Resolución de Problemas de Descartes de Paquetes Multicast en Firewall con Configuración PIM Bidir

Contenido

Problema

Estos síntomas se observan en Secure Firewall Threat Defence (FTD), que participa como salto intermedio en el dominio de routing multidifusión con multidifusión independiente de protocolo bidireccional (BIDIR-PIM), una variante de PIM Sparse-Mode (PIM-SM):

1. La ruta multicast para el grupo multicast específico 232.4.4.4 está ausente:

<#root>

device#

show mroute 232.4.4.4

No mroute entries found.

2. El contador "Otras caídas" para el rango del grupo 232.0.0.0/8 en la salida del comando show mfib count aumenta:

<#root>

device#

show mfib count

IP Multicast Statistics

6 routes, 3 groups, 0.00 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second

Other counts: Total

/RPF failed/

Other drops(OIF-null, rate-limit etc)

Group: 224.0.1.39
  RP-tree:
   Forwarding: 0/0/0/0, Other: 0/0/0
Group: 224.0.1.40
  RP-tree:
   Forwarding: 0/0/0/0, Other: 0/0/0

Group: 232.0.0.0/8

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

Other: 2551

/0/

2551 <----

device#

show mfib count

IP Multicast Statistics
6 routes, 3 groups, 0.00 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second

Other counts: Total

/RPF failed/

Other drops(OIF-null, rate-limit etc)

Group: 224.0.1.39
  RP-tree:
   Forwarding: 0/0/0/0, Other: 0/0/0
Group: 224.0.1.40
  RP-tree:
   Forwarding: 0/0/0/0, Other: 0/0/0

Group: 232.0.0.0/8

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

Other: 2864

/0/

2864

<----

3. Los paquetes de multidifusión se descartan con el motivo de la pérdida Punt rate limit exceeded (punt-rate-limit) en Accelerated Security Path (ASP). El contador de caídas aumenta continuamente:

<#root>

```
device#
```

cap capi trace interface inside match udp any host 232.4.4.4

```
device#
```

show cap capi trace

```
   2: 19:36:08.509205
```

192.168.1.2.12345 > 232.4.4.4.12345

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

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 13056 ns
Config:
```

```
Implicit Rule
Additional Information:
MAC Access list

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

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

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



device#

show asp drop



Frame drop:

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


  FP L2 rule drop (l2_acl)                                                        6

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

Flow drop:

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

show asp drop



Frame drop:

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


  FP L2 rule drop (l2_acl)                                                       37
```

4. Las capturas de la interfaz externa no muestran ningún paquete multicast de salida:

<#root>

device#

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

device#

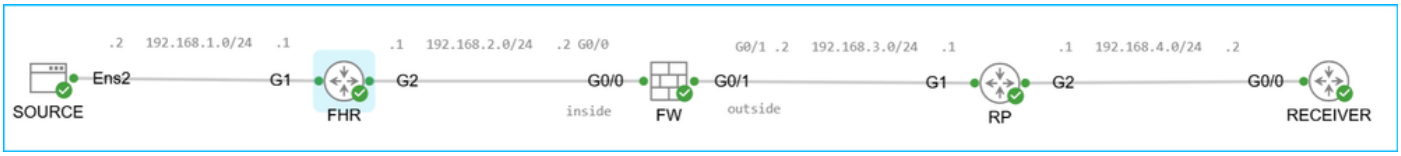
show cap capo

0 packet captured

0 packet shown

Entorno

Topología:



topology.png

Puntos clave:

- Los peers en el dominio multicast utilizan BIDIR-PIM.
- El "router" de este artículo hace referencia a un router de Cisco como CSR o ASR.

- Rendezvous Point (RP) es ASR1001-X que ejecuta el software Cisco IOS XE, versión 17.09.08. Otras plataformas y versiones de software también pueden verse afectadas.
- El router de primer salto (FHR) es C9200L-48T-4G que ejecuta el software Cisco IOS XE, versión 16.12.04. Otras plataformas y versiones de software también pueden verse afectadas.
- La dirección de punto de encuentro (RP) 10.4.4.4 en la interfaz Loopback0 para todo el rango de multidifusión 224.0.0.0/8 se propaga dinámicamente en el dominio de multidifusión mediante el router PIM Bootstrap (BSR). Las implementaciones con la configuración de dirección RP de PIM estática también pueden verse afectadas.

  Configuración de PIM en RP:

```
<#root>

device#

show run interface loopback0


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

device(config)#

ip pim bidir-enable


device(config)#

ip pim bsr-candidate Loopback0 0 1


device(config)#

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

- En aras de la simplicidad, en este caso, el RP se muestra como conectado al receptor, es decir, también es el router de último salto (LHR). Esto es opcional.
- El firewall es Secure Firewall 3110 con la versión 7.6.4. Otras plataformas de firewall, versiones de software y el software Adaptive Security Appliance (ASA) también pueden verse afectados.
- En el firewall, el routing multidifusión está activado y existe adyacencia PIM con el router de primer salto (FHR) y RP con la capacidad PIM BIDIR:

```
<#root>

device#
```

```
show run multicast-routing


multicast-routing


device#
show pim neighbor


Neighbor Address  Interface          Uptime    Expires DR pri Bidir
192.168.2.1       inside             1d12h     00:01:40 1
B

192.168.3.1       outside            1d12h     00:01:35 1
B
```

- En el firewall, a pesar del uso de PIM BSR, la dirección PIM RP 10.4.4.4 se configura manualmente. Esta es una configuración redundante. Como resultado, hay 2 mapeos RP a grupo entre el grupo 224.0.0.0/4 y la dirección RP 10.4.4.4:

<#root>

```
device#
show run pim


pim rp-address 10.4.4.4 bidir


device#
show pim group-map


Group Range         Proto   Client   Groups RP address      Info
224.0.1.39/32*      DM      static   0      0.0.0.0
224.0.1.40/32*      DM      static   0      0.0.0.0
224.0.0.0/24*       L-Local static   1      0.0.0.0
232.0.0.0/8*        SSM     config   0      0.0.0.0
224.0.0.0/4*        BD      BSR      0      10.4.4.4   RPF: outside,192.168.3.1 <-- * means the ma


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

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

Resolución

Antes de continuar, asegúrese de revisar la sección Causa.

Se espera que se produzcan descartes de paquetes en el firewall debido a la incompatibilidad entre la configuración deseada (BIDIR-PIM) y el tráfico que debe gestionarse mediante PIM SSM.

Si la configuración deseada es BIDIR-PIM, considere estas opciones:

- Utilice sólo grupos SSM que no sean PIM.
- Si se deben utilizar grupos PIM SSM, asegúrese de que el firewall maneja los grupos multicast del rango PIM SSM como direcciones de grupo no SSM. Consulte la sección Preguntas y respuestas para obtener más información.
- Considere el ID de bug de Cisco CSCwt9960.

Causa

La dirección 232.4.4.4 pertenece al intervalo de grupos de multidifusión específica de origen (SSM) reservado por la Autoridad de números asignados de Internet (IANA). El firewall reserva automáticamente el rango 232.0.0.0/8 para PIM SSM:

<#root>

```
device#

show pim group-map


Group Range          Proto   Client   Groups RP address      Info

224.0.1.39/32*       DM      static   0      0.0.0.0
224.0.1.40/32*       DM      static   0      0.0.0.0
224.0.0.0/24*        L-Local static   1      0.0.0.0
```

```
232.0.0.0/8*        SSM     config   0      0.0.0.0


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

Puntos clave sobre PIM SSM:

- Construye árboles basados en la fuente y utiliza rutas multicast (S, G).
- La infraestructura de árbol compartido basada en RP del protocolo PIM-SM no es necesaria. En otras palabras, no se utilizan rutas multicast RP o (*, G).
- Los receptores se unen normalmente al árbol de multidifusión mediante el protocolo de administración de grupos de Internet versión 3 (IGMPv3) con el "filtrado de origen", es decir, la capacidad de que un sistema informe del interés en recibir paquetes sólo de direcciones de origen específicas, o de todas las direcciones de origen excepto de las específicas, enviadas a una dirección de multidifusión concreta.

