使用Bidir PIM配置對防火牆上的組播資料包丟棄進行故障排除

目錄

問題

在使用雙向協定無關組播(BIDIR-PIM，PIM稀疏模式(PIM-SM)的變體，安全防火牆威脅防禦(FTD)作為中間跳加入組播路由域時可以觀察到以下症狀：

1.不存在特定組播組232.4.4.4的mroute:

<#root>

device#

show mroute 232.4.4.4

No mroute entries found.

2. show mfib count 命令輸出中232.0.0.0/8組範圍的「Other drops」計數器增加：

<#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.在加速安全路徑(ASP)中，當超過點數速率限制（點數速率限制）丟棄原因時，組播資料包會被丟棄。 丟棄計數器持續增加：

<#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
```

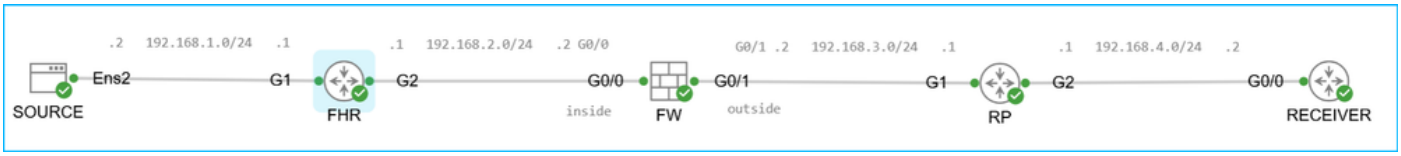
4.外部介面擷取不會顯示任何輸出多點傳送封包：

<#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

拓撲：



topology.png

重點：

- 組播域中的對等體使用BIDIR-PIM。
- 本文中的「路由器」指的是Cisco路由器，如CSR或ASR。
- 集結點(RP)是運行Cisco IOS XE軟體版本17.09.08的ASR1001-X。其他平台和軟體版本也可能會受到影響。
- 第一躍點路由器(FHR)是執行Cisco IOS XE軟體版本16.12.04的C9200L-48T-4G。其他平台和軟體版本也可能受到影響。
- 使用PIM引導路由器(BSR)在組播域中動態傳播整個組播範圍224.0.0.0/8loopback0 介面上的

交匯點(10.4.4.4)地址10.4.4。 使用靜態PIM RP地址配置的部署也會受到影響。

RP上的PIM配置：

```
<#root>

device#

show run interface loopback0


interface Loopback0
 description LOO
 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
```

- 為了簡便起見，在本例中，RP顯示為已連線到接收器，即它也是最後一跳路由器(LHR)。這是可選的。
- 防火牆是運行版本7.6.4的安全防火牆3110。其他防火牆平台、軟體版本和自適應安全裝置(ASA)軟體也可能會受到影響。
- 在防火牆上，組播路由已啟用，而且第一跳路由器(FHR)和RP具有PIM BIDIR功能：

```
<#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
```

- 在防火牆上，儘管使用PIM BSR，但PIM RP地址10.4.4.4是手動配置的。這是冗餘配置。因此，在組224.0.0.0/4和RP地址10.4.4.4之間存在2個RP到組的對映：

```
<#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
```

解析

在繼續操作之前，請確保複查「原因」部分。

由於預期配置(BIDIR-PIM)和需要使用PIM SSM處理的流量之間不相容，因此防火牆上可能會發生資料包丟棄。

如果目標配置是BIDIR-PIM，請考慮以下選項：

- 僅使用非PIM SSM組。
- 如果必須使用PIM SSM組，請確保防火牆將PIM SSM範圍內的組播組作為非SSM組地址處理。有關詳細資訊，請參閱問答部分。
- 考慮思科錯誤ID CSCwt9960。

原因

地址232.4.4.4屬於網際網路編號指派機構(IANA)保留的源特定組播(SSM)組範圍。 防火牆自動為PIM SSM保留232.0.0.0/8範圍：

<#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
```

有關PIM SSM的要點：

- 它構建源樹並使用(S， G)路由。
- 不需要基於RP的PIM-SM協定共用樹基礎架構。換句話說，不使用RP或(*, G)路由。

- 接收器通常通過使用網際網路組管理協定版本3(IGMPv3)和「源過濾」加入組播樹，即系統能夠報告只從特定源地址接收資料包的興趣，或者只從特定源地址接收傳送到特定組播地址的資料包。

