

firepower 위협 방어 IGMP 및 멀티캐스트 기본 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[IGMP 기본 사항](#)

[작업 1 - Control-Plane 멀티캐스트 트래픽](#)

[작업 2 - 기본 멀티캐스트 구성](#)

[IGMP 스누핑](#)

[작업 3 - IGMP 고정 그룹 vs IGMP 조인 그룹](#)

[igmp 정적 그룹](#)

[igmp 조인 그룹](#)

[작업 4 - IGMP Stub 멀티캐스트 라우팅 구성](#)

[알려진 문제](#)

[대상 영역에서 멀티캐스트 트래픽 필터링](#)

[IGMP 인터페이스 제한이 초과되면 방화벽에 의해 IGMP 보고서가 거부됨](#)

[방화벽이 232.x.x.x/8 주소 범위에 대한 IGMP 보고서를 무시함](#)

[관련 정보](#)

소개

이 문서에서는 멀티캐스트의 기본 사항과 FTD(Firepower Threat Defense)가 IGMP(Internet Group Management Protocol)를 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 내용은 ASA(Adaptive Security Appliance) 소프트웨어에도 적용됩니다.

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.
- ASA 버전 9.19.1

배경 정보

정의

- 유니캐스트 = 단일 호스트에서 다른 호스트로(일대일).
- 브로드캐스트 = 단일 호스트에서 모든 가능한 호스트로(일대다).
- 멀티캐스트 = 호스트 그룹의 호스트에서 호스트 그룹(일대다 또는 다대다)으로
- 애니캐스트 = 호스트에서 그룹의 가장 가까운 호스트로(일대다)

기본

- 멀티캐스트 RFC 988은 1986년에 Steve Deering에 의해 작성되었습니다.
- IPv4 멀티캐스트는 224.0.0.0/4(처음 4비트 1110) - 224.0.0.0 - 239.255.255.255 범위를 사용합니다.
- IPv4의 경우 L2 MAC 주소는 L3 멀티캐스트 IP에서 파생됩니다. 01005e(24비트) + 25번째 비트 항상 0 + 23개의 하위 비트 멀티캐스트 IPv4 주소입니다.
- IPv6 멀티캐스트는 FF00::/8 범위를 사용하며 RP(Rendezvous Point) IP를 포함할 수 있으므로 IPv4 멀티캐스트보다 유연합니다.
- IPv6의 경우 L2 MAC 주소는 L3 멀티캐스트에서 파생됩니다. 3333 + 32비트의 멀티캐스트 IPv6 주소입니다.
- 멀티캐스트의 이점: 소스의 로드가 감소하여 효율성 향상 트래픽 중복 또는 플러딩을 방지하므로 성능.
- 멀티캐스트의 단점: 신뢰할 수 없는 전송(UDP 기반), 혼잡 회피 없음, 시퀀스 외 전달.
- 멀티캐스트는 경로의 모든 디바이스가 활성화되어야 하므로 공용 인터넷에서 지원되지 않습니다. 일반적으로 모든 디바이스가 공통 관리 권한에 속하는 경우 사용됩니다.
- 일반적인 멀티캐스트 애플리케이션: 내부 비디오 스트림, 비디오 컨퍼런스.

멀티캐스트 대 복제 유니캐스트

복제된 유니캐스트에서 소스는 동일한 유니캐스트 패킷의 여러 복사본(복제본)을 생성하여 여러 대상 호스트로 전송합니다. 멀티캐스트는 소스 호스트에서 네트워크로 부담을 이동하는 반면, 복제된 유니캐스트에서는 모든 작업이 소스 호스트에서 수행됩니다.

구성

IGMP 기본 사항

- IGMP는 멀티캐스트 수신자와 로컬 L3 디바이스(일반적으로 라우터) 간에 사용되는 '언어'입니다.
- IGMP는 레이어 3 프로토콜(예: ICMP)이며 IP 프로토콜 번호 2를 사용합니다.
- 현재 3개의 IGMP 버전이 있습니다. 방화벽의 기본 IGMP 버전은 버전 2입니다. 현재 버전 1과 2만 지원됩니다.
- IGMPv1과 IGMPv2 간의 주요 차이점은 다음과 같습니다.
 - IGMPv1에 그룹 나가기 메시지가 없습니다.
 - IGMPv1에는 그룹별 쿼리가 없습니다(호스트가 멀티캐스트 그룹에서 나갈 때 방화벽에서 사용됨).
 - IGMPv1에는 쿼리 발송자 선택 프로세스가 없습니다.
- IGMPv3는 현재 ASA/FTD에서 지원되지 않지만, 참고로 IGMPv2와 IGMPv3의 중요한 차이점은 SSM(Source-Specific Multicast)에서 사용되는 IGMPv3에 Group-and-Source-Specific Query를 포함한다는 것입니다.
- IGMPv1/IGMPv2/IGMPv3 쿼리 = 224.0.0.1
 IGMPv2 Leave = 224.0.0.2
 IGMPv3 멤버십 보고서 = 224.0.0.22
- 호스트가 가입하려는 경우 요청되지 않은 IGMP 멤버십 보고서 메시지를 보낼 수 있습니다.

No.	Time	Delta	Source	Destination	Protocol	SGT	Identification	Length	Info
7	5.118518	0.000000	192.168.1.50	224.0.0.2	IGMPv2		0x01a7 (423)	46	Leave Group 230.10.10.10
8	5.127230	0.008712	192.168.1.50	230.10.10.10	IGMPv2		0x01a8 (424)	46	Membership Report group 230.10.10.10
9	5.593022	0.465792	192.168.1.50	230.10.10.10	IGMPv2		0x01a9 (425)	46	Membership Report group 230.10.10.10
114	74.756894	69.163872	192.168.1.24	224.0.0.1	IGMPv2		0x7280 (29312)	60	Membership Query, general
118	77.093155	2.336261	192.168.1.50	239.255.255.250	IGMPv2		0x01e9 (489)	46	Membership Report group 239.255.255.250
120	79.593298	2.500143	192.168.1.50	224.0.0.252	IGMPv2		0x01eb (491)	46	Membership Report group 224.0.0.252
122	81.093367	1.500069	192.168.1.50	230.10.10.10	IGMPv2		0x01ec (492)	46	Membership Report group 230.10.10.10
152	103.150111	22.056744	192.168.1.24	224.0.0.1	IGMPv2		0x1c5f (7263)	60	Membership Query, general
153	103.593643	0.443532	192.168.1.50	224.0.0.252	IGMPv2		0x0206 (518)	46	Membership Report group 224.0.0.252
154	104.593737	1.000094	192.168.1.50	239.255.255.250	IGMPv2		0x0208 (520)	46	Membership Report group 239.255.255.250
161	107.686998	3.093261	192.168.1.50	224.0.0.2	IGMPv2		0x020b (523)	46	Leave Group 230.10.10.10
162	107.687972	0.000974	192.168.1.24	230.10.10.10	IGMPv2		0x9b9d (39837)	60	Membership Query, specific for group 230.10.10.10
163	107.695137	0.007165	192.168.1.50	230.10.10.10	IGMPv2		0x020c (524)	46	Membership Report group 230.10.10.10
164	108.093934	0.398797	192.168.1.50	230.10.10.10	IGMPv2		0x020e (526)	46	Membership Report group 230.10.10.10

- 방화벽 관점에서 IGMP 쿼리에는 일반 쿼리와 그룹별 쿼리의 2가지 유형이 있습니다
- 방화벽에서 IGMP Leave Group(그룹 탈퇴) 메시지를 수신하면 서브넷에 해당 그룹의 다른 구성원이 있는지 확인해야 합니다. 따라서 방화벽은 다음과 같은 그룹별 쿼리를 전송합니다.

No.	Time	Delta	Source	Destination	Protocol	SGT	Identification	Length	Info
7	5.118518	0.000000	192.168.1.50	224.0.0.2	IGMPv2		0x01a7 (423)	46	Leave Group 230.10.10.10
8	5.127230	0.008712	192.168.1.50	230.10.10.10	IGMPv2		0x01a8 (424)	46	Membership Report group 230.10.10.10
9	5.593022	0.465792	192.168.1.50	230.10.10.10	IGMPv2		0x01a9 (425)	46	Membership Report group 230.10.10.10
114	74.756894	69.163872	192.168.1.24	224.0.0.1	IGMPv2		0x7280 (29312)	60	Membership Query, general
118	77.093155	2.336261	192.168.1.50	239.255.255.250	IGMPv2		0x01e9 (489)	46	Membership Report group 239.255.255.250
120	79.593298	2.500143	192.168.1.50	224.0.0.252	IGMPv2		0x01eb (491)	46	Membership Report group 224.0.0.252
122	81.093367	1.500069	192.168.1.50	230.10.10.10	IGMPv2		0x01ec (492)	46	Membership Report group 230.10.10.10
152	103.150111	22.056744	192.168.1.24	224.0.0.1	IGMPv2		0x1c5f (7263)	60	Membership Query, general
153	103.593643	0.443532	192.168.1.50	224.0.0.252	IGMPv2		0x0206 (518)	46	Membership Report group 224.0.0.252
154	104.593737	1.000094	192.168.1.50	239.255.255.250	IGMPv2		0x0208 (520)	46	Membership Report group 239.255.255.250
161	107.686998	3.093261	192.168.1.50	224.0.0.2	IGMPv2		0x020b (523)	46	Leave Group 230.10.10.10
162	107.687972	0.000974	192.168.1.24	230.10.10.10	IGMPv2		0x9b9d (39837)	60	Membership Query, specific for group 230.10.10.10
163	107.695137	0.007165	192.168.1.50	230.10.10.10	IGMPv2		0x020c (524)	46	Membership Report group 230.10.10.10
164	108.093934	0.398797	192.168.1.50	230.10.10.10	IGMPv2		0x020e (526)	46	Membership Report group 230.10.10.10

- 여러 라우터/방화벽이 있는 서브넷에서 쿼리(모든 IGMP 쿼리를 전송하는 디바이스)가 선택됩니다.

```
<#root>
```

```
firepower#
```

```
show igmp interface INSIDE
```

```
INSIDE is up, line protocol is up
  Internet address is 192.168.1.97/24
  IGMP is enabled on interface
  Current IGMP version is 2
  IGMP query interval is 125 seconds
  IGMP querier timeout is 60 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: 2
  Cumulative IGMP activity: 21 joins, 20 leaves
```

```
IGMP querying router is 192.168.1.97 (this system)
```

```
<-- IGMP querier
```

- FTD에서 기존 ASA와 마찬가지로 디버그 igmp를 활성화하여 IGMP 관련 메시지를 볼 수 있습니다.

```
<#root>
```

```
firepower#
```

```
debug igmp
```

```
IGMP debugging is on
IGMP: Received v2 Query on DMZ from 192.168.6.1

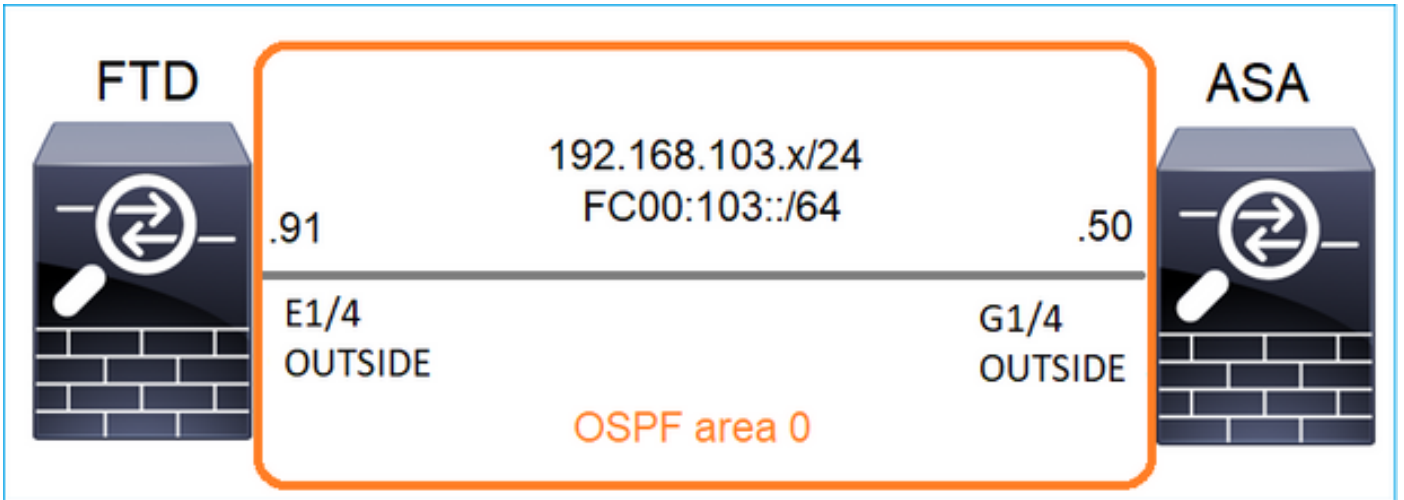
IGMP: Received v2 Report on INSIDE from 192.168.1.50 for 239.255.255.250

<-- Received an IGMP packet
IGMP: group_db: add new group 239.255.255.250 on INSIDE
IGMP: MRIB updated (*,239.255.255.250) : Success
IGMP: Switching to EXCLUDE mode for 239.255.255.250 on INSIDE
IGMP: Updating EXCLUDE group timer for 239.255.255.250
IGMP: Received v2 Report on INSIDE from 192.168.1.50 for 230.10.10.10
IGMP: group_db: add new group 230.10.10.10 on INSIDE
IGMP: MRIB updated (*,230.10.10.10) : Success
IGMP: Switching to EXCLUDE mode for 230.10.10.10 on INSIDE
IGMP: Updating EXCLUDE group timer for 230.10.10.10
IGMP: Send v2 general Query on INSIDE
IGMP: Received v2 Query on INSIDE from 192.168.1.97
IGMP: Send v2 general Query on OUTSIDE
IGMP: Received v2 Query on OUTSIDE from 192.168.103.91
IGMP: Received v2 Report on INSIDE from 192.168.1.50 for 239.255.255.250
IGMP: Updating EXCLUDE group timer for 239.255.255.250
IGMP: Received v2 Report on INSIDE from 192.168.1.50 for 230.10.10.10
IGMP: Updating EXCLUDE group timer for 230.10.10.10
```

- 호스트는 일반적으로 IGMPv2(Leave Group message)를 사용하여 멀티캐스트 그룹을 떠납니다.

No.	Time	Delta	Source	Destination	Protocol	Identification	Length	Info
7	5.118518	0.000000	192.168.1.50	224.0.0.2	IGMPv2	0x01a7 (423)	46	Leave Group 230.10.10.10
161	107.686998	102.568480	192.168.1.50	224.0.0.2	IGMPv2	0x020b (523)	46	Leave Group 230.10.10.10

작업 1 - Control-Plane 멀티캐스트 트래픽



FTD와 ASA 간에 OSPFv2 및 OSPFv3을 구성합니다. OSPF에서 생성된 L2 및 L3 멀티캐스트 트래픽을 2개의 디바이스에서 어떻게 처리하는지 확인합니다.

