

Resolución de problemas comunes de ASA Multicast

Contenido

[Introducción](#)

[Información sobre la Función](#)

[Abreviaturas/acrónimos](#)

[Componentes de multidifusión](#)

[Operación de modo disperso de PIM](#)

[Configuración de Ejemplo de PIM Sparse-Mode](#)

[Ejemplo de Modo Disperso PIM:](#)

[Funcionamiento en modo Stub IGMP](#)

[Configuración de modo Stub IGMP](#)

[Bidir PIM](#)

[Configuración de PIM Bidir](#)

[Metodología de Troubleshooting](#)

[Información Que Se Debe Recopilar Al Resolver Problemas De Multidifusión](#)

[Resultado útil del comando Show](#)

[Capturas de paquetes](#)

[Ejemplo de implementación de multidifusión en modo disperso de ASA PIM](#)

[Análisis de datos](#)

[Problemas Comunes](#)

[ASA No Puede Enviar Mensajes PIM Hacia Routers Ascendentes Debido A HSRP](#)

[El ASA ignora los informes IGMP porque no es el router designado en el segmento LAN](#)

[El firewall deniega los informes IGMP cuando se supera el límite de la interfaz IGMP](#)

[El ASA no puede reenviar el tráfico de multidifusión en el rango 232.x.x.x/8](#)

[ASA descarta paquetes de multidifusión debido a la verificación de reenvío de trayecto inverso](#)

[ASA no genera la unión de PIM al conmutar PIM al árbol de origen](#)

[ASA descarta paquetes de multidifusión debido a que se superó el tiempo de vida \(TTL\)](#)

[ASA Experimenta Un Uso Elevado De La CPU Y Paquetes Descartados Debido A Una Topología Multicast Específica](#)

[ASA Descarta Los Primeros Paquetes Cuando Se Inicia Por Primera Vez Un Flujo Multicast](#)

[Un Receptor De Multidifusión Que Se Desconecta Interrumpe La Recepción Del Grupo De Multidifusión En Otras Interfaces](#)

[ASA descarta paquetes de multidifusión debido a la política de seguridad de la lista de acceso saliente](#)

[El ASA descarta continuamente algunos paquetes \(pero no todos\) en un flujo multicast debido a la limitación de la velocidad del punto de control](#)

[La secuencia de multidifusión se ha detenido debido a un mensaje PIM ASSERT](#)

[ASA envía la unión PIM pero el vecino no la procesa debido al tamaño del paquete mayor que la MTU](#)

Introducción

Este documento describe el ruteo multicast en el Adaptive Security Appliance (ASA) y problemas comunes.

Información sobre la Función

Nota: para obtener información actualizada sobre el routing multidifusión en el dispositivo de seguridad adaptable (ASA), Firepower Threat Defence (FTD) o Secure Firewall Threat Defence (FTD), consulte estos artículos:

[Solución de problemas de Firepower Threat Defence IGMP y aspectos básicos de multidifusión](#)

[Solución de problemas de Firepower Threat Defense y ASA Multicast PIM](#)

Abreviaturas/acrónimos

Acrónimos	Explicación
FHR	Router de primer salto: un salto conectado directamente al origen del tráfico de multidifusión.
LHR	Router de último salto: un salto conectado directamente a los receptores del tráfico de multidifusión.
RP	Punto de encuentro
DR.	Router designado
SPT	Árbol de ruta más corta
RPT	Árbol de punto de encuentro (RP), árbol compartido
RPF	Reenvío de Trayectoria Inversa
PETRÓLEO	Lista de interfaces salientes
MRIB	Base de Información de Ruteo Multicast

MFIB	Base de Información de Reenvío Multicast
ASM	Multidifusión de cualquier fuente
BSR	Bootstrap Router
SSM	Multidifusión desde un origen específico
FP	Ruta rápida
SP	Trayecto lento
CP	Punto de control
PPS	Velocidad de paquetes por segundo

La multidifusión en el ASA se puede configurar en uno de estos dos modos:

- Modo disperso PIM (multidifusión independiente del protocolo: [RFC 4601](#))
- Modo de conexión única IGMP (protocolo de administración de grupos de Internet: [RFC 2236](#))

El modo disperso de PIM es la opción preferida, ya que ASA se comunica con los vecinos a través de un protocolo de routing multidifusión (PIM) real. El modo de conexión única IGMP era la única opción de configuración de multidifusión antes de que se lanzara la versión 7.0 de ASA, y funcionaba simplemente reenviando los informes IGMP recibidos de los clientes hacia los routers ascendentes.

Componentes de multidifusión

En general, una infraestructura de multidifusión se compone de estos componentes:

Sender => Host o dispositivo de red que origina la secuencia de multidifusión. Algunos ejemplos son los servidores que envían flujos de vídeo y/o audio y los dispositivos de red que ejecutan un protocolo de routing como EIGRP o OSPF.

Receiver => Host o dispositivo que recibe la secuencia de multidifusión. Este término se utiliza con más frecuencia para los hosts que están interesados activamente en el tráfico y utilizan IGMP para unirse o salir del grupo de multidifusión en cuestión.

Routers / ASA => Dispositivos de red responsables de procesar y reenviar el flujo/tráfico multidifusión a otros segmentos de la red cuando sea necesario desde el origen al cliente.

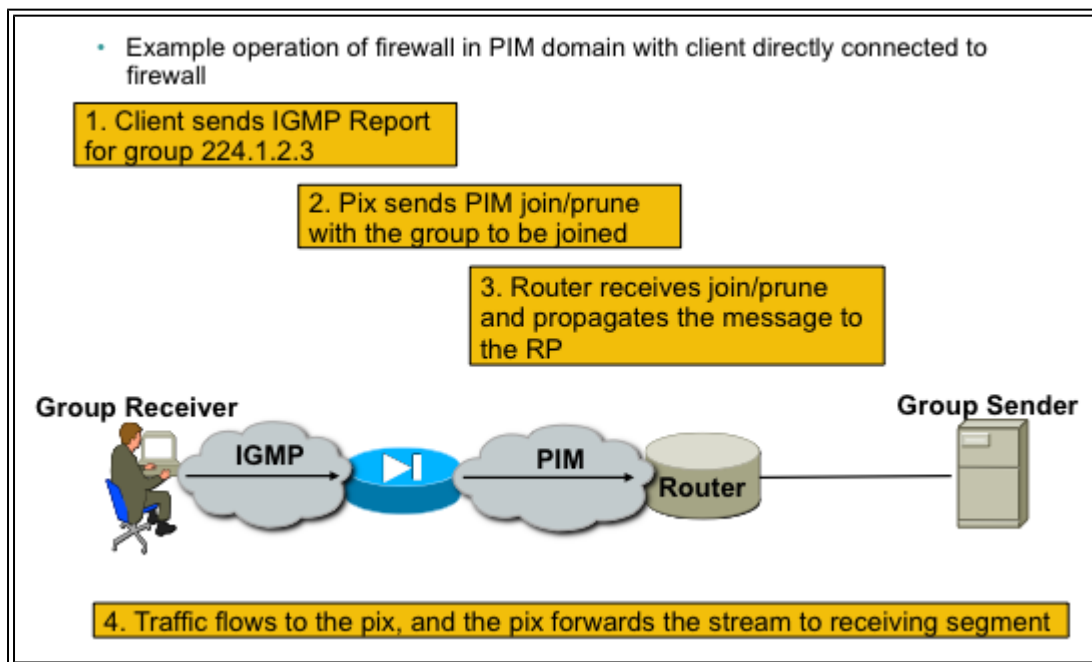
Multicast Routing Protocol => Protocol responsable de reenviar los paquetes multicast. El más común es PIM (Protocol Independent Multicast), pero hay otros como MOSPF por ejemplo.

