

# Dépannage de Firepower Threat Defense IGMP et des bases de la multidiffusion

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Notions de base IGMP](#)

[Tâche 1 - Trafic multidiffusion sur le plan de contrôle](#)

[Tâche 2 : configuration de la multidiffusion de base](#)

[IGMP Snooping](#)

[Tâche 3 : groupe IGMP statique et groupe IGMP de jointure](#)

[igmp static-group](#)

[igmp join-group](#)

[Tâche 4 : configuration du routage multidiffusion de stub IGMP](#)

[Problèmes identifiés](#)

[Filtrer le trafic multidiffusion sur les zones de destination](#)

[Les rapports IGMP sont refusés par le pare-feu lorsque la limite d'interface IGMP est dépassée](#)

[Le pare-feu ignore les rapports IGMP pour la plage d'adresses 232.x.x.x/8](#)

[Informations connexes](#)

---

## Introduction

Ce document décrit les bases de la multidiffusion et comment Firepower Threat Defense (FTD) implémente le protocole IGMP (Internet Group Management Protocol).

## Conditions préalables

### Exigences

Connaissances de base du routage IP.

### Composants utilisés

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau

est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Le contenu de cet article s'applique également au logiciel ASA (Adaptive Security Appliance).

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Firepower 4125 Threat Defense Version 7.1.0.
- Firepower Management Center (FMC) version 7.1.0.
- ASA version 9.19.1.

## Informations générales

### Définitions

- Monodiffusion = d'un hôte unique vers un autre hôte (un vers un).
- Diffusion = d'un hôte unique vers TOUS les hôtes possibles (un vers tous).
- Multidiffusion = d'un hôte d'un groupe d'hôtes vers un groupe d'hôtes (un-à-plusieurs ou plusieurs-à-plusieurs).
- Anycast = d'un hôte vers l'hôte le plus proche d'un groupe (un-à-un-parmi-plusieurs).

### Notions de base

- La RFC 988 multidiffusion a été écrite en 1986 par Steve Deering.
- La multidiffusion IPv4 utilise la plage 224.0.0.0/4 (4 premiers bits 110) - 224.0.0.0 - 239.255.255.255.
- Pour IPv4, l'adresse MAC de couche 2 provient de l'adresse IP de multidiffusion de couche 3 : 01005e (24 bits) + 25<sup>e</sup> bit toujours 0 + 23 bits inférieurs de l'adresse IPv4 de multidiffusion.
- La multidiffusion IPv6 utilise la plage FF00::/8 et elle est plus flexible que la multidiffusion IPv4 car elle peut intégrer l'IP Rendezvous Point (RP).
- Pour IPv6, l'adresse MAC de couche 2 provient de la multidiffusion de couche 3 : 333 + 32 bits inférieurs de l'adresse IPv6 de multidiffusion.
- Avantages de la multidiffusion : efficacité grâce à une charge réduite sur la source. Les performances, car elles évitent la duplication ou l'inondation du trafic.
- Inconvénients de la multidiffusion : transport non fiable (basé sur UDP), pas d'évitement d'encombrement, livraison hors séquence.
- La multidiffusion n'est pas prise en charge sur l'Internet public, car elle nécessite tous les périphériques du chemin pour l'activer. Généralement utilisé lorsque tous les périphériques sont sous une autorité administrative commune.
- Applications de multidiffusion standard : flux vidéo interne, vidéoconférence.

### Multidiffusion et monodiffusion répliquée

Dans la monodiffusion répliquée, la source crée plusieurs copies du même paquet de monodiffusion (réplicas) et les envoie à plusieurs hôtes de destination. La multidiffusion déplace la charge de l'hôte source vers le réseau, tandis que dans la monodiffusion répliquée, tout le travail est effectué sur l'hôte source.

# Configurer

## Notions de base IGMP

- IGMP est le « langage » parlé entre les récepteurs de multidiffusion et le périphérique L3 local (généralement un routeur).
- IGMP est un protocole de couche 3 (comme ICMP) et utilise le protocole IP numéro 2.
- Il existe actuellement 3 versions IGMP. La version par défaut d'IGMP sur le pare-feu est la version 2. Seules les versions 1 et 2 sont actuellement prises en charge.
- Entre IGMPv1 et IGMPv2, les principales différences sont les suivantes :
  - IGMPv1 n'a pas de message Leave Group.
  - IGMPv1 n'a pas de requête spécifique au groupe (utilisée par le pare-feu lorsqu'un hôte quitte un groupe de multidiffusion).
  - IGMPv1 n'a pas de processus de sélection de demandeur.
- IGMPv3 n'est pas actuellement pris en charge sur ASA/FTD, mais comme référence, la différence importante entre IGMPv2 et IGMPv3 est l'inclusion d'une requête spécifique au groupe et à la source dans IGMPv3 qui est utilisée dans la multidiffusion spécifique à la source (SSM).
- Requêtes IGMPv1/IGMPv2/IGMPv3 = 224.0.0.1  
IGMPv2 Leave = 224.0.0.2  
Rapport d'adhésion IGMPv3 = 224.0.0.22
- Si un hôte veut rejoindre peut envoyer un message non sollicité de rapport d'adhésion IGMP :

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

- Du point de vue du pare-feu, il existe 2 types de requêtes IGMP : les requêtes générales et les requêtes spécifiques à un groupe
- Lorsque le pare-feu reçoit un message IGMP Leave Group, il doit vérifier s'il y a d'autres membres de ce groupe sur le sous-réseau. Pour cette raison, le pare-feu envoie une requête spécifique au groupe :

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

- Sur les sous-réseaux où il y a plusieurs routeurs/pare-feu, un demandeur (un périphérique qui envoie toutes les requêtes IGMP) est sélectionné :

```
<#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
```

- Sur FTD, comme un ASA classique, vous pouvez activer debug igmp pour voir les messages relatifs à IGMP :

```
<#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

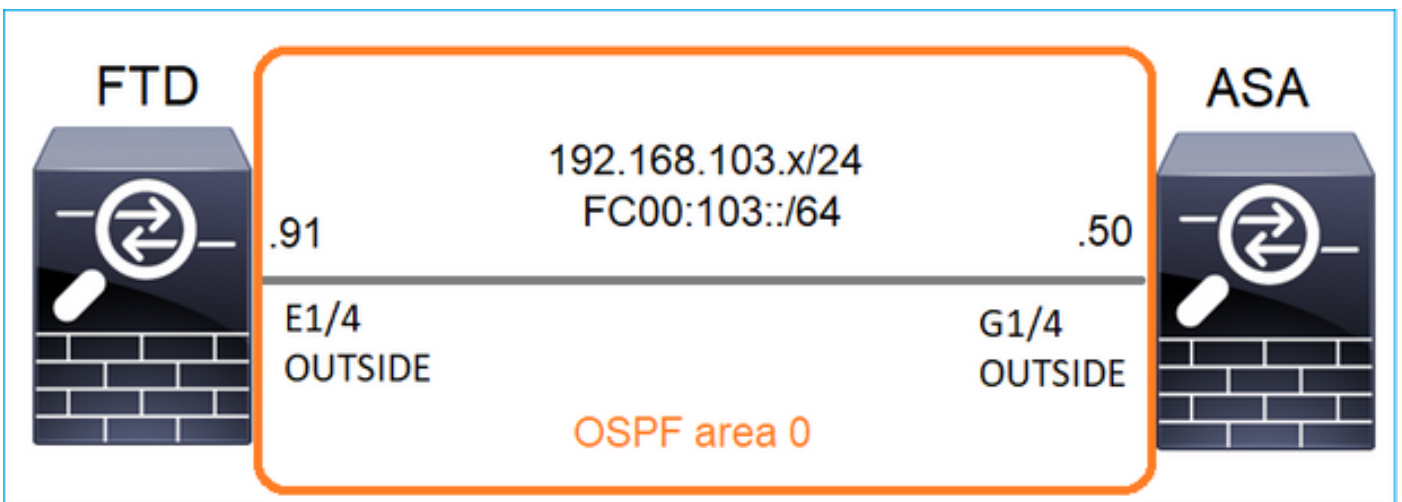
```

- Un hôte quitte normalement un groupe de multidiffusion avec un message Leave Group (IGMPv2).

The image shows a Wireshark capture of IGMPv2 traffic. The filter is 'igmp.type == 0x17'. Two packets are visible, both of type 'Leave Group' for the multicast address 230.10.10.10. The first packet is from source 192.168.1.50 to destination 224.0.0.2, with identification 0x01a7 (423). The second packet is from source 192.168.1.50 to destination 224.0.0.2, with identification 0x020b (523).

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

## Tâche 1 - Trafic multidiffusion sur le plan de contrôle



Configurez un OSPFv2 et un OSPFv3 entre le FTD et l'ASA. Vérifiez comment les deux périphériques gèrent le trafic de multidiffusion de couche 2 et de couche 3 généré par OSPF.

Solution

Configuration OSPFv2

Firewall Management Center  
Devices / NGFW Routing

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⓘ

FTD4125-1 Save Cancel

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	

De même, pour OSPFv3

Configuration sur CLI FTD :

```
<#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
```

La configuration crée ces entrées dans les tables d'autorisation FTD du chemin de sécurité

accéléré (ASP) afin que le trafic de multidiffusion entrant ne soit pas bloqué :

```
<#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
```

Pour IPv6 :

```
<#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
...

```

Les contiguïtés OSPFv2 et OSPFv3 sont UP :

```

<#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

```

Voici les sessions OSPF de multidiffusion terminées vers le boîtier :

```

<#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
```

À titre de test, activez la capture pour IPv4 et effacez les connexions au périphérique :

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

---

 Avertissement : ceci provoque une panne ! L'exemple est présenté à des fins de démonstration uniquement !

---

Les paquets OSPF capturés :

```
<#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]
```

Voici comment le paquet de multidiffusion OSPFv2 est géré par le pare-feu :

```
<#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

Voici comment le paquet de multidiffusion OSPFv3 est géré par le pare-feu :

<#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

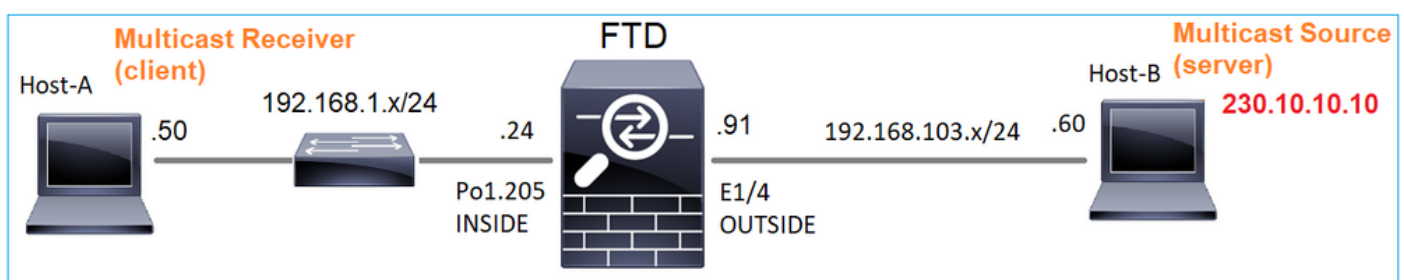
output-interface: NP Identity Ifc

Action: allow

Time Taken: 83448 ns

## Tâche 2 : configuration de la multidiffusion de base

### Topologie



## Exigence

Configurez le pare-feu de sorte que le trafic de multidiffusion provenant du serveur soit transmis au client de multidiffusion sur IP 230.10.10.10

## Solution

Du point de vue du pare-feu, la configuration minimale consiste à activer le routage de multidiffusion globalement. Cela active en arrière-plan les protocoles IGMP et PIM sur toutes les interfaces de pare-feu.

Sur l'interface utilisateur FMC :

The screenshot shows the FMC interface for device FTD4125-1. The 'Devices' tab is selected, and the 'Routing' sub-tab is active. A checkbox labeled 'Enable Multicast Routing (Enabling Multicast Routing checkbox will enable both IGMP and PIM on all interfaces.)' is checked and highlighted with an orange box. Below this, a table with columns 'Interface', 'PIM Enabled', 'DR Priority', and 'Hello Interval' is shown, but it contains no records. A left-hand navigation menu is visible, with 'PIM' selected under the 'Multicast Routing' section.

Sur l'interface de ligne de commande du pare-feu, voici la configuration poussée :

```
<#root>
firepower#
show run multicast-routing
multicast-routing
<-- Multicast routing is enabled
```

## Vérification IGMP

```
<#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		

## Vérification PIM

<#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

## Vérification MFIB

<#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

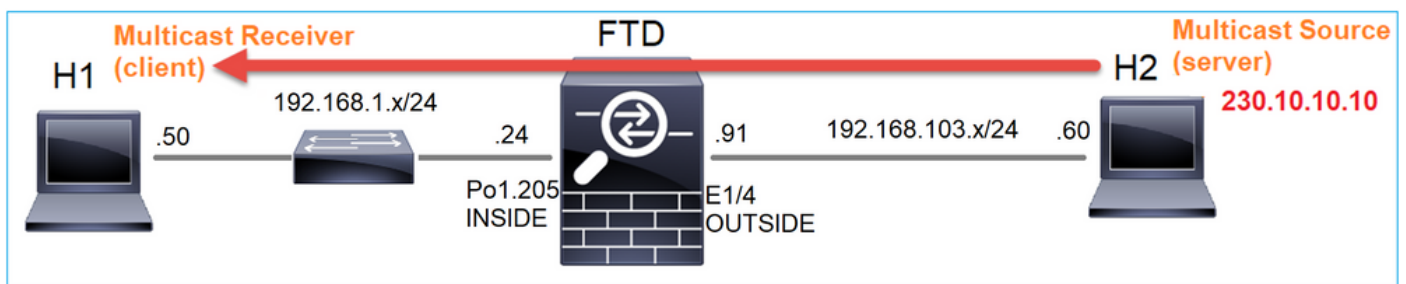
<-- The Other counters are: Total/RPF failed/Other drops

(\* ,232.0.0.0/8) Flags: K

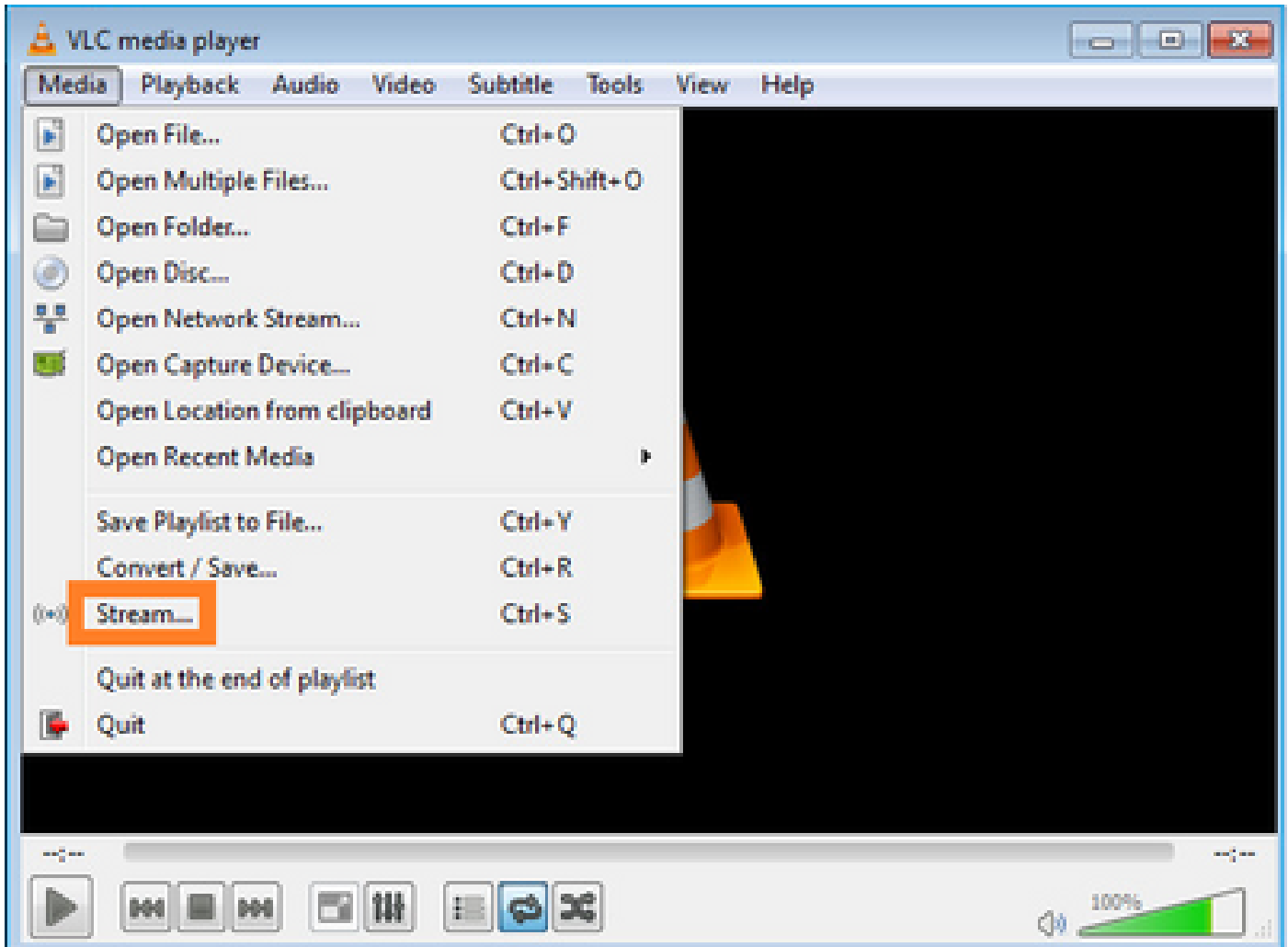
Forwarding: 0/0/0/0, Other: 0/0/0

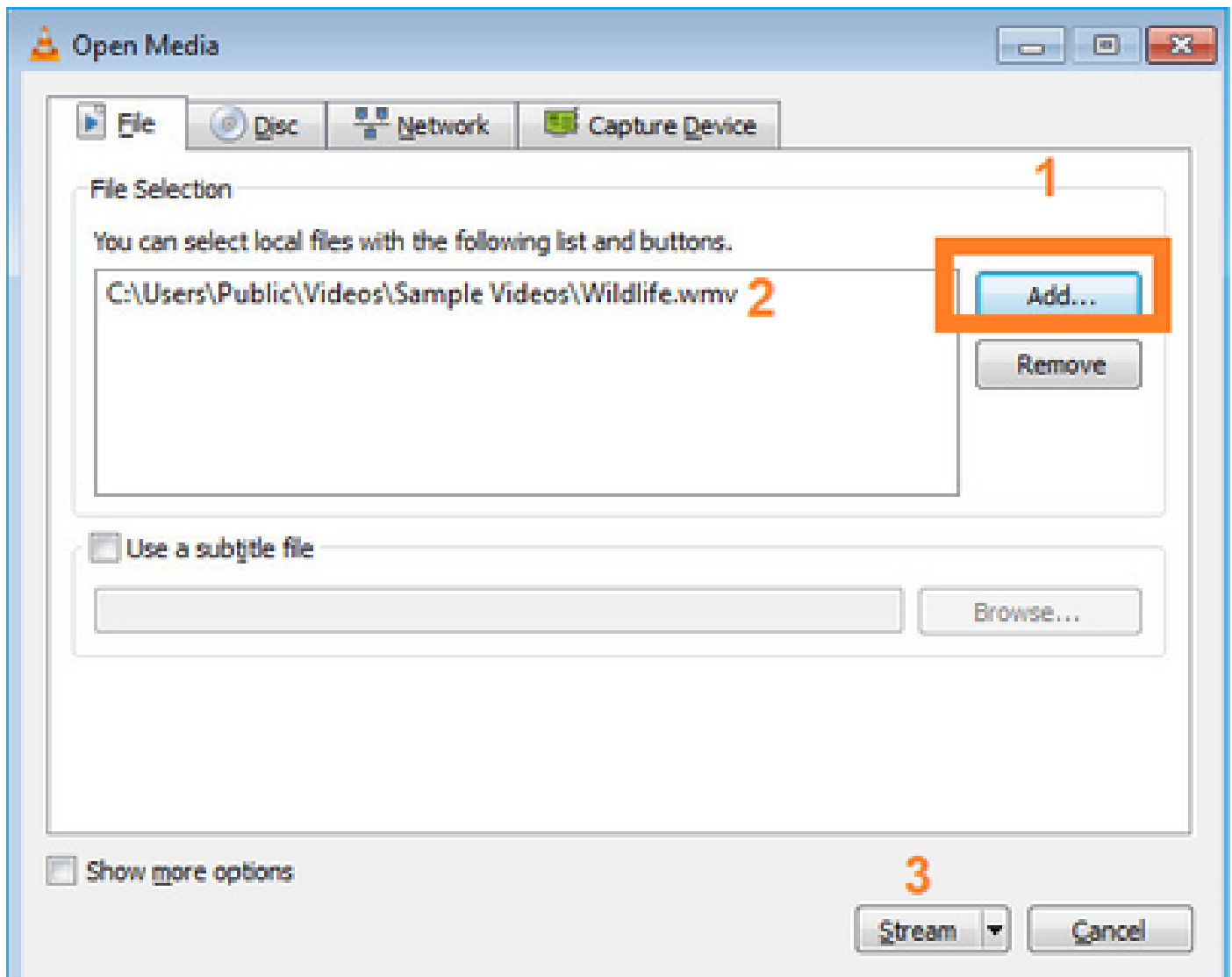
### Trafic de multidiffusion via le pare-feu

