使用Bidir PIM配置对不通过FTD防火墙的组播流量进行故障排除

目录

问题

可以看到以下所有症状：

- 组播流量停止了特定组播组的防火墙威胁防御(FTD)。
- FTD上没有该组（本例中为224.2.2.2）的组播路由(mroutes)。

<#root>

```
device#
```

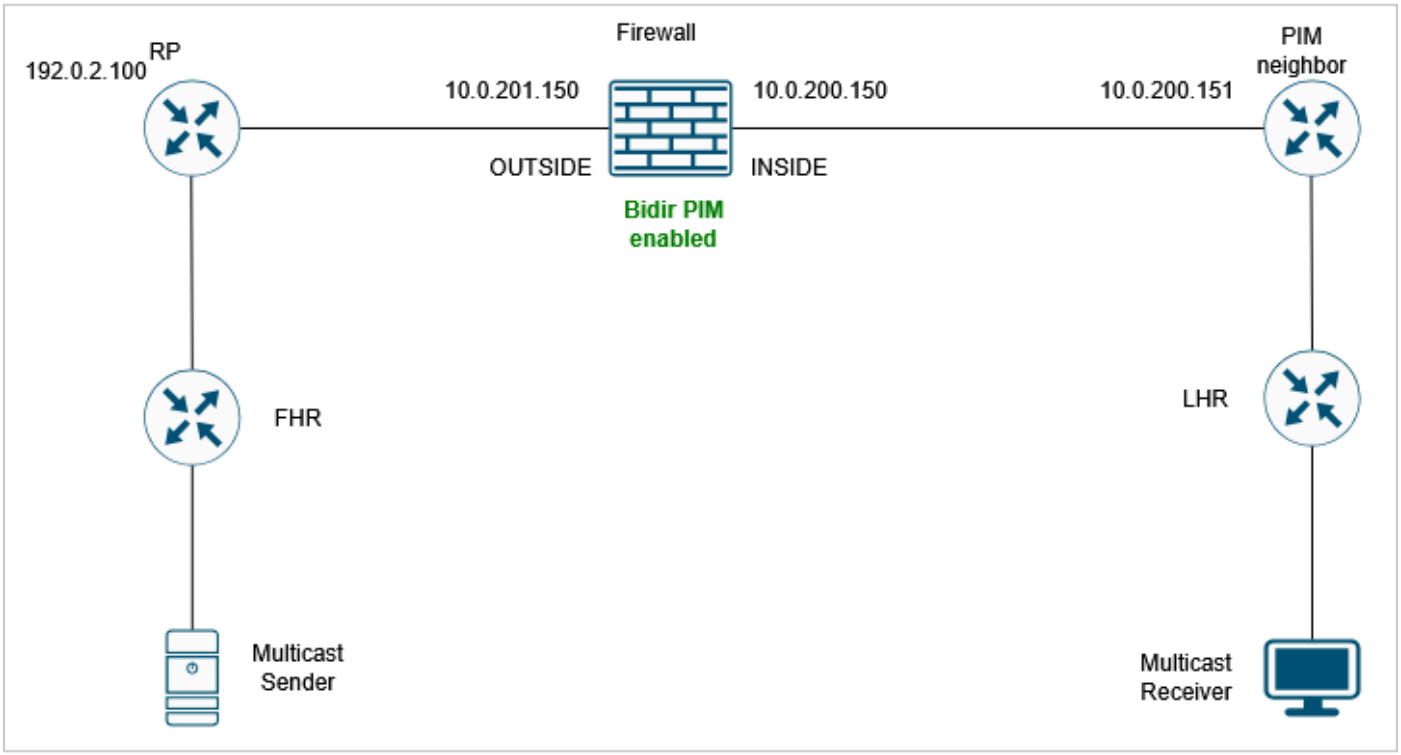
show mroute 224.2.2.2

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

环境

- 首次出现在FTD版本7.4中。其他软件版本（包括自适应安全设备[ASA]）也可能会受到影响。
- 在防火墙上启用双向协议独立组播(PIM)。

拓扑



inline_image_0.png

分辨率

步骤 1：查看当前组播配置。

检查网络路径中所有设备上的现有组播路由配置，确定可能阻止组播流量通过防火墙的任何配置错误或设置缺失。

防火墙上有双向PIM配置：

<#root>

device#

show run pim

pim rp-address 192.0.2.100 bidir

步骤 2：检验PIM邻居。

确认防火墙上正确显示了组播邻居：

```
<#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
```

