Troubleshooting y problemas comunes del Multicast ASA

Contenido

Introducción

Este documento explica las capacidades de multidifusión del dispositivo de seguridad adaptante (ASA), así como los problemas potenciales que pueden ser encontrados al usar la característica.

prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Multicast ASA

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Información sobre la Función

La guía del comando line configuration ASA delinea la característica del ruteo multicast y cómo configurarla:

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

El Multicast en el ASA se puede configurar en uno de dos modos:

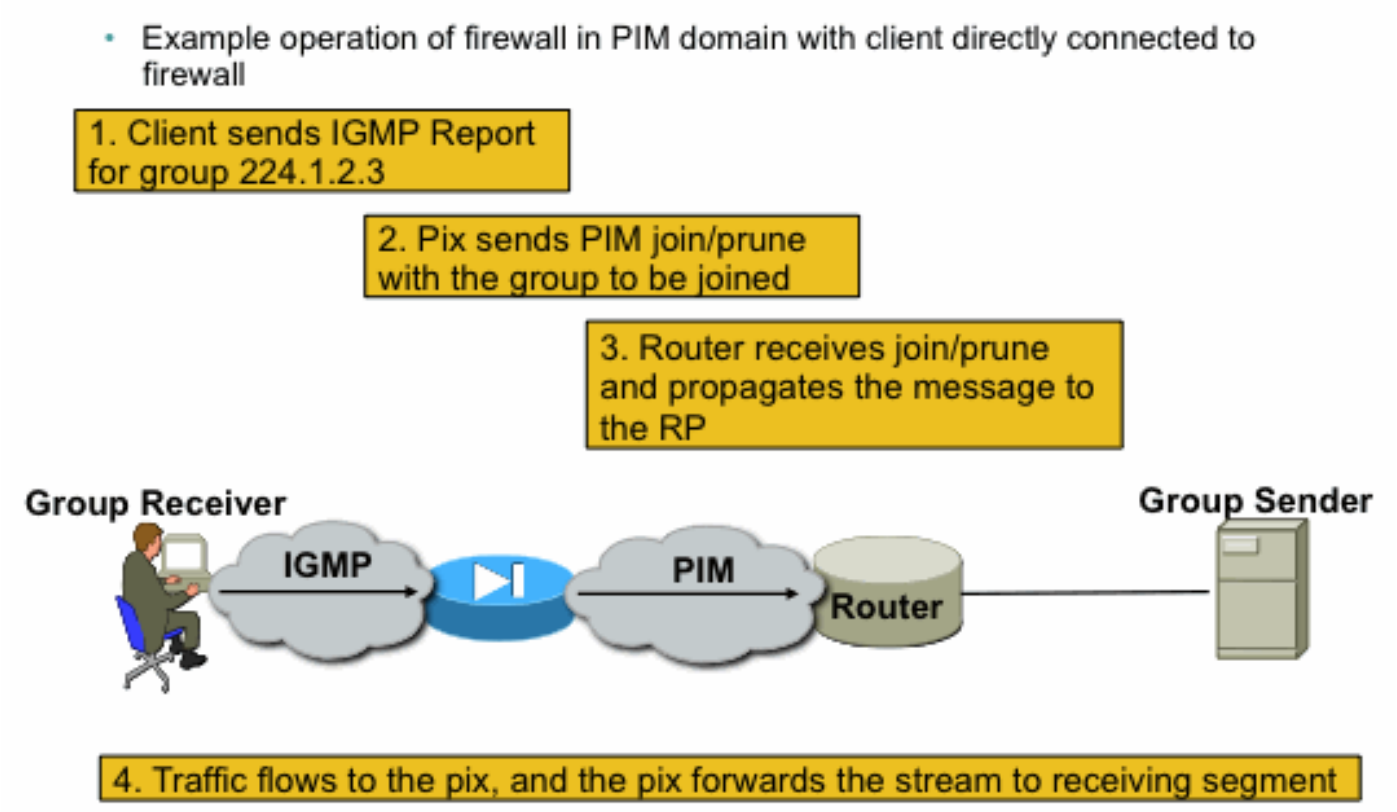
- Modo disperso de PIM (preferido)
- IGMP Stub-MODE (Internet Group Management Protocol, IGMPv2 del RFC 2236)

El modo disperso de PIM es la opción preferida porque el ASA comunica con los vecinos que usan un Multicast Routing Protocol verdadero (PIM). El IGMP Stub-MODE era la única opción de configuración del Multicast antes de que la Versión de ASA 7.0 fuera liberada, y actuada simplemente remitiendo los informes IGMP recibidos de los clientes hacia los routeres ascendentes.

