Solución de problemas de Firepower Threat Defence IGMP y aspectos básicos de multidifusión

Contenido

Introducción

Este documento describe los aspectos básicos de la multidifusión y cómo Firepower Threat Defence (FTD) implementa el protocolo de administración de grupos de Internet (IGMP).

Prerequisites

Requirements

Conocimientos básicos sobre IP Routing.

Componentes Utilizados

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

El contenido de este artículo también es aplicable al software Adaptive Security Appliance (ASA).

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Firepower 4125 Threat Defense Versión 7.1.0.
- Firepower Management Center (FMC) versión 7.1.0.
- ASA versión 9.19.1.

Antecedentes

Definiciones

- Unidifusión = de un único host a otro (uno a uno).
- Transmisión = desde un único host a TODOS los hosts posibles (uno a todos).
- **Multidifusión = desde un host de un grupo de hosts a un grupo de hosts (uno a varios o varios a varios).**
- Anycast = de un host al host más cercano de un grupo (uno a uno de varios).

Conceptos básicos

- La multidifusión RFC 988 fue escrita en 1986 por Steve Deering.
- La multidifusión IPv4 utiliza el intervalo 224.0.0.0/4 (primeros 4 bits 1110) - 224.0.0.0 - 239.255.255.255.
- Para IPv4, la dirección MAC de L2 deriva de la IP de multidifusión de L3: 01005e (24 bits) + 25º bit siempre 0 + 23 bits inferiores de la dirección IPv4 de multidifusión.
- La multidifusión IPv6 utiliza el rango FF00::/8 y es más flexible que la multidifusión IPv4, ya que puede integrar IP de punto de encuentro (RP).
- Para IPv6, la dirección MAC de L2 deriva de la multidifusión de L3: 3333 + 32 bits inferiores de la dirección IPv6 de multidifusión.
- Ventajas de la multidifusión: eficacia gracias a la reducción de la carga en el origen. Rendimiento, ya que evita la duplicación o inundación del tráfico.
- Desventajas de la multidifusión: transporte no fiable (basado en UDP), sin prevención de congestión y entrega fuera de secuencia.
- La multidifusión no se admite en la Internet pública, ya que requiere todos los dispositivos de la ruta para activarla. Normalmente, se utiliza cuando todos los dispositivos están bajo una autoridad administrativa común.
- Aplicaciones de multidifusión típicas: transmisión de vídeo interna y videoconferencia.

Multidifusión frente a unidifusión replicada

En la unidifusión replicada, el origen crea varias copias del mismo paquete de unidifusión (réplicas) y las envía a varios hosts de destino. La multidifusión traslada la carga del host de origen a la red, mientras que en la unidifusión replicada todo el trabajo se realiza en el host de origen.

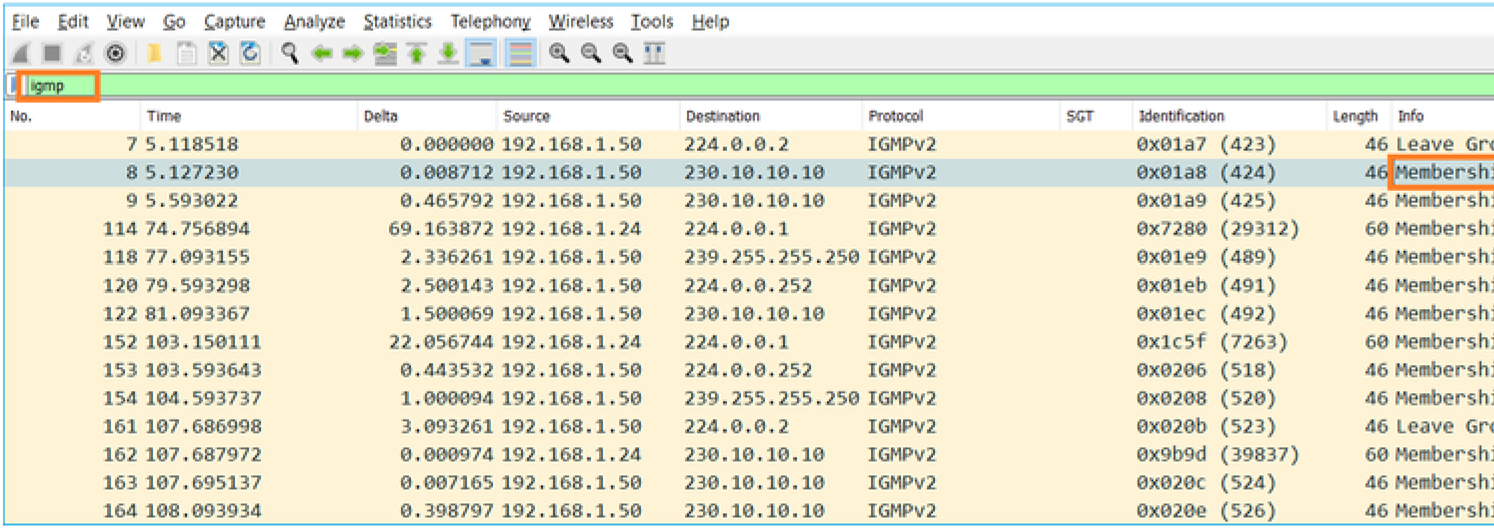
Configurar

Conceptos básicos de IGMP

- IGMP es el "idioma" hablado entre los receptores de multidifusión y el dispositivo L3 local (normalmente un router).
- IGMP es un protocolo de capa 3 (como ICMP) y utiliza el **protocolo IP número 2.**
- Actualmente hay 3 versiones de IGMP. La versión predeterminada de IGMP en el firewall es la versión 2. **Actualmente sólo se admiten las versiones 1 y 2.**
- Entre IGMPv1 e IGMPv2 las diferencias principales son:
    - IGMPv1 no tiene ningún mensaje Dejar grupo.
    - IGMPv1 no tiene ninguna consulta específica de grupo (utilizada por el firewall cuando un host

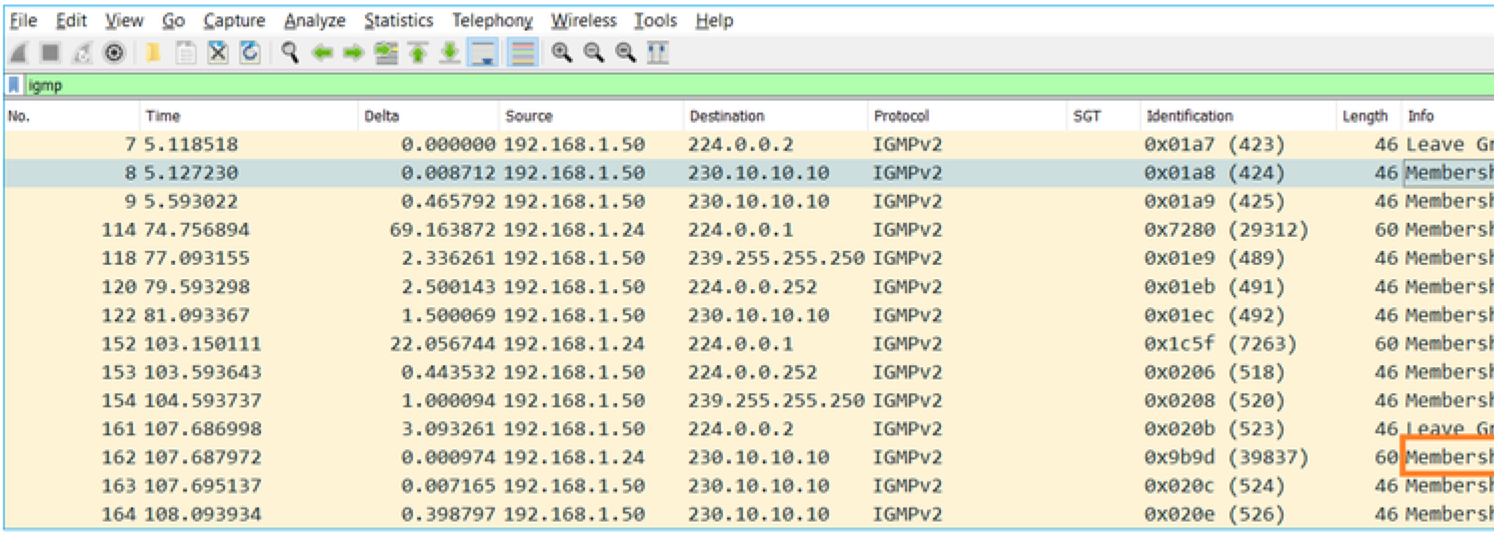
abandona un grupo de multidifusión).
  - IGMPv1 no tiene proceso de elección de consultor.

- **Actualmente, IGMPv3 no es compatible** en ASA/FTD, pero como referencia, la diferencia importante entre IGMPv2 e IGMPv3 es la inclusión de una consulta específica de grupo y origen en IGMPv3, que se utiliza en la multidifusión específica de la fuente (SSM).
- Consultas IGMPv1/IGMPv2/IGMPv3 = **224.0.0.1**
  IGMPv2 Leave = **224.0.0.2**
  Informe de afiliación a IGMPv3 = **224.0.0.22**
- Si un host desea unirse, puede enviar un mensaje de **informe de afiliación IGMP no solicitado**:



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 Gro
8	5.127230	0.008712	192.168.1.50	230.10.10.10	IGMPv2		0x01a8 (424)	46	Membershi
9	5.593022	0.465792	192.168.1.50	230.10.10.10	IGMPv2		0x01a9 (425)	46	Membershi
114	74.756894	69.163872	192.168.1.24	224.0.0.1	IGMPv2		0x7280 (29312)	60	Membershi
118	77.093155	2.336261	192.168.1.50	239.255.255.250	IGMPv2		0x01e9 (489)	46	Membershi
120	79.593298	2.500143	192.168.1.50	224.0.0.252	IGMPv2		0x01eb (491)	46	Membershi
122	81.093367	1.500069	192.168.1.50	230.10.10.10	IGMPv2		0x01ec (492)	46	Membershi
152	103.150111	22.056744	192.168.1.24	224.0.0.1	IGMPv2		0x1c5f (7263)	60	Membershi
153	103.593643	0.443532	192.168.1.50	224.0.0.252	IGMPv2		0x0206 (518)	46	Membershi
154	104.593737	1.000094	192.168.1.50	239.255.255.250	IGMPv2		0x0208 (520)	46	Membershi
161	107.686998	3.093261	192.168.1.50	224.0.0.2	IGMPv2		0x020b (523)	46	Leave Gro
162	107.687972	0.000974	192.168.1.24	230.10.10.10	IGMPv2		0x9b9d (39837)	60	Membershi
163	107.695137	0.007165	192.168.1.50	230.10.10.10	IGMPv2		0x020c (524)	46	Membershi
164	108.093934	0.398797	192.168.1.50	230.10.10.10	IGMPv2		0x020e (526)	46	Membershi

- Desde el punto de vista del firewall, hay **2 tipos de consultas IGMP: consultas generales** y **consultas específicas de grupo**
- Cuando el firewall recibe un mensaje de IGMP Leave Group , debe verificar si hay otros miembros de ese grupo en la subred. Por esa razón, el firewall envía una **consulta específica de grupo:**



