Bidir PIM 컨피그레이션으로 방화벽의 멀티캐스트 패킷 삭제 문제 해결

목차

문제

이러한 증상은 PIM-SM(Sparse-Mode)의 변형인 BIDIR-PIM(Bidirectional Protocol Independent Multicast)을 사용하는 멀티캐스트 라우팅 도메인에서 중간 홉으로 참여하는 FTD(Secure Firewall Threat Defense)에서 관찰됩니다.

1. 특정 멀티캐스트 그룹 232.4.4.4에 대한 mroute가 없습니다.

<#root>

device#

show mroute 232.4.4.4

No mroute entries found.

2. show mfib count 명령 출력의 232.0.0.0/8 그룹 범위에 대한 "Other drops" 카운터가 증가합니다.

<#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. ASP(Accelerated Security Path)에서 Punt rate limit exceeded(punt-rate-limit) drop reason으로 멀티캐스트 패킷이 삭제됩니다. 삭제 카운터가 계속 증가합니다.

<#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. 외부 인터페이스 캡처에는 이그레스 멀티캐스트 패킷이 표시되지 않습니다.

<#root>

device#

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

device#

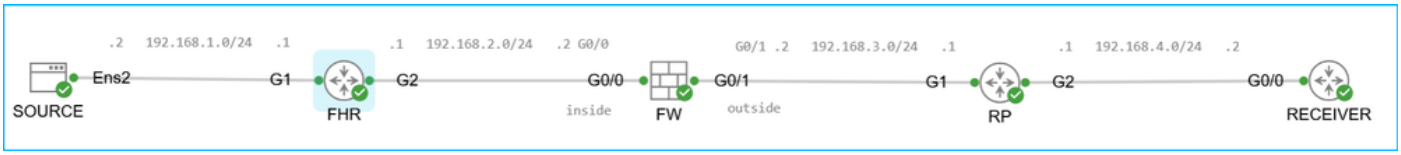
show cap capo

0 packet captured

0 packet shown

환경

토폴로지:



토폴로지.png

요점:

- 멀티캐스트 도메인의 피어는 BIDIR-PIM을 사용합니다.
- 이 문서의 "라우터"는 CSR 또는 ASR과 같은 Cisco 라우터를 가리킵니다.
- RP(Rendezvous Point)는 Cisco IOS XE Software, 버전 17.09.08을 실행하는 ASR1001-X입니다. 다른 플랫폼 및 소프트웨어 버전도 영향을 받을 수 있습니다.

- FHR(First Hop Router)은 Cisco IOS XE Software, 버전 16.12.04를 실행하는 C9200L-48T-4G입니다. 다른 플랫폼 및 소프트웨어 버전도 영향을 받을 수 있습니다.
- 전체 멀티캐스트 범위 224.0.0.0/8의 Loopback0 인터페이스에 있는 RP(Rendezvous Point) 주소 10.4.4.4는 PIM BSR(Bootstrap Router)을 사용하여 멀티캐스트 도메인에서 동적으로 전파됩니다. 고정 PIM RP 주소 컨피그레이션을 사용하는 구축도 영향을 받을 수 있습니다.

  RP의 PIM 구성:

```
<#root>

device#

show run interface loopback0


interface Loopback0
 description LO0
 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
```

- 간소화를 위해 이 경우 RP는 수신기에 연결된 것으로 표시됩니다. 즉, LHR(Last Hop Router)이기도 합니다. 이는 선택 사항입니다.
- 방화벽은 Secure Firewall 3110(버전 7.6.4)입니다. 다른 방화벽 플랫폼, 소프트웨어 버전 및 ASA(Adaptive Security Appliance) 소프트웨어도 영향을 받을 수 있습니다.
- 방화벽에서 멀티캐스트 라우팅이 활성화되어 있으며 FHR(First Hop Router)의 PIM 인접성과 PIM BIDIR 기능의 RP가 있습니다.

```
<#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
```

- 방화벽에서는 PIM BSR을 사용하더라도 PIM RP 주소 10.4.4.4가 수동으로 구성됩니다. 이는 중복 컨피그레이션입니다. 그 결과, 그룹 224.0.0.0/4과 RP 주소 10.4.4.4 사이에는 2개의 RP-to-group 매핑이 있습니다.

```
<#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
```

해결

계속하기 전에 Cause(원인) 섹션을 검토하십시오.

