Problemen oplossen met multicast-verkeer dat niet door de FTD-firewall gaat met Bidir PIM-configuratie

Inhoud

uitgeven

Al deze symptomen worden gezien:

- Multicast-verkeer is gestopt met werken aan Firewall Threat Defense (FTD) voor een specifieke multicast-groep.
- Er zijn geen multicast routes (mroutes) op de FTD voor de groep (224.2.2.2 in dit voorbeeld).

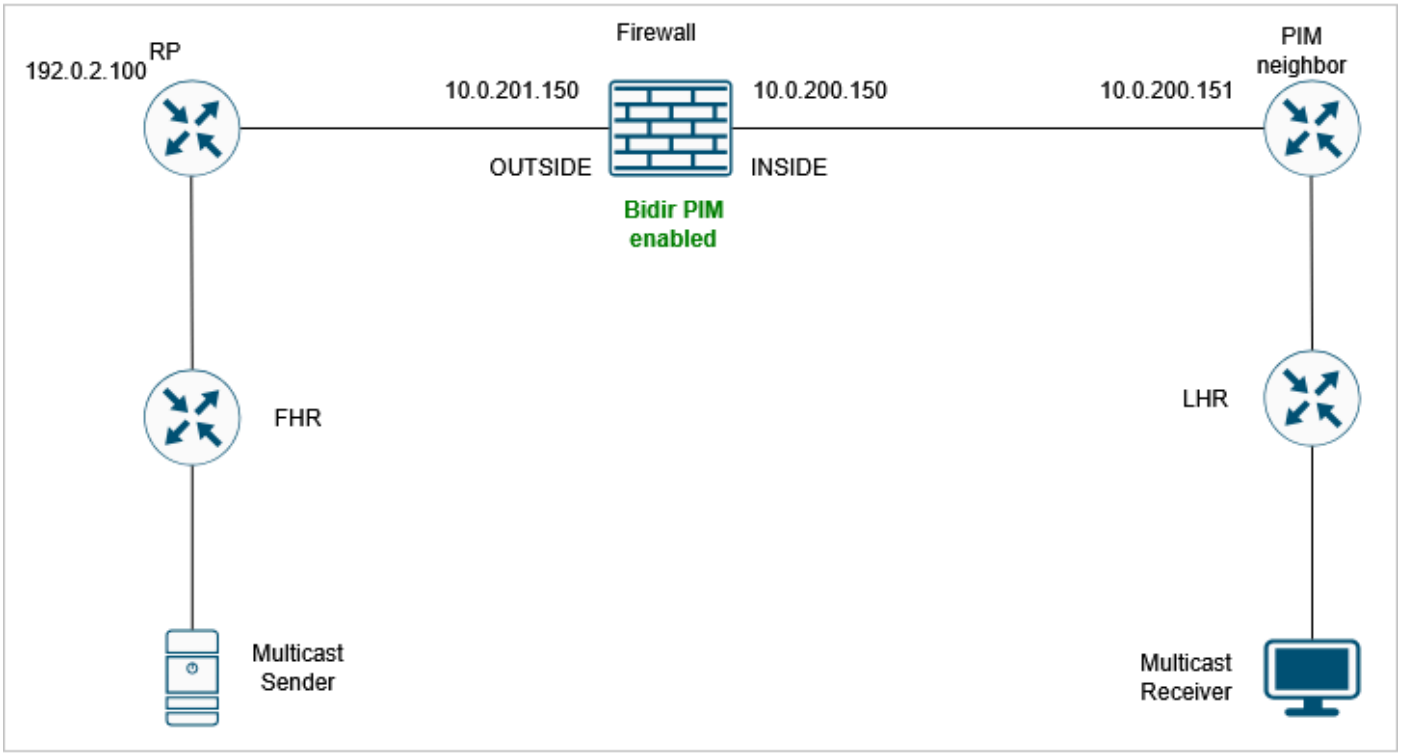
<#root>

```
device#

show mroute 224.2.2.2


No mroute entries found.
device#
```

milieu

- Het eerste deel van FTD versie 7.4. Andere softwareversies, waaronder Adaptive Security Appliance (ASA), kunnen ook worden beïnvloed.
- Bidirectional Protocol Independent Multicast (PIM) is ingeschakeld op de firewall.

Topologie



inline_image_0.png

resolutie

Stap 1: Controleer de huidige multicastconfiguratie.

Controleer de bestaande multicast-routeringsconfiguratie op alle apparaten in het netwerkpad om eventuele misconfiguraties of ontbrekende instellingen te identificeren die kunnen voorkomen dat multicast-verkeer de firewall passeert.

Op de firewall is er een bidirectionele PIM-configuratie:

<#root>

```
device#
```

show run pim

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

Stap 2: Controleer de PIM-buren.