在输出中，请注意，邻居10.0.201.200具有Bidir B标志，而10.0.200.151邻居没有该标志。

步骤 3：为组播组224.2.2.2启用PIM调试：

```
<#root>

FPR3100-14#

debug pim group 224.2.2.2


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

调试显示有一个因“no bidir df selection”而被丢弃的PIM加入/修剪数据包：

```
<#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
```

步骤 4：对10.0.200.151 PIM邻居启用PIM捕获。目标是提高对数据包内容的可视性：

<#root>

```
device#

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

步骤 5：从FTD设备收集防火墙捕获：

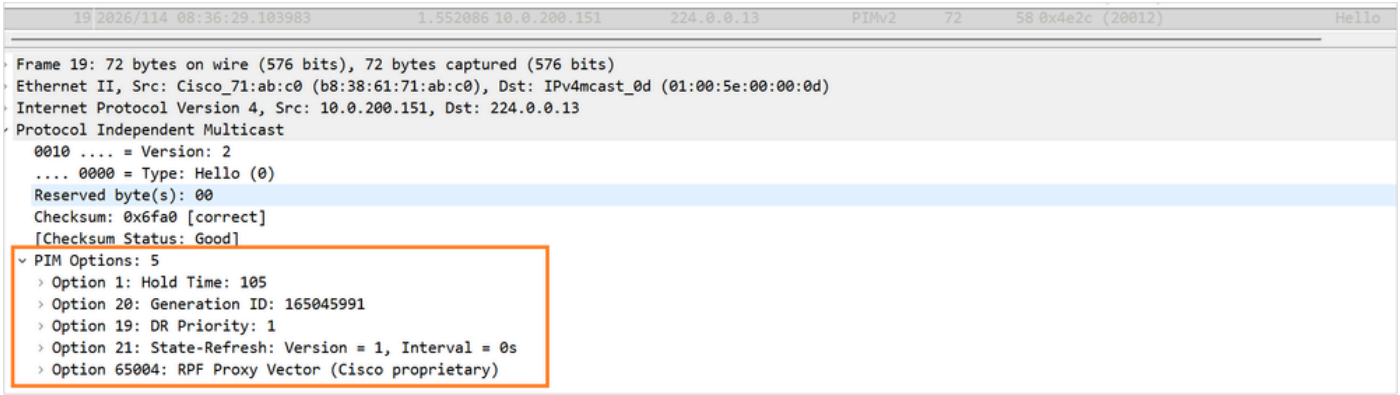
<#root>

```
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
```

使用https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html中所述的过程从FMC收集pcap文件

步骤 6：捕获分析。

PIM Hello数据包包含以下选项：



PIM_Hello_Options_no-bidir-capable.png

注意没有支持Bidir的标志。

步骤 7：在10.0.200.151邻居上启用双向PIM。

现在，将为两个邻居显示PIM Bidir B标志：

<#root>

device#

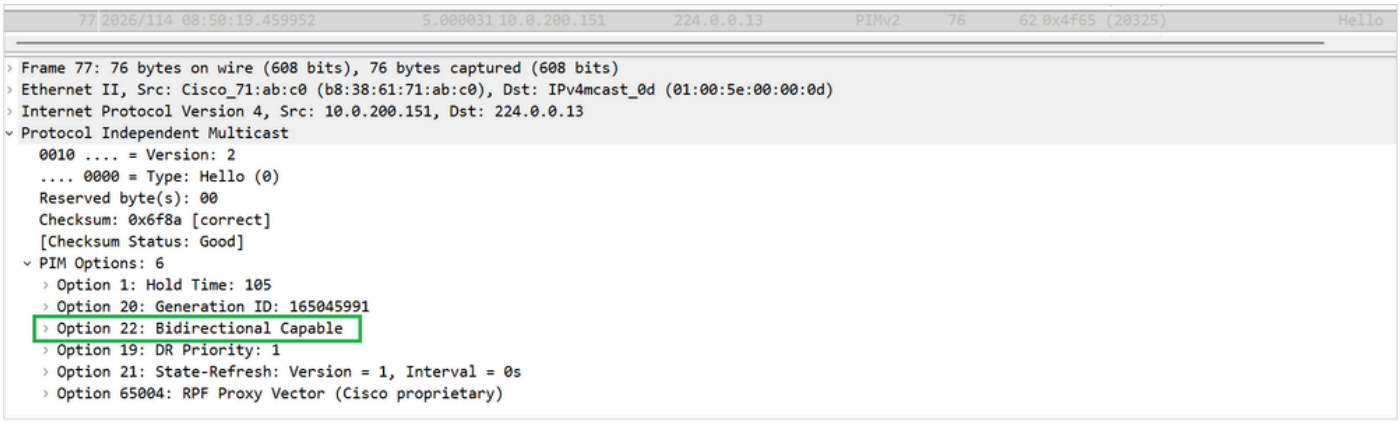
show pim neighbor

```
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
```