의도한 컨피그레이션(BIDIR-PIM)과 PIM SSM을 사용하여 처리해야 하는 트래픽 간의 비호환성으로 인해 방화벽의 패킷 드랍이 예상됩니다.

원하는 컨피그레이션이 BIDIR-PIM인 경우 다음 옵션을 고려하십시오.

- 비 PIM SSM 그룹만 사용합니다.
- PIM SSM 그룹을 사용해야 하는 경우 방화벽에서 PIM SSM 범위의 멀티캐스트 그룹을 비 SSM 그룹 주소로 처리하는지 확인합니다. 자세한 내용은 Q&A 섹션을 참조하십시오.
- Cisco 버그 ID CSCwt99960을 고려하십시오.

원인

주소 232.4.4.4는 IANA(Internet Assigned Numbers Authority)에서 예약한 SSM(Source Specific Multicast) 그룹 범위에 속합니다. 방화벽은 PIM SSM에 대해 232.0.0.0/8 범위를 자동으로 예약합니다.

<#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
```

PIM SSM의 주요 내용:

- 소스 기반 트리를 구축하고 (S, G) mroute를 사용합니다.
- PIM-SM 프로토콜의 RP 기반 공유 트리 인프라는 필요하지 않습니다. 즉, RP 또는 (*, G) 경로는 사용되지 않습니다.
- 수신자는 일반적으로 IGMPv3(Internet Group Management Protocol Version 3)를 "소스 필터링"으로 사용하여 멀티캐스트 트리에 조인합니다. 즉, 특정 소스 주소 또는 특정 소스 주소를 제외한 모든 주소에서 특정 멀티캐스트 주소로 전송된 패킷만 수신할 때 시스템에서 관심을 보고할 수 있습니다.

BIDIR-PIM의 주요 내용:

- 멀티캐스트 소스와 수신자를 연결하는 양방향 공유 트리를 구축합니다.
- 양방향 트리는 멀티캐스트 토폴로지의 각 링크에서 작동하는 DF(Fail-Safe Designated Forwarder) 선택 메커니즘을 사용하여 구축됩니다.
- DF의 지원을 받으면 멀티캐스트 데이터가 소스에서 RP로 전달되고 따라서 소스별 상태 없이 공유 트리를 따라 수신자에게 전달됩니다.
- BIDIR-PIM은 SPT(Shortest Path Tree) 및 (S, G) 항목을 사용하지 않습니다.
- BIDIR-PIM 피어는 (*, G) 항목을 사용하여 공유 트리를 구축합니다. 특정 멀티캐스트 그룹에 대한 이 항목은 mroute 테이블에 있어야 합니다.

PIM SSM과 BIDIR-PIM의 주요 특징과 대조하면 PIM SSM과 BIDIR-PIM은 함께 사용할 수 없는 기능을 가지고 있습니다.

이 경우 멀티캐스트 그룹이 IANA 및 PIM SSM용 방화벽에서 예약한 범위에 속하는 동안 멀티캐스트 도메인이 BIDIR-PIM을 사용하도록 구성됩니다. 멀티캐스트 도메인이 BIDIR-PIM을 사용하므로 방화벽에서는 PIM SSM에 필요한 (S, G) 경로를 사용할 수 없습니다. 경로 부족으로 인해 멀티캐스트 트래픽의 발신/이그레스 인터페이스를 사용할 수 없습니다. 이그레스/발신 인터페이스가 없으면 MFIB(Multicast Forwarding Information Base)에서 패킷이 삭제됩니다. drop은 show mfib 또는 show mfib count 명령을 사용하여 확인할 수 있습니다.

<#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
```

방화벽은 CP(제어 포인트)에 연결하여 발신/이그레스 인터페이스를 확인하려고 시도합니다. 이는 라우팅 프로토콜, 관리 액세스, 장애 조치/클러스터 관리, 방화벽 인터페이스로 향하는 패킷 처리, 멀티캐스트 또는 브로드캐스트 IP 주소 등과 같은 관리 및 컨트롤 플레인 기능을 주로 담당하는 중요한 방화벽 구성 요소입니다.

제어 지점의 과부하를 방지하기 위해 방화벽에는 보호 메커니즘이 내장되어 있습니다. 예를 들어, 방화벽은 데이터 플레인(DP)에서 제어 지점으로 전송되는 패킷의 속도를 제한합니다. 속도를 초과하는 패킷은 punt rate limit exceeded(punt-rate-limit) ASP 삭제 이유와 함께 삭제됩니다. punt rate는 show asp event dp-cp punt의 출력에서 확인할 수 있습니다 | begin EVENT-TYPE 명령:

<#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
```

요약하자면, 방화벽의 패킷 삭제는 의도한 컨피그레이션(BIDIR-PIM)과 PIM SSM을 사용하여 처리해야 하는 트래픽 간의 비호환성으로 인해 발생할 것으로 예상됩니다.

질문과 대답

이 섹션에서 "라우터"는 CSR과 같은 Cisco 라우터를 의미하며 "방화벽"은 ASA 또는 FTD를 실행하는 Cisco 방화벽을 의미합니다.

1. Q: 방화벽은 PIM SSM에 대해 232.0.0.0/8을 자동으로 예약합니까?

A : 예. 예를 들어, CSR과 같은 라우터와 달리 특정 컨피그레이션이 필요하지 않습니다. 라우터에서 PIM SSM 범위에는 다음과 같은 명시적 컨피그레이션이 필요합니다.

<#root>

```
device(config)#

ip pim ssm ?



  default  Use 232/8 group range for SSM



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

2. Q: MFIB "Other drops" 카운터는 방화벽에만 해당됩니까?

A : 아니요. 멀티캐스트 라우팅이 있는 Cisco 라우터에도 유사한 카운터가 있습니다.

3. Q: 방화벽 대신 라우터 같은 다른 디바이스에서도 그룹 232.4.4.4로 전송된 패킷을 삭제할까요?

A : 라우터가 주소 232.4.4.4를 처리하는 방식에 따라 다릅니다. 방화벽과 달리 기본적으로 라우터는 PIM SSM에 대해 232.0.0.0/8 범위를 예약하지 않습니다. 그러나 PIM SSM과 BIDIR-PIM이 모두 활성화되어 있고 라우터가 BIDIR-PIM 인식 RP이거나 Bidir 플래그가 있는 RP-to-group 매핑을 수신하고 PIM SSM 범위로 전송된 멀티캐스트 패킷을 수신하면 패킷이 삭제되고 MFIB "Other" 카운터가 증가합니다.

<#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
```

라우터에서 "Other drops" 카운터가 증가하는 방화벽과 달리, 증가 카운터는 "RPF failed"입니다.

4. Q: PIM SSM 범위의 그룹을 비 SSM 그룹 주소로 처리하도록 방화벽을 강제하는 방법

A : RP에서 232.0.0.0/8(더 긴 접두사)보다 더 구체적인 그룹에 RP-to-group 매핑을 광고하거나 방화벽에서 특정 그룹에 대한 RP 주소를 수동으로 구성하는지 확인합니다.

옵션 1. RP의 구성:

<#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
```

방화벽에서 확인:

<#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
```

옵션 2. 방화벽의 구성:

<#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

access-list는 호스트 항목 또는 마스크 255.255.255.255의 항목을 사용하지 않아야 합니다.

5. Q: 방화벽이 PIM SSM 범위의 그룹을 비 SSM 그룹 주소로 처리하는 경우 어떻게 됩니까?

A : 그룹 232.4.4.4가 비 SSM 주소로 처리된다고 가정합니다(질문 4 참조).

<#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
```

소프트웨어 버전이 Cisco 버그 ID CSCwt99960의 영향을 받는 경우 (*, G) 경로가 없고 멀티캐스트 플로우가 초당 50패킷 정도로 속도 제한됩니다. punt rate limit(punt-rate-limit) 초과 ASP 삭제 사유와 함께 과도한 패킷이 삭제됩니다.

<#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 (N/
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (N/
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (N/
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (N/
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (N/
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (N/
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (N/
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (N/
…
```

자세한 내용은 Cisco 버그 ID CSCwt99960을 참조하십시오.

관련 콘텐츠

- 소스별 멀티캐스트 블록
- Cisco 버그 ID CSCwt99960

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.