Bevestig dat multicast-buren correct worden weergegeven in de 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
```

In de output bericht dat buurman 10.0.201.200 heeft de Bidir B vlag, terwijl de 10.0.200.151 buurman heeft het niet.

Stap 3: PIM-debug inschakelen voor multicastgroep 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
```

Het debug laat zien dat er een PIM Join/Prune-pakket is dat wordt weggegooid vanwege 'geen bidir df-verkiezing':

<#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
```

Stap 4: PIM-opnamen inschakelen voor de 10.0.200.151 PIM-buur. Het doel is om meer zichtbaarheid te krijgen op de inhoud van het pakket:

```
<#root>

device#

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

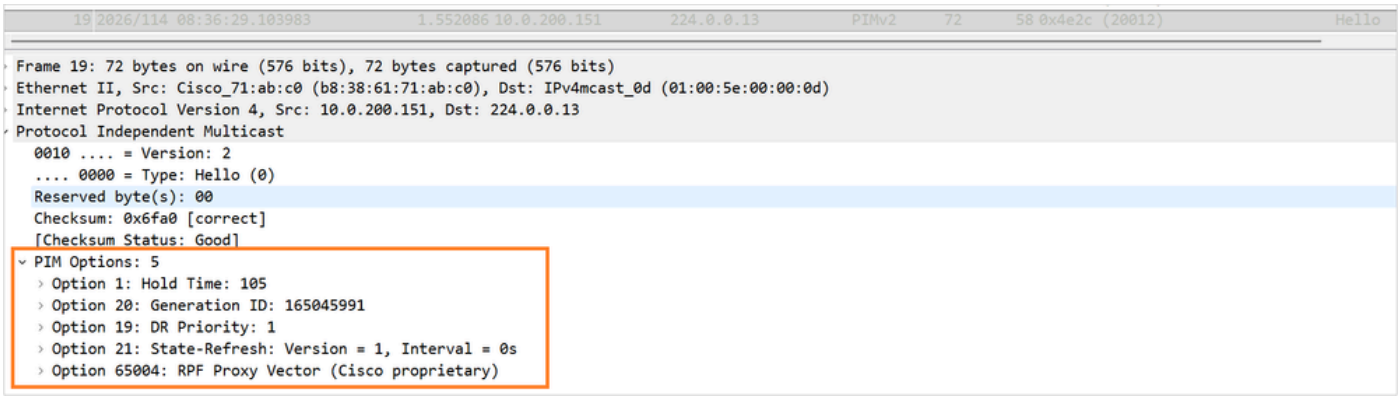
Stap 5: Verzamel de firewall-opname van het FTD-apparaat:

```
<#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
```

Verzamel het pcap-bestand van FMC volgens de procedure die wordt beschreven op https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html

Stap 6: Analyse vastleggen.

Het PIM Hello pakket bevat de volgende opties:



PIM_Hello_Options_no-bidir-capable.png

Let op de afwezigheid van de Bidir-capabele vlag.

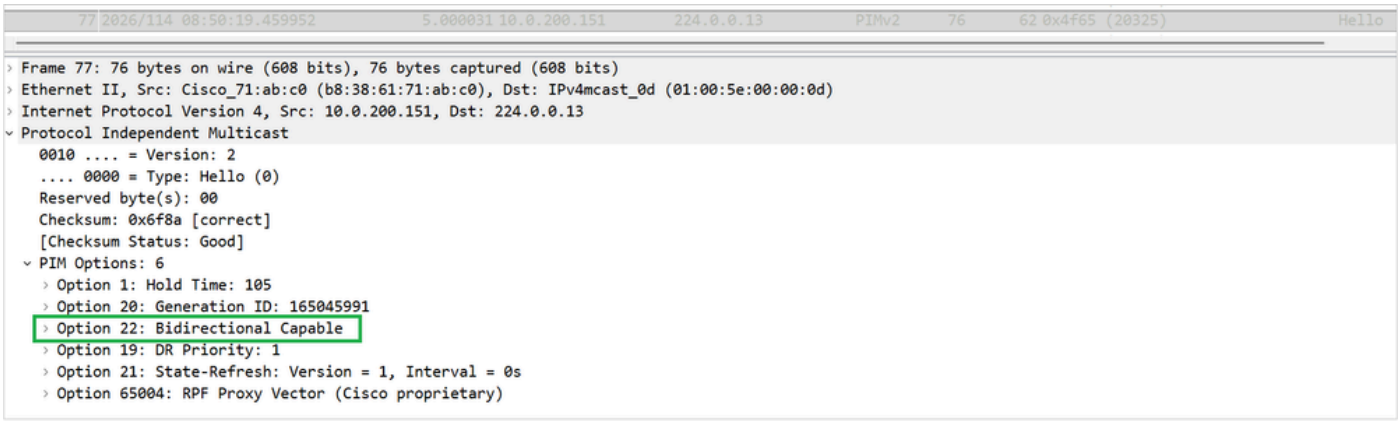
Stap 7: Schakel bidirectionele PIM in op de 10.0.200.151-buur.