步骤 8::收集新捕获并检查邻居10.0.200.151的PIM Hello选项。图中显示了PIM选项22(Bidirectional Capable):



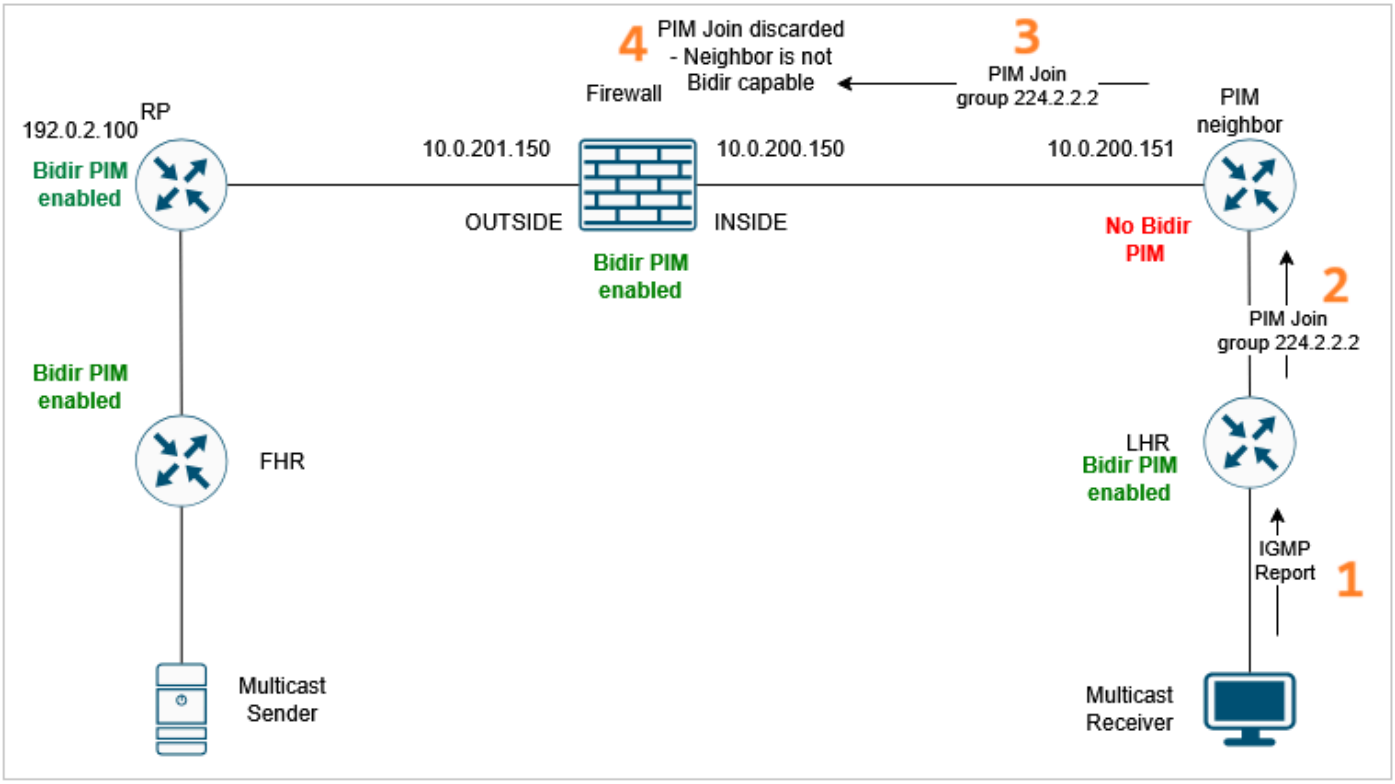
PIM_Hello_Options_option22.png

步骤 9：检验组播组224.2.2.2的mroute现在是否显示：

```
<#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
```

原因

组播流量故障是由相邻网络设备上的不正确或不完整组播和双向PIM配置引起的。特定配置问题导致FTD丢弃特定组播组的PIM加入/修剪消息。因此，防火墙无法为组播流量创建mroute。要使组播数据流量流经防火墙数据平面，控制平面(PIM)必须建立正确的mroute。



原因.png

相关内容

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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。