솔루션

OSPFv2 컨피그레이션

Firewall Management Center
Devices / NGFW Routing

FTD4125-1
Cisco Firepower 4125 Threat Defense

Device Routing Interfaces Inline Sets DHCP

Manage Virtual Routers
Global

Virtual Router Properties
ECMP
OSPF
OSPFv3
EIGRP
RIP
Policy Based Routing
BGP
IPv4
IPv6

Process 1 ID: 1

OSPF Role: Internal Router Enter Description here Advanced

Process 2 ID:

OSPF Role: Internal Router Enter Description here Advanced

Area Redistribution InterArea Filter Rule Summary Address Interface

OSPF Process	Area ID	Area Type	Networks	Options	Authentication	Cost	Range	Virtual-Link
1	0	normal	net_192.168.103.0	false	none			

Interface	Authentication	Point-to-Point	Cost	Priority	MTU Ignore	Database Filter	Neighbor
OUTSIDE	None	false	10	1	false	false	

마찬가지로, OSPFv3의 경우

FTD CLI 컨피그레이션:

```
<#root>
```

```
router ospf 1
  network 192.168.103.0 255.255.255.0 area 0
  log-adj-changes
  !
  ipv6 router ospf 1
    no graceful-restart helper
    log-adjacency-changes
    !
    interface Ethernet1/4
      nameif OUTSIDE
      security-level 0
      ip address 192.168.103.91 255.255.255.0
      ipv6 address fc00:103::91/64
      ospf authentication null
    ipv6 ospf 1 area 0
```

컨피그레이션에서는 인그레스 멀티캐스트 트래픽이 차단되지 않도록 FTD ASP(Accelerated Security Path) 허용 테이블에 다음 항목을 생성합니다.

```
<#root>
```

```
firepower#
show asp table classify domain permit
...
in id=0x14f922db85f0, priority=13,
domain=permit, deny=false
<-- permit the packets
  hits=1, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=89
  src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
```

```

dst ip/id=224.0.0.5, mask=255.255.255.255,
  port=0, tag=any, dscp=0x0, nsg_id=none    <-- OSPF for IPv4

input_ifc=OUTSIDE

(vrfid:0), output_ifc=identity(vrfid:0)    <-- ingress interface
in id=0x14f922db9350, priority=13,

domain=permit, deny=false

<-- permit the packets
  hits=0, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=89
  src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any

  dst ip/id=224.0.0.6, mask=255.255.255.255
, port=0, tag=any, dscp=0x0, nsg_id=none    <-- OSPF for IPv4

input_ifc=OUTSIDE

(vrfid:0), output_ifc=identity(vrfid:0)    <-- ingress interface

```

IPv6의 경우

```

<#root>

...
in id=0x14f923fb16f0, priority=13,

domain=permit, deny=false

<-- permit the packets
  hits=1, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=89
  src ip/id>::/0, port=0, tag=any

dst ip/id=ff02::5/128
, port=0, tag=any, , nsg_id=none    <-- OSPF for IPv6

input_ifc=OUTSIDE

(vrfid:0), output_ifc=identity(vrfid:0) <-- ingress interface
in id=0x14f66e9d4780, priority=13,

domain=permit, deny=false

<-- permit the packets
  hits=0, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=89
  src ip/id>::/0, port=0, tag=any

dst ip/id=ff02::6/128
, port=0, tag=any, , nsg_id=none    <-- OSPF for IPv6

```

```
input_ifc=OUTSIDE
```

```
(vrfid:0), output_ifc=identity(vrfid:0) <-- ingress interface
```

```
...
```

OSPFv2 및 OSPFv3 인접성은 UP입니다.

```
<#root>
```

```
firepower#
```

```
show ospf neighbor
```

```
Neighbor ID Pri State Dead Time Address Interface  
192.168.103.50 1
```

```
FULL/BDR
```

```
0:00:35 192.168.103.50 OUTSIDE <-- OSPF neighbor is up
```

```
firepower#
```

```
show ipv6 ospf neighbor
```

```
Neighbor ID Pri State Dead Time Interface ID Interface  
192.168.103.50 1
```

```
FULL/BDR
```

```
0:00:34 3267035482 OUTSIDE <-- OSPF neighbor is up
```

다음 상자에 종료되는 멀티캐스트 OSPF 세션입니다.

```
<#root>
```

```
firepower#
```

```
show conn all | include OSPF
```

```
OSPF OUTSIDE fe80::2be:75ff:fef6:1d8e NP Identity Ifc ff02::5, idle 0:00:09, bytes 5924, flags  
OSPF OUTSIDE 192.168.103.50 NP Identity Ifc 224.0.0.5, idle 0:00:03, bytes 8904, flags  
OSPF OUTSIDE ff02::5 NP Identity Ifc fe80::f6db:e6ff:fe33:442e, idle 0:00:01, bytes 6304, flags  
OSPF OUTSIDE 224.0.0.5 NP Identity Ifc 192.168.103.91, idle 0:00:00, bytes 25220, flags
```

테스트로, IPv4에 대한 캡처를 활성화하고 디바이스에 대한 연결을 지웁니다.

```
<#root>
```

```
firepower#
```

```
capture CAP interface OUTSIDE trace
```



```
firepower#
clear conn all

12 connection(s) deleted.
firepower#

clear capture CAP

firepower# !
```

 경고: 이렇게 하면 작동이 중단됩니다! 이 예는 데모용으로만 표시됩니다.

캡처된 OSPF 패킷:

<#root>

```
firepower# show capture CAP | include proto-89

1: 12:25:33.142189 192.168.103.50 > 224.0.0.5 ip-proto-89, length 60
2: 12:25:33.702691 192.168.103.91 > 224.0.0.5 ip-proto-89, length 60
7: 12:25:36.317000 192.168.206.100 > 224.0.0.5 ip-proto-89, length 56
8: 12:25:36.952587 fe80::2be:75ff:fef6:1d8e > ff02::5 ip-proto-89 40 [flowlabel 0xe] [hlim 1]
12: 12:25:41.282608 fe80::f6db:e6ff:fe33:442e > ff02::5 ip-proto-89 40 [flowlabel 0xe] [hlim 1]
```

방화벽에서 OSPFv2 멀티캐스트 패킷을 처리하는 방법은 다음과 같습니다.

<#root>

```
firepower#

show capture CAP packet-number 1 trace

115 packets captured

1: 12:25:33.142189 192.168.103.50 > 224.0.0.5 ip-proto-89, length 60

<-- The first packet of the flow
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 6344 ns
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 6344 ns
Config:
Implicit Rule
Additional Information:
```

MAC Access list

Phase: 3
Type: ROUTE-LOOKUP
Subtype: No ECMP load balancing
Result: ALLOW
Elapsed time: 10736 ns
Config:
Additional Information:
Destination is locally connected. No ECMP load balancing.
Found next-hop 192.168.103.50 using egress ifc OUTSIDE(vrfid:0)

Phase: 4
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 5205 ns
Config:
Implicit Rule
Additional Information:

Phase: 5
Type: NAT
Subtype: per-session
Result: ALLOW
Elapsed time: 5205 ns
Config:
Additional Information:

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Elapsed time: 5205 ns
Config:
Additional Information:

Phase: 7
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Elapsed time: 29280 ns
Config:
Additional Information:

Phase: 8
Type: MULTICAST
Subtype:
Result: ALLOW
Elapsed time: 976 ns
Config:
Additional Information:

Phase: 9

Type: OSPF

<-- The OSPF process

Subtype: ospf

Result: ALLOW

Elapsed time: 488 ns

Config:

Additional Information:

Phase: 10

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Elapsed time: 13176 ns

Config:

Additional Information:

New flow created with id 620, packet dispatched to next module

Result:

input-interface: OUTSIDE(vrfid:0)

input-status: up

input-line-status: up

output-interface: OUTSIDE(vrfid:0)

output-status: up

output-line-status: up

Action: allow

Time Taken: 82959 ns

방화벽에서 OSPFv3 멀티캐스트 패킷을 처리하는 방법은 다음과 같습니다.

<#root>

firepower#

show capture CAP packet-number 8 trace

274 packets captured

8: 12:25:36.952587 fe80::2be:75ff:fef6:1d8e > ff02::5 ip-proto-89 40 [flowlabel 0xe] [hlim 1]

<-- The first packet of the flow

Phase: 1

Type: CAPTURE

Subtype:

Result: ALLOW

Elapsed time: 7564 ns

Config:

Additional Information:

MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 7564 ns
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: ROUTE-LOOKUP
Subtype: No ECMP load balancing
Result: ALLOW
Elapsed time: 8296 ns
Config:
Additional Information:
Destination is locally connected. No ECMP load balancing.
Found next-hop ff02::5 using egress ifc identity(vrfid:0)

Phase: 4
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 8784 ns
Config:
Implicit Rule
Additional Information:

Phase: 5
Type: NAT
Subtype: per-session
Result: ALLOW
Elapsed time: 8784 ns
Config:
Additional Information:

Phase: 6
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Elapsed time: 27816 ns
Config:
Additional Information:

Phase: 7

Type: OSPF

<-- The OSPF process

Subtype: ospf

Result: ALLOW

Elapsed time: 976 ns

Config:

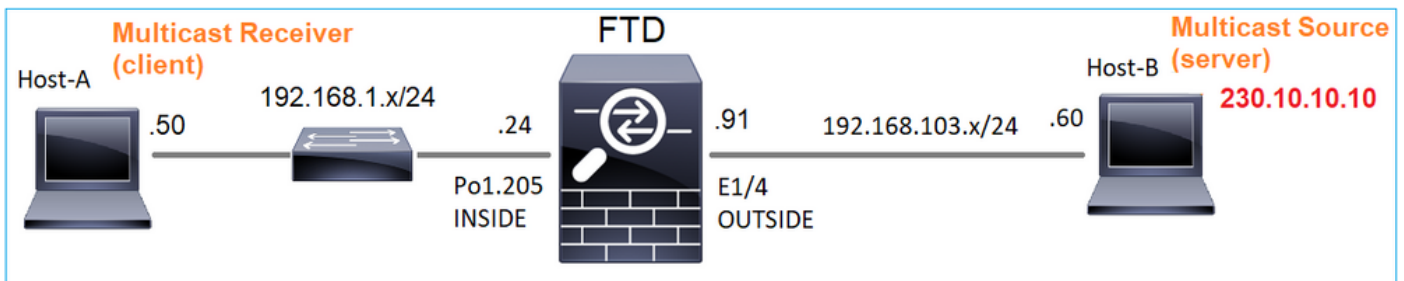
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 13664 ns
Config:
Additional Information:
New flow created with id 624, packet dispatched to next module

Result:
input-interface: OUTSIDE(vrfid:0)
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
Time Taken: 83448 ns

작업 2 - 기본 멀티캐스트 구성

토폴로지



요건

서버의 멀티캐스트 트래픽이 IP 230.10.10의 멀티캐스트 클라이언트로 스트리밍되도록 방화벽을 구성합니다

솔루션

방화벽 관점에서 최소 컨피그레이션은 멀티캐스트 라우팅을 전역적으로 활성화하는 것입니다. 그러면 모든 방화벽 인터페이스에서 백그라운드에서 IGMP 및 PIM이 활성화됩니다.

FMC UI에서:

Firewall Management Center
Devices / NGFW Routing

Overview Analysis Policies **Devices** Objects Integration Deploy

FTD4125-1
Cisco Firepower 4125 Threat Defense

Device Routing Interfaces Inline Sets DHCP

Enable Multicast Routing (Enabling Multicast Routing checkbox will enable both IGMP and PIM on all Interfaces.)

Manage Virtual Routers

Global

Virtual Router Properties

- ECMP
- OSPF
- OSPFv3
- EIGRP
- RIP
- Policy Based Routing
- BGP
 - IPv4
 - IPv6
 - Static Route
 - Multicast Routing
 - IGMP
 - PIM**

Protocol Neighbor Filter Bidirectional Neighbor Filter Rendezvous Points Route Tree Request Filter Bootstrap Router

Interface	PIM Enabled	DR Priority	Hello Interval
No records to display			

방화벽 CLI에서 이는 푸시된 컨피그레이션입니다.

```
<#root>
```

```
firepower#
```

```
show run multicast-routing
```

```
multicast-routing
```

```
<-- Multicast routing is enabled
```

IGMP 확인

```
<#root>
```

```
firepower#
```

```
show igmp interface
```

```
diagnostic is up, line protocol is up
 Internet address is 0.0.0.0/0
 IGMP is disabled on interface
```

```
INSIDE is up, line protocol is up
```

```
<-- The interface is UP
 Internet address is 192.168.1.24/24
```

```
IGMP is enabled on interface
```

```
<-- IGMP is enabled on the interface
```

Current IGMP version is 2

```
<-- IGMP version
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: 1
Cumulative IGMP activity: 4 joins, 3 leaves
IGMP querying router is 192.168.1.24 (this system)
```

OUTSIDE is up, line protocol is up

```
<-- The interface is UP
Internet address is 192.168.103.91/24
```

IGMP is enabled on interface

```
<-- IGMP is enabled on the interface
```

Current IGMP version is 2

```
<-- IGMP version
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: 1
Cumulative IGMP activity: 1 joins, 0 leaves
IGMP querying router is 192.168.103.91 (this system)
```

<#root>

firepower#

show igmp group

```
IGMP Connected Group Membership
Group Address Interface Uptime Expires Last Reporter
239.255.255.250 INSIDE 00:09:05 00:03:19 192.168.1.50
239.255.255.250 OUTSIDE 00:06:01 00:02:33 192.168.103.60
```

<#root>

firepower#

show igmp traffic

```
IGMP Traffic Counters
Elapsed time since counters cleared: 03:40:48 Received Sent
```

	Received	Sent	
Valid IGMP Packets	21	207	
Queries	0	207	
Reports	15	0	<-- IGMP Reports received and sent
Leaves	6	0	
Mtrace packets	0	0	

```

DVMRP packets          0          0
PIM packets            0          0

Errors:
Malformed Packets      0
Martian source         0
Bad Checksums          0

```

PIM 확인

<#root>

firepower#

show pim interface

Address	Interface	PIM	Nbr Count	Hello Intvl	DR Prior	DR
0.0.0.0	diagnostic	off	0	30	1	not elected
192.168.1.24	INSIDE	on	0	30	1	this system
192.168.103.91	OUTSIDE	on	0	30	1	this system

MFIB 확인

<#root>

firepower#

show mfib

Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
AR - Activity Required, K - Keepalive

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second

Other counts: Total/RPF failed/Other drops

Interface Flags: A - Accept, F - Forward, NS - Negate Signalling

IC - Internal Copy, NP - Not platform switched

SP - Signal Present

Interface Counts: FS Pkt Count/PS Pkt Count

(* ,224.0.1.39) Flags: S K

Forwarding: 0/0/0/0

, Other: 0/0/0 <-- The Forwarding counters are: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second

