Resolución de Problemas de Tráfico Multicast que No Pasa a Través de Firewall FTD con Configuración PIM Bidir

Contenido

Problema

Se observan todos estos síntomas:

- El tráfico de multidifusión dejó de funcionar en la defensa frente a amenazas de firewall (FTD) para un grupo de multidifusión específico.
- No hay rutas multicast (mroutes) en el FTD para el grupo (224.2.2.2 en este ejemplo).

<#root>

```
device#
```

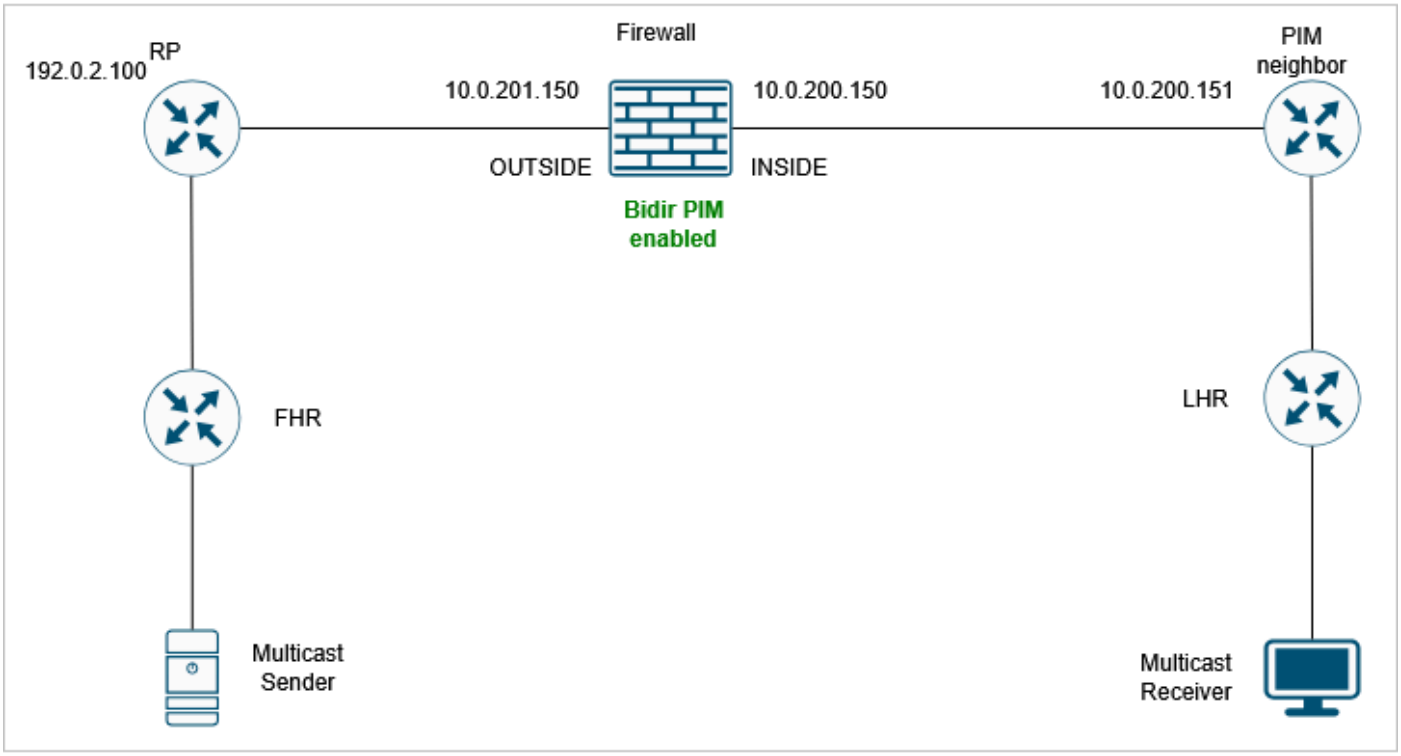
show mroute 224.2.2.2

```
No mroute entries found.
device#
```

Entorno

- Se detectó por primera vez en la versión 7.4 del FTD. Otras versiones de software, incluido el dispositivo de seguridad adaptable (ASA), también pueden verse afectadas.
- La multidifusión independiente de protocolo bidireccional (PIM) está activada en el firewall.