Puntos clave sobre BIDIR-PIM:

- Construye árboles compartidos bidireccionales que conectan fuentes y receptores multicast.
- Los árboles bidireccionales se crean mediante un mecanismo de elección de reenviador designado (DF) a prueba de fallos que funciona en cada vínculo de una topología de multidifusión.
- Con la ayuda del DF, los datos multicast se reenvían de forma nativa desde los orígenes al RP y, por lo tanto, a lo largo del árbol compartido a los receptores sin requerir el estado específico del origen.
- BIDIR-PIM no utiliza entradas de árboles de trayecto más corto (SPT) y (S, G).
- Los pares BIDIR-PIM crean árboles compartidos mediante entradas (*, G). Esta entrada para un grupo multicast determinado debe existir en la tabla mroute.

Al contrastar los puntos clave para PIM SSM y BIDIR-PIM, se muestra que PIM SSM y BIDIR-PIM tienen una funcionalidad mutuamente excluyente.

En este caso, el dominio multicast se configura para utilizar BIDIR-PIM, mientras que el grupo multicast pertenece al rango reservado por IANA y el firewall para PIM SSM. Dado que el dominio multicast utiliza BIDIR-PIM, las rutas multicast (S, G) necesarias para PIM SSM no están

disponibles en el firewall. Debido a la falta de rutas multicast, la interfaz de salida/egreso para el tráfico multicast no está disponible. La ausencia de interfaz de salida/salida provoca caídas de paquetes en la base de información de reenvío multidifusión (MFIB). Las caídas se pueden verificar mediante los comandos show mfib o show mfib count:

<#root>

```
device#

show mfib count



IP Multicast Statistics
6 routes, 3 groups, 0.00 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second

Other counts: Total

/RPF failed/

Other drops(OIF-null, rate-limit etc)



Group: 224.0.1.39
  RP-tree:
   Forwarding: 0/0/0/0, Other: 0/0/0
Group: 224.0.1.40
  RP-tree:
   Forwarding: 0/0/0/0, Other: 0/0/0

Group: 232.0.0.0/8



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

333797

/0/

333797
```

El firewall intenta resolver la interfaz de salida/salida activando el punto de control (CP). Este es el componente crítico del firewall que se encarga principalmente de las funciones del plano de control y gestión, como los protocolos de routing, el acceso a la gestión, la gestión de clústeres/conmutación por fallo, la gestión de paquetes destinados a la interfaz del firewall, las direcciones IP de difusión o multidifusión, etc.

Para evitar sobrecargar el punto de control, el firewall cuenta con mecanismos de protección integrados. Por ejemplo, el firewall limita la velocidad de los paquetes enviados desde el plano de datos (DP) al punto de control. Los paquetes que exceden la velocidad se descartan con el motivo de descarte de ASP de límite de velocidad de punteo excedido (punt-rate-limit). La velocidad de punt se puede verificar en la salida de show asp event dp-cp punt | begin EVENT-TYPE :

```
<#root>
device#

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


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

punt              1264746          0  1264746        0  1264746         44

<-- 15-second punt rate

  multicast       1250020          0  1250020        0  1250020         44



  pim               14726          0    14726        0    14726          0
```

En resumen, la conclusión es que se esperan caídas de paquetes en el firewall debido a la incompatibilidad entre la configuración deseada (BIDIR-PIM) y el tráfico que debe gestionarse mediante PIM SSM.

Preguntas y respuestas

En esta sección, "router" hace referencia a un router de Cisco como CSR y "firewall" hace referencia a los firewalls de Cisco que ejecutan ASA o FTD.

1. Q: ¿El firewall reserva automáticamente 232.0.0.0/8 para PIM SSM?

R: Yes. A diferencia, por ejemplo, de routers como CSR, no se requiere ninguna configuración específica. En los routers, el rango PIM SSM necesita una configuración explícita:

<#root>

```
device(config)#

ip pim ssm ?


  default  Use 232/8 group range for SSM


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

2. Q: ¿El contador "Otras caídas" de MFIB es específico para el firewall?

R: No. Existe un contador similar en los routers Cisco con ruteo multicast.

3. Q: ¿Otro dispositivo como un router en lugar de un firewall también descartaría paquetes enviados al grupo 232.4.4.4?

R: Depende de cómo el router trate la dirección 232.4.4.4. A diferencia de los firewalls, los routers predeterminados no reservan el rango 232.0.0.0/8 para PIM SSM. Sin embargo, si tanto PIM SSM como BIDIR-PIM están habilitados, y el router es RP que reconoce BIDIR-PIM o recibe mapeo RP a grupo con el indicador Bidir y recibe paquetes multicast enviados al rango PIM SSM, los paquetes se descartan y el contador "Otros" de MFIB aumenta:

<#root>

```
device#

show run | i pim


ip pim bidir-enable


no ip pim autorp

ip pim ssm default
```

```
device#
```

show ip pim rp mapping

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

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

bidir <-- mapping has the bidir flag

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

device#
```

show ip mfib count

```
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
```

Other counts: Total/RPF failed

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

Group: 232.0.0.0/8

```
  RP-tree,
```

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

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

device#
```

show ip mfib count

```
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
```

Other counts: Total/RPF failed

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

Group: 232.0.0.0/8


  RP-tree,



SW Forwarding: 0/0/0/0,

 Other: 106/106

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

Tenga en cuenta que, a diferencia del firewall con el contador de aumento "Otras caídas" en el router, el contador de aumento es "Error de RPF".

4. Q: ¿Cómo forzar a los firewalls a manejar un grupo desde el rango PIM SSM como una dirección de grupo no SSM?

R: Asegúrese de que RP anuncie la asignación RP a grupo para los grupos que son más específicos que 232.0.0.0/8 (prefijo más largo) o que en el firewall configure manualmente la dirección RP para grupos específicos.

Opción 1. Configuración en RP:

<#root>

```
device(config)#

access-list 1 permit host 232.4.4.4


device(config)#

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

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

Verificación en el firewall:

```
<#root>
device#

show pim group-map 232.4.4.4

Group Range         Proto   Client   Groups RP address      Info

232.4.4.4/32*       BD

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

Opción 2. Configuración en el firewall:

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

access-list mcast standard permit 232.4.4.4 255.255.255.254


device(config)#

pim rp-address 10.4.4.4 mcast bidir


device(config)#

show pim group-map 232.4.4.4


Group Range         Proto   Client   Groups RP address      Info


232.4.4.4/31*



BD

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

Tenga en cuenta que la lista de acceso no debe utilizar entradas de host o entradas con la máscara 255.255.255.255.

5. Q: ¿Qué sucede si el firewall maneja un grupo del rango PIM SSM como una dirección de grupo no SSM?

R: Suponga que el grupo 232.4.4.4 se maneja como una dirección no SSM (consulte la pregunta 4):

```
<#root>

device#

show pim group-map 232.4.4.4


Group Range         Proto   Client   Groups RP address      Info

232.4.4.4/32*       BD

      BSR      0      10.4.4.4   RPF: outside,192.168.3.1
```

Si la versión de software se ve afectada por el Id. de error de Cisco CSCwt9960, falta la ruta multicast (*, G) y el flujo multicast se limita a una velocidad de aproximadamente 50 paquetes por segundo. Los paquetes excesivos se descartan con el límite de velocidad de punteo excedido (punt-rate-limit) motivo de descarte de ASP:

```
<#root>

device#

show mroute 232.4.4.4


No mroute entries found.


device#

show mfib 232.4.4.4 count
```

```
IP Multicast Statistics
7 routes, 4 groups, 0.00 average sources per group
```

Forwarding Counts

```
: Pkt Count/
```

Pkts per second

```
/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Group: 232.4.4.4
  RP-tree:
   Forwarding: 23317/
```

50

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


device#
```

show mfib 232.4.4.4 count

```


IP Multicast Statistics
7 routes, 4 groups, 0.00 average sources per group
```

Forwarding Counts:

```
 Pkt Count/
```

Pkts per second

```
/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Group: 232.4.4.4
  RP-tree:
   Forwarding: 23540/
```

49

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

device#
```

capture capi interface inside trace match udp any host 232.4.4.4

```


device#
```

show capture capi trace | i Drop-reason

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

Para obtener más información, consulte el Id. de bug Cisco CSCwt9960.

Contenido relacionado

- Bloque de multidifusión específico del origen
- ID de bug de Cisco CSCwt99960

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).