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 Gr
8	5.127230	0.008712	192.168.1.50	230.10.10.10	IGMPv2		0x01a8 (424)	46	Membersh
9	5.593022	0.465792	192.168.1.50	230.10.10.10	IGMPv2		0x01a9 (425)	46	Membersh
114	74.756894	69.163872	192.168.1.24	224.0.0.1	IGMPv2		0x7280 (29312)	60	Membersh
118	77.093155	2.336261	192.168.1.50	239.255.255.250	IGMPv2		0x01e9 (489)	46	Membersh
120	79.593298	2.500143	192.168.1.50	224.0.0.252	IGMPv2		0x01eb (491)	46	Membersh
122	81.093367	1.500069	192.168.1.50	230.10.10.10	IGMPv2		0x01ec (492)	46	Membersh
152	103.150111	22.056744	192.168.1.24	224.0.0.1	IGMPv2		0x1c5f (7263)	60	Membersh
153	103.593643	0.443532	192.168.1.50	224.0.0.252	IGMPv2		0x0206 (518)	46	Membersh
154	104.593737	1.000094	192.168.1.50	239.255.255.250	IGMPv2		0x0208 (520)	46	Membersh
161	107.686998	3.093261	192.168.1.50	224.0.0.2	IGMPv2		0x020b (523)	46	Leave Gr
162	107.687972	0.000974	192.168.1.24	230.10.10.10	IGMPv2		0x9b9d (39837)	60	Membersh
163	107.695137	0.007165	192.168.1.50	230.10.10.10	IGMPv2		0x020c (524)	46	Membersh
164	108.093934	0.398797	192.168.1.50	230.10.10.10	IGMPv2		0x020e (526)	46	Membersh

- En las subredes donde hay varios routers/firewalls, se elige un **solicitante** (un dispositivo que envía todas las consultas IGMP):

<#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
```

- En FTD, similar a un ASA clásico, puede habilitar **debug igmp** para ver los mensajes relacionados con IGMP:

<#root>

```
firepower#
```

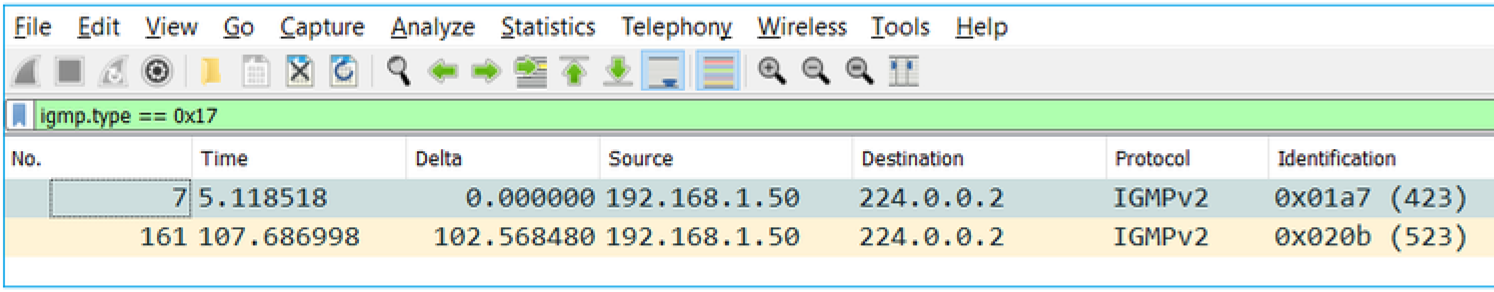
```
debug igmp
```

```
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
```

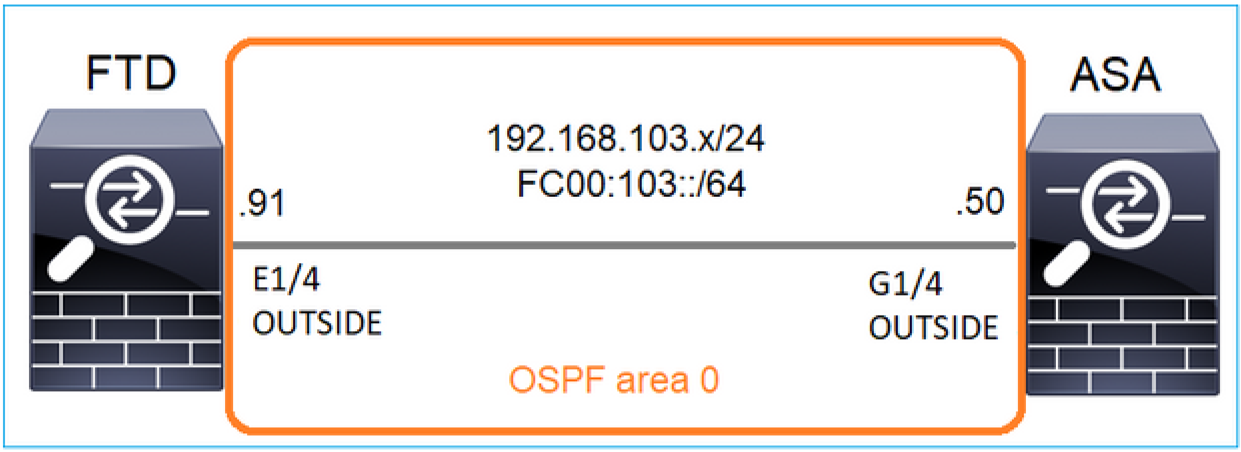
- Normalmente, un host abandona un grupo de multidifusión con un mensaje **Abandonar grupo** (IGMPv2).


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

igmp.type == 0x17

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

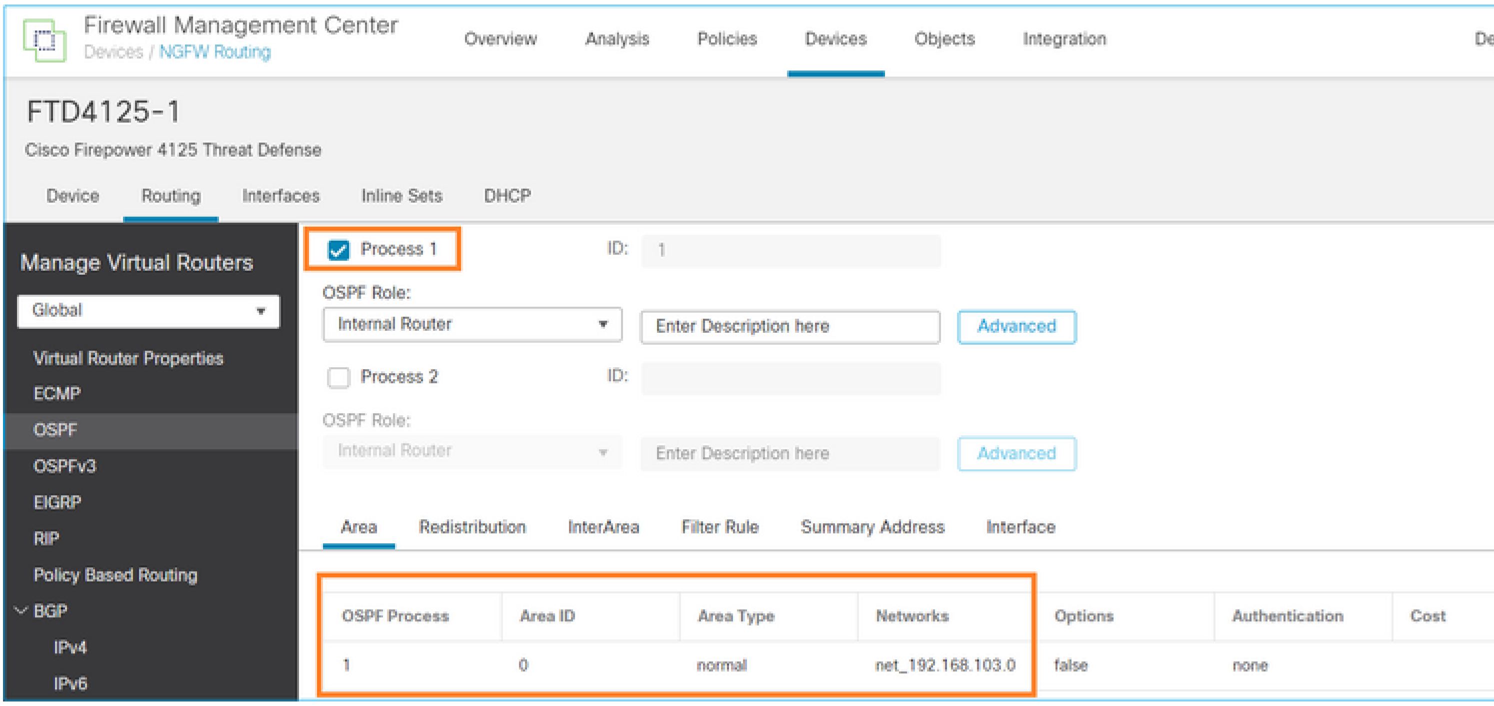
Tarea 1: Tráfico de multidifusión del plano de control



Configure un OSPFv2 y un OSPFv3 entre el FTD y el ASA. Compruebe cómo los 2 dispositivos manejan el tráfico Multicast L2 y L3 generado por OSPF.

Solución

configuración OSPFv2



FTD4125-1

Cisco Firepower 4125 Threat Defense

☑ Process 1 ID: 1

OSPF Role: Internal Router

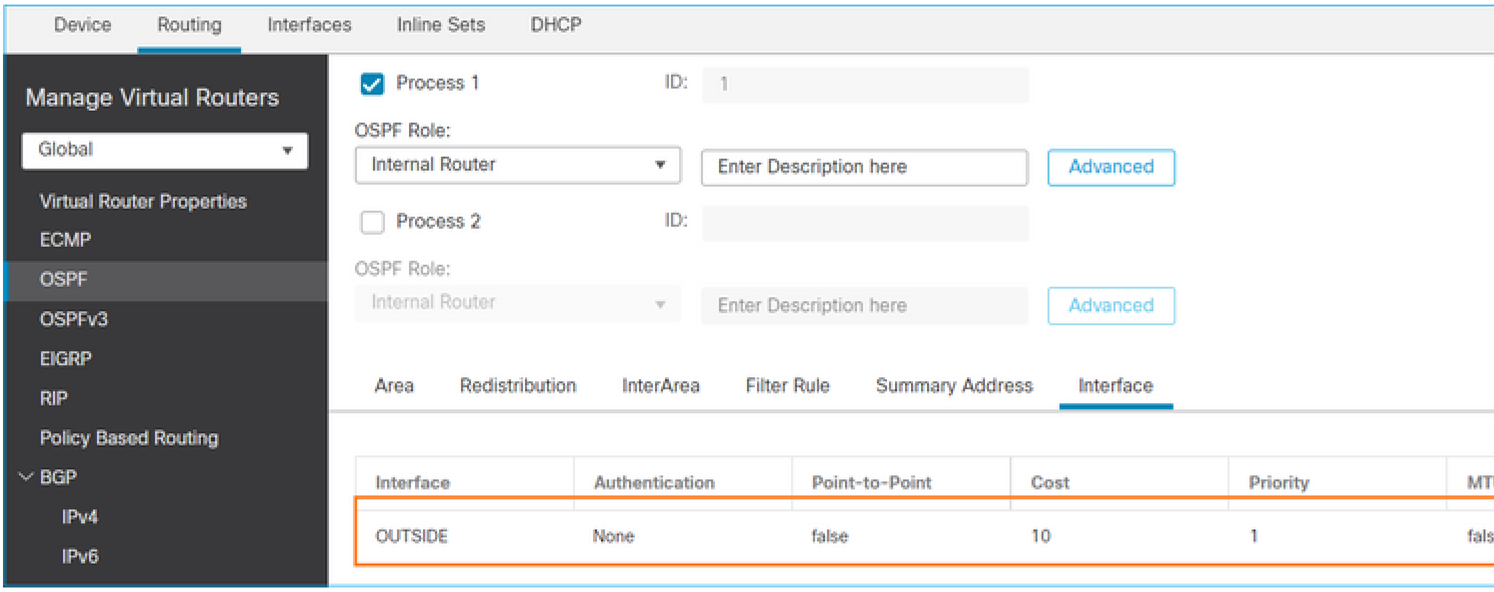
Enter Description here

☐ Process 2 ID:

OSPF Role: Internal Router

Enter Description here

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



☑ Process 1 ID: 1

OSPF Role: Internal Router

Enter Description here

□ Process 2 ID:

OSPF Role: Internal Router

Enter Description here

Interface	Authentication	Point-to-Point	Cost	Priority	MT
OUTSIDE	None	false	10	1	fals

De manera similar, para OSPFv3

Configuración en CLI de 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 configuración crea estas entradas en las tablas de permisos de ruta de seguridad acelerada (ASP) de FTD para que no se bloquee el tráfico de multidifusión de entrada:

```
<#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
```

Para 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
...
```

Las adyacencias OSPFv2 y OSPFv3 son 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
```

Estas son las sesiones OSPF multicast que terminaron en la caja:

<#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
```

Como prueba, active la captura para IPv4 y borre las conexiones al dispositivo:

<#root>

```
firepower#
```

```
capture CAP interface OUTSIDE trace

firepower#

clear conn all

12 connection(s) deleted.
firepower#

clear capture CAP

firepower# !
```

Advertencia: ¡Esto provoca una interrupción! El ejemplo sólo se muestra con fines de demostración.

