對沒有BVI名稱的網橋組成員進行組播資料包丟棄故障排除

目錄

問題

透過橋接群組成員介面的多點傳播封包會在防火牆上遭捨棄，且出現以下症狀：

1.多點傳送封包不會離開所需的輸出介面：

<#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.相關show conn命令輸出的輸出中的位元組為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傳入介面為空：

```
<#root>

firewall#
```

show mroute

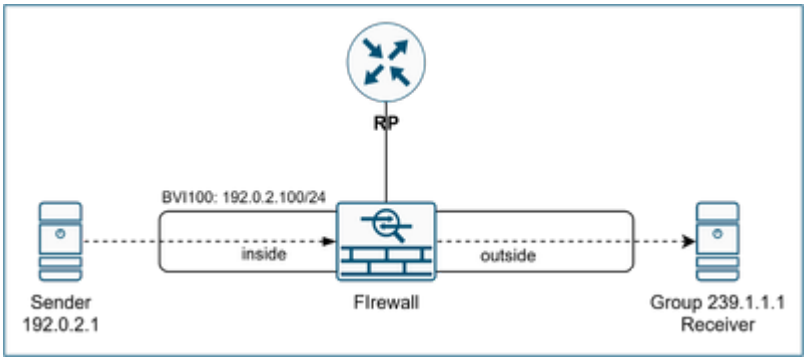
```
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface,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

環境

拓撲



- 運行安全防火牆威脅防禦的Firepower 4115。其他硬體平台和安全ASA也會受到影響。
- FTD 7.6.4版。其他軟體版本也可能受影響。
- 已啟用使用通訊協定無關多點傳送(PIM)稀疏模式(SM)的多點傳送路由。

- 組播流量路徑通過網橋組成員。
- 橋接器虛擬介面(BVI)沒有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
```

解析

分析

1.組播轉發資訊庫(MFIB)其他丟包計數器增加：

<#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資料包調試指示組播資料包丟棄：

<#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命令輸出顯示根192.0.2.1 消息的RPF查詢失敗:

<#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.已在網橋組成員上啟用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
```

網橋組成員不得參與組播路由協定。此問題會在思科錯誤ID CSCwv2349中追蹤。

解決方法是將nameif新增到BVI，然後刪除/重新新增橋接成員介面nameif。刪除名稱會產生影響。建議使用者自行決定，僅建議在受控維護期間更改此設定。

原因

由於Cisco錯誤ID CSCwv2349，如果BVI沒有nameif，則網橋組成員參與組播路由協定，即PIM，並且這些介面上啟用了網際網路組消息協定(IGMP)。啟用組播路由協定會執行所有協定級別檢查，其中一項是反向路徑轉發(RPF)檢查。

RPF檢查根據單播表(B)，將多播入口介面(A)與朝向多播傳送方的介面進行比較。 如果介面不匹配，組播資料包將因RPF故障而丟棄。

在這種情況下，inside是輸入介面。在路由表中，沒有指向IP地址為192.0.2.1的組播傳送方的單播路由。

```
<#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
```

考慮到網橋組成員不參與路由，路由表沒有經過網橋組成員的路由。如果網橋組成員參與路由協定，這將導致RPF檢查失敗。修正了Cisco錯誤ID CSCwv2349的版本免除這些介面使用多點傳送路由通訊協定。

警告：此缺陷專門針對網橋組成員參與組播路由協定。它不適用於通過網橋組成員的直插式組播，即上游/下游裝置之間的組播連線。

相關內容

- 思科錯誤ID CSCwv23349

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）。