Protocolo de administración de grupos de Internet (IGMP) => Proceso utilizado por los clientes para recibir una secuencia de multidifusión de un grupo determinado.

Operación de modo disperso de PIM

- El ASA soporta el modo disperso PIM y el modo bidireccional PIM.
- Los comandos PIM sparse-mode e IGMP stub-mode no se deben configurar simultáneamente.
- Con el modo disperso de PIM, todo el tráfico de multidifusión fluye inicialmente al punto de encuentro (RP) y, a continuación, se reenvía hacia los receptores. Después de algún tiempo, el flujo multicast va directamente desde el origen a los receptores (y omite el RP).

Esta imagen ilustra una implementación común donde el ASA tiene clientes multicast en una interfaz y vecinos PIM en otra:



Configuración de Ejemplo de PIM Sparse-Mode

1. Habilite el ruteo multicast (modo de configuración global).

```
<#root>
```

```
ASA(config)#
```

`multicast-routing`

2. Defina la dirección del punto de encuentro de PIM.

<#root>

ASA(config)#

`pim rp-address 172.18.123.3`

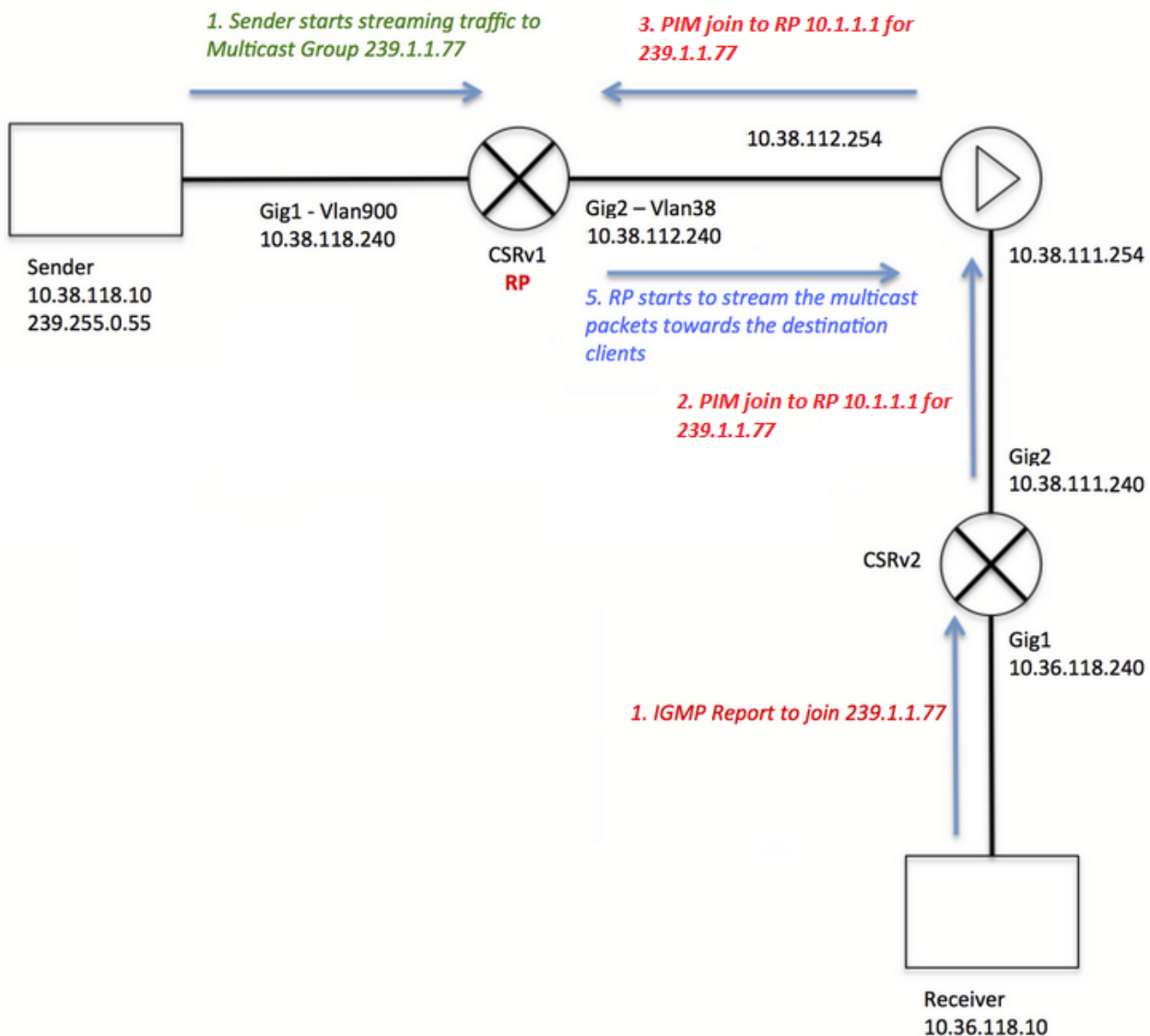
3. Permita que los paquetes multicast entren en la interfaz apropiada (necesario solamente si la política de seguridad del ASA bloquea los paquetes multicast entrantes).

<#root>

`access-list 105 extended permit ip any host 224.1.1.1`

`access-group 105 in interface outside`

Ejemplo de Modo Disperso PIM:



Observe que el registro de IGMP del cliente (pasos en rojo) y la secuencia recibida por el servidor (pasos en verde) se han coloreado de manera diferente, y esto se hizo de esta manera para probar que ambos procesos pueden ocurrir independientemente.

