BVI 이름 없이 브리지 그룹 구성원을 통한 멀티캐스트 패킷 삭제 문제 해결if

목차

문제

브리지 그룹 멤버 인터페이스를 통한 멀티캐스트 패킷은 다음과 같은 증상으로 방화벽에서 삭제됩니다.

1. 멀티캐스트 패킷이 의도한 이그레스 인터페이스를 벗어나지 않습니다.

<#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. 관련 show conn 명령 출력의 바이트는 0입니다.

<#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 수신 인터페이스가 Null입니다.

<#root>

```
firewall#
```

show mroute

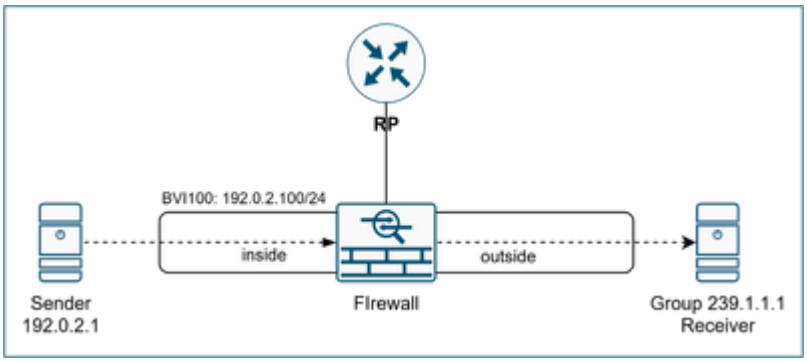
```
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface,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

환경

토폴로지



- Firepower 4115 보안 방화벽 위협 방어. 다른 하드웨어 플랫폼과 보안 ASA도 영향을 받을 수 있습니다.

- FTD 버전 7.6.4. 다른 소프트웨어 버전도 영향을 받을 수 있습니다.
- PIM(Protocol Independent Multicast) SM(Sparse Mode)을 사용하는 멀티캐스트 라우팅이 활성화됩니다.
- 멀티캐스트 트래픽 경로는 브리지 그룹 멤버를 통해 전달됩니다.
- BVI(Bridge Virtual Interface)에는 다음과 같은 이름이 없습니다.

<#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

해결

분석

1. MFIB(Multicast Forwarding Information Base) Other drops 카운터 증가:

<#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 패킷 디버깅은 멀티캐스트 패킷 삭제를 나타냅니다.

<#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 명령 출력에서는 루트 192.0.2.1 메시지에 대한 RPF 조회가 실패했음을 표시합니다.

<#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. PIM이 브리지 그룹 멤버에서 활성화됩니다.

<#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
```

브리지 그룹 멤버는 멀티캐스트 라우팅 프로토콜에 참여할 수 없습니다. 이 문제는 Cisco 버그 ID CSCwv23349에서 추적됩니다.

해결 방법은 nameif를 BVI에 추가한 다음 브리지 멤버 인터페이스 nameif를 제거/다시 추가하는 것입니다. nameifs를 제거하면 영향이 큽니다. 사용자 재량이 권장되며, 이러한 변경은 제어된 유지 관리 기간 동안에만 권장됩니다.

원인

Cisco 버그 ID CSCwv23349로 인해 BVI에 nameif가 없을 경우 브리지 그룹 멤버가 멀티캐스트 라우팅 프로토콜에 참여합니다. 즉, PIM과 IGMP(Internet Group Messaging Protocol)가 이 인터페이스에서 활성화됩니다. 멀티캐스트 라우팅 프로토콜을 활성화하면 모든 프로토콜 레벨 검사가 시행되며, 그중 하나가 RPF(Reverse Path Forwarding) 검사입니다.

RPF 검사는 유니캐스트 테이블(B)에 따라 멀티캐스트 인그레스 인터페이스(A)와 멀티캐스트 발신자를 향하는 인터페이스를 비교합니다. 인터페이스가 일치하지 않으면 RPF 실패로 인해 멀티캐스트 패킷이 삭제됩니다.

이 경우 내부는 인그레스 인터페이스입니다. 라우팅 테이블에는 IP 주소가 192.0.2.1인 멀티캐스트

발신자를 향하는 유니캐스트 경로가 없습니다.

```
<#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
```

브리지 그룹 멤버가 라우팅에 참여하지 않는다는 점을 고려하면 라우팅 테이블에는 브리지 그룹 멤버에 대한 경로가 없습니다. 브리지 그룹 멤버가 라우팅 프로토콜에 참여하는 경우 RPF 검사 오류가 발생합니다. Cisco 버그 ID CSCwv23349가 수정된 버전은 이러한 인터페이스를 멀티캐스트 라우팅 프로토콜에서 제외합니다.

경고: 이 결함은 특히 브리지 그룹 멤버가 멀티캐스트 라우팅 프로토콜에 참여하는 것에 관한 것입니다. 브리지 그룹 멤버를 통한 through-the-box 멀티캐스트, 즉 업스트림/다운스트림 디바이스 간의 멀티캐스트 연결에는 적용되지 않습니다.

관련 콘텐츠

- Cisco 버그 ID CSCwv23349

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.