使用Bidir PIM配置对防火墙上的组播丢包进行故障排除

目录

问题

这些症状在安全防火墙威胁防御(FTD)上观察到，该威胁防御使用双向协议独立组播（BIDIR-PIM，PIM-SM的变体）作为中间跳加入组播路由域。

1.不存在特定组播组232.4.4.4的mroute:

<#root>

device#

show mroute 232.4.4.4

No mroute entries found.

2. show mfib count命令输出中的232.0.0.0/8组范围的Other drops计数器增加：

<#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.组播数据包在加速安全路径(ASP)中因超过Punt速率限制(punt-rate-limit)丢弃原因而被丢弃。 丢包计数器持续增加：

<#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.外部接口捕获不显示任何出口组播数据包：

<#root>

```
device#

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


device#

show cap capo



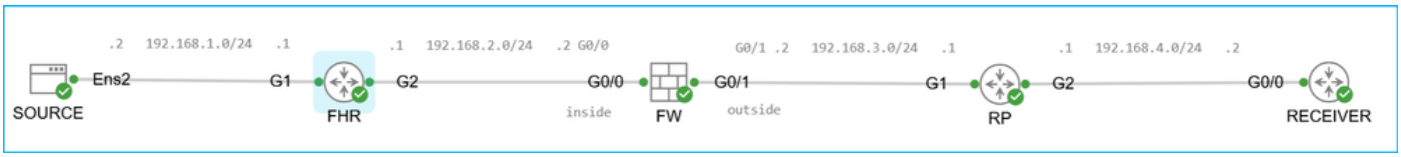
0 packet captured



0 packet shown
```

环境

拓扑



拓扑.png

要点

- 组播域中的对等体使用BIDIR-PIM。
- 本文中的路由器是指Cisco路由器，例如CSR或ASR。
- Rendezvous Point(RP)是运行Cisco IOS XE软件版本17.09.08的ASR1001-X。其他平台和软件版本也会受到影响。

- 第一跳路由器(FHR)是运行Cisco IOS XE软件版本16.12.04的C9200L-48T-4G。其他平台和软件版本也可能受到影响。
- 使用PIM引导路由器(BSR)在组播域中动态传播整个组播范围224.0.0.0/8的Loopback0接口上的交汇点(RP)地址10.4.4.4。 使用静态PIM RP地址配置的部署也会受到影响。

  RP上的PIM配置：

  ```
  <#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
  ```

- 为简单起见，在本例中，RP显示为已连接到接收器，即它也是最后一跳路由器(LHR)。 此操作为可选操作。
- 防火墙是运行版本7.6.4的安全防火墙3110。其他防火墙平台、软件版本和自适应安全设备(ASA)软件也可能会受到影响。
- 在防火墙上，组播路由已启用，而且第一跳路由器(FHR)和RP具有PIM BIDIR功能的PIM邻接关系：

  ```
  <#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
```

- 在防火墙上，尽管使用PIM BSR，但PIM RP地址10.4.4.4是手动配置的。这是冗余配置。因此，组224.0.0.0/4与RP地址10.4.4.4之间存在2个RP到组的映射：

```
<#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
```

分辨率

在继续操作之前，请务必查看下一个原因部分。

由于预期配置(BIDIR-PIM)和需要使用PIM SSM处理的流量之间不兼容，防火墙上可能会出现数据包丢弃。

如果预期配置是BIDIR-PIM，请考虑以下选项：

- 仅使用非PIM SSM组。
- 如果必须使用PIM SSM组，请确保防火墙将PIM SSM范围内的组播组作为非SSM组地址处理。有关详细信息，请参阅问答部分。
- 考虑思科漏洞ID CSCwt9960。

原因

地址232.4.4.4属于互联网编号指派机构(IANA)保留的源特定组播(SSM)组范围。 防火墙自动为PIM SSM保留232.0.0.0/8范围：

<#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的主要方面：

- 它构建基于源的树并使用(S， G)路由。
- 不需要基于RP的PIM-SM协议的共享树基础设施。换句话说，不使用RP或(*, G)路由。
- 接收方通常使用互联网组管理协议第3版(IGMPv3)加入组播树，并附带“源过滤”，即系统能够报告只从特定源地址接收数据包，或者只从特定源地址接收发送到特定组播地址的数据包。