Los paquetes OSPF capturados:

<#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]
```

El firewall administra el paquete de multidifusión OSPFv2 de la siguiente manera:

<#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
```

Así es como el firewall maneja el paquete de multidifusión OSPFv3:

<#root>

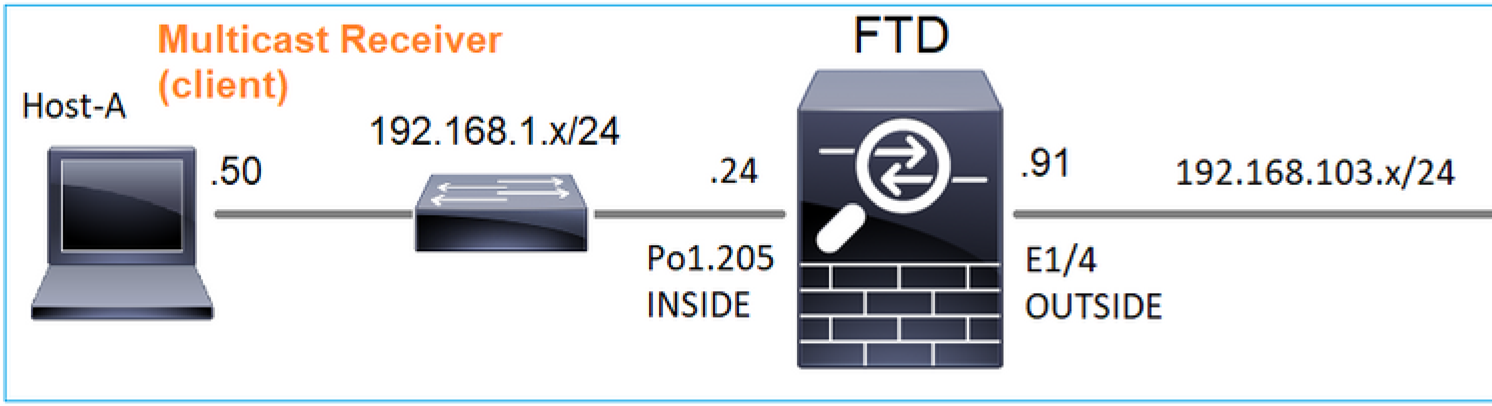
```
firepower#

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
```

Tarea 2: Configuración de la multidifusión básica

Topología



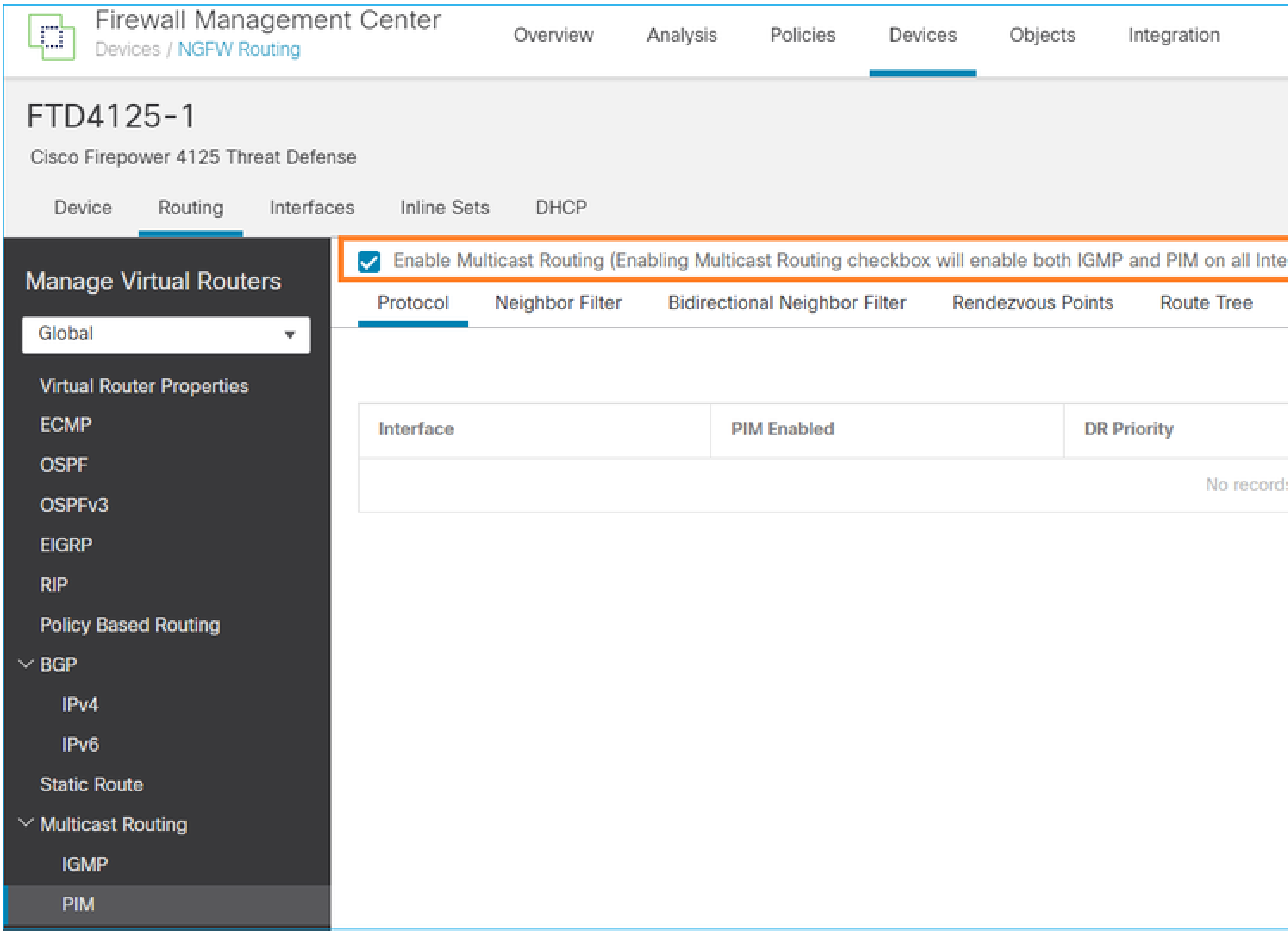
Requisito

Configure el firewall de modo que el tráfico multicast del servidor se transmita al cliente multicast en IP 230.10.10.10

Solución

Desde el punto de vista del firewall, la configuración mínima es habilitar el ruteo multicast globalmente. Esto habilita IGMP y PIM en segundo plano en todas las interfaces de firewall.

En la IU de FMC:


Firewall Management Center
Devices / NGFW Routing

FTD4125-1
Cisco Firepower 4125 Threat Defense

☑ Enable Multicast Routing (Enabling Multicast Routing checkbox will enable both IGMP and PIM on all Inte

Interface	PIM Enabled	DR Priority
		No record

En la CLI del firewall, esta es la configuración introducida:

<#root>

```
firepower#
```

show run multicast-routing

multicast-routing

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

Verificación de 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
```

Verificación de PIM

<#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
```

Verificación de 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
```

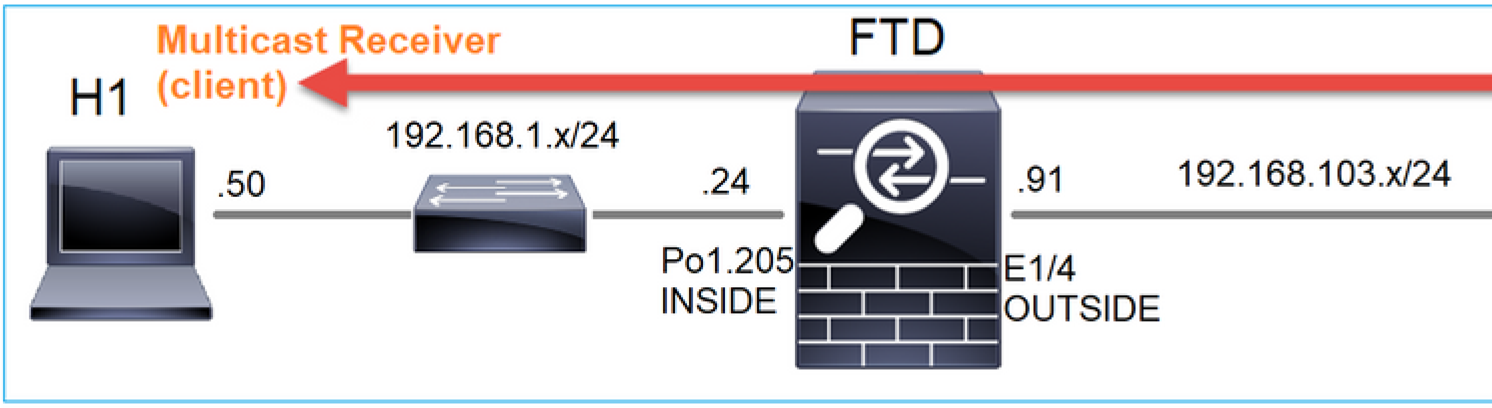
Forwarding: 0/0/0/0

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

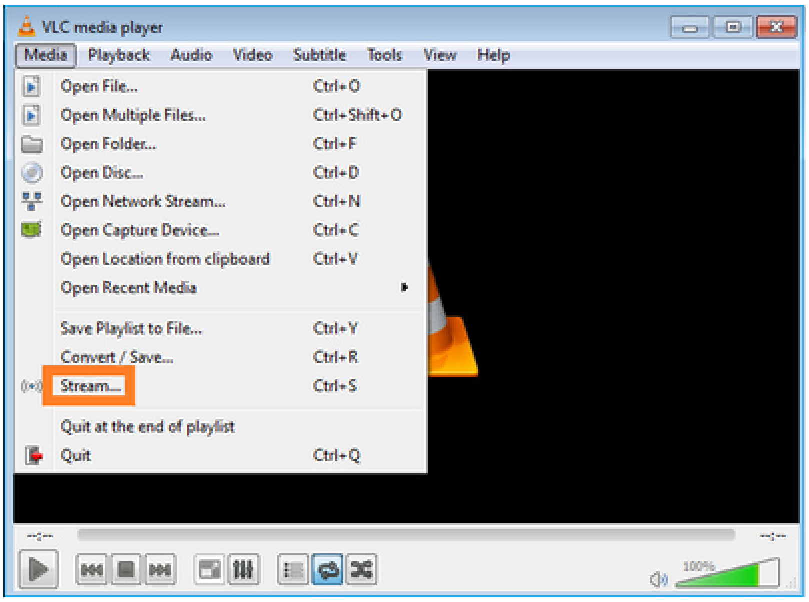
```
(*,224.0.1.40) Flags: S K
   Forwarding: 0/0/0/0,

