Bidir PIM設定を使用したFTDファイアウォールを通過しないマルチキャストトラフィックのトラブルシューティング

内容

お問い合わせ内容

次の症状がすべて見られます。

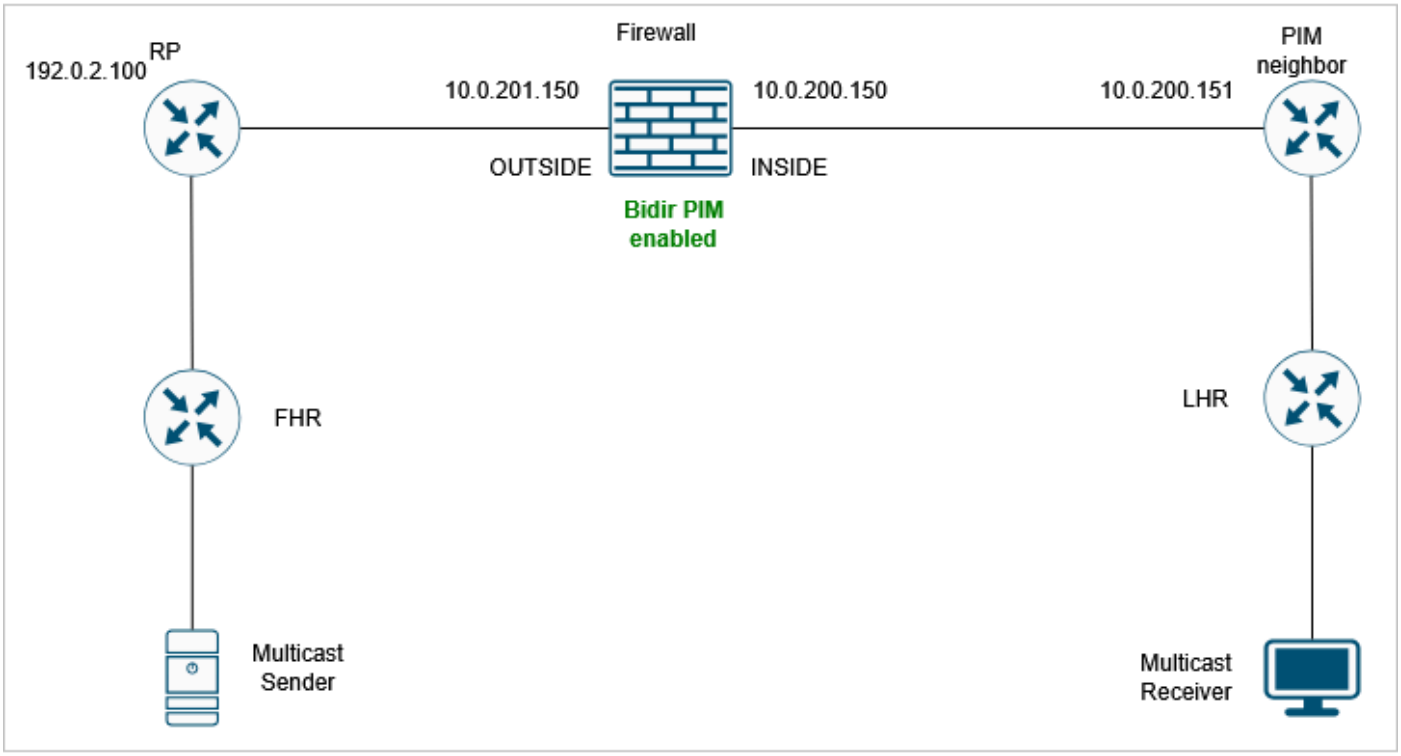
- 特定のマルチキャストグループに対するファイアウォール脅威対策(FTD)で、マルチキャストトラフィックの処理が停止しました。
- FTDにはグループのマルチキャストルート(mroute)がありません（この例では224.2.2.2）。

```
<#root>

device#

show mroute 224.2.2.2


No mroute entries found.
device#
```

環境

- FTDバージョン7.4で初めて確認されました。適応型セキュリティアプライアンス(ASA)など、その他のソフトウェアバージョンも影響を受ける可能性があります。
- ファイアウォールでBidirectional Protocol Independent Multicast(PIM)が有効になっている。

トポロジ



inline_image_0.png (インラインイメージ_0.png)

解決策

ステップ1:現在のマルチキャスト設定を確認します。

ネットワークパス内のすべてのデバイスの既存のマルチキャストルーティング設定を調べて、マルチキャストトラフィックによるファイアウォールの通過を妨げる可能性のある設定の誤りや設定の欠落を特定します。

ファイアウォールには、双方向PIM(BIDIR-PIM)設定があります。

<#root>

device#

show run pim

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

手順2:PIMネイバーを確認します。

マルチキャストネイバーがファイアウォールで正しく表示されていることを確認します。

<#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

出力では、ネイバー10.0.201.200にBidir Bフラグがあるのに対し、ネイバー10.0.200.151にはないことがわかります。

ステップ3:マルチキャストグループ224.2.2.2に対してPIMデバッグを有効にします。

<#root>

```
FPR3100-14#
```

debug pim group 224.2.2.2

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

デバッグは、「no bidir df election」が原因で廃棄されたPIM Join/Pruneパケットがあることを示しています。

<#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
```

ステップ4:10.0.200.151 PIMネイバーに対するPIMキャプチャを有効にします。目標は、パケットコンテンツの可視性を高めることです。

<#root>

```
device#

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

ステップ5:FTDデバイスからファイアウォールキャプチャを収集します。

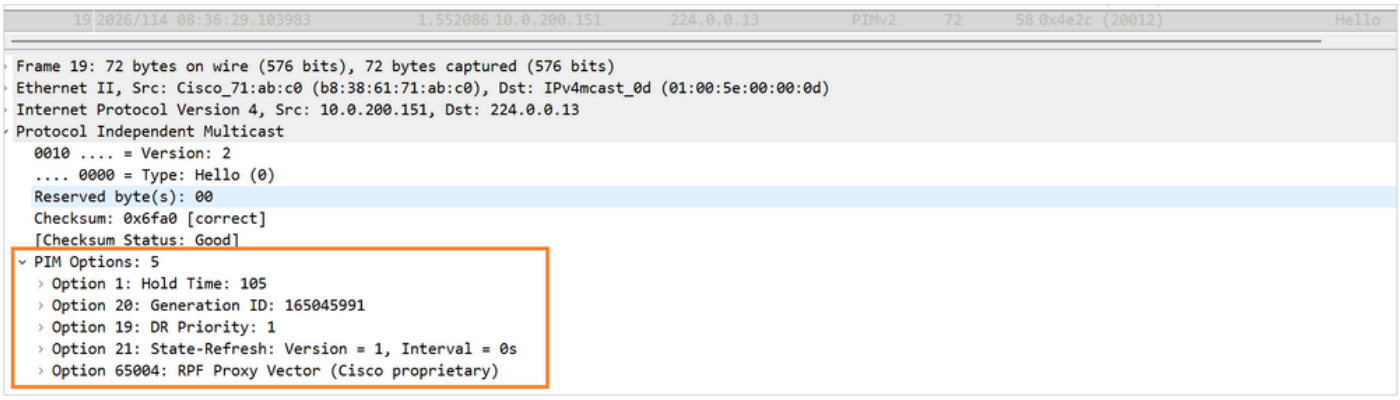
<#root>

```
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.html で説明されている手順を使用して、FMCからpcapファイルを収集します。

ステップ6：分析をキャプチャします。

PIM Helloパケットには、次のオプションが含まれます。



PIM_Hello_Options_no-bidir-capable.png (双方向パスを使用できない場合)

Bidir-capableフラグがないことに注意してください。

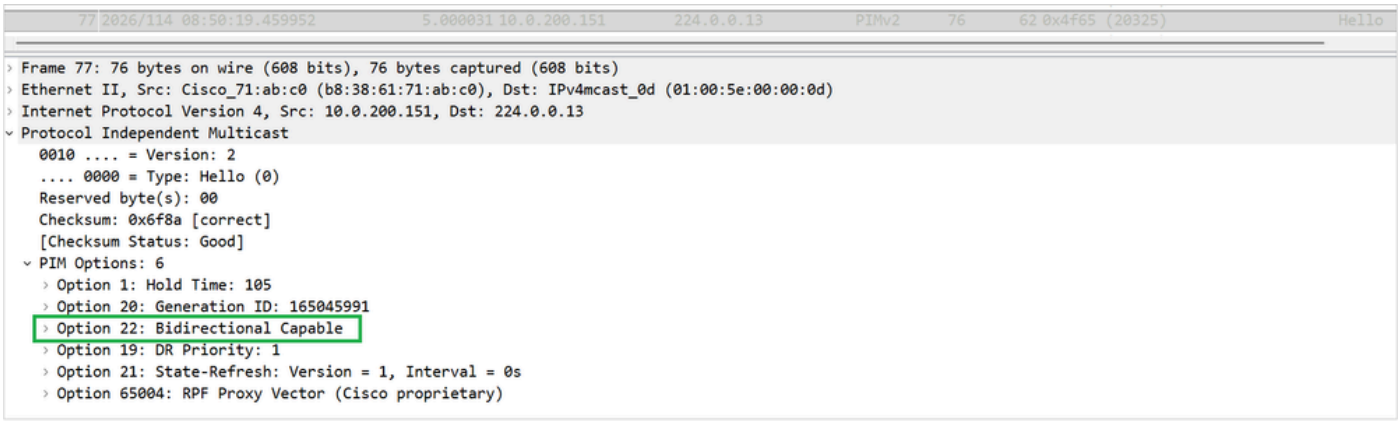
ステップ7:10.0.200.151ネイバーで双方向PIMを有効にします。

これで、両方のネイバーのPIM Bidir Bフラグが表示されます。

<#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
```

ステップ8:新しいキャプチャを収集して、ネイバー10.0.200.151のPIM Helloオプションを確認します。PIMオプション22(Bidirectional Capable)を次に示します。



PIM_Hello_オプション_オプション22.png

手順9:マルチキャストグループ224.2.2.2のmrouteが表示されていることを確認します。

<#root>

device#

show mroute

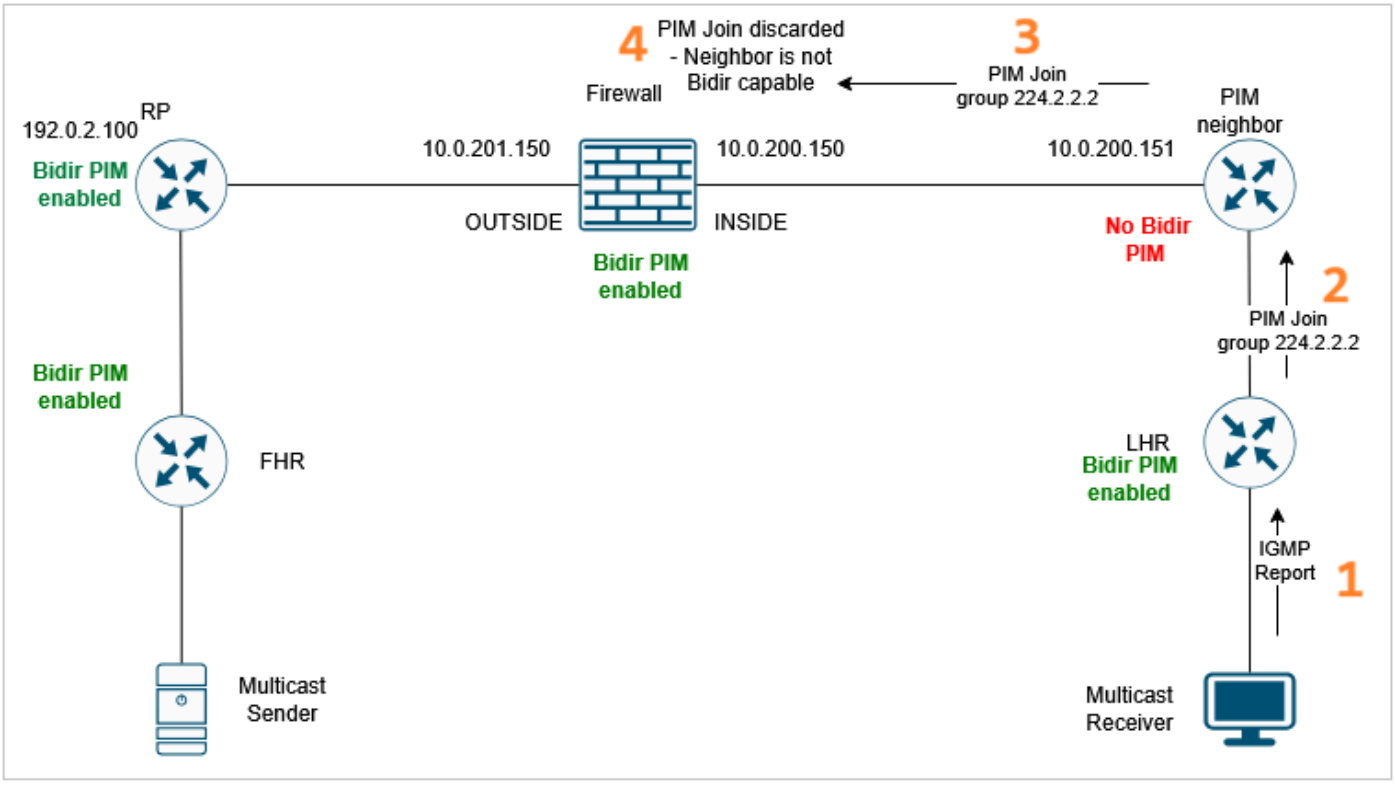
```
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface,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

マルチキャストトラフィックの障害は、隣接するネットワークデバイスでのマルチキャストおよび双方向PIMの設定が正しくないか、不完全であることが原因で発生しました。特定の設定の問題が原因で、FTDは特定のマルチキャストグループのPIM Join/Pruneメッセージを破棄しました。その結果、ファイアウォールはマルチキャストトラフィック用のmrouteを作成できませんでした。マルチキャストデータトラフィックがファイアウォールデータプレーンを通過するには、コントロールプレーン(PIM)が適切なmrouteを確立する必要があります。



原因.png

関連コンテンツ

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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。