** (où l'asp est une capture de baisse d'ASP configurée sur l'ASA pour capturer les paquets lâchés) et vous pouvez voir les paquets de multidiffusion qui ont été lâchés pour cette raison :

```
ASA # sh 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 rate limit exceeded
   2: 16:14:49.919172 10.23.2.2.810 > 239.255.123.123.890:  udp 32 Drop-reason:
 (punt-rate-limit) Punt rate limit exceeded
2 packets shown
```

Informations connexes

- Support et documentation techniques - Cisco Systems