Operación del modo disperso de PIM

- El ASA soporta el modo disperso de PIM y el modo bidireccional PIM.
- El modo disperso de PIM y los comandos IGMP stub-MODE no deben ser configurados en paralelo.
- Con el modo disperso de PIM que todo el tráfico Multicast fluye al (RP) del punto de encuentro, después que se remite inicialmente hacia los receptores. Después de que algunos midan el tiempo el flujo del Multicast irá directamente de la fuente a los receptores (que desvían el RP).

La imagen abajo ilustra una instalación común donde el ASA tiene los clientes del Multicast en una interfaz, y a los vecinos del PIM en otra:



Configuración de muestra del modo disperso de PIM

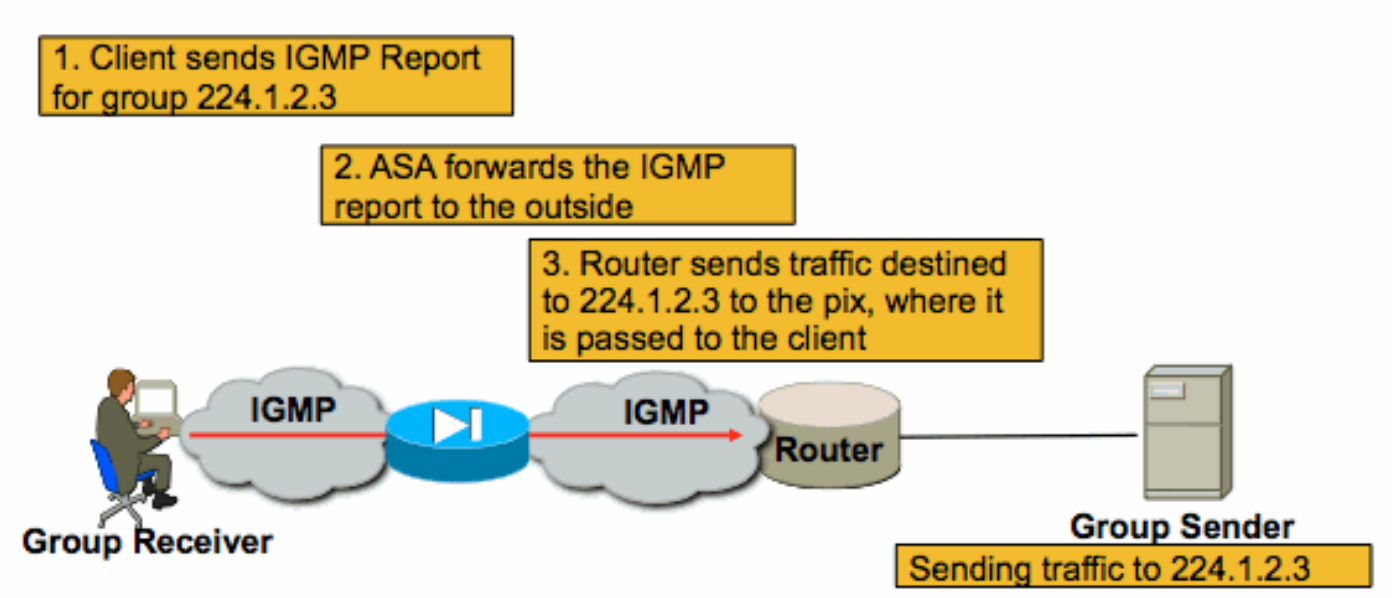
Complete estos pasos:

1. Habilite el ruteo multicast (modo de configuración global).`ASA(config)# multicast-routing`
2. Defina el direccionamiento del punto de encuentro PIM.`ASA(config)# pim rp-address 172.18.123.3`
3. Permita los paquetes de multidifusión adentro en la interfaz apropiada (necesaria solamente si la política de seguridad del ASA está bloqueando los paquetes de multidifusión entrantes).`access-list 105 extended permit ip any host 224.1.2.3`
`access-group 105 in interface outside`

