Troubleshoot Multicast Packet Drops on Firewall with Bidir PIM Configuration

Contents

Issue

These symptoms are observed on Secure Firewall Threat Defense (FTD) that participates as an intermediary hop in then multicast routing domain with the Bidirectional Protocol Independent Multicast (BIDIR-PIM), a variant of PIM Sparse-Mode (PIM-SM).

1. The mroute for the specific multicast group 232.4.4.4 is absent:

<#root>

device#

show mroute 232.4.4.4

No mroute entries found.

2. The **Other drops** counter for the 232.0.0.0/8 group range in the output of the **show mfib count** command output increases:

<#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. Multicast packets are dropped with the **Punt rate limit exceeded (punt-rate-limit)** drop reason in the Accelerated Security Path (ASP). The drop counter continuously increases:

<#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. The outside interface captures do not show any egress multicast packets:

```
<#root>

device#
```

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

```
device#
```

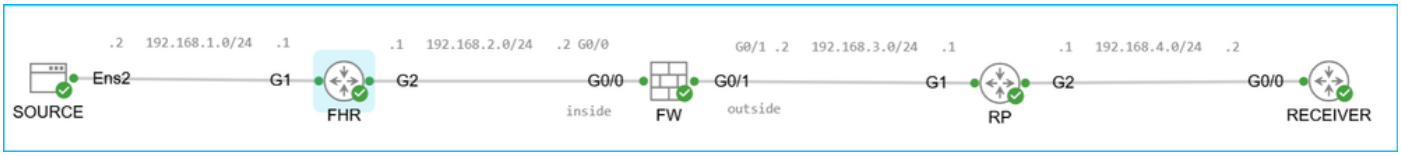
```
show cap capo
```

```
0 packet captured
```

```
0 packet shown
```

Environment

Topology



topology.png

Key Points

- The peers in the multicast domain use BIDIR-PIM.
- The router in this article refers to a Cisco router like CSR or ASR.
- Rendezvous Point (RP) is ASR1001-X running Cisco IOS XE Software, Version 17.09.08. Other platforms and software versions can also be affected.
- First Hop Router (FHR) is C9200L-48T-4G running Cisco IOS XE Software, Version 16.12.04. Other platforms and software versions can also be affected.
- Rendezvous Point (RP) address **10.4.4.4** on **Loopback0** interfacefor the entire multicast range

224.0.0.0/8 is dynamically propagated in the multicast domain using the PIM Bootstrap router (BSR). Deployments with the static PIM RP address configuration can also be affected.

PIM configuration on RP:

```
<#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
```

- For the sake of simplicity, in this case, the RP is shown as connected to the receiver, that is, it is also the last hop router (LHR). This is optional.
- The firewall is Secure Firewall 3110 running version 7.6.4. Other firewall platforms, software versions and Adaptive Security Appliance (ASA) software can also be affected.
- On the firewall, multicast routing is enabled and there is PIM adjacency with the First Hop Router (FHR) and RP with the PIM BIDIR capability:

```
<#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
```

- On the firewall, despite using PIM BSR the PIM RP address 10.4.4.4 is manually configured. This is a redundant configuration. As a result, there are 2 RP-to-group mappings between the group 224.0.0.0/4 and the RP address 10.4.4.4:

```
<#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
```

Resolution

Before proceeding, ensure to review the next *Cause* section.

The packet drops on the firewall are expected due to incompatibility between the intended configuration (BIDIR-PIM) and traffic that needs handling using PIM SSM.

If the intended configuration is BIDIR-PIM, then consider these options:

- Use only non-PIM SSM groups.
- If PIM SSM groups must be used, then ensure the firewall handles multicast groups from the PIM SSM range as non-SSM group addresses. Refer to the Q&A section for more information.
- Consider Cisco bug ID CSCwt99960.