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
```

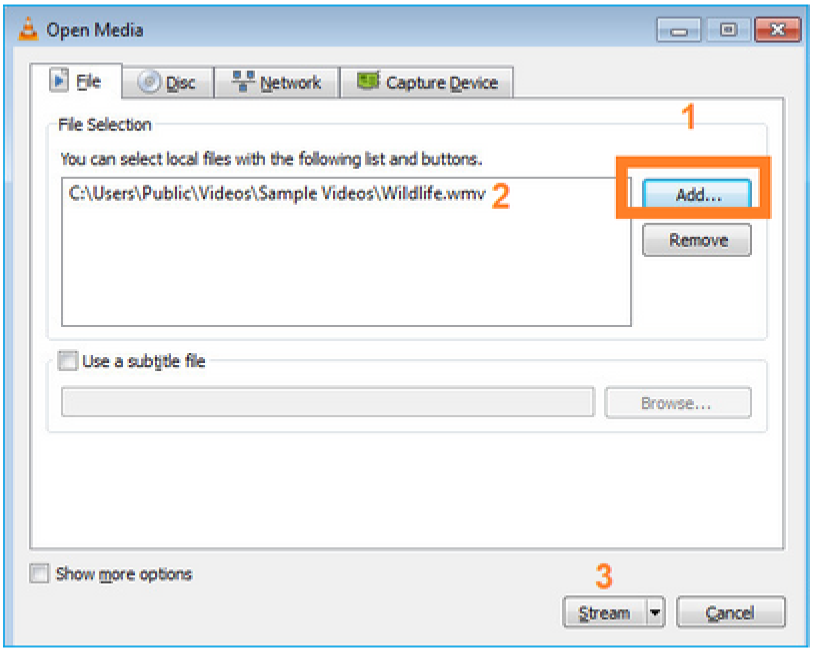
Tráfico de multidifusión a través del firewall

En este caso, la aplicación de reproductor multimedia VLC se utiliza como un servidor multicast y un cliente para probar el tráfico multicast:



Configuración del servidor de multidifusión VLC:





File Selection

You can select local files with the following list and buttons.

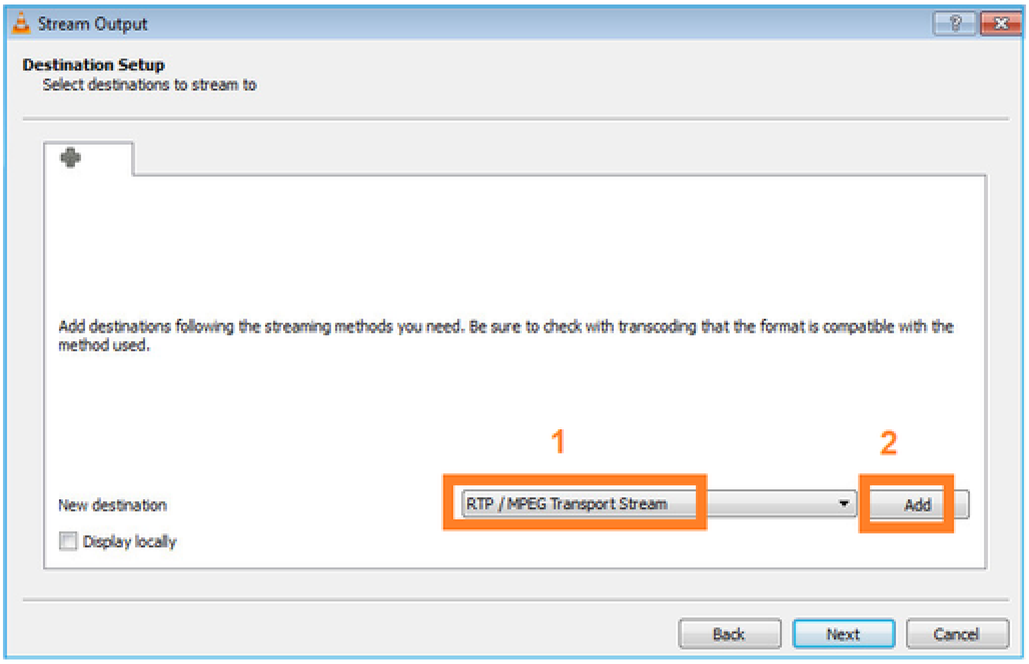
C:\Users\Public\Videos\Sample Videos\Wildlife.wmv 2

□ Use a subtitle file

□ Show more options

En la siguiente pantalla, seleccione **Next** (**Siguiente).**

Seleccione el formato:



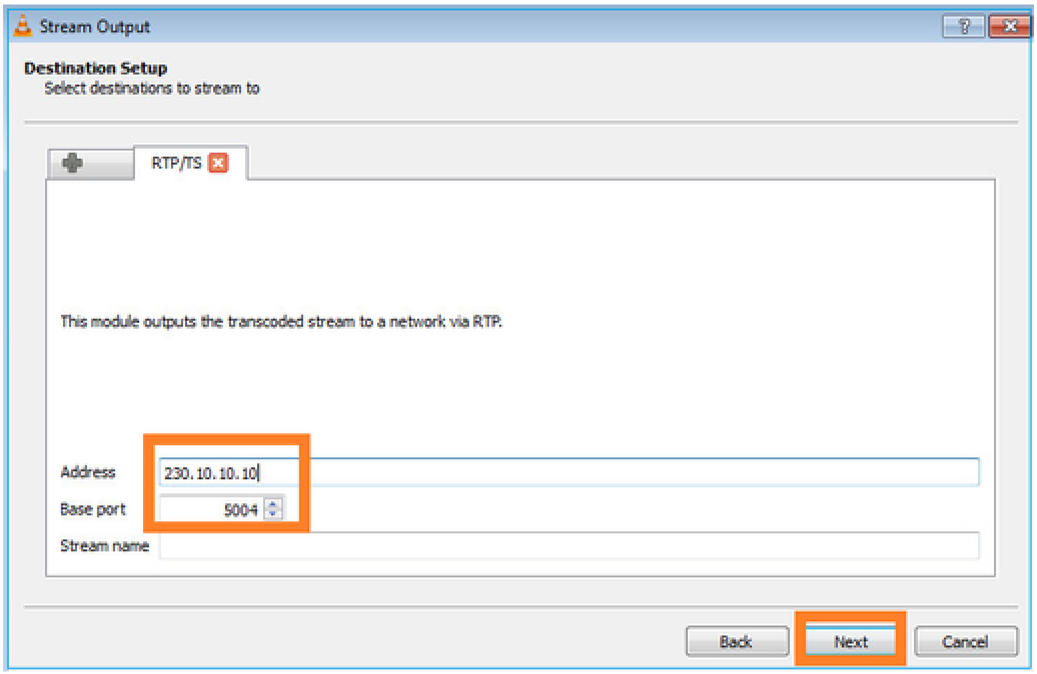
Destination Setup
Select destinations to stream to

Add destinations following the streaming methods you need. Be sure to check with transcoding that the format is compatible with the method used.

New destination: RTP / MPEG Transport Stream

□ Display locally

Especifique la IP y el puerto de multidifusión:



Stream Output

Destination Setup

Select destinations to stream to

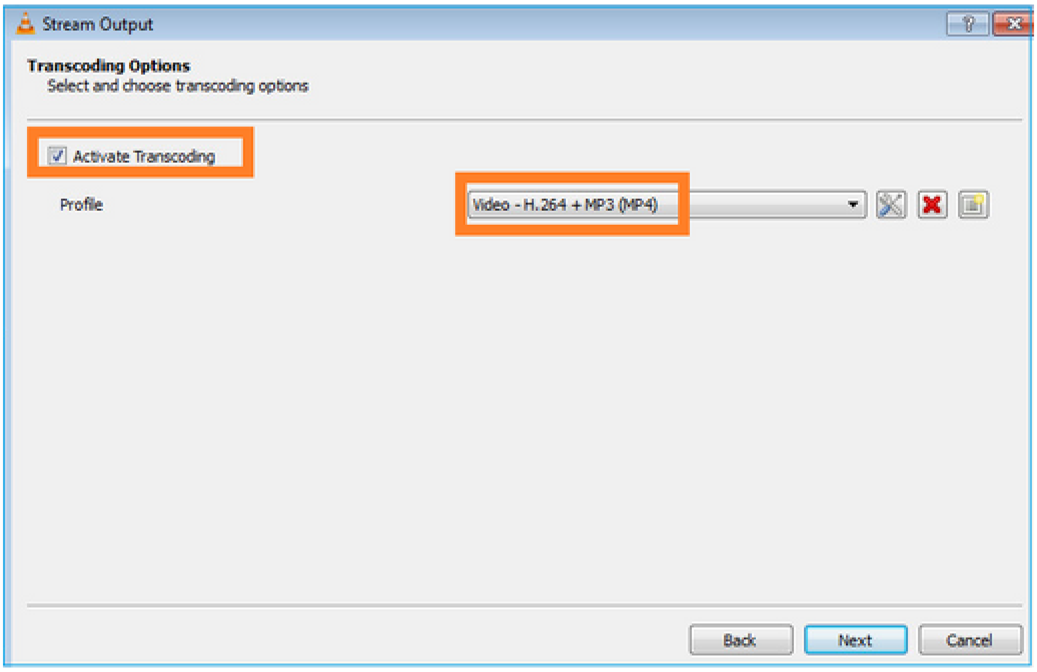
RTP/TS

This module outputs the transcoded stream to a network via RTP.

Address: 230.10.10.10

Base port: 5004

Stream name:



Stream Output

Transcoding Options

Select and choose transcoding options

☑ Activate Transcoding

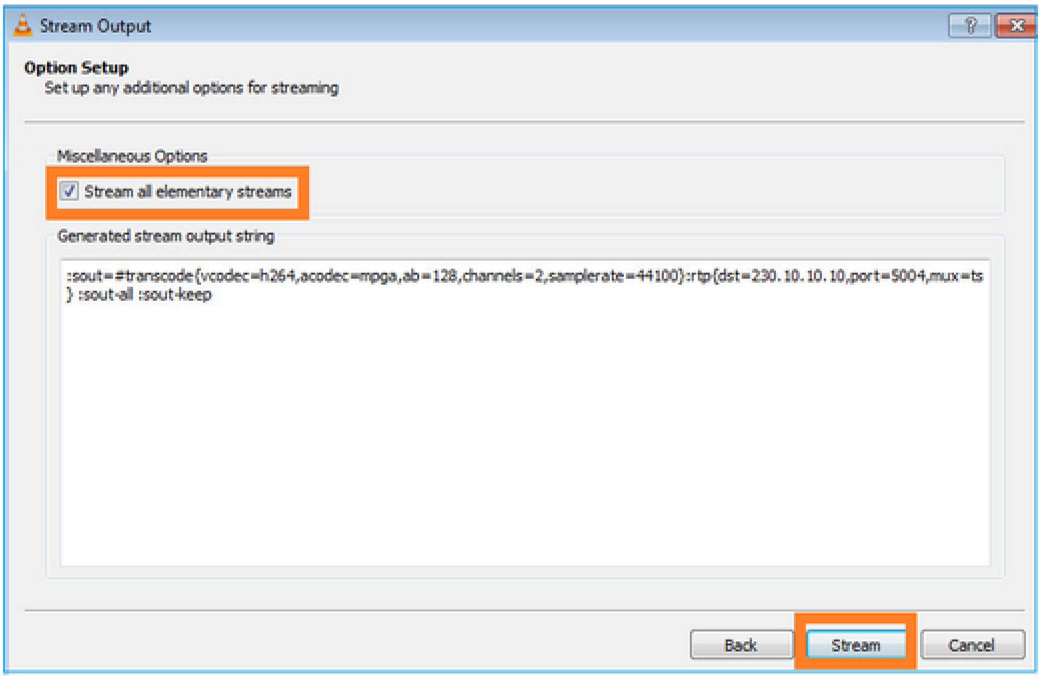
Profile: Video - H.264 + MP3 (MP4)

Habilitar capturas LINA en el firewall 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
```