Pasos de registro del cliente (pasos rojos):

1. El cliente envía un informe IGMP para el grupo 239.1.1.77
2. El router envía un mensaje de unión PIM al RP estático configurado (10.1.1.1) para el grupo 239.1.1.77.
3. ASA envía a RP un mensaje de unión PIM para el grupo 239.1.1.77.

ASA muestra la entrada PIM *,G en la salida del comando 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
```

Pero como el servidor de origen no ha iniciado ningún flujo, la salida "show mfib" en el ASA no muestra ningún paquete recibido:

```
<#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
```

Antes de que el servidor comience a enviar tráfico al grupo multicast, el RP sólo muestra una entrada "*.G" sin interfaz entrante en la lista, como por ejemplo:

```
<#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

```

Una vez que el servidor comienza a transmitir al grupo multicast, el RP crea una entrada "S,G" y pone la interfaz frente al remitente en la lista de interfaz entrante y comienza a enviar el tráfico de flujo descendente al 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

```

Utilice estos comandos para las verificaciones:

- show mroute muestra una entrada "S,G"
- show mfib muestra los contadores de paquetes de reenvío
- El comando show conn muestra la conexión relacionada con el ip del grupo multicast

```

<#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 -

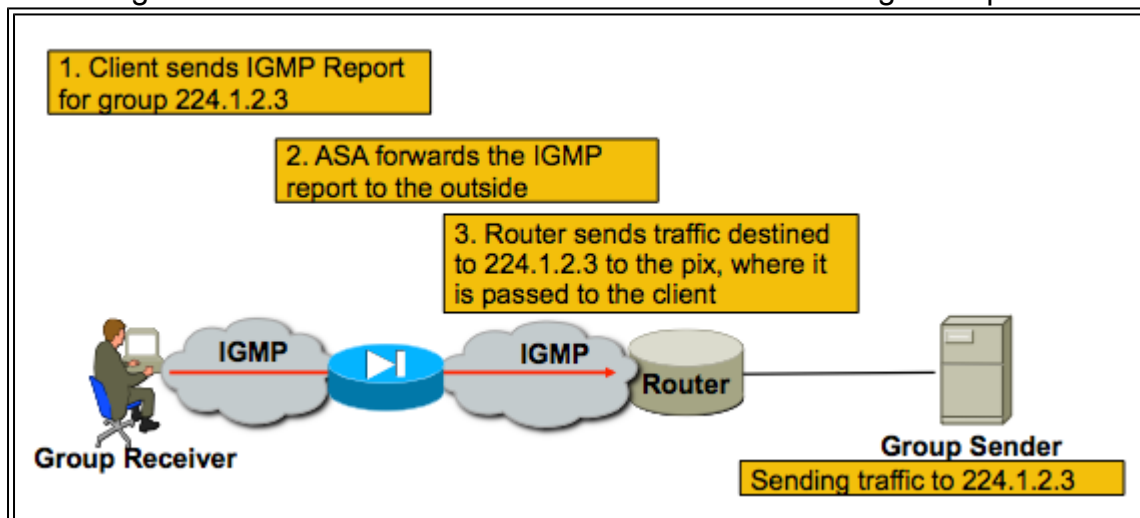
Nota: Una vez que el cliente cierra la aplicación cliente de multidifusión, el host envía un mensaje de consulta IGMP.

En caso de que este sea el único host conocido por el router como un cliente que desea recibir la secuencia, el router envía un mensaje IGMP Prune al RP.

Funcionamiento en modo Stub IGMP

- En el modo IGMP Stub, ASA actúa como un cliente multicast y genera o reenvía informes IGMP (también conocidos como "uniones" IGMP) hacia los routers adyacentes, para activar la recepción de tráfico multicast
- Los routers envían periódicamente consultas a los hosts para ver si algún nodo de la red desea continuar recibiendo el tráfico de multidifusión.
- No se recomienda el modo Stub de IGMP porque el modo disperso de PIM ofrece muchas ventajas sobre el modo Stub (con flujos de tráfico multicast más eficientes, capacidad de participar en PIM, etc).

Esta imagen ilustra el funcionamiento básico de un ASA configurado para IGMP Stub-mode:



Configuración de modo Stub IGMP

1. Habilite el ruteo multicast (modo de configuración global).

```
<#root>
```

```
ASA(config)#
```

```
multicast-routing
```

2. En la interfaz en la que el firewall recibe los informes igmp, configure el comando igmp forward-interface. Reenvíe los paquetes fuera de la interfaz hacia el origen del flujo. En este ejemplo, los receptores de multidifusión están conectados directamente a la interfaz interna y el origen de multidifusión está más allá de la interfaz externa.

```
<#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. Permita que los paquetes multicast entren en la interfaz apropiada (sólo es necesario si la política de seguridad del ASA niega el tráfico multicast entrante).