Dans ce cas, l'application de lecteur multimédia VLC est utilisée comme serveur de multidiffusion et comme client pour tester le trafic de multidiffusion :



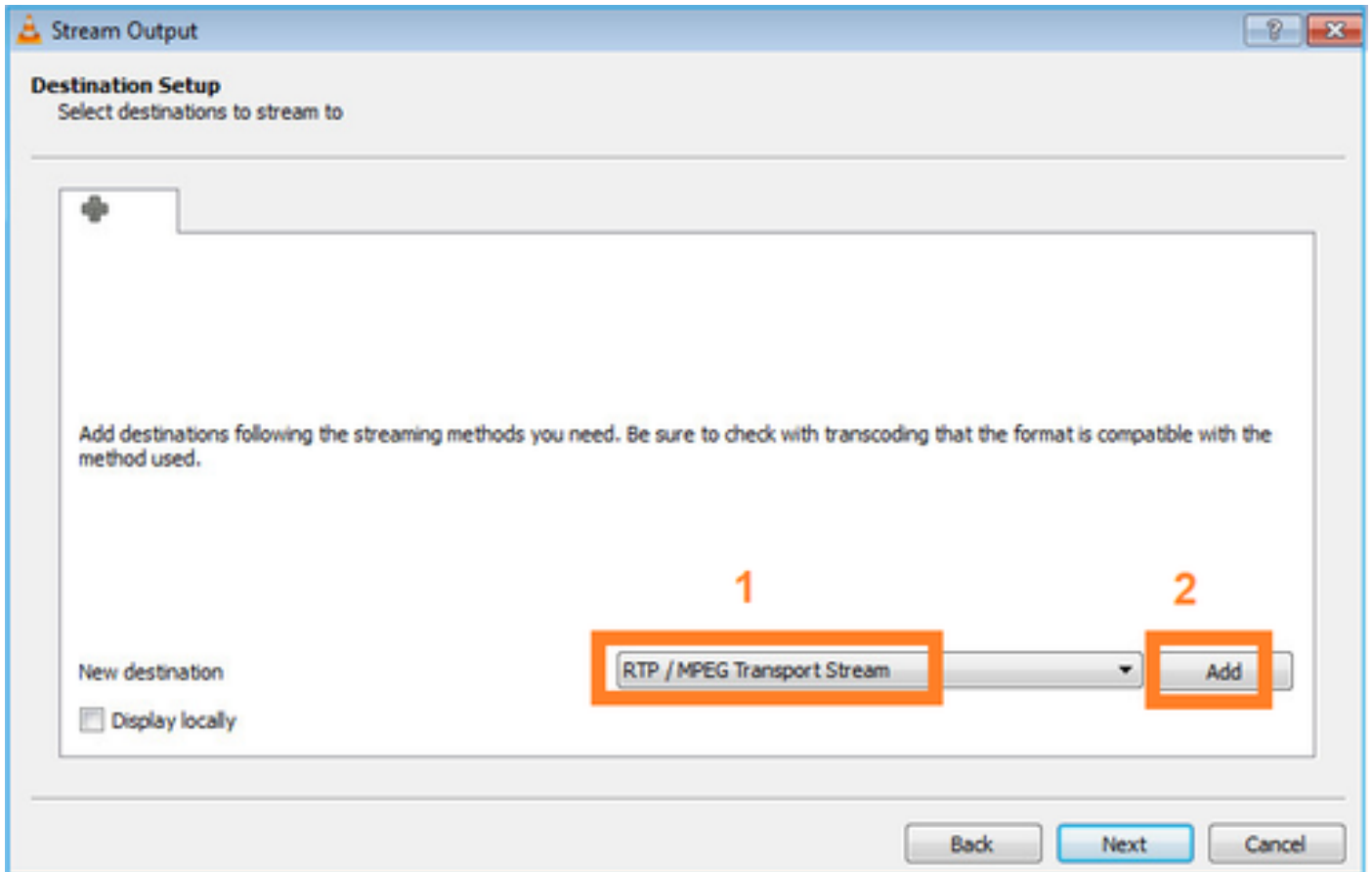
Configuration du serveur de multidiffusion VLC :



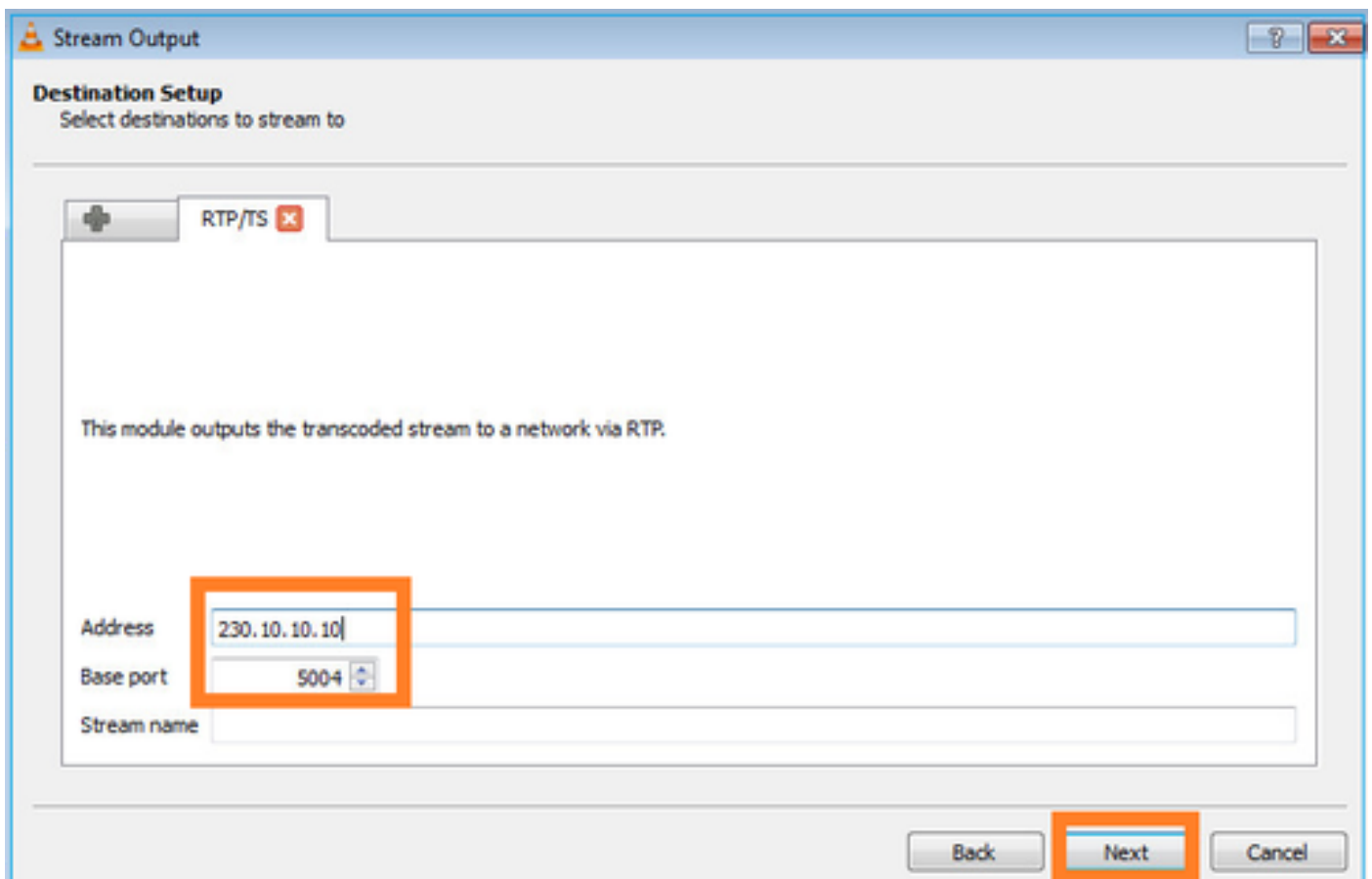


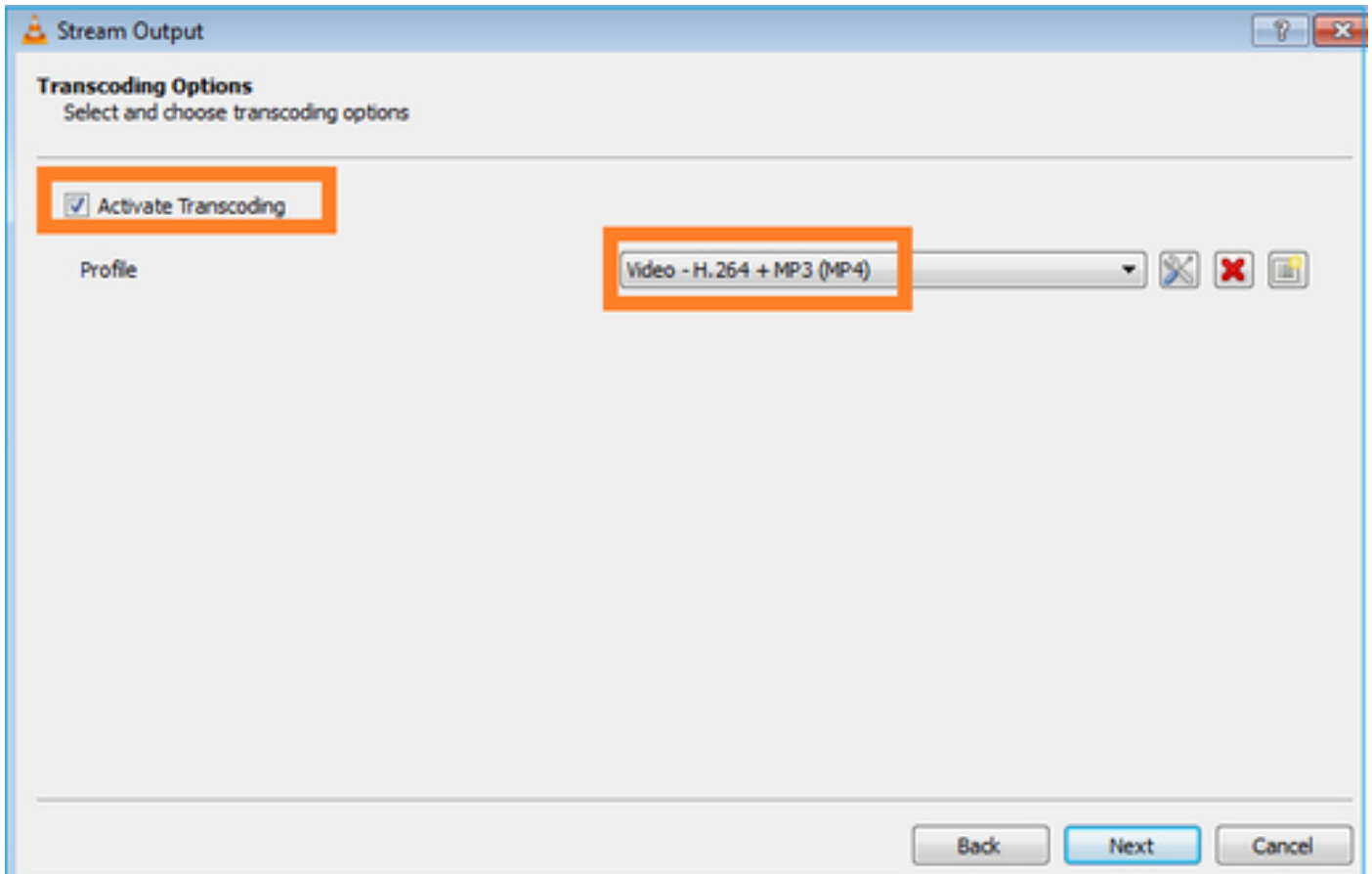
Dans l'écran suivant, sélectionnez Suivant.

Sélectionnez le format :



Spécifiez l'adresse IP et le port de multidiffusion :





Activez les captures LINA sur le pare-feu FTD :

```
<#root>
```

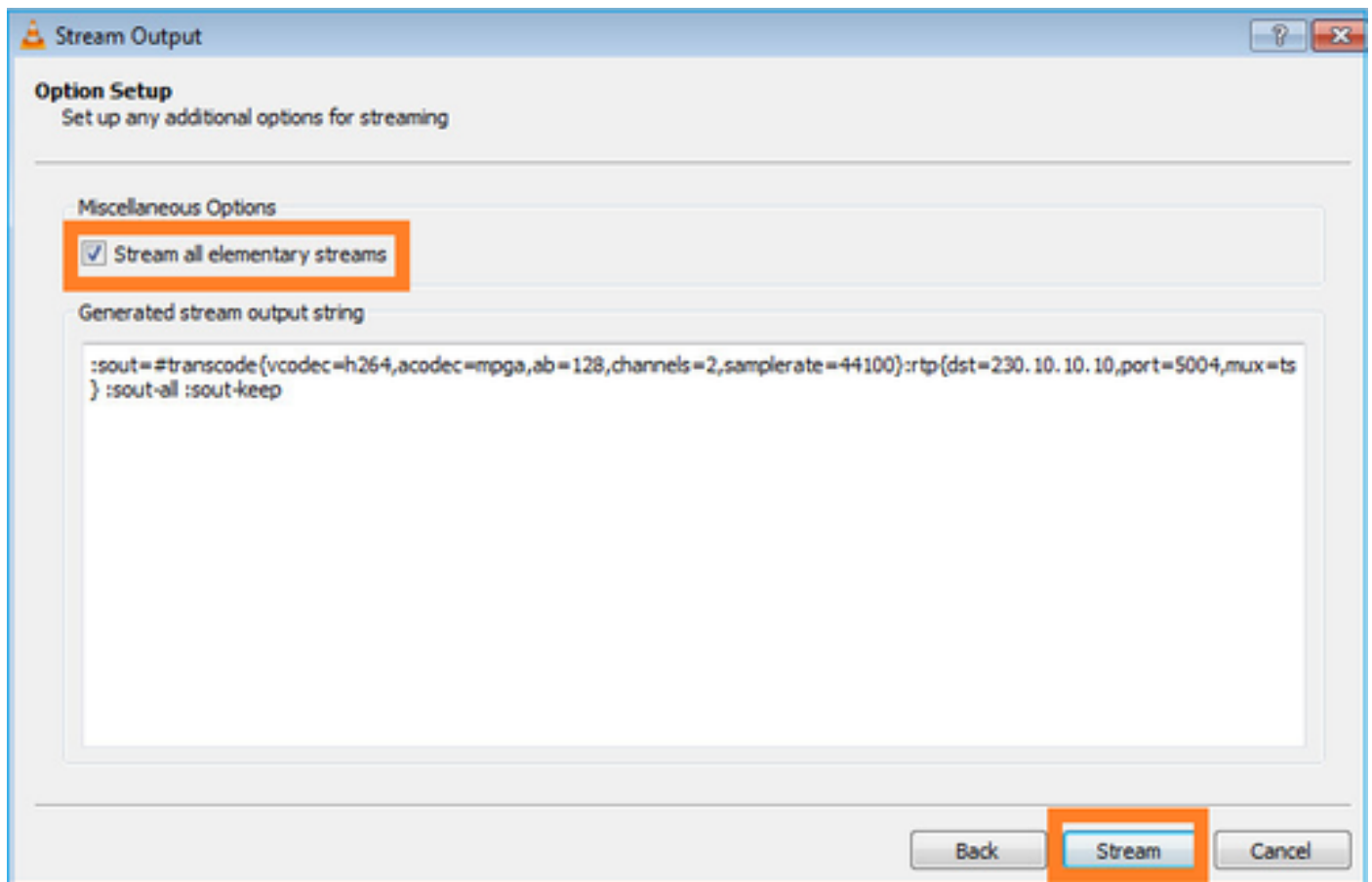
```
firepower#
```

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

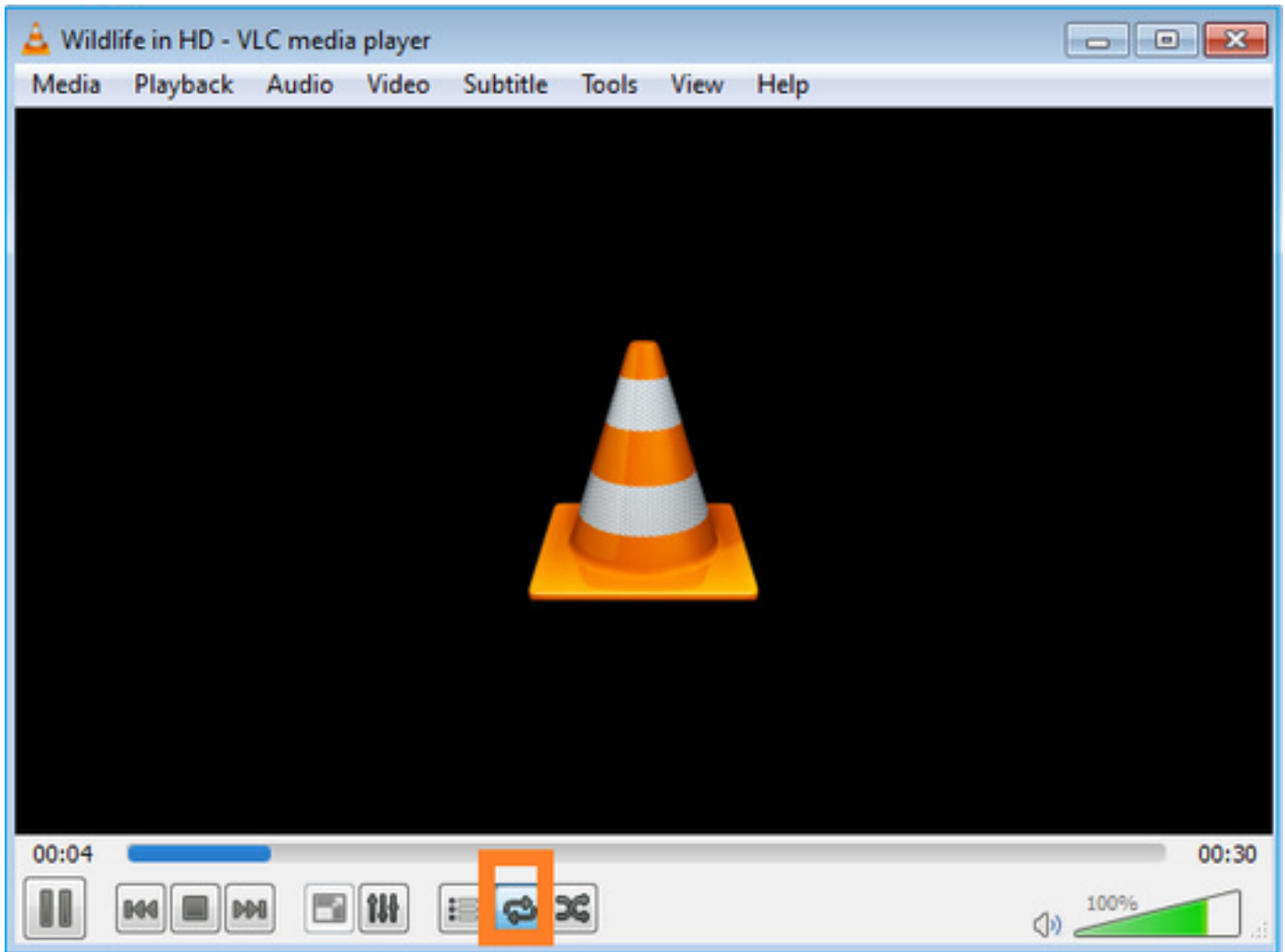
```
firepower#
```

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

Sélectionnez le bouton Stream pour que le périphérique démarre le flux de multidiffusion :



Activez l'option « loop » pour que le flux soit envoyé en continu :



Vérification (scénario non opérationnel)

Ce scénario est une démonstration d'un scénario non opérationnel. L'objectif est de démontrer le comportement du pare-feu.

Le périphérique pare-feu obtient le flux de multidiffusion, mais ne le transfère pas :

```
<#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
```

Firewall LINA ASP drops show :

```
<#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
```

Pour suivre un paquet, il est nécessaire de capturer le premier paquet du flux de multidiffusion.  
Pour cette raison, effacez les flux actuels :

```
<#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  
...
```



L'option « detail » indique l'adresse MAC de multidiffusion :

```
<#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)
```

```
...
```

La trace d'un paquet réel montre que le paquet est autorisé, mais ce n'est pas ce qui se passe réellement :

```
<#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

En fonction des compteurs mroute et mfib, les paquets sont abandonnés car la liste d'interfaces sortantes (OIL) est vide :

<#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

Les compteurs MFIB montrent des échecs RPF qui dans ce cas ne sont pas ce qui se passe réellement :

<#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

Échecs RPF similaires dans la sortie « show mfib count » :

<#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:

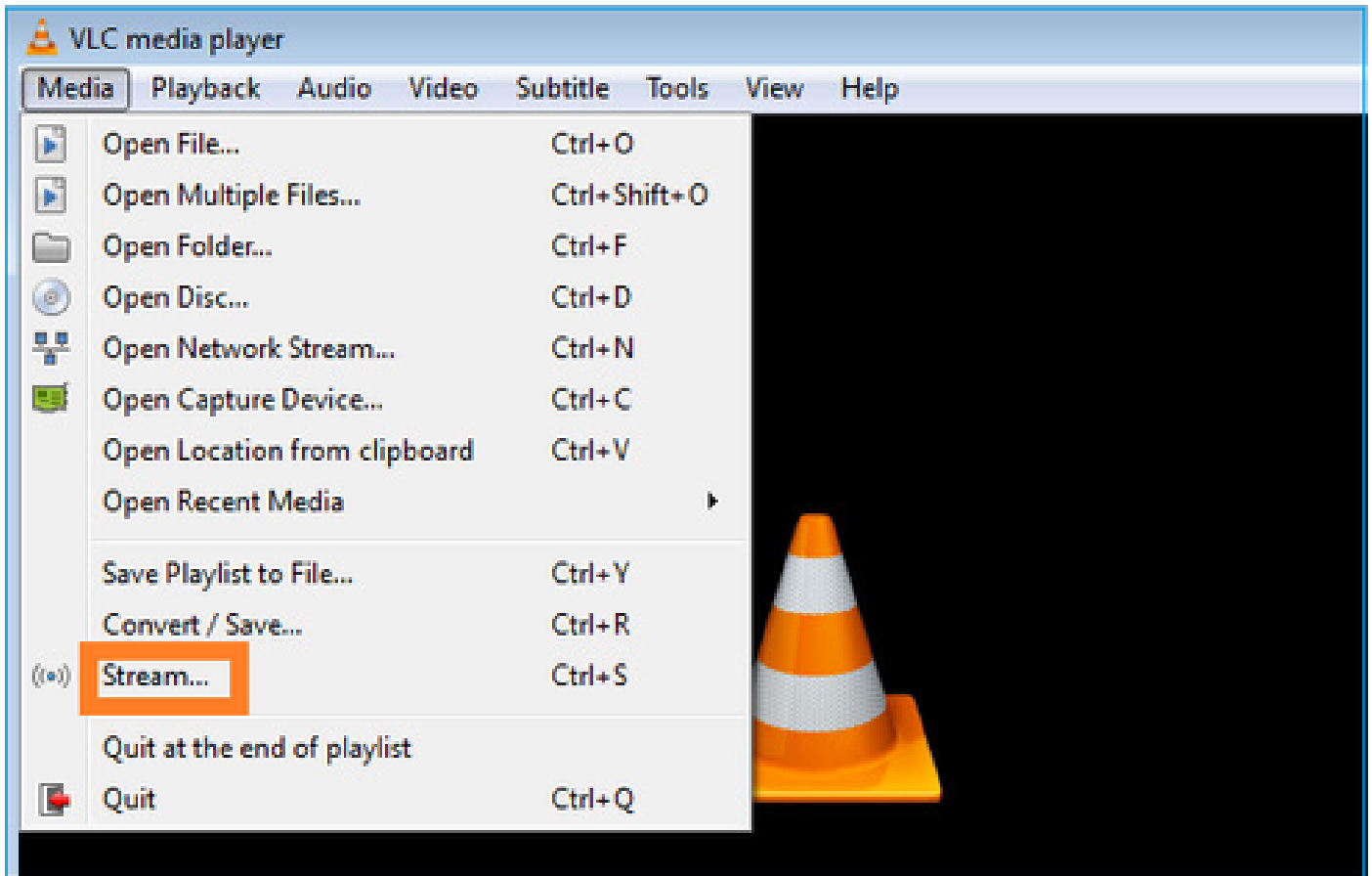
Forwarding: 0/0/0/0, Other: 0/0/0

Group: 239.255.255.250

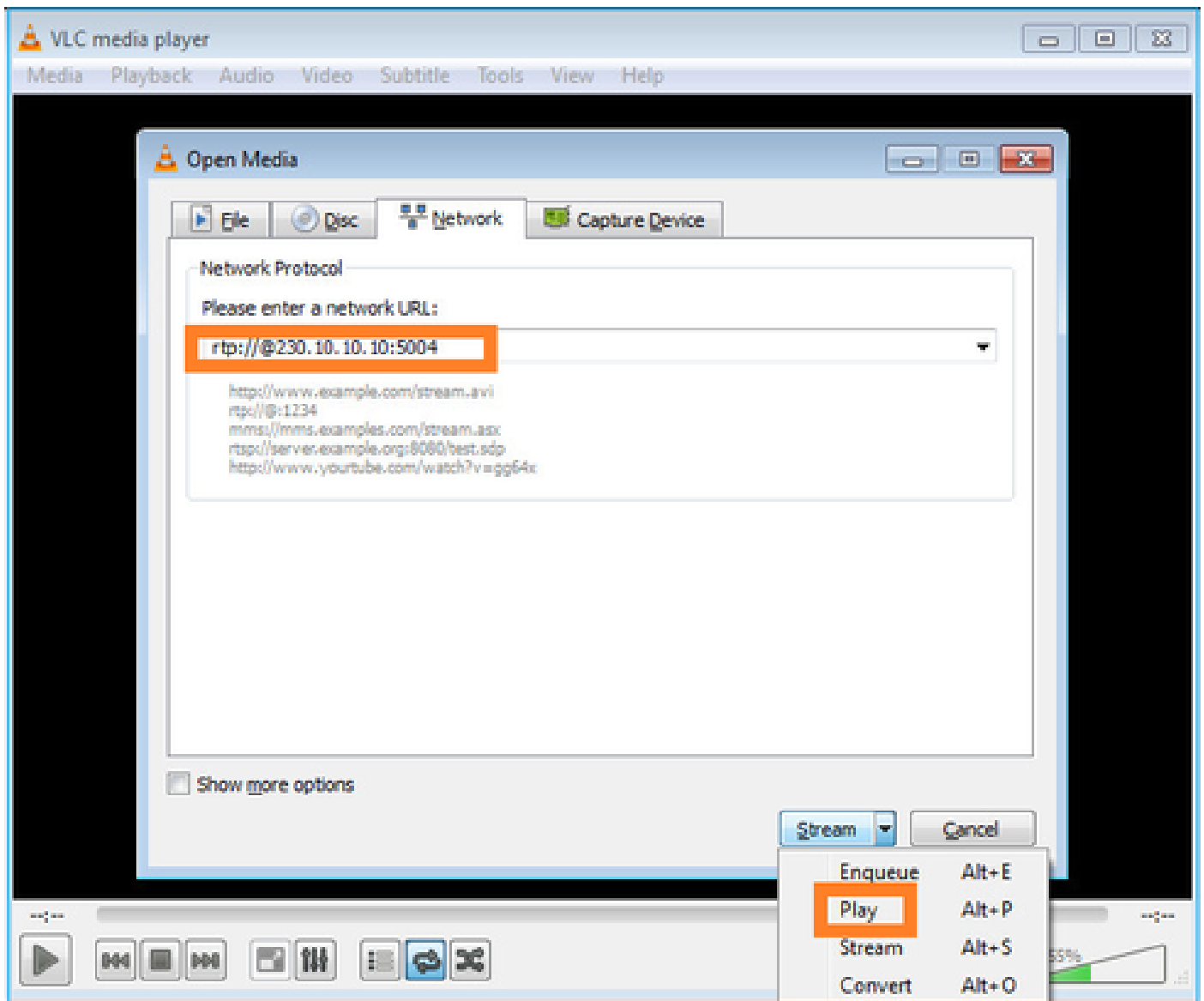
RP-tree:

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

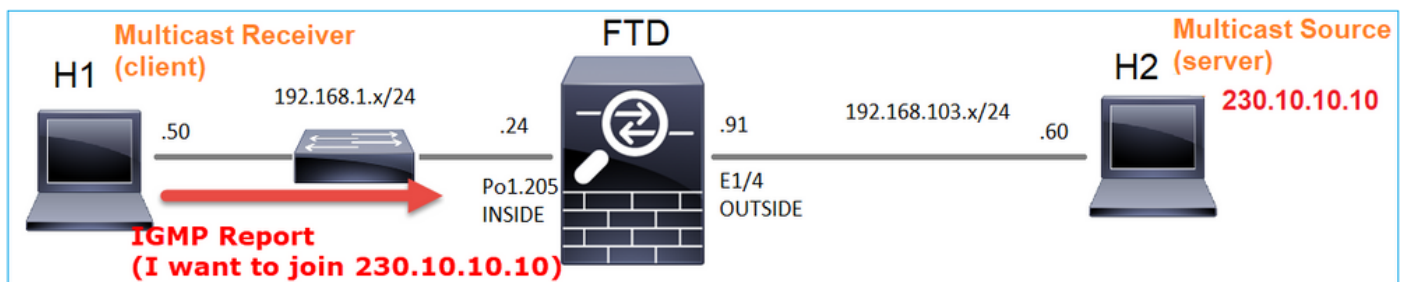
Configurez le récepteur de multidiffusion VLC :



Spécifiez l'adresse IP source de multidiffusion et sélectionnez Lire :



Dans le back-end, dès que vous sélectionnez Play, l'hôte annonce sa volonté de rejoindre le groupe de multidiffusion spécifique et envoie un message de rapport IGMP :



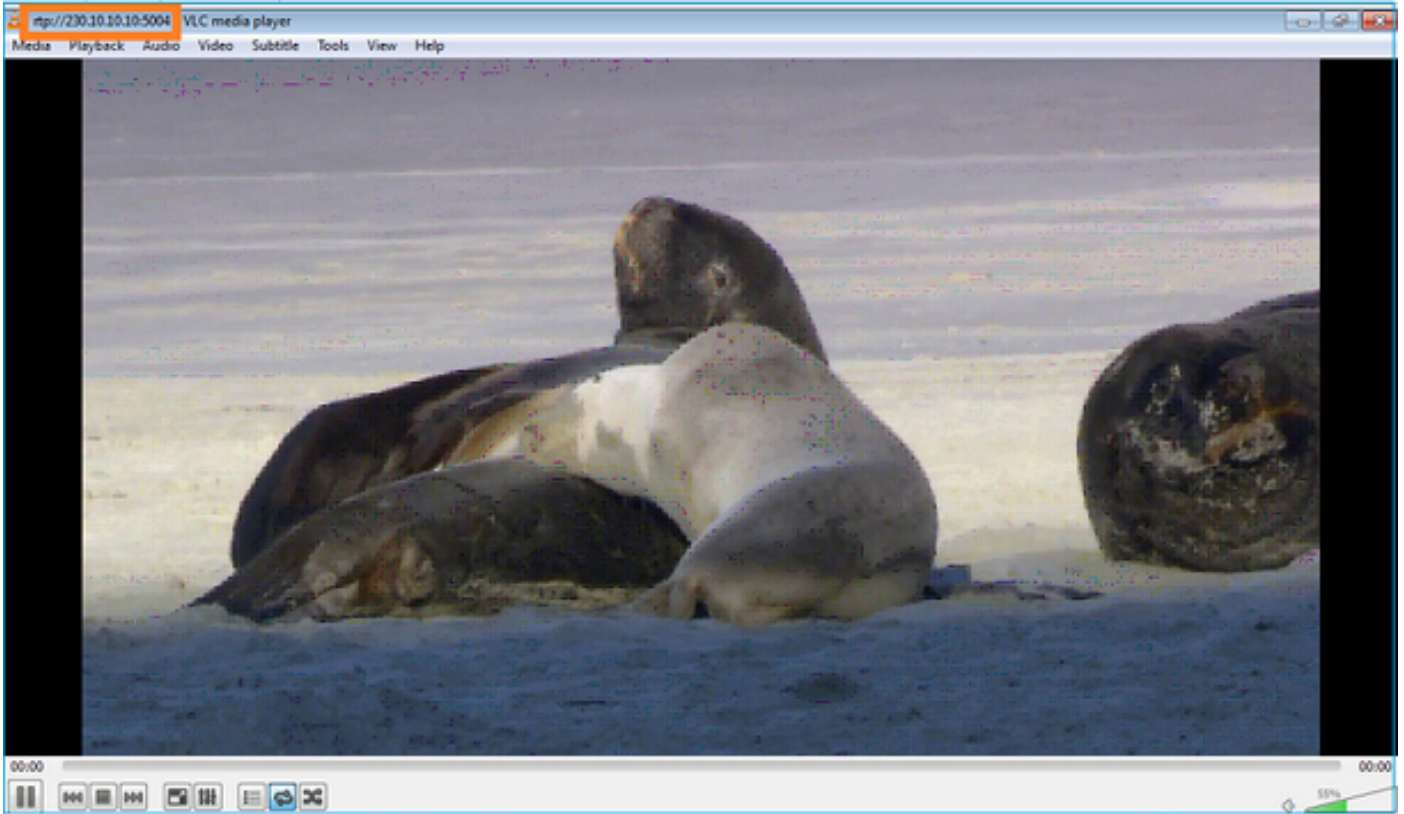
Si vous activez un débogage, vous pouvez voir les messages de rapport IGMP :

```
<#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
```

Le flux commence :



Vérification (scénario opérationnel)

```
<#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
```



La table mroute du pare-feu :

<#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

compteurs mfib :

<#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 Snooping

- La surveillance IGMP est un mécanisme utilisé sur les commutateurs afin d'empêcher l'inondation de multidiffusion.
- Le commutateur surveille les rapports IGMP pour déterminer où se trouvent les hôtes (récepteurs).
- Le commutateur surveille les requêtes IGMP pour déterminer où se trouvent les routeurs/pare-feu (expéditeurs).
- La surveillance IGMP est activée par défaut sur la plupart des commutateurs Cisco. Pour plus d'informations, consultez les guides de commutation associés. Voici l'exemple de sortie d'un commutateur Catalyst de couche 3 :

<#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	V1206: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

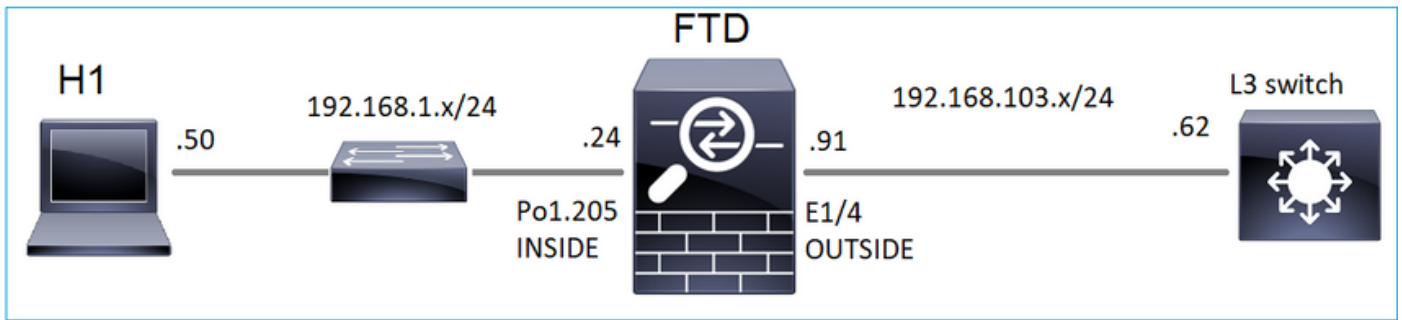
### Tâche 3 : groupe IGMP statique et groupe IGMP de jointure

#### Aperçu

	ip igmp static-group	ip igmp join-group
Appliqué sur l'interface FTD ?	Oui	Oui
Le FTD attire-t-il un flux de multidiffusion ?	Oui, une jointure PIM est envoyée vers le périphérique en amont. vers la source ou vers le point de rendez-vous (RP). Cela se produit uniquement si le FTD avec cette commande est le routeur désigné PIM (DR) sur cette interface.	Oui, une jointure PIM est envoyée vers le périphérique en amont. vers la source ou vers le point de rendez-vous (RP). Cela se produit uniquement si le FTD avec cette commande est le routeur désigné PIM (DR) sur cette interface.
Le FTD achemine-t-il le trafic de multidiffusion depuis l'interface ?	Oui	Oui
Le FTD consomme-t-il le trafic de multidiffusion et y répond-il ?	Non	Oui, le FTD envoie le flux de multidiffusion au processeur, l'utilise et répond à la source.
Impact sur le processeur	Minimal car le paquet n'est pas envoyé au processeur.	Peut affecter le CPU FTD puisque chaque paquet multicast qui appartient au groupe est envoyé au CPU FTD.

#### Exigence de la tâche

Considérez cette topologie :



Sur le pare-feu, activez les captures suivantes :

```
<#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. Utilisez la commande ping ICMP à partir du commutateur L3 pour envoyer le trafic de multidiffusion vers IP 230.11.11.11 et vérifiez la manière dont le pare-feu gère cette opération.
2. Activez la commande igmp static-group sur l'interface INSIDE du pare-feu et vérifiez comment le flux de multidiffusion (IP 230.11.11.11) est géré par le pare-feu.
3. Activez la commande igmp static-group sur l'interface INSIDE du pare-feu et vérifiez comment le flux de multidiffusion (IP 230.11.11.11) est géré par le pare-feu.

Solution

Le pare-feu n'a pas de mroutes pour l'adresse IP 230.11.11.11 :

```
<#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

L'outil ping ICMP constitue un moyen simple de tester la multidiffusion. Dans ce cas, lancez une requête ping à partir de R2 vers l'adresse IP de multidiffusion 230.11.11.11 :

<#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:

.....

Sur le pare-feu, un mroute est créé dynamiquement et l'OIL est vide :

<#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

La capture sur le pare-feu montre :

<#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
```

Le pare-feu crée des connexions pour chaque requête ping, mais supprime silencieusement les paquets :

```
<#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
```



Remarque : la capture d'abandon LINA ASP n'affiche pas les paquets abandonnés

---

L'indication principale des abandons de paquets de multidiffusion est :

```
<#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,
```

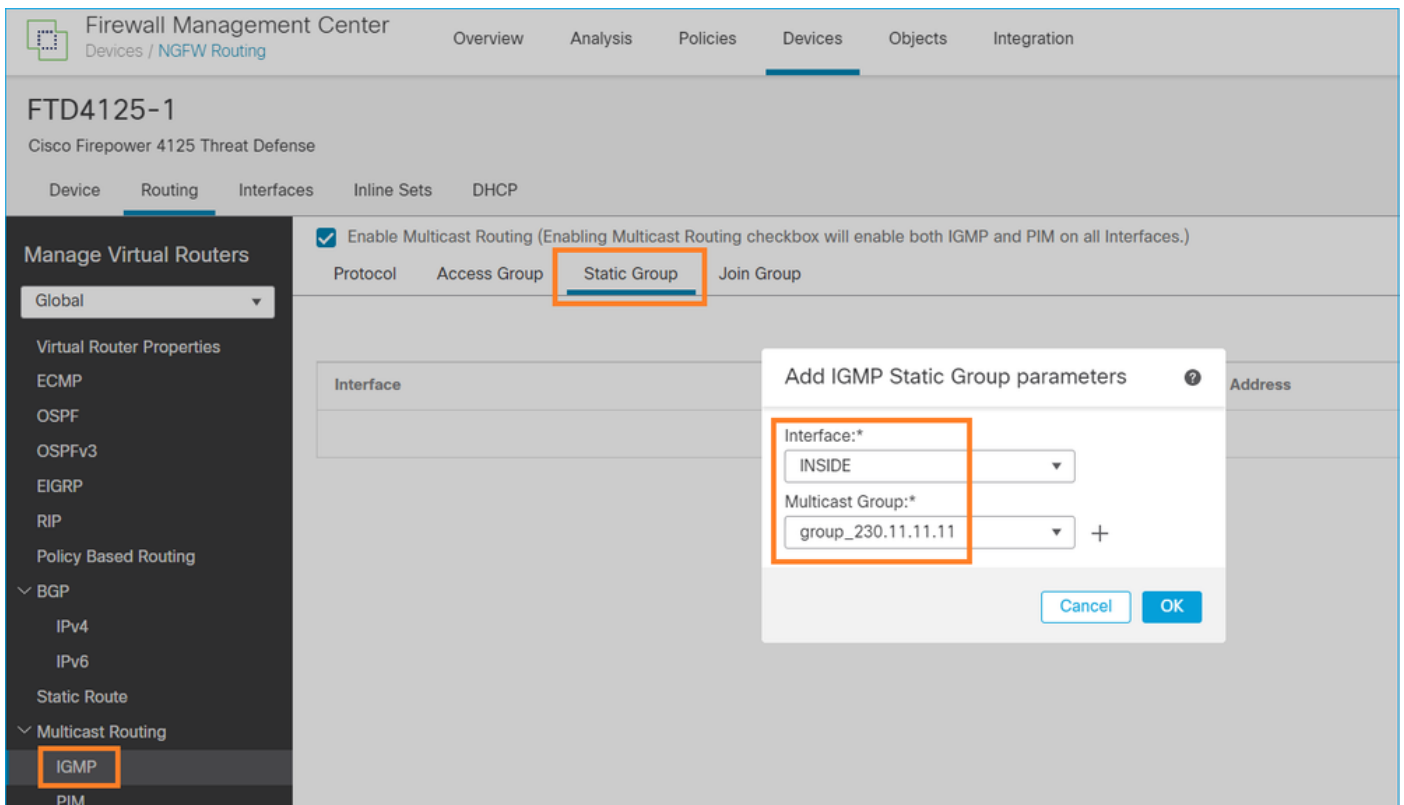
```
Other: 27/27/0
```

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

```
igmp static-group
```

Sur FMC, configurez un groupe IGMP statique :





Voici ce qui est déployé en arrière-plan :

```
<#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
```

La requête ping échoue, mais le trafic de multidiffusion ICMP est maintenant transféré via le pare-feu :

```
<#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
```

---

 Remarque : la trace du paquet indique une sortie incorrecte (l'interface d'entrée est identique à l'interface de sortie). Pour plus de détails, consultez l'ID de bogue Cisco [CSCvm89673](https://www.cisco.com/cisco/webbugtool/bugdetails.do?bugID=CSCvm89673).

---

```
<#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



Conseil : vous pouvez envoyer une requête ping avec timeout 0 à partir de l'hôte source et vérifier les compteurs mfib du pare-feu :

---

<#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 join-group

Sur FMC remote, configurez le groupe statique précédemment configuré et configurez un groupe de jonction IGMP :

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

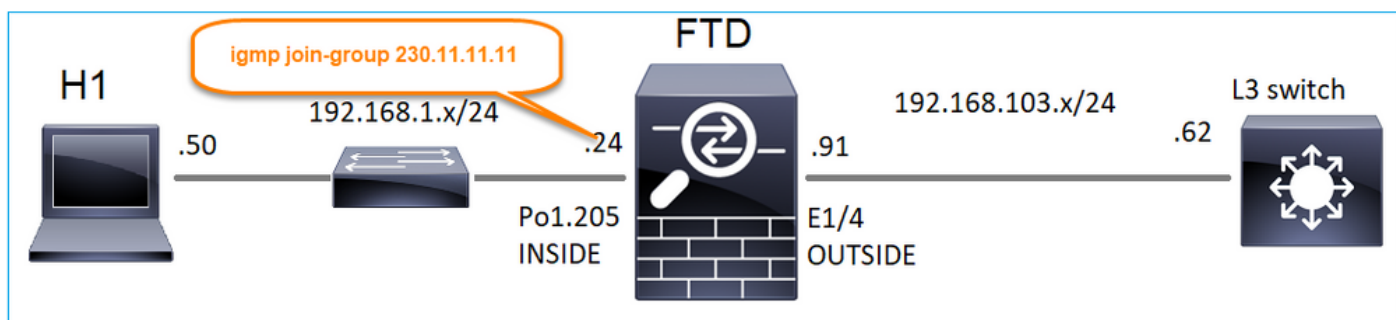
▼ Multicast Routing

**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



La configuration déployée :

```
<#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
```

Le groupe IGMP :

```
<#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
```

À partir de l'hôte source, essayez le premier test de multidiffusion ICMP vers 230.11.11.11 IP :

```
<#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
```

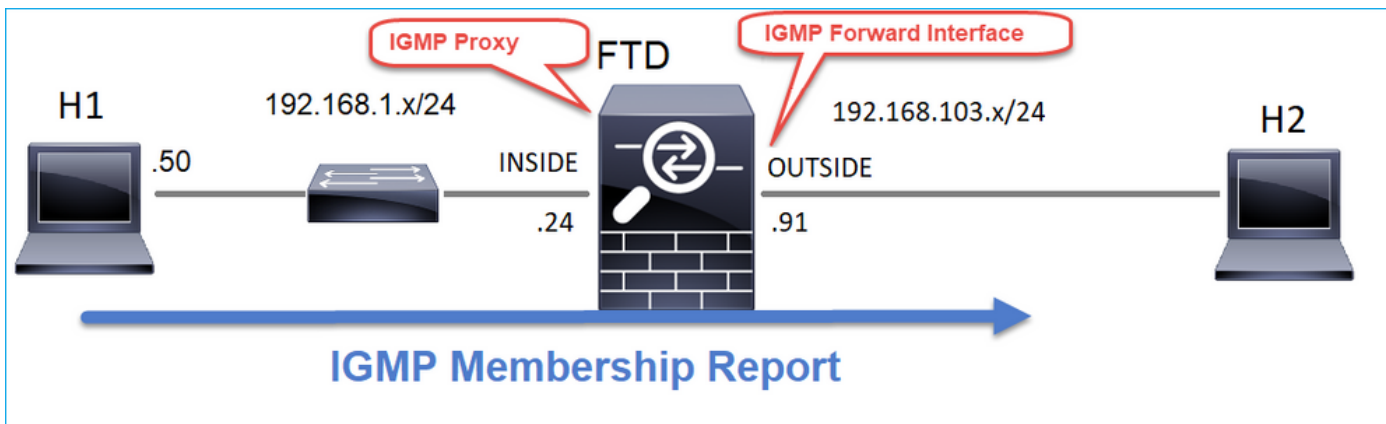


Remarque : si vous ne voyez pas toutes les réponses, vérifiez l'ID de bogue Cisco [CSCvm90069](https://tools.cisco.com/bugsearch/bug/CSCvm90069).

---

Tâche 4 : configuration du routage multidiffusion de stub IGMP





Configurez le routage de multidiffusion d'extrémité sur FTD de sorte que les messages IGMP Membership Report reçus sur l'interface INSIDE soient transférés vers l'interface OUTSIDE.

### Solution

The screenshot shows the Firewall Management Center (FMC) interface for device FTD4125-1. The 'Routing' tab is selected, and the 'Multicast Routing' section is expanded to show 'IGMP' configuration. The 'Enable Multicast Routing' checkbox is checked. The 'Protocol' tab is selected, and a table shows the configuration for the 'INSIDE' interface, where the 'Forward Interface' is set to 'OUTSIDE' and the 'Version' is '2'.

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

La configuration déployée :

```
<#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
```

## Vérification

Activer les captures sur FTD :

```
<#root>
```

```
firepower#
```

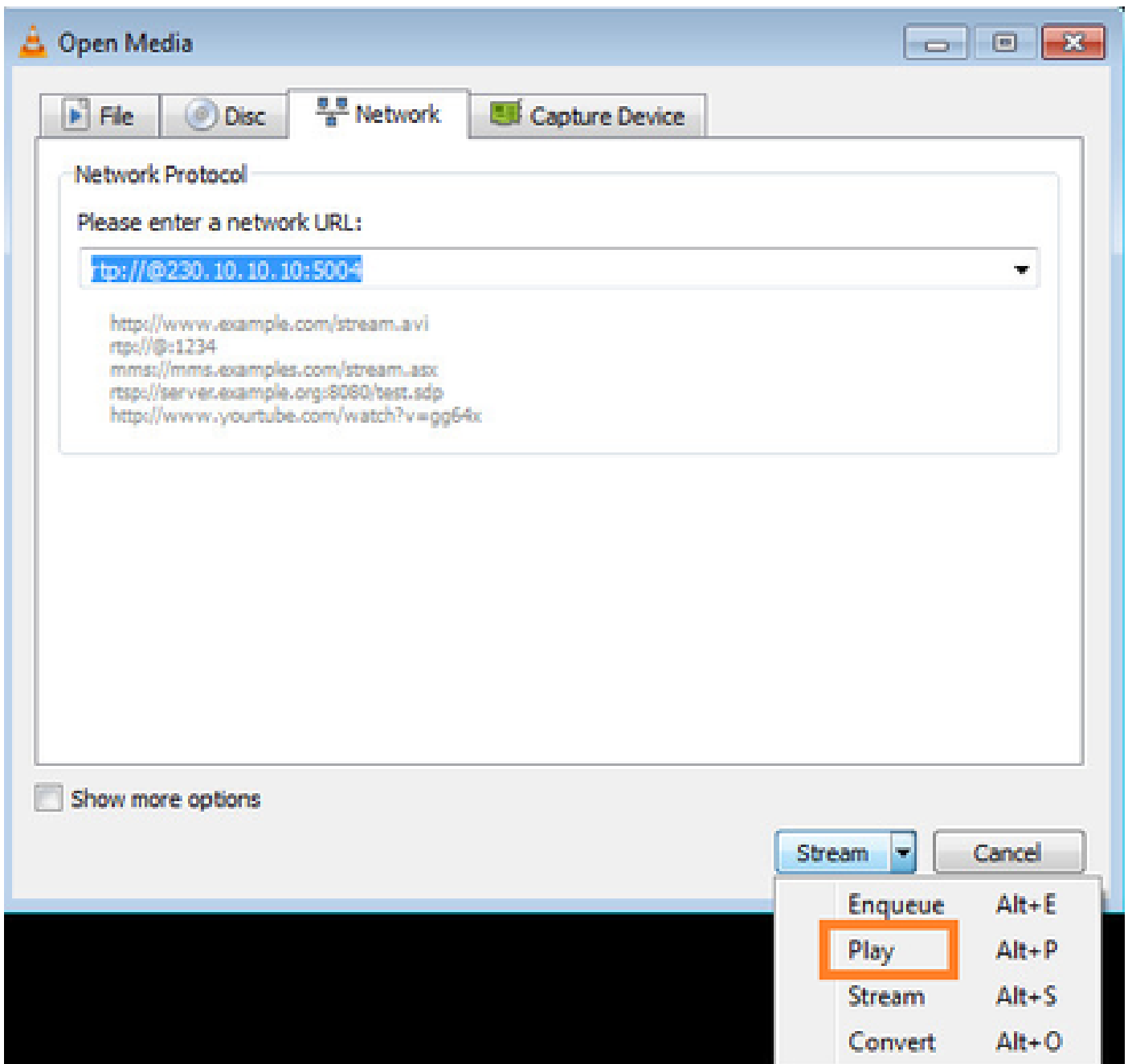
```
capture CAPI interface INSIDE trace match igmp any host 230.10.10.10
```

