Bidir PIM 컨피그레이션으로 FTD 방화벽을 통과하지 못하는 멀티캐스트 트래픽 문제 해결

목차

문제

이러한 모든 증상이 나타납니다.

- 멀티캐스트 트래픽이 특정 멀티캐스트 그룹의 FTD(Firewall Threat Defense)에서 작동을 중지했습니다.
- 그룹(이 예에서는 224.2.2.2)의 FTD에 멀티캐스트 경로(mroutes)가 없습니다.

<#root>

```
device#
```

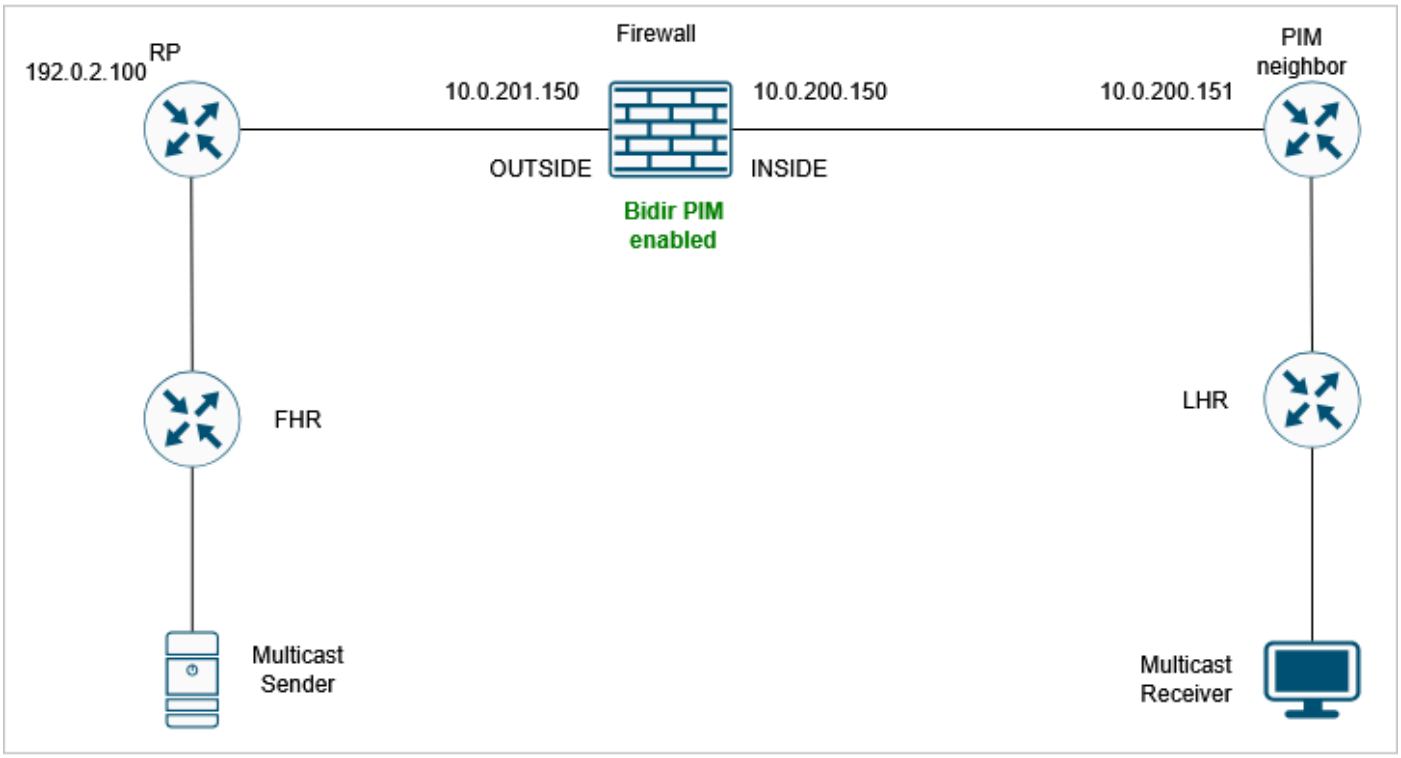
show mroute 224.2.2.2

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

환경

- FTD 버전 7.4에 처음 표시되었습니다. ASA(Adaptive Security Appliance)를 비롯한 다른 소프트웨어 버전도 영향을 받을 수 있습니다.
- 방화벽에서 PIM(Bidirectional Protocol Independent Multicast)이 활성화됩니다.

토폴로지



inline_image_0.png

해결

1단계: 현재 멀티캐스트 컨피그레이션을 검토합니다.

네트워크 경로의 모든 디바이스에서 기존 멀티캐스트 라우팅 컨피그레이션을 검사하여 멀티캐스트 트래픽이 방화벽을 통과하지 못하게 할 수 있는 잘못된 컨피그레이션 또는 누락된 설정을 식별합니다.

방화벽에는 양방향 PIM 컨피그레이션이 있습니다.

<#root>

```
device#
```

show run pim

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

2단계: PIM 인접 디바이스를 확인합니다.