Operación IGMP Stub-MODE

- En IGMP Stub-MODE el ASA actúa como cliente del Multicast generando o remitiendo los informes IGMP (también conocidos como IGMP “se une a”) hacia los routeres adyacentes, para accionar la recepción del tráfico Multicast
- El Routers enviará periódicamente las interrogaciones a los host para ver si cualquier nodo en la red quiere continuar recibiendo el tráfico Multicast.
- El IGMP Stub-MODE no se recomienda porque el modo disperso de PIM ofrece muchas ventajas sobre el Stub-MODE (tráfico Multicast más eficiente incluyendo fluye, capacidad de participar en el PIM, etc).

La imagen abajo ilustra la operación básica de un ASA configurado para IGMP Stub-MODE.



Configuración IGMP Stub-MODE

Complete estos pasos:

1. Habilite el ruteo multicast (modo de configuración global).`ASA(config)# multicast-routing`
2. En la interfaz en la cual usted recibirá los informes del igmp, configure el comando de la delantero-interfaz del igmp. Remita a paquetes hacia fuera la interfaz hacia la fuente de la secuencia. En el ejemplo abajo, los receptores de multidifusión están conectados directamente con la interfaz interior, y el origen de multidifusión está más allá de la interfaz

exterior.`!`

```
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. Permita los paquetes de multidifusión adentro en la interfaz apropiada (solamente necesaria si la política de seguridad del ASA niega el tráfico Multicast entrante).`access-list 105 extended permit ip any host 224.1.2.3`

   `access-group 105 in interface outside`A menudo hay confusión alrededor de los diversos comandos de la **interfaz sub-MODE del igmp**, y el diagrama a continuación intenta describir cuando utilizar cada
   uno:

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.

Metodología de Troubleshooting

Información para recolectar al resolver problemas los problemas de multidifusión

Para entender y diagnosticar totalmente un problema del Reenvío de multicast en el ASA, una cierta o todo esta información pudieron ser necesarios:

- Una descripción de la topología de red, incluyendo la ubicación FO los remitentes del Multicast, de los receptores, y del punto de encuentro.

- La dirección IP específica del grupo que el tráfico está utilizando, así como los puertos y protocolos empleados.
- Syslog generados por el ASA cuando la secuencia de multidifusión tiene problema.
- Salida del comando show específica de la interfaz de línea de comando ASA, incluyendo:`show mroute`
  `show mfib`
  `show pim neighbor`
  `show route`
  `show tech-support`
- Capturas de paquetes para mostrar si los datos de multidifusión llegan el ASA, y si los paquetes se remiten con el ASA.
- Capturas de paquetes que muestran el IGMP y/o los paquetes PIM.
- Información de los dispositivos adyacentes del Multicast (Routers) por ejemplo la “ruta multicast de la demostración” y el “mfib de la demostración”.
- Capturas de paquetes y/o comandos show de determinar si el ASA está cayendo los paquetes de multidifusión. “El comando del descenso de la demostración ASP” se puede utilizar para determinar si el ASA está cayendo los paquetes. Además, las capturas de paquetes del tipo “ASP-descenso” pueden ser utilizadas para capturar todos los paquetes que el ASA cae, después ser examinadas para considerar si los paquetes de multidifusión están presentes en la captura del descenso.

Salida del comando show útil

La salida de comando de la **ruta multicast de la demostración** muestra los diversos grupos y información de reenvío, y es muy similar al comando de la **ruta multicast de la demostración** IOS. El comando del **mfib de la demostración** visualiza el estatus de la expedición de los diversos grupos de multidifusión. Es especialmente importante observar al contador de paquetes de la *expedición*, así como *otro* (que indica los descensos):

```
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#
```

El comando **claro de los contadores del mfib** se puede utilizar para borrar los contadores, que es muy útil durante la prueba:

```
ciscoasa# clear mfib counters
ciscoasa#
```

Usando las capturas de paquetes para capturar el tráfico Multicast

La utilidad a bordo de la captura de paquetes ASA es muy útil para resolver problemas los problemas de multidifusión. En el ejemplo abajo, todos los paquetes que llegan el DMZ ASA interconectan, destinaron a 239.17.17.17 serán capturados:

```
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
....
```

Las capturas de paquetes son también útiles para capturar el tráfico PIM y IGMP. La captura abajo muestra que la interfaz interior ha recibido un paquete IGMP (protocolo IP 2) originado de 10.0.0.2:

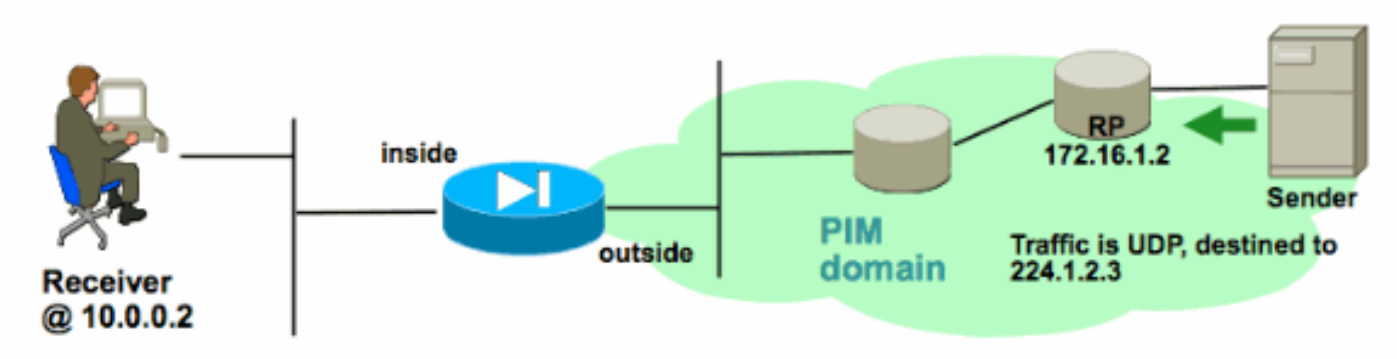
```
ciscoasa# capture capin interface inside
ciscoasa# capture capin match igmp any any
ciscoasa# show cap capin
1 packets captured
1: 10:47:53.540346 802.1Q vlan#15 P0 10.0.0.2 > 224.1.2.3:
  ip-proto-2, length 8
ciscoasa#
```

Despliegue del Multicast del modo disperso de PIM del ejemplo ASA

Los diagramas a continuación ilustran cómo el ASA obra recíprocamente con los dispositivos vecinos para conseguir fluir de tráfico Multicast con el modo disperso de PIM. En este ejemplo específico, el ASA recibe.

Comprensión de la topología de red

Determine exactamente donde residen el remitente y el receptor de la secuencia de multidifusión específica usted están probando. También, determine el IP Address del grupo de multidifusión que es utilizado, así como la ubicación del punto de encuentro.



En este caso, los datos se deben recibir en la interfaz exterior del ASA, y remitir al receptor de multidifusión en la interfaz interior. Porque el receptor está en la misma subred IP que la interfaz interior del ASA, espere ver un informe IGMP recibido en la interfaz interior ASA cuando los pedidos de cliente de recibir la secuencia. La dirección IP del remitente es 192.168.1.50.

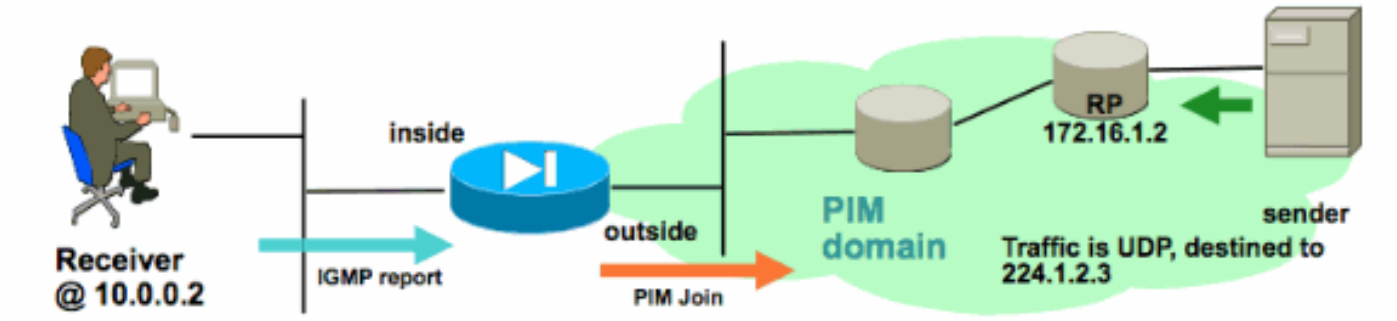
Verificar el ASA recibe el informe IGMP del receptor

En este ejemplo, el informe IGMP es generado por el receptor y procesado por el ASA.

Las capturas de paquetes y la salida del igmp del debug pueden ser utilizadas para verificar que el ASA recibido, y con éxito procesado el mensaje IGMP.

Verificar el ASA envía un mensaje de incorporación PIM hacia el punto de encuentro

El ASA interpreta el informe IGMP y genera un mensaje de incorporación PIM, después le manda la interfaz hacia el RP.



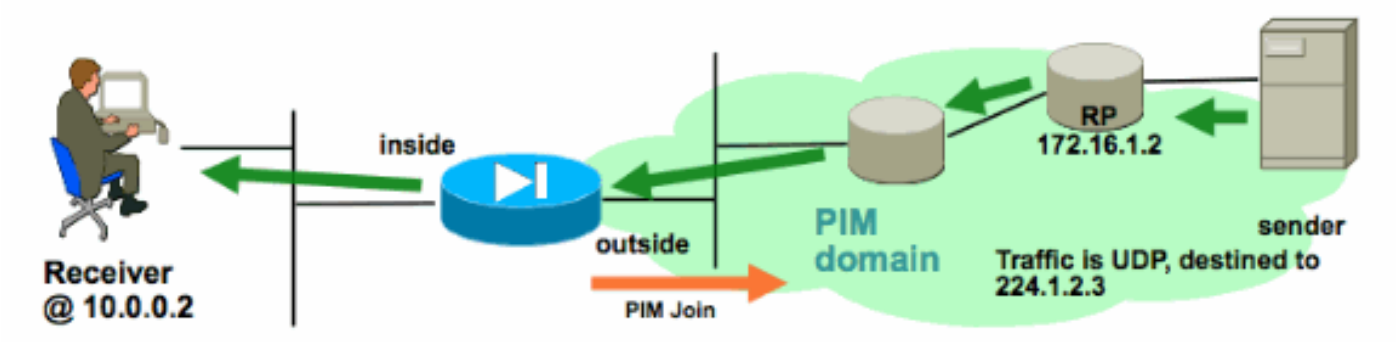
La salida abajo es de grupo 224.1.2.3 del pim del debug y muestra el ASA que envía con éxito el mensaje de incorporación PIM. El remitente de la secuencia de multidifusión es 192.168.1.50