Cause

The address 232.4.4.4 belongs to the Source Specific Multicast (SSM) group range reserved by the Internet Assigned Numbers Authority (IANA). The firewall automatically reserves the **232.0.0.0/8** range for PIM SSM:

<#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
```

Key aspects of PIM SSM:

- It builds source-based trees and uses (S, G) mroutes.
- RP-based shared tree infrastructure of PIM-SM protocol is not required. In other words, RP or (*, G) mroutes are not used.

- Receivers typically join the multicast tree by using the Internet Group Management Protocol Version 3 (IGMPv3) with "source filtering", that is, the ability for a system to report interest in receiving packets only from specific source addresses, or from all but specific source addresses, sent to a particular multicast address.

Key aspects of BIDIR-PIM:

- It builds bidirectional shared trees connecting multicast sources and receivers.
- Bidirectional trees are built using a fail-safe Designated Forwarder (DF) election mechanism operating on each link of a multicast topology.
- With the assistance of the DF, multicast data is natively forwarded from sources to the RP and hence along the shared tree to receivers without requiring source-specific state.
- BIDIR-PIM does not use Shortest Path Trees (SPT) and (S, G) entries.
- BIDIR-PIM peers build shared trees using (*, G) entries. This entry for a particular multicast group must exist in the mroute table.

Contrasting the key aspects of PIM SSM and BIDIR-PIM shows that PIM SSM and BIDIR-PIM have mutually exclusive functionality.

In this case, the multicast domain is configured to use BIDIR-PIM, while the multicast group belongs to the range reserved by IANA and the firewall for PIM SSM. Since the multicast domain is using BIDIR-PIM, (S, G) mroutes required for PIM SSM are unavailable on the firewall. Due to lack of mroutes, the outgoing/egress interface for the multicast traffic are not available. The absence of egress/outgoing interface results in packet drops in the multicast forwarding information base (MFIB). The drops can be verified using the **show mfib** or **show mfib count** commands:

<#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
```

The firewall attempts to resolve the outgoing/egress interface by engaging the **control point** (CP). This is the critical firewall component mainly responsible for management and control plane functions, like routing protocols, management access, failover/cluster management, handling packets destined to the firewall interface, multicast or broadcast IP addresses, and so on.

To avoid overloading the control point, the firewall has built-in protection mechanisms. For example, firewall limits the rate of packets sent from the data plane (DP) to the control point. Packet exceeding the rate are dropped with the **punt rate limit exceeded (punt-rate-limit)** ASP drop reason. The punt rate can be verified in the output of the **show asp event dp-cp punt | begin EVENT-TYPE** command:

```
<#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
```

To summarize, the conclusion is that packet drops on the firewall are expected due to incompatibility

between the intended configuration (BIDIR-PIM) and traffic that needs handling using PIM SSM.

Q&A

In this section, router refers to a Cisco router like CSR and firewall refers to Cisco firewalls running ASA or FTD.

Q: Does the firewall automatically reserve 232.0.0.0/8 for PIM SSM?

A: Yes. Unlike, for example, routers like CSR, no specific configuration is required. On routers, the PIM SSM range needs explicit configuration:

<#root>

```
device(config)#

ip pim ssm ?


  default  Use 232/8 group range for SSM


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

Q: Is the MFIB **Other drops** counter specific to firewall?

A: No. Similar counter exists on Cisco routers with multicast routing.

Q: Would another device like a router in place of a firewall also drop packets sent to the group 232.4.4.4?

A: It depends on how the router treats the address 232.4.4.4. Unlike firewalls, by default routers do not reserve the range 232.0.0.0/8 for PIM SSM. However, if both PIM SSM and BIDIR-PIM are enabled, and the router is either BIDIR-PIM aware RP or receives RP-to-group mapping with the Bidir flag and receives multicast packets sent to the PIM SSM range, the packets are dropped and the MFIB "Other” counter increases:

<#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
```

Note that the unlike the firewall with the increasing “Other drops” counter on the router the increasing counter is “RPF failed”.

Q: How to force firewalls to handle a group from the PIM SSM range as a non-SSM group address?

A: Ensure that either RP advertises RP-to-group mapping for groups that are more specific than 232.0.0.0/8 (longer prefix) or on the firewall manually configure RP address for specific groups.

Option 1. Configuration on RP:

<#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
```

Verification on firewall:

```
<#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
```

Option 2. Configuration on firewall:

```
<#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
```

Note that the access-list must not use host entries or entries with the mask 255.255.255.255.

Q: What happens if the firewall handles a group from the PIM SSM range as a non-SSM group address?

A: Assume that group 232.4.4.4 is handled as a non-SSM address (refer to question 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
```

If the software version is affected by Cisco bug ID CSCwt99960, the (*, G) mroute is missing, and the multicast flow is rate-limited at around 50 packets per second rate. Excessive packets are dropped with the punt rate limit exceeded (punt-rate-limit) ASP drop reason:

```
<#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
…
```

For more information, refer to the Cisco bug ID CSCwt99960.

Related Content

- Source-Specific Multicast Block
- Cisco bug ID CSCwt99960