<#root>

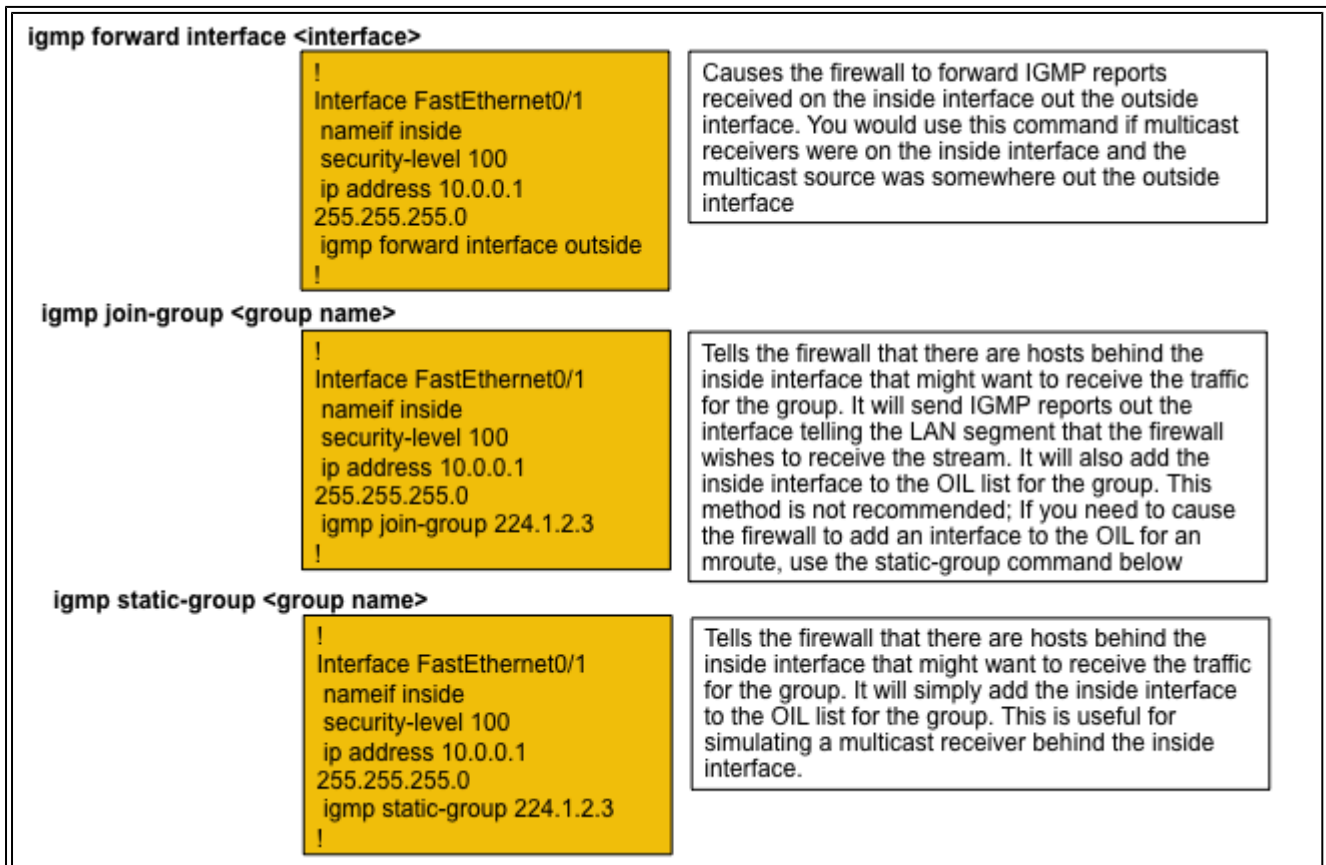
```

ASA(config)#
access-list 105 extended permit ip any host 224.1.2.3

ASA(config)#
access-group 105 in interface outside

```

A menudo hay confusión en torno a los diferentes comandos de submodo de interfaz igmp, y este diagrama describe cuándo utilizar cada uno:



Bidir PIM

En el PIM bidireccional, no hay ningún árbol compartido (SPT). Esto significa tres cosas:

1. El router del primer salto (conectado al remitente) no envía paquetes de registro PIM al RP.
2. El RP no envía mensajes PIM JOIN para unirse al árbol de origen.
3. Los routers en la trayectoria al receptor envían mensajes de unión PIM hacia el RP para unirse al RPT.

Esto significa que el ASA no genera un (S,G) porque los dispositivos no se unen al SPT. Todo el tráfico multicast pasa a través del RP. El ASA reenvía todo el tráfico multicast mientras haya un (*,G). Si no hay (*,G), eso significa que ASA nunca recibió un paquete de unión PIM. Si ese es el caso, el ASA no debe reenviar los paquetes multicast.

Configuración de PIM Bidir

1. Habilite el ruteo multicast (modo de configuración global).

```
<#root>
```

```
ASA(config)#
```

```
  multicast-routing
```

2. Defina la dirección del punto de encuentro de PIM.

```
<#root>
```

```
ASA(config)#
```

```
pim rp-address 172.18.123.3 bidir
```

3. Permita que los paquetes multicast entren en la interfaz apropiada (necesario solamente si la política de seguridad del ASA bloquea los paquetes multicast entrantes).

```
<#root>
```

```
access-list 105 extended permit ip any host 224.1.1.1
```

```
access-group 105 in interface outside
```

Metodología de Troubleshooting

Información Que Se Debe Recopilar Al Resolver Problemas De Multidifusión

Para comprender y diagnosticar completamente un problema de reenvío de multidifusión en ASA, se necesita parte o toda esta información:

- Una descripción de la topología de red, la ubicación de los remitentes de multidifusión, los receptores y el punto de encuentro.
- La dirección IP específica del grupo, así como los puertos y protocolos empleados.
- Registros del sistema generados por el ASA en el momento en que el flujo multicast tiene problemas.
- Salida específica del comando show desde la interfaz de línea de comandos ASA:

```
<#root>
```

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

- Capturas de paquetes para mostrar si los datos de multidifusión llegan al ASA y si los paquetes se reenvían a través del ASA (tome nota del tiempo de vida de IP (TTL) del paquete). Esto se puede ver con el comando 'show capture x detail')
- Capturas de paquetes para paquetes IGMP y PIM. Ejemplo:

```
<#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
```

- Información de dispositivos de multidifusión adyacentes (routers) como "show mroute" y "show mfib".
- Capturas de paquetes y/o comandos show para determinar si ASA descarta los paquetes multicast. El comando 'show asp drop' se puede utilizar para determinar si ASA descarta los paquetes. Además, las capturas de paquetes del tipo 'asp-drop' se pueden utilizar para capturar todos los paquetes que descarta ASA y, a continuación, se examinan para ver si los paquetes de multidifusión están presentes en la captura de descarte.

Resultado útil del comando Show

El resultado del comando show mroute muestra los diversos grupos e información de reenvío, y es muy similar al comando IOS show mroute. El comando show mfib muestra el estado de reenvío de los diversos grupos multicast. Es especialmente importante observar el contador de paquetes Forwarding, así como Other (que indica caídas):

```
<#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#
```

El comando clear mfib counters se puede utilizar para borrar los contadores, lo cual es muy útil durante la prueba:

```
<#root>
```

```
ciscoasa#
```

```
clear mfib counters
```

Capturas de paquetes

La utilidad de captura de paquetes integrada es muy útil para resolver problemas de multidifusión. En este ejemplo, se capturan todos los paquetes de ingreso en la interfaz DMZ, destinados a 239.17.17.17:

```
<#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
....
```

La salida del comando show capture x detail muestra el TTL de los paquetes, lo cual es bastante útil. En esta salida, el TTL del paquete es 1 (y el ASA pasa este paquete ya que no disminuye el TTL de los paquetes IP de forma predeterminada) pero un router de flujo descendente descartaría los paquetes:

```
<#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 0)
```

Las capturas de paquetes también son útiles para capturar el tráfico PIM e IGMP. Esta captura muestra que la interfaz interna ha recibido un paquete IGMP (protocolo IP 2) originado desde 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#
```

Observe que el TTL de los paquetes se puede ver con el comando 'show capture x detail'.

Aquí podemos ver las capturas de caídas de ASP tomadas que muestran los paquetes multicast caídos y la razón de las caídas (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
```

