排除通过没有BVI名称的网桥组成员的组播数据包丢弃故障

目录

问题

通过网桥组成员接口的组播数据包在防火墙上丢弃，具有以下症状：

1.组播数据包不会离开预期出口接口：

<#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.相关show conn命令输出的输出中的字节为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. S，G mroute传入接口为空：

<#root>

```
firewall#
```

show mroute

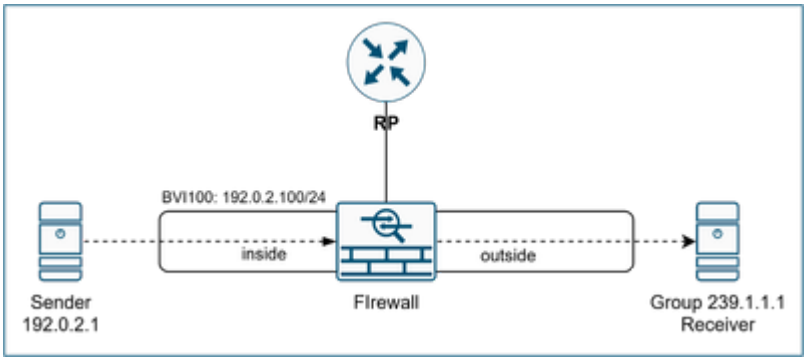
```
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, 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
```

环境

拓扑



- 运行安全防火墙威胁防御的Firepower 4115。其他硬件平台和安全ASA也会受到影响。
- FTD版本7.6.4。其它软件版本也可能会受到影响。
- 启用了协议无关组播(PIM)稀疏模式(SM)的组播路由。

- 组播流量路径通过网桥组成员。
- 网桥虚拟接口(BVI)没有名称if:

<#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
```

分辨率

分析

1.组播转发信息库(MFIB)其他丢包计数器增加：

<#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. MFIB数据包调试指示组播数据包丢弃：

<#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. debug pim命令输出显示根192.0.2.1消息的RPF查找失败:

<#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.已在网桥组成员上启用PIM:

<#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
```

网桥组成员不得参与组播路由协议。此问题在Cisco Bug ID CSCwv23349中跟踪。

解决方法是将nameif添加到BVI，然后删除/重新添加网桥成员接口的nameif。删除名称会有一定影响。建议用户自行决定，仅在受控维护窗口期间建议进行此更改。

原因

由于Cisco Bug ID CSCwv2349，如果BVI没有名称，则网桥组成员参与组播路由协议，即PIM，并且这些接口上启用了互联网组消息协议(IGMP)。激活组播路由协议会执行所有协议级别检查，其中一项是反向路径转发(RPF)检查。

RPF检查根据单播表(B)将组播入口接口(A)与指向组播发送方的接口进行比较。 如果接口不匹配，则组播数据包将由于RPF故障而被丢弃。

在本例中，inside是入口接口。在路由表中，没有指向IP地址为192.0.2.1的组播发送方的单播路由。

```
<#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
```

考虑到网桥组成员不参与路由，路由表没有网桥组成员上的路由。如果网桥组成员参与路由协议，这将导致RPF检查失败。具有思科漏洞ID CSCwv2349修复程序的版本免除这些接口使用组播路由协议。

警告：此缺陷专门针对网桥组成员参与组播路由协议。它不适用于通过网桥组成员的通过设备组的多播，即上游/下游设备之间的组播连接。

相关内容

- Cisco Bug ID CSCwv23349

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）。