```
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
```

Verificar el ASA recibe y adelante la secuencia de multidifusión

El ASA comienza a recibir el tráfico Multicast en la interfaz exterior (ilustrada por las flechas

verdes), y a remitirlo a los receptores en el interior.



La ruta multicast de la demostración y los comandos del **mfib de la demostración**, así como las capturas de paquetes, se pueden utilizar para verificar el ASA recibe y adelante los paquetes de multidifusión.

Una conexión será construida en la tabla de conexiones ASA para representar la secuencia de multidifusión:

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

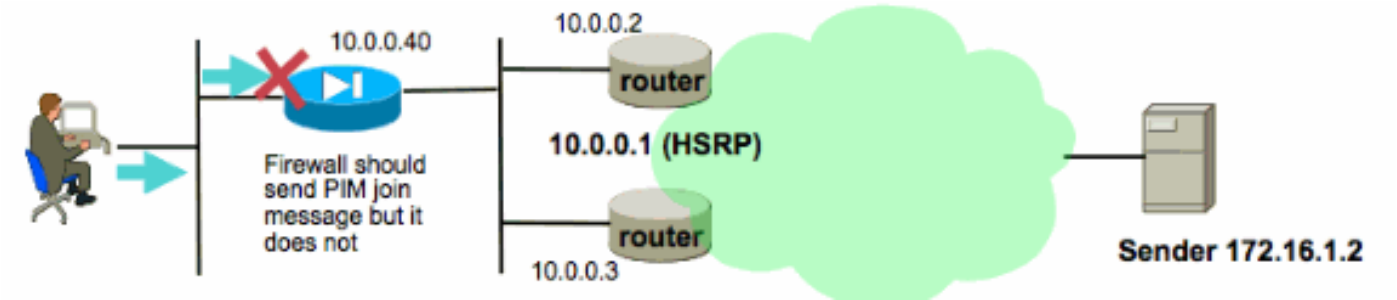
Análisis de datos

Problemas Comunes

Esta sección proporciona una serie de problemas relacionados del mundo real del Multicast ASA que los administradores de la red han encontrado en el pasado.

El ASA no puede enviar los mensajes PIM hacia los routeres ascendentes debido al HSRP

Cuando se encuentra este problema, el ASA no puede mandar ningunos mensajes PIM una interfaz. El diagrama a continuación muestra que el ASA no puede enviar los mensajes PIM hacia el remitente, pero el mismo problema puede ser considerado cuando el ASA necesita enviar un mensaje PIM hacia el RP.



La salida del **pim del debug** muestra que el ASA no puede enviar el mensaje PIM al Next Hop Router por aguas arriba:

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

Este problema no es específico al ASA, y también afecta al Routers. El problema es accionado

por la combinación de la configuración de la tabla de ruteo ASA y de la configuración HSRP usadas por los vecinos del PIM.

La tabla de ruteo ASA señala al IP 10.0.0.1 del HSRP como el dispositivo de Next Hop:

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

Sin embargo, la relación del vecino del PIM se forma entre los IP Addresses de la interfaz física del Routers, y no el IP del 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)
```