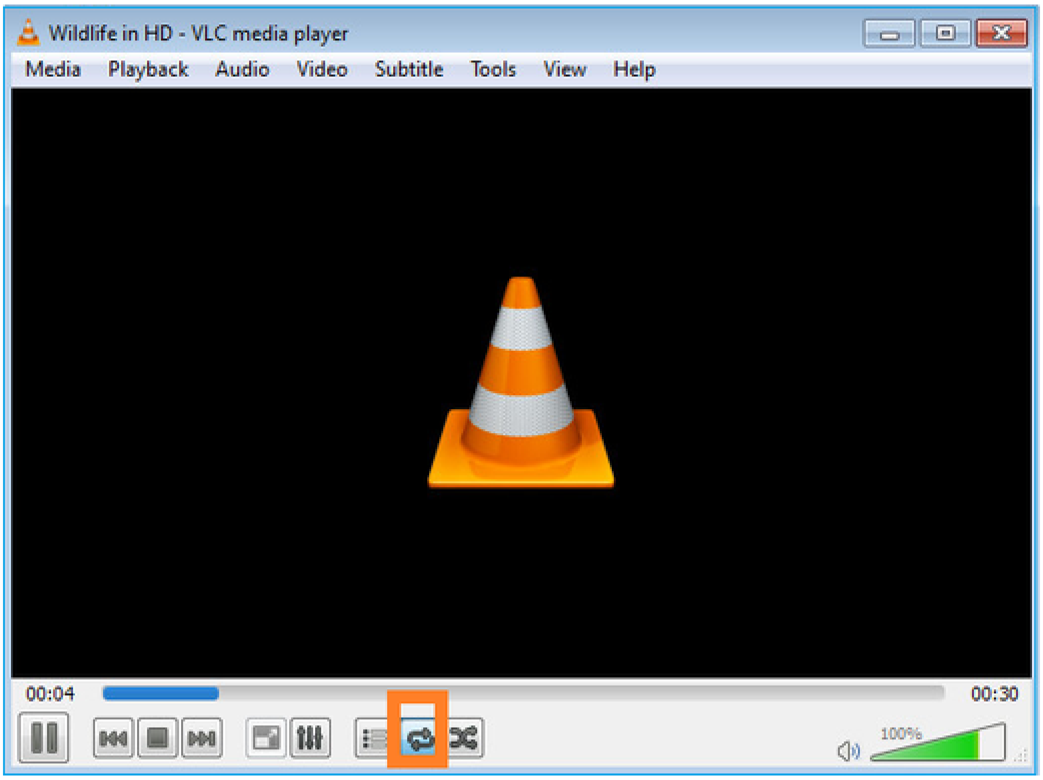
Seleccione el botón **Stream** para que el dispositivo inicie el flujo de multidifusión:



Stream Output
Option Setup
Set up any additional options for streaming
Miscellaneous Options
☑ Stream all elementary streams
Generated stream output string
Back
Stream
Cancel

```
:sout=#transcode{vcodec=h264,acodec=mpga,ab=128,channels=2,samplerate=44100}:rtp{dst=230.10.10.10,port=5004,mux=ts
} :sout-all :sout-keep
```

Habilite la opción â€˜loopâ€™ para que el flujo se envíe continuamente:



Verificación (escenario no operativo)

Este escenario es una demostración de un escenario no operativo. El objetivo es demostrar el comportamiento del firewall.

El dispositivo de firewall obtiene el flujo de multidifusión, pero no lo reenvía:

<#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
```

Para rastrear un paquete, es necesario capturar el primer paquete del flujo de multidifusión. Por esta razón, borre los flujos actuales:

<#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
...
```

La opción "detail" (detalles) muestra la dirección MAC de multidifusión:

<#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)
...
```

El seguimiento de un paquete real muestra que el paquete está permitido, pero esto no es lo que realmente sucede:

<#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
```

Según los contadores mroute y mfib, los paquetes se descartan porque la Lista de interfaz saliente (OIL) está vacía:

<#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
```

Los contadores MFIB muestran fallas RPF que en este caso no es lo que realmente sucede:

<#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
```

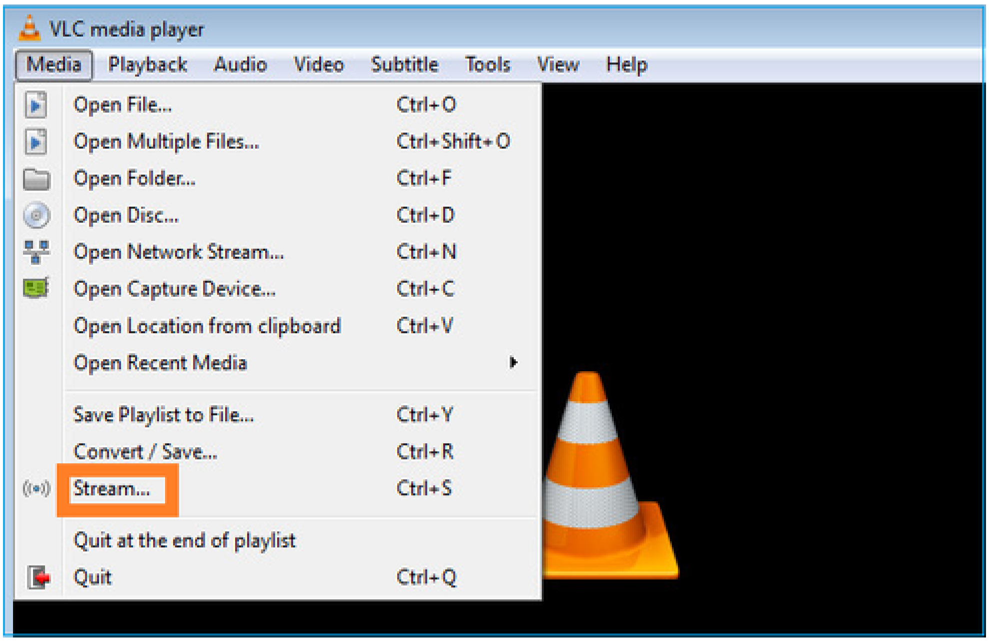
```
,

Other: 650/650

/0       <-- Allowed and dropped multicast packets
```

Fallos RPF similares en la salida 'show mfib count':

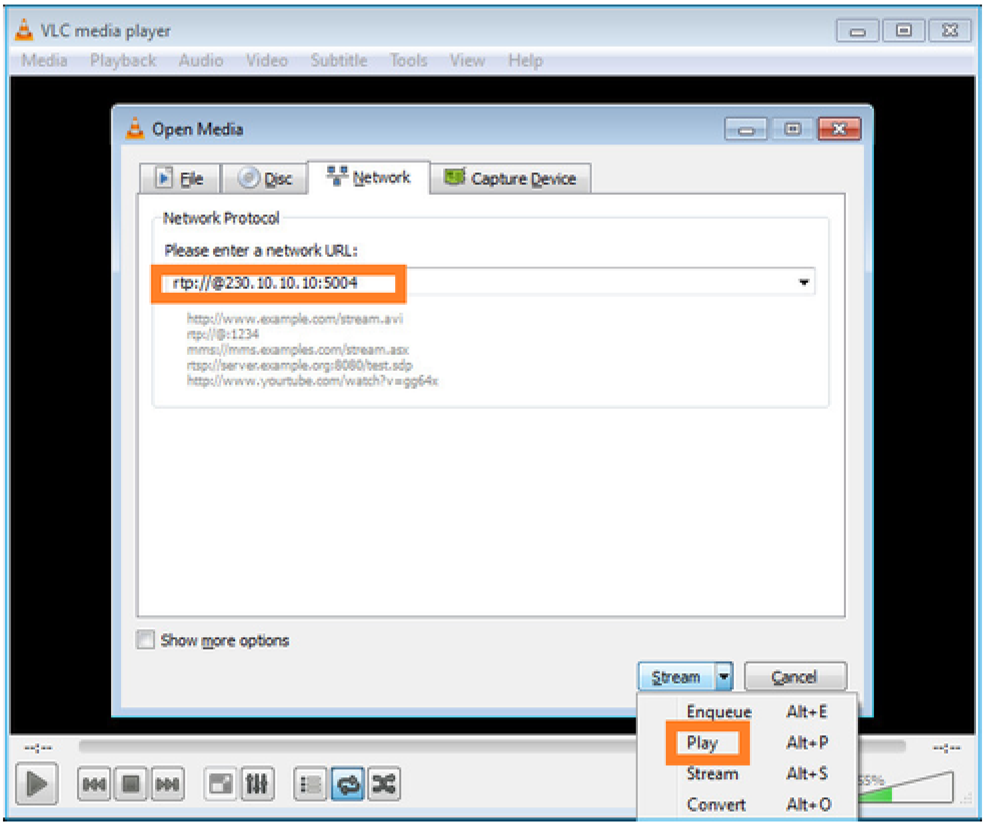
<#root>

```
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
```

Configure el receptor de multidifusión VLC:

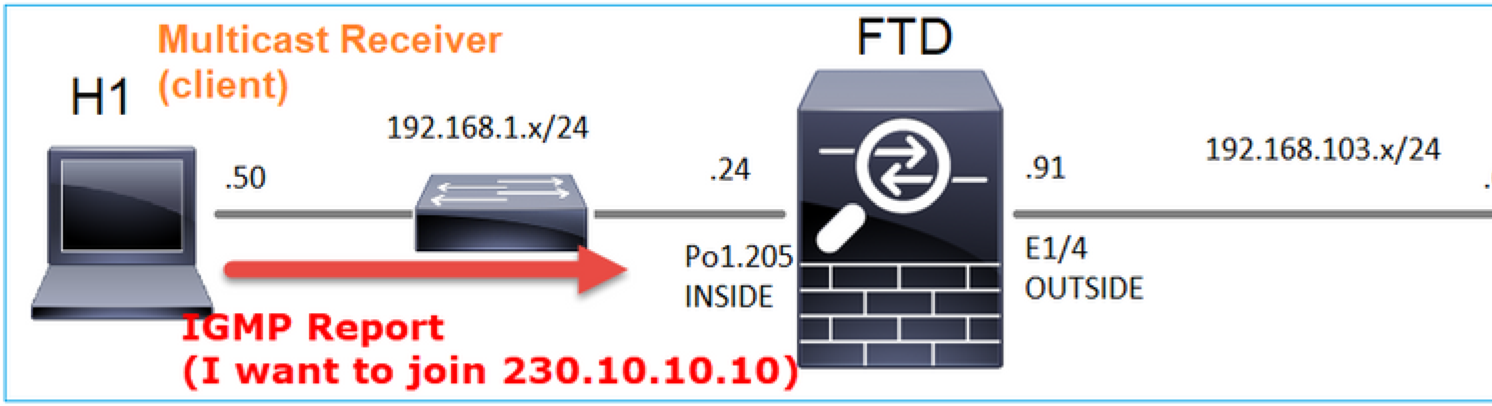

VLC media player
Media Playback Audio Video Subtitle Tools View Help
Open File... Ctrl+O
Open Multiple Files... Ctrl+Shift+O
Open Folder... Ctrl+F
Open Disc... Ctrl+D
Open Network Stream... Ctrl+N
Open Capture Device... Ctrl+C
Open Location from clipboard Ctrl+V
Open Recent Media
Save Playlist to File... Ctrl+Y
Convert / Save... Ctrl+R
Stream... Ctrl+S
Quit at the end of playlist
Quit Ctrl+Q

Especifique la IP de origen de multidifusión y seleccione **Play:**


VLC media player
Media Playback Audio Video Subtitle Tools View Help
Open Media
File Disc Network Capture Device
Network Protocol
http://www.example.com/stream.avi
rtp://@:1234
mms://mms.examples.com/stream.asx
rtsp://server.example.org:8080/test.sdp
http://www.yourtube.com/watch?v=gg64x
□ Show more options
Stream Cancel
Enqueue Alt+E
Play Alt+P
Stream Alt+S
Convert Alt+O

Please enter a network URL: rtp://@230.10.10.10:5004

En el backend, tan pronto como seleccione **Play** el host anuncia su voluntad de unirse al grupo multicast específico y envía un mensaje de **Informe IGMP**:

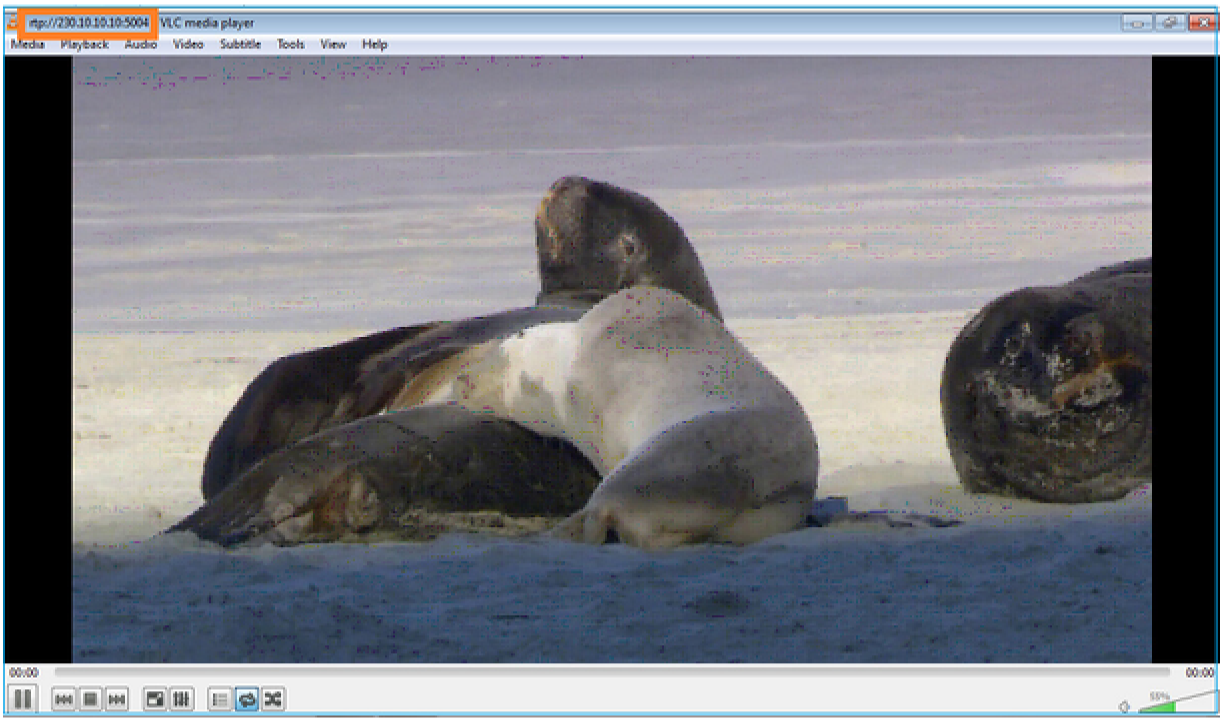


Si habilita una depuración, puede ver los mensajes del informe IGMP:

<#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
```

Comienza la secuencia:



Verificación (escenario operativo)

<#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 tabla mroute del firewall:

<#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
```

contadores de 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 indagación IGMP es un mecanismo utilizado en los switches para evitar la inundación de multidifusión.
- El switch supervisa los informes IGMP para determinar dónde se encuentran los hosts (receptores).
- El switch supervisa las consultas IGMP para determinar dónde se encuentran los routers/firewalls (remitentes).
- La función IGMP Snooping está activada de forma predeterminada en la mayoría de los switches de Cisco. Consulte las guías de switching correspondientes para obtener más información. Este es el ejemplo de salida de un switch Catalyst L3:

<#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
```

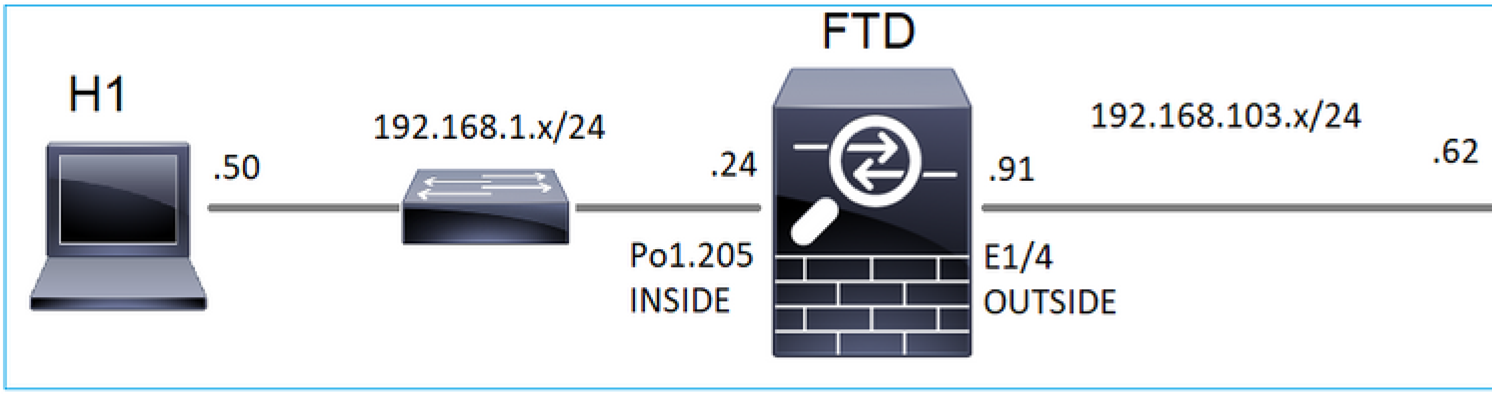
Tarea 3: IGMP static-group vs IGMP join-group

Overview

	ip igmp static-group	**ip igmp join-group**
¿Aplicado en la interfaz FTD?	Yes	Yes
¿El FTD atrae un flujo de multidifusión?	Sí, se envía una unión PIM hacia el dispositivo ascendente. el origen o hacia el punto de encuentro (RP). Esto solo ocurre si el FTD con este comando es el router designado (DR) PIM en esa interfaz.	Sí, se envía una unión PIM hacia el dispositivo ascendente. el origen o hacia el punto de encuentro (RP). Esto solo ocurre si el FTD con este comando es el router designado (DR) PIM en esa interfaz.
¿El FTD reenvía el tráfico multicast fuera de la interfaz?	Yes	Yes
¿Consume y responde el FTD al tráfico de multidifusión?	No	Sí, el FTD dirige la secuencia de multidifusión a la CPU, la consume y responde al origen.
Impacto de CPU	Mínimo, ya que el paquete no se envía a la CPU.	Puede afectar a la CPU de FTD, ya que cada paquete de multidifusión que pertenece al grupo se envía a la CPU de FTD.

Tarea requerida

Tenga en cuenta esta topología:



En el firewall, habilite estas capturas:

<#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. Utilice el ping ICMP del switch L3 para enviar tráfico multicast a IP 230.11.11.11 y verifique cómo el firewall lo maneja.
2. Habilite el comando **igmp static-group** en la interfaz firewall INSIDE y verifique cómo el firewall maneja el flujo multicast (IP 230.11.11.11).
3. Habilite el comando **igmp static-group** en la interfaz firewall INSIDE y verifique cómo el firewall maneja el flujo multicast (IP 230.11.11.11).

Solución

El firewall no tiene ninguna ruta multicast para 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
```

Una forma sencilla de probar la multidifusión es utilizar la herramienta de ping ICMP. En este caso, inicie un ping desde R2 a la dirección IP multicast 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:
...............................
```

En el firewall, se crea una ruta multicast dinámicamente y el OIL está vacío:

<#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 captura en el firewall muestra:

<#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
```

El firewall crea conexiones para cada ping, pero descarta silenciosamente los paquetes:

<#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
May 17 2022 11:05:47: %FTD-6-302020: Built inbound ICMP connection for faddr 192.168.103.62/6 gaddr 230.
May 17 2022 11:05:49: %FTD-6-302021: Teardown ICMP connection for faddr 192.168.1.99/6 gaddr 230.11.11.1
May 17 2022 11:05:49: %FTD-6-302021: Teardown ICMP connection for faddr 192.168.103.62/6 gaddr 230.11.11
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
May 17 2022 11:05:51: %FTD-6-302020: Built inbound ICMP connection for faddr 192.168.103.62/6 gaddr 230.
May 17 2022 11:05:53: %FTD-6-302021: Teardown ICMP connection for faddr 192.168.1.99/6 gaddr 230.11.11.1
May 17 2022 11:05:53: %FTD-6-302021: Teardown ICMP connection for faddr 192.168.103.62/6 gaddr 230.11.11
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
```

Nota: La captura de caídas de LINA ASP no muestra los paquetes caídos

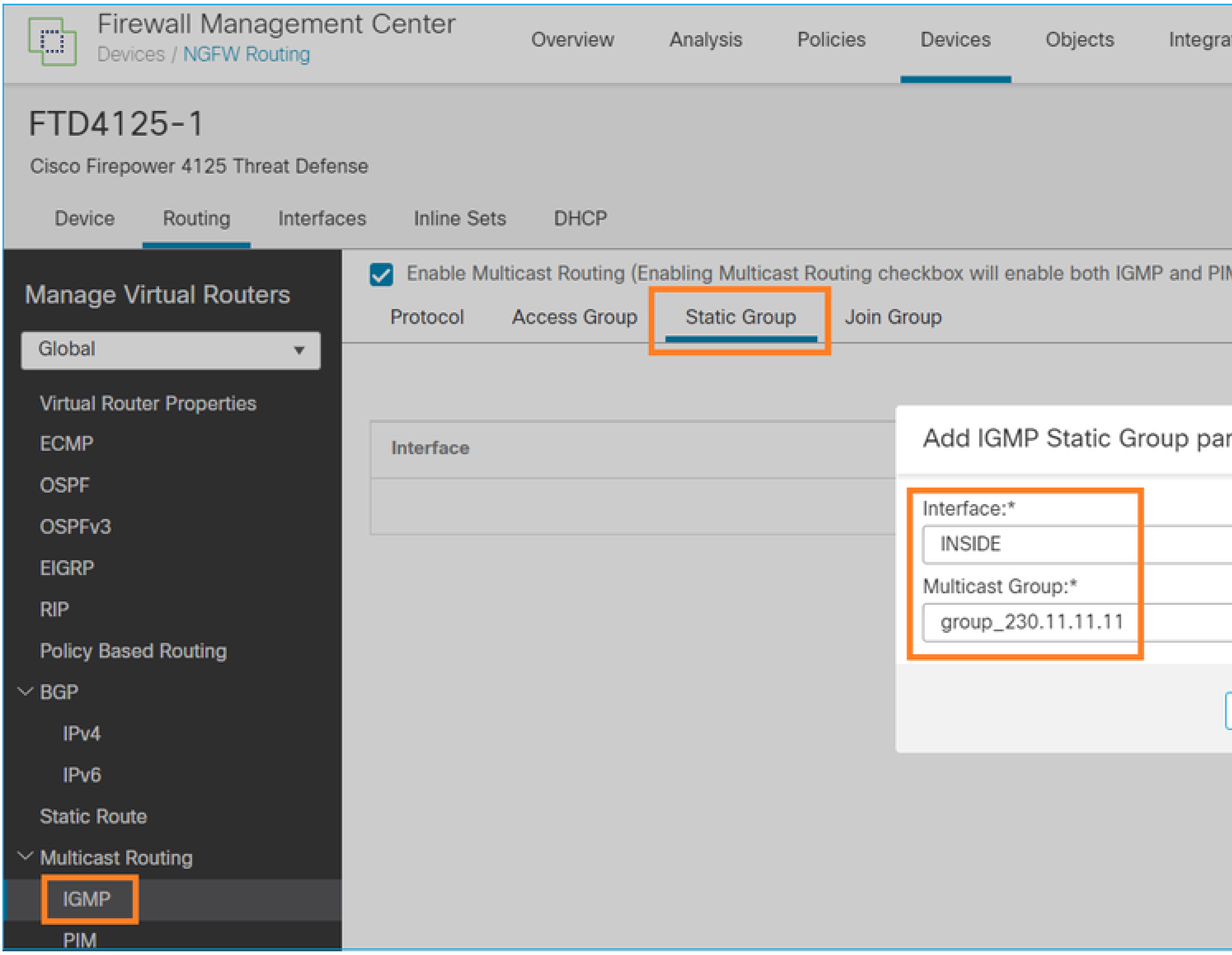
La indicación principal de caídas de paquetes multicast es:

<#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

En FMC configure un grupo IGMP estático:



☑ Enable Multicast Routing (Enabling Multicast Routing checkbox will enable both IGMP and PIM

Interface:* INSIDE

Multicast Group:* group_230.11.11.11

Esto es lo que se implementa en segundo plano:

<#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
```

El ping falla, pero el tráfico multicast ICMP ahora se reenvía a través del firewall:

<#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 P0 192.168.103.62 > 230.11.11.11 icmp: echo request
2: 11:31:34.470404 802.1Q vlan#205 P0 192.168.103.62 > 230.11.11.11 icmp: echo request
3: 11:31:36.470861 802.1Q vlan#205 P0 192.168.103.62 > 230.11.11.11 icmp: echo request
4: 11:31:38.470816 802.1Q vlan#205 P0 192.168.103.62 > 230.11.11.11 icmp: echo request
```

Nota: El seguimiento del paquete muestra una salida incorrecta (la interfaz de entrada es la misma que la de salida). Para obtener más detalles, consulte el ID de bug de Cisco 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
```

> **Sugerencia**: Puede hacer ping con el tiempo de espera 0 desde el host de origen y puede verificar los contadores mfib del firewall:

<#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:
......................................................................
......................................................................
......................................................................
```

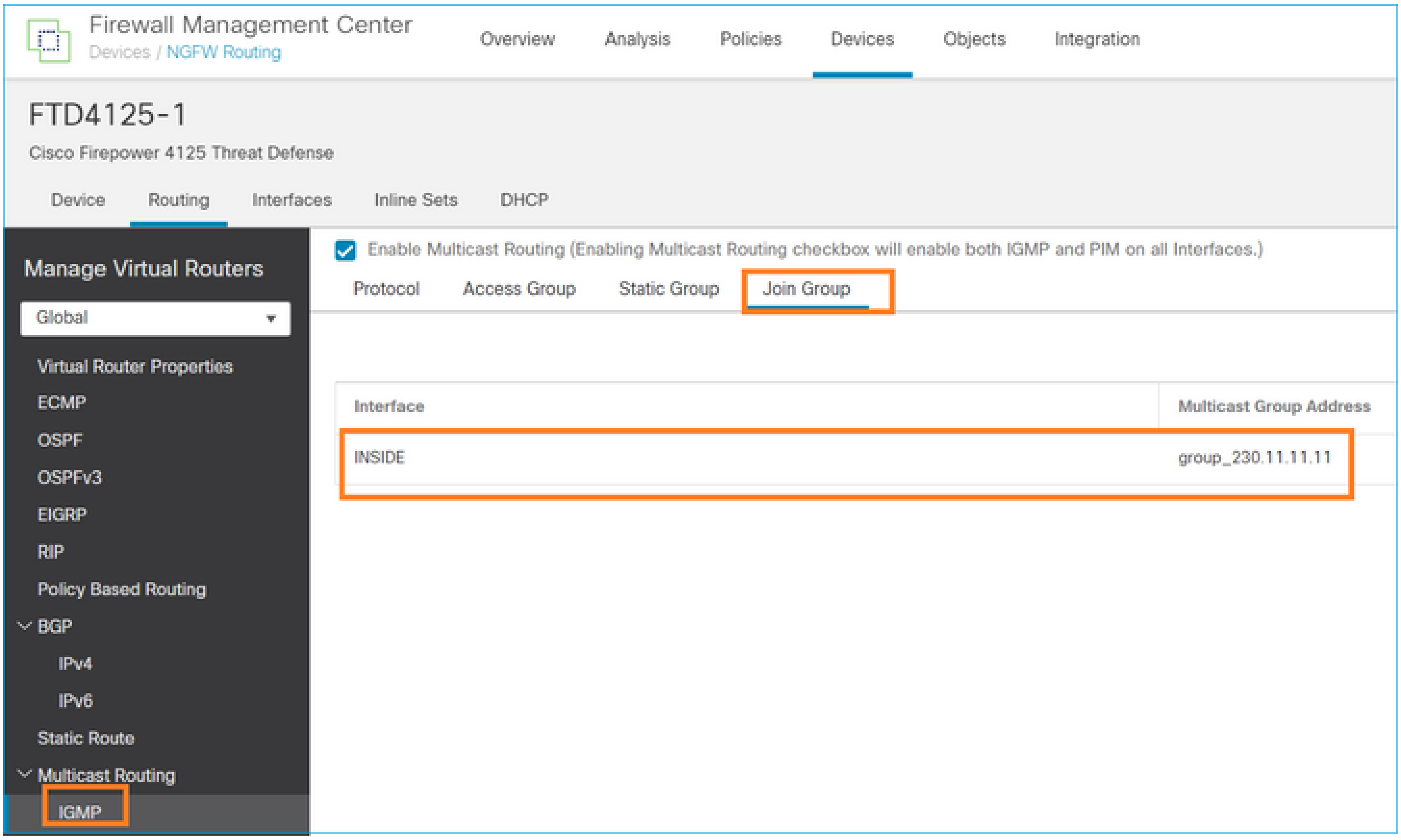
```
....................
```

<#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
```

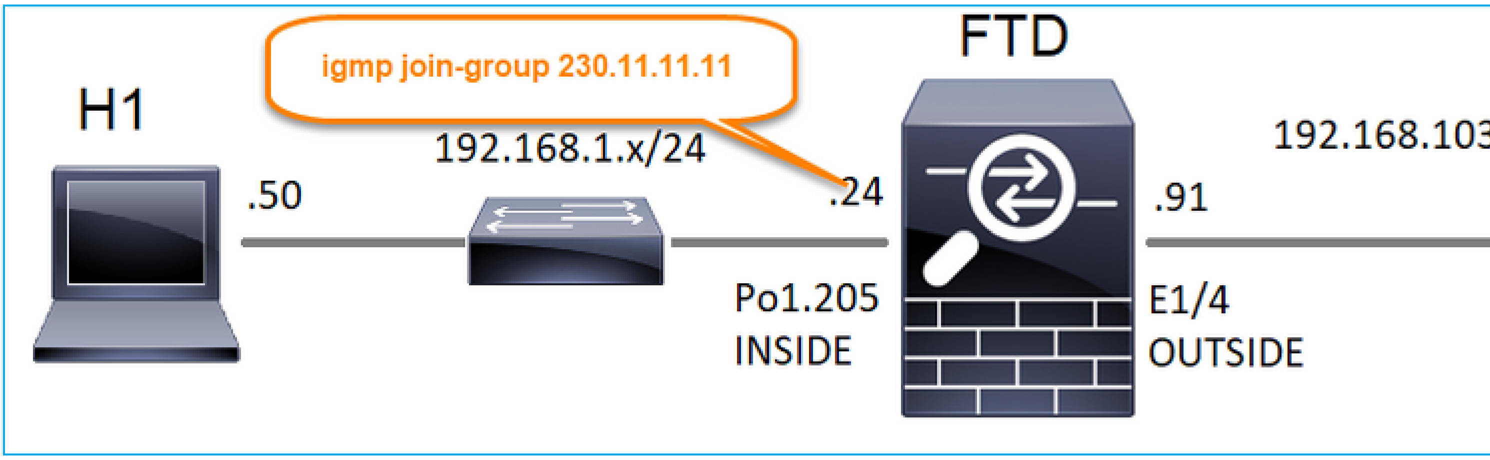
igmp join-group

En FMC remoto, la configuración de grupo estático previamente configurada y configurar un grupo de unión IGMP:



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

Interface	Multicast Group Address
INSIDE	group_230.11.11.11



La configuración implementada:

<#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
```

El grupo 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
```

Desde el host de origen, intente la primera prueba de multidifusión ICMP hacia la IP 230.11.11.11:

<#root>

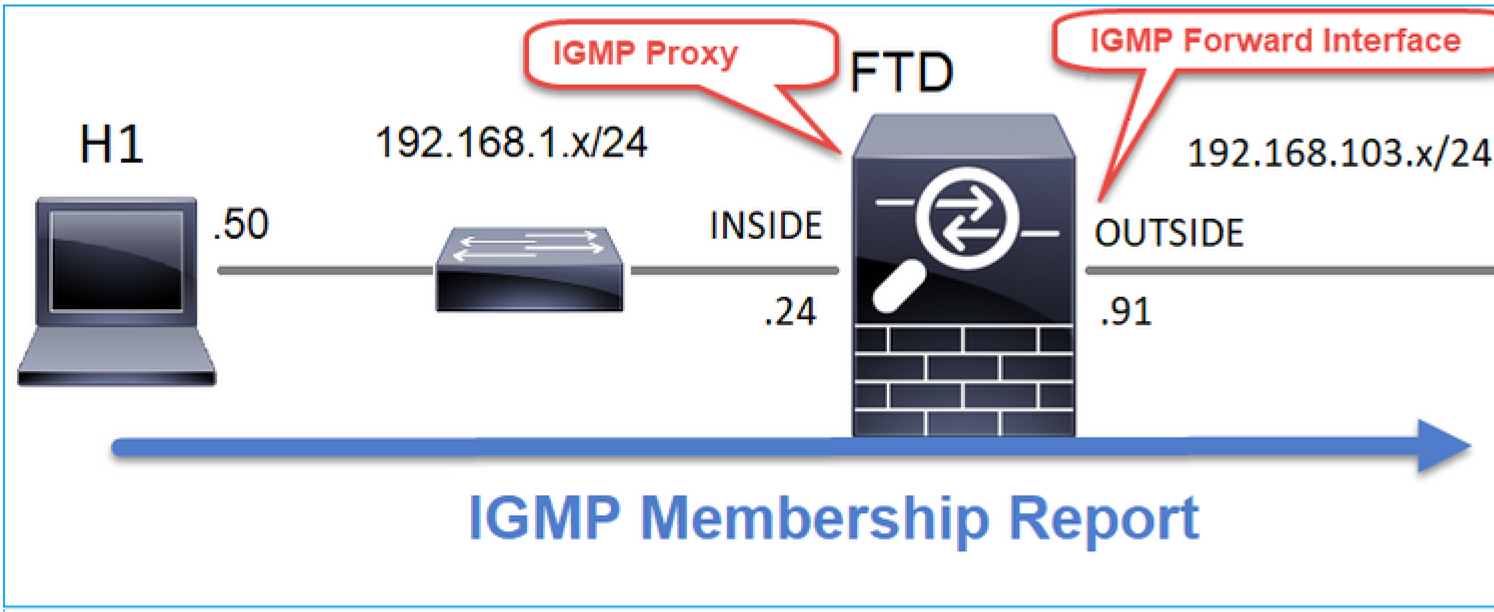
```
L3-Switch#
```

```
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
```

