Bidir PIM設定を使用したファイアウォールでのマルチキャストパケットドロップのトラブルシューティング

内容

お問い合わせ内容

これらの症状は、PIMスパースモード(PIM-SM)のバリアントであるBidirectional Protocol Independent Multicast(BIDIR-PIM)を使用したマルチキャストルーティングドメインで、中間ホップとして参加するSecure Firewall Threat Defense(FTD)で発生します。

1. 特定のマルチキャストグループ232.4.4.4のmrouteが存在しない場合：

<#root>

device#

show mroute 232.4.4.4

No mroute entries found.

2. show mfib countコマンド出力の、232.0.0.0/8グループ範囲に対する「Other drops」カウンタが増加します。

<#root>

device#

show mfib count

IP Multicast Statistics

6 routes, 3 groups, 0.00 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second

Other counts: Total

/RPF failed/

Other drops(OIF-null, rate-limit etc)

Group: 224.0.1.39
  RP-tree:
   Forwarding: 0/0/0/0, Other: 0/0/0
Group: 224.0.1.40
  RP-tree:
   Forwarding: 0/0/0/0, Other: 0/0/0

Group: 232.0.0.0/8

  RP-tree:
   Forwarding: 0/0/0/0,

Other: 2551

/0/

2551 <----

device#

show mfib count

IP Multicast Statistics
6 routes, 3 groups, 0.00 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second

Other counts: Total

/RPF failed/

Other drops(OIF-null, rate-limit etc)

Group: 224.0.1.39
  RP-tree:
   Forwarding: 0/0/0/0, Other: 0/0/0
Group: 224.0.1.40
  RP-tree:
   Forwarding: 0/0/0/0, Other: 0/0/0

Group: 232.0.0.0/8

  RP-tree:
   Forwarding: 0/0/0/0,

Other: 2864

/0/

2864

<----

3. 高速セキュリティパス(ASP)で、パントレート制限を超えた（パントレート制限）ドロップの理由で、マルチキャストパケットがドロップされます。 ドロップカウンタが継続的に増加します。

<#root>

device#

cap capi trace interface inside match udp any host 232.4.4.4

device#

show cap capi trace

   2: 19:36:08.509205

192.168.1.2.12345 > 232.4.4.4.12345

: udp 0
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 13056 ns
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 13056 ns
Config:

```
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Elapsed time: 2560 ns
Config:
Additional Information:
Found flow with id 4876, using existing flow

Result:
input-interface: inside
input-status: up
input-line-status: up
Action: drop
Time Taken: 28672 ns

Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (NA



device#

show asp drop



Frame drop:

  Punt rate limit exceeded (punt-rate-limit)                                    142


  FP L2 rule drop (l2_acl)                                                        6

Last clearing: 19:38:00 UTC Apr 29 2026 by admin

Flow drop:

Last clearing: 19:38:00 UTC Apr 29 2026 by admin
…
device#

show asp drop



Frame drop:

  Punt rate limit exceeded (punt-rate-limit)                                    780


  FP L2 rule drop (l2_acl)                                                       37
```