¿Refiérase a por qué no lo hace el trabajo del modo disperso de PIM con una Static ruta a una dirección HSRP? para más información.

Un extracto del documento:

¿"Por qué el router no está enviando el mensaje de unión/separación? Los estados del RFC 2362 que "un router envía un mensaje de unión/separación periódico a cada vecino RPF distintivo se asociaron a cada (S, G), (, G) y (*, *, RP) entrada. Se envían los mensajes de unión/separación solamente si el vecino RPF es un vecino del PIM."*

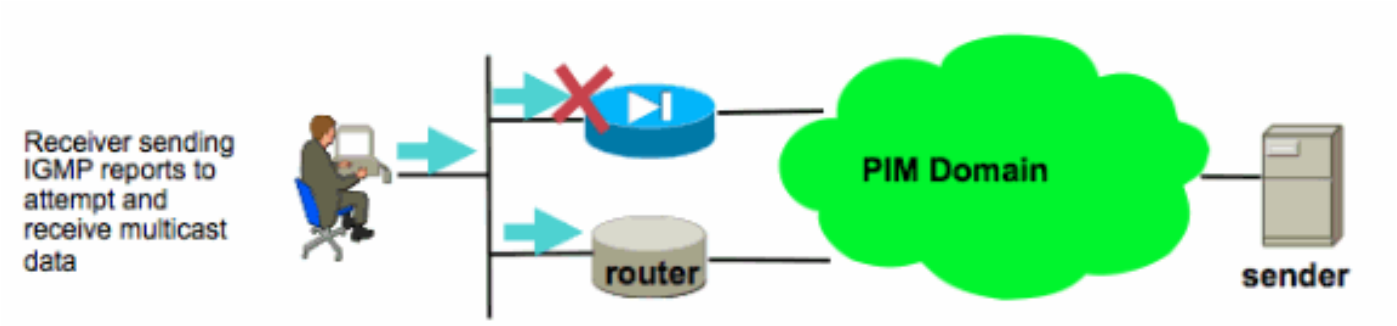
Para atenuar el problema, agregue una entrada del mRoute estático en el ASA para el tráfico en la pregunta. Aseegurese que señala a uno IP Addresses de la interfaz de dos del router (10.0.0.2 o 10.0.0.3 en el ejemplo anterior). En este caso, el siguiente comando permite que el ASA envíe los mensajes PIM dirigidos hacia el remitente del Multicast en 172.16.1.2:

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

Una vez que se hace esto el tabla de Multicast Routing reemplazará la tabla de Unicast Routing del ASA, y el ASA enviará los mensajes PIM directamente al vecino de 10.0.0.3.