有關BIDIR-PIM的要點：

- 它建立連線組播源和接收器的雙向共用樹。
- 使用在組播拓撲的每個鏈路上運行的故障安全指定轉發器(DF)選舉機制來構建雙向樹。
- 在DF的幫助下，組播資料從源自發地轉發到RP，並且因此沿著共用樹轉發到接收器，而不需要源特定的狀態。
- BIDIR-PIM不使用最短路徑樹(SPT)和(S， G)條目。
- BIDIR-PIM對等體使用(*, G)條目構建共用樹。特定組播組的此項必須存在於mroute表中。

通過比較PIM SSM和BIDIR-PIM的關鍵點，可以看出PIM SSM和BIDIR-PIM具有互斥的功能。

在這種情況下，組播域配置為使用BIDIR-PIM，而組播組屬於IANA和防火牆為PIM SSM保留的範圍。由於組播域使用BIDIR-PIM，因此PIM SSM所需的(S， G)路由在防火牆上不可用。由於缺少路由，組播流量的傳出/輸出介面不可用。沒有輸出/輸出介面會導致多點傳送轉送資訊庫(MFIB)中的封包捨棄。 可以使用show mfib或show mfib count命令驗證丟棄情況：

<#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

防火牆會嘗試透過使用控制點(CP)來解析傳出/輸出介面。 這是關鍵的防火牆元件，主要負責管理和控制層面的功能，如路由協定、管理訪問、故障切換/群集管理、處理髮往防火牆介面的資料包、組播或廣播IP地址等。

為避免控制點過載，防火牆具有內建的保護機制。例如，防火牆會限制從資料平面(DP)傳送到控制點的封包速率。超出速率的資料包將被丟棄，同時超出位元率限制(punt-rate-limit)ASP丟棄原因。可在show asp event dp-cp punt的輸出中驗證punt rate | begin EVENT-TYPE 命令：

<#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**

總之，結論是，由於預期配置(BIDIR-PIM)和需要使用PIM SSM處理的流量之間的不相容性，因此防火牆可能會發生資料包丟棄。

問答

在本節中，「路由器」指的是CSR這樣的Cisco路由器，「防火牆」指運行ASA或FTD的Cisco防火牆。

1.Q:防火牆是否自動為PIM SSM保留232.0.0.0/8?

A:會。與CSR之類的路由器不同，不需要特定的配置。在路由器上，PIM SSM範圍需要顯式配置：

<#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 「Other drops」計數器是否特定於防火牆？

A:不能。具有多點傳送路由的Cisco路由器上存在類似的計數器。

3.Q:其它裝置（例如路由器代替防火牆）是否也會丟棄傳送到組232.4.4.4的資料包？

A:這取決於路由器如何處理地址232.4.4.4。與防火牆不同，預設情況下，路由器不為PIM SSM保留範圍232.0.0.0/8。但是，如果同時啟用了PIM SSM和BIDIR-PIM，並且路由器是BIDIR-PIM感知RP或接收具有Bidir標誌的RP到組對映並接收傳送到PIM SSM範圍的組播資料包，則資料包將被丟棄，MFIB「Other」計數器增加：

<#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
```

請注意，與路由器上具有遞增「Other drops」計數器的防火牆不同，遞增計數器為「RPF failed」。

4.Q:如何強制防火牆將來自PIM SSM範圍的組作為非SSM組地址進行處理？

A:確保RP通告特定於232.0.0.0/8（更長字首）的組的RP到組對映，或者在防火牆上為特定組手動配置RP地址。

選項1.RP上的配置：

<#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
```

在防火牆上驗證：

<#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
```

選項2.防火牆上的配置：

<#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
```

請注意，存取清單不得使用遮罩為255.255.255的主機專案或專案。

5.Q:如果防火牆將來自PIM SSM範圍的組作為非SSM組地址處理，會發生什麼情況？

A:假設組232.4.4.4作為非SSM地址處理（請參閱問題4）：

```
<#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
```

如果軟體版本受到思科錯誤ID CSCwt9960影響，則(*, G)mroute遺失，且多點傳播流量受速率限制，約為每秒50個封包。當超出點數速率限制（點數速率限制）ASP丟棄原因時，會丟棄過多的資料包：

```
<#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/
…
```

如需更多資訊，請參閱Cisco錯誤ID CSCwt9960。

相關內容

- 來源特定多點傳送區塊
- 思科錯誤ID CSCwt99960

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。