Nu wordt de PIM Bidir B-vlag getoond voor beide buren:

<#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
```

Stap 8: Verzamel een nieuwe opname en controleer de PIM Hello-opties voor buurman 10.0.200.151. PIM-optie 22 (Bidirectional Capable) wordt weergegeven:



PIM_Hello_Options_option22.png

Stap 9: Controleer of de mroute voor multicastgroep 224.2.2.2 nu wordt weergegeven:

<#root>

device#

show mroute

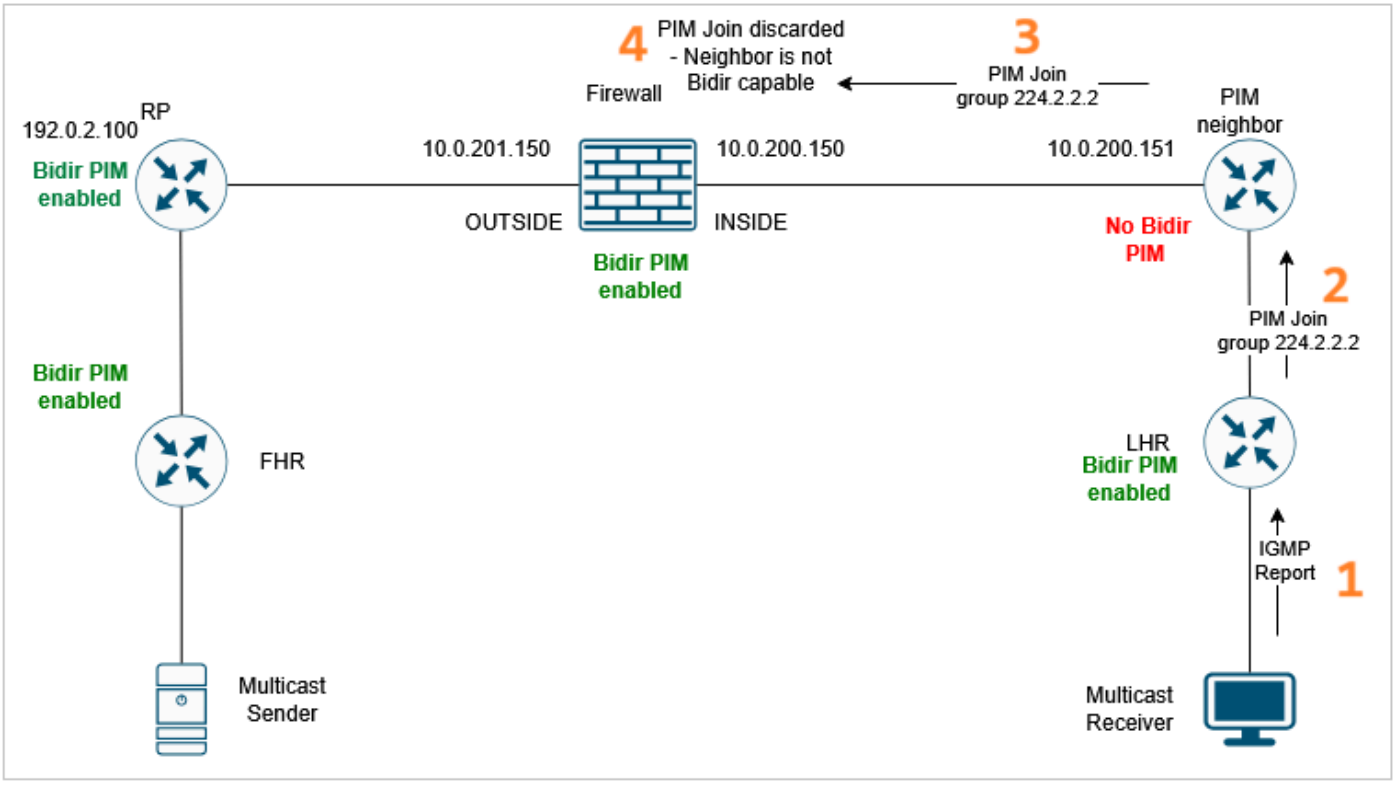
```
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, 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
```

Oorzaak

De multicast-verkeersstoring werd veroorzaakt door onjuiste of onvolledige multicast- en bidirectionele PIM-configuratie op het aangrenzende netwerkapparaat. Het specifieke configuratieprobleem leidde ertoe dat FTD het PIM Join/Prune-bericht voor de specifieke multicastgroep weggooide. Als gevolg hiervan kon de firewall de mroute voor het multicast-verkeer niet maken. Om multicast-dataverkeer door het firewall-gegevensvlak te laten stromen, moet het controlevlak (PIM) de juiste route vaststellen.



Oorzaak.png

Verwante inhoud

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.