4. Outsideインターフェイスのキャプチャでは、出力マルチキャストパケットは表示されません。

<#root>

device#

capture capo type raw-data interface outside match udp any host 232.4.4.4

device#

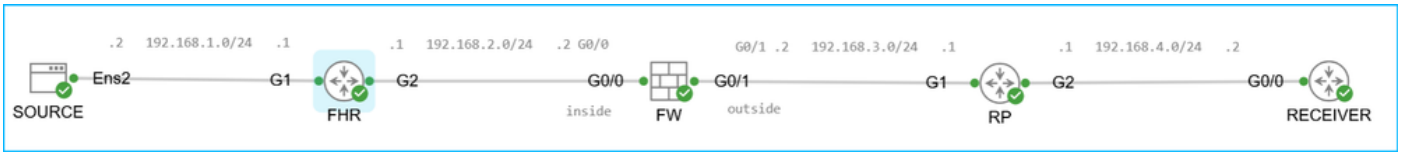
show cap capo

0 packet captured

0 packet shown

環境

トポロジ：



トポロジ.png

キー ポイント：

- マルチキャストドメインのピアはBIDIR-PIMを使用します。
- この記事の「ルータ」は、CSRやASRなどのCiscoルータを指します。

- ランデブーポイント(RP)は、Cisco IOS XEソフトウェアバージョン17.09.08を実行するASR1001-Xです。他のプラットフォームや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。
- ファーストホップルータ(FHR)は、Cisco IOS XEソフトウェアバージョン16.12.04を実行するC9200L-48T-4Gです。他のプラットフォームや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。
- ランデブーポイント(RP)アドレス10.4.4.4 をLoopback0 インターフェイス上でマルチキャスト範囲全体(224.0.0.0/8)に対して動的に伝搬されるのは、PIMブートストラップルータ(BSR)を使用してです。 スタティックPIM RPアドレス設定を使用した展開も影響を受ける可能性があります。

  RPでのPIM設定：

  <#root>

  device#

  show run interface loopback0

  interface Loopback0
   description LO0
   ip address 10.4.4.4 255.255.255.255
   ip pim sparse-mode

  device(config)#

  ip pim bidir-enable

  device(config)#

  ip pim bsr-candidate Loopback0 0 1

  device(config)#

  ip pim rp-candidate Loopback0 interval 10 priority 1 bidir

- わかりやすくするために、この例では、RPは受信側に接続されていると示されています。つまり、RPはラストホップルータ(LHR)でもあるということです。これはオプションです。
- ファイアウォールは、バージョン7.6.4を実行するセキュアファイアウォール3110です。他のファイアウォールプラットフォーム、ソフトウェアバージョン、および適応型セキュリティアプライアンス(ASA)ソフトウェアも影響を受ける可能性があります。
- ファイアウォールでは、マルチキャストルーティングが有効で、ファーストホップルータ(FHR)とPIM隣接関係があり、PIM BIDIR機能を持つRPがあります。

  <#root>

```
device#
show run multicast-routing


multicast-routing


device#
show pim neighbor


Neighbor Address  Interface          Uptime    Expires DR pri Bidir
192.168.2.1       inside             1d12h     00:01:40 1
B
192.168.3.1       outside            1d12h     00:01:35 1
B
```

- ファイアウォールでは、PIM BSRを使用しているにもかかわらず、PIM RPアドレス10.4.4.4は手動で設定されます。これは冗長構成です。その結果、グループ224.0.0.0/4とRPアドレス10.4.4.4の間に2つのRP間マッピングが存在します。

```
<#root>
device#
show run pim


pim rp-address 10.4.4.4 bidir


device#
show pim group-map


Group Range         Proto   Client   Groups RP address      Info
224.0.1.39/32*      DM      static   0      0.0.0.0
224.0.1.40/32*      DM      static   0      0.0.0.0
224.0.0.0/24*       L-Local static   1      0.0.0.0
232.0.0.0/8*        SSM     config   0      0.0.0.0
224.0.0.0/4*        BD      BSR      0      10.4.4.4   RPF: outside,192.168.3.1 <-- * means the ma
```

```
224.0.0.0/4          BD      config   0      10.4.4.4    RPF: outside,192.168.3.1

224.0.0.0/4          SM      static   0      0.0.0.0          RPF: ,0.0.0.0
```

解決策

先に進む前に、「原因」セクションを必ず確認してください。

ファイアウォールでのパケットドロップは、意図した設定(BIDIR-PIM)と、PIM SSMを使用した処理が必要なトラフィックとの間の非互換性が原因で発生すると考えられます。

目的の設定がBIDIR-PIMの場合は、次のオプションを検討します。

- 非PIM SSMグループのみを使用します。
- PIM SSMグループを使用する必要がある場合は、ファイアウォールがPIM SSM範囲からのマルチキャストグループを非SSMグループアドレスとして処理することを確認します。詳細については、「Q&A」のセクションを参照してください。
- Cisco Bug ID CSCwt99960を参照してください。