El ASA ignora los informes IGMP porque no es el router designado en el segmento LAN

Para este problema, el ASA recibe un informe IGMP de un receptor de multidifusión directamente conectado, con todo lo ignora. No se generará a ninguna salida de los debugs y el paquete se cae simplemente, y la recepción de la secuencia falla.



Para este problema, el ASA está ignorando el paquete porque no es el router designado elegido PIM en el segmento LAN donde residen los clientes.

La salida ASA CLI abajo muestra que un diverso dispositivo es el router designado (denotado por el "DR") en la red de la interfaz interior:

```
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)
```

Por abandono, el PIM se habilita en todas las interfaces ASA cuando el comando del **ruteo multicast** se agrega a la configuración ASA. Si hay otros vecinos del PIM (otro Routers o ASA) en la interfaz interior del ASA (donde residen los clientes) y eligieron uno de esos vecinos porque el DR para ese segmento, después otro, los routeres que no sea DR caerá los informes IGMP. La solución es inhabilitar el PIM en la interfaz ASA (con el **ningún comando pim** en la interfaz implicada), o hacer el ASA el DR para el segmento usando el **comando interface de la DR-prioridad del pim**.

El ASA no puede remitir el tráfico Multicast en el rango 232.x.x.x/8

Este intervalo de direcciones está para el uso con el Source Specific Multicast (SSM) que el ASA no soporta actualmente.

La salida del **igmp del debug** mostrará este error:

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

Los paquetes de multidifusión de los descensos ASA debido al control del reenvío de trayecto inverso

En este caso, el ASA recibe el tráfico Multicast en una interfaz, pero no se remite encendido al receptor. Los paquetes son caídos por el ASA porque fallan la revisión de seguridad del reenvío de trayecto inverso (RPF). El RPF se habilita en todas las interfaces para el tráfico Multicast y no puede ser inhabilitado (para los paquetes de unidifusión el control no está prendido por abandono, y se habilita con el **IP verifica el comando interface del trayecto inverso**).

Debido al revisión de "RPF", cuando el tráfico Multicast se recibe en una interfaz, el ASA marca para ver que tiene una ruta de nuevo a la fuente del tráfico del tráfico Multicast (marca el unicast y el tabla de Multicast Routing) en esa interfaz. Si no tiene una ruta al remitente, cae el paquete. Estos descensos se pueden considerar como contador en la salida del **descenso de la demostración ASP**:

```
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
```

Este problema puede ser atenuado agregando una entrada de tabla específica del ruteo multicast al ASA para el remitente del tráfico. En el ejemplo abajo, se utiliza el comando de la ruta multicast de satisfacer revisión de "RPF" para el tráfico Multicast originado de 172.16.1.2 recibió en la interfaz exterior:

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

El ASA no genera el PIM se une a sobre el intercambio PIM al Fuente-árbol

Inicialmente, los paquetes de multidifusión del modo disperso de PIM fluirán del remitente del Multicast al RP, después del RP al receptor vía un árbol de multidifusión compartido. Sin

embargo, una vez que la velocidad de bits global alcanza cierto umbral, el router más cercano al receptor de multidifusión intentará recibir el tráfico a lo largo del árbol fuente-específico. Este router generará un nuevo PIM se une a para el grupo y lo envía hacia el remitente de la secuencia de multidifusión (y no hacia el RP, como antes).

Dependiendo de la topología de red, el remitente del tráfico Multicast pudo residir en una diversa interfaz ASA que el RP. Cuando el ASA recibe el PIM únase a para conmutar al árbol específico de la fuente, el ASA debe tener una ruta a la dirección IP del remitente. Si esta ruta no se encuentra, el PIM se une al paquete será caído y el siguiente mensaje será considerado en la salida del **pim del debug**:

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

La solución para este problema es agregar una entrada del mRoute estático para el remitente de la secuencia, señalando la interfaz ASA apagado cuyo reside el remitente.