(* ,224.0.1.40) Flags: S K

Forwarding: 0/0/0/0,

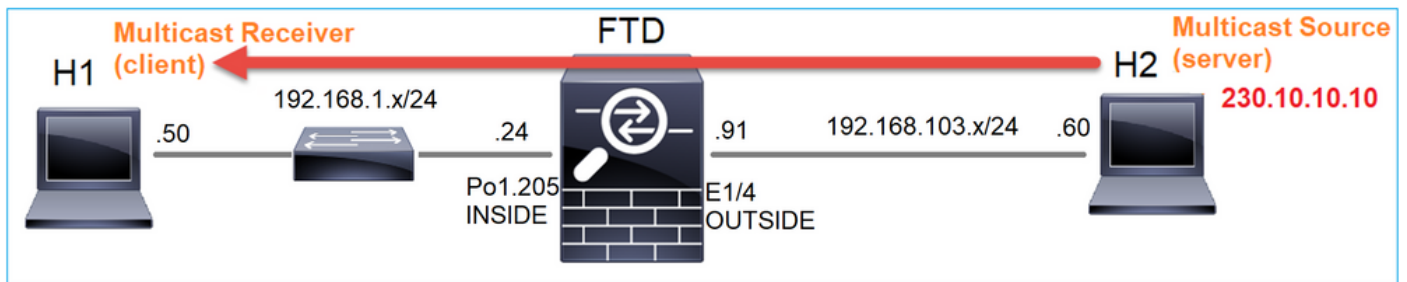
Other: 8/8/0

<-- The Other counters are: Total/RPF failed/Other drops

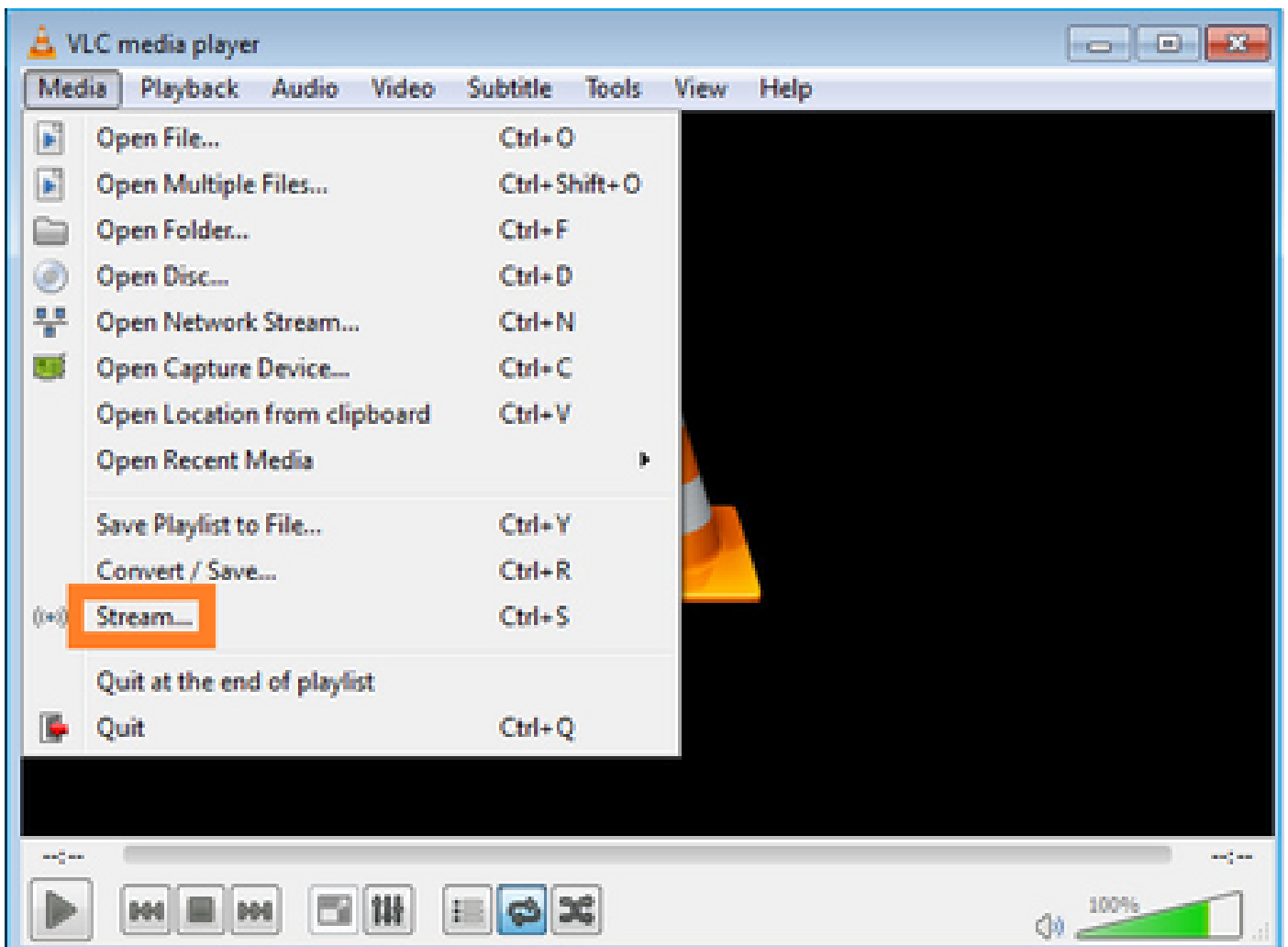
(* ,232.0.0.0/8) FFlags: K
Forwarding: 0/0/0/0, Other: 0/0/0

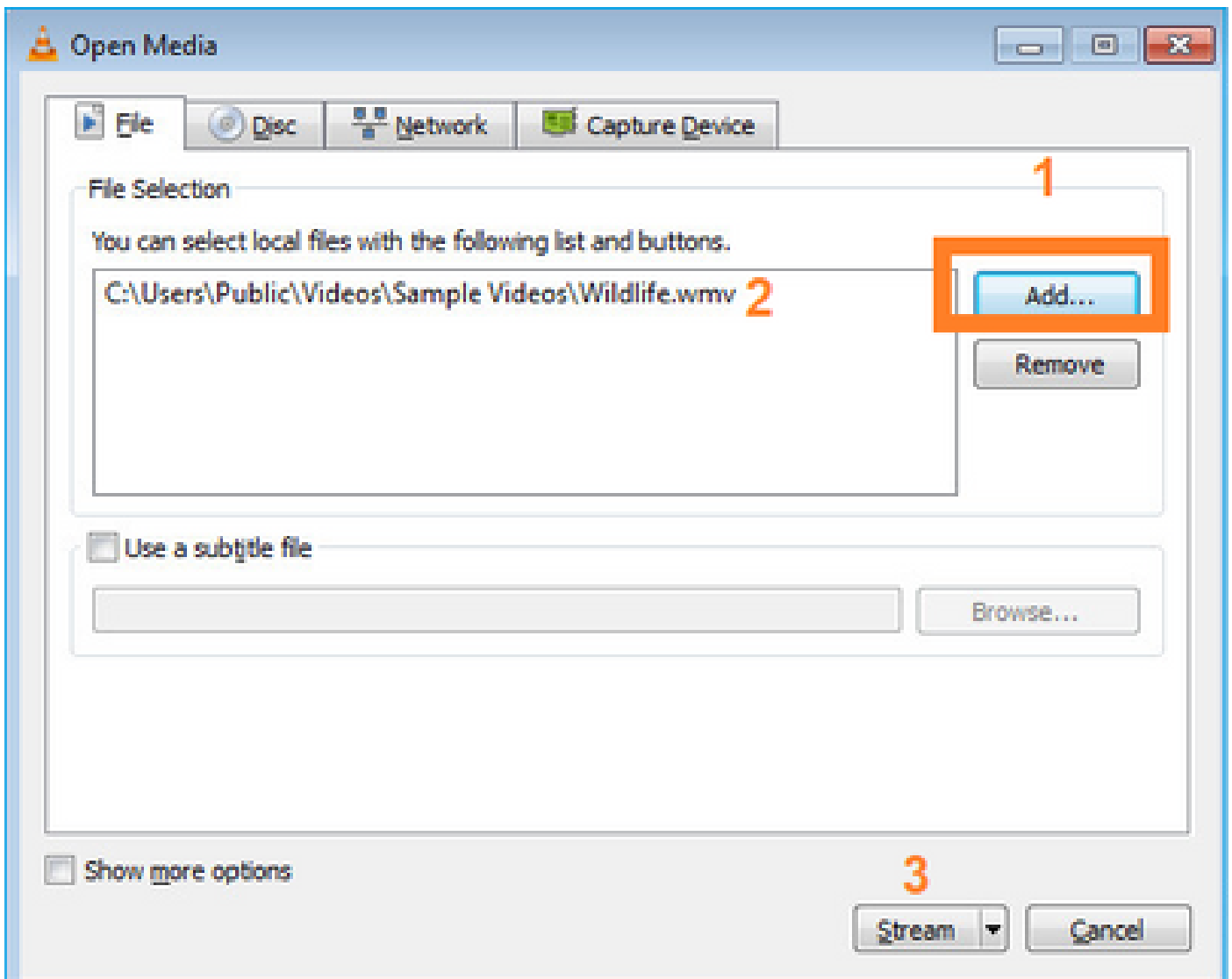
방화벽을 통과하는 멀티캐스트 트래픽

이 경우 VLC 미디어 플레이어 애플리케이션은 멀티캐스트 서버 및 클라이언트로 사용되어 멀티캐스트 트래픽을 테스트합니다.



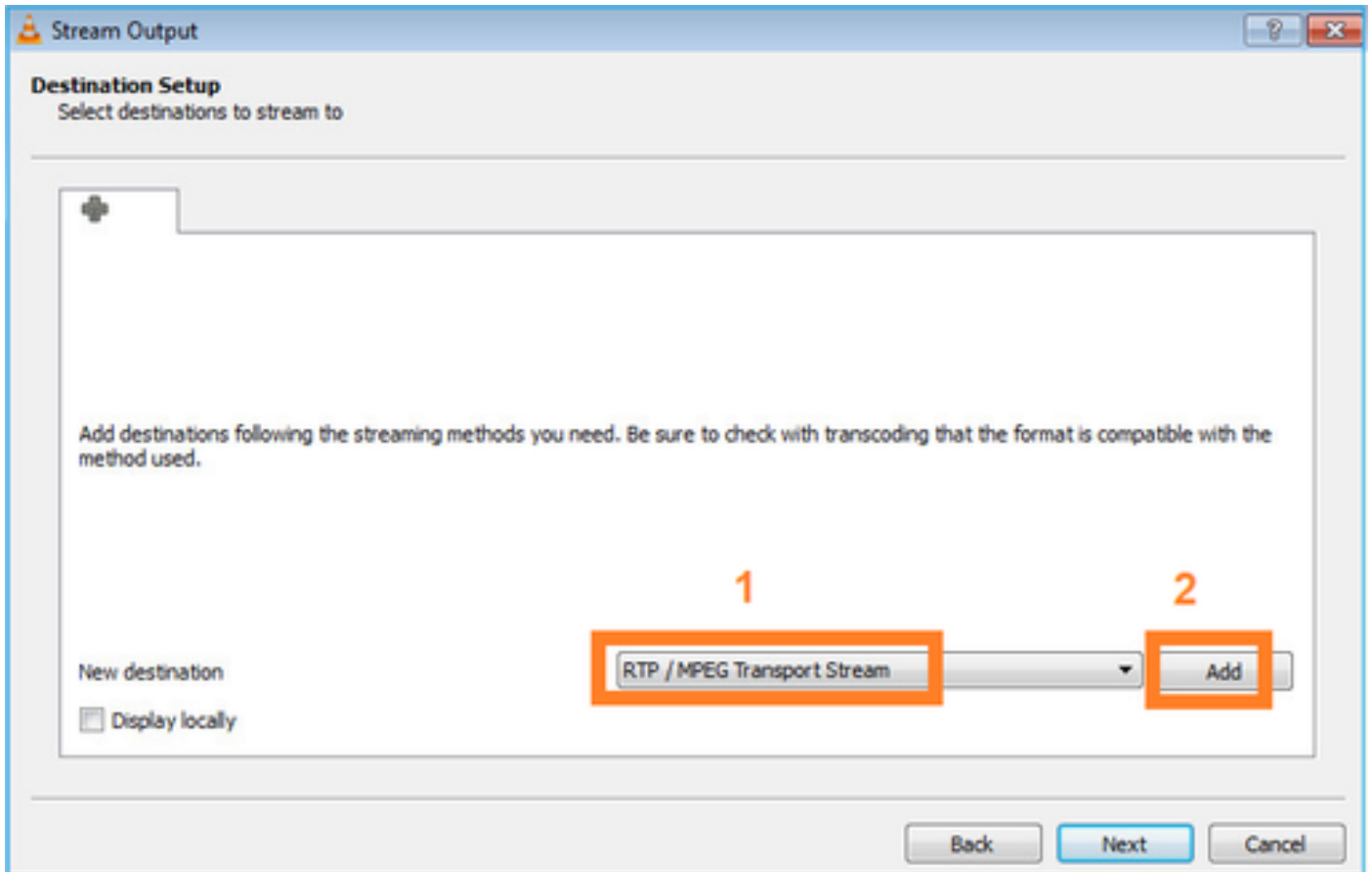
VLC 멀티캐스트 서버 구성:



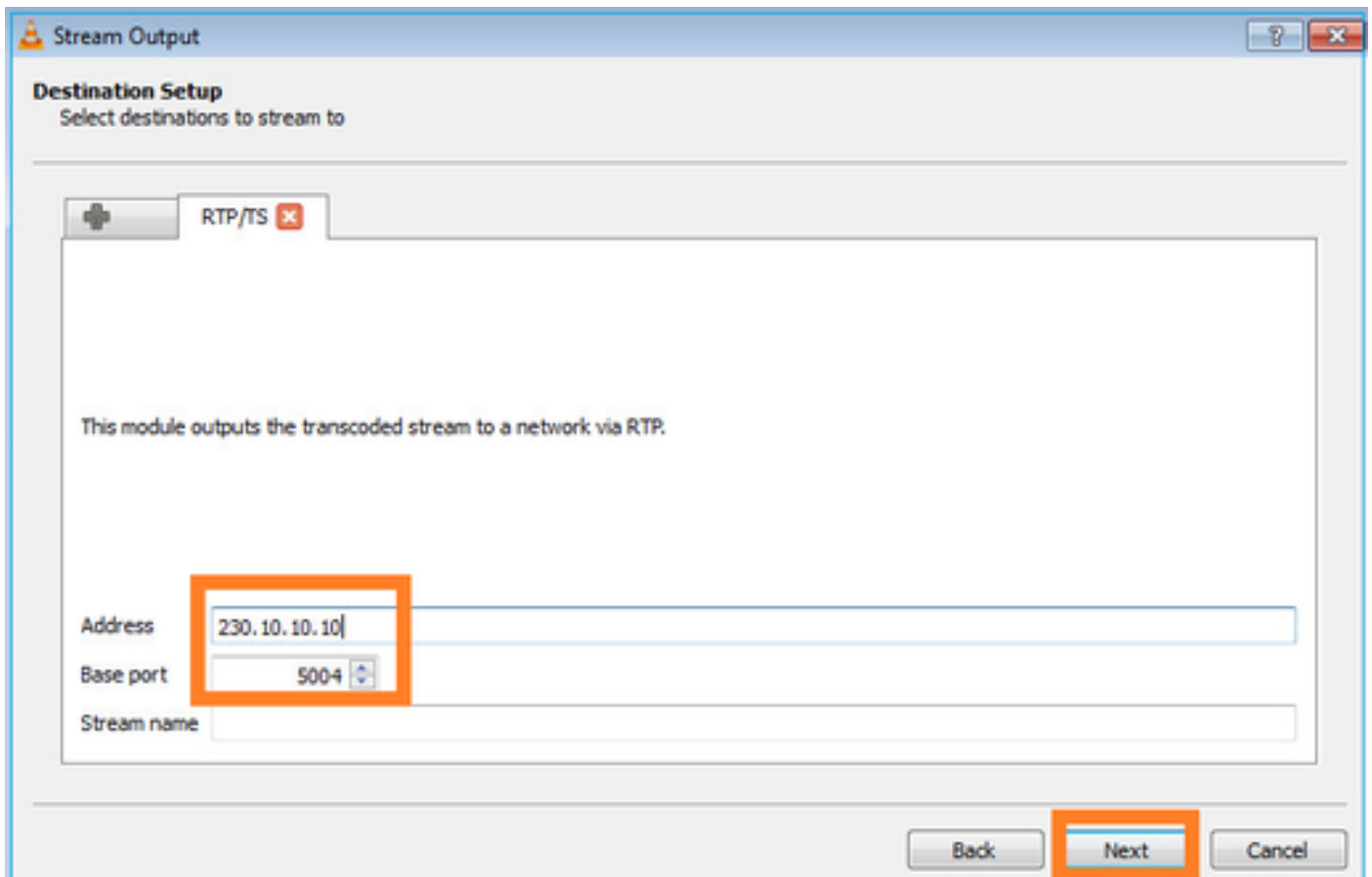


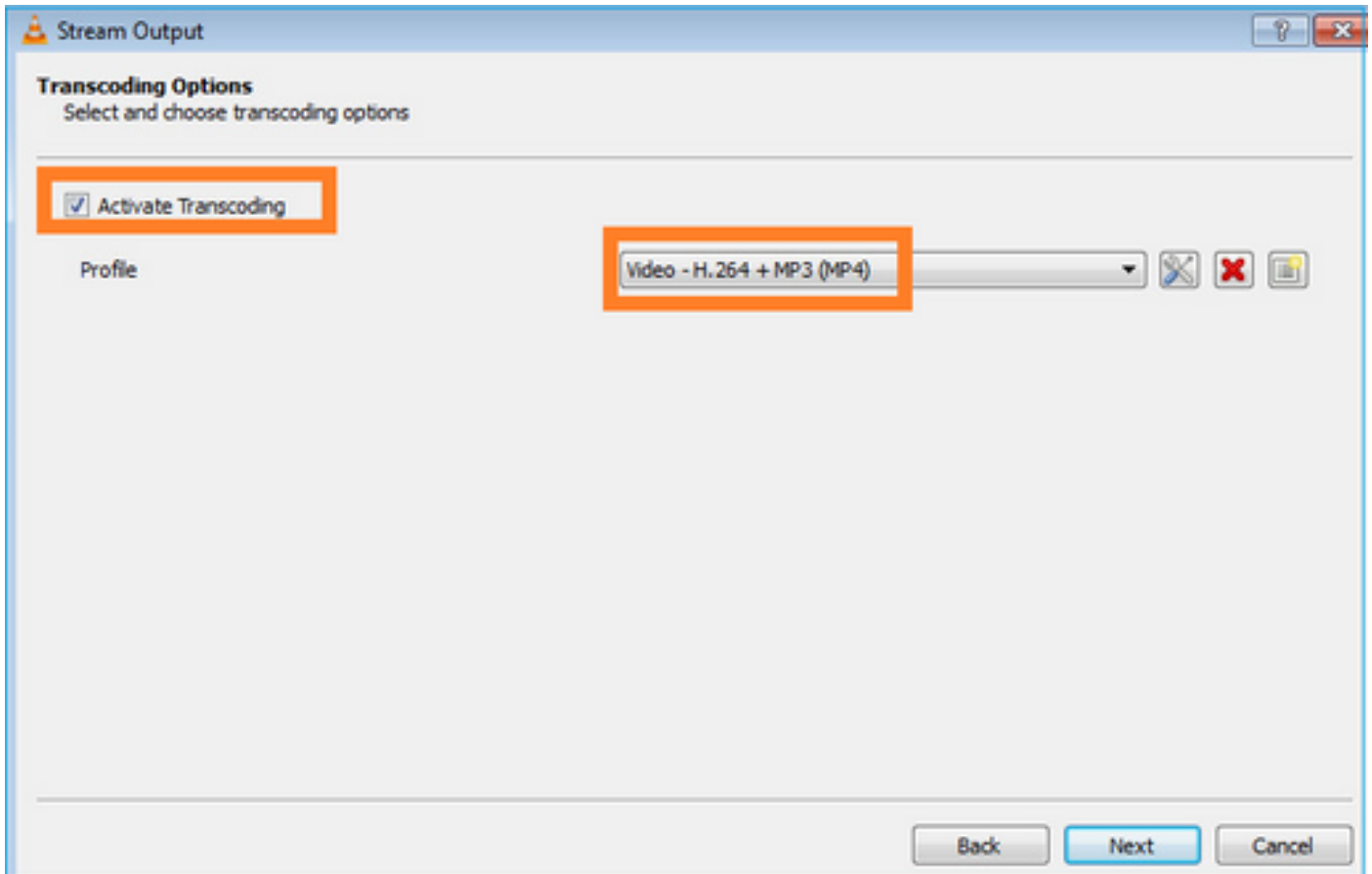
다음 화면에서 Next(다음)를 선택합니다.

형식 선택:



멀티캐스트 IP 및 포트를 지정합니다.





FTD 방화벽에서 LINA 캡처를 활성화합니다.

```
<#root>
```

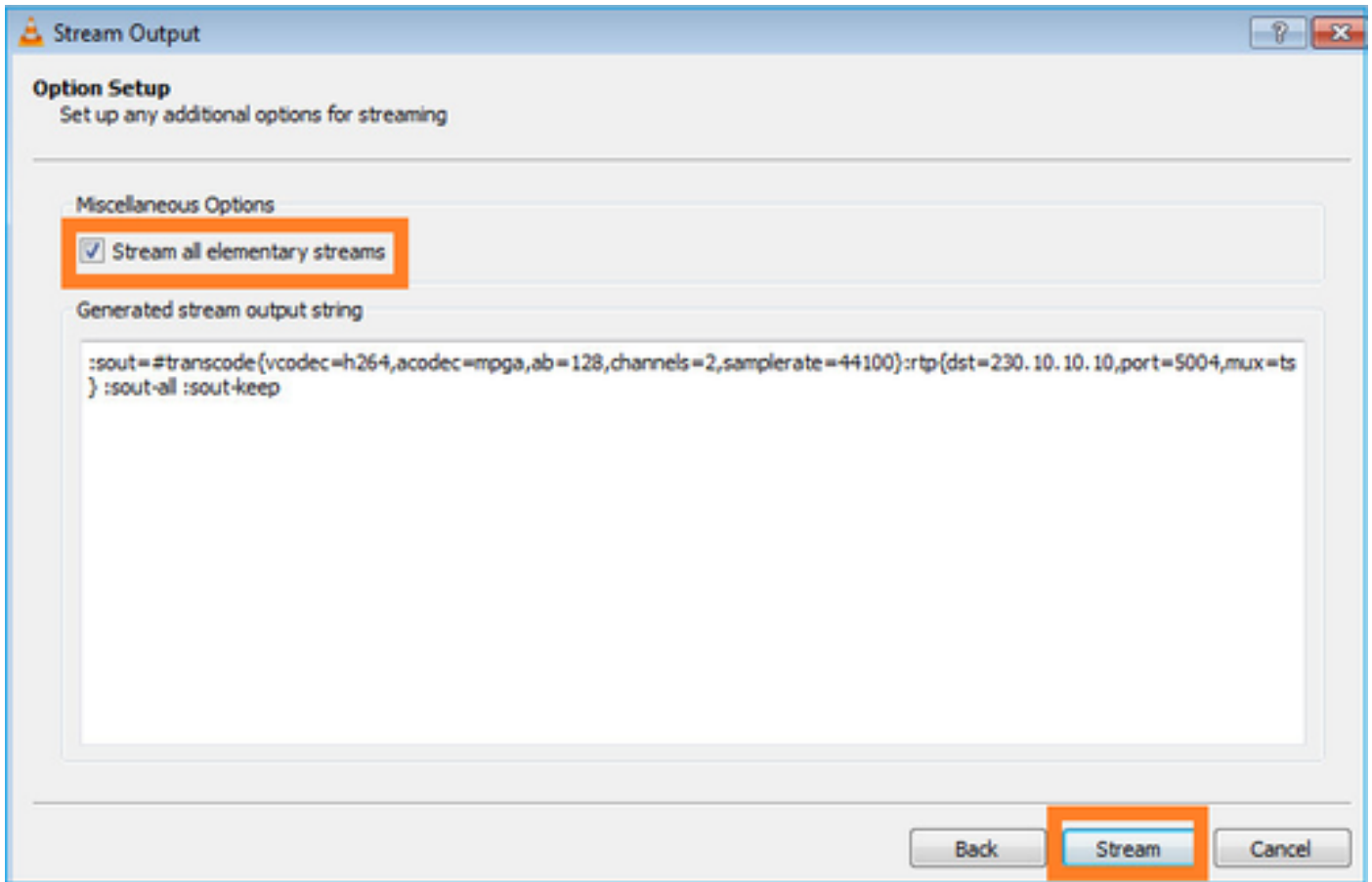
```
firepower#
```

```
capture INSIDE interface INSIDE match ip host 192.168.103.60 host 230.10.10.10
```

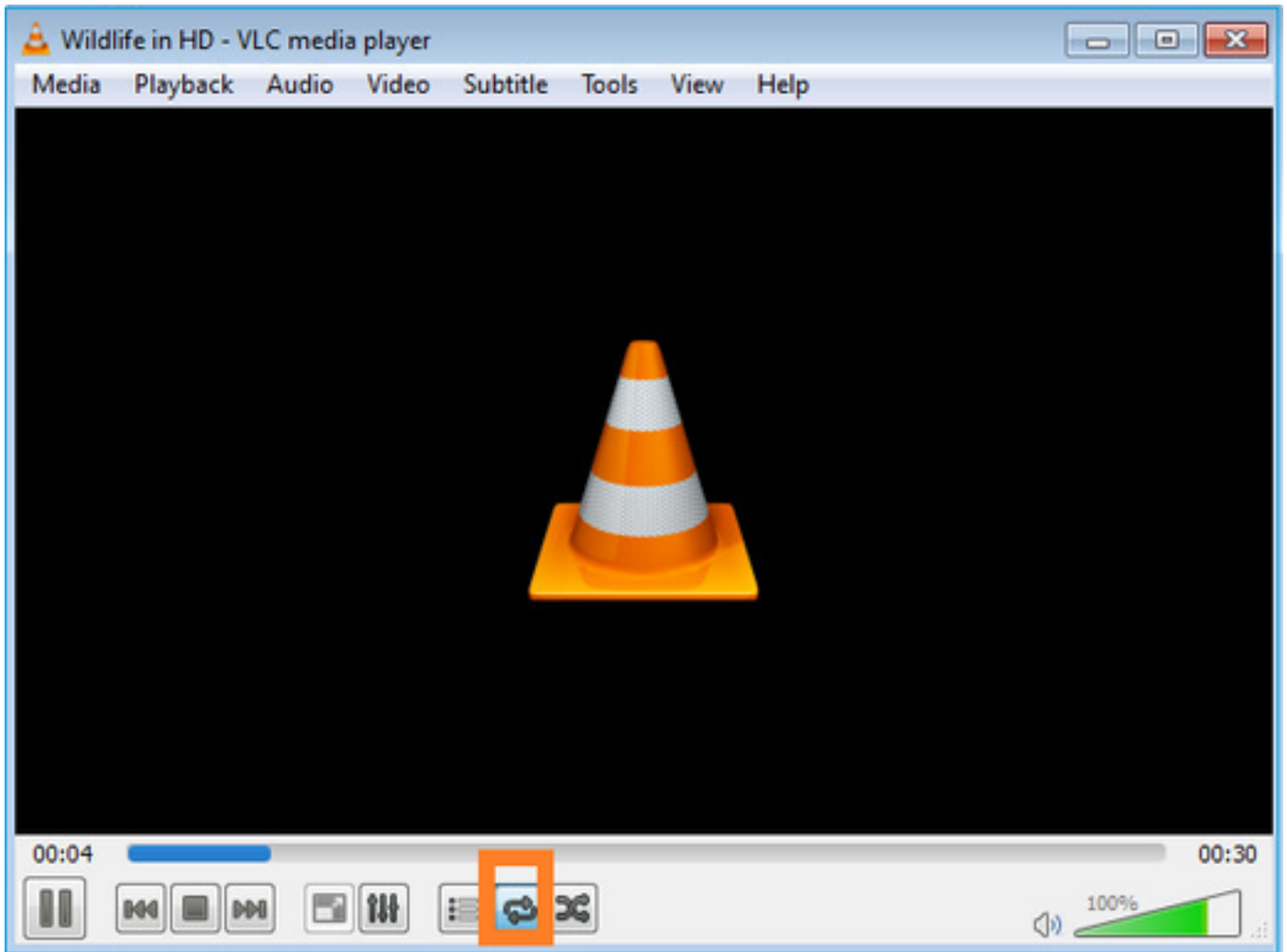
```
firepower#
```

```
capture OUTSIDE interface OUTSIDE trace match ip host 192.168.103.60 host 230.10.10.10
```

멀티캐스트 스트림을 시작할 디바이스에 대한 Stream 버튼을 선택합니다.



스트림이 연속적으로 전송되도록 'loop' 옵션을 활성화합니다.



확인(비작동 시나리오)

이 시나리오는 비작동 시나리오를 보여 주는 예입니다. 목표는 방화벽 동작을 시연하는 것입니다. 방화벽 디바이스는 멀티캐스트 스트림을 가져오지만 전달하지는 않습니다.

```
<#root>
```

```
firepower#
```

```
show capture
```

```
capture INSIDE type raw-data interface INSIDE
```

```
[Capturing - 0 bytes]
```

```
<-- No packets sent or received
```

```
match ip host 192.168.103.60 host 230.10.10.10
```

```
capture OUTSIDE type raw-data trace interface OUTSIDE
```

```
[Buffer Full - 524030 bytes]
```

```
<-- The buffer is full
```

```
match ip host 192.168.103.60 host 230.10.10.10
```

방화벽 LINA ASP 삭제는 다음과 같습니다.

```
<#root>
```

```
firepower#
```

```
clear asp drop
```

```
firepower#
```

```
show asp drop
```

Frame drop:

```
Punt rate limit exceeded (punt-rate-limit)                232
```

```
<-- The multicast packets were dropped  
  Flow is denied by configured rule (acl-drop)            2  
  FP L2 rule drop (l2_acl)                                2
```

```
Last clearing: 18:38:42 UTC Oct 12 2018 by enable_15
```

Flow drop:

```
Last clearing: 08:45:41 UTC May 17 2022 by enable_15
```

패킷을 추적하려면 멀티캐스트 흐름의 첫 번째 패킷을 캡처해야 합니다. 이러한 이유로 현재 흐름을 지웁니다.

```
<#root>
```

```
firepower#
```

```
clear capture OUTSIDE
```

```
firepower#
```

```
clear conn all addr 230.10.10.10
```

```
2 connection(s) deleted.
```

```
firepower#
```

```
show capture OUTSIDE
```

```
379 packets captured
```

```
1: 08:49:04.537875 192.168.103.60.54100 > 230.10.10.10.5005: udp 64  
2: 08:49:04.537936 192.168.103.60.54099 > 230.10.10.10.5004: udp 1328  
3: 08:49:04.538027 192.168.103.60.54099 > 230.10.10.10.5004: udp 1328  
4: 08:49:04.538058 192.168.103.60.54099 > 230.10.10.10.5004: udp 1328  
5: 08:49:04.538058 192.168.103.60.54099 > 230.10.10.10.5004: udp 1328  
6: 08:49:04.538073 192.168.103.60.54099 > 230.10.10.10.5004: udp 1328  
...
```

'detail' 옵션은 멀티캐스트 MAC 주소를 나타냅니다.

```
<#root>
```

```
firepower#
```

```
show capture OUTSIDE detail
```

```
379 packets captured
```

```
1: 08:49:04.537875 0050.569d.344a
```

```
0100.5e0a.0a0a
```

```
0x0800 Length: 106
```

```
192.168.103.60.54100 > 230.10.10.10.5005: [udp sum ok] udp 64 (ttl 100, id 19759)
```

```
2: 08:49:04.537936 0050.569d.344a
```

```
0100.5e0a.0a0a
```

```
0x0800 Length: 1370
```

```
192.168.103.60.54099 > 230.10.10.10.5004: [udp sum ok] udp 1328 (ttl 100, id 19760)
```

```
3: 08:49:04.538027 0050.569d.344a 0100.5e0a.0a0a 0x0800 Length: 1370
```

```
192.168.103.60.54099 > 230.10.10.10.5004: [udp sum ok] udp 1328 (ttl 100, id 19761)
```

```
...
```

실제 패킷의 추적은 해당 패킷이 허용됨을 보여주지만, 실제로 일어나는 일은 아닙니다.

```
<#root>
```

```
firepower#
```

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

```
379 packets captured
```

```
1: 08:49:04.537875 192.168.103.60.54100 > 230.10.10.10.5005: udp 64
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Elapsed time: 11712 ns
```

```
Config:
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Elapsed time: 11712 ns
```

```
Config:
```

```
Implicit Rule
```


Additional Information:

MAC Access list

Phase: 3

Type: ROUTE-LOOKUP

Subtype: No ECMP load balancing

Result: ALLOW

Elapsed time: 7808 ns

Config:

Additional Information:

Destination is locally connected. No ECMP load balancing.

Found next-hop 192.168.103.60 using egress ifc OUTSIDE(vrfid:0)

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Elapsed time: 5246 ns

Config:

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434432

access-list CSM_FW_ACL_ remark rule-id 268434432: ACCESS POLICY: mzafeiro_empty - Default

access-list CSM_FW_ACL_ remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5

Type: CONN-SETTINGS

Subtype:

Result: ALLOW

Elapsed time: 5246 ns

Config:

class-map class-default

match any

policy-map global_policy

class class-default

set connection advanced-options UM_STATIC_TCP_MAP

service-policy global_policy global

Additional Information:

Phase: 6

Type: NAT

Subtype: per-session

Result: ALLOW

Elapsed time: 5246 ns

Config:

Additional Information:

Phase: 7

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Elapsed time: 5246 ns

Config:

Additional Information:

Phase: 8

Type: CLUSTER-REDIRECT

Subtype: cluster-redirect

Result: ALLOW

Elapsed time: 31232 ns

Config:

Additional Information:

Phase: 9

Type: MULTICAST

<-- multicast process

Subtype:

Result: ALLOW

Elapsed time: 976 ns

Config:

Additional Information:

Phase: 10

Type: FLOW-CREATION

<-- the packet belongs to a new flow

Subtype:

Result: ALLOW

Elapsed time: 20496 ns

Config:

Additional Information:

New flow created with id 3705, packet dispatched to next module

Result:

input-interface: OUTSIDE(vrfid:0)

input-status: up

input-line-status: up

output-interface: OUTSIDE(vrfid:0)

output-status: up

output-line-status: up

Action: allow

<-- The packet is allowed

Time Taken: 104920 ns

mroute 및 mfib 카운터를 기준으로 OIL(Outgoing Interface List)이 비어 있으므로 패킷이 삭제됩니다.

<#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

(192.168.103.60, 230.10.10.10), 00:01:33/00:01:56, flags: SPF

Incoming interface: OUTSIDE

RPF nbr: 192.168.103.60

Outgoing interface list: Null

<-- The OIL is empty!

(* , 239.255.255.250), 00:01:50/never, RP 0.0.0.0, flags: SCJ

Incoming interface: Null

RPF nbr: 0.0.0.0

Immediate Outgoing interface list:

INSIDE, Forward, 00:01:50/never

MFIB 카운터는 RPF 실패를 보여줍니다. 이 경우 실제로 발생하는 것은 아닙니다.

<#root>

firepower#

show mfib 230.10.10.10

Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
AR - Activity Required, K - Keepalive

firepower# show mfib 230.10.10.10

Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
AR - Activity Required, K - Keepalive

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second

<-- Multicast forwarding counters

Other counts: Total/RPF failed

/Other drops <-- Multicast drop counters

Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
IC - Internal Copy, NP - Not platform switched
SP - Signal Present

Interface Counts: FS Pkt Count/PS Pkt Count

(192.168.103.60,230.10.10.10) Flags: K

Forwarding: 0/0/0/0

,

Other: 650/650

/0 <-- Allowed and dropped multicast packets

'show mfib count' 출력에서 유사한 RPF 실패:

<#root>

firepower#

show mfib 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: 224.0.1.39

RP-tree:

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

Group: 224.0.1.40

RP-tree:

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

Group: 230.10.10.10

Source: 192.168.103.60,

Forwarding: 0/0/0/0,

Other: 1115/1115

/0 <-- Allowed and dropped multicast packets

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

Group: 232.0.0.0/8

RP-tree:

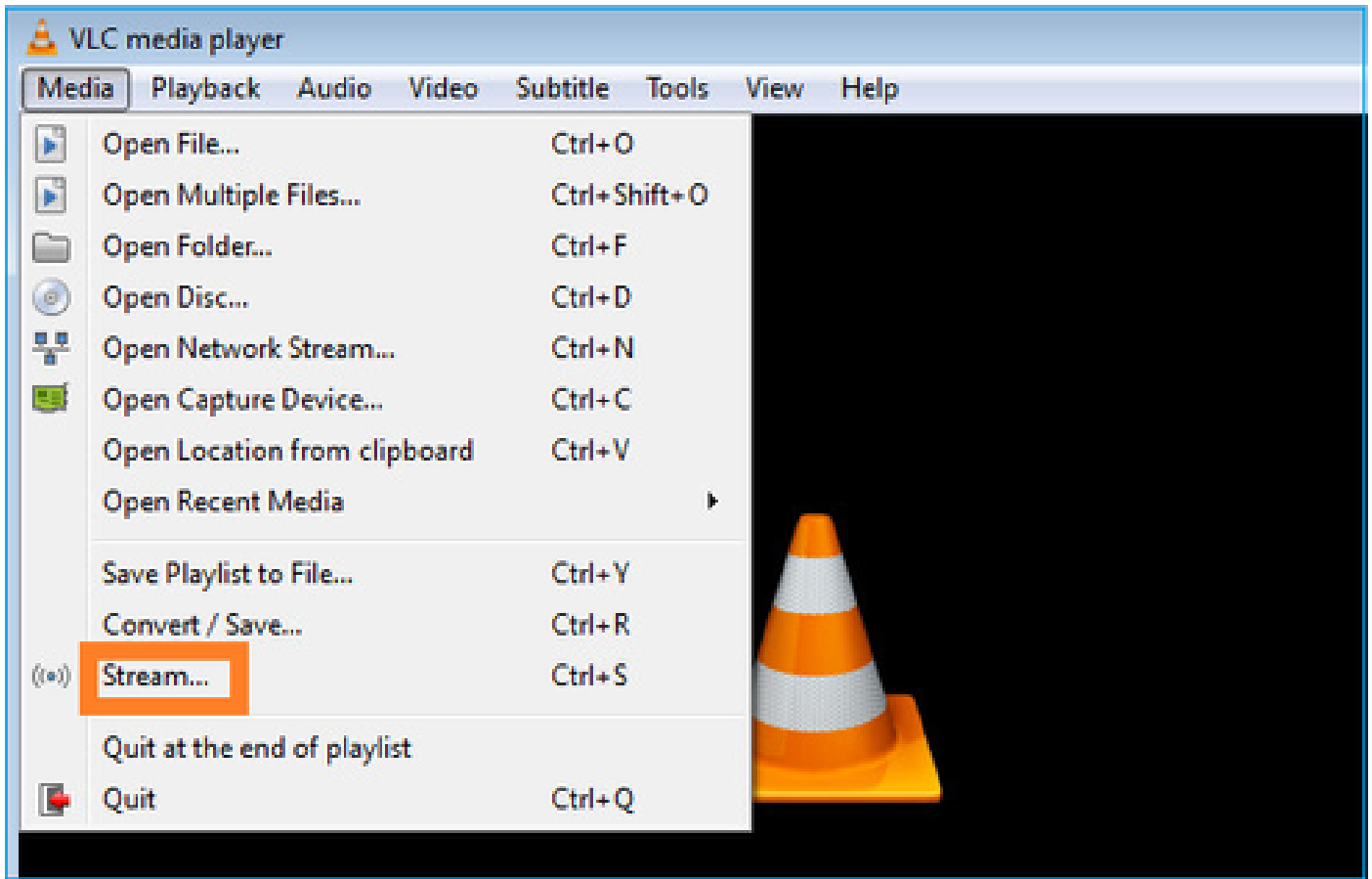
Forwarding: 0/0/0/0, Other: 0/0/0

Group: 239.255.255.250

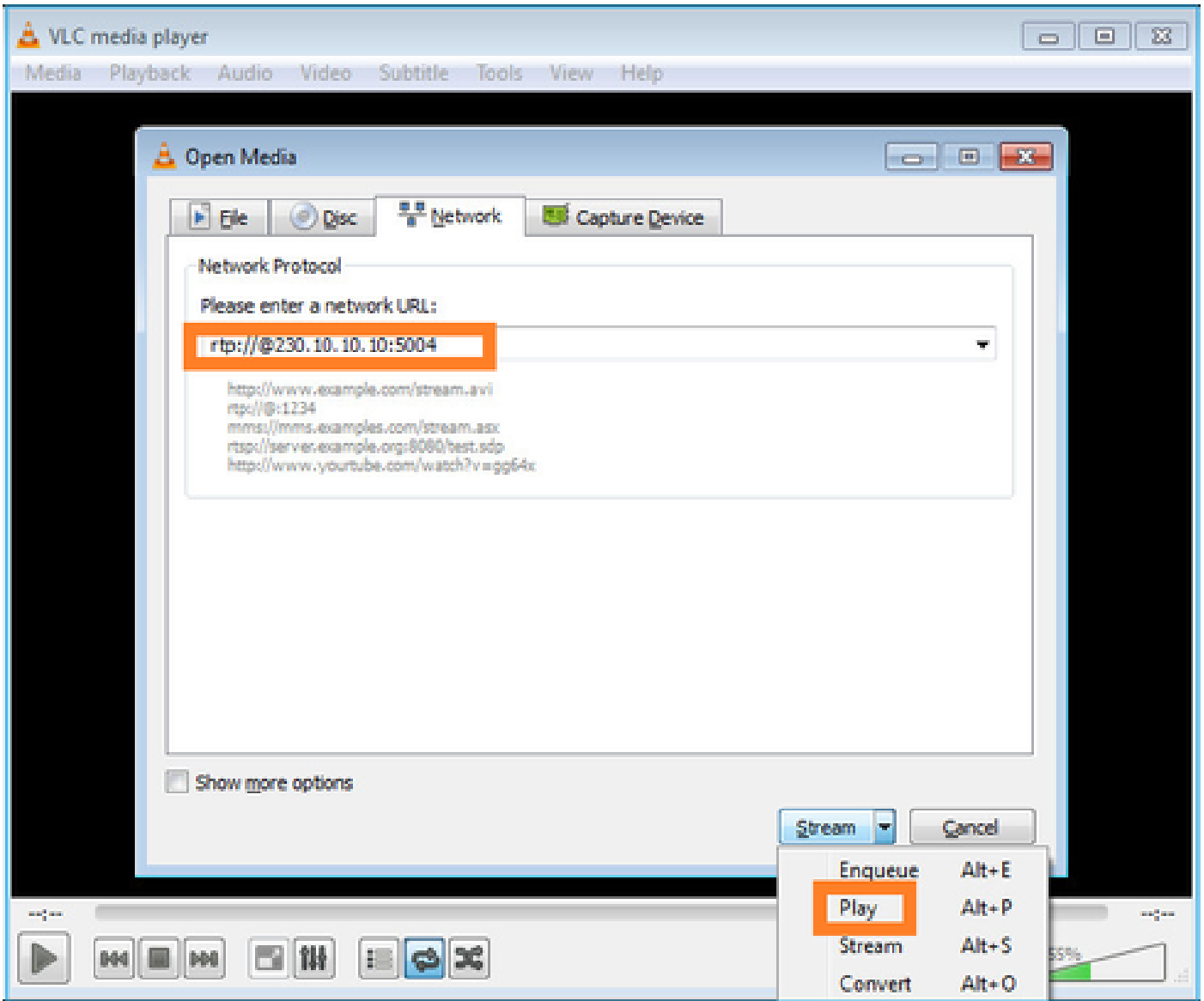
RP-tree:

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

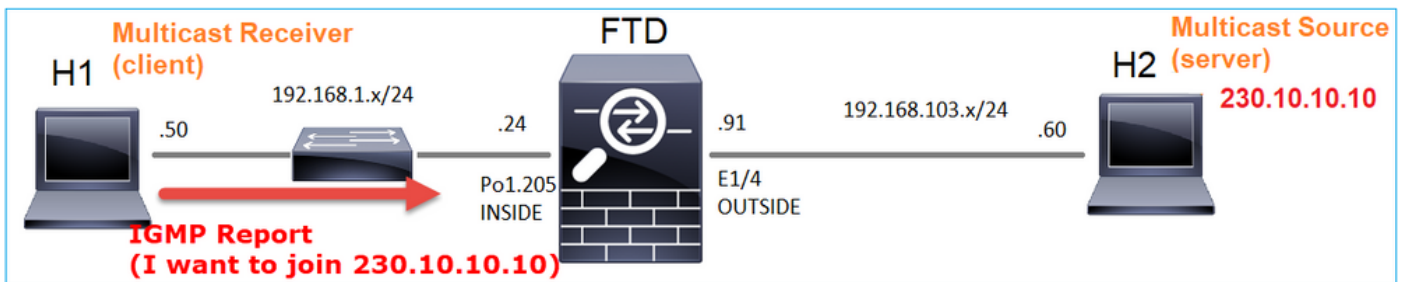
VLC 멀티캐스트 수신기를 구성합니다.



멀티캐스트 소스 IP를 지정하고 Play를 선택합니다.



백엔드에서 Play(재생)를 선택하는 즉시 호스트가 특정 멀티캐스트 그룹에 가입할 의사를 알리고 IGMP Report(IGMP 보고서) 메시지를 전송합니다.



디버그를 활성화하면 IGMP 보고서 메시지를 볼 수 있습니다.

```
<#root>
```

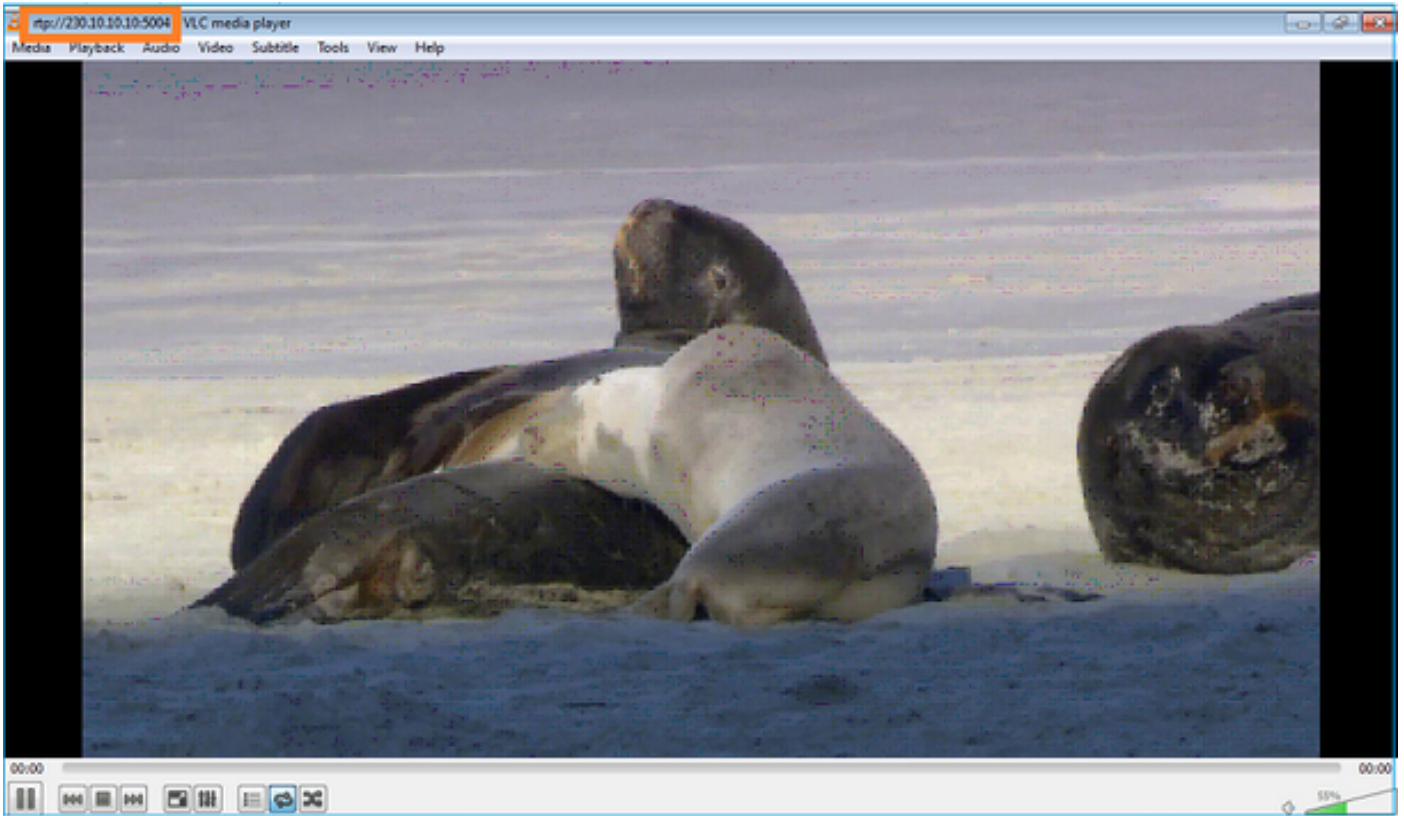
```
firepower#
```

```
debug igmp group 230.10.10.10
```

```
IGMP: Received v2 Report on INSIDE from 192.168.1.50 for 230.10.10.10
```

```
<-- IGMPv2 Report received  
IGMP: group_db: add new group 230.10.10.10 on INSIDE  
IGMP: MRIB updated (*,230.10.10.10) : Success  
IGMP: Switching to EXCLUDE mode for 230.10.10.10 on INSIDE  
IGMP: Updating EXCLUDE group timer for 230.10.10.10
```

스트림은 다음과 같이 시작됩니다.



확인(운영 시나리오)

```
<#root>
```

```
firepower#
```

```
show capture
```

```
capture INSIDE type raw-data interface INSIDE
```

```
[Buffer Full - 524156 bytes]
```

```
<-- Multicast packets on the egress interface  
match ip host 192.168.103.60 host 230.10.10.10  
capture OUTSIDE type raw-data trace interface OUTSIDE
```

```
[Buffer Full - 524030 bytes]
```

```
<-- Multicast packets on the ingress interface  
match ip host 192.168.103.60 host 230.10.10.10
```

방화벽의 mroute 테이블:

<#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

(* , 230.10.10.10), 00:00:34/never, RP 0.0.0.0, flags: SCJ

Incoming interface: Null

RPF nbr: 0.0.0.0

Immediate Outgoing interface list:

INSIDE, Forward, 00:00:34/never

(192.168.103.60 , 230.10.10.10), 00:01:49/00:03:29, flags: SFJT

Incoming interface: OUTSIDE

RPF nbr: 192.168.103.60

Inherited Outgoing interface list:

INSIDE, Forward, 00:00:34/never

<-- The OIL shows an interface

<#root>

firepower#

show mfib 230.10.10.10

Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
AR - Activity Required, K - Keepalive

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second

Other counts: Total/RPF failed/Other drops

Interface Flags: A - Accept, F - Forward, NS - Negate Signalling

IC - Internal Copy, NP - Not platform switched
SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count

(* ,230.10.10.10) Flags: C K
Forwarding: 0/0/0/0, Other: 0/0/0
INSIDE Flags: F NS
Pkts: 0/0

(192.168.103.60,230.10.10.10) Flags: K

Forwarding: 6373/0/1354/0,

Other: 548/548/0 <-- There are multicast packets forwarded

OUTSIDE Flags: A

INSIDE Flags: F NS

Pkts: 6373/6

mfib 카운터:

<#root>

firepower#

show mfib count

IP Multicast Statistics

10 routes, 5 groups, 0.40 average sources per group

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second

Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group: 224.0.1.39

RP-tree:

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

Group: 224.0.1.40

RP-tree:

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

Group: 230.10.10.10

RP-tree:

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

Source: 192.168.103.60,

Forwarding: 7763/0/1354/0,

Other: 548/548/0 <-- There are multicast packets forwarded

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

Group: 232.0.0.0/8

RP-tree:

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

Group: 239.255.255.250

RP-tree:

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

Source: 192.168.1.50,

Forwarding: 7/0/500/0, Other: 0/0/0

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

IGMP 스누핑

- IGMP 스누핑은 멀티캐스트 플러딩을 방지하기 위해 스위치에서 사용되는 메커니즘입니다.
- 스위치는 IGMP 보고서를 모니터링하여 호스트(수신기)의 위치를 확인합니다.
- 스위치는 IGMP 쿼리를 모니터링하여 라우터/방화벽(발신자)의 위치를 확인합니다.
- IGMP 스누핑은 대부분의 Cisco 스위치에서 기본적으로 활성화되어 있습니다. 자세한 내용은 관련 스위칭 가이드를 참조하십시오. 다음은 L3 Catalyst 스위치의 샘플 출력입니다.

<#root>

switch#

show ip igmp snooping statistics

```
Current number of Statistics entries      : 15
Configured Statistics database limit      : 32000
Configured Statistics database threshold: 25600
Configured Statistics database limit      : Not exceeded
Configured Statistics database threshold: Not exceeded
```

Snooping statistics for Vlan204

#channels: 3

#hosts : 5

Source/Group	Interface	Reporter	Uptime	Last-Join	Last-Leave
0.0.0.0/230.10.10.10	Vl204:Gi1/48	192.168.1.50	2d13h	-	2d12h
0.0.0.0/230.10.10.10	Vl204:Gi1/48	192.168.1.97	2d13h	2d12h	-
0.0.0.0/230.10.10.10	Vl204:Gi2/1	192.168.1.50	2d10h	02:20:05	02:20:00
0.0.0.0/239.255.255.250	Vl204:Gi2/1	192.168.1.50	2d11h	02:20:05	02:20:00
0.0.0.0/239.255.255.250	Vl204:Gi2/1	192.168.2.50	2d14h	2d13h	-
0.0.0.0/239.255.255.250	Vl204:Gi2/1	192.168.6.50	2d13h	-	2d13h
0.0.0.0/224.0.1.40	Vl204:Gi2/26	192.168.2.1	2d14h	00:00:39	2d13h

Snooping statistics for Vlan206

#channels: 4

#hosts : 3

Source/Group	Interface	Reporter	Uptime	Last-Join	Last-Leave
0.0.0.0/230.10.10.10	Vl206:Gi1/48	192.168.6.91	00:30:15	2d13h	2d13h

0.0.0.0/239.10.10.10	V1206:Gi1/48	192.168.6.91	2d14h	2d13h	-
0.0.0.0/239.255.255.250	V1206:Gi2/1	192.168.6.50	2d12h	00:52:49	00:52:45
0.0.0.0/224.0.1.40	V1206:Gi2/26	192.168.6.1	00:20:10	2d13h	2d13h
0.0.0.0/230.10.10.10	V1206:Gi2/26	192.168.6.1	2d13h	2d13h	-
0.0.0.0/230.10.10.10	V1206:Gi2/26	192.168.6.91	2d13h	-	2d13h
0.0.0.0/239.10.10.10	V1206:Gi2/26	192.168.6.1	2d14h	2d14h	-
0.0.0.0/239.10.10.10	V1206:Gi2/26	192.168.6.91	2d14h	-	2d14h

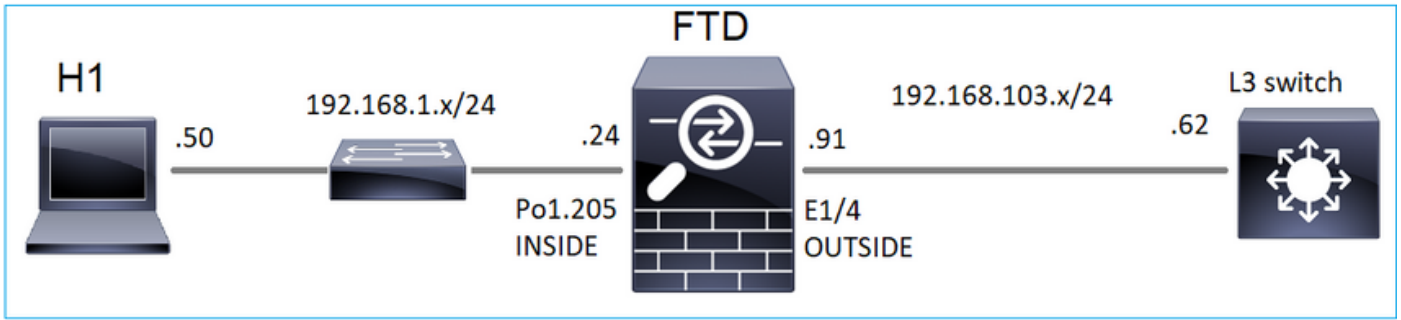
작업 3 - IGMP 고정 그룹 vs IGMP 조인 그룹

개요

	ip igmp 고정 그룹	ip igmp 조인 그룹
FTD 인터페이스에 적용됩니까?	예	예
FTD가 멀티캐스트 스트림을 끌어오는가?	예, PIM 조인이 업스트림 장치 또는 RP(Rendezvous Point)로 전송됩니다. 이 명령을 사용하는 FTD가 해당 인터페이스의 PIM DR(Designated Router)인 경우에만 발생합니다.	예, PIM 조인이 업스트림 장치 또는 RP(Rendezvous Point)로 전송됩니다. 이 명령을 사용하는 FTD가 해당 인터페이스의 PIM DR(Designated Router)인 경우에만 발생합니다.
FTD에서 멀티캐스트 트래픽을 인터페이스 외부로 전달합니까?	예	예
FTD에서 멀티캐스트 트래픽을 사용하고 이에 응답합니까?	아니요	예, FTD는 멀티캐스트 스트림을 CPU에 푸시하고, 이를 소비하고, 소스에 응답합니다.
CPU 영향	패킷이 CPU에 할당되지 않으므로 최소입니다.	그룹에 속한 각 멀티캐스트 패킷이 FTD CPU에 대해 편딩되므로 FTD CPU에 영향을 줄 수 있습니다.

작업 요구 사항

다음 토폴로지를 고려하십시오.



방화벽에서 다음 캡처를 활성화합니다.

<#root>

firepower#

```
capture CAPI interface OUTSIDE trace match icmp host 192.168.103.62 any
```

firepower#

```
capture CAPO interface INSIDE match icmp host 192.168.103.62 any
```

1. L3 스위치에서 ICMP ping을 사용하여 멀티캐스트 트래픽을 IP 230.11.11.11로 전송하고 방화벽에서 이를 어떻게 처리하는지 확인합니다.
2. 방화벽 INSIDE 인터페이스에서 igmp static-group 명령을 활성화하고 멀티캐스트 스트림(IP 230.11.11.11)이 방화벽에서 처리되는 방식을 확인합니다.
3. 방화벽 INSIDE 인터페이스에서 igmp static-group 명령을 활성화하고 멀티캐스트 스트림(IP 230.11.11.11)이 방화벽에서 처리되는 방식을 확인합니다.

솔루션

방화벽에는 IP 230.11.11.11에 대한 경로가 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

```
(*, 239.255.255.250), 00:43:21/never, RP 0.0.0.0, flags: SCJ
```

```
Incoming interface: Null
```

```
RPF nbr: 0.0.0.0
```

```
Immediate Outgoing interface list:
```

```
OUTSIDE, Forward, 00:05:41/never
```

```
INSIDE, Forward, 00:43:21/never
```

멀티캐스트를 테스트하는 간단한 방법은 ICMP ping 툴을 사용하는 것입니다. 이 경우 R2에서 멀티캐스트 IP 주소 230.11.11.11로 ping을 시작합니다.

```
<#root>
```

```
L3-Switch#
```

```
ping 230.11.11.11 re 100
```

```
Type escape sequence to abort.
```

```
Sending 100, 100-byte ICMP Echos to 230.11.11.11, timeout is 2 seconds:
```

```
.....
```

방화벽에서 mroute는 동적으로 생성되며 OIL은 비어 있습니다.

```
<#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
```

```
(192.168.103.62, 230.11.11.11), 00:02:33/00:00:56, flags: SPF
```

```
<-- The mroute is added
```

```
    Incoming interface: OUTSIDE
```

```
    RPF nbr: 192.168.103.62
```

```
    Outgoing interface list: Null
```

```
<-- The OIL is empty
```

방화벽의 캡처에는 다음이 표시됩니다.

```
<#root>
```

```
firepower# show capture
```

```
capture CAPI type raw-data trace interface OUTSIDE
```

```
[Capturing - 1040 bytes]
```

```
<-- There are ICMP packets captured on ingress interface  
match icmp host 192.168.103.62 any  
capture CAPO type raw-data interface INSIDE
```

```
[Capturing - 0 bytes]
```

```
<-- There are no ICMP packets on egress  
match icmp host 192.168.103.62 any
```

방화벽은 각 ping에 대한 연결을 생성하지만, 패킷을 자동으로 삭제합니다.

```
<#root>
```

```
firepower#
```

```
show log | include 230.11.11.11
```

```
May 17 2022 11:05:47: %FTD-7-609001:
```

```
Built local-host identity:230.11.11.11
```

```
<-- A new connection is created
```

```
May 17 2022 11:05:47: %FTD-6-302020: Built inbound ICMP connection for faddr 192.168.1.99/6 gaddr 230.11.11.11
```

```
May 17 2022 11:05:47: %FTD-6-302020: Built inbound ICMP connection for faddr 192.168.103.62/6 gaddr 230.11.11.11
```

```
May 17 2022 11:05:49: %FTD-6-302021: Teardown ICMP connection for faddr 192.168.1.99/6 gaddr 230.11.11.11
```

```
May 17 2022 11:05:49: %FTD-6-302021: Teardown ICMP connection for faddr 192.168.103.62/6 gaddr 230.11.11.11
```

```
May 17 2022 11:05:49: %FTD-7-609002:
```

```
Teardown local-host identity:230.11.11.11 duration 0:00:02
```

```
<-- The connection is closed
```

```
May 17 2022 11:05:51: %FTD-7-609001:
```

```
Built local-host identity:230.11.11.11
```

```
<
```

```
--
```

```
A new connection is created
```

```
May 17 2022 11:05:51: %FTD-6-302020: Built inbound ICMP connection for faddr 192.168.1.99/6 gaddr 230.11.11.11
```

```
May 17 2022 11:05:51: %FTD-6-302020: Built inbound ICMP connection for faddr 192.168.103.62/6 gaddr 230.11.11.11
```

```
May 17 2022 11:05:53: %FTD-6-302021: Teardown ICMP connection for faddr 192.168.1.99/6 gaddr 230.11.11.11
```

```
May 17 2022 11:05:53: %FTD-6-302021: Teardown ICMP connection for faddr 192.168.103.62/6 gaddr 230.11.11.11
```

```
May 17 2022 11:05:53: %FTD-7-609002:
```

```
Teardown local-host identity:230.11.11.11 duration 0:00:02
```

```
<-- The connection is closed
```



참고: LINA ASP 삭제 캡처에는 삭제된 패킷이 표시되지 않습니다

멀티캐스트 패킷 삭제의 주요 표시는 다음과 같습니다.

<#root>

firepower#

show mfib

Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
AR - Activity Required, K - Keepalive
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second

Other counts: Total/RPF failed/Other drops

Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
IC - Internal Copy, NP - Not platform switched
SP - Signal Present

Interface Counts: FS Pkt Count/PS Pkt Count

(* ,224.0.1.39) Flags: S K
Forwarding: 0/0/0/0, Other: 0/0/0

(* ,224.0.1.40) Flags: S K
Forwarding: 0/0/0/0, Other: 0/0/0

(192.168.103.62,230.11.11.11)

Flags: K <-- The multicast stream
Forwarding: 0/0/0/0,

Other: 27/27/0

<-- The packets are dropped

igmp 정적 그룹

FMC에서 고정 IGMP 그룹을 구성합니다.

The screenshot displays the Firewall Management Center (FMC) interface for device FTD4125-1. The 'Routing' tab is active, and the 'Static Group' sub-tab is selected. A modal dialog titled 'Add IGMP Static Group parameters' is open, showing the configuration for a static group. The 'Interface' dropdown is set to 'INSIDE', and the 'Multicast Group' dropdown is set to 'group_230.11.11.11'. The 'Enable Multicast Routing' checkbox is checked. The left sidebar shows the 'Manage Virtual Routers' menu with 'IGMP' selected under 'Multicast Routing'.

백그라운드에서 배포되는 항목은 다음과 같습니다.

```
<#root>
```

```
interface Port-channel1.205
vlan 205
nameif INSIDE
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.1.24 255.255.255.0

igmp static-group 230.11.11.11
```

```
<-- IGMP static group is enabled on the interface
```

ping이 실패하지만 이제 ICMP 멀티캐스트 트래픽이 방화벽을 통해 전달됩니다.

```
<#root>
```

```
L3-Switch#
```

```
ping 230.11.11.11 re 10000
```

```
Type escape sequence to abort.
```

```
Sending 10000, 100-byte ICMP Echos to 230.11.11.11, timeout is 2 seconds:
```

```
.....
```

```
<#root>
```

```
firepower#
```

```
show capture
```

```
capture CAPI type raw-data trace interface OUTSIDE
```

```
[Capturing - 650 bytes]
```

```
<-- ICMP packets are captured on ingress interface
```

```
match icmp host 192.168.103.62 any
```

```
capture CAPO type raw-data interface INSIDE
```

```
[Capturing - 670 bytes]
```

```
<-- ICMP packets are captured on egress interface
```

```
match icmp host 192.168.103.62 any
```

```
<#root>
```

```
firepower#
```

```
show capture CAPI
```


8 packets captured


```
1: 11:31:32.470541 192.168.103.62 > 230.11.11.11 icmp: echo request
2: 11:31:34.470358 192.168.103.62 > 230.11.11.11 icmp: echo request
3: 11:31:36.470831 192.168.103.62 > 230.11.11.11 icmp: echo request
4: 11:31:38.470785 192.168.103.62 > 230.11.11.11 icmp: echo request
...
```

firepower#

show capture CAPO

11 packets captured

```
1: 11:31:32.470587 802.1Q vlan#205 PO 192.168.103.62 > 230.11.11.11 icmp: echo request
2: 11:31:34.470404 802.1Q vlan#205 PO 192.168.103.62 > 230.11.11.11 icmp: echo request
3: 11:31:36.470861 802.1Q vlan#205 PO 192.168.103.62 > 230.11.11.11 icmp: echo request
4: 11:31:38.470816 802.1Q vlan#205 PO 192.168.103.62 > 230.11.11.11 icmp: echo request
```

 참고: 패킷 추적에 잘못된 출력이 표시됩니다(인그레스 인터페이스는 이그레스(egress)와 동일합니다. 자세한 내용은 Cisco 버그 ID CSCvm[89673](https://tools.cisco.com/bugcenter/bug/?bugID=CSCvm89673)을 확인하십시오.

<#root>

firepower#

show capture CAPI packet-number 1 trace

```
1: 11:39:33.553987 192.168.103.62 > 230.11.11.11 icmp: echo request
```

```
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 3172 ns
Config:
Additional Information:
MAC Access list
```

```
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 3172 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 192.168.103.62 using egress ifc OUTSIDE(vrfid:0)

Phase: 4
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 5368 ns
Config:
Implicit Rule
Additional Information:

Phase: 5
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Elapsed time: 5368 ns
Config:
class-map class-default
match any
policy-map global_policy
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
service-policy global_policy global
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Elapsed time: 5368 ns
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Elapsed time: 5368 ns
Config:
Additional Information:

Phase: 8
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Elapsed time: 31720 ns
Config:
Additional Information:

Phase: 9
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Elapsed time: 488 ns
Config:
class-map inspection_default
match default-inspection-traffic
policy-map global_policy
class inspection_default
inspect icmp

service-policy global_policy global

Additional Information:

Phase: 10

Type: INSPECT

Subtype: np-inspect

Result: ALLOW

Elapsed time: 2440 ns

Config:

Additional Information:

Phase: 11

Type: MULTICAST

<-- The packet is multicast

Subtype:

Result: ALLOW

Elapsed time: 976 ns

Config:

Additional Information:

Phase: 12

Type: FLOW-CREATION

<-- A new flow is created

Subtype:

Result: ALLOW

Elapsed time: 56120 ns

Config:

Additional Information:

New flow created with id 5690, packet dispatched to next module

Phase: 13

Type: CAPTURE

Subtype:

Result: ALLOW

Elapsed time: 10248 ns

Config:

Additional Information:

MAC Access list

Result:

input-interface: OUTSIDE(vrfid:0)


input-status: up

```
input-line-status: up
output-interface: OUTSIDE(vrfid:0)

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

Action: allow

<-- The packet is allowed
Time Taken: 139568 ns
```

 **팁:** 소스 호스트에서 시간 제한 0으로 ping하고 방화벽 mfib 카운터를 확인할 수 있습니다.

```
<#root>
```

```
L3-Switch#
```

```
ping 230.11.11.11 re 500 timeout 0
```

```
Type escape sequence to abort.
```

```
Sending 1000, 100-byte ICMP Echos to 230.11.11.11, timeout is 0 seconds:
```

```
.....
.....
.....
.....
```

```
<#root>
```

```
firepower# clear mfib counters
```

```
firepower# !ping from the source host.
```

```
firepower#
```

```
show mfib 230.11.11.11
```

```
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
AR - Activity Required, K - Keepalive
```

```
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
```

```
Other counts: Total/RPF failed/Other drops
```

```
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
```

```
IC - Internal Copy, NP - Not platform switched
```

```
SP - Signal Present
```

```
Interface Counts: FS Pkt Count/PS Pkt Count
```

```
(* ,230.11.11.11) Flags: C K
```

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

```
INSIDE Flags: F NS
```

```
Pkts: 0/0
```

```
(192.168.103.62,230.11.11.11) Flags: K
```

Forwarding: 500/0/100/0, Other: 0/0/0

<-- 500 multicast packets forwarded. The average size of each packet is 100 Bytes

OUTSIDE Flags: A
INSIDE Flags: F NS
Pkts: 500/0

igmp 조인 그룹

FMC 원격 사이트에서 이전에 구성한 고정 그룹 컨피그레이션을 선택하고 IGMP 조인 그룹을 구성합니다.

Firewall Management Center
Devices / NGFW Routing

Overview Analysis Policies Devices Objects Integration

FTD4125-1
Cisco Firepower 4125 Threat Defense

Device Routing Interfaces Inline Sets DHCP

Manage Virtual Routers

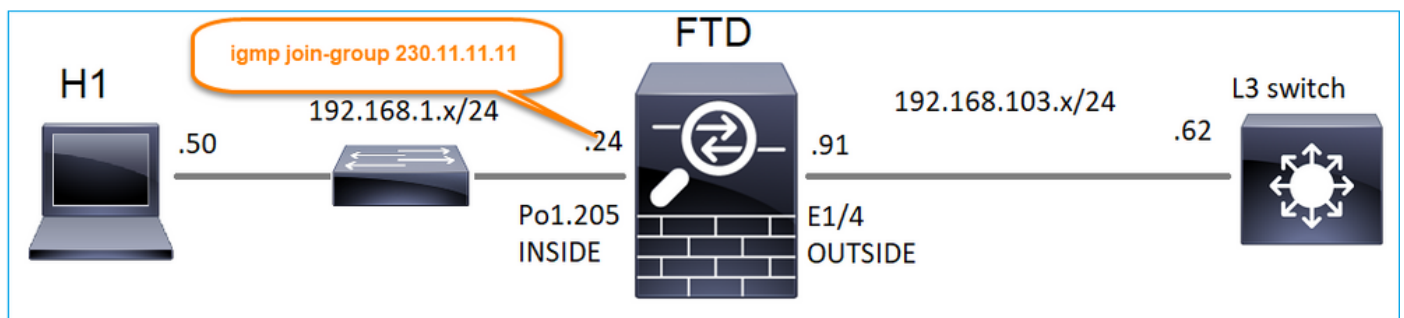
Global

Virtual Router Properties
ECMP
OSPF
OSPFv3
EIGRP
RIP
Policy Based Routing
BGP
IPv4
IPv6
Static Route
Multicast Routing
IGMP

Enable Multicast Routing (Enabling Multicast Routing checkbox will enable both IGMP and PIM on all Interfaces.)

Protocol	Access Group	Static Group	Join Group

Interface	Multicast Group Address
INSIDE	group_230.11.11.11



구축된 컨피그레이션:

<#root>

firepower#

show run interface Port-channel1.205

```
!  
interface Port-channel1.205  
vlan 205  
nameif INSIDE  
cts manual  
propagate sgt preserve-untag  
policy static sgt disabled trusted  
security-level 0  
ip address 192.168.1.24 255.255.255.0  
  
igmp join-group 230.11.11.11  
  
<-- The interface joined the multicast group
```

IGMP 그룹:

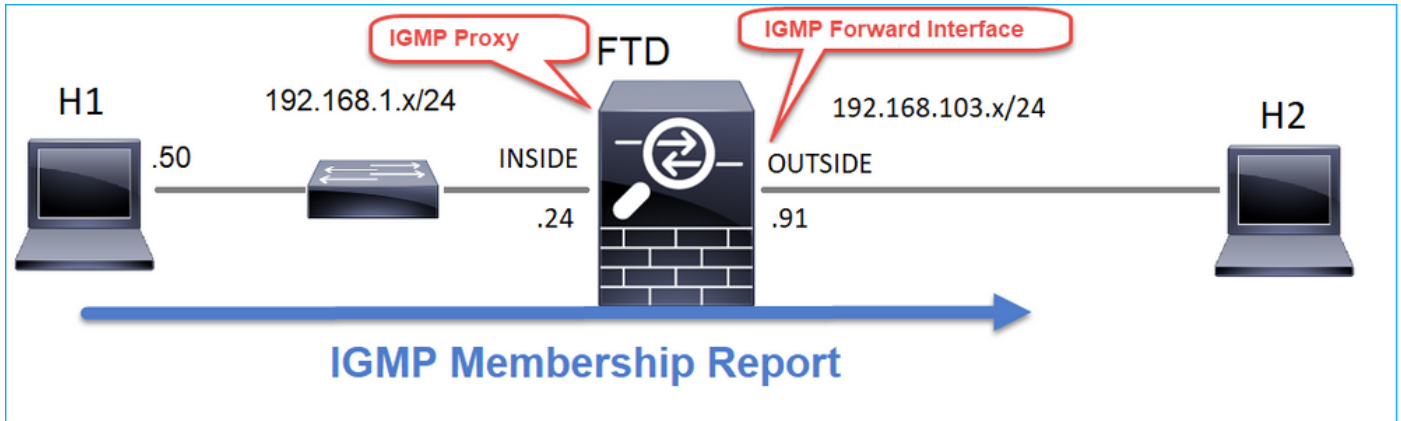
```
<#root>  
  
firepower#  
  
show igmp group  
  
IGMP Connected Group Membership  
Group Address Interface Uptime Expires Last Reporter  
230.11.11.11 INSIDE 00:30:43 never 192.168.1.24  
  
<-- The group is enabled on the interface
```

소스 호스트에서 230.11.11.11 IP에 대한 첫 번째 ICMP 멀티캐스트 테스트를 시도합니다.

```
<#root>  
  
L3-Switch#  
  
ping 230.11.11.11 repeat 10  
  
Type escape sequence to abort.  
Sending 10, 100-byte ICMP Echos to 230.11.11.11, timeout is 2 seconds:  
  
Reply to request 0 from 192.168.1.24, 12 ms  
Reply to request 1 from 192.168.1.24, 8 ms  
Reply to request 2 from 192.168.1.24, 8 ms  
Reply to request 3 from 192.168.1.24, 8 ms  
Reply to request 4 from 192.168.1.24, 8 ms  
Reply to request 5 from 192.168.1.24, 12 ms  
Reply to request 6 from 192.168.1.24, 8 ms  
Reply to request 7 from 192.168.1.24, 8 ms  
Reply to request 8 from 192.168.1.24, 8 ms  
Reply to request 9 from 192.168.1.24, 8 ms
```

참고: 회신이 모두 표시되지 않으면 Cisco 버그 ID CSCvm90069을 [확인하십시오](#).

작업 4 - IGMP Stub 멀티캐스트 라우팅 구성



INSIDE 인터페이스에서 수신한 IGMP Membership Report 메시지가 OUTSIDE 인터페이스로 전달 되도록 FTD에서 stub 멀티캐스트 라우팅을 구성합니다.

솔루션

Firewall Management Center
Devices / NGFW Routing

FTD4125-1
Cisco Firepower 4125 Threat Defense

Device Routing Interfaces Inline Sets DHCP

Manage Virtual Routers
Global

Virtual Router Properties
ECMP
OSPF
OSPFv3
EIGRP
RIP
Policy Based Routing
BGP
IPv4
IPv6
Static Route
Multicast Routing
IGMP

Enable Multicast Routing (Enabling Multicast Routing checkbox will enable both IGMP and PIM on all Interfaces.)

Protocol Access Group Static Group Join Group

Interface	Enabled	Forward Interface	Version	Query Interval	Response Time
INSIDE	true	OUTSIDE	2		

구축된 컨피그레이션:

<#root>

```
firepower#
show run multicast-routing

multicast-routing
<-- Multicast routing is enabled
firepower#

show run interface Port-channel1.205

!
interface Port-channel1.205
vlan 205
nameif INSIDE
cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
security-level 0
ip address 192.168.1.24 255.255.255.0

igmp forward interface OUTSIDE
<-- The interface does stub multicast routing
```

확인

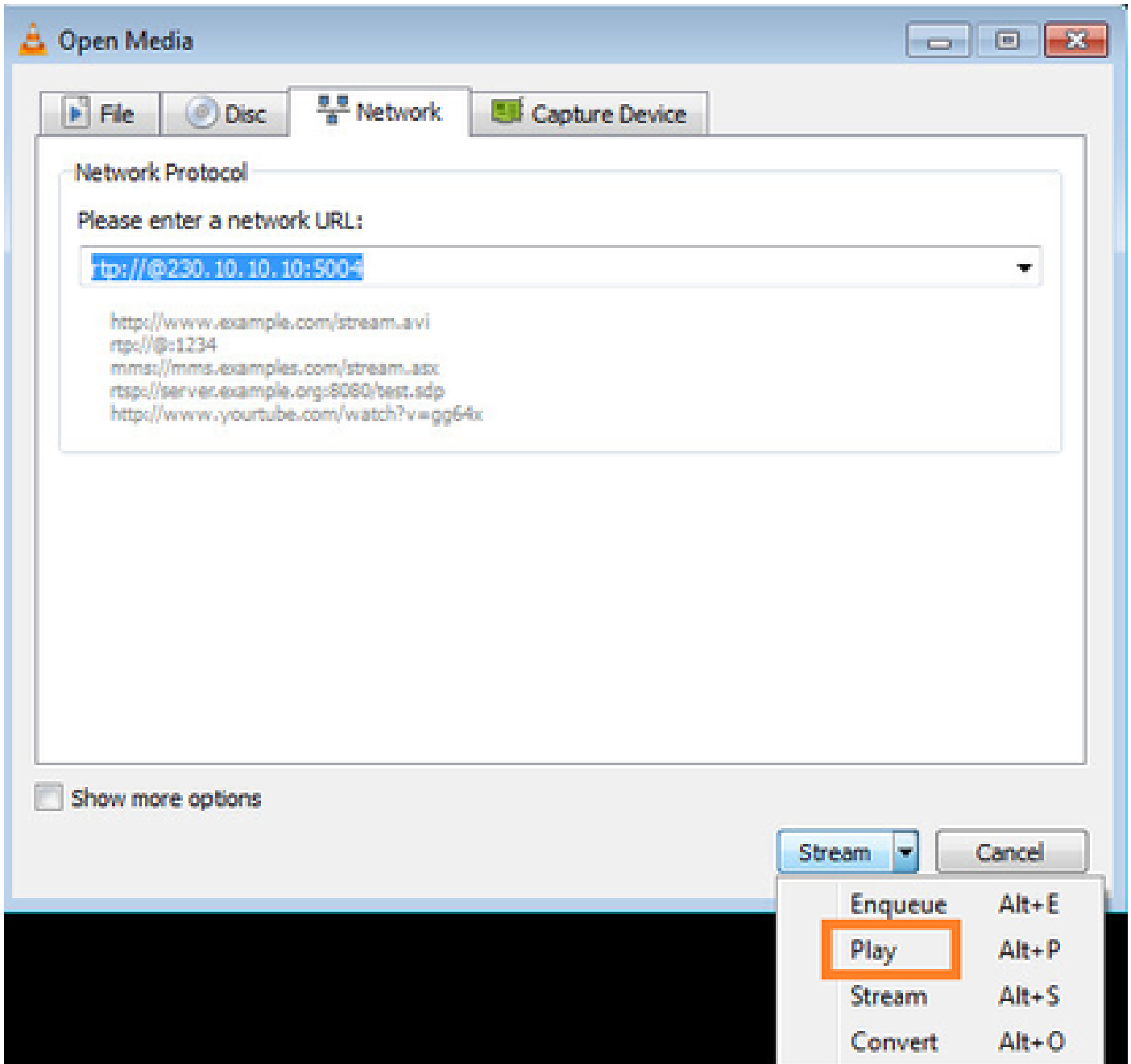
FTD에서 캡처 사용:

```
<#root>
firepower#
capture CAPI interface INSIDE trace match igmp any host 230.10.10.10

firepower#
capture CAPO interface OUTSIDE match igmp any host 230.10.10.10
```

확인

IGMP 멤버십 보고서를 강제로 실행하려면 VLC와 같은 애플리케이션을 사용할 수 있습니다.



FTD는 IGMP 패킷을 프록시합니다.

```
<#root>
```

```
firepower#
```

```
show capture
```

```
capture CAPI type raw-data trace interface INSIDE
```

```
[Capturing - 66 bytes]
```

```
<-- IGMP packets captured on ingress
```

```
match igmp any host 230.10.10.10
```

```
capture CAPO type raw-data interface OUTSIDE
```

```
[Capturing - 62 bytes]
```

```
<-- IGMP packets captured on egress
match igmp any host 230.10.10.10
```

FTD는 소스 IP를 변경합니다.

```
<#root>
```

```
firepower#
```

```
show capture CAPI
```

```
1 packet captured
```

```
1: 12:21:12.820483 802.1Q v1an#205 P6
```

```
192.168.1.50
```

```
> 230.10.10.10 ip-proto-2, length 8 <-- The source IP of the packet on ingress interface
1 packet shown
```

```
firepower#
```

```
show capture CAPO
```

```
1 packet captured
```

```
1: 12:21:12.820743
```

```
192.168.103.91
```

```
> 230.10.10.10 ip-proto-2, length 8 <-- The source IP of the packet on egress interface
1 packet shown
```

Wireshark에서 pcap를 확인하면 패킷이 방화벽에 의해 완전히 재생성되는 것을 확인할 수 있습니다(IP ID 변경).

FTD에 그룹 항목이 생성됩니다.

```
<#root>
```

```
firepower#
```

```
show igmp group
```

```
IGMP Connected Group Membership
Group Address    Interface          Uptime    Expires    Last Reporter
230.10.10.10     INSIDE             00:15:22  00:03:28  192.168.1.50
```

```
<-- IGMP group is enabled on the ingress interface
```

```
239.255.255.250 INSIDE             00:15:27  00:03:29  192.168.1.50
```

FTD 방화벽은 2개의 컨트롤 플레인 연결을 생성합니다.

```
<#root>
```

```
firepower#
```

```
show conn all address 230.10.10.10
```

```
9 in use, 28 most used
```

```
Inspect Snort:
```

```
preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect
```

```
IGMP INSIDE 192.168.1.50 NP Identity Ifc 230.10.10.10, idle 0:00:09, bytes 8, flags
```

```
<-- Connection terminated on the ingress interface
```

```
IGMP OUTSIDE 230.10.10.10 NP Identity Ifc 192.168.103.91, idle 0:00:09, bytes 8, flags
```

```
<-- Connection terminated on the egress interface
```

첫 번째 패킷의 추적:

```
<#root>
```

```
firepower#
```

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

```
6 packets captured
```

```
1: 12:21:12.820483 802.1Q vlan#205 P6 192.168.1.50 > 230.10.10.10 ip-proto-2, length 8
```

```
<-- The first packet of the flow
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Elapsed time: 5124 ns
```

```
Config:
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Elapsed time: 5124 ns
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 3
```

```
Type: ROUTE-LOOKUP
```

```
Subtype: No ECMP load balancing
```

Result: ALLOW
Elapsed time: 7808 ns
Config:
Additional Information:
Destination is locally connected. No ECMP load balancing.
Found next-hop 192.168.1.50 using egress ifc INSIDE(vrfid:0)

Phase: 4
Type: CLUSTER-DROP-ON-SLAVE
Subtype: cluster-drop-on-slave
Result: ALLOW
Elapsed time: 5368 ns
Config:
Additional Information:

Phase: 5
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 5368 ns
Config:
Implicit Rule
Additional Information:

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Elapsed time: 5368 ns
Config:
Additional Information:

Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Elapsed time: 5368 ns
Config:
Additional Information:

Phase: 8
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Elapsed time: 40504 ns
Config:
Additional Information:

Phase: 9

Type: MULTICAST

<-- The packet is multicast

Subtype:

Result: ALLOW

Elapsed time: 976 ns

Config:

Additional Information:

Phase: 10

Type: FLOW-CREATION

<-- A new flow is created

Subtype:

Result: ALLOW

Elapsed time: 17568 ns

Config:

Additional Information:

New flow created with id 5945, packet dispatched to next module

Phase: 11

Type: FLOW-CREATION

<-- A second flow is created

Subtype:

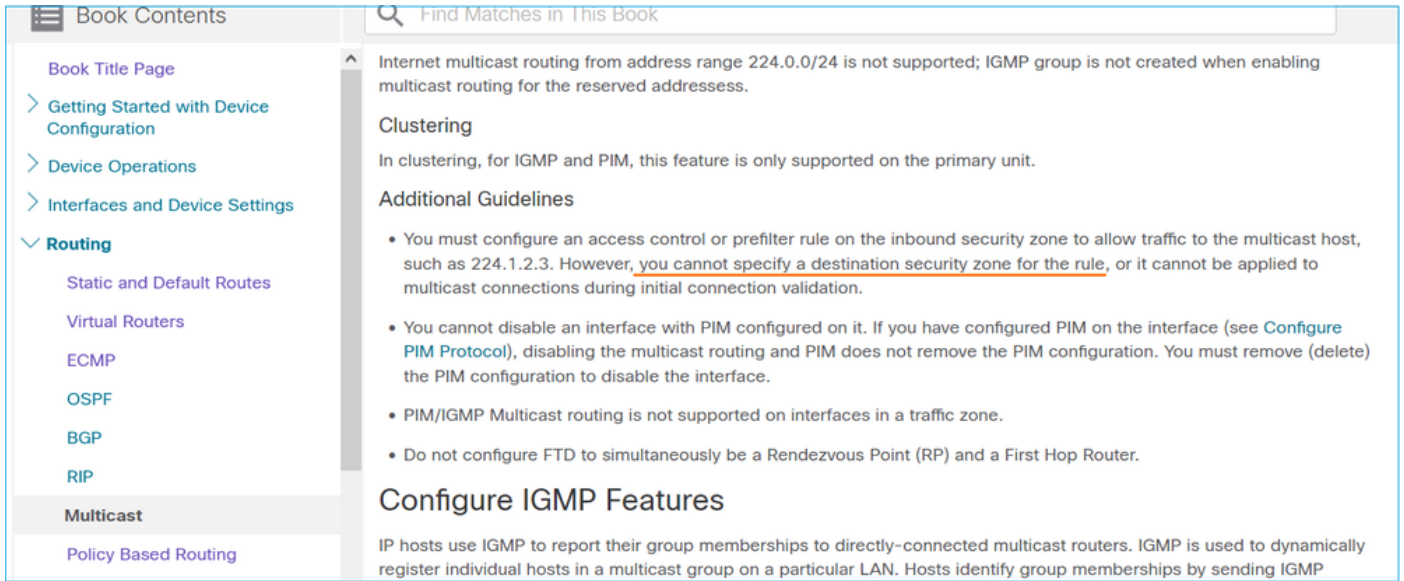
Result: ALLOW

Elapsed time: 39528 ns

Config:

Additional Information:

이 내용은 FMC 사용 설명서에도 설명되어 있습니다.



IGMP 인터페이스 제한이 초과되면 방화벽에 의해 IGMP 보고서가 거부됨

기본적으로 방화벽은 인터페이스에서 최대 500개의 현재 활성 조인(보고서)을 허용합니다. 이 임계 값을 초과하면 방화벽은 멀티캐스트 수신기에서 추가로 들어오는 IGMP 보고서를 무시합니다.

IGMP 제한과 활성 조인을 확인하려면 `show igmp interface nameif` 명령을 실행합니다.

```
<#root>
```

```
asa#
```

```
show igmp interface inside
```

```
inside is up, line protocol is up
Internet address is 10.10.10.1/24
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: 500

Cumulative IGMP activity: 0 joins, 0 leaves
IGMP querying router is 10.10.10.1 (this system)
```

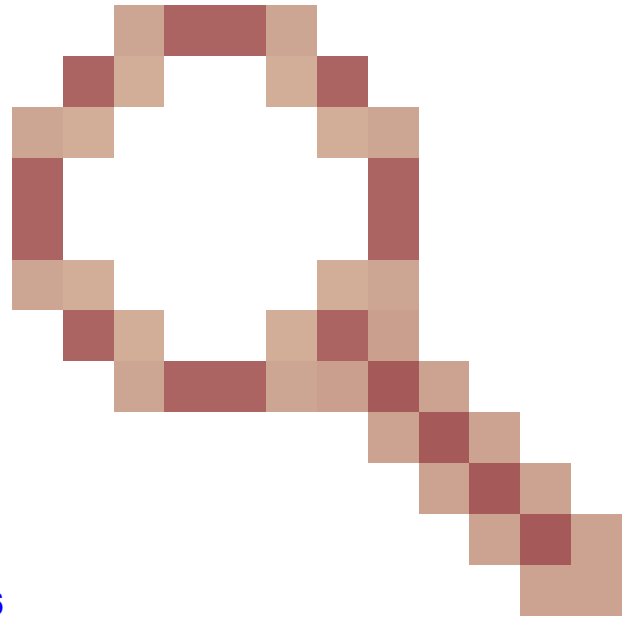
IGMP debug 명령 `debug igmp`는 다음 출력을 표시합니다.

```
<#root>
```

```
asa#
```

```
debug igmp
```

Apr 20 2023 09:37:10: %ASA-7-711001: IGMP: Group 230.1.2.3 limit denied on inside



Cisco 버그 ID CSCvw가 수정된 소프트웨어 [버전60976](#)
사용자가 인터페이스별로 최대 5000개의 그룹을 구성할 수 있습니다.

방화벽이 232.x.x.x/8 주소 범위에 대한 IGMP 보고서를 무시함

232.x.x.x/8 주소 범위는 SSM(Source Specific Multicast)에 사용됩니다. 방화벽은 PIM SSM(Source Specific Multicast) 기능 및 관련 컨피그레이션을 지원하지 않습니다.

IGMP debug 명령 debug igmp는 다음 출력을 표시합니다.

```
<#root>
```

```
asa#
```

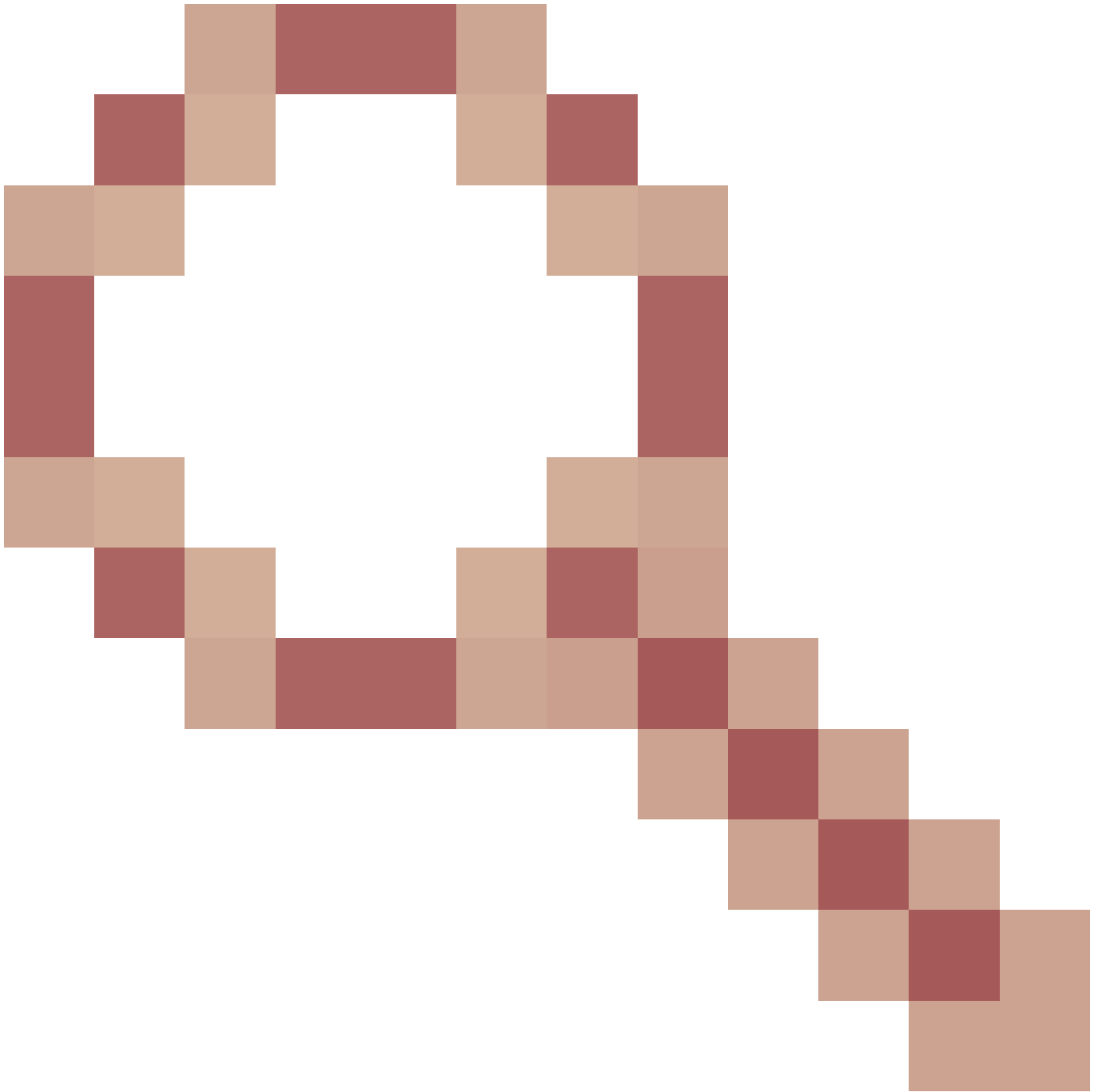
```
debug igmp
```

```
Apr 20 2023 09:37:10: %ASA-7-711001: IGMP: Received v2 Report on inside from 10.10.10.11 for 232.179.89.
```

```
Apr 20 2023 09:37:10: %ASA-7-711001: IGMP: group_db: add new group 232.179.89.253 on inside
```

```
Apr 20 2023 09:37:10: %ASA-7-711001: IGMP: Exclude report on inside ignored for SSM group 232.179.89.253
```

Cisco 버그 ID [CSCsr53916](#)



ssm 범위를 지원하기 위한 개선 사항을 추적합니다.

관련 정보

- [firepower 위협 방어를 위한 멀티캐스트 라우팅](#)
- [firepower 위협 방어 및 ASA Multicast PIM 문제 해결](#)

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.