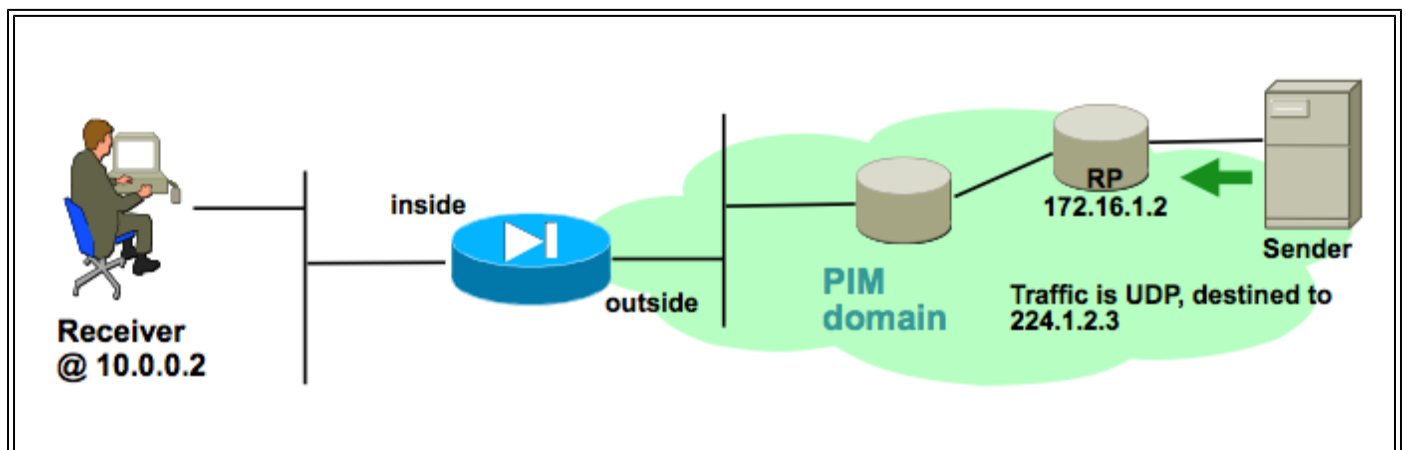
```
802.1Q vlan#1007 P0 10.76.4.95.1806 > 239.255.2.195.5000: [udp sum ok] udp 1316 (DF) [ttl 1] (id
```

Ejemplo de implementación de multidifusión en modo disperso de ASA PIM

Estos diagramas ilustran cómo ASA interactúa con los dispositivos vecinos en el modo disperso de PIM.

Comprender la topología de la red

Determine exactamente la ubicación de los remitentes y receptores de la secuencia de multidifusión específica. Además, determine la dirección IP del grupo multicast, así como la ubicación del punto de encuentro.



En este caso, los datos se pueden recibir en la interfaz exterior del ASA y reenviar al receptor multicast en la interfaz interior. Debido a que el receptor está en la misma subred IP que la interfaz interna del ASA, espere ver un informe IGMP recibido en la interfaz interna cuando el cliente solicite recibir la secuencia. La dirección IP del remitente es 192.168.1.50.

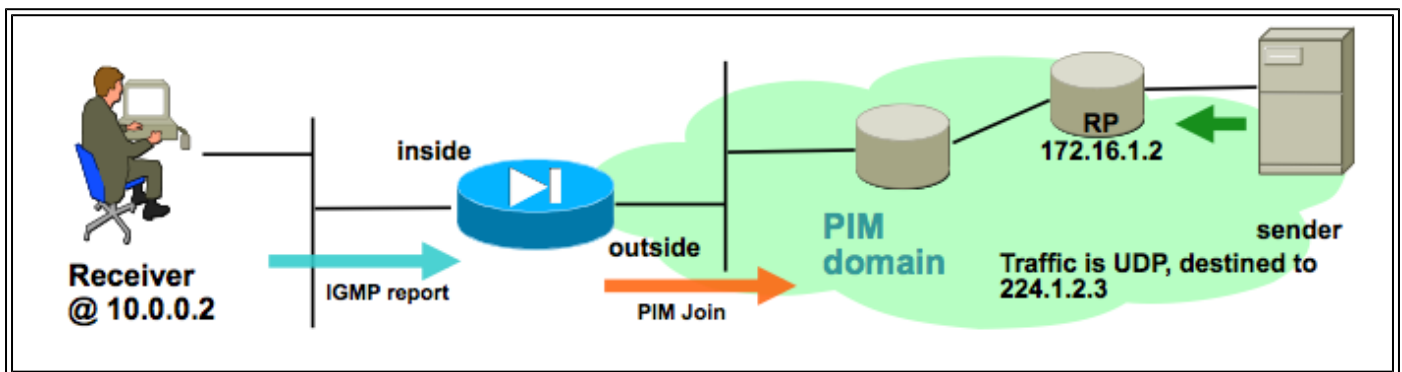
Verifique que ASA reciba el informe IGMP del receptor

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

Las capturas de paquetes y la salida de debug igmp se pueden utilizar para verificar que el ASA recibió y procesó con éxito el mensaje IGMP.

Verifique que ASA envíe un mensaje de unión PIM hacia el punto de encuentro

El ASA interpreta el informe IGMP y genera un mensaje de unión PIM, luego lo envía por la interfaz hacia el RP.

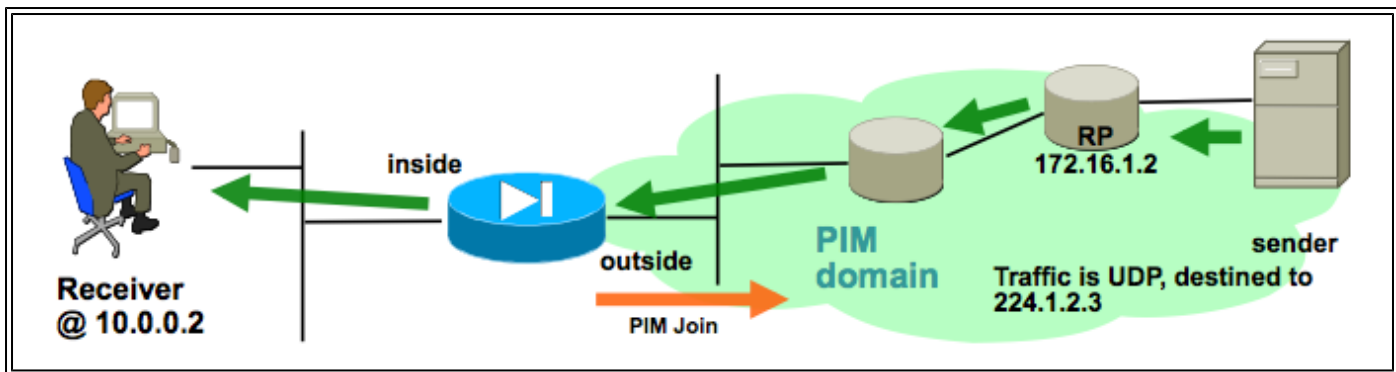


Este resultado proviene de debug pim group 224.1.2.3 y muestra que ASA envía satisfactoriamente el mensaje de unión PIM. El remitente del flujo de multidifusión es 192.168.1.50.

```
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 192.168.1.50
```

Verifique que ASA reciba y reenvíe el flujo de multidifusión

El ASA comienza a recibir tráfico multicast en la interfaz exterior (ilustrado por las flechas verdes) y lo reenvía a los receptores en el interior.



Los comandos `show mroute` y `show mfib`, así como las capturas de paquetes, se pueden utilizar para verificar que el ASA recibe y reenvía los paquetes multicast.

Se crea una conexión en la tabla de conexiones para representar la secuencia de multidifusión:

```
<#root>
```

```
ciscoasa#
```

```
show conn
```

```
59 in use, 29089 most used
```

```
...
```

```
UDP outside:192.168.1.50/52075 inside:224.1.2.3/1234 flags -
```

```
...
```

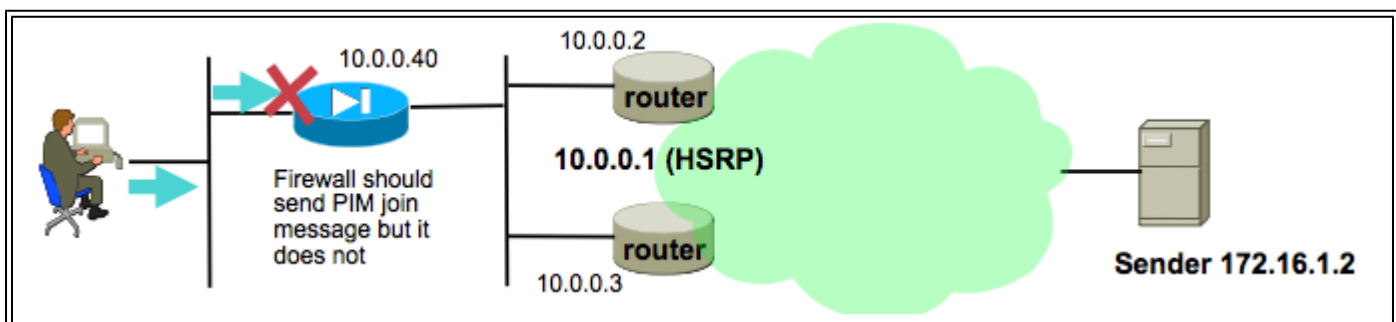
Análisis de datos

Problemas Comunes

Esta sección proporciona una serie de problemas relacionados con la multidifusión ASA real

ASA No Puede Enviar Mensajes PIM Hacia Routers Ascendentes Debido A HSRP

Cuando se encuentra este problema, el ASA no puede enviar ningún mensaje PIM fuera de una interfaz. Este diagrama muestra que el ASA no puede enviar mensajes PIM hacia el remitente, pero el mismo problema se puede ver cuando el ASA necesita enviar un mensaje PIM hacia el RP.



La salida del comando debug pim muestra que ASA no puede enviar el mensaje PIM al router de salto siguiente ascendente:

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

Este problema no es específico de ASA y también afecta a los routers. El problema es provocado por la combinación de la configuración de la tabla de ruteo y la configuración HSRP utilizada por los vecinos PIM.

La tabla de ruteo señala al HSRP IP 10.0.0.1 como el dispositivo de salto siguiente:

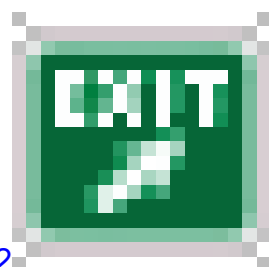
```
<#root>
ciscoasa#
show run route
route outside 0.0.0.0 0.0.0.0 10.0.0.1 1
```

Sin embargo, la relación de vecino PIM se forma entre las direcciones IP de la interfaz física de los routers, y no la 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)
```

Consulte "[¿Por qué no funciona el modo disperso de PIM con una ruta estática a una dirección HSRP?](#)" para obtener más información.

Un extracto del documento:



¿Por qué el router no envía el mensaje de incorporación/separación? [RFC 2362](#) establece que "un router envía un mensaje periódico de unión/separación a cada vecino RPF distinto asociado con cada entrada (S,G), (*,G) y (*,*,RP). Los mensajes Join/Prune se envían

solamente si el vecino RPF es un vecino PIM."

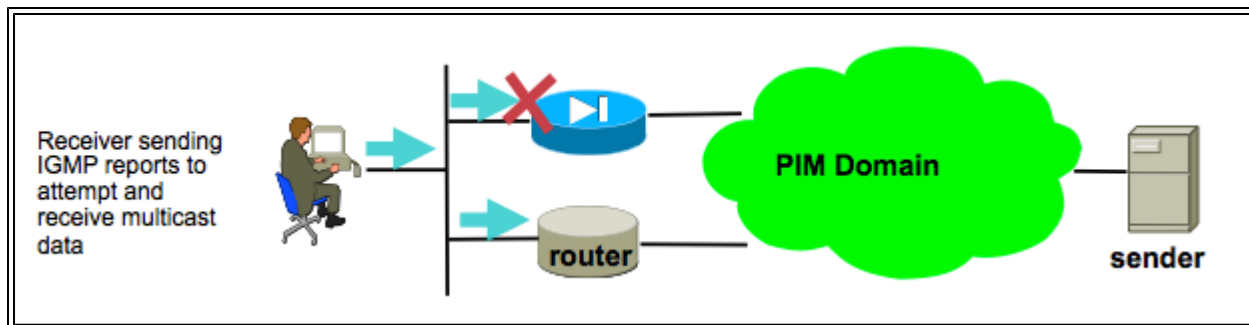
Para mitigar el problema, agregue una entrada de ruta multicast estática en el ASA para el tráfico en cuestión. Asegúrese de que apunta a una de las dos direcciones IP de interfaz del router (10.0.0.2 o 10.0.0.3). En este caso, este comando permite que el ASA envíe mensajes PIM dirigidos hacia el remitente multicast en 172.16.1.2:

```
<#root>  
ciscoasa(config)#  
mroute 172.16.1.2 255.255.255.255 10.0.0.3
```

Una vez hecho esto, la tabla de ruteo multicast invalida la tabla de ruteo unicast del ASA, y el ASA envía los mensajes PIM directamente al vecino 10.0.0.3.

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

Para este problema, ASA recibe un informe IGMP de un receptor multicast conectado directamente, pero lo ignora. No se genera ninguna salida de depuración y el paquete simplemente se descarta, y la recepción de la secuencia falla.



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

Este resultado de la CLI de ASA muestra que un dispositivo diferente es el router designado (indicado con "DR") en la red de la interfaz interna:

```
<#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)

De forma predeterminada, el PIM se habilita en todas las interfaces ASA cuando se agrega el comando multicast-routing a la configuración. Si hay otros vecinos PIM (otros routers o ASA) en la interfaz interna del ASA (donde residen los clientes) y uno de esos vecinos fue elegido porque el DR para ese segmento, entonces otros routers no DR descartan informes IGMP. La solución es inhabilitar PIM en la interfaz (con el comando no pim en la interfaz involucrada), o hacer que ASA sea el DR para el segmento a través del comando de interfaz pim dr-priority.

El firewall deniega los informes IGMP cuando se supera el límite de la interfaz IGMP

De forma predeterminada, ASA permite realizar un seguimiento de 500 uniones activas actuales (informes) en una interfaz. Este es el valor máximo configurable. Si los clientes de una interfaz solicitan un gran número de secuencias de multidifusión, se puede encontrar el máximo de 500 uniones activas y el ASA podría ignorar los informes IGMP entrantes adicionales de los receptores de multidifusión.

Para confirmar si esta es la causa de una falla de multidifusión, ejecute el comando 'show igmp interface interfazname' y busque la información 'IGMP limit' para la interfaz.

```
<#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
```

El ASA no puede reenviar el tráfico de multidifusión en el rango 232.x.x.x/8

Este rango de direcciones se utiliza con Source Specific Multicast (SSM) que ASA no admite actualmente.

La salida del comando debug igmp muestra este error:

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

ASA descarta paquetes de multidifusión debido a la verificación de reenvío de trayecto inverso

En este caso, ASA recibe tráfico multicast en una interfaz, pero no se reenvía al receptor. ASA descarta los paquetes porque no pasan la comprobación de seguridad de Reenvío de ruta inversa (RPF). El RPF está habilitado en todas las interfaces para el tráfico multicast y no se puede inhabilitar (para los paquetes unicast, la verificación no está activada de forma predeterminada y se habilita con el comando `ip verify reverse-path interface`).

Debido a la verificación RPF, cuando se recibe tráfico multicast en una interfaz, ASA verifica que tenga una ruta de regreso al origen del tráfico multicast (verifica la tabla de ruteo unicast y multicast) en esa interfaz. Si no tiene una ruta al remitente, descarta el paquete. Estas caídas se pueden ver como un contador en el resultado 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

Una opción es agregar una ruta multicast para el remitente del tráfico. En este ejemplo, el comando `mroute` se utiliza para satisfacer la verificación RPF para el tráfico multicast originado en 172.16.1.2 recibido en la interfaz externa:

```
<#root>
```

```
ciscoasa(config)#
```

```
mroute 172.16.1.2 255.255.255.255 outside
```

ASA no genera la unión de PIM al conmutar PIM al árbol de origen

Inicialmente, los paquetes de multidifusión en modo disperso PIM fluyen desde el remitente de

multidifusión al RP y, a continuación, desde el RP al receptor a través de un árbol de multidifusión compartido. Sin embargo, una vez que la velocidad de bits agregada alcanza un cierto umbral, el router más cercano al receptor multicast intenta recibir tráfico a lo largo del árbol específico del origen. Este router genera una nueva unión PIM para el grupo y la envía hacia el remitente del flujo de multidifusión (y no hacia el RP, como antes).

El remitente del tráfico multicast puede residir en una interfaz ASA diferente que el RP. Cuando ASA recibe la unión PIM para conmutar al árbol específico de origen, ASA debe tener una ruta a la dirección IP del remitente. Si no se encuentra esta ruta, se descarta el paquete de unión PIM y este mensaje se ve en la salida de debug pim

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

La solución para este problema es agregar una entrada de ruta multicast estática para el remitente del flujo, que señala la interfaz ASA de la cual reside el remitente.

ASA descarta paquetes de multidifusión debido a que se superó el tiempo de vida (TTL)

En este caso, el tráfico multicast falla porque el TTL de los paquetes es demasiado bajo. Esto hace que el ASA, o algún otro dispositivo de la red, los descarte.

A menudo, los paquetes multicast tienen el valor IP TTL establecido muy bajo por la aplicación que los envió. A veces, esto se hace de forma predeterminada para ayudar a garantizar que el tráfico de multidifusión no se desplace demasiado a través de la red. Por ejemplo, de forma predeterminada, la opción Vídeo LAN La aplicación cliente (un popular transmisor de multidifusión y herramienta de prueba) establece el TTL en el paquete IP en 1 de forma predeterminada.

ASA Experimenta Un Uso Elevado De La CPU Y Paquetes Descartados Debido A Una Topología Multicast Específica

El ASA puede experimentar un uso elevado de la CPU y el flujo de multidifusión puede experimentar caídas de paquetes si todo esto es cierto acerca de la topología de multidifusión:

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

Si se encuentran todos los síntomas mencionados, entonces debido a una limitación de diseño, ASA se ve obligado a procesar el tráfico de multidifusión del switch. Esto da como resultado flujos de multidifusión de alta velocidad de datos para experimentar caídas de paquetes. El contador show asp drop que aumenta cuando estos paquetes se descartan es punt-rate-limit.

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

Paso 1: Verifique si ASA es el RP:

```
<#root>  
  
show run pim  
show pim tunnel
```

Paso 2: Verifique si el ASA es el router del último salto:

```
<#root>  
  
show igmp group  
  
<mcast_group_IP>
```

Paso 3: Verifique si el ASA es el primer router de salto:

```
<#root>  
  
show mroute  
  
<mcast_group_IP>
```

Para mitigar este problema, se pueden tomar las siguientes medidas:

- Modifique la topología para que ASA no sea el RP. O bien, haga que el emisor o el receptor no estén conectados directamente al ASA
- En lugar de PIM, utilice el modo stub de IGMP para el reenvío de multidifusión.

ASA Descarta Los Primeros Paquetes Cuando Se Inicia Por Primera Vez Un Flujo Multicast

Cuando los primeros paquetes de un flujo multicast llegan al ASA, el ASA debe construir esa conexión multicast particular y la entrada mroute asociada para reenviar los paquetes. Mientras la entrada está en proceso de creación, algunos paquetes multicast se pueden descartar hasta que se hayan establecido la ruta multicast y las conexiones (generalmente esto toma menos de un segundo). Una vez que se completa la configuración de la secuencia de multidifusión, los paquetes ya no se limitan a la velocidad.

Los paquetes descartados por esta razón tienen la razón de caída ASP de "(punt-rate-limit) Punt rate limit exceeded". Este es el resultado de 'show capture asp' (donde asp es una captura de

caída de ASP configurada en ASA para capturar paquetes perdidos) y puede ver los paquetes multicast que se perdieron por esta razón:

```
<#root>
```

```
ASA #
```

```
show capture asp
```

```
2 packets captured
```

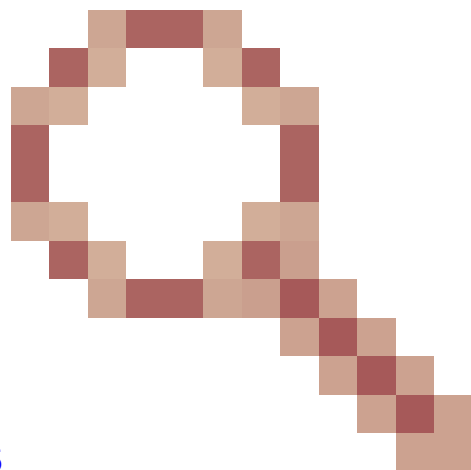
```
1: 16:14:49.419091 10.23.2.2.810 > 239.255.123.123.890:  udp 32 Drop-reason: (punt-rate-limit) Punt
```

```
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 Receptor De Multidifusión Que Se Desconecta Interrumpe La Recepción Del Grupo De Multidifusión En Otras Interfaces

Solo los ASA que funcionan en modo Stub IGMP experimentan este problema. Los ASA que participan en el ruteo multidifusión PIM no se ven afectados.



El problema se identifica con el ID de bug de Cisco [CSCeg48235](#)
IGMP Leave en una interfaz interrumpe el tráfico multicast en otras interfaces.

Esta es la nota de lanzamiento 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 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

ASA descarta paquetes de multidifusión debido a la política de seguridad de la lista de acceso saliente

Con este problema específico, ASA descarta paquetes de multidifusión (según la política de seguridad configurada). Sin embargo, es difícil para el administrador de red identificar la razón de las caídas de paquetes. En este caso, ASA descarta paquetes debido a la lista de acceso saliente configurada para una interfaz. La solución alternativa es permitir el flujo multicast en la lista de acceso saliente.

Cuando esto ocurre, los paquetes de multidifusión se descartan con el contador de descarte de ASP "FP no mcast output intrf (no-mcast-intrf)".

El ASA descarta continuamente algunos paquetes (pero no todos) en un flujo multicast debido a la limitación de la velocidad del punto de control

Lo más probable es que el tráfico esté limitado por la velocidad del punto de control debido al límite de velocidad de punt. Observe el resultado de la caída de asp y las capturas para confirmar:

```
<#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
```

La entrada mfib muestra que todo el tráfico es conmutado por proceso:

```
<#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 tabla de ruteo multicast muestra un (*,G) pero no (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
```

El problema aquí es que el TTL de los paquetes y los paquetes de datos multicast que llegan al ASA es 1. El ASA está reenviando estos paquetes al dispositivo de flujo descendente (porque no disminuye el TTL), pero el router de flujo descendente descarta los paquetes. Como resultado, el router de flujo descendente no envía una unión PIM (S,G) (una unión específica de la fuente) al ASA hacia el remitente. El ASA no crea una entrada (S,G) hasta que recibe esta unión PIM. Debido a que el (S,G) no está construido, todo el tráfico multicast es conmutado por proceso que resulta en un límite de velocidad.

La solución a este problema es asegurar que el TTL de los paquetes no sea 1, que permite que el dispositivo de flujo descendente envíe la unión específica de la fuente hacia el remitente; esto hace que el ASA instale una ruta multicast específica de la fuente en la tabla, y luego todos los paquetes se conmutan rápidamente (en lugar de conmutados procesados) y el tráfico debe fluir a través del ASA sin ningún problema.

La secuencia de multidifusión se ha detenido debido a un mensaje PIM ASSERT

Si dos dispositivos de red reenvían los mismos paquetes de multidifusión a la misma subred entonces, idealmente, uno de ellos debe dejar de reenviar los paquetes (ya que es una pérdida duplicar el flujo). Si los routers que ejecutan PIM detectan que reciben los mismos paquetes que también generan en la misma interfaz, generan mensajes ASSERT en esa LAN para seleccionar qué dispositivo de red deja de reenviar la secuencia.

Puede ver más información sobre este mensaje en una [sección de RFC 4601 relacionada con el proceso ASSERT](#).

Las depuraciones muestran que ASA recibe un informe IGMP para el grupo 239.1.1.227, pero ignora el informe debido al mensaje de aserción que recibe de un router vecino:

```
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)
```

Este problema se observó en una red de producción en la que dos sitios se conectaron accidentalmente en puente en la capa 2, de modo que la LAN en la que se encontraban los receptores de multidifusión tenía dos dispositivos que reenviaban tráfico de multidifusión hacia ellos. Debido a otro problema de red, el ASA y otro dispositivo no pudieron detectarse entre sí a través de saludos PIM y, por lo tanto, ambos asumieron la función de router designado para la LAN. Esto hizo que el tráfico multicast funcionara por un tiempo y luego fallara cuando los dispositivos enviaban los mensajes ASSERT. Para resolver el problema, se deshabilitó la conexión incorrecta que conectaba los dispositivos de la capa 2 y, a continuación, se resolvió el problema.

ASA envía la unión PIM pero el vecino no la procesa debido al tamaño del paquete mayor que la MTU

Esto se observó en 629575899. El ASA se configuró para las tramas Jumbo y el 4900 no. Cuando el cliente solicitaba más de 73 secuencias de multidifusión, algunas secuencias de multidifusión no funcionaban. 73 SG crearía un mensaje de PIM Join del tamaño 1494, que aún estaba dentro de MTU. 74SG crearía un mensaje de PIM Join mayor que 1500, lo que hizo que 4900M descartara el paquete entrante.

La solución para este problema fue:

1. Asegúrese de que las tramas gigantes estén habilitadas globalmente en el 4900M
2. Configure tanto la interfaz física como la SVI con una MTU de 9216

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).