El ASA cae los paquetes de multidifusión debido al Time to Live (TTL) excedido

En este caso, el tráfico Multicast está fallando porque TTL de los paquetes es demasiado bajo. Esto hace el ASA, o un poco de otro dispositivo en la red, para caerlos.

Los paquetes de multidifusión tienen a menudo el valor establecidovalor establecido IP TTL muy bajo por la aplicación que los envió. Esto se hace a veces por abandono para ayudar a asegurarse de que no viaja el tráfico Multicast demasiado lejos sin embargo la red. Por ejemplo, por abandono la aplicación de cliente LAN video (un transmisor y una herramienta para pruebas populares del Multicast) fija TTL en el paquete del IP a 1 por abandono.

El ASA experimenta CPU elevada el uso y los paquetes perdidos debido a la topología específica del Multicast

El ASA pudo experimentar CPU elevada y la secuencia de multidifusión pudo experimentar las caídas de paquetes si todos los siguientes son verdades sobre la topología del Multicast:

1. El ASA está actuando como el RP.
2. El ASA es el primer receptor del salto de la secuencia de multidifusión. Esto significa que el remitente del Multicast es en la misma subred IP una interfaz ASA.
3. El ASA es el router del último salto de la secuencia de multidifusión. Esto significa que un receptor de multidifusión está en la misma subred IP que una interfaz ASA.

Si todos los antedichos son verdades, después la deuda hace una limitación de diseño que el ASA será forzado para procesar el Switch el tráfico Multicast. Esto da lugar a las altas secuencias de multidifusión de la velocidad de datos para experimentar las caídas de paquetes. El contador de caídas de la demostración ASP que incrementa cuando se caen estos paquetes es batea-tarifa-límite.

Para determinar si un ASA está experimentando este problema, complete estos pasos:

Paso 1: Marque si el ASA es el RP usando los dos comandos:

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

Paso 2: Marque si el ASA es el router del último salto usando este comando:

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

Paso 3: Marque si el ASA es el primer router de saltos usando este comando:

```
show mroute <mcast_group_IP>
```

Un receptor de multidifusión de desconexión interrumpe a la recepción del grupo de multidifusión en otras interfaces

Solamente los ASA que actúan en IGMP Stub-MODE experimentan este problema. Los ASA que participan en el ruteo multicast PIM no son afectados.

El problema es identificado por el bug CSCeg48235 - IGMP: La detención del rcvr del grupo interrumpe a la recepción del grupo en otras interfaces

Éste es el Release Note del bug, que explica el problema:

```
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.
```

El ASA cae los paquetes de multidifusión debido a la política de seguridad de lista de acceso saliente

Con este problema específico el ASA está cayendo correctamente los paquetes de multidifusión (por la política de seguridad configurada). Sin embargo, es difícil que el administrador de la red identifique la razón de las caídas de paquetes. En este caso, el ASA está cayendo los paquetes debido a la lista de acceso saliente configurada para una interfaz. La solución alternativa es permitir la secuencia de multidifusión en la lista de acceso saliente.

Cuando ocurre esto, los paquetes de multidifusión serán caídos y el contador de caídas ASP será “FP ningún intrf de la salida del mcast (ninguno-mcast-intrf)”.

El ASA cae los primeros paquetes cuando una secuencia de multidifusión primero se comienza

Cuando los primeros paquetes de una secuencia de multidifusión llegan el ASA, el ASA debe construir esa conexión determinada del Multicast y la entrada mroute asociada para remitir los paquetes. Mientras que se está creando la entrada algunos paquetes de multidifusión se pudieron caer hasta la ruta multicast y se han establecido las conexiones (ésta toma generalmente menos que un segundo). Una vez que la configuración de la secuencia de multidifusión es completa, los

paquetes serán no más tarifa limitada.

Los paquetes caídos por este motivo tendrán la razón del descenso ASP “del límite de velocidad de la batea (del batea-tarifa-límite) excedido”. Abajo está la salida de la **captura ASP de la demostración** (donde está una captura el ASP del descenso ASP configurada en el ASA para capturar los paquetes perdidos) y usted puede ver los paquetes de multidifusión que fueron caídos por este motivo:

```
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
```

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems