

# firepower脅威対策IGMPおよびマルチキャストの 基本のトラブルシューティング

## 内容

---

### [概要](#)

### [前提条件](#)

#### [要件](#)

#### [使用するコンポーネント](#)

### [背景説明](#)

### [設定](#)

#### [IGMPの基本](#)

#### [作業1: コントロールプレーンのマルチキャストトラフィック](#)

#### [作業2: 基本的なマルチキャストの設定](#)

#### [IGMP スヌーピング](#)

#### [作業3:IGMPスタティックグループとIGMP参加グループの比較](#)

#### [IGMPスタティックグループ](#)

#### [IGMP参加グループ](#)

#### [作業4:IGMPスタブマルチキャストルーティングの設定](#)

### [既知の問題](#)

#### [宛先ゾーンでのマルチキャストトラフィックのフィルタリング](#)

#### [IGMPインターフェイスの制限を超えると、ファイアウォールによってIGMPレポートが拒否される](#)

#### [ファイアウォールが232.x.x.x/8アドレス範囲のIGMPレポートを無視する](#)

### [関連情報](#)

---

## 概要

このドキュメントでは、マルチキャストの基本と、Firepower Threat Defense(FTD)がInternet Group Management Protocol(IGMP)を実装する方法について説明します。

## 前提条件

### 要件

IPルーティングに関する基礎知識

### 使用するコンポーネント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま

す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

この記事の内容は、適応型セキュリティアプライアンス(ASA)ソフトウェアにも適用されます。

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CiscoFirepower4125 Threat Defenseバージョン7.1.0
- Firepower Management Center ( FMC ) バージョン 7.1.0.
- ASA バージョン 9.19.1.

## 背景説明

### 定義

- ユニキャスト= 1つのホストから別のホストへ ( 1対1 )。
- ブロードキャスト= 1台のホストからすべての可能なホストへ ( 1対全 )。
- マルチキャスト=ホストのグループのホストからホストのグループ ( 1対多または多対多 )
- エニーキャスト=ホストからグループの最も近いホスト ( 1対多 )。

### 基本

- マルチキャストRFC 988は、Steve Deeringによって1986年に作成されました。
- IPv4マルチキャストは、224.0.0.0/4 ( 最初の4ビットが1110 ) ~ 224.0.0.0 ~ 239.255.255.255の範囲を使用します。
- IPv4の場合、L2 MACアドレスはL3マルチキャストIPから派生します。01005e ( 24ビット ) + 25番目のビットは常に0 +マルチキャストIPv4アドレスの下位23ビットです。
- IPv6マルチキャストは範囲FF00::/8を使用し、ランデブーポイント(RP)IPを埋め込むことができるため、IPv4マルチキャストよりも柔軟性があります。
- IPv6では、L2 MACアドレスはL3マルチキャストから派生します。マルチキャストIPv6アドレスの3333 +下位32ビット。
- マルチキャストの利点：送信元の負荷が軽減されるため、効率が向上します。パフォーマンス。トラフィックの重複やフラグディングを回避します。
- マルチキャストの欠点：信頼性の低い転送 ( UDPベース )、輻輳回避なし、順不同の配信。
- パブリックインターネットでは、パス内のすべてのデバイスでマルチキャストを有効にする必要があるため、マルチキャストはサポートされていません。通常、すべてのデバイスが共通の管理権限の下にある場合に使用されます。
- 一般的なマルチキャストアプリケーション：内部ビデオストリーム、ビデオ会議

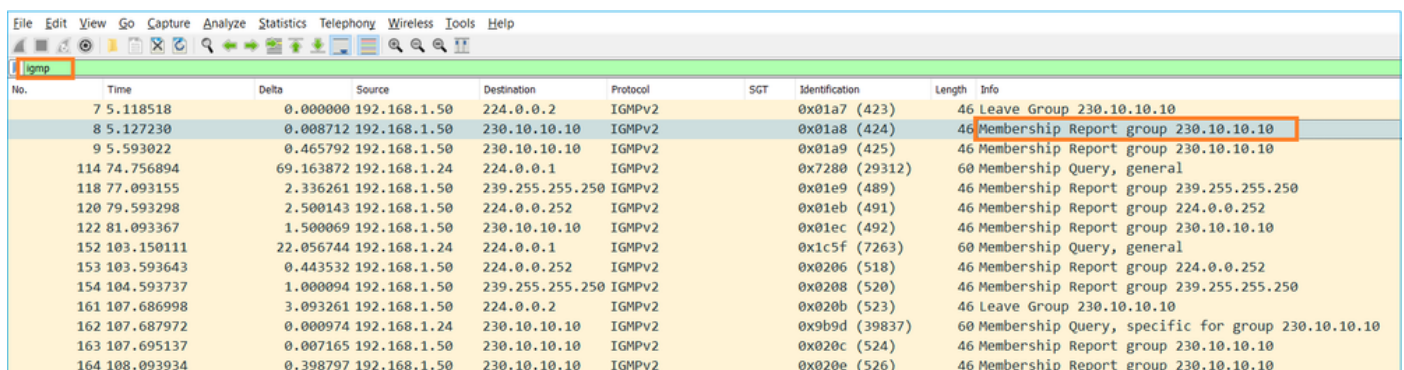
### マルチキャストと複製されたユニキャスト

複製されたユニキャストでは、送信元は同じユニキャストパケット ( レプリカ ) の複数のコピーを作成し、それらを複数の宛先ホストに送信します。マルチキャストは送信元ホストからネットワークに負荷を移動し、複製されたユニキャストではすべての作業が送信元ホストで行われます。

# 設定

## IGMPの基本

- IGMPは、マルチキャスト受信側（通常はルータ）とローカルL3デバイス（通常はルータ）の間で話される「言語」です。
- IGMPは（ICMPと同様に）レイヤ3プロトコルであり、IPプロトコル番号2を使用します。
- 現在、3つのIGMPバージョンがあります。ファイアウォールのデフォルトIGMPバージョンはバージョン2です。現在サポートされているのはバージョン1と2だけです。
- IGMPv1とIGMPv2の主な違いは次のとおりです。
  - IGMPv1にはLeave Groupメッセージがありません。
  - IGMPv1にはGroup-Specific Query（GQUERY；グループ固有クエリ）がありません（ホストがマルチキャストグループから脱退するときにファイアウォールによって使用されます）。
  - IGMPv1にはクエリア選択プロセスがありません。
- IGMPv3は現在ASA/FTDではサポートされていませんが、IGMPv2とIGMPv3の重要な違いは、Source-Specific Multicast(SSM)で使用されるIGMPv3にGroup-and-Source-Specific Query(GSSM)が含まれていることです。
- IGMPv1/IGMPv2/IGMPv3クエリ= 224.0.0.1  
IGMPv2脱退= 224.0.0.2  
IGMPv3メンバーシップレポート= 224.0.0.22
- ホストが参加を希望する場合、非要請IGMPメンバーシップレポートメッセージを送信できません。



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		0x9b0d (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

- ファイアウォールの観点からは、IGMPクエリには一般クエリとグループ固有クエリの2種類があります
- ファイアウォールがIGMP Leave Groupメッセージを受信すると、サブネット上にそのグループの他のメンバーが存在するかどうかを確認する必要があります。そのため、ファイアウォールはGroup-Specific Query:

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

- 複数のルータ/ファイアウォールがあるサブネットでは、クエリア (すべてのIGMPクエリを送信するデバイス) が選択されます。

```
<#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
```

- FTDでは、従来のASAと同様に、debug igmpを有効にしてIGMP関連のメッセージを表示できます。

```
<#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

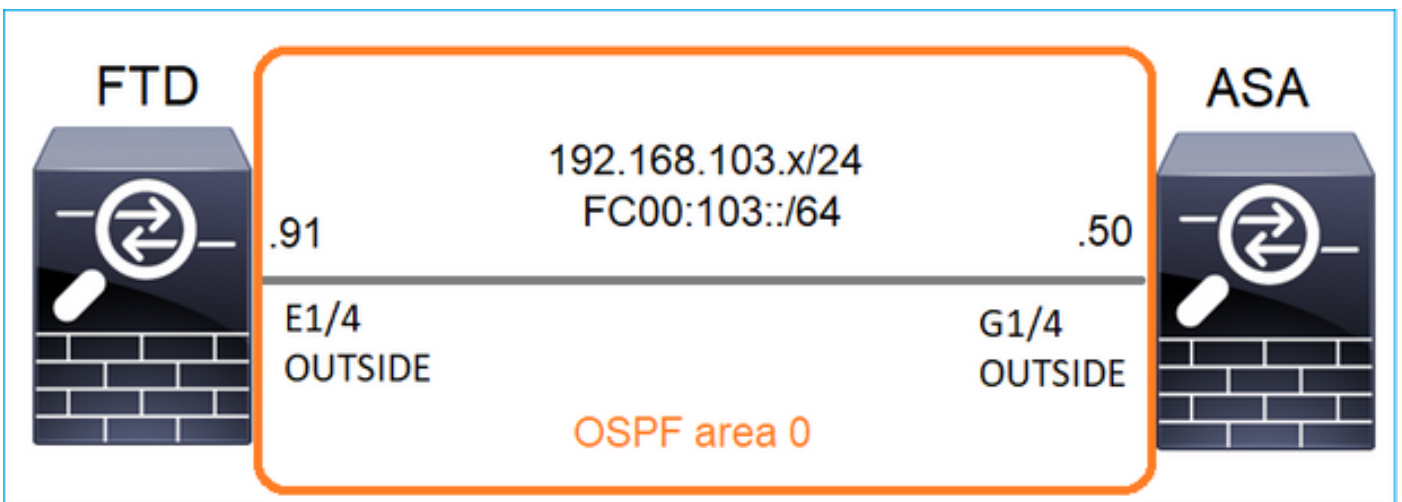
```

- ホストは通常、Leave Groupメッセージ(IGMPv2)を使用してマルチキャストグループから脱退します。

The image shows a Wireshark packet capture window with the filter 'igmp.type == 0x17'. Two packets are visible, both of type IGMPv2 Leave Group. The first packet (No. 7) has a source of 192.168.1.50 and a destination of 224.0.0.2. The second packet (No. 161) also has a source of 192.168.1.50 and a destination of 224.0.0.2. The 'Info' column for both packets shows 'Leave Group 230.10.10.10'.