Topología



inline_image_0.png

Resolución

Paso 1: Revise la configuración de multidifusión actual.

Examine la configuración de routing multidifusión existente en todos los dispositivos de la ruta de red para identificar cualquier configuración incorrecta o que falte que pueda impedir que el tráfico multidifusión atraviese el firewall.

En el firewall hay una configuración PIM bidireccional :

<#root>

```
device#
```

show run pim

```
pim rp-address 192.0.2.100 bidir
```

Paso 2: Verifique los vecinos PIM.

Confirme que los vecinos multicast se muestren correctamente en el firewall:

<#root>

```
device#

show pim neighbor


Neighbor Address  Interface          Uptime    Expires DR pri Bidir
10.0.200.151      INSIDE             19:13:30  00:01:24 1 (DR)
10.0.201.200      OUTSIDE            00:01:31  00:01:42 1 (DR)

B
```

En la salida, observe que el vecino 10.0.201.200 tiene el indicador Bidir B, mientras que el vecino 10.0.200.151 no lo tiene.

Paso 3: Habilite la depuración PIM para el grupo multicast 224.2.2.2:

<#root>

```
FPR3100-14#

debug pim group 224.2.2.2


IPv4 PIM group debugging is on
 for group 224.2.2.2
```

La depuración muestra que hay un paquete PIM Join/Prune que se descarta debido a 'no bidir df election':

<#root>

```
IPv4 PIM: J/P entry: Join root: 192.0.2.100 group: 224.2.2.2 flags:  RPT WC S
IPv4 PIM: (*,224.2.2.2) J/P with RP 192.0.2.100 on INSIDE

discarded, no bidir df election-state on this intf
```

Paso 4: Habilite las capturas PIM hacia el vecino PIM 10.0.200.151. El objetivo es obtener más visibilidad del contenido del paquete:

<#root>

```
device#

capture CAPI interface INSIDE trace match pim host 10.0.200.151 any
```

Paso 5: Recopile la captura del firewall del dispositivo FTD:

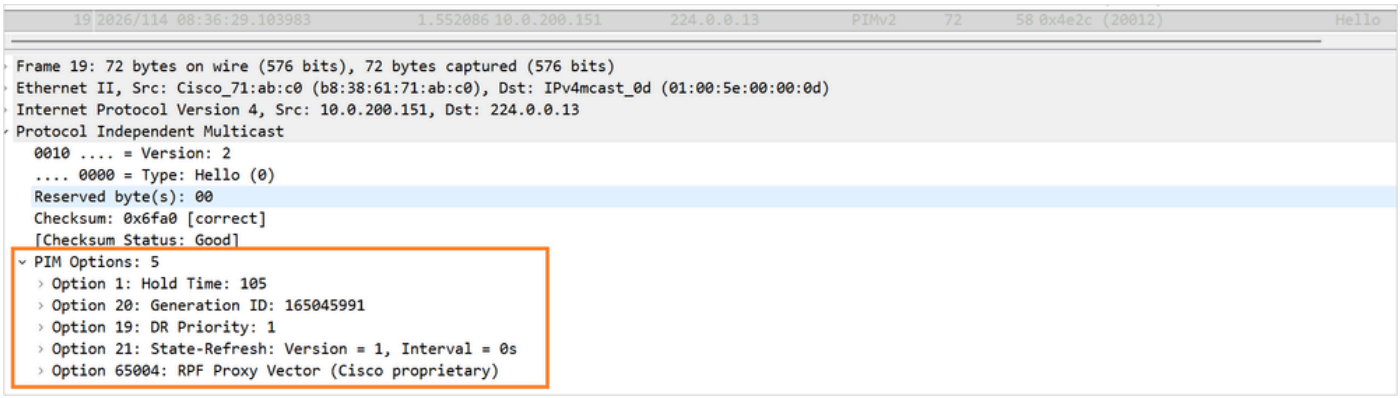
<#root>

```
device#

copy /pcap capture:CAPI CAPI.pcap


Source capture name [CAPI]?
Destination filename [CAPI.pcap]?
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
!
28 packets copied in 0.0 secs
```

Recopile el archivo pcap de FMC mediante el procedimiento descrito en https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html

Paso 6: Capturar análisis.

El paquete PIM Hello contiene estas opciones:



PIM_Hello_Options_no-bidir-capable.png

Observe la ausencia de la bandera con capacidad Bidir.

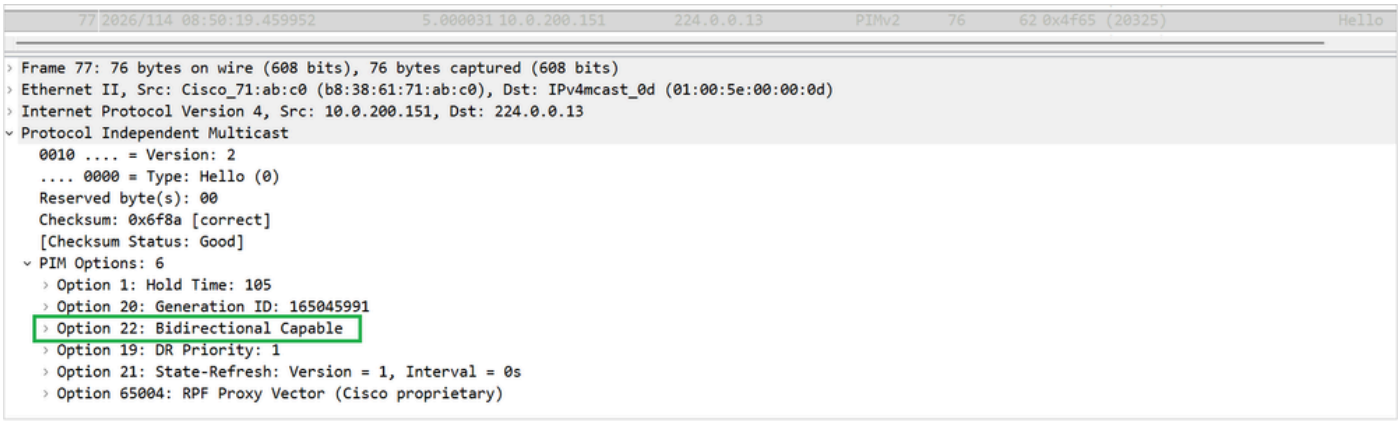
Paso 7: Habilite el PIM bidireccional en el vecino 10.0.200.151.

Ahora, la bandera PIM Bidir B se muestra para ambos vecinos:

<#root>

```
device#

show pim neighbor


Neighbor Address  Interface          Uptime    Expires DR pri Bidir
10.0.200.151      INSIDE             19:34:26  00:01:38 1 (DR)

B


10.0.201.200      OUTSIDE            00:22:27  00:01:23 1 (DR) B
```

Paso 8: Recopile una nueva captura y verifique las opciones PIM Hello para el vecino 10.0.200.151. Se muestra la opción PIM 22 (apta para bidireccionales):



PIM_Hello_Options_option22.png

Paso 9: Verifique que ahora se muestre la ruta multicast para el grupo multicast 224.2.2.2:

<#root>

device#

show mroute

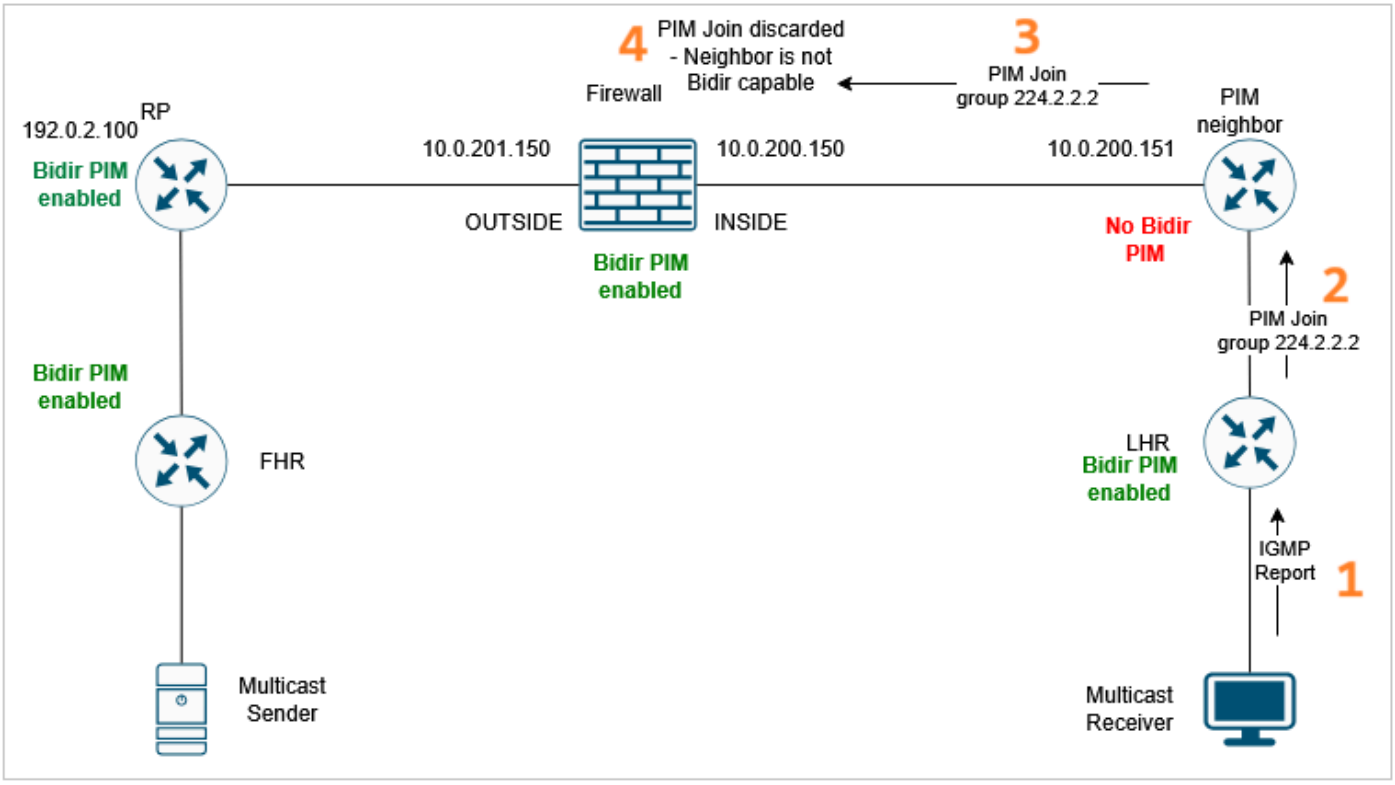
```
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State
(*, 224.0.1.40), 19:41:44/never, RP 0.0.0.0, flags: DPC
  Incoming interface: Null
  RPF nbr: 0.0.0.0
  Immediate Outgoing interface list:
    INSIDE, Null, 19:41:44/never
```

(*, 224.2.2.2)

```
, 00:06:29/00:02:53, RP 192.0.2.100, flags: B
  Bidir-Upstream: OUTSIDE
  RPF nbr: 10.0.201.200
  Immediate Outgoing interface list:
    INSIDE, Forward, 00:06:29/00:02:53
```

Causa

La falla de tráfico multicast fue causada por una configuración PIM bidireccional y multicast incorrecta o incompleta en el dispositivo de red adyacente. El problema de configuración específico hizo que FTD descartara el mensaje de unión/separación de PIM para el grupo multicast específico. Como resultado, el firewall no pudo crear la ruta multicast para el tráfico multicast. Para que el tráfico de datos multidifusión fluya a través del plano de datos del firewall, el plano de control (PIM) debe establecer la ruta multicast adecuada.



Causa.png

Contenido relacionado

- https://datatracker.ietf.org/doc/html/rfc5015#section-3.7.4

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).