Troubleshoot Multicast Packet Drop Via Bridge Members Without BVI nameif

Contents

Issue

Multicast packets through bridge group member interfaces are dropped on the firewall with these symptoms:

1. The multicast packets do not leave the intended egress interface:

<#root>

```
firewall#

show bridge-group


Static mac-address entries:  0 (in use), 16384 (max)
Dynamic mac-address entries: 2 (in use), 16384 (max)


 Bridge Group: 100


 Interfaces:

 GigabitEthernet0/2



 GigabitEthernet0/3



firewall#

show nameif


Interface               Name                    Security
..

GigabitEthernet0/2      inside                  100
```

```
GigabitEthernet0/3      outside                  0
```

```
firewall#
```

```
show capture
```

```
capture capi type raw-data trace interface inside[
```

```
Capturing - 15642 bytes
```

```
]
  match udp any host 239.1.1.1
capture capo type raw-data interface outside [
```

```
Capturing - 0 bytes
```

```
]
  match udp any host 239.1.1.1
```

2. The bytes in the output of the relevant **show conn** command output is 0:

<#root>

```
firewall#
```

```
show conn address 239.1.1.1
```

```
16 in use, 17 most used
```

```
UDP inside  192.0.2.1:50609 outside  239.1.1.1:5555, idle 0:01:03,
```

```
bytes 0
```

```
, flags -
```

3. The S,G mroute incoming interface is null:

<#root>

```
firewall#
```

```
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

(*, 239.1.1.1), 3d01h/never, RP 198.51.100.100, flags: SCJ
  Incoming interface: rp
  RPF nbr: 198.51.100.100
  Immediate Outgoing interface list:
    outside, Forward, 3d01h/never

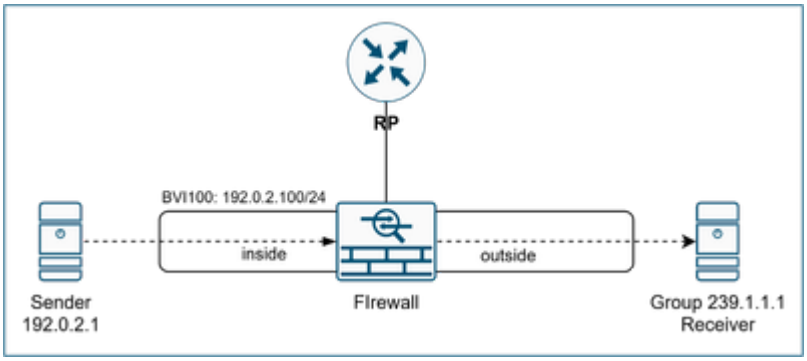
(192.0.2.1, 239.1.1.1), 00:02:48/00:00:41, flags: SJ


Incoming interface: Null


  RPF nbr: 0.0.0.0
  Inherited Outgoing interface list:
    outside, Forward, 3d01h/never
```

Environment

Topology



- Firepower 4115 running Secure Firewall Threat Defense, other hardware platforms, and Security ASA can be affected.
- FTD version 7.6.4 and other software versions can be affected.
- Multicast routing with the Protocol Independent Multicast (PIM) Sparse Mode (SM) is enabled.
- Multicast traffic path is through bridge group members.

- The bridge virtual interface (BVI) does not have nameif.

<#root>

```
firewall#

show bridge-group


Static mac-address entries:  0 (in use), 16384 (max)
Dynamic mac-address entries: 2 (in use), 16384 (max)


 Bridge Group: 100


 Interfaces:

 GigabitEthernet0/2



 GigabitEthernet0/3



firewall#

show nameif


Interface                Name                     Security
..

GigabitEthernet0/2       inside                     100



GigabitEthernet0/3       outside                  0



firewall#

show run int bvi100



interface BVI100
```

```
no nameif


security-level 0
ip address 192.0.2.100 255.255.255.0
```

Resolution

Analysis

1. The multicast forwarding information base (MFIB) **Other** drops counter increase:

<#root>

```
firewall#

show mfib 239.1.1.1


Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, K - Keepalive
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count

(*,239.1.1.1) Flags: C K
   Forwarding: 0/0/0/0, Other: 0/0/0
   rp Flags: A NS
   outside Flags: F NS
     Pkts: 0/0
(192.0.2.1,239.1.1.1) Flags: K
   Forwarding: 0/0/0/0

, Other: 2620/0/2620



   OBNS-FWinside Flags: A
   outside Flags: F NS
     Pkts: 0/0

firewall#

show mfib 239.1.1.1


…
(192.0.2.1,239.1.1.1) Flags: K
```

```
   Forwarding: 0/0/0/0,

Other: 2629/0/2629


   rp Flags: A
   outside Flags: F NS
     Pkts: 0/0
```

2. The MFIB packet debugs indicate multicast packet drops:

```
<#root>

firewall#

debug mfib pak 239.1.1.1


MFIB IPv4 pak debugging enabled
  all MFIB debugging is for 239.1.1.1

MFIB: Pkt (192.0.2.1,239.1.1.1) from inside (PS) dropping



MFIB: Pkt (192.0.2.1,239.1.1.1) from inside (PS) dropping
```

3. The **debug pim** command output shows **RPF lookup failed for root 192.0.2.1** messages**:**

```
<#root>

firewall#

debug pim



IPv4 PIM:    RPF lookup failed for root 192.0.2.1
IPv4 PIM:    RPF lookup failed for root 192.0.2.1
```

4. PIM is enabled on bridge group members:

```
<#root>

firewall#

show pim interface
```

```
Address          Interface          PIM  Nbr   Hello  DR         DR
                                         Count Intvl  Prior

239.1.1.1        inside             on   0     30     1          this system


239.1.1.1        outside            on   0     30     1          this system
```

Bridge group members must not participate in multicast routing protocols. This issue is tracked in Cisco bug ID: CSCwv23349. The workaround is to add the nameif to the BVI, then remove/re-add the bridge member interface nameif. Removal of nameifs is impactful and user discretion is advised. This change is recommended only during a controlled maintenance window.

Cause

Due to Cisco bug ID: CSCwv23349, if the BVI does not have a nameif, the bridge group members participating in multicast routing protocols (that is PIM and the Internet Group Messaging Protocol (IGMP)) are enabled on these interfaces. Activation of multicast routing protocol results in enforcement of all protocol level checks, one of which is the reverse path forwarding (RPF) check.

RPF check compares the multicast ingress interface (A) to the interface toward the multicast sender according to the unicast table (B). If the interfaces do not match, multicast packets are dropped due to RPF failure. In this case, **inside** is the ingress interface. In the routing table there is no unicast route towards the multicast sender with the IP address: 192.0.2.1.

```
<#root>

firewall#

show route 192.0.2.1


% Network not in table

firewall#

show asp table routing address 192.0.2.1


route table timestamp: 46
```

Considering bridge group members do not participate in routing, routing tables do not have routes over bridge group members. This results in RPF-check failures if bridge group members participate in routing protocols. The versions with the fix of Cisco bug ID: CSCwv23349 exempt these interfaces from multicast routing protocols.

Warning: This defect is specifically on the bridge group members participation in multicast routing protocols. It does not apply to the through-the-box multicast through the bridge group members, that is multicast connectivity between upstream/downstream devices.

Related Content

- Cisco bug ID CSCwv23349