

firepower 위협 방어 및 ASA Multicast PIM 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[멀티캐스트 라우팅 기본 사항](#)

[약어/약어](#)

[작업 1 - PIM 스페스 모드\(고정 RP\)](#)

[작업 2 - PIM BSR\(부트스트랩 라우터\) 구성](#)

[문제 해결 방법론](#)

[PIM 트러블슈팅 명령\(치트 시트\)](#)

[알려진 문제](#)

[vPC Nexus에서 PIM이 지원되지 않음](#)

[대상 영역이 지원되지 않습니다.](#)

[방화벽은 HSRP로 인해 업스트림 라우터로 메시지를 PIM하지 않음](#)

[LAN 세그먼트의 DR이 아닌 방화벽은 LHR로 간주되지 않음](#)

[역방향 경로 전달 확인 실패로 인해 방화벽에서 멀티캐스트 패킷 삭제](#)

[방화벽은 소스 트리로의 PIM 전환 시 PIM 조인을 생성하지 않습니다.](#)

[Punt rate Limit으로 인해 방화벽에서 처음 몇 개의 패킷 삭제](#)

[ICMP 멀티캐스트 트래픽 필터링](#)

[알려진 PIM 멀티캐스트 결함](#)

[관련 정보](#)

소개

이 문서에서는 FTD(Firepower Threat Defense) 및 ASA(Adaptive Security Appliance)가 PIM(Protocol Independent Multicast)을 구현하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

기본 IP 라우팅 지식

사용되는 구성 요소

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Firepower 4125 Threat Defense 버전 7.1.0.
- FMC(firepower 관리 센터) 버전 7.1.0.
- Cisco Adaptive Security Appliance 소프트웨어 버전 9.17(1)9.

배경 정보

멀티캐스트 라우팅 기본 사항

- 유니캐스트는 패킷을 목적지로 전달하고, 멀티캐스트는 패킷을 소스에서 멀리 전달합니다.
- 멀티캐스트 네트워크 디바이스(방화벽/라우터 등)는 RPF(Reverse Path Forwarding)를 통해 패킷을 전달합니다. RPF는 특정 유형의 공격을 방지하기 위해 유니캐스트에서 사용되는 uRPF와 동일하지 않습니다. RPF는 멀티캐스트 수신자를 향하는 인터페이스에서 멀티캐스트 패킷을 소스에서 멀리 전달하는 메커니즘으로 정의할 수 있습니다. 기본 역할은 트래픽 루프를 방지하고 올바른 트래픽 경로를 확인하는 것입니다.
- PIM과 같은 멀티캐스트 프로토콜에는 3가지 주요 기능이 있습니다.
 1. 업스트림 인터페이스(소스에 가장 가까운 인터페이스)를 찾습니다.
 2. 특정 멀티캐스트 스트림과 연결된 다운스트림 인터페이스(수신자를 향한 인터페이스)를 찾습니다.
 3. 멀티캐스트 트리를 유지 관리합니다(트리 분기 추가 또는 제거).
- 멀티캐스트 트리는 암시적 조인(flood-and-prune) 또는 명시적 조인(pull model)의 두 가지 방법 중 하나로 구축 및 유지 관리할 수 있습니다. PIM Dense Mode(PIM-DM)에서는 암시적 조인을 사용하는 반면 PIM Sparse Mode(PIM-SM)에서는 명시적 조인을 사용합니다.
- 멀티캐스트 트리는 공유 또는 소스 기반일 수 있습니다.
 - 공유 트리는 RP(Rendezvous Point) 개념을 사용하며 (*, G)로 표시됩니다. 여기서 G는 멀티캐스트 그룹 IP입니다.
 - 소스 기반 트리는 소스에 뿌리를 두고 RP를 사용하지 않으며 (S, G)로 표시됩니다. 여기서 S는 멀티캐스트 소스/서버의 IP입니다.
- 멀티캐스트 포워딩 모델:
 - ASM(Any-Source Multicast) 전달 모드는 모든 소스에서 멀티캐스트 스트림을 전송할 수 있는 공유 트리(*, G)를 사용합니다.
 - SSM(Source-Specific Multicast)은 소스 기반 트리(S, G) 및 IP 범위 232/8을 사용합니다.
 - 양방향(BiDir)은 컨트롤 플레인 및 데이터 플레인 트래픽이 모두 RP를 통과하는 공유 트리의 유형(*, G)입니다.
- Rendezvous Point는 다음 방법 중 하나로 구성하거나 선택할 수 있습니다.

- 고정 RP
- 자동 RP
- 부트스트랩 라우터(BSR)

PIM 모드 요약


PIM 모드	RP	공유 트 리	표기법	IGMP	ASA/FTD 지원
PIM 스파스 모드	예	예	(*, G) 및 (S, G)	v1/v2/v3	예
PIM 밀집형 모드	아니 요	아니요	(S, G)	v1/v2/v3	아니요*
PIM 양방향 모드	예	예	(*, G)	v1/v2/v3	예
PIM SSM(Source-Specific-Multicast) 모드	아니 요	아니요	(S, G)	v3	아니요**

*Auto-RP = Auto-RP 트래픽이 통과할 수 있음

** ASA/FTD는 마지막 홉 디바이스가 될 수 없습니다.

RP 컨피그레이션 요약

랑데부 지점 컨피그레이션	ASA/FTD
고정 RP	예
자동 RP	아니요. 하지만 Auto-RP 컨트롤 플레인 트래픽은 통과할 수 있습니다.
BSR	예(C-RP 지원은 아님)

 참고: 멀티캐스트 문제의 트러블슈팅을 시작하기 전에 멀티캐스트 토폴로지를 명확하게 파악하는 것이 매우 중요합니다. 특히, 최소한 다음 사항을 알아야 합니다.

- ✎ - 멀티캐스트 토폴로지에서 방화벽의 역할은 무엇입니까?
- RP는 누구입니까?
- 멀티캐스트 스트림(소스 IP 및 멀티캐스트 그룹 IP)의 발신자는 누구입니까?
- 멀티캐스트 스트림의 수신자는 누구입니까?
- 컨트롤 플레인(IGMP/PIM) 또는 데이터 플레인(멀티캐스트 스트림) 자체에 문제가 있습니까?

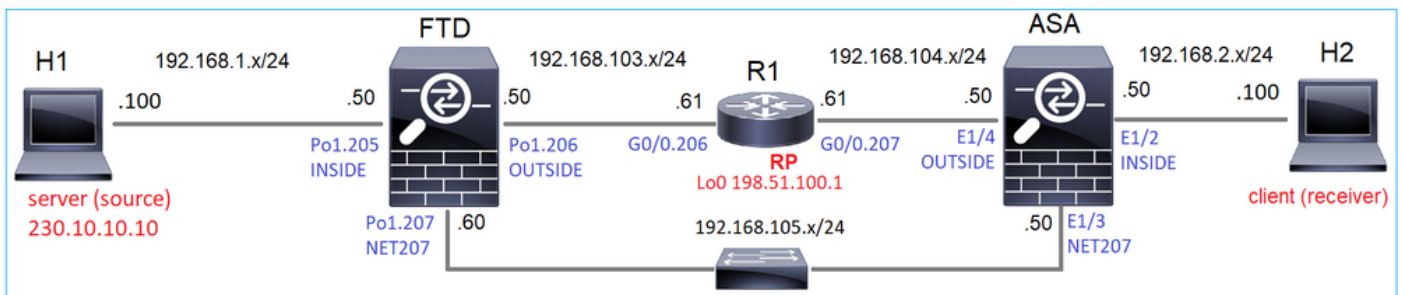
약어/약어

약어	설명
FHR	First-Hop Router - 멀티캐스트 트래픽의 소스에 직접 연결된 홉입니다.
LHR	Last-Hop Router - 멀티캐스트 트래픽의 수신자에 직접 연결된 홉입니다.
RP	랑데부 지점
박사	전용 라우터
SPT	최단 경로 트리
RPT	RP(Rendezvous-Point) 트리, 트리 공유
RPF	역방향 경로 전달
석유	발송 인터페이스 목록
MRIB	멀티캐스트 라우팅 정보 기반
MFIB	멀티캐스트 전달 정보 베이스
ASM	Any-Source 멀티캐스트

BSR	부트스트랩 라우터
SSM	소스별 멀티캐스트
FP	빠른 경로
SP	느린 경로
CP	제어 지점
PPS	패킷/초 비율

작업 1 - PIM 스파스 모드(고정 RP)

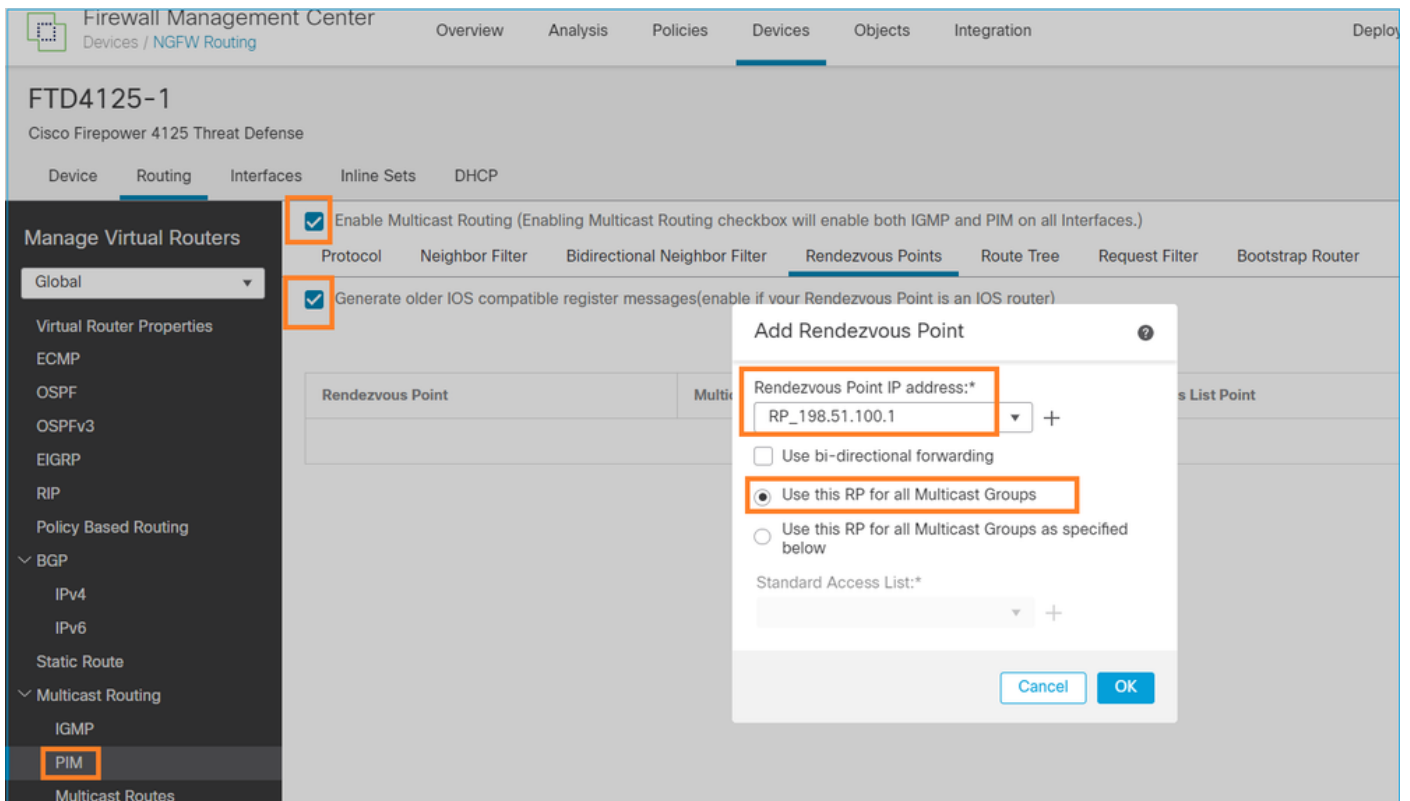
토폴로지



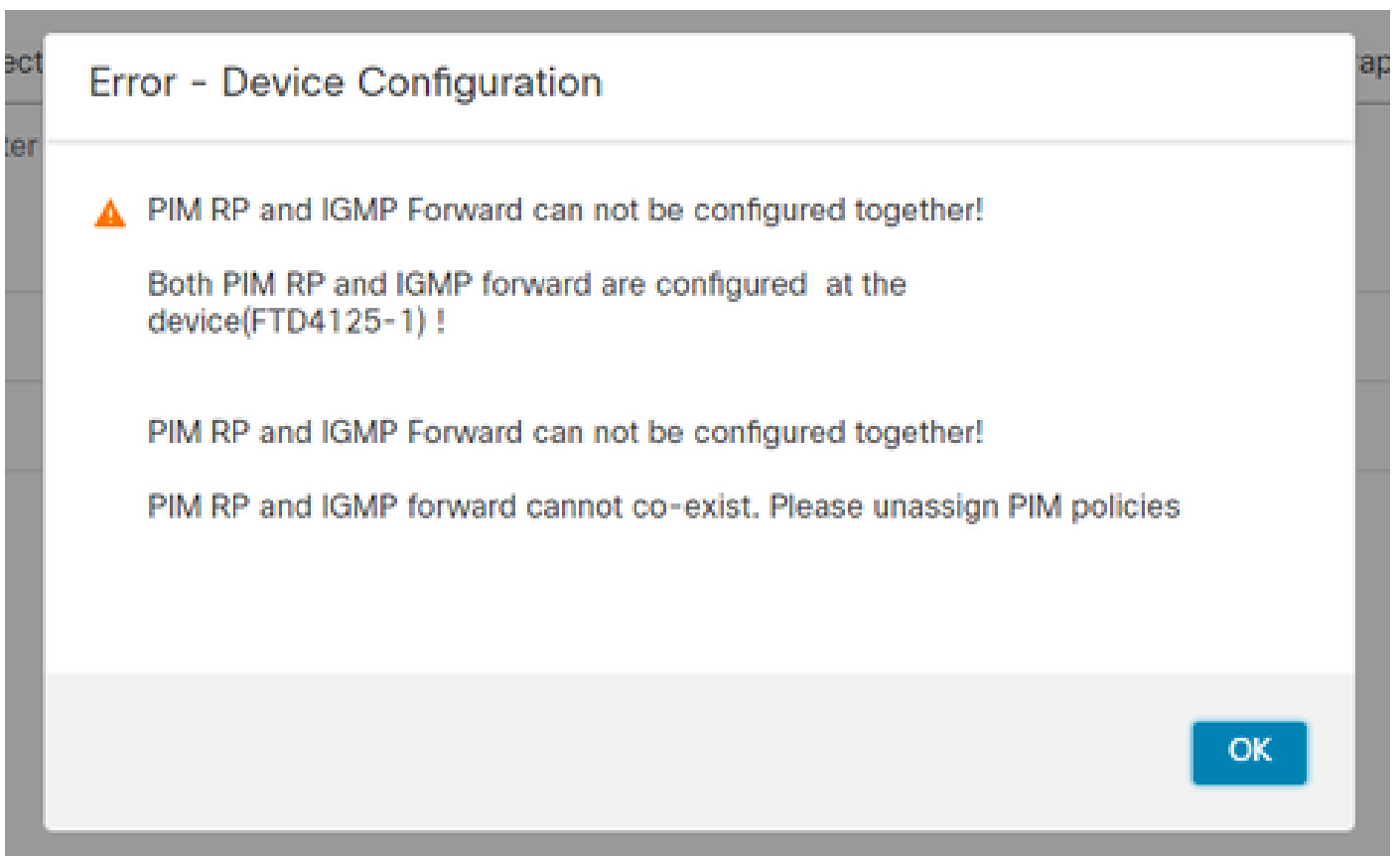
R1(198.51.100.1)이 RP인 토폴로지에서 멀티캐스트 PIM sparse-mode를 구성합니다.

솔루션

FTD 구성:



IGMP Stub 라우팅 및 PIM에 대해 ASA/FTD를 동시에 구성할 수 없습니다.



FTD에 대한 결과 컨피그레이션:

<#root>

```
firepower#
show running-config multicast-routing

multicast-routing

<-- Multicast routing is enabled globally on the device

firepower#
show running-config pim

pim rp-address 198.51.100.1          <-- Static RP is configured on the firewall

firepower#
ping 198.51.100.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.51.100.1, timeout is 2 seconds:
!!!!!                               <-- The RP is reachable

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

ASA 방화벽에는 유사한 컨피그레이션이 있습니다.

```
<#root>
asa(config)#
multicast-routing

asa(config)#
pim rp-address 198.51.100.1
```

RP 구성(Cisco 라우터):

```
<#root>
ip multicast-routing

ip pim rp-address 198.51.100.1          <-- The router is the RP
```

```

!
interface GigabitEthernet0/0.206
 encapsulation dot1Q 206
 ip address 192.168.103.61 255.255.255.0

 ip pim sparse-dense-mode          <-- The interface participates in multicast routing

 ip ospf 1 area 0
!
interface GigabitEthernet0/0.207
 encapsulation dot1Q 207
 ip address 192.168.104.61 255.255.255.0

 ip pim sparse-dense-mode          <-- The interface participates in multicast routing

 ip ospf 1 area 0
!
interface Loopback0

 ip address 198.51.100.1 255.255.255.255

<-- The router is the RP

 ip pim sparse-dense-mode          <-- The interface participates in multicast routing

 ip ospf 1 area 0

```

확인

멀티캐스트 트래픽(발신자 또는 수신자)이 없는 경우 FTD에서 멀티캐스트 컨트롤 플레인을 확인합니다.

```
<#root>
```

```
firepower#
```

```
show pim interface
```

Address	Interface	PIM	Nbr Count	Hello Intvl	DR Prior	DR	
192.168.105.60	NET207	on	1	30	1	this system	
<-- PIM enabled on the interface. There is 1 PIM neighbor							
192.168.1.50	INSIDE	on	0	30	1	this system	<-- PIM enabled on t
0.0.0.0	diagnostic	off	0	30	1	not elected	
192.168.103.50	OUTSIDE	on	1	30	1	192.168.103.61	<-- PIM enabled on t

PIM 인접 디바이스를 확인합니다.

<#root>

firepower#

show pim neighbor

Neighbor Address	Interface	Uptime	Expires	DR	pri	Bidir
192.168.105.50	NET207	00:05:41	00:01:28	1		B
192.168.103.61	OUTSIDE	00:05:39	00:01:32	1	(DR)	

RP는 전체 멀티캐스트 그룹 범위를 광고합니다.

<#root>

firepower#

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*	SM	config	2	198.51.100.1	RPF: OUTSIDE,192.168.103.61 <-- The mult
224.0.0.0/4	SM	static	0	0.0.0.0	RPF: ,0.0.0.0

방화벽 mroute 테이블에는 일부 관련 없는 항목이 있습니다(239.255.255.250은 MAC OS 및 Microsoft Windows와 같은 공급업체에서 사용하는 SSDP(Simple Service Discovery Protocol)임).

<#root>

firepower#

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

```
(*, 239.255.255.250), 00:17:35/never, RP 198.51.100.1, flags: SCJ
  Incoming interface: OUTSIDE
  RPF nbr: 192.168.103.61
  Immediate Outgoing interface list:
    INSIDE, Forward, 00:17:35/never
```

방화벽과 RP 사이에 PIM 터널이 구축되어 있습니다.

```
<#root>
firepower#
show pim tunnel

Interface          RP Address          Source Address
Tunnel0            198.51.100.1       192.168.103.50
```

<-- PIM tunnel between the FTD and the RP

PIM 터널은 방화벽 연결 테이블에서도 볼 수 있습니다.

```
<#root>
firepower#
show conn all detail address 198.51.100.1
...
PIM OUTSIDE: 198.51.100.1/0 NP Identity Ifc: 192.168.103.50/0,
```

```
<-- PIM tunnel between the FTD and the RP
, flags , idle 16s, uptime 3m8s, timeout 2m0s, bytes 6350
Connection lookup keyid: 153426246
```

ASA 방화벽 확인:

```
<#root>
asa#
show pim neighbor

Neighbor Address  Interface      Uptime      Expires DR pri Bidir
192.168.105.60    NET207         2d21h       00:01:29 1 (DR) B
192.168.104.61    OUTSIDE        00:00:18    00:01:37 1 (DR)
```

```
<#root>
asa#
show pim tunnel

Interface          RP Address          Source Address
Tunnel0            198.51.100.1       192.168.104.50
```

<-- PIM tunnel between the ASA and the RP

RP(Cisco 라우터) RP 확인. SSDP 및 Auto-RP를 위한 몇 가지 멀티캐스트 그룹이 있습니다.

```
<#root>
```

```
Router1#
```

```
show ip pim rp
```

```
Group: 239.255.255.250, RP: 198.51.100.1, next RP-reachable in 00:01:04  
Group: 224.0.1.40, RP: 198.51.100.1, next RP-reachable in 00:00:54
```

수신자가 존재를 알리면 확인



참고: 이 섹션에 나와 있는 firewall 명령은 ASA 및 FTD에 모두 적용됩니다.

ASA는 IGMP Membership Report(IGMP 멤버십 보고서) 메시지를 가져오고 IGMP 및 mroute(*, G) 항목을 생성합니다.

```
<#root>
```

```
asa#
```

```
show igmp group 230.10.10.10
```

```
IGMP Connected Group Membership
```

```
Group Address      Interface          Uptime    Expires    Last Reporter
```

```
230.10.10.10      INSIDE            00:01:15  00:03:22  192.168.2.100    <-- Host 192.168.2.100 report
```

ASA 방화벽은 멀티캐스트 그룹에 대한 mroute를 생성합니다.

```
<#root>
```

```
asa#
```

```
show mroute 230.10.10.10
```

```
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
```

```
(*, 230.10.10.10)
```

```
, 00:00:17/never,
```

```
RP 198.51.100.1
```

```
, flags: SCJ
```

```
<-- The mroute for group 230.10.10.10
```

```
Incoming interface: OUTSIDE
```

```
<-- Expected interface for a multicast packet from the source. If the packet is not received on this int
```

```
RPF nbr: 192.168.104.61
```

```
Immediate Outgoing interface list:  
INSIDE, Forward, 00:01:17/never
```

```
<-- The OIL points towards the recei
```

또 다른 방화벽 확인은 PIM 토폴로지 출력입니다.

```
<#root>
```

```
asa#
```


```
show pim topology 230.10.10.10
```

```
...
```

```
(* ,230.10.10.10) SM Up: 00:07:15 RP: 198.51.100.1
```

```
<-- An entry for multicast group 23
```

```
JP: Join(00:00:33) RPF: OUTSIDE,192.168.104.61 Flags: LH  
INSIDE 00:03:15 fwd LI LH
```

 참고: 방화벽에 RP로 향하는 경로가 없는 경우 디버그 pim 출력에 RPF 조회 실패가 표시됩니다

디버그 pim 출력에서 RPF 조회가 실패했습니다.

```
<#root>
```

```
asa#
```

```
debug pim
```

```
IPv4 PIM: RPF lookup failed for root 198.51.100.1
```

```
<-- The RPF look fails because ther
```

```
IPv4 PIM: RPF lookup failed for root 198.51.100.1
```

```
IPv4 PIM: (*,230.10.10.10) Processing Periodic Join-Prune timer
```

```
IPv4 PIM: (*,230.10.10.10) J/P processing
```

```
IPv4 PIM: (*,230.10.10.10) Periodic J/P scheduled in 50 secs
```

IPv4 PIM: (*,230.10.10.10) No RPF neighbor to send J/P

모든 것이 정상인 경우 방화벽은 RP에 PIM Join-Prune 메시지를 전송합니다.

<#root>

asa#

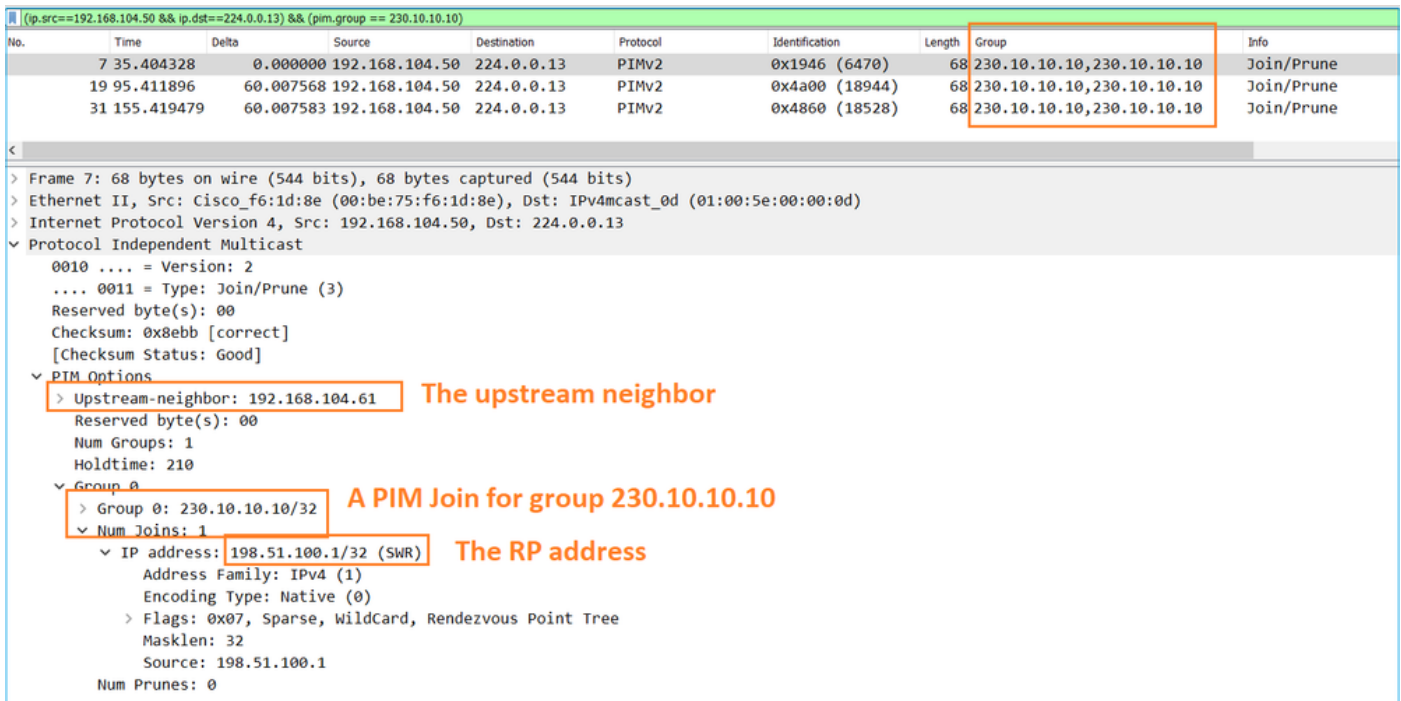
debug pim group 230.10.10.10

IPv4 PIM group debugging is on
for group 230.10.10.10

IPv4 PIM: (*,230.10.10.10) J/P scheduled in 0.0 secs
IPv4 PIM: [0] (*,230.10.10.10/32) MRIB modify A NS
IPv4 PIM: [0] (*,230.10.10.10/32) NULLIF-skip MRIB modify !A !NS
IPv4 PIM: [0] (*,230.10.10.10/32) OUTSIDE MRIB modify A NS
IPv4 PIM: (*,230.10.10.10) Processing timers
IPv4 PIM: (*,230.10.10.10) J/P processing
IPv4 PIM: (*,230.10.10.10) Periodic J/P scheduled in 50 secs

IPv4 PIM: (*,230.10.10.10) J/P adding Join on OUTSIDE

캡처는 PIM Join 메시지가 1분마다, PIM Hello가 30초마다 전송되는 것을 보여줍니다. PIM은 IP 224.0.0.13을 사용합니다.



No.	Time	Delta	Source	Destination	Protocol	Identification	Length	Group	Info
7	35.404328	0.000000	192.168.104.50	224.0.0.13	PIMv2	0x1946 (6470)	68	230.10.10.10,230.10.10.10	Join/Prune
19	95.411896	60.007568	192.168.104.50	224.0.0.13	PIMv2	0x4a00 (18944)	68	230.10.10.10,230.10.10.10	Join/Prune
31	155.419479	60.007583	192.168.104.50	224.0.0.13	PIMv2	0x4860 (18528)	68	230.10.10.10,230.10.10.10	Join/Prune

> Frame 7: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
 > Ethernet II, Src: Cisco_f6:1d:8e (00:be:75:f6:1d:8e), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
 > Internet Protocol Version 4, Src: 192.168.104.50, Dst: 224.0.0.13
 v Protocol Independent Multicast
 0010 ... = Version: 2
 ... 0011 = Type: Join/Prune (3)
 Reserved byte(s): 00
 Checksum: 0x8ebb [correct]
 [Checksum Status: Good]
 v PIM Options
 > Upstream-neighbor: 192.168.104.61 The upstream neighbor
 Reserved byte(s): 00
 Num Groups: 1
 Holdtime: 210
 v Group 0
 > Group 0: 230.10.10.10/32 A PIM Join for group 230.10.10.10
 v Num Joins: 1
 v IP address: 198.51.100.1/32 (SWR) The RP address
 Address Family: IPv4 (1)
 Encoding Type: Native (0)
 > Flags: 0x07, Sparse, WildCard, Rendezvous Point Tree
 Masklen: 32
 Source: 198.51.100.1
 Num Prunes: 0



팁: Wireshark 디스플레이 필터: (ip.src==192.168.104.50 && ip.dst==224.0.0.13) && (pim.group == 230.10.10.10)

- 192.168.104.50은 이그레스 인터페이스의 방화벽 IP입니다(업스트림 PIM 네이버 방향).
- 224.0.0.13은 PIM 조인 및 프룬이 전송되는 PIM 멀티캐스트 그룹입니다.

🔍 - 230.10.10.10은 다음에 대한 PIM Join/Prune을 전송하는 멀티캐스트 그룹입니다.

RP는 (*, G) mroute를 생성합니다. 아직 서버가 없으므로 Incoming Interface는 Null입니다.

<#root>

Router1#

```
show ip mroute 230.10.10.10 | b \(\
```

```
(*, 230.10.10.10), 00:00:27/00:03:02, RP 198.51.100.1, flags: S
```

<-- The mroute for the multicast

```
Incoming interface: Null
```

```
, RPF nbr 0.0.0.0 <-- No incoming multicast stream
```

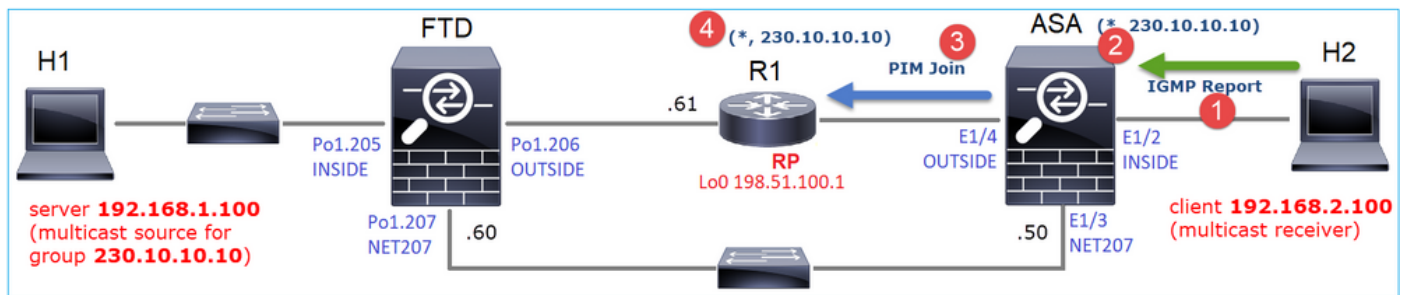
```
Outgoing interface list:
```

```
GigabitEthernet0/0.207
```

```
, Forward/Sparse-Dense, 00:00:27/00:03:02
```

```
<-- There was a PIM Join on this interface
```

이는 다음과 같이 시각화할 수 있습니다.



1. ASA에서 IGMP 보고서가 수신되었습니다.
2. A(*, G) mroute가 추가됩니다.
3. ASA는 RP(198.51.100.1)에 PIM Join 메시지를 보냅니다.
4. RP는 Join 메시지를 수신하고 (*, G) mroute를 추가합니다.

동시에 FTD에는 IGMP 보고서도 없고 PIM 조인도 수신되지 않았으므로 mroutes가 없습니다.

<#root>

firepower#

```
show mroute 230.10.10.10
```

```
No mroute entries found.
```

서버가 멀티캐스트 스트림을 전송할 때 확인

FTD는 H1에서 멀티캐스트 스트림을 가져오고 RP를 사용하여 PIM 등록 프로세스를 시작합니다. FTD는 유니캐스트 PIM 레지스터 메시지를 RP에 전송합니다. RP는 멀티캐스트 트리에 참가하기 위해 FHR(First-Hop-Router)에 PIM 참가 메시지를 보냅니다(이 경우 FTD). 그런 다음 Register-Stop 메시지를 전송합니다.

```
<#root>
```

```
firepower#
```

```
debug pim group 230.10.10.10
```

```
IPv4 PIM group debugging is on
```

```
for group 230.10.10.10
```

```
firepower#
```

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB update (f=20,c=20)
```

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on INSIDE
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10) Create entry
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10) RPF changed from 0.0.0.0/- to 192.168.1.100/INSIDE
```

```
<-- The FTD receives a multicast stream on INSIDE interface for group 230.10.10.10
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10) Connected status changed from off to on
```

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify NS
```

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) MRIB modify DC
```

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify A NS
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10) Set alive timer to 210 sec
```

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify !NS
```

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) MRIB modify !DC
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10) Start registering to 198.51.100.1
```

```
<-- The FTD
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 J/P state changed from Null to Join
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 FWD state change from Prune to Forward
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10) Updating J/P status from Null to Join
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10) J/P scheduled in 0.0 secs
```

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB modify NS
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10) Set SPT bit
```

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) MRIB modify NS
```

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify !A
```

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB modify A !NS
```

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) Tunnel0 MRIB modify F NS
```

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB modify !SP
```

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB update (f=2,c=20)
```

```
IPv4 PIM: J/P entry: Join root: 192.168.1.100 group: 230.10.10.10 flags: S
```

```
<-- The FTD
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE J/P state changed from Null to Join
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE FWD state change from Prune to Forward
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify F NS
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE Raise J/P expiration timer to 210 seconds
IPv4 PIM: J/P entry: Join root: 192.168.1.100 group: 230.10.10.10 flags: S
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE Raise J/P expiration timer to 210 seconds
IPv4 PIM: (192.168.1.100,230.10.10.10) Processing timers
IPv4 PIM: (192.168.1.100,230.10.10.10) J/P processing
IPv4 PIM: (192.168.1.100,230.10.10.10) Suppress J/P to connected source
IPv4 PIM: (192.168.1.100,230.10.10.10) Suppress J/P to connected source
IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 Processing timers
IPv4 PIM: J/P entry: Join root: 192.168.1.100 group: 230.10.10.10 flags: S
IPv4 PIM: (192.168.1.100,230.10.10.10) NET207 J/P state changed from Null to Join
IPv4 PIM: (192.168.1.100,230.10.10.10) NET207 FWD state change from Prune to Forward
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify F NS
IPv4 PIM: (192.168.1.100,230.10.10.10) NET207 Raise J/P expiration timer to 210 seconds
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=29,c=20)
IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on NET207
IPv4 PIM: (192.168.1.100,230.10.10.10) Send [0/0] Assert on NET207
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify !SP
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=9,c=20)
IPv4 PIM: J/P entry: Prune root: 192.168.1.100 group: 230.10.10.10 flags: S
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE J/P state changed from Join to Null
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE FWD state change from Forward to Prune
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify !F !NS
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=29,c=20)
IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on NET207
IPv4 PIM: (192.168.1.100,230.10.10.10) Send [0/0] Assert on NET207
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify !SP
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=9,c=20)
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE Processing timers
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
```

```
<-- The RP s
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10) Stop registering
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 J/P state changed from Join to Null
IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 FWD state change from Forward to Prune
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) Tunnel0 MRIB modify !F !NS
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 Processing timers
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB update (f=22,c=20)
IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on INSIDE
IPv4 PIM: (192.168.1.100,230.10.10.10) Set alive timer to 210 sec
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB modify !SP
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB update (f=2,c=20)
```

PIM 레지스터 메시지는 PIM 레지스터 정보와 함께 UDP 데이터를 전달하는 PIM 메시지입니다.

No.	Time	Delta	Source	Destination	Protocol	Identification	Length	Group	Info
23	15.829623	0.000015	192.168.1.100	230.10.10.10	PIMv2	0x9802 (38914)...	1402		Register
24	15.829623	0.000000	192.168.1.100	230.10.10.10	PIMv2	0x9902 (39170)...	1402		Register
25	15.829653	0.000030	192.168.1.100	230.10.10.10	PIMv2	0x9a02 (39426)...	1402		Register
26	15.829653	0.000000	192.168.1.100	230.10.10.10	PIMv2	0x9b02 (39682)...	1402		Register
27	15.833224	0.003571	198.51.100.1	192.168.103.50	PIMv2	0x107c (4220)	56	230.10.10.10,230.10.10.10	Register-stop
28	15.833468	0.000244	198.51.100.1	192.168.103.50	PIMv2	0x107d (4221)	56	230.10.10.10,230.10.10.10	Register-stop
29	15.833681	0.000213	198.51.100.1	192.168.103.50	PIMv2	0x107e (4222)	56	230.10.10.10,230.10.10.10	Register-stop
30	15.833910	0.000229	198.51.100.1	192.168.103.50	PIMv2	0x107f (4223)	56	230.10.10.10,230.10.10.10	Register-stop
31	15.834109	0.000199	198.51.100.1	192.168.103.50	PIMv2	0x1080 (4224)	56	230.10.10.10,230.10.10.10	Register-stop
32	15.836092	0.001983	198.51.100.1	192.168.103.50	PIMv2	0x108f (4239)	56	230.10.10.10,230.10.10.10	Register-stop
33	15.836306	0.000214	198.51.100.1	192.168.103.50	PIMv2	0x1090 (4240)	56	230.10.10.10,230.10.10.10	Register-stop
34	15.836535	0.000229	198.51.100.1	192.168.103.50	PIMv2	0x1091 (4241)	56	230.10.10.10,230.10.10.10	Register-stop

> Frame 26: 1402 bytes on wire (11216 bits), 1402 bytes captured (11216 bits)
 > Ethernet II, Src: Cisco_33:44:5d (f4:db:e6:33:44:5d), Dst: Cisco_fc:fc:d8 (4c:4e:35:fc:fc:d8)
 > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 206
 > Internet Protocol Version 4, Src: 192.168.103.50, Dst: 198.51.100.1
 > Protocol Independent Multicast
 0010 = Version: 2
 ... 0001 = Type: Register (1)
 Reserved byte(s): 00
 > Checksum: 0x966a incorrect, should be 0xdef
 [Checksum Status: Bad]
 > PIM Options
 > Internet Protocol Version 4, Src: 192.168.1.100, Dst: 230.10.10.10
 > User Datagram Protocol, Src Port: 64742 (64742), Dst Port: avt-profile-1 (5004)
 > Data (1328 bytes)

PIM Register-Stop 메시지:

No.	Time	Delta	Source	Destination	Protocol	Identification	Length	Group	Info
23	15.829623	0.000015	192.168.1.100	230.10.10.10	PIMv2	0x9802 (38914)...	1402		Register
24	15.829623	0.000000	192.168.1.100	230.10.10.10	PIMv2	0x9902 (39170)...	1402		Register
25	15.829653	0.000030	192.168.1.100	230.10.10.10	PIMv2	0x9a02 (39426)...	1402		Register
26	15.829653	0.000000	192.168.1.100	230.10.10.10	PIMv2	0x9b02 (39682)...	1402		Register
27	15.833224	0.003571	198.51.100.1	192.168.103.50	PIMv2	0x107c (4220)	56	230.10.10.10,230.10.10.10	Register-stop
28	15.833468	0.000244	198.51.100.1	192.168.103.50	PIMv2	0x107d (4221)	56	230.10.10.10,230.10.10.10	Register-stop
29	15.833681	0.000213	198.51.100.1	192.168.103.50	PIMv2	0x107e (4222)	56	230.10.10.10,230.10.10.10	Register-stop
30	15.833910	0.000229	198.51.100.1	192.168.103.50	PIMv2	0x107f (4223)	56	230.10.10.10,230.10.10.10	Register-stop
31	15.834109	0.000199	198.51.100.1	192.168.103.50	PIMv2	0x1080 (4224)	56	230.10.10.10,230.10.10.10	Register-stop
32	15.836092	0.001983	198.51.100.1	192.168.103.50	PIMv2	0x108f (4239)	56	230.10.10.10,230.10.10.10	Register-stop
33	15.836306	0.000214	198.51.100.1	192.168.103.50	PIMv2	0x1090 (4240)	56	230.10.10.10,230.10.10.10	Register-stop
34	15.836535	0.000229	198.51.100.1	192.168.103.50	PIMv2	0x1091 (4241)	56	230.10.10.10,230.10.10.10	Register-stop

> Frame 27: 56 bytes on wire (448 bits), 56 bytes captured (448 bits)
 > Ethernet II, Src: Cisco_fc:fc:d8 (4c:4e:35:fc:fc:d8), Dst: Cisco_33:44:5d (f4:db:e6:33:44:5d)
 > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 206
 > Internet Protocol Version 4, Src: 198.51.100.1, Dst: 192.168.103.50
 > Protocol Independent Multicast
 0010 = Version: 2
 ... 0010 = Type: Register-stop (2)
 Reserved byte(s): 00
 Checksum: 0x29be [correct]
 [Checksum Status: Good]
 > PIM Options

 **팁:** Wireshark에서 PIM Register 및 PIM Register-Stop 메시지만 표시하려면 {1.2}의 pim.type 표시 필터를 사용합니다.

방화벽(last-hop 라우터)은 인터페이스 OUTSIDE에서 멀티캐스트 스트림을 가져오고 인터페이스 NET207로 SPT(Shortest Path Tree) 전환을 시작합니다.

```
<#root>
```

```
asa#
```

```
debug pim group 230.10.10.10
```

```
IPv4 PIM group debugging is on  
for group 230.10.10.10
```

IPv4 PIM: (*,230.10.10.10) Processing Periodic Join-Prune timer
IPv4 PIM: (*,230.10.10.10) J/P processing
IPv4 PIM: (*,230.10.10.10) Periodic J/P scheduled in 50 secs
IPv4 PIM: (*,230.10.10.10) J/P adding Join on OUTSIDE

<-- A PIM Join message is sent from the interface OUTSIDE

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB update (f=20,c=20)

IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on OUTSIDE

<-- The n

IPv4 PIM: (192.168.1.100,230.10.10.10) Create entry

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify NS

IPv4 PIM: (192.168.1.100,230.10.10.10) RPF changed from 0.0.0.0/- to 192.168.105.60/NET207

<-- The SPT switchover starts from the interface OUTSIDE to the interface NET207

IPv4 PIM: (192.168.1.100,230.10.10.10) Source metric changed from [0/0] to [110/20]

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) MRIB modify DC

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify A NS

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB modify F NS

IPv4 PIM: (192.168.1.100,230.10.10.10) Set alive timer to 210 sec

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify !NS

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) MRIB modify !DC

IPv4 PIM: (192.168.1.100,230.10.10.10) Updating J/P status from Null to Join

IPv4 PIM: (192.168.1.100,230.10.10.10) J/P scheduled in 0.0 secs

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify NS

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify !SP

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB update (f=2,c=20)

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=28,c=20)

IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on NET207

IPv4 PIM: (192.168.1.100,230.10.10.10)

Set SPT bit

<-- The SPT bit is set

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) MRIB modify !SP

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify !A

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify A !NS

IPv4 PIM: (192.168.1.100,230.10.10.10)RPT Updating J/P status from Null to Prune

IPv4 PIM: (192.168.1.100,230.10.10.10)RPT Create entry

IPv4 PIM: (192.168.1.100,230.10.10.10)RPT J/P scheduled in 0.0 secs

IPv4 PIM: (192.168.1.100,230.10.10.10) Set alive timer to 210 sec

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify !SP

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=2,c=20)

IPv4 PIM: (192.168.1.100,230.10.10.10)RPT Processing timers

IPv4 PIM: (192.168.1.100,230.10.10.10)RPT J/P processing

IPv4 PIM: (192.168.1.100,230.10.10.10)RPT J/P adding Prune on OUTSIDE

<-- A PIM Prune message is sent from the interface OUTSIDE

IPv4 PIM: (192.168.1.100,230.10.10.10)RPT Delete entry

IPv4 PIM: (192.168.1.100,230.10.10.10) Processing timers

IPv4 PIM: (192.168.1.100,230.10.10.10) J/P processing

IPv4 PIM: (192.168.1.100,230.10.10.10) Periodic J/P scheduled in 50 secs

```
IPv4 PIM: (192.168.1.100,230.10.10.10) J/P adding Join on NET207
```

```
<-- A PIM Join message is sent from the interface NET207
```

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=22,c=20)
IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on NET207
IPv4 PIM: (192.168.1.100,230.10.10.10) Set alive timer to 210 sec
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify !SP
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=2,c=20)
```

전환이 발생할 때 FTD의 PIM 디버그:

```
<#root>
```

```
IPv4 PIM: J/P entry: Join root: 192.168.1.100 group: 230.10.10.10 flags: S
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10) NET207 J/P state changed from Null to Join
```

```
<-- A PIM Join message is sent from the interface NET207
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10) NET207 FWD state change from Prune to Forward
```

```
<-- The packets are sent from the interface NET207
```

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify F NS
IPv4 PIM: (192.168.1.100,230.10.10.10) NET207 Raise J/P expiration timer to 210 seconds
IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 Processing timers
...
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=9,c=20)
IPv4 PIM: J/P entry: Prune root: 192.168.1.100 group: 230.10.10.10 flags: S
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE J/P state changed from Join to Null
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE FWD state change from Forward to Prune
```

```
<-- A PIM Prune message is sent from the interface OUTSIDE
```

SPT 전환이 시작되면 FTD mroute:

```
<#root>
```

```
firepower#
```

```
show mroute 230.10.10.10
```

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

(192.168.1.100, 230.10.10.10), 00:00:06/00:03:23, flags: SF

T <-- SPT-bit is set when the switchover occurs

Incoming interface: INSIDE

RPF nbr: 192.168.1.100, Registering

Immediate Outgoing interface list:

NET207, Forward, 00:00:06/00:03:23

<-- Both interfaces are shown in

OUTSIDE, Forward, 00:00:06/00:03:23

<-- Both interfaces are shown in

Tunnel0, Forward, 00:00:06/never

SPT 전환이 끝나면 FTD의 OIL에는 NET207 인터페이스만 표시됩니다.

<#root>

firepower#

show mroute 230.10.10.10

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

(192.168.1.100, 230.10.10.10), 00:00:28/00:03:01, flags: SFT

Incoming interface: INSIDE

RPF nbr: 192.168.1.100

Immediate Outgoing interface list:

NET207, Forward

, 00:00:28/00:03:01

<-- The interface NET207 forwards the multicast stream after the SPT switchover

ASA(last-hop router)에서는 SPT 비트도 설정됩니다.

```
<#root>
```

```
asa#
```

```
show mroute 230.10.10.10
```

```
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
```

```
(*, 230.10.10.10), 01:43:09/never, RP 198.51.100.1, flags: SCJ
```

```
  Incoming interface: OUTSIDE
```

```
  RPF nbr: 192.168.104.61
```

```
  Immediate Outgoing interface list:
```

```
    INSIDE, Forward, 01:43:09/never
```

```
(192.168.1.100, 230.10.10.10)
```

```
, 00:00:03/00:03:27, flags: SJ
```

```
T      <-- SPT switchover for group 230.10.10.10
```

```
Incoming interface:
```

```
NET207
```

```
<-- The multicast packets arrive on interface NET207
```

```
  RPF nbr: 192.168.105.60
```

```
  Inherited Outgoing interface list:
```

```
    INSIDE, Forward, 01:43:09/never
```

ASA NET207 인터페이스(전환을 수행한 첫 번째 홉 라우터)로부터의 전환. PIM Join(PIM 조인) 메시지가 FTD(업스트림 디바이스)로 전송됩니다.

No.	Time	Delta	Source	Destination	Protocol	Identification	Length	Group	Info
202	61.891684	0.000000	192.168.105.50	224.0.0.13	PIMv2	0x1c71 (7281)	68	230.10.10.10,230.10.10.10	Join/Prune
1073	120.893225	59.001541	192.168.105.50	224.0.0.13	PIMv2	0x68ac (26796)	68	230.10.10.10,230.10.10.10	Join/Prune
1174	180.894766	60.001541	192.168.105.50	224.0.0.13	PIMv2	0x0df8 (3576)	68	230.10.10.10,230.10.10.10	Join/Prune
1276	240.896307	60.001541	192.168.105.50	224.0.0.13	PIMv2	0x6858 (26712)	68	230.10.10.10,230.10.10.10	Join/Prune

```

> Frame 202: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
> Ethernet II, Src: Cisco_f6:1d:ae (00:be:75:f6:1d:ae), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
> Internet Protocol Version 4, Src: 192.168.105.50, Dst: 224.0.0.13
v Protocol Independent Multicast
  0010 .... = Version: 2
  ... 0011 = Type: Join/Prune (3)
  Reserved byte(s): 00
  Checksum: 0xf8e4 [correct]
  [Checksum Status: Good]
  v PIM Options
    > Upstream-neighbor: 192.168.105.60
    Reserved byte(s): 00
    Num Groups: 1
    Holdtime: 210
  v Group 0
    > Group 0: 230.10.10.10/32
    v Num Joins: 1
      > IP address: 192.168.1.100/32 (S)
    Num Prunes: 0
  
```

OUTSIDE 인터페이스에서 PIM Prune 메시지가 RP로 전송되어 멀티캐스트 스트림을 중지합니다.

No.	Time	Delta	Source	Destination	Protocol	Identification	Length	Group	Info
202	61.891668	0.000000	192.168.104.50	224.0.0.13	PIMv2	0x3a56 (14934)	68	230.10.10.10,230.10.10.10	Join/Prune
2818	1137.915409	1076.023741	192.168.104.50	224.0.0.13	PIMv2	0x1acf (6863)	68	230.10.10.10,230.10.10.10	Join/Prune
5124	1257.917103	120.001694	192.168.104.50	224.0.0.13	PIMv2	0x0b52 (2898)	68	230.10.10.10,230.10.10.10	Join/Prune

```

> Frame 202: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
> Ethernet II, Src: Cisco_f6:1d:8e (00:be:75:f6:1d:8e), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
> Internet Protocol Version 4, Src: 192.168.104.50, Dst: 224.0.0.13
v Protocol Independent Multicast
  0010 .... = Version: 2
  ... 0011 = Type: Join/Prune (3)
  Reserved byte(s): 00
  Checksum: 0xf8e3 [correct]
  [Checksum Status: Good]
  v PIM Options
    > Upstream-neighbor: 192.168.104.61
    Reserved byte(s): 00
    Num Groups: 1
    Holdtime: 210
  v Group 0
    > Group 0: 230.10.10.10/32
    Num Joins: 0
    v Num Prunes: 1
      > IP address: 192.168.1.100/32 (SR)
  
```

PIM 트래픽 확인:

```
<#root>
```

```
firepower#
```

```
show pim traffic
```

PIM Traffic Counters

Elapsed time since counters cleared: 1w2d

	Received	Sent	
Valid PIM Packets	53934	63983	
Hello	36905	77023	
Join-Prune	6495	494	<-- PIM Join/Prune messages
Register	0	2052	<-- PIM Register messages
Register Stop	1501	0	<-- PIM Register Stop messages
Assert	289	362	
Bidir DF Election	0	0	
Errors:			
Malformed Packets		0	
Bad Checksums		0	
Send Errors		0	
Packet Sent on Loopback Errors		0	
Packets Received on PIM-disabled Interface		0	
Packets Received with Unknown PIM Version		0	
Packets Received with Incorrect Addressing		0	

느린 경로 대 빠른 경로 대 제어 지점에서 처리된 패킷 수를 확인하려면 다음을 수행합니다.

```
<#root>
```

```
firepower#
```

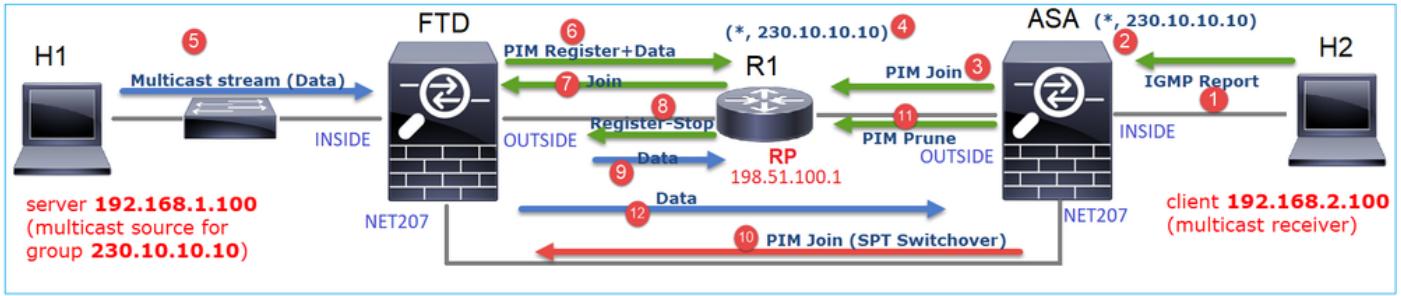
```
show asp cluster counter
```

Global dp-counters:

Context specific dp-counters:

MCAST_FP_FROM_PUNT	2712	Number of multicast packets punted from CP to FP
MCAST_FP_FORWARDED	94901	Number of multicast packets forwarded in FP
MCAST_FP_TO_SP	1105138	Number of multicast packets punted from FP to SP
MCAST_SP_TOTAL	1107850	Number of total multicast packets processed in SP
MCAST_SP_FROM_PUNT	2712	Number of multicast packets punted from CP to SP
MCAST_SP_FROM_PUNT_FORWARD	2712	Number of multicast packets coming from CP that are forwarded
MCAST_SP_PKTS	537562	Number of multicast packets that require slow-path attention
MCAST_SP_PKTS_TO_FP_FWD	109	Number of multicast packets that skip over punt rule and are forwarded
MCAST_SP_PKTS_TO_CP	166981	Number of multicast packets punted to CP from SP
MCAST_FP_CHK_FAIL_NO_HANDLE	567576	Number of multicast packets failed with no flow mcast_handle
MCAST_FP_CHK_FAIL_NO_ACCEPT_IFC	223847	Number of multicast packets failed with no accept interface
MCAST_FP_CHK_FAIL_NO_SEQ_NO_MATCH	131	Number of multicast packets failed with no matched sequence
MCAST_FP_CHK_FAIL_NO_FP_FWD	313584	Number of multicast packets that cannot be fast-path forwarded
MCAST_FP_UPD_FOR_UNMATCH_IFC	91	Number of times that multicast flow's ifc_out cannot be updated

단계별로 수행되는 작업을 보여 주는 다이어그램:



1. 엔드 호스트(H2)는 멀티캐스트 스트림 230.10.10.10에 가입하기 위해 IGMP 보고서를 전송합니다.
2. PIM DR인 ASA(last-hop router)는 (*, 230.10.10.10) 항목을 생성합니다.
3. ASA는 그룹 230.10.10.10에 대해 RP로 PIM Join 메시지를 보냅니다.
4. RP는 (*, 230.10.10.10) 항목을 생성합니다.
5. 서버는 멀티캐스트 스트림 데이터를 전송합니다.
6. FTD는 PIM 레지스터 메시지에서 멀티캐스트 패킷을 캡슐화하여 RP로 전송(유니캐스트)합니다. 이 시점에서 RP는 활성 수신기가 있음을 확인하고 멀티캐스트 패킷을 역캡슐화하여 수신기로 전송합니다.
7. RP는 PIM Join(PIM 조인) 메시지를 FTD에 전송하여 멀티캐스트 트리에 조인합니다.
8. RP는 FTD에 PIM Register-Stop 메시지를 전송합니다.
9. FTD는 RP를 향해 네이티브 멀티캐스트 스트림(PIM 캡슐화 없음)을 전송합니다.
10. ASA(last-hop router)는 소스(192.168.1.100)가 NET207 인터페이스에서 더 나은 경로를 가지고 있음을 확인하고 전환을 시작합니다. PIM Join(PIM 조인) 메시지를 업스트림 디바이스(FTD)로 전송합니다.
11. 마지막 홉 라우터는 RP에 PIM Prune 메시지를 보냅니다.
12. FTD는 멀티캐스트 스트림을 NET207 인터페이스로 전달합니다. ASA가 공유 트리(RP 트리)에서 소스 트리(SPT)로 이동합니다.

작업 2 - PIM BSR(부트스트랩 라우터) 구성

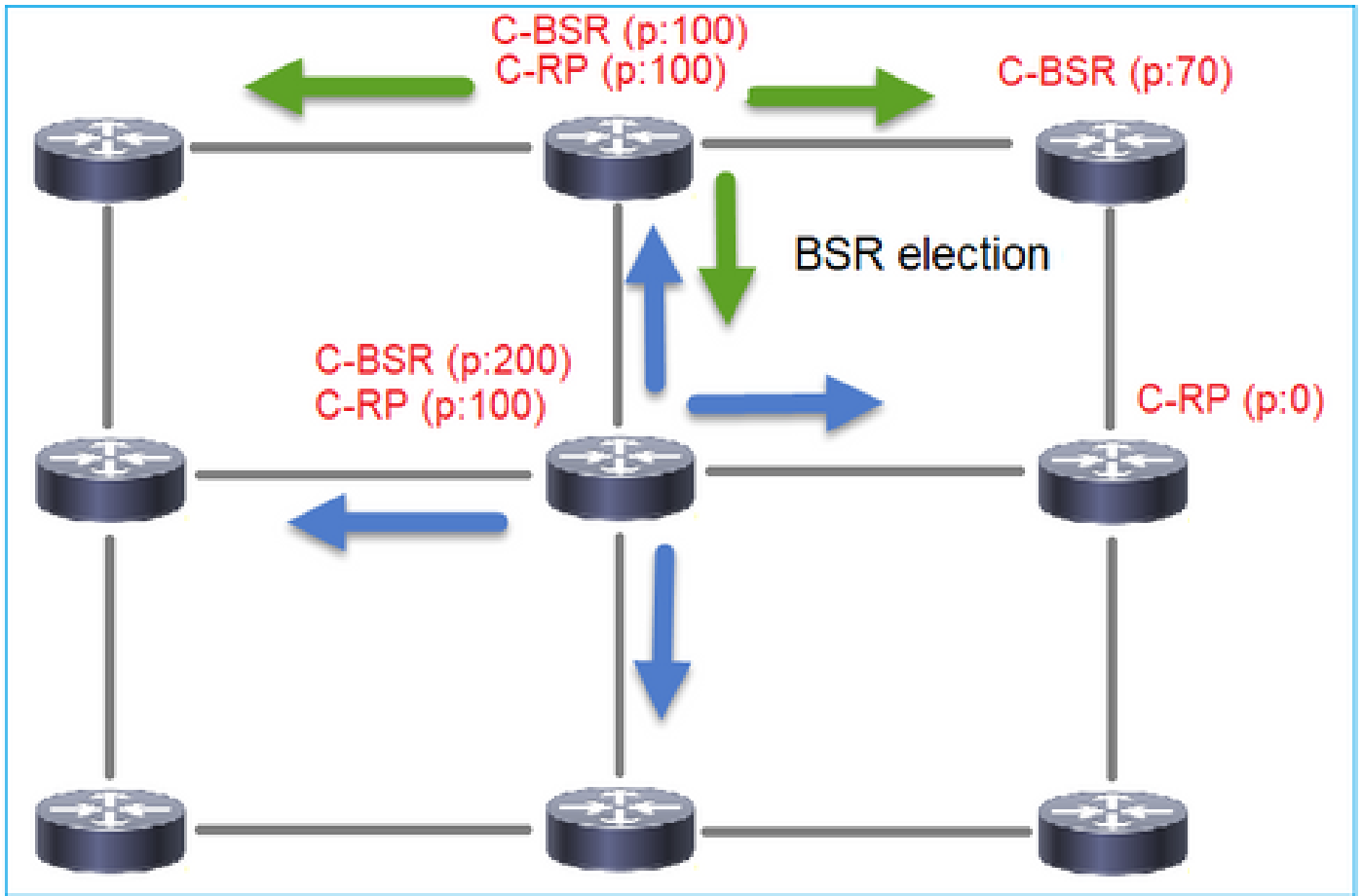
BSR 기본 사항

- BSR(RFC 5059)은 PIM 프로토콜을 사용하며 디바이스가 RP 정보를 동적으로 학습할 수 있도록 하는 컨트롤 플레인 멀티캐스트 메커니즘입니다.
- BSR 정의:
 - 후보 RP(C-RP): RP가 되기를 원하는 디바이스입니다.
 - Candidate BSR (C-BSR) : BSR이 되고자 하는 장치로 RP-sets를 다른 장치로 광고한다.
 - BSR : 많은 C-BSR들 중에서 BSR로 선정된 디바이스이다. 가장 높은 BSR 우선순위가 선거에서 승리한다.
 - RP-set: 모든 C-RP 및 해당 우선 순위의 목록입니다.
 - RP: RP 우선순위가 가장 낮은 장치가 선택에 성공합니다.
 - BSR PIM 메시지(비어 있음): BSR 선택에 사용되는 PIM 메시지입니다.
 - BSR PIM 메시지(일반): 224.0.0.13 IP로 전송되는 PIM 메시지로, RP-set 및 BSR 정보가 포함되어 있습니다.

BSR의 작동 방식

1. BSR 선출기구

각 C-BSR은 우선순위를 포함하는 빈 PIM BSR 메시지를 전송한다. 우선순위가 가장 높은 (fallback이 가장 높은 IP임) 장치가 선거에서 승리하여 BSR이 된다. 나머지 장치는 더 이상 빈 BSR 메시지를 보내지 않는다.



선거 과정에서 사용되는 BSR 메시지는 C-BSR 우선순위 정보만을 포함한다.

No.	Time	Delta	Source	Destination	Protocol	Identification	Length	Group	Info
2	6.437401	0.000000	192.168.103.50	224.0.0.13	PIMv2	0x2740 (10048)	52		Bootstrap
8	66.643725	60.206324	192.168.103.50	224.0.0.13	PIMv2	0x1559 (5465)	52		Bootstrap
13	126.850014	60.206289	192.168.103.50	224.0.0.13	PIMv2	0x0d32 (3378)	52		Bootstrap

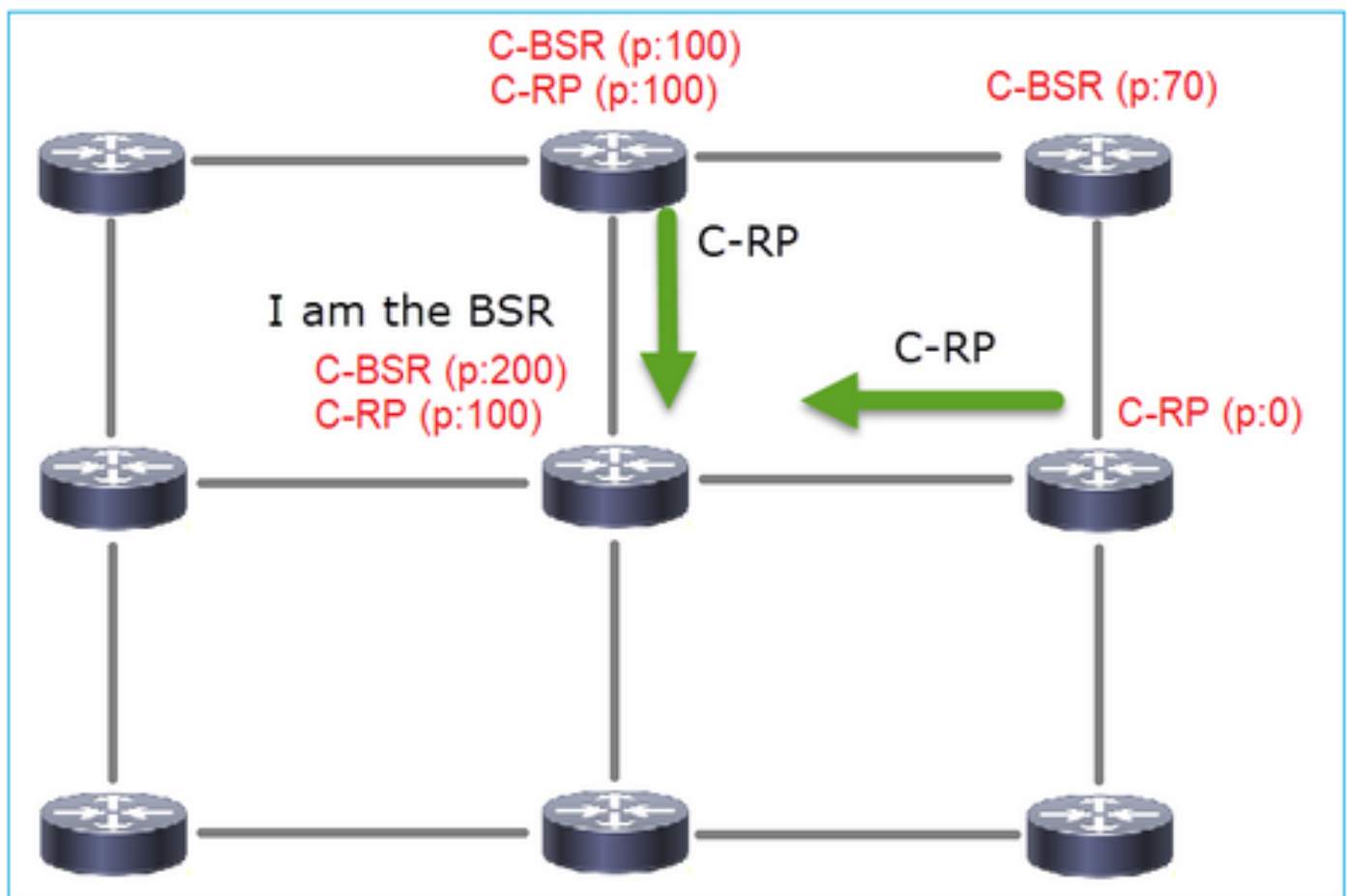

```

> Frame 2: 52 bytes on wire (416 bits), 52 bytes captured (416 bits)
> Ethernet II, Src: Cisco_33:44:5d (f4:db:e6:33:44:5d), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 206
> Internet Protocol Version 4, Src: 192.168.103.50, Dst: 224.0.0.13
v Protocol Independent Multicast
  0010 .... = Version: 2
  .... 0100 = Type: Bootstrap (4)
  Reserved byte(s): 00
  Checksum: 0x4aa9 [correct]
  [Checksum Status: Good]
v PIM Options
  Fragment tag: 0x687b
  Hash mask len: 0
  BSR priority: 0
  > BSR: 192.168.103.50

```

Wireshark에서 BSR 메시지를 표시하려면 다음 표시 필터를 사용합니다. pim.type == 4

2. C-RP는 C-RP 우선 순위가 포함된 BSR로 유니캐스트 BSR 메시지를 전송합니다.



후보 RP 메시지:

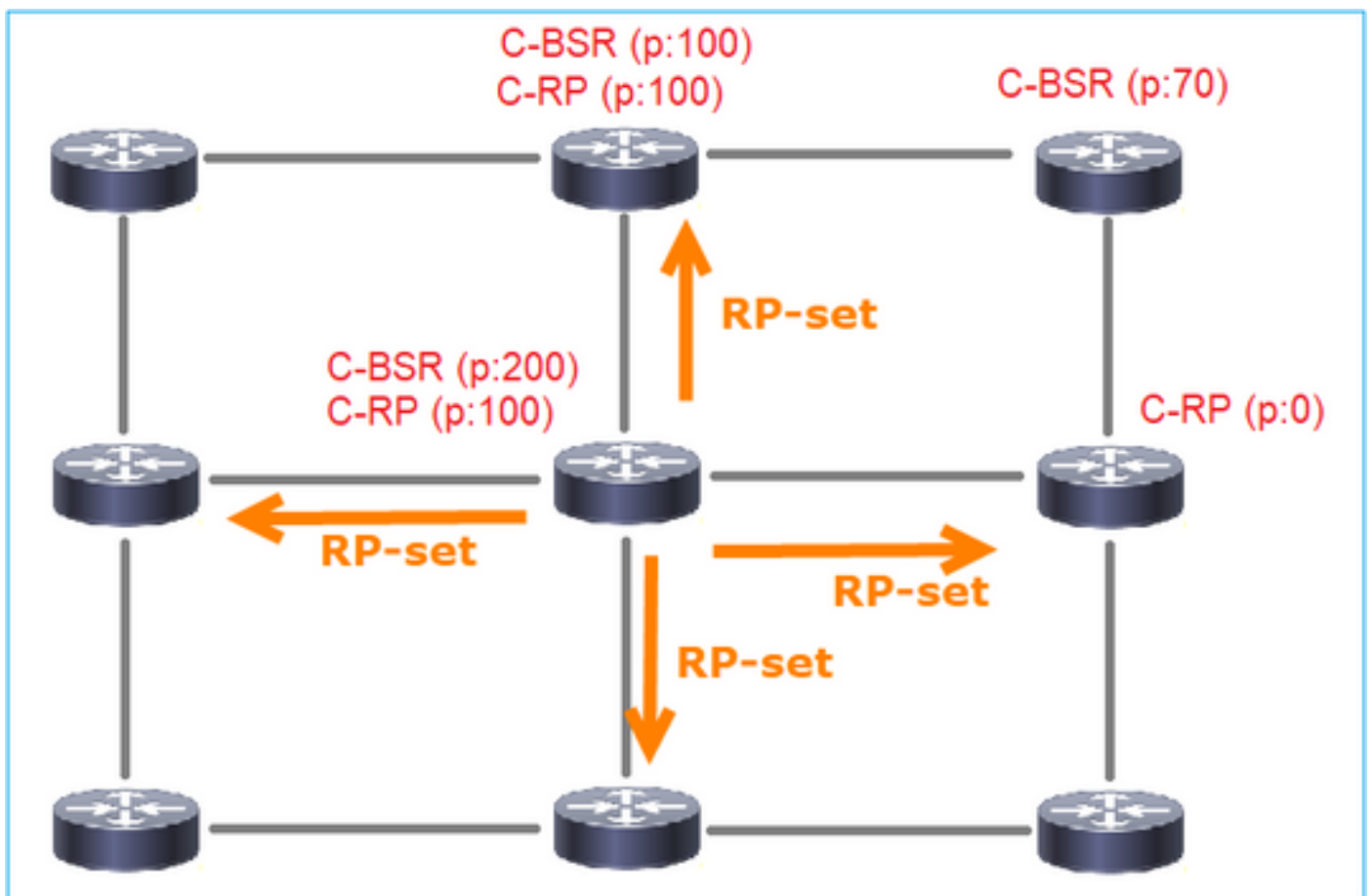
No.	Time	Delta	Source	Destination	Protocol	Identification	Length	Group	Info
35	383.703125	0.000000	192.0.2.1	192.168.103.50	PIMv2	0x4ca8 (19624)	60	224.0...	Candidate-RP-Advertisement

```

> Frame 35: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: Cisco_fc:fc:d8 (4c:4e:35:fc:fc:d8), Dst: Cisco_33:44:5d (f4:db:e6:33:44:5d)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 206
> Internet Protocol Version 4, Src: 192.0.2.1, Dst: 192.168.103.50
v Protocol Independent Multicast
  0010 .... = Version: 2
  .... 1000 = Type: Candidate-RP-Advertisement (8)
  Reserved byte(s): 00
  Checksum: 0x3263 [correct]
  [Checksum Status: Good]
  v PIM Options
    Prefix-count: 1
    Priority: 0
    Holdtime: 150
    v RP: 192.0.2.1
      Address Family: IPv4 (1)
      Encoding Type: Native (0)
      Unicast: 192.0.2.1
      v Group 0: 224.0.0.0/4
        Address Family: IPv4 (1)
        Encoding Type: Native (0)
    > Flags: 0x00
    Masklen: 4
    Group: 224.0.0.0
  
```

Wireshark에서 BSR 메시지를 표시하려면 다음 표시 필터를 사용합니다. `pim.type == 8`

3. BSR은 RP-set을 구성하고 모든 PIM 네이버에 광고합니다.



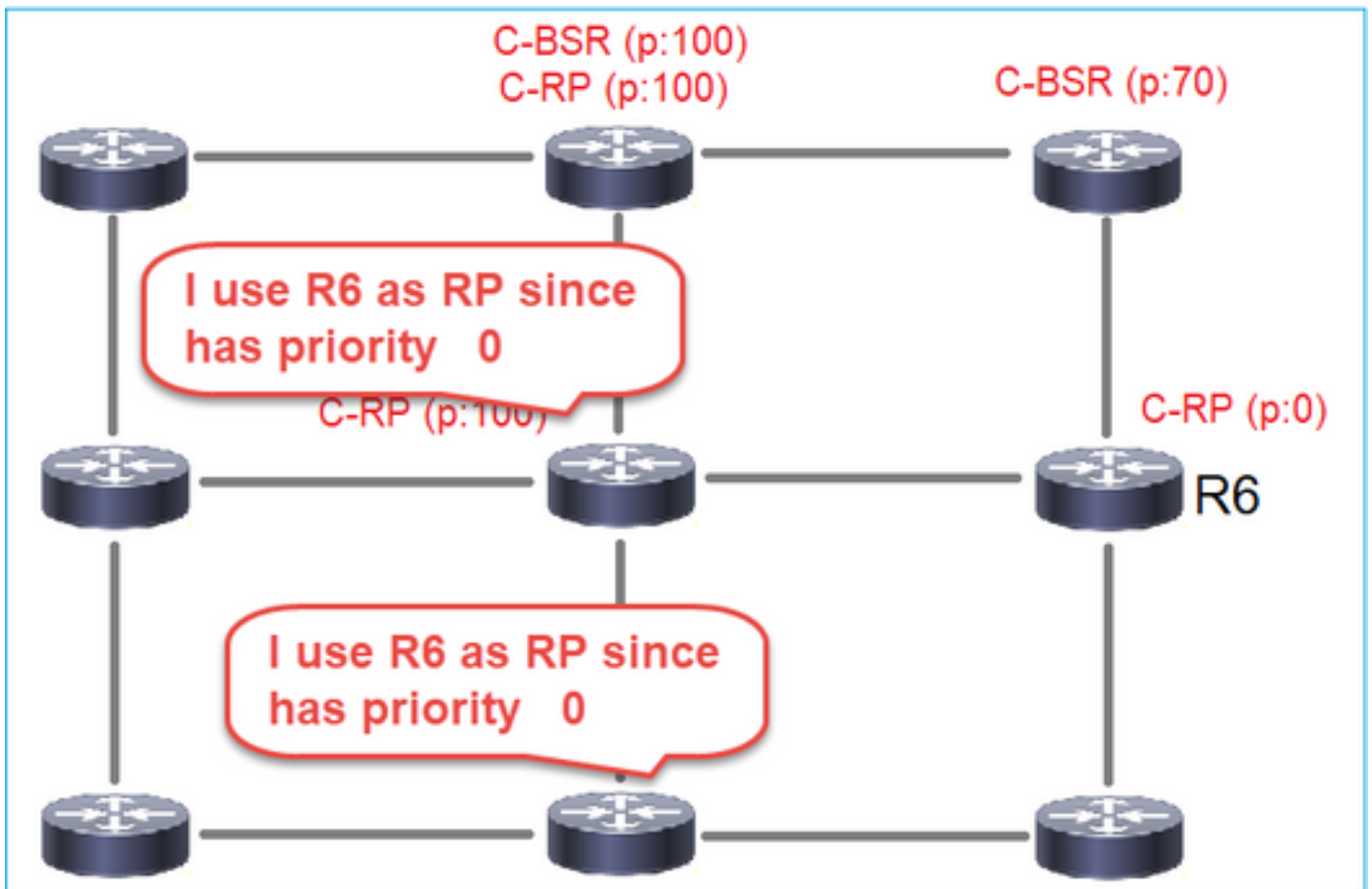
```

(ip.src == 192.168.105.60) && (pim.type == 4)
No.    Time           Delta           Source           Destination      Protocol  Identification  Length  Group           Info
-----
152 747.108256      1.001297 192.168.105.60  224.0.0.13      PIMv2     0x0bec (3052)    84     224.0.0.0,224.0.0.0  Bootstrap

<
> Frame 152: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
> Ethernet II, Src: Cisco_33:44:5d (f4:db:e6:33:44:5d), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
> 802.1Q Virtual LAN, PRI: 6, DEI: 0, ID: 207
> Internet Protocol Version 4, Src: 192.168.105.60, Dst: 224.0.0.13
v Protocol Independent Multicast
  0010 .... = Version: 2
  .... 0100 = Type: Bootstrap (4)
  Reserved byte(s): 00
  Checksum: 0x264f [correct]
  [Checksum Status: Good]
  v PIM Options
    Fragment tag: 0x2412
    Hash mask len: 0
    BSR priority: 100
    > BSR: 192.0.2.2
  v Group 0: 224.0.0.0/4
    Address Family: IPv4 (1)
    Encoding Type: Native (0)
    > Flags: 0x00
    Masklen: 4
    Group: 224.0.0.0
    RP count: 2
    FRP count: 2
    Priority: 0
    Priority: 100
    > RP 0: 192.0.2.1
    Holdtime: 150
    > RP 1: 192.0.2.2
    Holdtime: 150
    Reserved byte(s): 00
    Reserved byte(s): 00

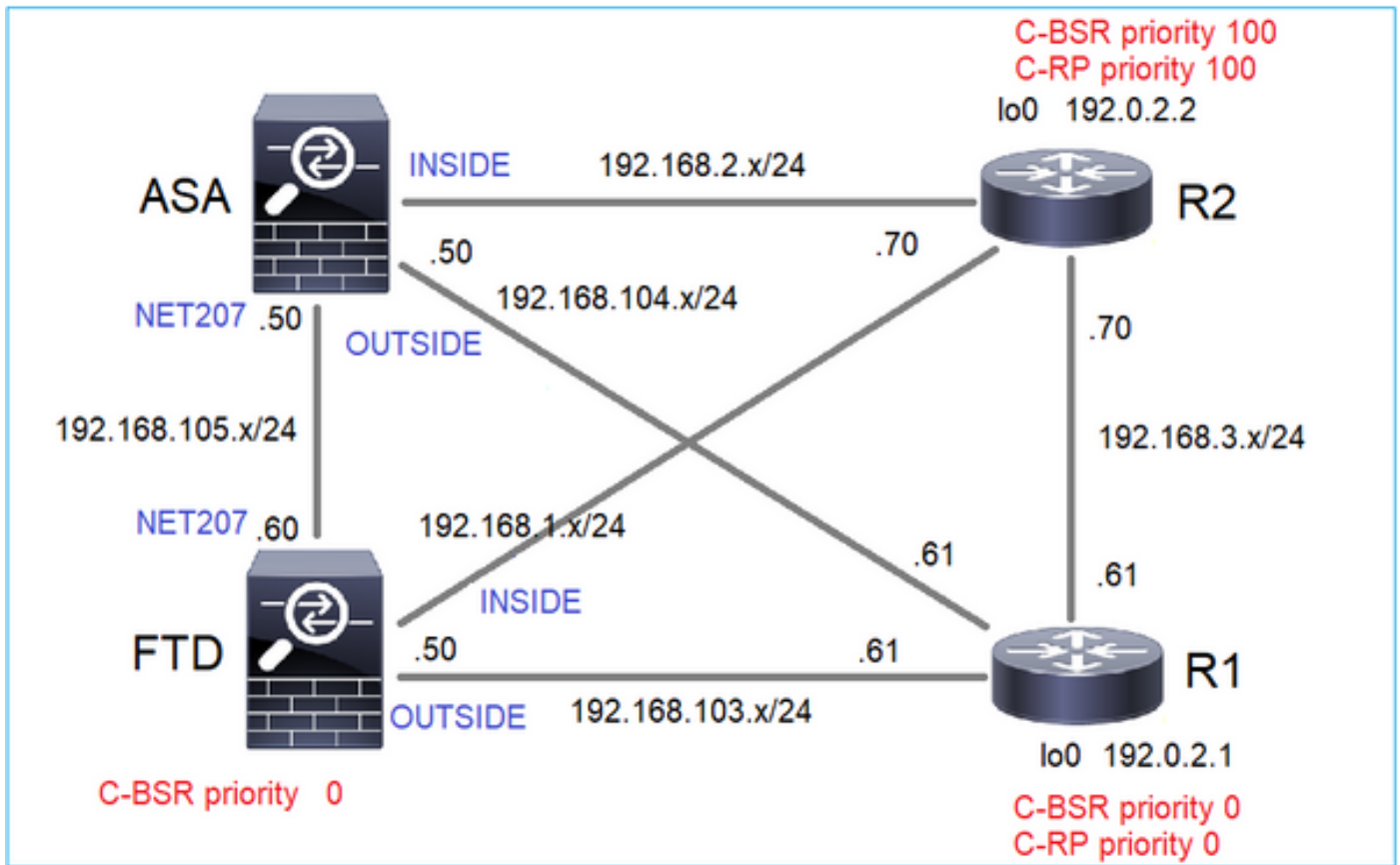
```

4. 라우터/방화벽이 RP 세트를 가져오고 가장 낮은 우선순위에 따라 RP를 선택합니다.



작업 요구 사항

이 토폴로지에 따라 C-BSR 및 C-RP를 구성합니다.



이 작업을 위해 FTD는 BSR priority 0으로 OUTSIDE 인터페이스의 C-BSR로 자신을 발표해야 합니다.

솔루션

FTD에 대한 FMC 구성:

구축된 컨피그레이션:

```
multicast-routing
!
pim bsr-candidate OUTSIDE 0 0
```

다른 디바이스의 컨피그레이션:

```
R1

ip multicast-routing
ip pim bsr-candidate Loopback0 0
ip pim rp-candidate Loopback0
!
interface Loopback0
 ip address 192.0.2.1 255.255.255.255
 ip pim sparse-mode
!
! PIM is also enabled on the transit interfaces (e.g. G0/0.203, G0/0.207, G0/0.205)
```

R2에서도 동일하지만 C-BSR 및 C-RP 우선 순위가 다름

```
ip pim bsr-candidate Loopback0 0 100
ip pim rp-candidate Loopback0 priority 100
```

ASA에서는 전역적으로 활성화된 멀티캐스트만 있습니다. 이렇게 하면 모든 인터페이스에서 PIM이 활성화됩니다.

```
multicast-routing
```

확인

R2는 가장 높은 우선순위로 인해 선출된 BSR입니다.

```
<#root>
```

```
firepower#
```

```
show pim bsr-router
```

```
PIMv2 BSR information
```

```
BSR Election Information
```

```
BSR Address: 192.0.2.2          <-- This is the IP of the BSR (R1 lo0)
```

```
Uptime: 00:03:35, BSR Priority: 100
```

```
,
```

```
Hash mask length: 0
```

```
RPF: 192.168.1.70,INSIDE
```

```
<-- The interface to the BSR
```

```
BS Timer: 00:01:34
```

```
This system is candidate BSR
```

```
Candidate BSR address: 192.168.103.50, priority: 0, hash mask length: 0
```

R1은 우선순위가 가장 낮아 RP로 선택됩니다.

```
<#root>
```

```
firepower#
```

```
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

*

SM

BSR

0

192.0.2.1

RPF: OUTSIDE,192.168.103.61

<-- The elected BSR

224.0.0.0/4	SM	BSR	0	192.0.2.2	RPF: INSIDE,192.168.1.70
224.0.0.0/4	SM	static	0	0.0.0.0	RPF: ,0.0.0.0

BSR 메시지는 RPF 검사를 받습니다. debug pim bsr을 활성화하여 다음을 확인할 수 있습니다.

<#root>

IPv4 BSR: Received BSR message from 192.168.105.50 for 192.0.2.2, BSR priority 100 hash mask length 0
IPv4 BSR:

BSR message

from 192.168.105.50/

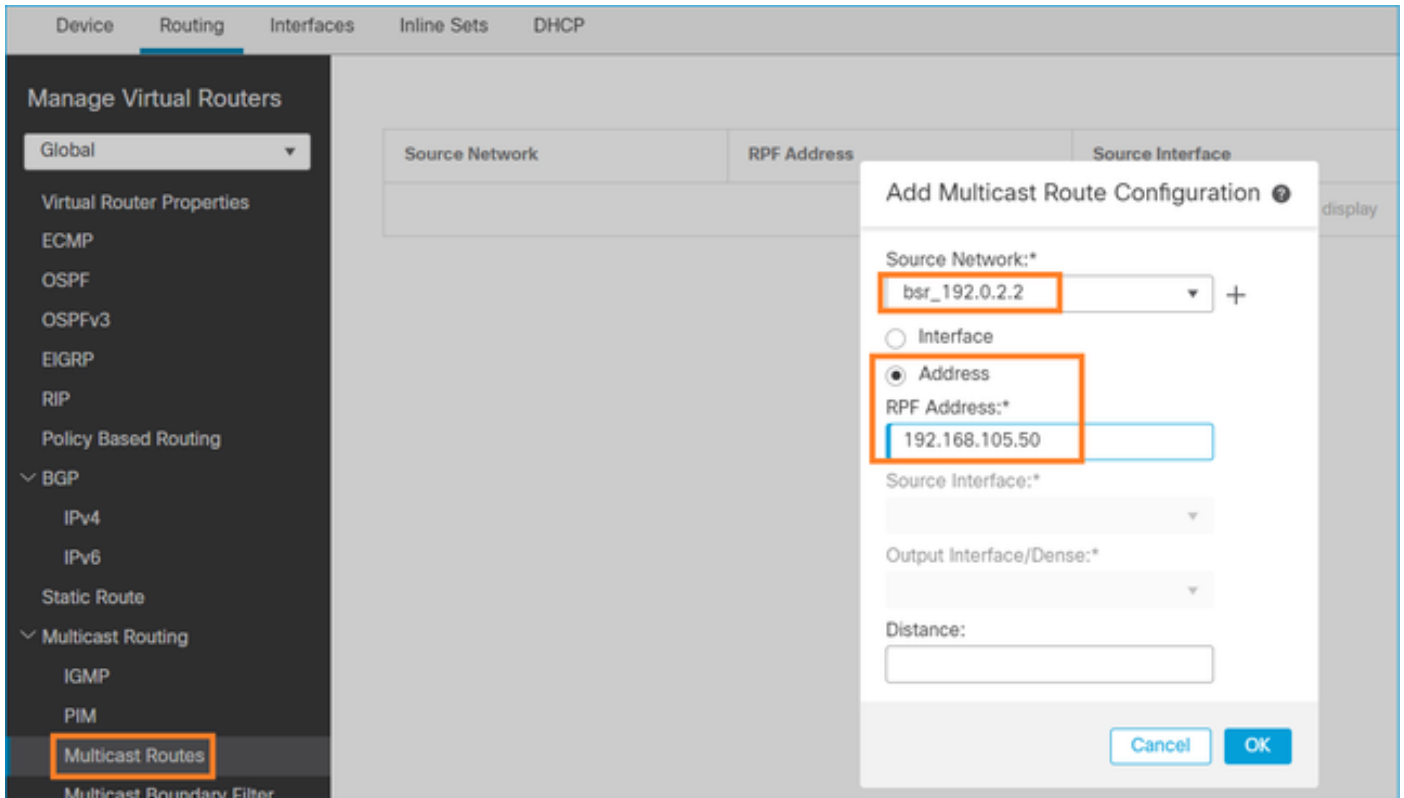
NET207

for 192.0.2.2

RPF failed, dropped

<-- The RPF check for the received BSR message failed

RPF 인터페이스를 변경하려면 고정 mroute를 구성할 수 있습니다. 이 예에서 방화벽은 IP 192.168.105.50의 BSR 메시지를 수락합니다.



```
<#root>
```

```
firepower#
```

```
show run mroute
```

```
mroute 192.0.2.2 255.255.255.255 192.168.105.50
```

```
<#root>
```

```
firepower#
```

```
show pim bsr-router
```

```
PIMv2 BSR information
```

```
BSR Election Information
```

```
BSR Address: 192.0.2.2
```

```
Uptime: 01:21:38, BSR Priority: 100, Hash mask length: 0
```

```
RPF: 192.168.105.50,NET207
```

```
<-- The RPF check points to the static mroute
```

```
BS Timer: 00:01:37
```

```
This system is candidate BSR
```

```
Candidate BSR address: 192.168.103.50, priority: 0, hash mask length: 0
```

이제 NET207 인터페이스의 BSR 메시지는 수락되지만 INSIDE에서는 삭제됩니다.

```
<#root>
```

```
IPv4 BSR: Received BSR message from 192.168.1.70 for 192.0.2.2, BSR priority 100 hash mask length 0
```

```
IPv4 BSR: BSR message from 192.168.1.70/INSIDE for 192.0.2.2 RPF failed, dropped
```

```
...
```

```
IPv4 BSR: Received BSR message from 192.168.105.50 for 192.0.2.2, BSR priority 100 hash mask length 0
```

```
<-- RPF check is OK
```

방화벽에서 trace를 통한 capture를 활성화하고 BSR 메시지가 처리되는 방식을 확인합니다.

```
<#root>
```

```
firepower#
```

```
show capture
```

```
capture CAPI type raw-data trace interface INSIDE [Capturing - 276 bytes]  
  match pim any any
```

```
capture CAPO type raw-data trace interface OUTSIDE [Capturing - 176 bytes]  
  match pim any any
```

PIM 연결은 방화벽에서 종료되므로 추적에서 유용한 정보를 표시하려면 상자에 대한 연결을 지워야 합니다.

```
<#root>
```

```
firepower#
```

```
show conn all | i PIM
```

```
firepower# show conn all | include PIM
```

```
PIM OUTSIDE 192.168.103.61 NP Identity Ifc 224.0.0.13, idle 0:00:23, bytes 116802, flags
```

```
PIM NET207 192.168.104.50 NP Identity Ifc 224.0.0.13, idle 0:00:17, bytes 307296, flags
```

```
PIM NET207 192.168.104.61 NP Identity Ifc 224.0.0.13, idle 0:00:01, bytes 184544, flags
```

```
PIM NET207 192.168.105.50 NP Identity Ifc 224.0.0.13, idle 0:00:18, bytes 120248, flags
```

```
PIM INSIDE 192.168.1.70 NP Identity Ifc 224.0.0.13, idle 0:00:27, bytes 15334, flags
```

```
PIM OUTSIDE 224.0.0.13 NP Identity Ifc 192.168.103.50, idle 0:00:21, bytes 460834, flags
```

```
PIM INSIDE 224.0.0.13 NP Identity Ifc 192.168.1.50, idle 0:00:00, bytes 441106, flags
```

```
PIM NET207 224.0.0.13 NP Identity Ifc 192.168.105.60, idle 0:00:09, bytes 458462, flags
```

```
firepower#
```

```
clear conn all addr 224.0.0.13
```

```
8 connection(s) deleted.
```

```
firepower#
```

```
clear cap /all
```

<#root>

firepower#

show capture CAPI packet-number 2 trace

6 packets captured

2: 11:31:44.390421 802.1Q vlan#205 P6

192.168.1.70 > 224.0.0.13

ip-proto-103, length 38

<-- Ingress PIM packet

Phase: 1

Type: CAPTURE

Subtype:

Result: ALLOW

Elapsed time: 4880 ns

Config:

Additional Information:

MAC Access list

Phase: 2

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Elapsed time: 4880 ns

Config:

Implicit Rule

Additional Information:

MAC Access list

Phase: 3

Type: ROUTE-LOOKUP

Subtype: No ECMP load balancing

Result: ALLOW

Elapsed time: 9760 ns

Config:

Additional Information:

Destination is locally connected. No ECMP load balancing.

Found next-hop 192.168.1.70 using egress ifc INSIDE(vrfid:0)

Phase: 4

Type: CLUSTER-DROP-ON-SLAVE

Subtype: cluster-drop-on-slave

Result: ALLOW

Elapsed time: 4392 ns

Config:

Additional Information:

Phase: 5

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Elapsed time: 4392 ns

Config:

Implicit Rule

Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Elapsed time: 4392 ns
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Elapsed time: 4392 ns
Config:
Additional Information:

Phase: 8
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Elapsed time: 18056 ns
Config:
Additional Information:

Phase: 9

Type: MULTICAST <-- The multicast process

Subtype: pim

Result: ALLOW
Elapsed time: 976 ns
Config:
Additional Information:

Phase: 10
Type: MULTICAST
Subtype:
Result: ALLOW
Elapsed time: 488 ns
Config:
Additional Information:

Phase: 11
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 20008 ns
Config:
Additional Information:
New flow created with id 25630, packet dispatched to next module

Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
output-interface: INSIDE(vrfid:0)
output-status: up

output-line-status: up

Action: allow

Time Taken: 76616 ns

RPF 실패로 인해 PIM 패킷이 삭제되면 추적은 다음과 같이 표시됩니다.

<#root>

firepower#

show capture NET207 packet-number 4 trace

85 packets captured

4: 11:31:42.385951 802.1Q vlan#207 P6

192.168.104.61 > 224.0.0.13 ip-proto-103

, length 38

<-- Ingress PIM packet

Phase: 1

Type: CAPTURE

Subtype:

Result: ALLOW

Elapsed time: 5368 ns

Config:

Additional Information:

MAC Access list

Phase: 2

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Elapsed time: 5368 ns

Config:

Implicit Rule

Additional Information:

MAC Access list

Phase: 3

Type: INPUT-ROUTE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Elapsed time: 11224 ns

Config:

Additional Information:

Found next-hop 192.168.103.61 using egress ifc OUTSIDE(vrfid:0)

Phase: 4

Type: INPUT-ROUTE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Elapsed time: 3416 ns

Config:
Additional Information:
Found next-hop 192.168.103.61 using egress ifc OUTSIDE(vrfid:0)

Result:
input-interface: NET207(vrfid:0)
input-status: up
input-line-status: up
output-interface: OUTSIDE(vrfid:0)
output-status: up
output-line-status: up
Action: drop
Time Taken: 25376 ns

Drop-reason: (rpf-violated) Reverse-path verify failed, Drop-location: frame 0x0000558f240d6e15 flow (NA

<-- the packet is dropped due to RPF check failure

ASP 테이블이 삭제 및 캡처되면 다음과 같이 show RPF-failed 패킷이 표시됩니다.

<#root>

firepower#

show asp drop

Frame drop:

Reverse-path verify failed (rpf-violated)	122
<-- Multicast RPF drops	
Flow is denied by configured rule (acl-drop)	256
FP L2 rule drop (l2_acl)	768

RPF 실패로 인해 삭제된 패킷을 캡처하려면

<#root>

firepower#

capture ASP type asp-drop rpf-violated

<#root>

firepower#

show capture ASP | include 224.0.0.13

2: 11:36:20.445960 802.1Q vlan#207 P6 192.168.104.50 > 224.0.0.13 ip-proto-103, length 38
10: 11:36:38.787846 802.1Q vlan#207 P6 192.168.104.61 > 224.0.0.13 ip-proto-103, length 38

15: 11:36:48.299743 802.1Q vlan#207 P6 192.168.104.50 > 224.0.0.13 ip-proto-103, length 46
16: 11:36:48.300063 802.1Q vlan#207 P6 192.168.104.61 > 224.0.0.13 ip-proto-103, length 46

문제 해결 방법론

방화벽에 대한 트러블슈팅 방법론은 주로 멀티캐스트 토폴로지에서 방화벽의 역할에 따라 달라집니다. 문제 해결을 위한 권장 단계 목록입니다.

1. 문제 설명 및 증상에 대한 자세한 내용을 명확히 합니다. 범위를 컨트롤 플레인(IGMP/PIM) 또는 데이터 플레인(멀티캐스트 스트림) 문제로 좁혀 보십시오.
2. 방화벽에서 멀티캐스트 문제를 트러블슈팅하기 위한 필수 전제 조건은 멀티캐스트 토폴로지를 명확히 하는 것입니다. 최소한 다음 사항을 확인해야 합니다.
 - 멀티캐스트 토폴로지에서 방화벽의 역할 - FHR, LHR, RP 또는 다른 중간 역할.
 - 방화벽에 멀티캐스트 인그레스 및 이그레스 인터페이스가 필요합니다.
 - RP.
 - 발신자 소스 IP 주소.
 - 멀티캐스트는 IP 주소 및 목적지 포트를 그룹화합니다.
 - 멀티캐스트 스트림의 수신기입니다.
3. 멀티캐스트 라우팅 유형(Stub 또는 PIM 멀티캐스트 라우팅)을 식별합니다.
 - Stub 멀티캐스트 라우팅 - 동적 호스트 등록을 제공하고 멀티캐스트 라우팅을 용이하게 합니다. stub 멀티캐스트 라우팅에 대해 구성된 경우 ASA는 IGMP 프록시 에이전트 역할을 합니다. ASA는 멀티캐스트 라우팅에 완전히 참여하는 대신 IGMP 메시지를 업스트림 멀티캐스트 라우터로 전달합니다. 업스트림 멀티캐스트 라우터는 멀티캐스트 데이터 전달을 설정합니다. stub 모드 라우팅을 식별하려면 show igmp interface 명령을 사용하고 IGMP forward 컨피그 레이션을 확인합니다.

<#root>

firepower#

show igmp interface

```
inside is up, line protocol is up
  Internet address is 192.168.2.2/24
  IGMP is disabled on interface
outside is up, line protocol is up
  Internet address is 192.168.3.1/24
  IGMP is enabled on interface
  Current IGMP version is 2
  IGMP query interval is 125 seconds
  IGMP querier timeout is 255 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1 seconds
  Inbound IGMP access group is:
  IGMP limit is 500, currently active joins: 0
  Cumulative IGMP activity: 0 joins, 0 leaves
```

IGMP forwarding on interface inside

IGMP querying router is 192.168.3.1 (this system)

PIM은 인터페이스에서 활성화되지만 인접 관계가 설정되지 않습니다.

<#root>

firepower#

show pim interface

Address	Interface	PIM	Nbr Count	Hello Intvl	DR Prior	DR
192.168.2.2	inside	on	0	30	1	this system
192.168.3.1	outside	on	0	30	1	this system

firepower# show pim neighbor

No neighbors found.

PIM-SM/Bidir 및 IGMP 전달은 동시에 지원되지 않습니다.

RP 주소와 같은 옵션은 구성할 수 없습니다.

<#root>

%Error: PIM-SM/Bidir and IGMP forwarding are not supported concurrently

- PIM 멀티캐스트 라우팅 - PIM 멀티캐스트 라우팅이 가장 일반적인 구축입니다. 방화벽은 PIM-SM 및 양방향 PIM을 모두 지원합니다. PIM-SM은 기본 유니캐스트 라우팅 정보 기반 또는 별도의 멀티캐스트 지원 라우팅 정보 기반을 사용하는 멀티캐스트 라우팅 프로토콜입니다. 멀티캐스트 그룹당 단일 RP(Rendezvous Point)에 루트가 있는 단방향 공유 트리를 구축하고 선택적으로 멀티캐스트 소스당 최단 경로 트리를 생성합니다. 이 구축 모드에서는 stub 모드와 달리 사용자가 일반적으로 RP 주소 컨피그레이션을 구성하며, 방화벽은 피어와의 PIM 인접성을 설정합니다.

<#root>

firepower#

show run pim

pim rp-address 10.10.10.1

firepower#

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*    SM     config  1       10.10.10.1  RPF: inside,192.168.2.1 <--- RP address is 10.10.10.1

224.0.0.0/4     SM     static  0       0.0.0.0     RPF: ,0.0.0.0

```

firepower#

show pim neighbor

```

Neighbor Address  Interface      Uptime    Expires DR pri Bidir
192.168.2.1      inside         00:02:52  00:01:19 1
192.168.3.100   outside        00:03:03  00:01:39 1 (DR)

```

4. RP IP 주소가 구성되고 도달 가능성이 있는지 확인합니다.

<#root>

firepower#

show run pim

```
pim rp-address 10.10.10.1
```

firepower#

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*    SM     config  1       10.10.10.1  RPF: inside,192.168.2.1 <--- RP is 10.10.10.1

224.0.0.0/4     SM     static  0       0.0.0.0     RPF: ,0.0.0.0

```

<#root>

firepower#

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*    SM      config  1      192.168.2.2    RPF: Tunnel0,192.168.2.2 (us) <--- "us" mean

224.0.0.0/4     SM      static  0      0.0.0.0        RPF: ,0.0.0.0

```

 경고: 방화벽은 동시에 RP와 FHR이 될 수 없습니다.

5. 멀티캐스트 토폴로지에서 방화벽의 역할과 문제 증상에 따라 추가 출력을 확인합니다.

FHR

- 인터페이스 Tunnel0 상태를 확인합니다. 이 인터페이스는 PIM 페이로드 내부의 원시 멀티캐스트 트래픽을 캡슐화하고 PIM 레지스터 비트 집합이 있는 RP에 유니캐스트 패킷을 전송하는 데 사용됩니다.

<#root>

firepower#

show interface detail | b Interface Tunnel0

```
Interface Tunnel0 "", is up, line protocol is up
```

```

Hardware is Available but not configured via nameif
  MAC address 0000.0000.0000, MTU not set
  IP address unassigned
Control Point Interface States:
  Interface number is un-assigned
  Interface config status is active
  Interface state is active

```

firepower#

show pim tunnel

```

Interface      RP Address      Source Address
Tunnel0       10.10.10.1     192.168.2.2

```

- mroutes 확인:

<#root>

firepower#

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

(192.168.2.1, 230.1.1.1), 00:00:07/00:03:22, flags: SFT

Incoming interface: inside

RPF nbr: 192.168.2.1, Registering <--- Registering state

Immediate Outgoing interface list:

outside, Forward, 00:00:07/00:03:26

Tunnel0, Forward, 00:00:07/never <--- Tunnel0 is in OIL, that indicates raw traffic is encapsulated.

방화벽이 Register-Stop 비트가 포함된 PIM 패킷을 수신하면 Tunnel0이 OIL에서 제거됩니다. 그런 다음 방화벽은 캡슐화를 중지하고 이그레스 인터페이스를 통해 원시 멀티캐스트 트래픽을 전송합니다.

<#root>

firepower#

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

(192.168.2.1, 230.1.1.1), 00:07:26/00:02:59, flags: SFT

Incoming interface: inside

RPF nbr: 192.168.2.1

Immediate Outgoing interface list:

outside, Forward, 00:07:26/00:02:59

- PIM 레지스터 카운터 확인:

<#root>

firepower#

show pim traffic

PIM Traffic Counters

Elapsed time since counters cleared: 00:13:13

	Received	Sent	
Valid PIM Packets	42	58	
Hello	27	53	
Join-Prune	9	0	
Register	0	8	<--- Sent to the RP
Register Stop	6	0	<--- Received from the RP
Assert	0	0	
Bidir DF Election	0	0	
Errors:			
Malformed Packets		0	
Bad Checksums		0	
Send Errors		0	
Packet Sent on Loopback Errors		0	
Packets Received on PIM-disabled Interface		0	
Packets Received with Unknown PIM Version		0	
Packets Received with Incorrect Addressing		0	

- 방화벽과 RP 간의 유니캐스트 PIM 패킷 캡처를 확인합니다.

```
<#root>
```

```
firepower#
```

```
capture capo interface outside match pim any host 10.10.10.1 <--- RP IP
```

```
firepower#
```

```
show capture capi
```

```
4 packets captured
```

```
1: 09:53:28.097559      192.168.3.1 > 10.10.10.1  ip-proto-103, length 50      <--- Unicast to RP
2: 09:53:32.089167      192.168.3.1 > 10.10.10.1  ip-proto-103, length 50
3: 09:53:37.092890      192.168.3.1 > 10.10.10.1  ip-proto-103, length 50
4: 09:53:37.095850      10.10.10.1 > 192.168.3.1  ip-proto-103, length 18      <--- Unicast from RP
```

- 추가 출력을 수집합니다(x.x.x.x는 멀티캐스트 그룹, y.y.y.y는 RP IP). 출력을 몇 번 수집하는 것이 좋습니다.

<#root>

show conn all protocol udp address x.x.x.x

show local-host x.x.x.x

show asp event dp-cp

show asp drop

show asp cluster counter

show asp table routing y.y.y.y

show route y.y.y.y

show mroute

show pim interface

show pim neighbor

show pim traffic

show igmp interface

show mfib count

- 원시 멀티캐스트 인터페이스 패킷 및 ASP 삭제 캡처를 수집합니다.

<#root>

capture capi interface

buffer 32000000 match udp host X host Z <--- (ingress capture for multicast UDP traffic from host

```
capture capo interface
```

```
buffer 32000000 match udp host X host Z <--- (egress capture for multicast UDP traffic from host X)
```

```
capture asp type asp-drop buffer 32000000 match udp host X host Z <--- (ASP drop capture for multicast U
```

- Syslog 메시지 - 공통 ID는 302015, 302016 및 710005.

RP

- 인터페이스 Tunnel0 상태를 확인합니다. 이 인터페이스는 PIM 페이로드 내의 원시 멀티캐스트 트래픽을 캡슐화하고 PIM-stop 비트 집합이 있는 FHR에 유니캐스트 패킷을 전송하는 데 사용됩니다.

```
<#root>
```

```
firepower#
```

```
show interface detail | b Interface Tunnel0
```

```
Interface Tunnel0 "", is up, line protocol is up
```

```
Hardware is Available but not configured via nameif
MAC address 0000.0000.0000, MTU not set
IP address unassigned
```

```
Control Point Interface States:
Interface number is un-assigned
Interface config status is active
Interface state is active
```

```
firepower#
```

```
show pim tunnel
```

```
Interface          RP Address          Source Address
```

```
Tunnel0          192.168.2.2      192.168.2.2
```

```
Tunnel0          192.168.2.2      -
```

- mroutes 확인:

```
<#root>
```

```
firepower#
```

```
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
```

```
(* , 230.1.1.1), 01:04:30/00:02:50, RP 192.168.2.2, flags: S <--- *,G entry
```

```
Incoming interface: Tunnel0
```

```
RPF nbr: 192.168.2.2
```

```
Immediate Outgoing interface list:
```

```
outside
```

```
, Forward, 01:04:30/00:02:50
```

```
(192.168.1.100, 230.1.1.1), 00:00:04/00:03:28, flags: ST S <--- S,G entry
```

```
Incoming interface:
```

```
inside
```

```
RPF nbr: 192.168.2.1
```

```
Immediate Outgoing interface list:
```

```
outside, Forward, 00:00:03/00:03:25
```

- PIM 카운터 확인:

```
<#root>
```

```
firepower #
```

```
show pim traffic
```

```
PIM Traffic Counters
```

```
Elapsed time since counters cleared: 02:24:37
```

	Received	Sent
Valid PIM Packets	948	755
Hello	467	584
Join-Prune	125	32
Register	344	16
Register Stop	12	129
Assert	0	0
Bidir DF Election	0	0
Errors:		
Malformed Packets		0
Bad Checksums		0
Send Errors		0
Packet Sent on Loopback Errors		0
Packets Received on PIM-disabled Interface		0
Packets Received with Unknown PIM Version		0
Packets Received with Incorrect Addressing		0

- 추가 출력을 수집합니다(x.x.x.x는 멀티캐스트 그룹, y.y.y.y는 RP IP). 출력을 몇 번 수집하는 것이 좋습니다.

```
<#root>
```

```
show conn all protocol udp address x.x.x.x
```

```
show conn all | i PIM
```

```
show local-host x.x.x.x
```

```
show asp event dp-cp
```

```
show asp drop
```



```
show asp cluster counter
```

```
show asp table routing y.y.y.y
```

```
show route y.y.y.y
```

```
show mroute
```

```
show pim interface
```

```
show pim neighbor
```

```
show igmp interface
```

```
show mfib count
```

- 원시 멀티캐스트 인터페이스 패킷 및 ASP 삭제 캡처를 수집합니다.

```
<#root>
```

```
capture capi interface
```

```
buffer 32000000 match udp host X host Z <--- (ingress capture for multicast UDP traffic from host X)
```

```
capture capo interface
```

```
buffer 32000000 match udp host X host Z <--- (egress capture for multicast UDP traffic from host X)
```

```
capture asp type asp-drop buffer 3200000 match udp host X host Z <--- (ASP drop capture for multicast U
```

- Syslog - 공통 ID는 302015, 302016 및 710005.

LHR

RP 및 이러한 추가 확인에 대한 섹션에서 설명한 단계를 고려하십시오.

- Mroutes:

```
<#root>
```

```
firepower#
```

```
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
```

```
(* , 230.1.1.1), 00:23:30/never, RP 10.10.10.1, flags: SCJ <--- C flag means connected receiver
```

```
Incoming interface:
```

```
inside
```

```
RPF nbr: 192.168.2.1
```

```
Immediate Outgoing interface list:
```

```
outside
```

```
, Forward, 00:23:30/never
```

```
(192.168.1.100, 230.1.1.1), 00:00:36/00:03:04, flags: SJT <--- J flag indicates switchover to SPT, T fla
```

```
Incoming interface:
```

```
inside
```

```
RPF nbr: 192.168.2.1
```

```
Inherited Outgoing interface list:
```

outside

, Forward, 00:23:30/never

(* , 230.1.1.2), 00:01:50/never, RP 10.10.10.1, flags: SCJ <--- C flag means connected receiver

Incoming interface:

inside

RPF nbr: 192.168.2.1

Immediate Outgoing interface list:

outside

, Forward, 00:01:50/never

(192.168.1.100, 230.1.1.2), 00:00:10/00:03:29, flags: SJT <--- <--- J flag indicates switchover to SPT,

Incoming interface:

inside

RPF nbr: 192.168.2.1

Inherited Outgoing interface list:

outside

, Forward, 00:01:50/never

- IGMP 그룹:

<#root>

firepower#

show igmp groups detail <--- The list of IGMP groups

Interface: outside

Group: 230.1.1.1

Uptime: 00:21:42

Router mode: EXCLUDE (Expires: 00:03:17)

Host mode: INCLUDE

Last reporter: 192.168.3.100 <--- Host joined group 230.1.1.1

Source list is empty

Interface: outside

Group: 230.1.1.2

```

Uptime:          00:00:02
Router mode:     EXCLUDE (Expires: 00:04:17)
Host mode:       INCLUDE

Last reporter:  192.168.3.101 <--- Host joined group 230.1.1.2

```

Source list is empty

- IGMP 트래픽 통계:

```
<#root>
```

```
firepower#
```

```
show igmp traffic
```

```
IGMP Traffic Counters
Elapsed time since counters cleared: 1d04h
```

	Received	Sent
Valid IGMP Packets	2468	856
Queries	2448	856
Reports	20	0
Leaves	0	0
Mtrace packets	0	0
DVMRP packets	0	0
PIM packets	0	0

```
Errors:
```

Malformed Packets	0
Martian source	0
Bad Checksums	0

PIM 트러블슈팅 명령(치트 시트)

명령을 사용합니다	설명
show running-config 멀티캐스트 라우팅	방화벽에서 멀티캐스트 라우팅이 활성화되어 있는지 확인하려면
show run mroute	방화벽에 구성된 고정 경로를 보려면
show running-config pim	방화벽의 PIM 컨피그레이션을 보려면

show pim 인터페이스	PIM이 활성화된 방화벽 인터페이스 및 PIM 네이버를 확인합니다.
show pim neighbor	PIM 네이버를 보려면
show pim group-map	RP에 매핑된 멀티캐스트 그룹을 보려면
mroute 표시	전체 멀티캐스트 라우팅 테이블을 보려면
mroute 230.10.10.10 표시	특정 멀티캐스트 그룹에 대한 멀티캐스트 테이블을 보려면
show pim tunnel	방화벽과 RP 사이에 PIM 터널이 구축되어 있는지 확인합니다.
show conn all detail address RP_IP_ADDRESS	방화벽과 RP 사이에 연결(PIM 터널)이 설정되어 있는지 확인
show pim 토폴로지	방화벽 PIM 토폴로지 출력을 보려면
디버그 pim	이 디버그는 방화벽에서 보내고 받는 모든 PIM 메시지를 표시합니다
디버그 pim 그룹 230.10.10	이 디버그는 특정 멀티캐스트 그룹의 방화벽에서 보내고 받는 모든 PIM 메시지를 표시합니다
show pim traffic	수신 및 전송된 PIM 메시지에 대한 통계를 보려면
show asp cluster 카운터	느린 경로 대 빠른 경로 대 제어 지점에서 처리되는 패킷 수 확인
asp 드롭 표시	방화벽의 모든 소프트웨어 레벨 삭제를 보려면
capture CAP interface INSIDE trace match pim any	방화벽에서 인그레스 PIM 멀티캐스트 패킷을 캡처 및 추적하려면

capture CAP interface INSIDE trace match udp host 224.1.2.3 any	인그레스 멀티캐스트 스트림을 캡처 및 추적하려면
show pim bsr-router	누가 선출된 BSR 라우터인지 확인하기
show conn all address 224.1.2.3	상위 멀티캐스트 연결을 표시하려면
show local-host 224.1.2.3	하위/스텝 멀티캐스트 연결 표시

방화벽 캡처 확인에 대한 자세한 내용: [Firepower Threat Defense 캡처 및 패킷 추적기 사용](#)

알려진 문제

Firepower 멀티캐스트 제한 사항:

- IPv6을 지원하지 않습니다.
- PIM/IGMP 멀티캐스트는 EMCP(트래픽 영역)의 인터페이스에서 지원되지 않습니다.
- 방화벽은 동시에 RP와 FHR이 될 수 없습니다.
- show conn all 명령은 ID 멀티캐스트 연결만 표시합니다. stub/secondary 멀티캐스트 연결을 표시하려면 show local-host <group IP> 명령을 사용합니다.

vPC Nexus에서 PIM이 지원되지 않음

Nexus vPC와 방화벽 간에 PIM 인접성을 구축하려고 하면 여기에 설명된 대로 Nexus 제한이 있습니다.

[Nexus 플랫폼에서 가상 포트 채널을 통한 라우팅에 대해 지원되는 토폴로지](#)

NGFW 관점에서 보면 capture with trace this drop이 표시됩니다.

```
<#root>
```

```
Result:
```

```
input-interface: NET102
```

```
input-status: up
```

```
input-line-status: up
```

```
output-interface: NET102
```

```
output-status: up
```

```
output-line-status: up
```

```
Action: drop
```

```
Drop-reason: (no-mcast-intrf) FP no mcast output intrf      <-- The ingress multicast packet is dropped
```

방화벽에서 RP 등록을 완료할 수 없습니다.

<#root>

firepower#

show mroute 224.1.2.3

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

(* , 224.1.2.3), 01:05:21/never, RP 10.1.0.209, flags: SCJ

Incoming interface: OUTSIDE

RPF nbr: 10.1.104.10

Immediate Outgoing interface list:

Server_102, Forward, 01:05:21/never

(10.1.1.48, 224.1.2.3), 00:39:15/00:00:04, flags: SFJT

Incoming interface: NET102

RPF nbr: 10.1.1.48, Registering

<-- The RP Registration is stuck

Immediate Outgoing interface list:

Tunnel0, Forward, 00:39:15/never

대상 영역이 지원되지 않습니다.

멀티캐스트 트래픽과 일치하는 액세스 제어 정책 규칙에 대해 대상 보안 영역을 지정할 수 없습니다.

The screenshot shows the Firewall Management Center (FMC) interface. At the top, there are navigation tabs: Overview, Analysis, Policies, Devices, Objects, and Integration. The current page is titled "FTD_Access_Control_Policy" and includes buttons for "Analyze Hit Counts", "Save", and "Cancel". Below the title, there are tabs for "Rules", "Security Intelligence", "HTTP Responses", "Logging", and "Advanced". A red error message is displayed: "Misconfiguration! The Dest Zones must be empty!". Below the error message, there is a table of rules. The table has columns for #, Name, Source Zones, Dest Zones, Source Networks, Dest Networks, VLAN Tags, Users, Applicat..., Source Ports, Dest Ports, URLs, Source Dynamic Attributes, Destinat... Dynamic Attributes, and Action. The first rule is "Mandatory - FTD_Access_Control_Policy (1-1)" with ID 1, Name "allow_multicast", Source Zones "INSIDE_ZONE", and Dest Zones "OUTSIDE_ZONE". The "Dest Zones" column is highlighted with a red box. Below the table, there is a note: "There are no rules in this section. Add Rule or Add Category".

이 내용은 FMC 사용 설명서에도 설명되어 있습니다.

Book Contents

Find Matches in This Book

- Book Title Page
- Getting Started with Device Configuration
- Device Operations
- Interfaces and Device Settings
- Routing**
 - Static and Default Routes
 - Virtual Routers
 - ECMP
 - OSPF
 - BGP
 - RIP
 - Multicast**
 - Policy Based Routing

Internet multicast routing from address range 224.0.0/24 is not supported; IGMP group is not created when enabling multicast routing for the reserved addresses.

Clustering

In clustering, for IGMP and PIM, this feature is only supported on the primary unit.

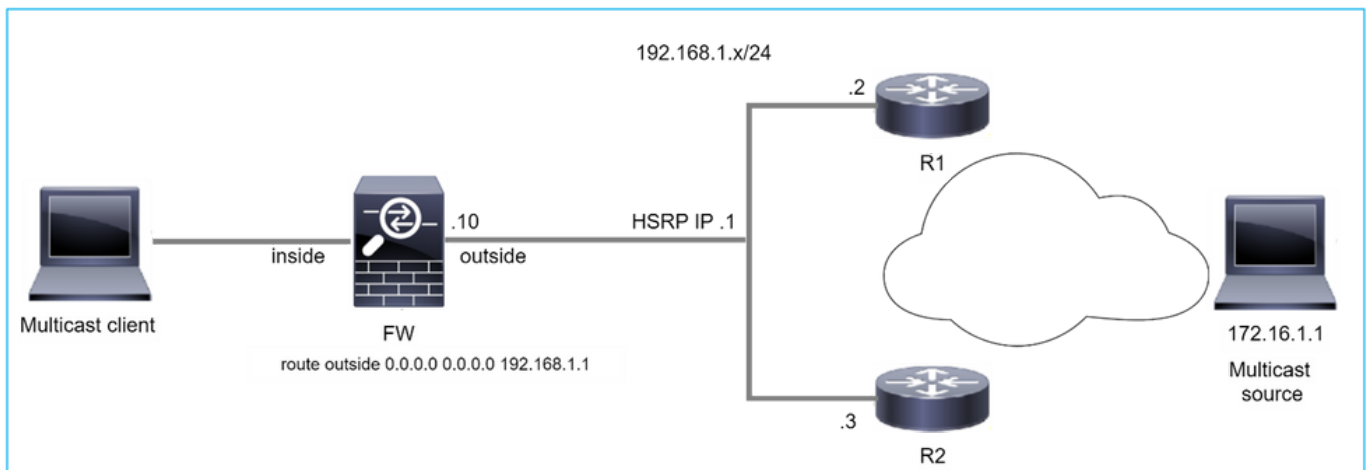
Additional Guidelines

- You must configure an access control or prefilter rule on the inbound security zone to allow traffic to the multicast host, such as 224.1.2.3. However, you cannot specify a destination security zone for the rule, or it cannot be applied to multicast connections during initial connection validation.
- You cannot disable an interface with PIM configured on it. If you have configured PIM on the interface (see [Configure PIM Protocol](#)), disabling the multicast routing and PIM does not remove the PIM configuration. You must remove (delete) the PIM configuration to disable the interface.
- PIM/IGMP Multicast routing is not supported on interfaces in a traffic zone.
- Do not configure FTD to simultaneously be a Rendezvous Point (RP) and a First Hop Router.

Configure IGMP Features

IP hosts use IGMP to report their group memberships to directly-connected multicast routers. IGMP is used to dynamically register individual hosts in a multicast group on a particular LAN. Hosts identify group memberships by sending IGMP

방화벽은 HSRP로 인해 업스트림 라우터로 메시지를 PIM하지 않음



이 경우 방화벽에는 HSRP(Hot Standby Redundancy Protocol) IP 192.168.1.1 및 라우터 R1 및 R2와의 PIM 네이버를 통한 기본 경로가 있습니다.

<#root>

firepower#

show run route

route outside 0.0.0.0 0.0.0.0 192.168.1.1 1

방화벽은 R1 및 R2에서 외부와 물리적 인터페이스 IP 사이에 PIM 인접성을 가집니다.

<#root>

firepower#

show pim neighbor

Neighbor Address	Interface	Uptime	Expires	DR	pri	Bidir
192.168.1.1	outside	01:18:27	00:01:25	1		
192.168.1.2	outside	01:18:03	00:01:29	1	(DR)	

방화벽은 PIM Join 메시지를 업스트림 네트워크로 전송하지 않습니다. PIM debug 명령 debug pim은 다음 출력을 표시합니다.

```
<#root>
```

```
firepower#
```

```
debug pim
```

```
...
```

```
IPv4 PIM: Sending J/P to an invalid neighbor: outside 192.168.1.1
```

[RFC 2362](#)는 "라우터가 각 (S,G), (*,G) 및 (*,*,RP) 항목과 연결된 각 개별 RPF 인접 디바이스에 주기적인 Join/Prune 메시지를 보냅니다. Join/Prune 메시지는 RPF 인접 디바이스가 PIM 인접 디바이스인 경우에만 전송됩니다."

문제를 완화하기 위해 사용자는 방화벽에 고정 mroute 엔트리를 추가할 수 있습니다. 라우터는 두 라우터 인터페이스 IP 주소 중 하나(192.168.1.2 또는 192.168.1.3)를 가리켜야 합니다(일반적으로 HSRP 활성 라우터 IP).

예:

```
<#root>
```


```
firepower#
```

```
show run mroute
```

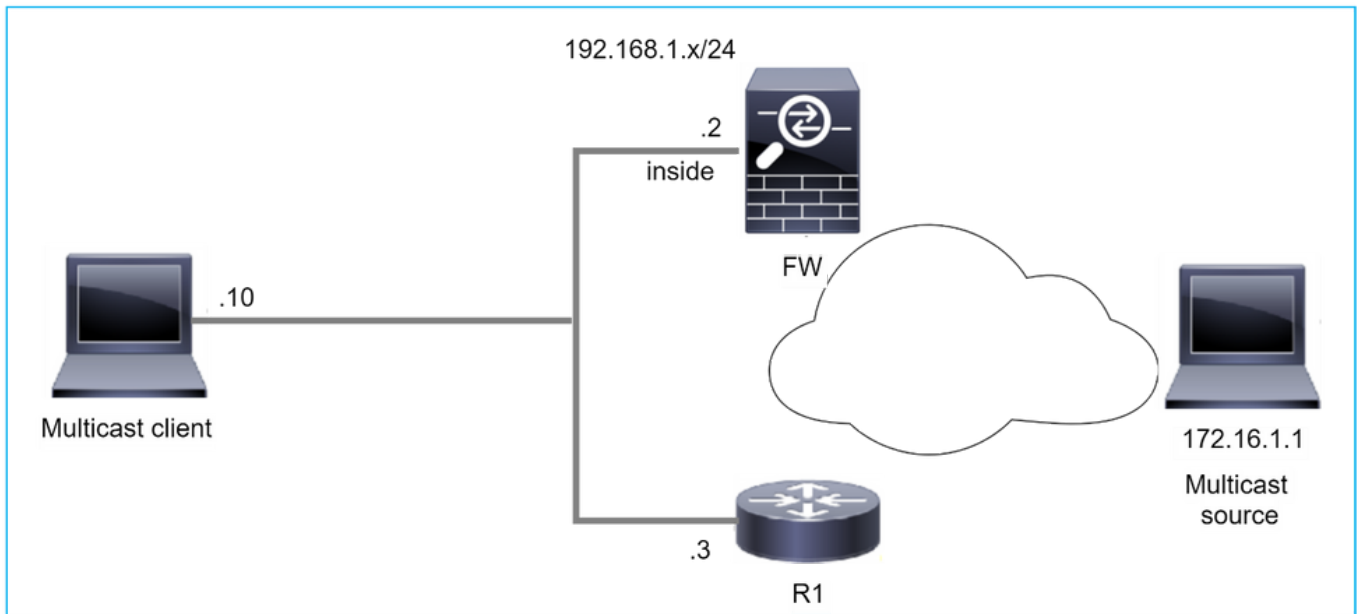
```
firepower#
```

```
mroute 172.16.1.1 255.255.255.255 192.168.1.2
```

고정 mroute 컨피그레이션이 자리 잡으면, RPF 조회를 위해 방화벽은 ASA의 유니캐스트 라우팅 테이블 대신 멀티캐스트 라우팅 테이블을 우선시하며 PIM 메시지를 인접 디바이스 192.168.1.2로 직접 전송합니다.

 참고: 고정 경로는 주소/넷마스크 조합당 1개의 next-hop만 허용하므로 일부 확장에 대해서는 HSRP 이중화의 유용성이 떨어집니다. mroute 명령에 지정된 다음 홉이 실패하거나 연결할 수 없게 되면 방화벽이 다른 라우터로 폴백되지 않습니다.

LAN 세그먼트의 DR이 아닌 방화벽은 LHR로 간주되지 않음



방화벽은 LAN 세그먼트의 PIM 인접 디바이스로 R1을 가집니다. R1은 PIM DR입니다.

```
<#root>
```

```
firepower#
```

```
show pim neighbor
```

Neighbor Address	Interface	Uptime	Expires	DR	pri	Bidir
192.168.1.3	inside	00:12:50	00:01:38	1	(DR)	

클라이언트로부터 IGMP 가입 요청이 수신되면 방화벽이 LHR이 되지 않습니다.

mroute는 OIL로 추가 Null을 표시하고 Pruned 플래그를 갖습니다.

```
<#root>
```

```
firepower#
```

```
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

```
(* , 230.1.1.1), 00:06:30/never, RP 0.0.0.0,  
flags  
: S  
P  
C  
  Incoming interface: Null  
  RPF nbr: 0.0.0.0  
  Immediate Outgoing interface list:  
  
inside, Null, 00:06:30/never <--- OIL has inside and Null
```

방화벽을 LHR로 만들기 위해 인터페이스 DR 우선순위를 높일 수 있습니다.

```
<#root>  
firepower#  
interface GigabitEthernet0/0  
  
firepower#  
pim dr-priority 2  
  
firepower#  
show pim neighbor  
  
Neighbor Address  Interface          Uptime    Expires DR pri Bidir  
192.168.1.3      inside            17:05:28  00:01:41 1
```

PIM debug 명령 debug pim은 다음 출력을 표시합니다.

```
<#root>  
firepower#  
debug pim  
firepower#  
  
IPv4 PIM: (*,230.1.1.1) inside Start being last hop <--- Firewall considers itself as the lasp hop  
  
IPv4 PIM: (*,230.1.1.1) Start being last hop
```

```
IPv4 PIM: (*,230.1.1.1) Start signaling sources
IPv4 PIM: [0] (*,230.1.1.1/32) NULLIF-skip MRIB modify NS
IPv4 PIM: (*,230.1.1.1) inside FWD state change from Prune to Forward
IPv4 PIM: [0] (*,230.1.1.1/32) inside MRIB modify F NS
IPv4 PIM: (*,230.1.1.1) Updating J/P status from Null to Join
IPv4 PIM: (*,230.1.1.1) J/P scheduled in 0.0 secs
IPv4 PIM: (*,230.1.1.1) Processing timers
IPv4 PIM: (*,230.1.1.1) J/P processing
IPv4 PIM: (*,230.1.1.1) Periodic J/P scheduled in 50 secs
IPv4 PIM: (*,230.1.1.1) No RPF interface to send J/P
```

Pruned 플래그 및 Null은 mroute에서 제거됩니다.

```
<#root>
```

```
firepower#
```

```
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
```

```
(*, 230.1.1.1), 16:48:23/never, RP 0.0.0.0, flags:
```

```
SCJ
```

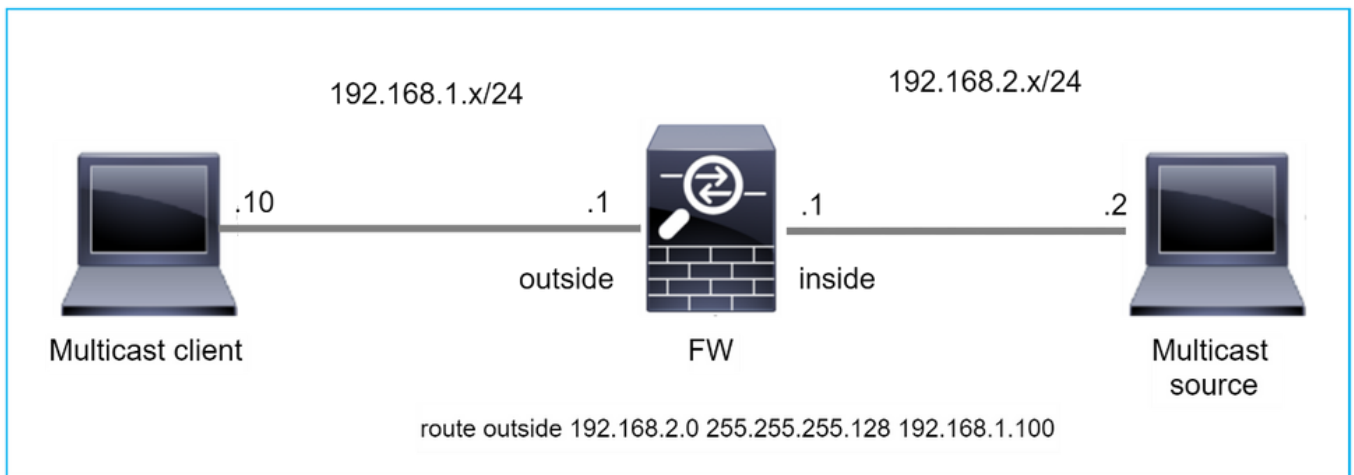
```
  Incoming interface: Null
```

```
  RPF nbr: 0.0.0.0
```

```
  Immediate Outgoing interface list:
```

```
    inside, Forward, 16:48:23/never
```

역방향 경로 전달 확인 실패로 인해 방화벽에서 멀티캐스트 패킷 삭제



이 경우 방화벽이 외부 인터페이스를 통해 마스크 255.255.255.128을 사용하는 더 구체적인 경로를 가지므로 RPF 오류로 인해 멀티캐스트 UDP 패킷이 삭제됩니다.

```
<#root>
```

```
firepower#
```

```
capture capi type raw-data trace interface inside match udp any any
```

```
firepower#
```

```
show capture capi packet-number 1 trace
```

```
106 packets captured
```

```
1: 08:57:18.867234 192.168.2.2.12345 > 230.1.1.1.12354: udp 500
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Elapsed time: 2684 ns
```

```
Config:
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Elapsed time: 2684 ns
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 3
```

```
Type: INPUT-ROUTE-LOOKUP
```

```
Subtype: Resolve Egress Interface
```

```
Result: ALLOW
```

```
Elapsed time: 13664 ns
```

Config:
Additional Information:
Found next-hop 192.168.1.100 using egress ifc outside

Phase: 4
Type: INPUT-ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Elapsed time: 8296 ns
Config:
Additional Information:
Found next-hop 192.168.1.100 using egress ifc outside

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: drop
Time Taken: 27328 ns

Drop-reason: (rpf-violated) Reverse-path verify failed, Drop-location: frame 0x0000556bcb1069dd flow

(NA)/NA

firepower#

show route static

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF

Gateway of last resort is not set

S 192.168.2.0 255.255.255.128 [1/0] via 192.168.1.100, outside

ASP 삭제 캡처에는 rpf가 위반한 삭제 사유가 표시됩니다.

<#root>

firepower#

show capture asp

Target: OTHER
Hardware: ASAV
Cisco Adaptive Security Appliance Software Version 9.19(1)
ASLR enabled, text region 556bc9390000-556bcd0603dd

21 packets captured

```
1: 09:00:53.608290      192.168.2.2.12345 > 230.1.1.1.12354:  udp 500 Drop-reason: (rpf-violated) Rever
2: 09:00:53.708032      192.168.2.2.12345 > 230.1.1.1.12354:  udp 500 Drop-reason: (rpf-violated) R
3: 09:00:53.812152      192.168.2.2.12345 > 230.1.1.1.12354:  udp 500 Drop-reason: (rpf-violated) R
4: 09:00:53.908613      192.168.2.2.12345 > 230.1.1.1.12354:  udp 500 Drop-reason: (rpf-violated) R
```

MFIB 출력의 RPF 실패 카운터가 증가합니다.

<#root>

firepower#

show mfib 230.1.1.1 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: 230.1.1.1

RP-tree:

Forwarding: 0/0/0/0, Other: 6788/6788/0

...

firepower#

show mfib 230.1.1.1 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: 230.1.1.1

RP-tree:

Forwarding: 0/0/0/0, Other: 6812/6812/0 <--- RPF failed counter increased

해결책은 RPF 검사 실패를 수정하는 것입니다. 한 가지 옵션은 고정 경로를 제거하는 것입니다.

더 이상 RPF 확인 오류가 없으면 패킷이 전달되고 MFIB 출력의 Forwarding 카운터가 증가합니다.

<#root>

firepower#

```
show mfib 230.1.1.1 count
```

```
IP Multicast Statistics
```

```
8 routes, 4 groups, 0.25 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: 230.1.1.1
```

```
RP-tree:
```

```
Forwarding: 0/0/0/0, Other: 9342/9342/0
```

```
Source: 192.168.2.2,
```

```
Forwarding: 1033/9/528/39
```

```
, Other: 0/0/0
```

```
Tot. shown: Source count: 1, pkt count: 0
```

```
...
```

```
firepower#
```

```
show mfib 230.1.1.1 count
```

```
IP Multicast Statistics
```

```
8 routes, 4 groups, 0.25 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: 230.1.1.1
```

```
RP-tree:
```

```
Forwarding: 0/0/0/0, Other: 9342/9342/0
```

```
Source: 192.168.2.2,
```

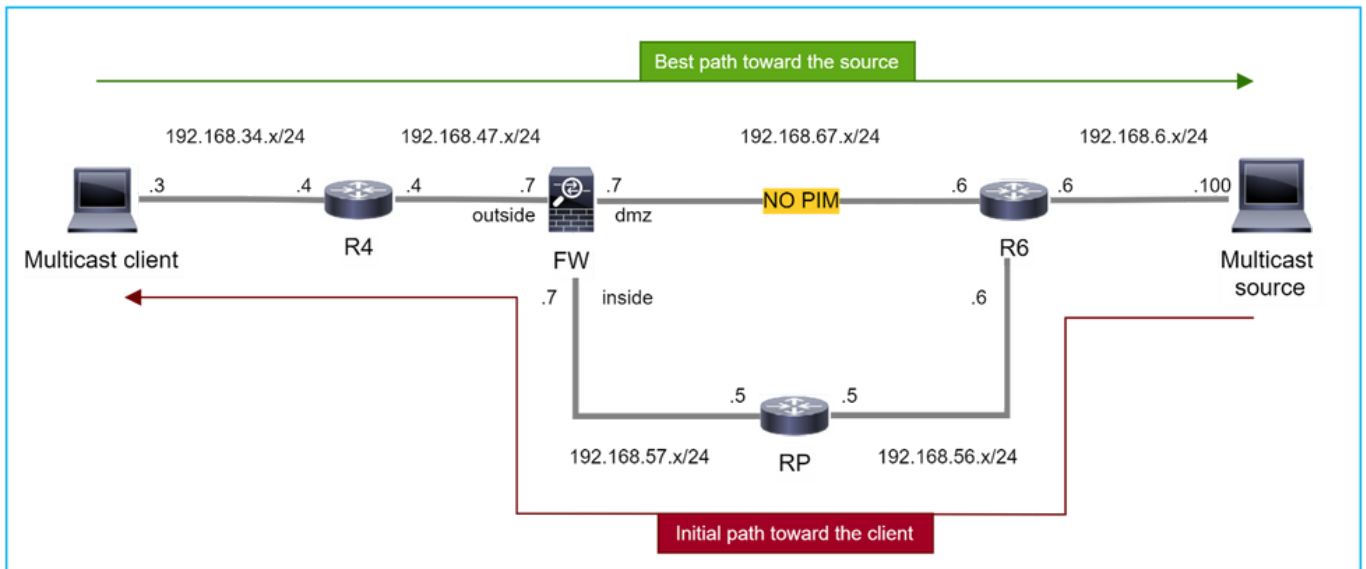
```
Forwarding: 1044/10/528/41
```

```
, Other: 0/0/0
```

```
<--- Forward counter increased
```

```
Tot. shown: Source count: 1, pkt count: 0
```

방화벽은 소스 트리로의 PIM 전환 시 PIM 조인을 생성하지 않습니다.



이 경우 방화벽은 dmz 인터페이스 R4 > FW > R6을 통해 멀티캐스트 소스로 향하는 경로를 학습하는 반면, 소스에서 클라이언트로의 초기 트래픽 경로는 R6 > RP > DW > R4입니다.

```
<#root>
```

```
firepower#
```

```
show route 192.168.6.100
```

```
Routing entry for 192.168.6.0 255.255.255.0
  Known via "ospf 1", distance 110, metric 11, type intra area
```

```
Last update from 192.168.67.6 on dmz, 0:36:22 ago
```

```
Routing Descriptor Blocks:
```

```
* 192.168.67.6, from 192.168.67.6, 0:36:22 ago, via dmz
```

```
Route metric is 11, traffic share count is 1
```

R4는 SPT 전환을 시작하고 SPT 전환 임계값에 도달하면 소스별 PIM 조인 메시지를 전송합니다. SPT 전환이 발생하지 않는 방화벽에서는 (S,G) 경로에 T 플래그가 없습니다.

```
<#root>
```

```
firepower#
```

```
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

(* , 230.1.1.1), 00:00:05/00:03:24, RP 10.5.5.5, flags: S

Incoming interface: inside

RPF nbr: 192.168.57.5

Immediate Outgoing interface list:

outside, Forward, 00:00:05/00:03:24

(192.168.6.100, 230.1.1.1), 00:00:05/00:03:24, flags: S

Incoming interface: dmz

RPF nbr: 192.168.67.6

Immediate Outgoing interface list:

outside, Forward, 00:00:05/00:03:2

PIM debug 명령 debug pim은 (*,G) 및 (S,G)에 대해 피어 R4에서 2개의 수신된 PIM 조인 요청을 보여줍니다. 방화벽에서 (*,G) 업스트림에 대한 PIM 조인 요청을 보냈으며, 잘못된 인접 디바이스 192.168.67.6으로 인해 소스별 요청을 보내지 못했습니다.

<#root>

firepower#

debug pim

IPv4 PIM: Received J/P on outside from 192.168.47.4 target: 192.168.47.7 (to us) <--- 1st PIM join to th

IPv4 PIM: J/P entry: Join root: 10.5.5.5 group: 230.1.1.1 flags: RPT WC S <--- 1st PIM join with root a

IPv4 PIM: (*,230.1.1.1) Create entry

IPv4 PIM: [0] (*,230.1.1.1/32) MRIB modify DC

IPv4 PIM: [0] (*,230.1.1.1/32) inside MRIB modify A

IPv4 PIM: (*,230.1.1.1) outside J/P state changed from Null to Join

IPv4 PIM: (*,230.1.1.1) outside Raise J/P expiration timer to 210 seconds

IPv4 PIM: (*,230.1.1.1) outside FWD state change from Prune to Forward

IPv4 PIM: [0] (*,230.1.1.1/32) outside MRIB modify F NS

IPv4 PIM: (*,230.1.1.1) Updating J/P status from Null to Join

IPv4 PIM: (*,230.1.1.1) J/P scheduled in 0.0 secs

IPv4 PIM: (*,230.1.1.1) Processing timers

IPv4 PIM: (*,230.1.1.1) J/P processing

IPv4 PIM: (*,230.1.1.1) Periodic J/P scheduled in 50 secs

IPv4 PIM: (*,230.1.1.1) J/P adding Join on inside

IPv4 PIM: Sending J/P message for neighbor 192.168.57.5 on inside for 1 groups <--- PIM Join sent from

IPv4 PIM: Received J/P on outside from 192.168.47.4 target: 192.168.47.7 (to us) <--- 1st PIM join to th

IPv4 PIM: J/P entry: Join root: 192.168.6.100 group: 230.1.1.1 flags: S <--- 1st PIM join with

IPv4 PIM: (192.168.6.100,230.1.1.1) Create entry
IPv4 PIM: Adding monitor for 192.168.6.100
IPv4 PIM: RPF lookup for root 192.168.6.100: nbr 192.168.67.6, dmz via the rib
IPv4 PIM: (192.168.6.100,230.1.1.1) RPF changed from 0.0.0.0/- to 192.168.67.6/dmz
IPv4 PIM: (192.168.6.100,230.1.1.1) Source metric changed from [0/0] to [110/11]
IPv4 PIM: [0] (192.168.6.100,230.1.1.1/32) MRIB modify DC
IPv4 PIM: [0] (192.168.6.100,230.1.1.1/32) inside MRIB modify A
IPv4 PIM: [0] (192.168.6.100,230.1.1.1/32) outside MRIB modify F NS
IPv4 PIM: (192.168.6.100,230.1.1.1) outside J/P state changed from Null to Join
IPv4 PIM: (192.168.6.100,230.1.1.1) outside Imm FWD state change from Prune to Forward
IPv4 PIM: (192.168.6.100,230.1.1.1) Updating J/P status from Null to Join
IPv4 PIM: (192.168.6.100,230.1.1.1) J/P scheduled in 0.0 secs
IPv4 PIM: [0] (192.168.6.100,230.1.1.1/32) dmz MRIB modify NS
IPv4 PIM: (192.168.6.100,230.1.1.1) outside Raise J/P expiration timer to 210 seconds
IPv4 PIM: (192.168.6.100,230.1.1.1) Processing timers
IPv4 PIM: (192.168.6.100,230.1.1.1) J/P processing
IPv4 PIM: (192.168.6.100,230.1.1.1) Periodic J/P scheduled in 50 secs
IPv4 PIM: (192.168.6.100,230.1.1.1) J/P adding Join on dmz

IPv4 PIM: Sending J/P to an invalid neighbor: dmz 192.168.67.6

<--- Invalid neighbor

show pim neighbour 명령 출력에 R6이 없습니다.

<#root>

firepower#

show pim neighbor

Neighbor Address	Interface	Uptime	Expires	DR	pri	Bidir
192.168.47.4	outside	00:21:12	00:01:44	1		
192.168.57.5	inside	02:43:43	00:01:15	1		

PIM은 방화벽 인터페이스 dmz에서 활성화됩니다.

<#root>

firepower#

show pim interface

Address	Interface	PIM	Nbr Count	Hello Intvl	DR Prior	DR
192.168.47.7	outside	on	1	30	1	this system

```

192.168.67.7    dmz            on 0    30    1      this system
192.168.57.7    inside        on 1    30    1      this system

```

PIM은 R6 인터페이스에서 비활성화됩니다.

```
<#root>
```

```
R6#
```

```
show ip interface brief
```

```

Interface                IP-Address      OK? Method Status        Protocol
GigabitEthernet0/0       192.168.6.1     YES manual  up            up
GigabitEthernet0/1       192.168.56.6   YES manual  up            up
GigabitEthernet0/2       unassigned      YES unset   administratively down down
GigabitEthernet0/3       192.168.67.6   YES manual  up            up

Tunnel0                   192.168.56.6   YES unset   up            up

```

```
R6#
```

```
show ip pim interface GigabitEthernet0/3 detail
```

```

GigabitEthernet0/3 is up, line protocol is up
  Internet address is 192.168.67.6/24
  Multicast switching: fast
  Multicast packets in/out: 0/123628
  Multicast TTL threshold: 0

```

```
PIM: disabled <--- PIM is disabled
```

```
Multicast Tagswitching: disabled
```

해결책은 R6의 인터페이스 GigabitEthernet0/3에서 PIM을 활성화하는 것입니다.

```
<#root>
```

```
R6(config-if)#
```

```
interface GigabitEthernet0/3
```

```
R6(config-if)#
```

```
ip pim sparse-mode
```

```
R6(config-if)#
```

```
*Apr 21 13:17:14.575: %PIM-5-NBRCHG: neighbor 192.168.67.7 UP on interface GigabitEthernet0/3
```

*Apr 21 13:17:14.577: %PIM-5-DRCHG: DR change from neighbor 0.0.0.0 to 192.168.67.7 on interface Gigabit

방화벽은 SPT 전환을 나타내는 T 플래그를 설치합니다:

<#root>

firepower#

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

(* , 230.1.1.1), 00:26:30/00:02:50, RP 10.5.5.5, flags: S
Incoming interface: inside
RPF nbr: 192.168.57.5
Immediate Outgoing interface list:
outside, Forward, 00:26:30/00:02:50

(192.168.6.100, 230.1.1.1), 00:26:30/00:03:29, flags: ST

Incoming interface: dmz
RPF nbr: 192.168.67.6
Immediate Outgoing interface list:
outside, Forward, 00:26:30/00:02:39

Punt rate Limit으로 인해 방화벽에서 처음 몇 개의 패킷 삭제

방화벽이 FP에서 새로운 멀티캐스트 스트림의 첫 번째 패킷을 수신하는 경우, CP에 의한 추가 처리가 필요할 수 있습니다. 이 경우, FP는 추가 작업을 위해 SP(FP > SP > CP)를 통해 패킷을 CP에 적용합니다.

- 인그레스 인터페이스와 ID 인터페이스 간의 FP에서 상위 연결 생성
- RPF 검증, PIM 캡슐화(방화벽이 FHR인 경우), OIL 확인 등의 추가 멀티캐스트 관련 확인.
- mroute 테이블에서 수신 및 발신 인터페이스를 사용하여 (S,G) 항목을 생성합니다.
- 수신 인터페이스와 발신 인터페이스 간의 FP에서 하위/스텝 연결 생성

컨트롤 플레인 보호의 일환으로 방화벽은 내부적으로 CP에 적용되는 패킷의 속도를 제한합니다.

속도를 초과하는 패킷은에서 punt-rate-limit 삭제 사유로 삭제됩니다.

<#root>

```
firepower#
show asp drop
```

Frame drop:

```
Punt rate limit exceeded (punt-rate-limit) 2062
```

show asp cluster counter 명령을 사용하여 SP에서 CP로 보내진 멀티캐스트 패킷 수를 확인합니다.

```
<#root>
```

```
firepower#
show asp cluster counter
```

Global dp-counters:

Context specific dp-counters:

MCAST_FP_FROM_PUNT	30	Number of multicast packets punted from CP to FP
MCAST_FP_TO_SP	2680	Number of multicast packets punted from FP to SP
MCAST_SP_TOTAL	2710	Number of total multicast packets processed in SP
MCAST_SP_FROM_PUNT	30	Number of multicast packets punted from CP to SP <--- Number of
MCAST_SP_FROM_PUNT_FORWARD	30	Number of multicast packets coming from CP that are forwarded
MCAST_SP_PKTS	30	Number of multicast packets that require slow-path attention
MCAST_SP_PKTS_TO_CP	30	Number of multicast packets punted to CP from SP
MCAST_FP_CHK_FAIL_NO_HANDLE	2650	Number of multicast packets failed with no flow mcast_handle
MCAST_FP_CHK_FAIL_NO_FP_FWD	30	Number of multicast packets that cannot be fast-path forwarded

show asp event dp-cp punt 명령을 사용하여 FP > CP 큐의 패킷 수 및 15초 속도를 확인합니다.

```
<#root>
```

```
firepower#
show asp event dp-cp punt | begin EVENT-TYPE
```

EVENT-TYPE	ALLOC	ALLOC-FAIL	ENQUEUED	ENQ-FAIL	RETIRED	15SEC-RATE
punt	24452	0	24452	0	10852	1402

```
multicast
```

```
23800 0
```

```
23800
```

```
0 10200
```

```
1402
```

pim 652 0 652 0 652 0

mroute가 채워지고 FP에서 상위/하위 연결이 설정되면 패킷은 기존 연결의 일부로 FP에서 전달됩니다. 이 경우 FP는 패킷을 CP에 푸시하지 않습니다.

방화벽이 새 멀티캐스트 스트림의 첫 번째 패킷을 어떻게 처리합니까?

방화벽이 데이터 경로에 있는 새 멀티캐스트 스트림의 첫 번째 패킷을 수신하면 다음과 같은 작업을 수행합니다.

1. 보안 정책에서 패킷을 허용하는지 확인합니다.
2. 경로 FP를 통해 패킷을 CP에 적용합니다.
3. 인그레스 인터페이스와 ID 인터페이스 간에 상위 연결을 생성합니다.

<#root>

firepower#

show capture capi packet-number 1 trace

10 packets captured

1: 08:54:15.007003 192.168.1.100.12345 > 230.1.1.1.12345: udp 400

Phase: 1

Type: CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

MAC Access list

Phase: 2

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

MAC Access list

Phase: 3

Type: INPUT-ROUTE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

Found next-hop 192.168.2.1 using egress ifc inside

Phase: 4

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:
Implicit Rule
Additional Information:

Phase: 5
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: QOS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 9

Type: MULTICAST

Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 10

Type: FLOW-CREATION

Subtype:
Result: ALLOW
Config:
Additional Information:

New flow created with id 19, packet dispatched to next module <--- New flow

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up

Action: allow

Syslog:

<#root>

```
firepower# Apr 24 2023 08:54:15: %ASA-7-609001: Built local-host inside:192.168.1.100
```

```
Apr 24 2023 08:54:15: %FTD-7-609001: Built local-host identity:230.1.1.1
```

```
Apr 24 2023 08:54:15: %FTD-6-302015: Built inbound UDP connection 19 for inside:192.168.1.100/12345 (192.168.1.100)
```

이 연결은 show conn all 명령의 출력에서 표시됩니다.

<#root>

```
firepower#
```

```
show conn all protocol udp
```

```
13 in use, 17 most used
```

```
UDP inside 192.168.1.100:12345 NP Identity Ifc 230.1.1.1:12345, idle 0:00:02, bytes 0, flags -
```

4. CP는 RPF 검증, PIM 캡슐화(방화벽이 FHR인 경우), OIL 확인 등과 같은 추가적인 멀티캐스트 관련 확인을 위해 멀티캐스트 프로세스에 참여합니다.
5. CP는 mroute에 수신 및 발신 인터페이스가 있는 (S,G) 항목을 생성합니다.

<#root>

```
firepower#
```

```
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
```

```
(*, 230.1.1.1), 00:19:28/00:03:13, RP 192.168.192.168, flags: S
```

```
Incoming interface: inside
```

```
RPF nbr: 192.168.2.1
```

```
Immediate Outgoing interface list:
```

```
outside, Forward, 00:19:28/00:03:13
```

(192.168.1.100, 230.1.1.1), 00:08:50/00:03:09, flags: ST

Incoming interface: inside

RPF nbr: 192.168.2.1

Immediate Outgoing interface list:

outside, Forward, 00:00:32/00:02:57

6. CP는 CP > SP > FP 경로를 통해 FP에게 수신 및 발신 인터페이스 간 하위/스텝 연결을 생성하도록 지시합니다.

이 연결은 show local-host 명령의 출력에서만 표시됩니다.

<#root>

firepower#

show local-host

Interface outside: 5 active, 5 maximum active

local host: <224.0.0.13>,

local host: <192.168.3.100>,

local host: <230.1.1.1>,

Conn:

UDP outside 230.1.1.1:12345 inside 192.168.1.100:12345, idle

0:00:04, bytes 4000, flags -

local host: <224.0.0.5>,

local host: <224.0.0.1>,

Interface inside: 4 active, 5 maximum active

local host: <192.168.1.100>,

Conn:

UDP outside 230.1.1.1:12345 inside 192.168.1.100:12345, idle

0:00:04, bytes 4000, flags -

local host: <224.0.0.13>,

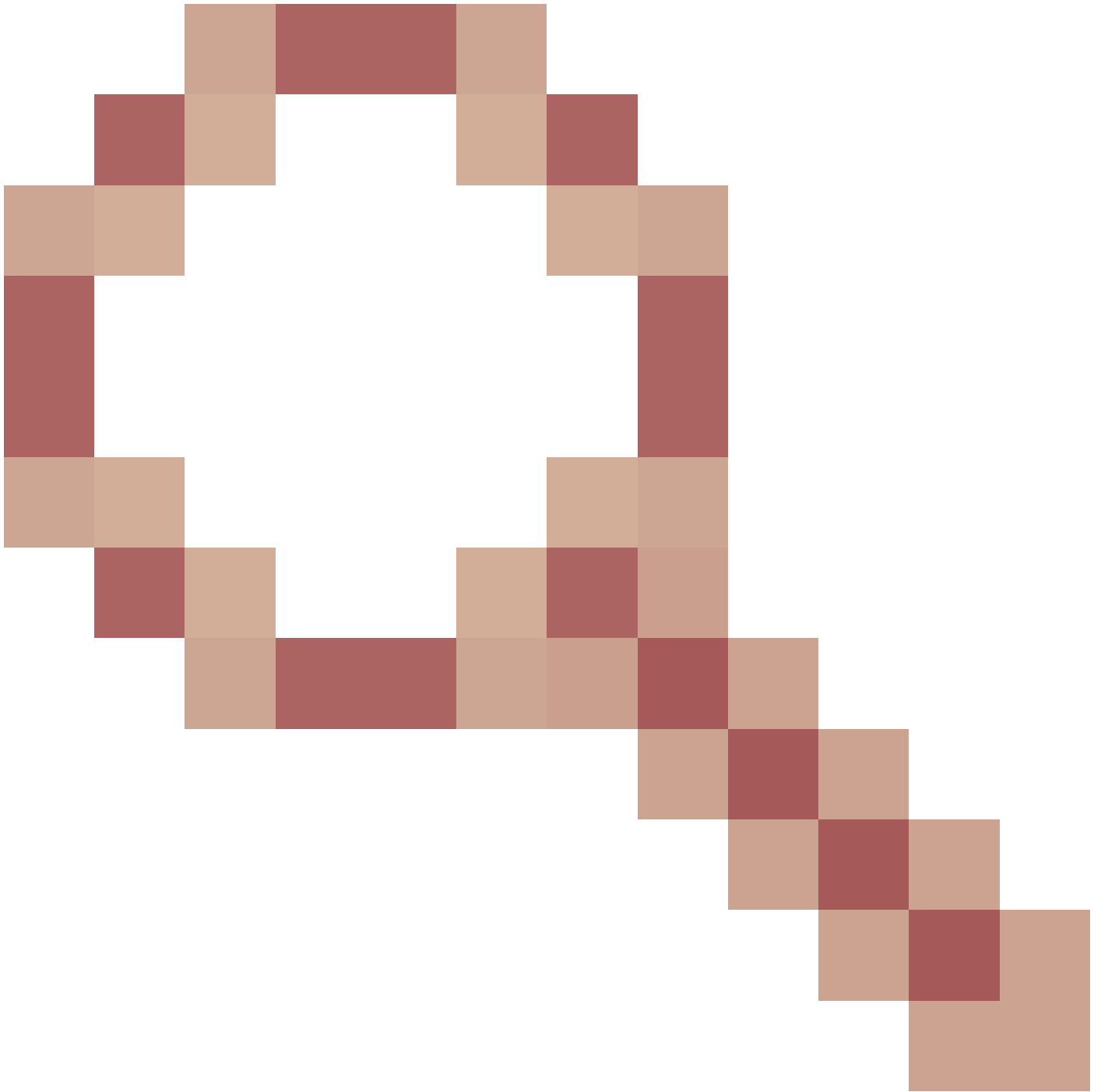
local host: <192.168.2.1>,

local host: <224.0.0.5>,

Interface nlp_int_tap: 0 active, 2 maximum active

Interface any: 0 active, 0 maximum active

Cisco 버그 ID CSCwe가 수정된 소프트웨어 버전 [21280](#)



또한 하위/스텝 302015에 대한 syslog 메시지도 생성됩니다.

<#root>

Apr 24 2023 08:54:15: %FTD-6-302015:

Built outbound UDP connection 20 for outside:230.1.1.1/12345 (230.1.1.1/12345) to inside:192.168.1.100/1

상위 및 하위/스텝 연결이 모두 설정되면 인그레스 패킷이 기존 연결과 일치하며 FP에서 전달됩니다.

<#root>

```
firepower#
```

```
show capture capi trace packet-number 2
```

```
10 packets captured
```

```
2: 08:54:15.020567      192.168.1.100.12345 > 230.1.1.1.12345:  udp 400
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 3
```

```
Type: FLOW-LOOKUP
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
Found flow with id 19, using existing flow <--- Existing flow
```

```
Result:
```

```
input-interface: inside
```

```
input-status: up
```

```
input-line-status: up
```

```
Action: allow
```

ICMP 멀티캐스트 트래픽 필터링

ICMP 멀티캐스트 트래픽은 ACL로 필터링할 수 없습니다. 컨트롤 플레인 정책(ICMP)을 사용해야 합니다.

Cisco 버그 ID [CSCsl26860](#) ASA는 멀티캐스트 ICMP 패킷을 필터링하지 않음

알려진 PIM 멀티캐스트 결함

알려진 결함에 대해서는 버그 검색 툴을 사용할 수 있습니다.

<https://bst.cloudapps.cisco.com/bugsearch>

대부분의 ASA 및 FTD 결합은 'Cisco ASA(Adaptive Security Appliance) 소프트웨어' 제품 아래에 나열됩니다.

The screenshot shows the Cisco Bug Search Tool interface. At the top, there are navigation links for Products, Support & Learn, Partners, and Events & Videos. The main heading is "Bug Search Tool". Below this, there is a search form with the following fields:

- Search For:** A text input field containing "PIM", highlighted with a red box and a red circle with the number "1".
- Product:** A dropdown menu showing "Series/Model" and a text input field containing "Cisco Adaptive Security Appliance (ASA) Software", highlighted with a red box and a red circle with the number "2".
- Release:** A dropdown menu showing "Affecting or Fixed in Releases" and an empty text input field.

Below the search form, there are buttons for "Save Search", "Email Search", "Clear", and "Search". A red callout bubble labeled "The results" points to the results section. The results section shows "94 Results | Sorted by Severity" and "Sort By: Show All". The first two results are:

- CSCsy08778 no pim on one subif disables eigrp on same physical of 4 ge module**
Symptom: eigrp stops working on one subinterface, if "no pim" is issued on another subinterface which belongs to the same physical interface. **Conditions:** The physical interface belongs to the 4-GE module. If using the main-board
Severity: 2 | Status: Fixed | Updated: Nov 09, 2016 | Cases:3 | ★ ★ ★ ★ ★ (0)
- CSCtg52478 PIM nbr jp_buffer can be corrupted under stress**
Symptom: memory corruption of pim nbr structure **Conditions:** multicast w/ PIM-SM and heavy traffic and CLI

관련 정보

- [ASA 멀티캐스트 트러블슈팅 및 일반 문제](#)
- [Firepower Management Center 멀티캐스트](#)
- [firepower 멀티캐스트 플래그 요약](#)

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.