멀티캐스트 네이버가 방화벽에 제대로 표시되는지 확인합니다.

<#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
```

출력 알림에서 네이버 10.0.201.200에는 Bidir B 플래그가 있는 반면 10.0.200.151 네이버에는 Bidir B 플래그가 없습니다.

3단계: 멀티캐스트 그룹 224.2.2.2에 대한 PIM 디버그 활성화:

<#root>

```
FPR3100-14#

debug pim group 224.2.2.2


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

디버그는 'no bidir df selection'(bidir df 선택 안 함)으로 인해 삭제된 PIM Join/Prune 패킷이 있음을 보여줍니다.

<#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
```

4단계: 10.0.200.151 PIM 네이버에 대해 PIM 캡처를 활성화합니다. 목표는 패킷 내용에 대한 가시성을 확보하는 것입니다.

```
<#root>

device#

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

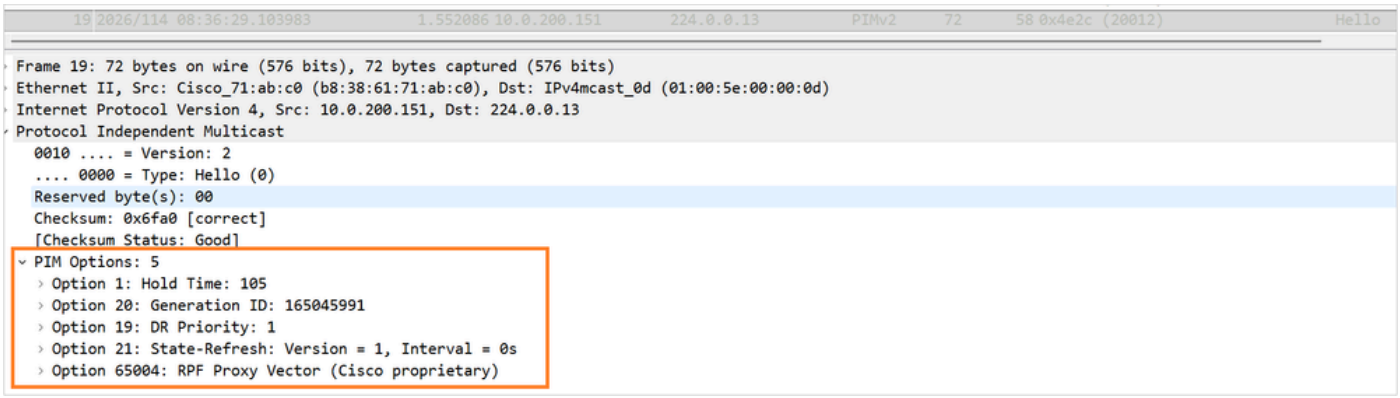
5단계: FTD 디바이스에서 방화벽 캡처를 수집합니다.

```
<#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
```

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html에 설명된 절차를 사용하여 FMC에서 pcap 파일을 수집합니다

6단계: 캡처 분석

PIM Hello 패킷에는 다음 옵션이 포함됩니다.



PIM_Hello_Options_no-bidir-capable.png

Bidir-capable 플래그가 없음을 확인합니다.

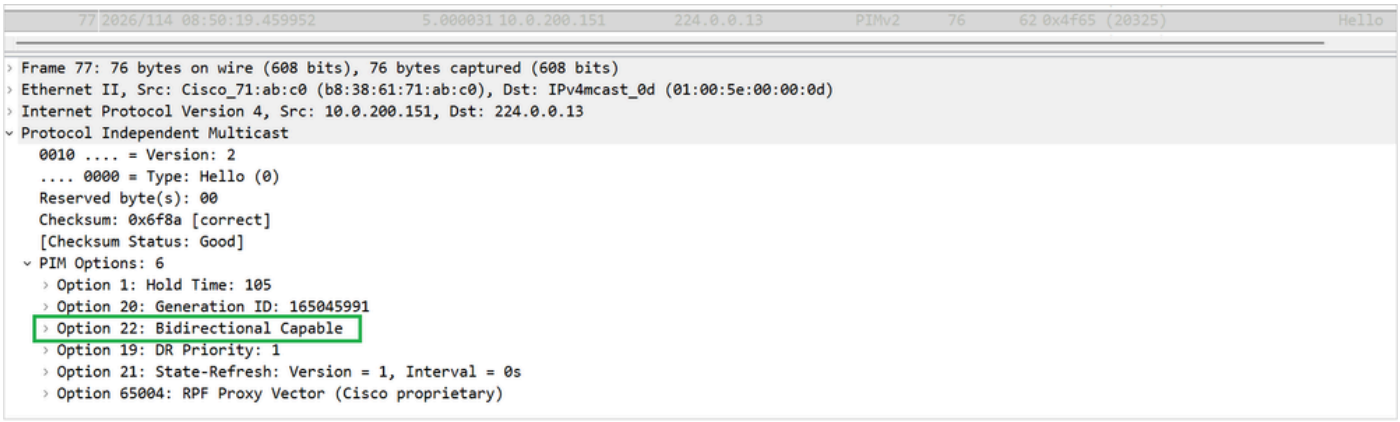
7단계: 10.0.200.151 네이버에서 양방향 PIM을 활성화합니다.