原因

アドレス232.4.4.4は、Internet Assigned Numbers Authority(IANA)によって予約されたSource Specific Multicast(SSM)グループ範囲に属しています。 ファイアウォールでは、PIM SSM用に232.0.0.0/8の範囲が自動的に予約されます。

<#root>

```
device#

show pim group-map


Group Range          Proto   Client   Groups RP address      Info

224.0.1.39/32*       DM      static   0      0.0.0.0
```

```
224.0.1.40/32*      DM      static   0      0.0.0.0
224.0.0.0/24*       L-Local static   1      0.0.0.0

232.0.0.0/8*        SSM     config   0      0.0.0.0



224.0.0.0/4*        BD      BSR      0      10.4.4.4   RPF: outside,192.168.3.1
224.0.0.0/4         BD      config   0      10.4.4.4   RPF: outside,192.168.3.1
224.0.0.0/4         SM      static   0      0.0.0.0         RPF: ,0.0.0.0
```

PIM SSMに関する重要ポイント：

- ソースベースのツリーを構築し、(S、G)mrouteを使用する
- PIM-SMプロトコルのRPベースの共有ツリーインフラストラクチャは必要ありません。つまり、RPまたは(*, G)mrouteは使用されません。
- 受信者は通常、「送信元フィルタリング」を備えたInternet Group Management Protocol Version 3(IGMPv3)を使用してマルチキャストツリーに参加します。これは、特定の送信元アドレスからのパケットだけを受信するか、特定のマルチキャストアドレスに送信された特定の送信元アドレス以外のパケットを受信するかを対象とするレポートをシステムが作成する機能です。

BIDIR-PIMに関する要点：

- マルチキャストの送信側と受信側を接続する双方向共有ツリーを構築する
- 双方向ツリーは、マルチキャストトポロジの各リンクで動作するフェールセーフの指定フォワーダ(DF)選択メカニズムを使用して構築されます。
- DFの支援により、マルチキャストデータは送信元からRPにネイティブに転送されるため、送信元固有の状態を必要とせずに共有ツリーに沿って受信側に転送されます。
- BIDIR-PIMは、最短パスツリー(SPT)および(S、G)エントリを使用しません。
- BIDIR-PIMピアは(*, G)エントリを使用して共有ツリーを構築します。特定のマルチキャストグループに対するこのエントリは、mrouteテーブルに存在している必要があります。

PIM SSMとBIDIR-PIMのキーポイントを対比すると、PIM SSMとBIDIR-PIMは相互に排他的な機能を持ちます。

この場合、マルチキャストドメインはBIDIR-PIMを使用するように設定されますが、マルチキャストグループはIANAによって予約された範囲とPIM SSM用のファイアウォールに属します。マルチキャストドメインはBIDIR-PIMを使用しているため、PIM SSMに必要な(S、G)mrouteはファイ

アウォールで使用できません。mrouteがないため、マルチキャストトラフィックの発信/出力インターフェイスは使用できません。出力/出力インターフェイスが存在しないと、マルチキャスト転送情報ベース(MFIB)でパケットがドロップされます。 ドロップは、show mfibまたはshow mfib countコマンドを使用して確認できます。

<#root>

```
device#

show mfib count



IP Multicast Statistics
6 routes, 3 groups, 0.00 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second

Other counts: Total

/RPF failed/

Other drops(OIF-null, rate-limit etc)



Group: 224.0.1.39
  RP-tree:
   Forwarding: 0/0/0/0, Other: 0/0/0
Group: 224.0.1.40
  RP-tree:
   Forwarding: 0/0/0/0, Other: 0/0/0

Group: 232.0.0.0/8



  RP-tree:
   Forwarding: 0/0/0/0, Other:

333797

/0/

333797
```

ファイアウォールは、Control Point（CP；コントロールポイント）を使って発信/出力インターフェイスの解決を試みます。 これは、ルーティングプロトコル、管理アクセス、フェールオーバー/クラスタ管理、ファイアウォールインターフェイス宛てのパケットの処理、マルチキャストまたはブロードキャストIPアドレスなど、管理およびコントロールプレーンの機能を主に担う重要なファイアウォールコンポーネントです。

コントロールポイントの過負荷を回避するために、ファイアウォールには保護メカニズムが組み込まれています。たとえば、ファイアウォールは、データプレーン(DP)からコントロールポイントに送信されるパケットのレートを制限します。レートを超過したパケットは、punt rate limit exceeded (punt-rate-limit) ASPドロップの理由でドロップされます。パントレートは、show asp event dp-cp punt | begin EVENT-TYPEコマンドの出力で確認できます。

```
<#root>

device#

show asp event dp-cp punt | begin EVENT-TYPE


EVENT-TYPE          ALLOC ALLOC-FAIL ENQUEUED ENQ-FAIL  RETIRED 15SEC-RATE

punt              1264746          0  1264746        0  1264746         44

<-- 15-second punt rate

  multicast       1250020          0  1250020        0  1250020         44



  pim               14726          0    14726        0    14726          0
```

つまり、ファイアウォールでのパケットドロップは、意図した設定(BIDIR-PIM)と、PIM SSMを使用した処理が必要なトラフィックとの間の非互換性が原因であると考えられます。

Q&A

このセクションで、「ルータ」はCSRなどのCiscoルータを指し、「ファイアウォール」はASAまたはFTDを実行するCiscoファイアウォールを指します。

1. Q:ファイアウォールはPIM SSM用に232.0.0.0/8を自動的に予約しますか。

A:はい。たとえばCSRなどのルータとは異なり、特定の設定は必要ありません。ルータでは、PIM SSM範囲を明示的に設定する必要があります。

```
<#root>
```

```
device(config)#

ip pim ssm ?


  default  Use 232/8 group range for SSM


  range    ACL for group range to be used for SSM
```

2. Q: MFIBの「Other drops」カウンタはファイアウォールに固有のものですか。

A:いいえ。同様のカウンタが、マルチキャストルーティングを行うCiscoルータにも存在します。

3. Q:ファイアウォールの代わりにルータのような別のデバイスでも、グループ232.4.4.4に送信されたパケットをドロップしますか。

A:これは、ルータがアドレス232.4.4.4をどのように扱うかによって異なります。ファイアウォールとは異なり、デフォルトでは、ルータはPIM SSM用に232.0.0.0/8の範囲を予約しません。ただし、PIM SSMとBIDIR-PIMの両方が有効で、ルータがBIDIR-PIM対応RPであるか、Bidirフラグを使用してRPからグループへのマッピングを受信し、PIM SSM範囲に送信されたマルチキャストパケットを受信する場合、パケットはドロップされ、MFIBの「Other」カウンタが増加します。

<#root>

```
device#

show run | i pim


ip pim bidir-enable


no ip pim autorp

ip pim ssm default
```

```
device#
```

show ip pim rp mapping

```
Auto-RP is not enabled
PIM Group-to-RP Mappings

Group(s) 224.0.0.0/4
  RP 10.4.4.4 (?), v2,
```

bidir <-- mapping has the bidir flag

```
    Info source: 10.4.4.4 (?), via bootstrap, priority 1, holdtime 150
         Uptime: 17:32:39, expires: 00:02:05

device#
```

show ip mfib count

```
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
```

Other counts: Total/RPF failed

```
/Other drops(OIF-null, rate-limit etc)
Default
 9 routes, 6 (*,G)s, 3 (*,G/m)s
Group: 224.0.0.0/4
  RP-tree,
   SW Forwarding: 1/0/28/0, Other: 41037/41037/0
   HW Forwarding:   3428217/0/64/0, Other: 0/0/0
```

Group: 232.0.0.0/8

```
  RP-tree,
```

SW Forwarding: 0/0/0/0, Other: 97/97

```
/0 <----
   HW Forwarding:   0/0/0/0, Other: 0/0/0

device#
```

show ip mfib count

```
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
```