BIDIR-PIM的主要方面：

- 它构建连接组播源和接收器的双向共享树。
- 使用在组播拓扑的每个链路上运行的故障安全指定转发器(DF)选举机制构建双向树。
- 在DF的帮助下，组播数据从源本地转发到RP，从而沿着共享树转发到接收器，而不需要源特定状态。
- BIDIR-PIM不使用最短路径树(SPT)和(S， G)条目。
- BIDIR-PIM对等体使用(*, G)条目构建共享树。此特定组播组的条目必须存在于mroute表中。

通过比较PIM SSM和BIDIR-PIM的主要方面，可以看出PIM SSM和BIDIR-PIM具有互斥的功能。

在这种情况下，组播域配置为使用BIDIR-PIM，而组播组属于IANA和防火墙为PIM SSM保留的范围。由于组播域使用BIDIR-PIM，因此PIM SSM所需的(S， G)路由在防火墙上不可用。由于缺少路由，组播流量的传出/出口接口不可用。缺少出口/传出接口会导致组播转发信息库(MFIB)中的数据包丢弃。 可以使用show mfib或show mfib count命令验证丢弃：

```
<#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
```

防火墙尝试通过连接控制点(CP)来解析传出/出口接口。 这是关键的防火墙组件，主要负责管理和控制平面功能，如路由协议、管理访问、故障切换/集群管理、处理发往防火墙接口的数据包、组播或广播IP地址等。

为了避免控制点过载，防火墙具有内置保护机制。例如，防火墙会限制从数据平面(DP)发送到控制点的数据包的速率。超过速率的数据包将被丢弃，同时超过punt rate limit(punt-rate-limit)ASP丢弃原因。可在show asp event dp-cp punt的输出中验证该传送速率 | 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
```

总之，结论是，由于预期配置(BIDIR-PIM)和需要使用PIM SSM处理的流量之间不兼容，防火墙上可能会出现丢包现象。

问题解答

在本节中，路由器指的是CSR等思科路由器，防火墙指运行ASA或FTD的思科防火墙。

问:防火墙是否自动为PIM SSM保留232.0.0.0/8?

A：Yes.与CSR等路由器不同，不需要特定的配置。在路由器上，PIM SSM范围需要显式配置：

```
<#root>
device(config)#
ip pim ssm ?

  default  Use 232/8 group range for SSM

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

问:MFIB Other drops计数器是否特定于防火墙？

A：否。具有组播路由的Cisco路由器上存在类似的计数器。

问:其它设备（例如路由器代替防火墙）是否也会丢弃发送到组232.4.4.4的数据包？

A：这取决于路由器如何处理地址232.4.4.4。与防火墙不同，默认情况下，路由器不为PIM SSM保留范围232.0.0.0/8。但是，如果同时启用PIM SSM和BIDIR-PIM，并且路由器为BIDIR-PIM感知

RP或接收带有Bidir标志的RP到组的映射，并接收发送到PIM SSM范围的组播数据包，则数据包将被丢弃，MFIB“Other”计数器增加：

<#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
```

请注意，与路由器上计数器增加“Other drops”的防火墙不同，计数器增加“RPF failed”。

问:如何强制防火墙将来自PIM SSM范围的组作为非SSM组地址进行处理？

A：确保RP通告比232.0.0.0/8（更长的前缀）更具体的组的RP到组的映射，或者在防火墙上为特定组手动配置RP地址。

选项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

防火墙验证：

<#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

选项2.防火墙配置：

<#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
```

请注意，访问列表不得使用掩码为255.255.255.255的主机条目。

问:如果防火墙将来自PIM SSM范围的组作为非SSM组地址处理，会发生什么情况？

A：假设组232.4.4.4作为非SSM地址处理（请参阅问题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
```

如果软件版本受Cisco Bug ID CSCwt9960影响，则缺少(*, G)mroute，并且组播流量受速率限制，每秒大约50个数据包。超出的数据包被丢弃，同时超出了punt rate limit(punt-rate-limit)ASP丢弃原因：

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

有关详细信息，请参阅Cisco Bug ID CSCwt9960。

相关内容

- 源特定组播块
- Cisco Bug ID CSCwt99960

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）。