이제 두 네이버 모두에 대해 PIM Bidir B 플래그가 표시됩니다.

<#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
```

8단계: 새 캡처를 수집하고 인접 디바이스 10.0.200.151에 대한 PIM Hello 옵션을 확인합니다. PIM 옵션 22(Bidirectional Capable)가 표시됩니다.



PIM_Hello_Options_option22.png

9단계: 멀티캐스트 그룹 224.2.2.2에 대한 mroute가 표시되는지 확인합니다.

<#root>

device#

show mroute

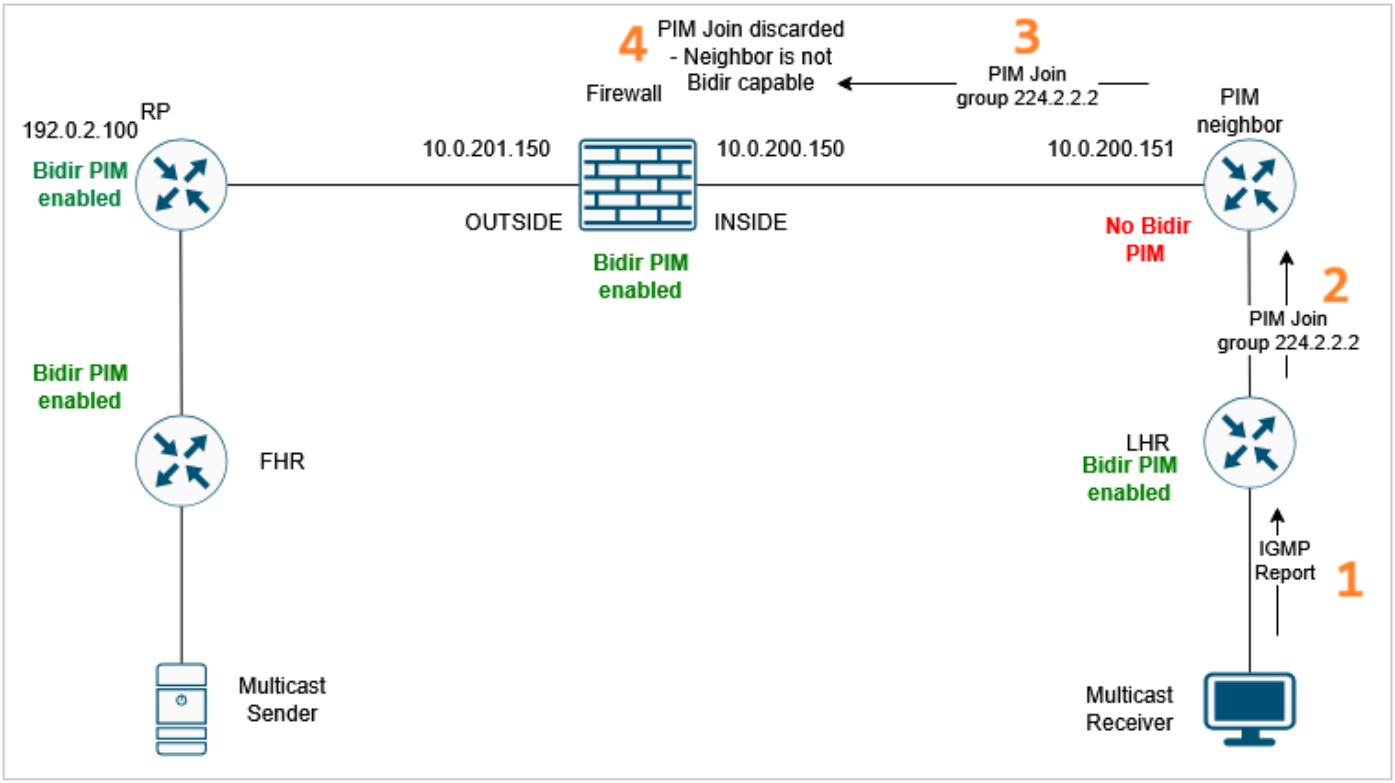
```
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface,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

원인

멀티캐스트 트래픽 실패는 인접 네트워크 디바이스에서 잘못되거나 불완전한 멀티캐스트 및 양방향 PIM 컨피그레이션으로 인해 발생했습니다. 특정 컨피그레이션 문제로 인해 FTD가 특정 멀티캐스트 그룹에 대한 PIM Join/Prune 메시지를 삭제합니다. 따라서 방화벽에서 멀티캐스트 트래픽에 대한 mroute를 생성할 수 없습니다. 멀티캐스트 데이터 트래픽이 방화벽 데이터 플레인을 통과하도록 하려면 PIM(제어 플레인)에서 적절한 경로를 설정해야 합니다.



원인.png

관련 콘텐츠

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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.