```
firepower#
```

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

## Vérification

Pour forcer un rapport d'adhésion IGMP, vous pouvez utiliser une application comme VLC :



Le FTD proxie les paquets IGMP :

```
<#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
```

Le FTD modifie l'adresse IP source :

```
<#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
```

Si vous vérifiez le pcap dans Wireshark, vous pouvez voir que le paquet est complètement régénéré par le pare-feu (les changements d'identification IP).

Une entrée de groupe est créée sur le FTD :

```
<#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
-----------------	--------	----------	----------	--------------

Le pare-feu FTD crée 2 connexions de plan de contrôle :

```
<#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
```

Trace du premier paquet :

```
<#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

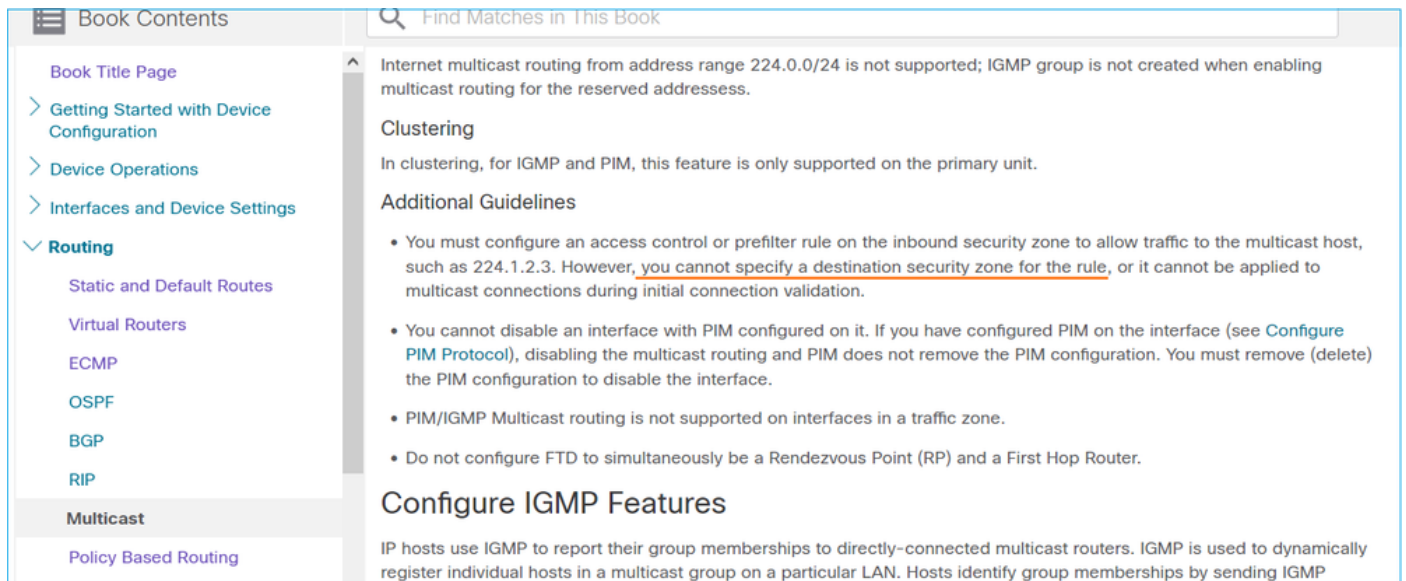
Config:

Additional Information:





Ceci est également documenté dans le guide de l'utilisateur FMC :



The screenshot shows a web-based user guide interface. On the left is a navigation menu with categories like 'Getting Started with Device Configuration', 'Device Operations', 'Interfaces and Device Settings', and 'Routing'. Under 'Routing', 'Multicast' is selected. The main content area has a search bar at the top and a search result for 'Configure IGMP Features'. The text in the main area includes: 'Internet multicast routing from address range 224.0.0/24 is not supported; IGMP group is not created when enabling multicast routing for the reserved addressess.', 'Clustering' section stating 'In clustering, for IGMP and PIM, this feature is only supported on the primary unit.', 'Additional Guidelines' with four bullet points: 1. 'You must configure an access control or prefilter rule on the inbound security zone to allow traffic to the multicast host, such as 224.1.2.3. However, you cannot specify a destination security zone for the rule, or it cannot be applied to multicast connections during initial connection validation.' 2. 'You cannot disable an interface with PIM configured on it. If you have configured PIM on the interface (see Configure PIM Protocol), disabling the multicast routing and PIM does not remove the PIM configuration. You must remove (delete) the PIM configuration to disable the interface.' 3. 'PIM/IGMP Multicast routing is not supported on interfaces in a traffic zone.' 4. 'Do not configure FTD to simultaneously be a Rendezvous Point (RP) and a First Hop Router.' Below this is the heading 'Configure IGMP Features' and a paragraph: 'IP hosts use IGMP to report their group memberships to directly-connected multicast routers. IGMP is used to dynamically register individual hosts in a multicast group on a particular LAN. Hosts identify group memberships by sending IGMP'.

## Les rapports IGMP sont refusés par le pare-feu lorsque la limite d'interface IGMP est dépassée

Par défaut, le pare-feu autorise un maximum de 500 jointures actives (rapports) sur une interface. Si ce seuil est dépassé, le pare-feu ignore les rapports IGMP entrants supplémentaires des récepteurs de multidiffusion.

Pour vérifier la limite IGMP et les jointures actives, exécutez la commande `show igmp interface name if`:

```
<#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)
```

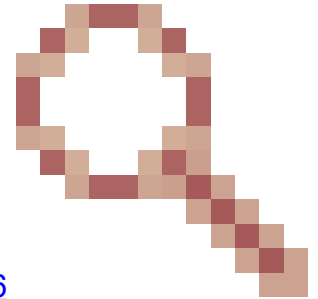
La commande de débogage `IGMP debug igmp` affiche ce résultat :

```
<#root>
```

```
asa#
```

```
debug igmp
```

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



Les versions logicielles avec le correctif de l'ID de bogue Cisco [CSCvw60976](#) permettent aux utilisateurs de configurer jusqu'à 5 000 groupes par interface.

### Le pare-feu ignore les rapports IGMP pour la plage d'adresses 232.x.x.x/8

La plage d'adresses 232.x.x.x/8 doit être utilisée avec le protocole SSM (Source Specific Multicast). Le pare-feu ne prend pas en charge la fonctionnalité PIM Source Specific Multicast (SSM) et la configuration associée.

La commande de débogage IGMP `debug igmp` affiche ce résultat :

```
<#root>
```

```
asa#
```

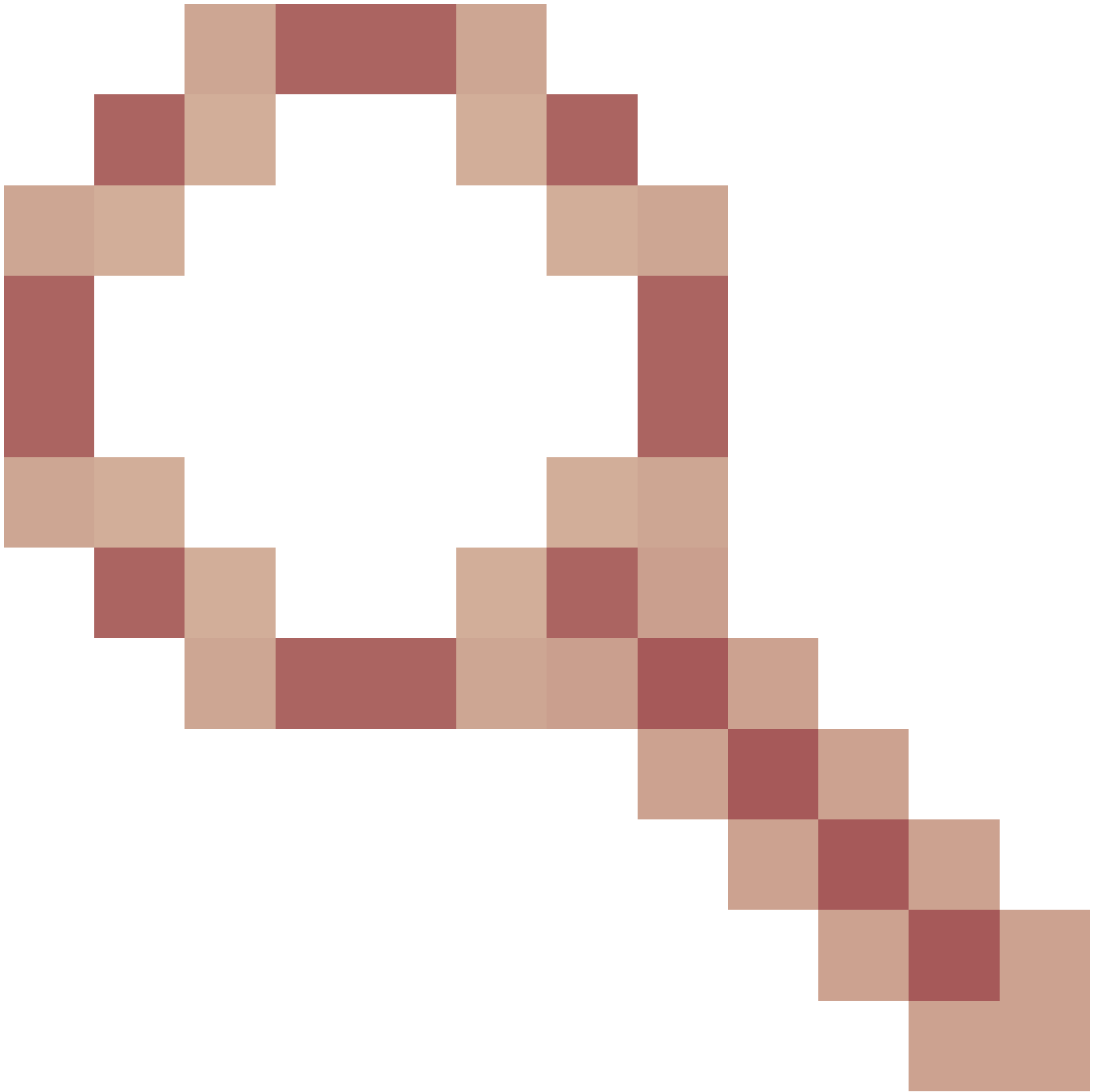
```
debug igmp
```

```
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
```

ID de bogue Cisco [CSCsr53916](#)



suit l'amélioration pour prendre en charge la gamme SSM.

## Informations connexes

- [Routage multidiffusion pour Firepower Threat Defense](#)
- [Dépannage de Firepower Threat Defense et ASA Multicast PIM](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.