Other counts: Total/RPF failed

```
/Other drops(OIF-null, rate-limit etc)
Default
 9 routes, 6 (*,G)s, 3 (*,G/m)s
Group: 224.0.0.0/4
  RP-tree,
   SW Forwarding: 1/0/28/0, Other: 41037/41037/0
   HW Forwarding:   3428217/0/64/0, Other: 0/0/0

Group: 232.0.0.0/8


  RP-tree,



SW Forwarding: 0/0/0/0,

 Other: 106/106

/0 <----
   HW Forwarding:   0/0/0/0, Other: 0/0/0
```

ルータの「Other drops」カウンタが増加しているファイアウォールとは異なり、増加しているカウンタは「RPF failed」です。

4. Q:ファイアウォールでPIM SSM範囲のグループを非SSMグループアドレスとして処理させる方法を教えてください。

A: 232.0.0.0/8 (より長いプレフィクス) よりも詳細なグループに対してRPからグループへのマッピングをアドバタイズするか、またはファイアウォールで特定のグループに対してRPアドレスを手動で設定するか、どちらかの方法をRPがアドバタイズするようにします。

オプション 1RPの設定：

<#root>

```
device(config)#

access-list 1 permit host 232.4.4.4


device(config)#

ip pim rp-candidate Loopback0 group 1 interval 10 priority 1 bidir

<-- group refers to the access-list
```

ファイアウォールの検証：

<#root>

device#

show pim group-map 232.4.4.4

Group Range Proto Client Groups RP address Info

232.4.4.4/32* BD

BSR 0 10.4.4.4 RPF: outside,192.168.3.1 <-- Proto is BD, not SSM

オプション 2ファイアウォールの設定：

<#root>

device(config)#

access-list mcast standard permit 232.4.4.4 255.255.255.254

device(config)#

pim rp-address 10.4.4.4 mcast bidir

device(config)#

show pim group-map 232.4.4.4

Group Range Proto Client Groups RP address Info

232.4.4.4/31*

BD

config 0 10.4.4.4 RPF: outside,192.168.3.1 <-- Proto is BD, not SSM

アクセスリストでは、ホストエントリ、またはマスクが255.255.255.255のエントリを使用できないことに注意してください。

5. Q:ファイアウォールがPIM SSM範囲のグループを非SSMグループアドレスとして処理するとどうなりますか。

A：グループ232.4.4.4が非SSMアドレスとして処理されると仮定します（質問4を参照）。

```
<#root>

device#

show pim group-map 232.4.4.4


Group Range         Proto   Client   Groups RP address      Info

232.4.4.4/32*       BD

      BSR      0      10.4.4.4   RPF: outside,192.168.3.1
```

ソフトウェアバージョンがCisco Bug ID CSCwt99960の影響を受ける場合は、(*, G) mrouteが欠落しており、マルチキャストフローは1秒あたり約50パケットでレート制限されています。Punt rate limit exceeded (punt-rate-limit) ASPドロップの理由で、過剰なパケットがドロップされます。

```
<#root>

device#

show mroute 232.4.4.4


No mroute entries found.


device#

show mfib 232.4.4.4 count
```

```
IP Multicast Statistics
7 routes, 4 groups, 0.00 average sources per group
```

Forwarding Counts

```
: Pkt Count/
```

Pkts per second

```
/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Group: 232.4.4.4
  RP-tree:
   Forwarding: 23317/
```

50

```
/28/10, Other: 0/0/0


device#
```

show mfib 232.4.4.4 count

```


IP Multicast Statistics
7 routes, 4 groups, 0.00 average sources per group
```

Forwarding Counts:

```
 Pkt Count/
```

Pkts per second

```
/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Group: 232.4.4.4
  RP-tree:
   Forwarding: 23540/
```

49

```
/28/10, Other: 0/0/0

device#
```

capture capi interface inside trace match udp any host 232.4.4.4

```


device#
```

show capture capi trace | i Drop-reason

```
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (N/
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (N/
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (N/
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (N/
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (N/
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (N/
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (N/
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (N/
…
```

詳細については、Cisco Bug ID CSCwt99960を参照してください。

関連コンテンツ

- Source-Specific Multicastブロック
- Cisco Bug ID CSCwt99960

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。