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

## 作業1：コントロールプレーンのマルチキャストトラフィック



FTDとASAの間にOSPFv2とOSPFv3を設定します。2台のデバイスがOSPFによって生成されたL2およびL3マルチキャストトラフィックをどのように処理するかを確認します。

### 解決方法

#### OSPFv2の設定

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

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			

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**

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

同様に、OSPFv3の場合

FTD CLIの設定 :

<#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

この設定では、入カマルチキャストトラフィックがブロックされないように、FTD Accelerated

Security Path(ASP)許可テーブルに次のエントリが作成されます。

```
<#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
```

IPv6の場合

```
<#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とOSPFv3のアジャセンシー関係はアップしています。

```

<#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

```

これらは、ボックスに対して終了するマルチキャストOSPFセッションです。

```

<#root>

firepower#

show conn all | include OSPF

```



```
OSPF OUTSIDE fe80::2be:75ff:fe6:1d8e 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
```

テストとして、IPv4のキャプチャを有効にし、デバイスへの接続をクリアします。

```
<#root>
firepower#
capture CAP interface OUTSIDE trace
firepower#
clear conn all
12 connection(s) deleted.
firepower#
clear capture CAP
firepower# !
```

---

 警告：停止が発生しました。この例はデモ目的でのみ使用されています。

---

キャプチャされたOSPFパケット：

```
<#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:fe6:1d8e > 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]
```

OSPFv2マルチキャストパケットがファイアウォールでどのように処理されるかを次に示します。

```
<#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

OSPFv3マルチキャストパケットは、次のようにファイアウォールによって処理されます。

<#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

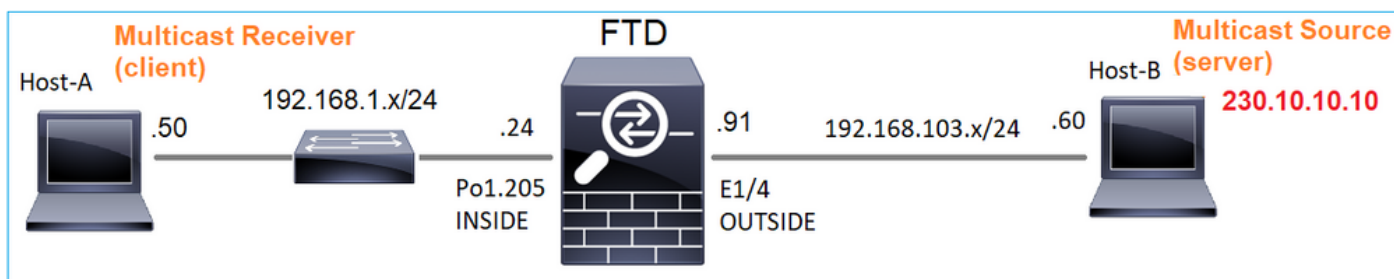
output-interface: NP Identity Ifc

Action: allow

Time Taken: 83448 ns

## 作業2：基本的なマルチキャストの設定

トポロジ



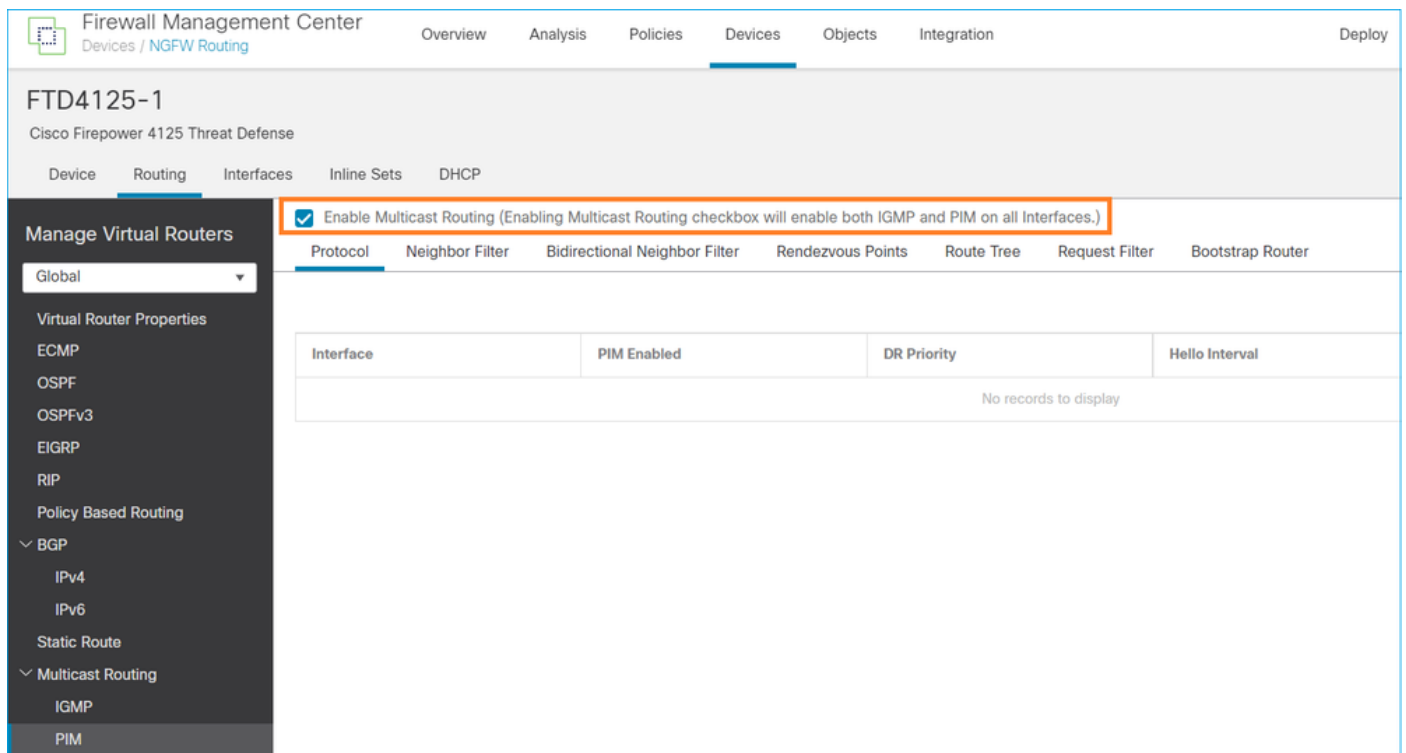
## Requirement

サーバからのマルチキャストトラフィックがIP 230.10.10.10のマルチキャストクライアントにストリーミングされるようにファイアウォールを設定します

## 解決方法

ファイアウォールの観点からは、マルチキャストルーティングをグローバルに有効にすることが最小限の設定です。これにより、バックグラウンドですべてのファイアウォールインターフェイスでIGMPとPIMが有効になります。

FMC UIで次の操作を行います。



The screenshot shows the FMC UI for device FTD4125-1. The 'Routing' tab is selected, and the 'Multicast Routing' section is expanded. The 'Enable Multicast Routing' checkbox is checked, with a red box highlighting it and the text: "Enable Multicast Routing (Enabling Multicast Routing checkbox will enable both IGMP and PIM on all interfaces.)". Below this, a table with columns 'Interface', 'PIM Enabled', 'DR Priority', and 'Hello Interval' is shown, with the message "No records to display" in the center.

ファイアウォールCLIでは、プッシュされた設定は次のとおりです。

```
<#root>
```

```
firepower#
```

```
show run multicast-routing
```

```
multicast-routing
```

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

## IGMPの検証

```
<#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の検証

<#root>

firepower#

show pim interface

Address	Interface	PIM	Nbr	Hello	DR	DR
			Count	Intvl	Prior	
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の検証

<#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

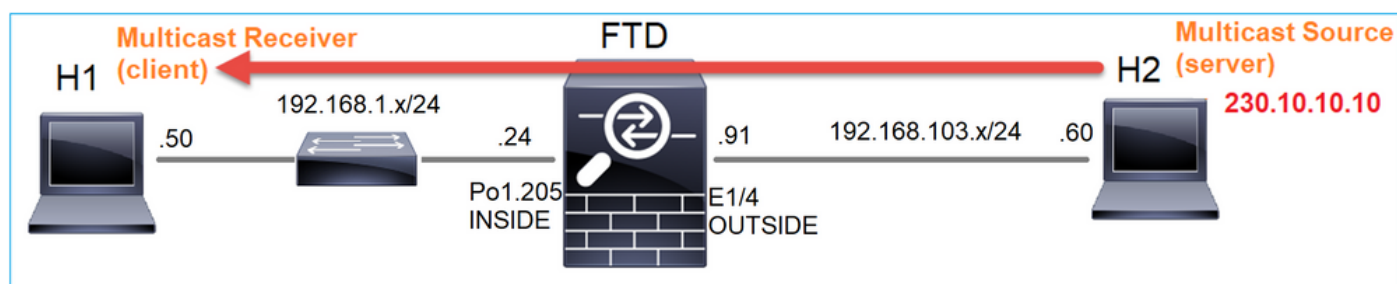
<-- The Other counters are: Total/RPF failed/Other drops

(\* ,232.0.0.0/8) Flags: K

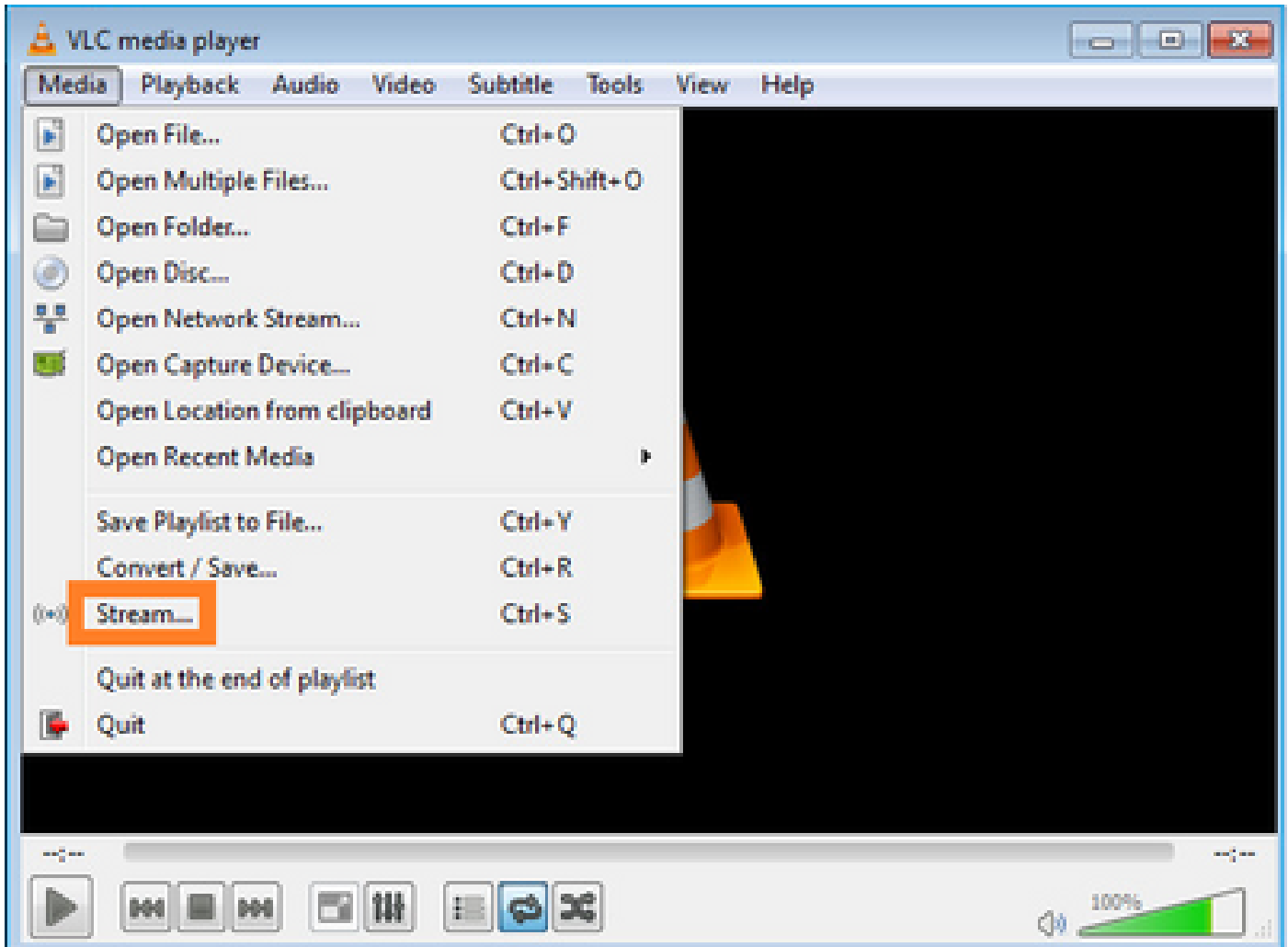
Forwarding: 0/0/0/0, Other: 0/0/0

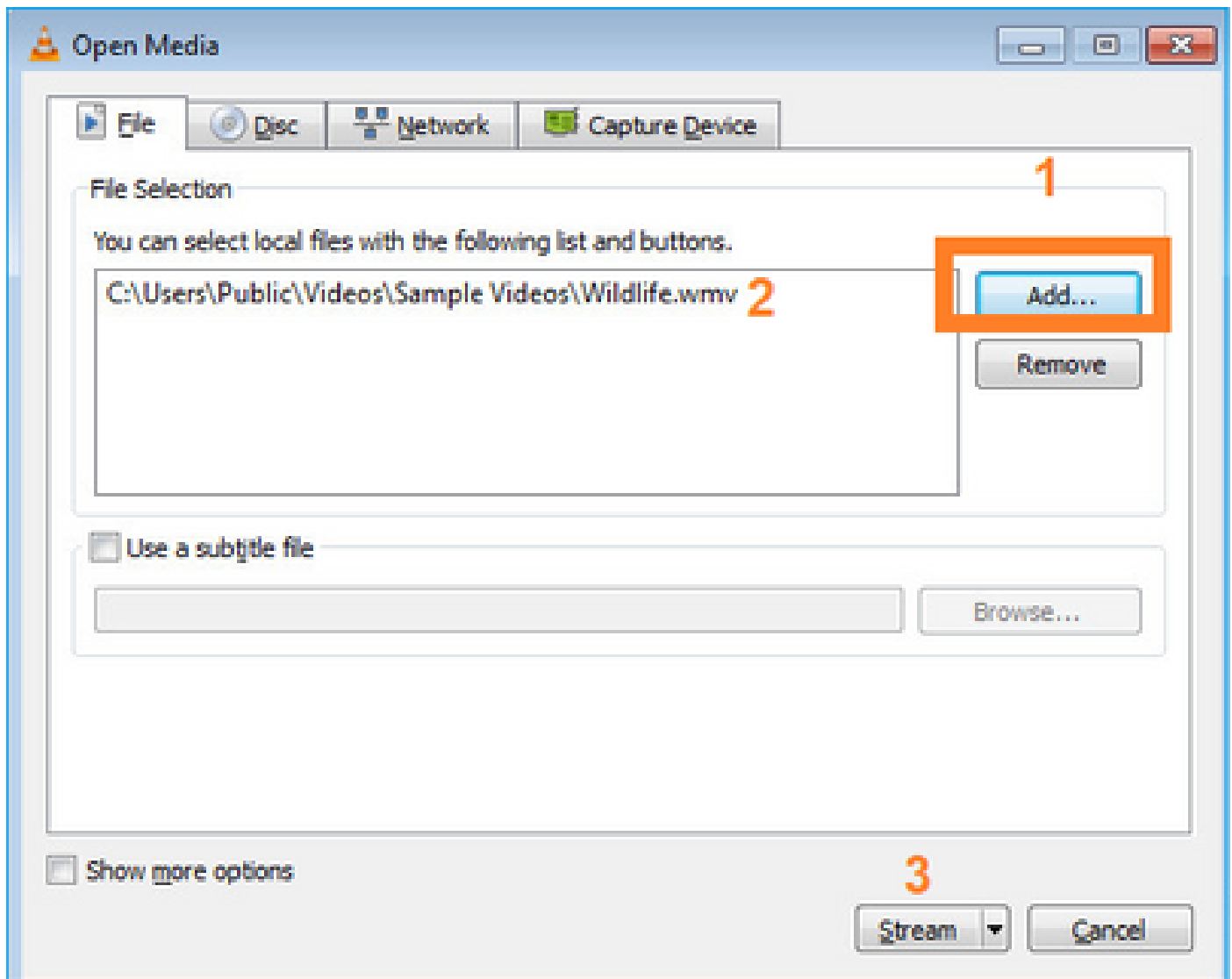
## ファイアウォールを通過するマルチキャストトラフィック

この場合、VLCメディアプレーヤーアプリケーションは、マルチキャストサーバおよびマルチキャストトラフィックをテストするクライアントとして使用されます。



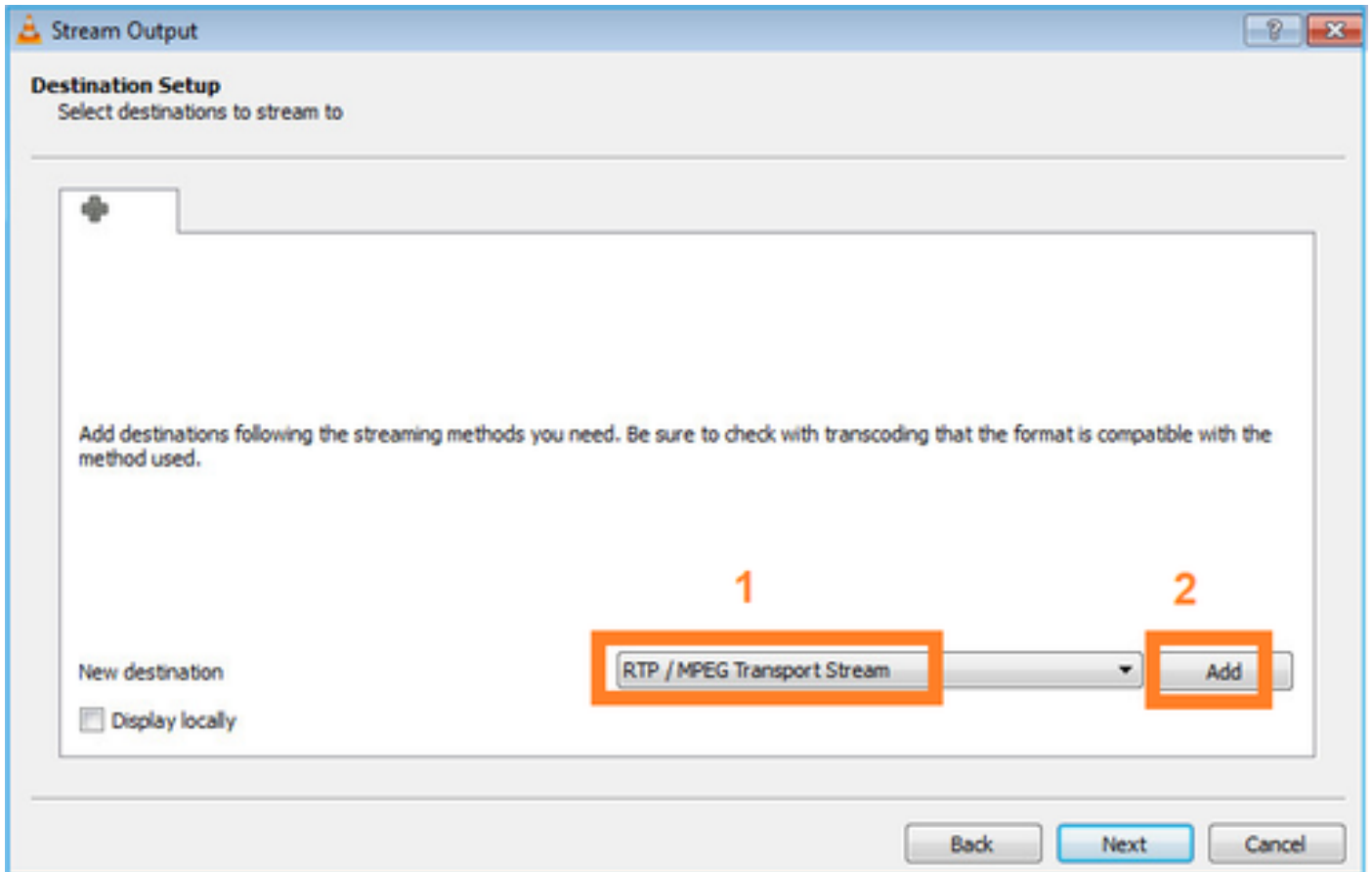
VLCマルチキャストサーバ設定 :



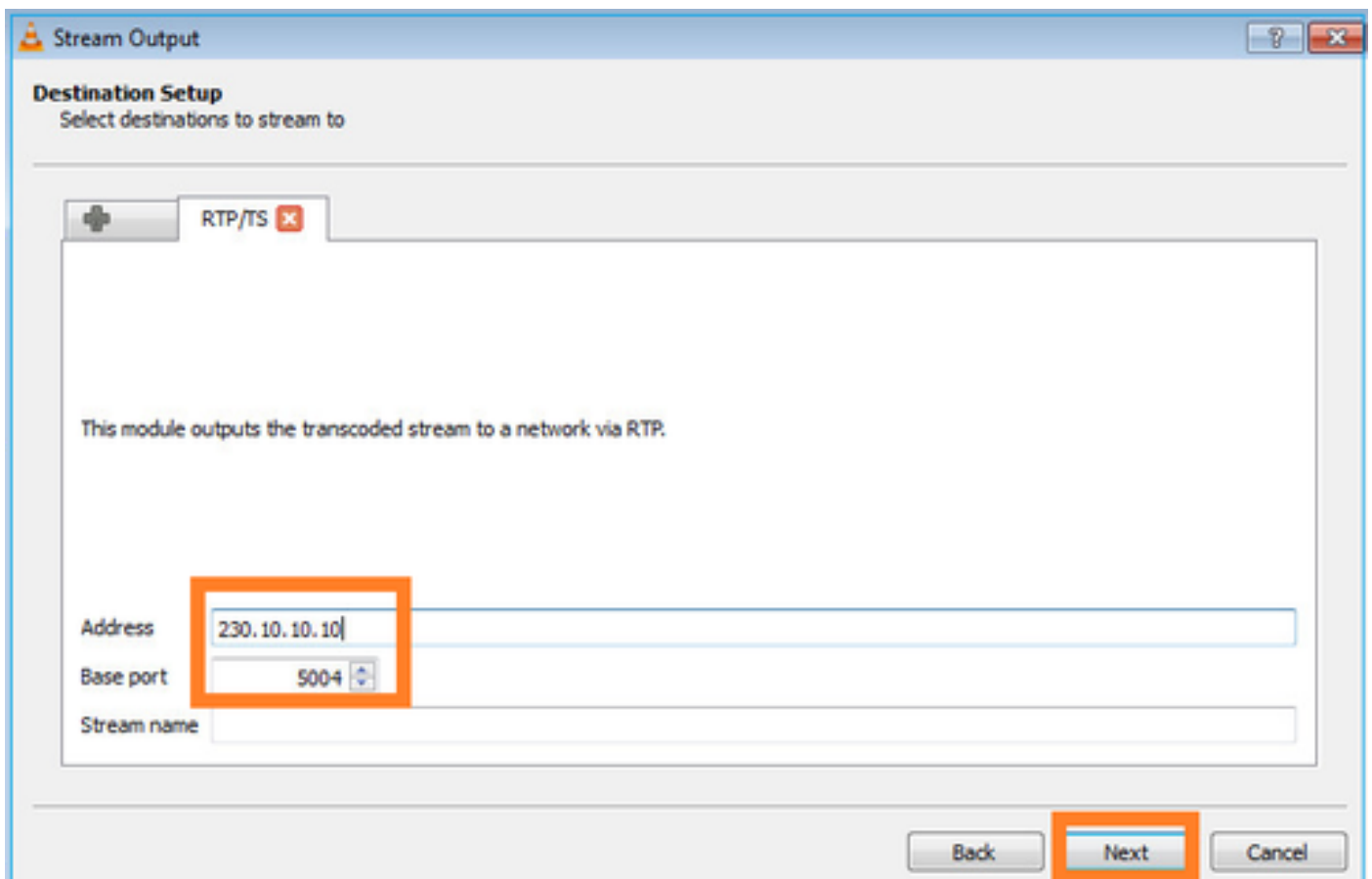


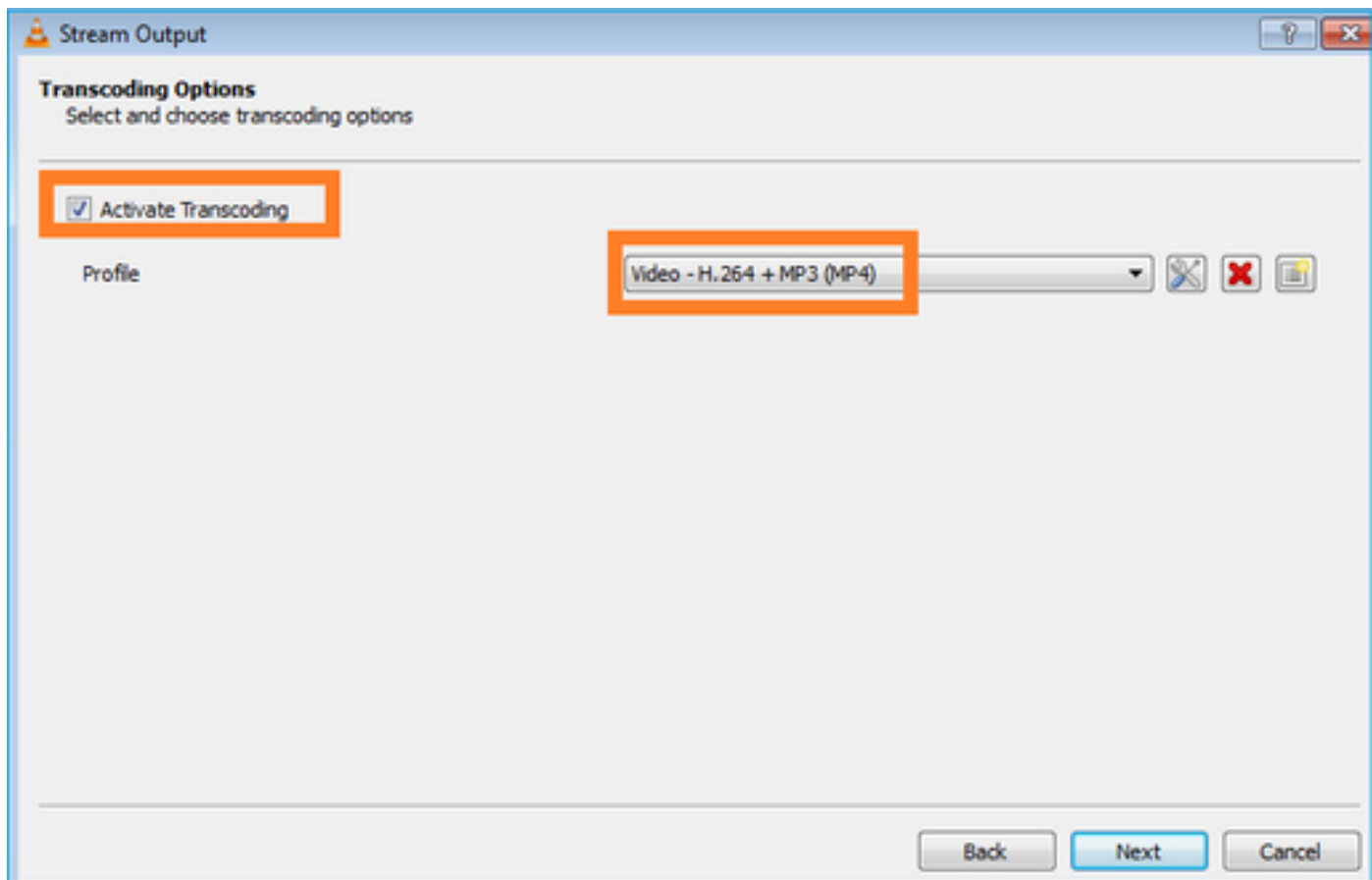
次の画面でNextを選択します。

フォーマットを選択します。



マルチキャストIPとポートを指定します。





FTDファイアウォールでLINAキャプチャを有効にします。

```
<#root>
```

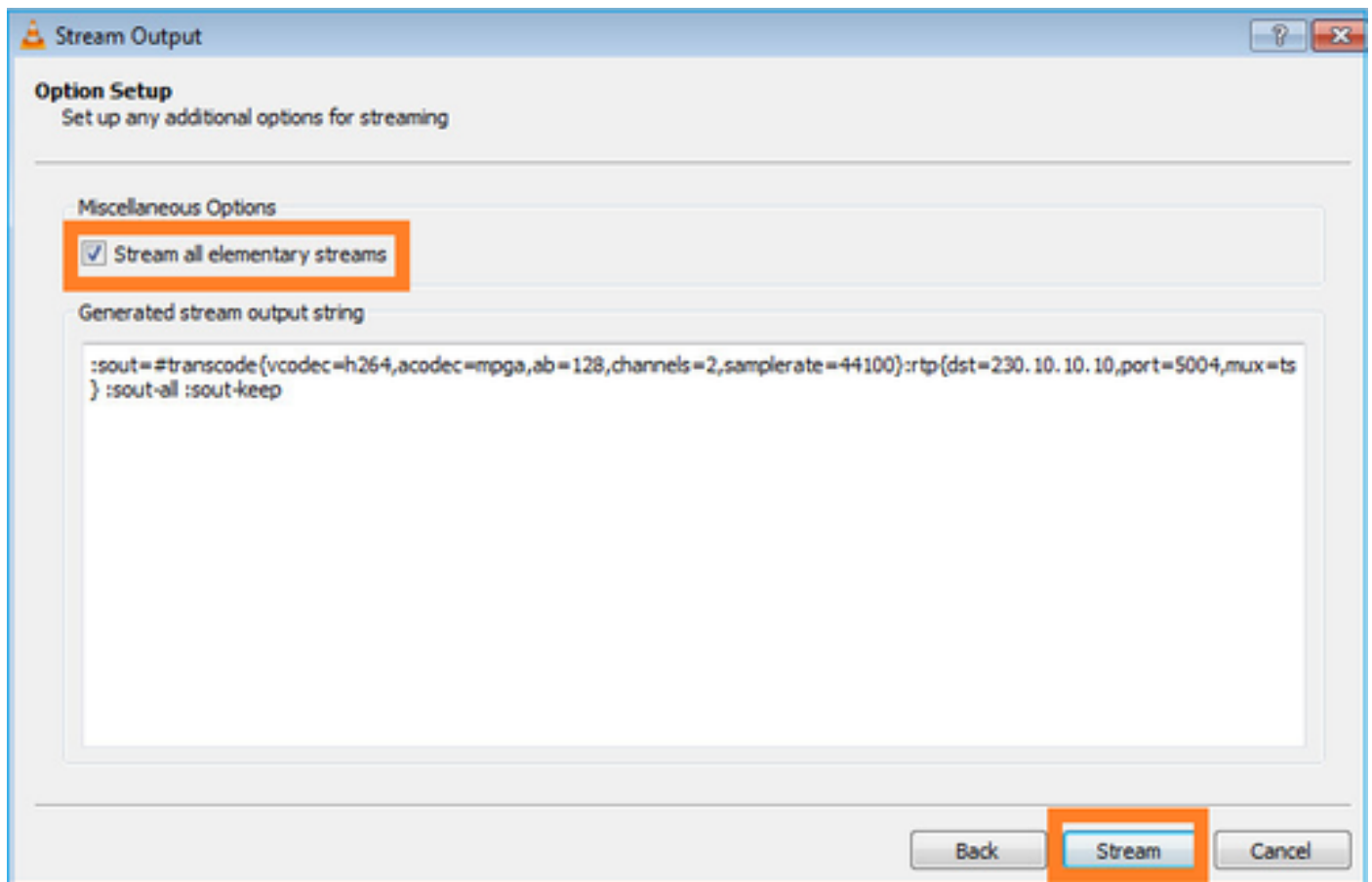
```
firepower#
```

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

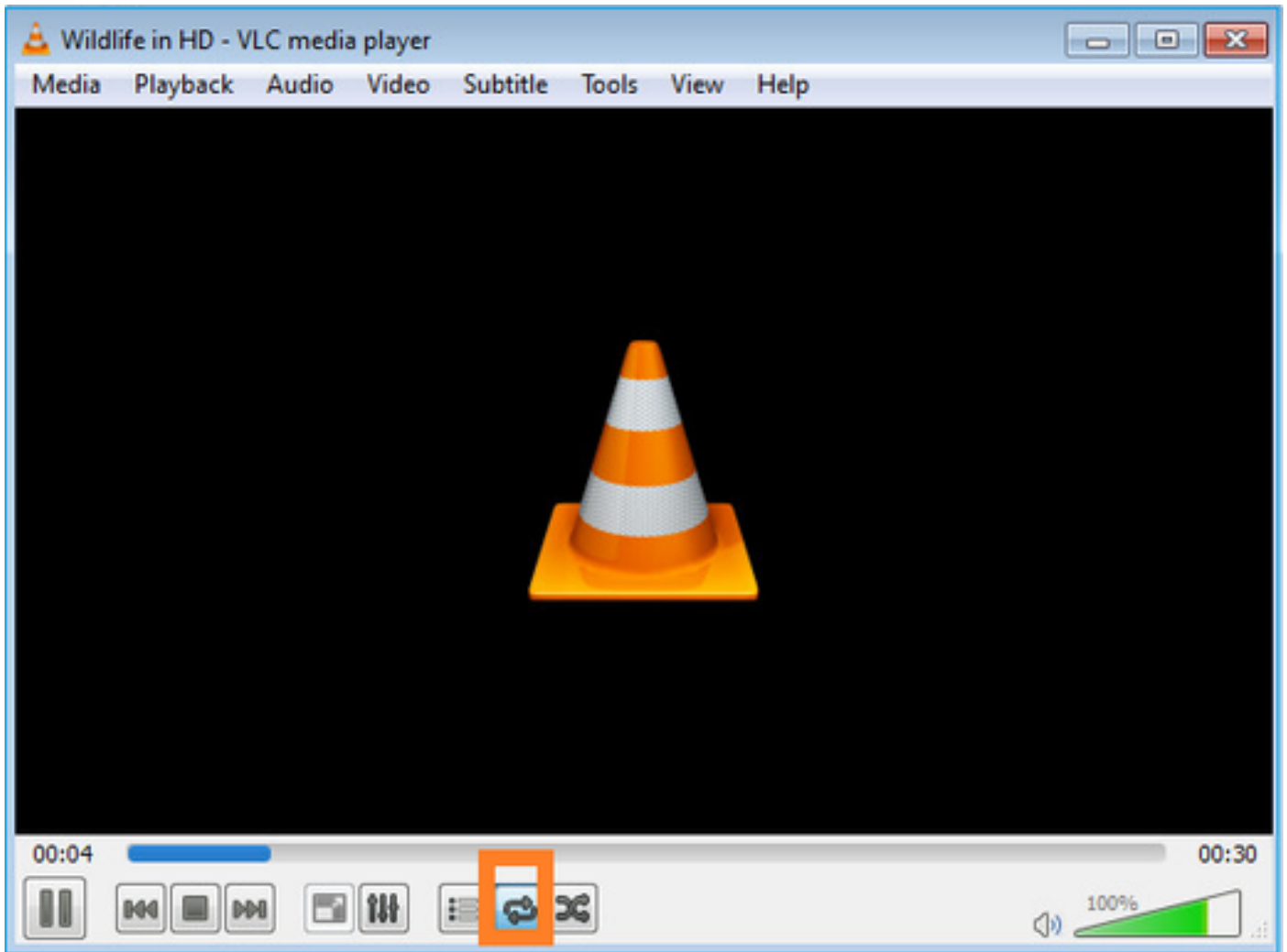
```
firepower#
```

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

デバイスのStreamボタンを選択して、マルチキャストストリームを開始します。



ストリームが継続的に送信されるように、「loop」オプションを有効にします。



### 検証 ( 非動作時のシナリオ )

このシナリオは、非動作シナリオのデモです。ここでの目的は、ファイアウォールの動作を実証することです。

ファイアウォールデバイスはマルチキャストストリームを取得しますが、それを転送しません。

```
<#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
```

ファイアウォールLINA ASPドロップの表示：

```
<#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
```

パケットをトレースするには、マルチキャストフローの最初のパケットをキャプチャする必要があります。この理由から、現在のフローをクリアします。

```
<#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」オプションを使用すると、マルチキャストMACアドレスが表示されます。

```
<#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)
```

```
...
```

実際のパケットのトレースは、パケットが許可されていることを示しますが、実際には次のことが起こりません。

```
<#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カウンタとmfibカウンタに基づいて、発信インターフェイスリスト(OIL)が空であるため、パケットはドロップされます。

<#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カウンタはRPF障害を示しますが、この場合は実際には発生しません。

<#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」の出力でも同様のRPF障害が発生します。

<#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:

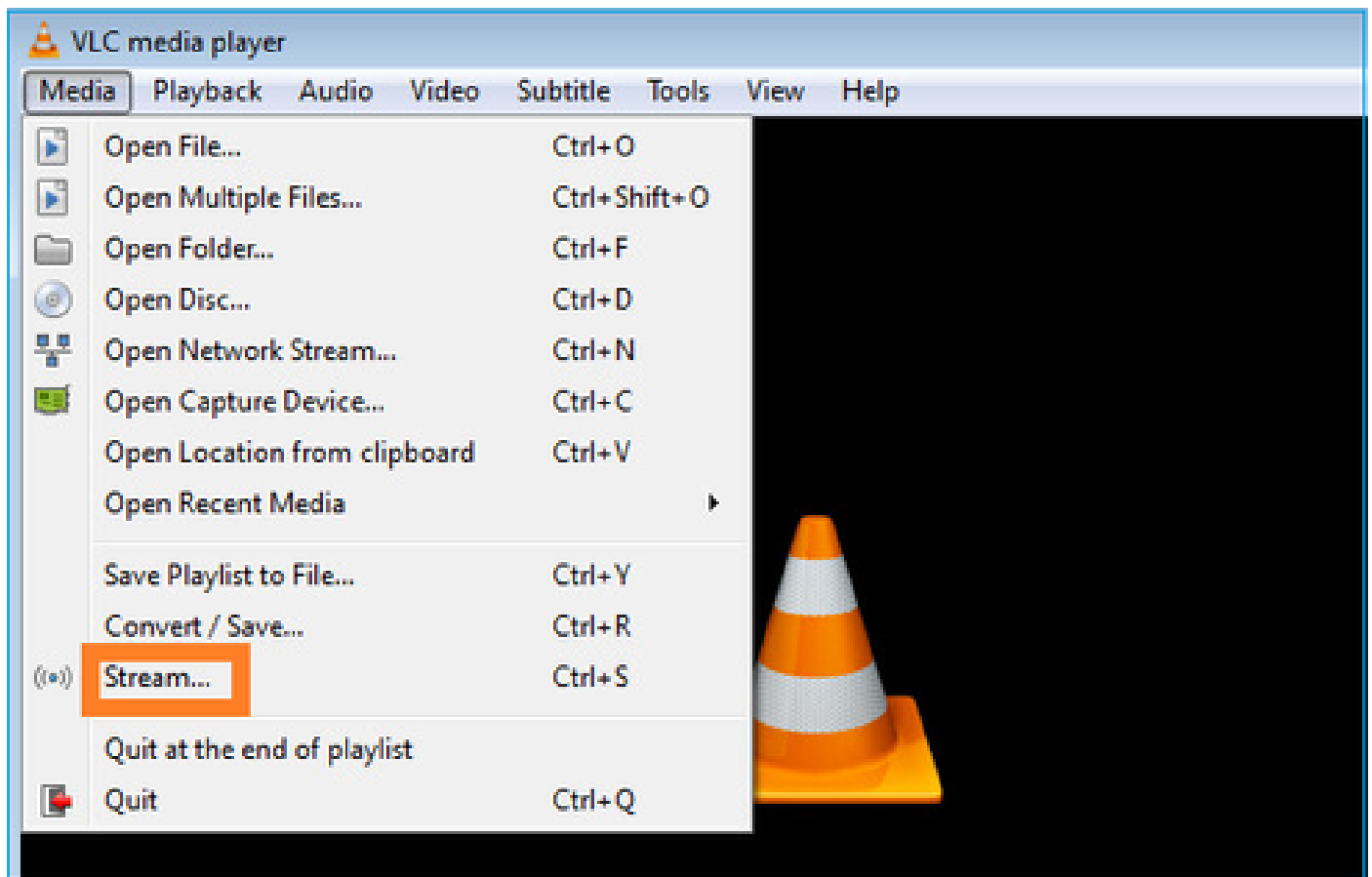
Forwarding: 0/0/0/0, Other: 0/0/0

Group: 239.255.255.250

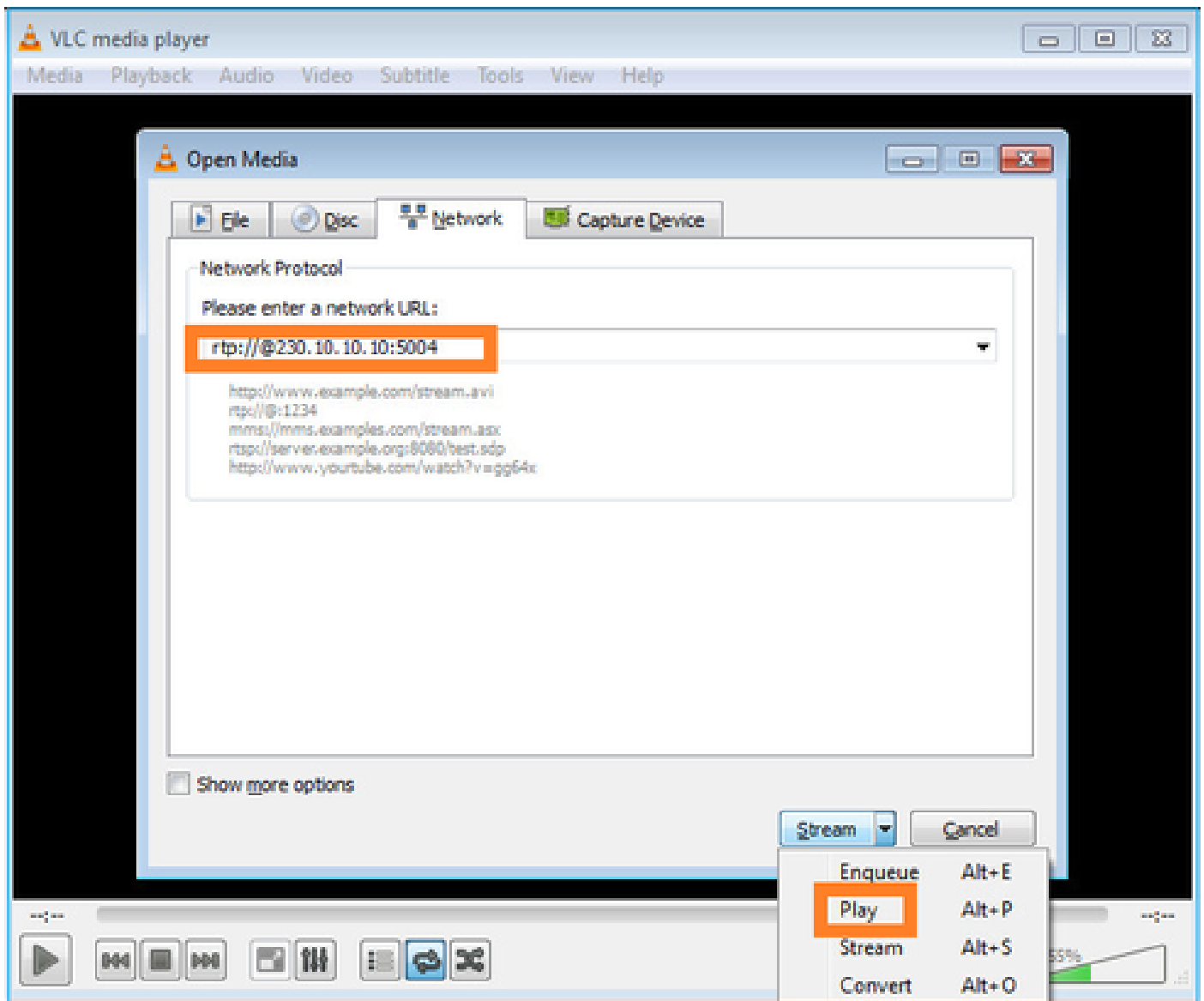
RP-tree:

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

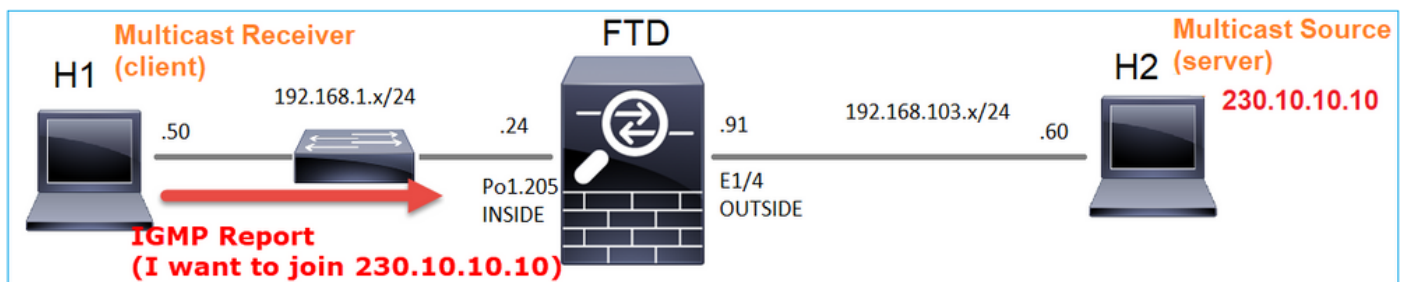
VLCマルチキャストレシーバを設定します。



マルチキャスト送信元IPを指定し、Play:



バックエンドでは、Playを選択するとすぐに、ホストが特定のマルチキャストグループに参加する意思をアナウンスし、IGMP Reportメッセージを送信します。



デバッグを有効にすると、IGMPレポートメッセージを確認できます。

```
<#root>
```

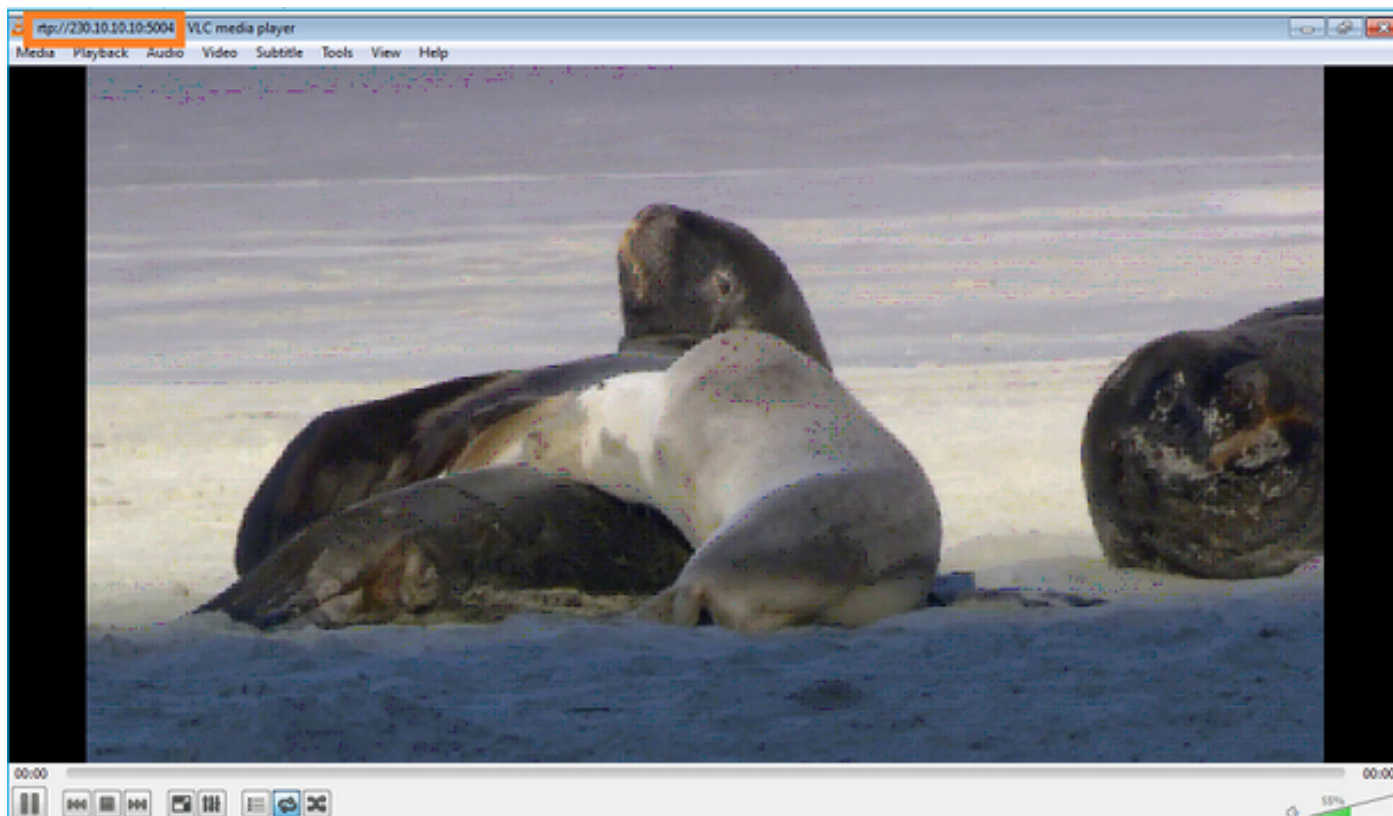
```
firepower#
```

```
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
```

ストリームが開始されます。



検証 ( 運用シナリオ )

```
<#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
```



ファイアウォールのmrouteテーブル :

<#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カウンタ :

<#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 スヌーピング

- IGMPスヌーピングは、マルチキャストフラッディングを防ぐためにスイッチで使用されるメカニズムです。
- スイッチはIGMPレポートをモニタして、ホスト（レシーバ）の位置を判別します。
- スイッチはIGMPクエリを監視して、ルータ/ファイアウォール（送信者）の場所を特定します。
- IGMPスヌーピングは、ほとんどのCiscoスイッチでデフォルトで有効になっています。詳細については、関連するスイッチングガイドを参照してください。L3 Catalystスイッチからの出力例を次に示します。

```
<#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	Vl206:Gi1/48	192.168.6.91	2d14h	2d13h	-
0.0.0.0/239.255.255.250	Vl206:Gi2/1	192.168.6.50	2d12h	00:52:49	00:52:45
0.0.0.0/224.0.1.40	Vl206:Gi2/26	192.168.6.1	00:20:10	2d13h	2d13h
0.0.0.0/230.10.10.10	Vl206:Gi2/26	192.168.6.1	2d13h	2d13h	-
0.0.0.0/230.10.10.10	Vl206:Gi2/26	192.168.6.91	2d13h	-	2d13h
0.0.0.0/239.10.10.10	Vl206:Gi2/26	192.168.6.1	2d14h	2d14h	-
0.0.0.0/239.10.10.10	Vl206:Gi2/26	192.168.6.91	2d14h	-	2d14h

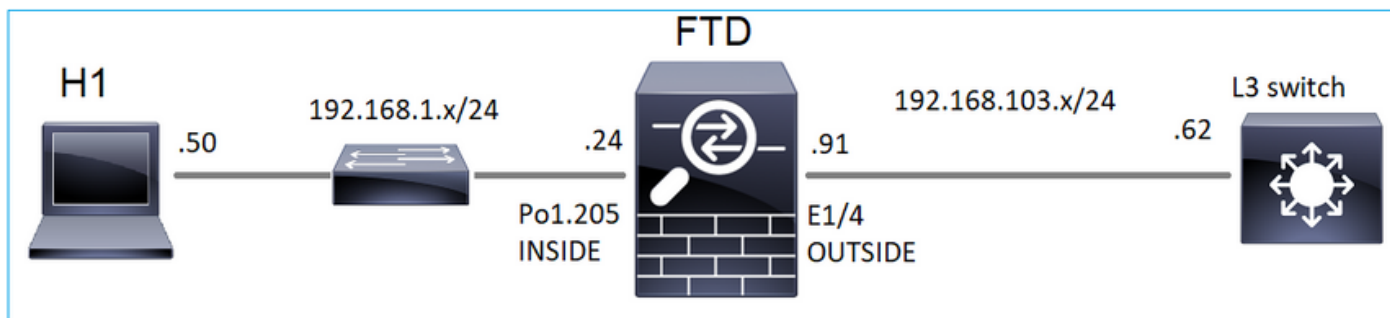
### 作業3:IGMPスタティックグループとIGMP参加グループの比較

#### 概要

	ip igmp static-group	ip igmp join-group
FTDインターフェイスに適用されますか。	Yes	Yes
FTDはマルチキャストストリームを引き付けますか。	はい。PIM Joinはアップストリームデバイスに送信されます。送信元またはランデブーポイント(RP)に送信されます。これは、このコマンドを使用したFTDがそのインターフェイスのPIM代表ルータ(DR)である場合にのみ発生します。	はい。PIM Joinはアップストリームデバイスに送信されます。送信元またはランデブーポイント(RP)に送信されます。これは、このコマンドを使用したFTDがそのインターフェイスのPIM代表ルータ(DR)である場合にのみ発生します。
FTDはマルチキャストトラフィックをインターフェイスから転送しますか。	Yes	Yes
FTDはマルチキャストトラフィックを消費し、応答しますか。	いいえ	はい。FTDはマルチキャストストリームをCPUにパントし、それを消費して送信元に応答します。
CPUへの影響	パケットはCPUにパントされないため、最小限です。	グループに属する各マルチキャストパケットはFTD CPUにパントされるため、FTD CPUに影響を与える可能性があります。

#### タスクの要件

このトポロジを参照してください。



ファイアウォールで、次のキャプチャを有効にします。

```
<#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スイッチからICMP pingを使用してマルチキャストトラフィックをIP 230.11.11.11に送信し、これがファイアウォールでどのように処理されるかを確認します。
2. ファイアウォールのINSIDEインターフェイスでigmp static-groupコマンドをイネーブルにして、マルチキャストストリーム(IP 230.11.11.11)がファイアウォールでどのように処理されるかを確認します。
3. ファイアウォールのINSIDEインターフェイスでigmp static-groupコマンドをイネーブルにして、マルチキャストストリーム(IP 230.11.11.11)がファイアウォールでどのように処理されるかを確認します。

## 解決方法

ファイアウォールにはIP 230.11.11.11のmrouteがありません。

```
<#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
```

マルチキャストをテストする簡単な方法は、ICMP pingツールを使用することです。この場合は、R2からマルチキャストIPアドレス230.11.11.11にpingを実行します。

<#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:

.....

ファイアウォールでは、mrouteが動的に作成され、OILは空です。

<#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

ファイアウォールのキャプチャは次のように表示されます。

<#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
```

ファイアウォールは各pingの接続を作成しますが、パケットをサイレントにドロップします。

<#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
```

---

 注：LINA ASPドロップキャプチャには、ドロップされたパケットは表示されません

---

マルチキャストパケットドロップの主な兆候は次のとおりです。

```
<#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,
```

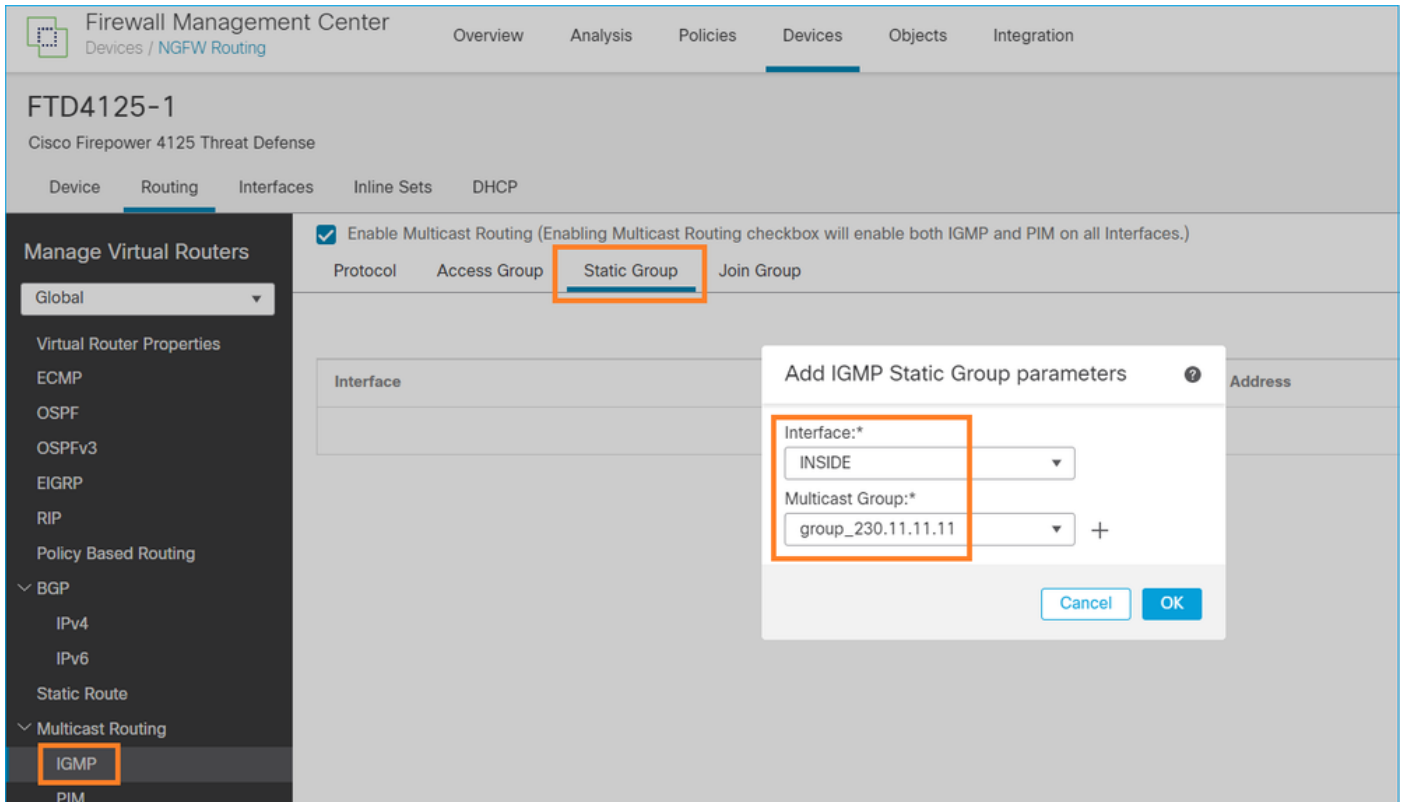
```
Other: 27/27/0
```

```
<-- The packets are dropped
```

## IGMPスタティックグループ

FMCで、スタティックIGMPグループを設定します。





バックグラウンドで導入される機能は次のとおりです。

```
<#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
```

pingは失敗しますが、ICMPマルチキャストトラフィックはファイアウォールを介して転送されま  
す。

```
<#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
```

---

 注：パケットのトレースに正しくない出力が示されています(入インターフェイスは出力と同じです。詳細については、Cisco Bug ID [CSCvm89673](https://tools.cisco.com/bugsearch/bug/CSCvm89673)を参照してください。)

---

```
<#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

---

 ヒント：発信元ホストからタイムアウト0でpingを実行し、ファイアウォールのmfibカウンタを確認できます。

---

<#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参加グループ

FMCリモートで、以前に設定したスタティックグループ設定とIGMP加入グループを設定します。

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

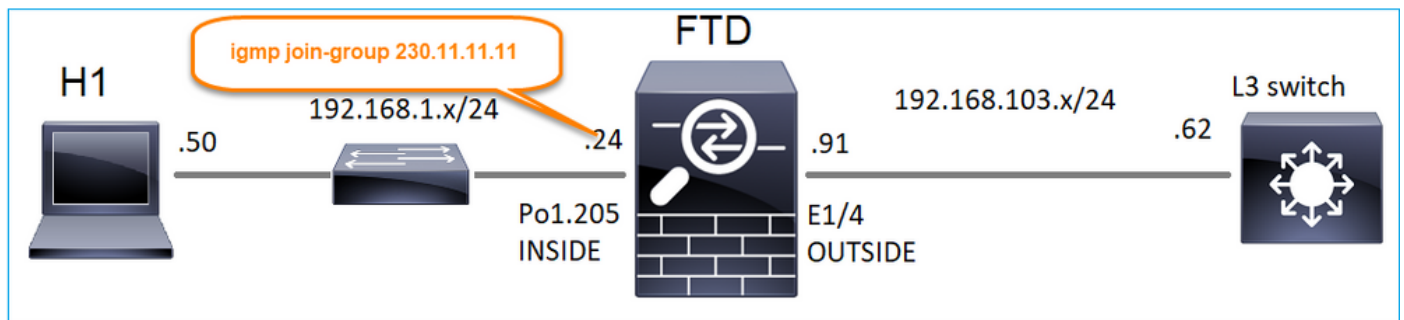
Virtual Router Properties

- 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



導入された設定は次のとおりです。

```
<#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グループ :

```
<#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
```

送信元ホストから、230.11.11.11 IPに対して最初のICMPマルチキャストテストを試行します。

```
<#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
```

---

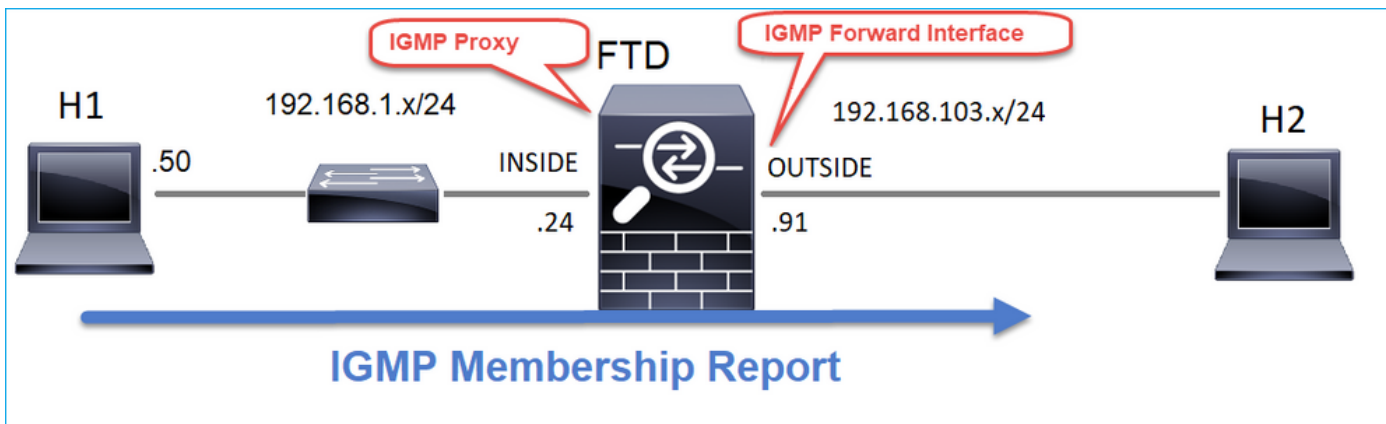
 注 : すべての応答が表示されない場合は、Cisco Bug ID [CSCvm90069](https://tools.cisco.com/bugsearch/bug/CSCvm90069)を確認してください

[o](#)

---

作業4:IGMPスタブマルチキャストルーティングの設定





FTDでスタブマルチキャストルーティングを設定して、INSIDEインターフェイスで受信したIGMPメンバーシップレポートメッセージがOUTSIDEインターフェイスに転送されるようにします。

### 解決方法

The screenshot shows the FMC interface for device FTD4125-1. The 'Routing' tab is active, and the 'IGMP' configuration is shown. The 'Enable Multicast Routing' checkbox is checked. The 'Protocol' tab is selected, and the 'INSIDE' interface is configured with 'Enabled' set to 'true' and 'Forward Interface' set to 'OUTSIDE'.

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

導入された設定は次のとおりです。

```
<#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
```

## 検証

FTDでキャプチャを有効にします。

```
<#root>
```

```
firepower#
```

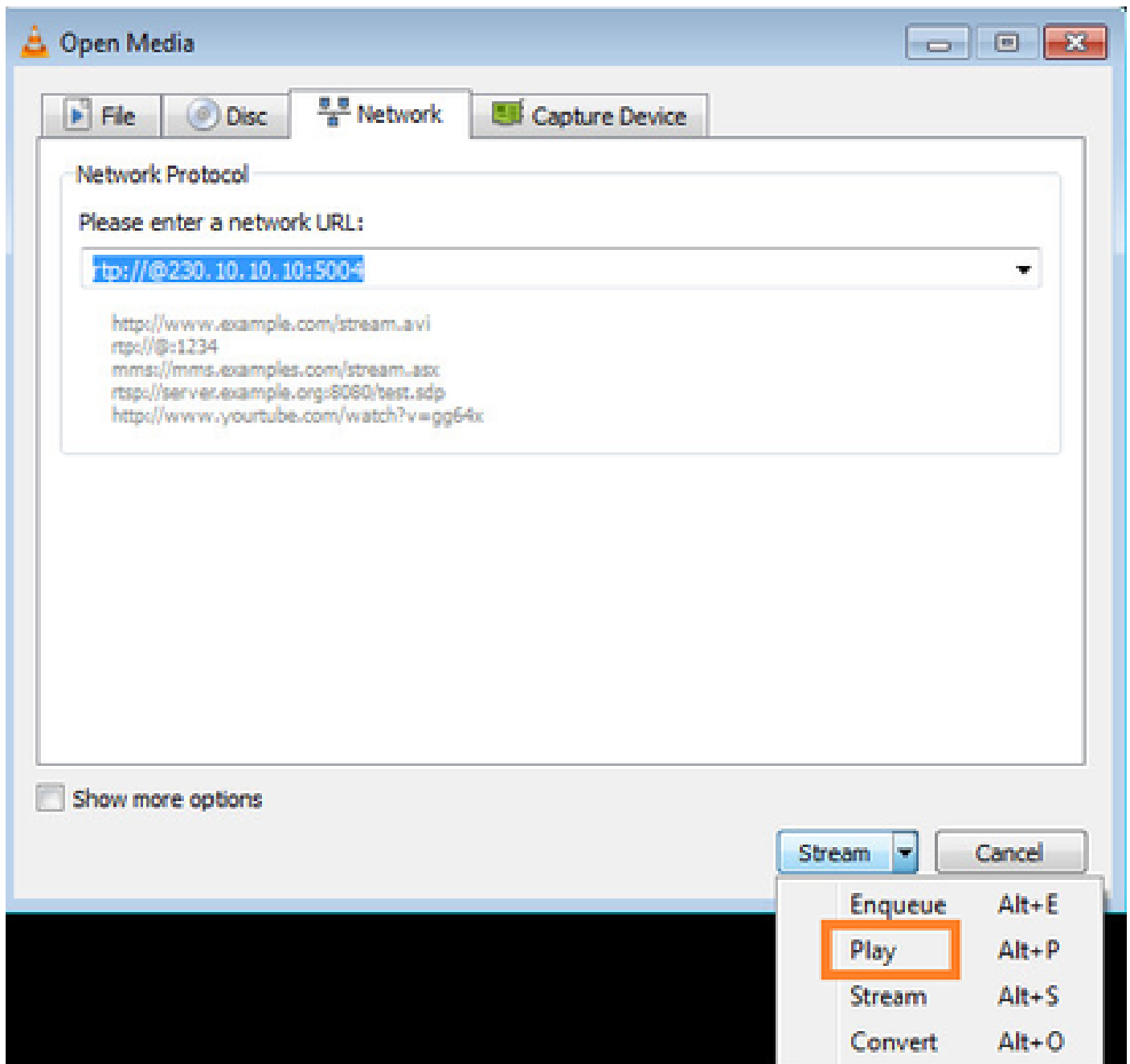
```
capture CAPI interface INSIDE trace match igmp any host 230.10.10.10
```

```
firepower#
```

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

## 検証

IGMPメンバーシップレポートを強制するには、VLCなどのアプリケーションを使用できます。



FTDはIGMPパケットをプロキシします。

```
<#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
```

FTDが送信元IPを変更します。

```
<#root>
```

```
firepower#
```

```
show capture CAPI
```

```
1 packet 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 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
```

Wiresharkでpcapを確認すると、パケットがファイアウォールによって完全に再生成されたことがわかります ( IP識別情報が変更されます )。

FTDにグループエントリが作成されます。

```
<#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ファイアウォールは、次の2つのコントロールプレーン接続を作成します。

```
<#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
```

最初のパケットのトレース :

```
<#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

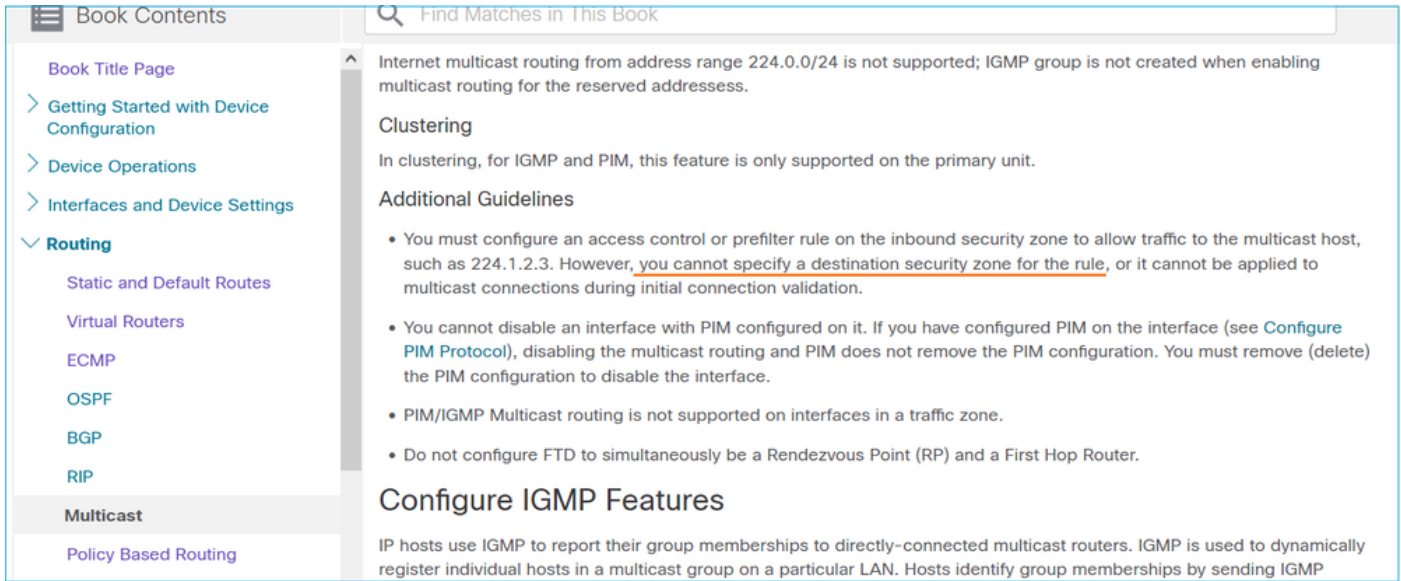
Config:

Additional Information:





これは、FMCユーザガイドにも記載されています。



## IGMPインターフェイスの制限を超えると、ファイアウォールによってIGMPレポートが拒否される

デフォルトでは、ファイアウォールは1つのインターフェイスで最大500の現在のActive Join ( レポート ) を許可します。このしきい値を超えると、ファイアウォールはマルチキャスト受信側からの追加の着信IGMPレポートを無視します。

IGMPの制限とアクティブな加入を確認するには、`show igmp interface nameif`コマンドを実行します。

```
<#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)
```

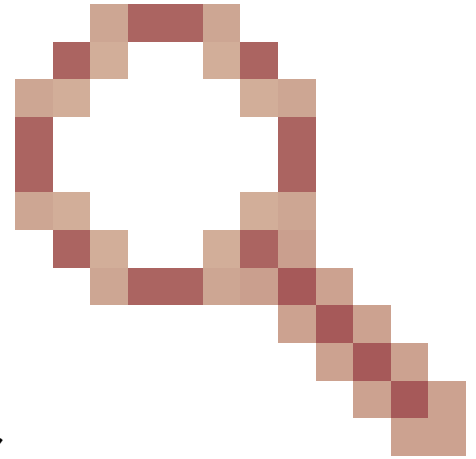
IGMP debugコマンド`debug igmp`は、次の出力を示します。

```
<#root>
```

```
asa#
```

```
debug igmp
```

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



Cisco Bug ID [CSCvw60976](#)の修正を含むソフトウェアバージョン  
インターフェイスごとに最大5000のグループを設定できます。

### ファイアウォールが232.x.x.x/8アドレス範囲のIGMPレポートを無視する

232.x.x.x/8のアドレス範囲は、Source Specific Multicast(SSM)で使用されます。ファイアウォールは、PIM Source Specific Multicast(SSM)機能および関連する設定をサポートしていません。

IGMP debugコマンドdebug igmpは、次の出力を示します。

```
<#root>
```

```
asa#
```

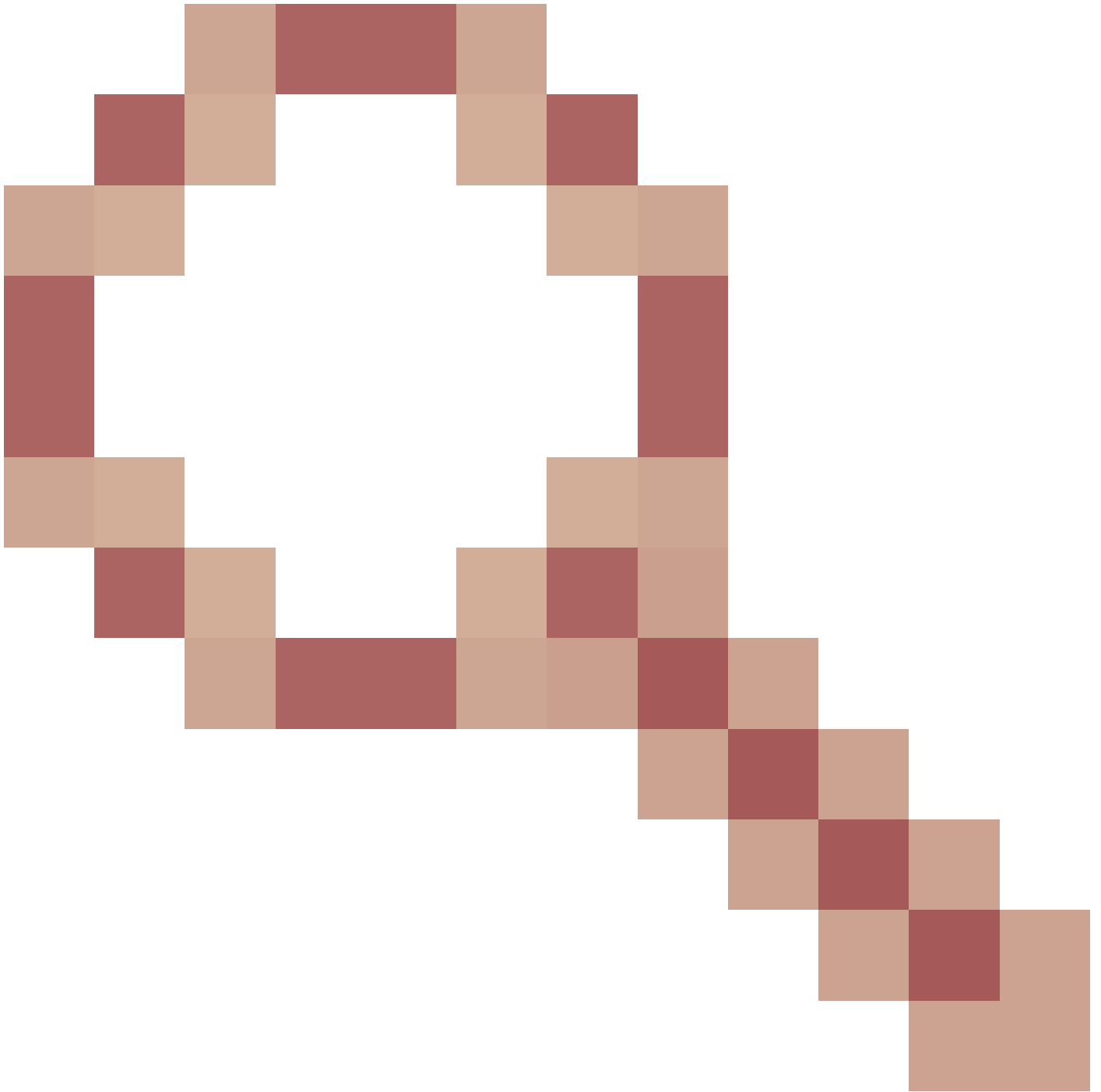
```
debug igmp
```

```
Apr 20 2023 09:37:10: %ASA-7-711001: IGMP: Received v2 Report on inside from 10.10.10.11 for 232.179.89.253
```

```
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 Bug ID [CSCsr53916](#)



は、SSM範囲をサポートする拡張機能を追跡します。

## 関連情報

- [firepower脅威対策のためのマルチキャストルーティング](#)
- [firepower脅威対策およびASAマルチキャストPIMのトラブルシューティング](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。