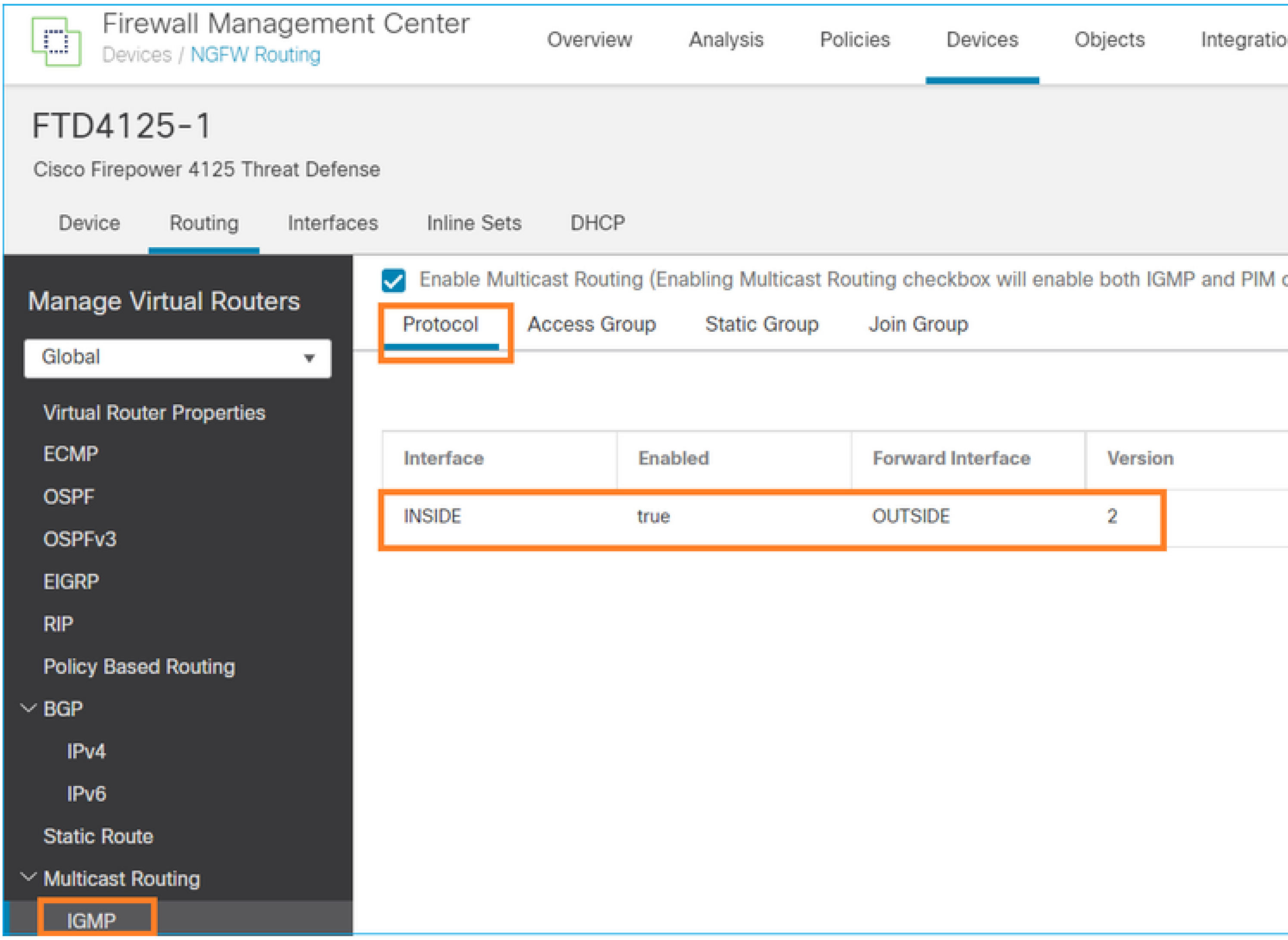
Nota: Si no ve todas las respuestas, verifique Cisco bug ID CSCvm90069.

Tarea 4 - Configuración del Ruteo Multicast Stub IGMP



Configure el ruteo de multidifusión stub en FTD de modo que los mensajes de informe de afiliación IGMP recibidos en la interfaz INSIDE se reenvíen a la interfaz OUTSIDE.

Solución



☑ Enable Multicast Routing (Enabling Multicast Routing checkbox will enable both IGMP and PIM o

Interface	Enabled	Forward Interface	Version
INSIDE	true	OUTSIDE	2

La configuración implementada:

```
<#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
```

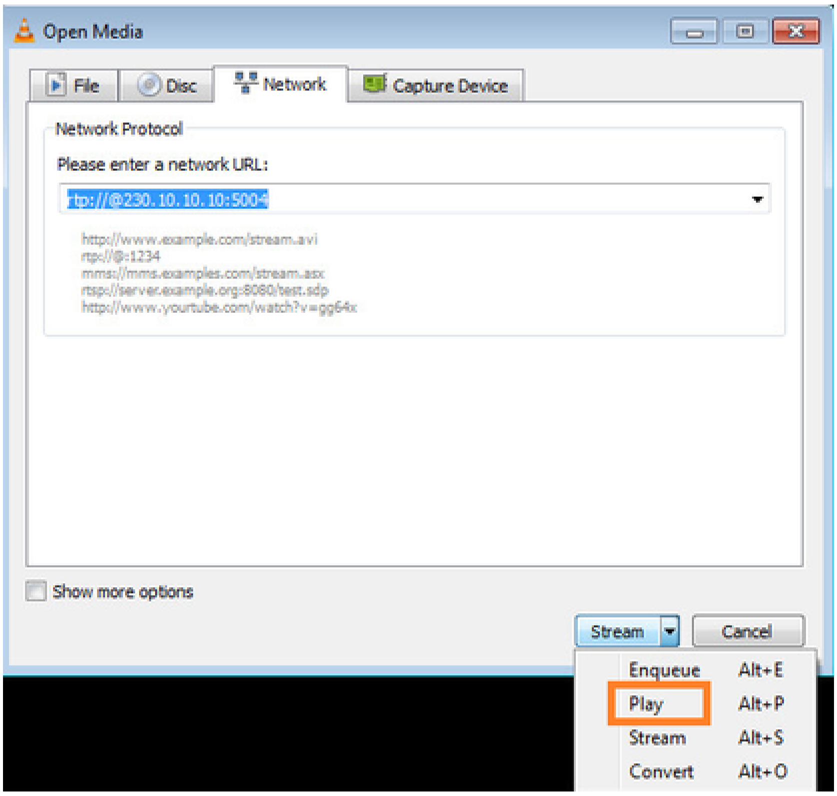
Verificación

Habilitar capturas en 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
```

Verificación

Para forzar un informe de afiliación IGMP, puede utilizar una aplicación como VLC:



Network Protocol

Please enter a network URL:

rtp://@230.10.10.10:5004

Open Media
File
Disc
Network
Capture Device
http://www.example.com/stream.avi
rtp://@:1234
mms://mms.examples.com/stream.asx
rtsp://server.example.org:8080/test.sdp
http://www.youtube.com/watch?v=gg64x
Show more options
Stream
Cancel
Enqueue Alt+E
Play Alt+P
Stream Alt+S
Convert Alt+O

El FTD hace proxy de los paquetes 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
```

El FTD cambia la IP de origen:

```
<#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
```

Si verifica el pcap en Wireshark, puede ver que el firewall ha regenerado completamente el paquete (la identificación de IP cambia).

Se crea una entrada de grupo en 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
```

El firewall FTD crea 2 conexiones de plano de control:

<#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
```

Seguimiento del primer paquete:

<#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:
```

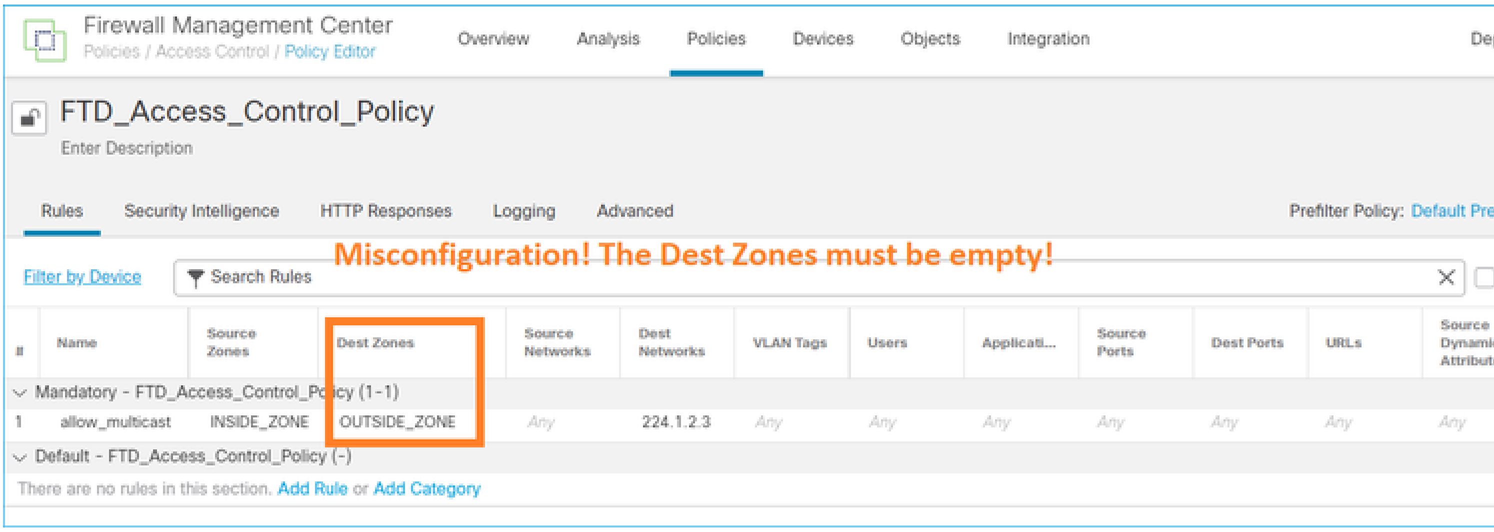
```
Result: ALLOW

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:

New flow created with id 5946, packet dispatched to next module


Phase: 12
Type: NEXTHOP-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Lookup Nexthop on interface
Result: ALLOW
Elapsed time: 6344 ns
Config:
Additional Information:
Found next-hop 230.10.10.10 using egress ifc OUTSIDE(vrfid:0)

Phase: 13
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 9760 ns
```

```
Config:
Additional Information:
MAC Access list

Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
output-interface: INSIDE(vrfid:0)
output-status: up
output-line-status: up
Action: allow
Time Taken: 154208 ns
```

Problemas conocidos

Filtrado de Tráfico Multicast en Zonas de Destino

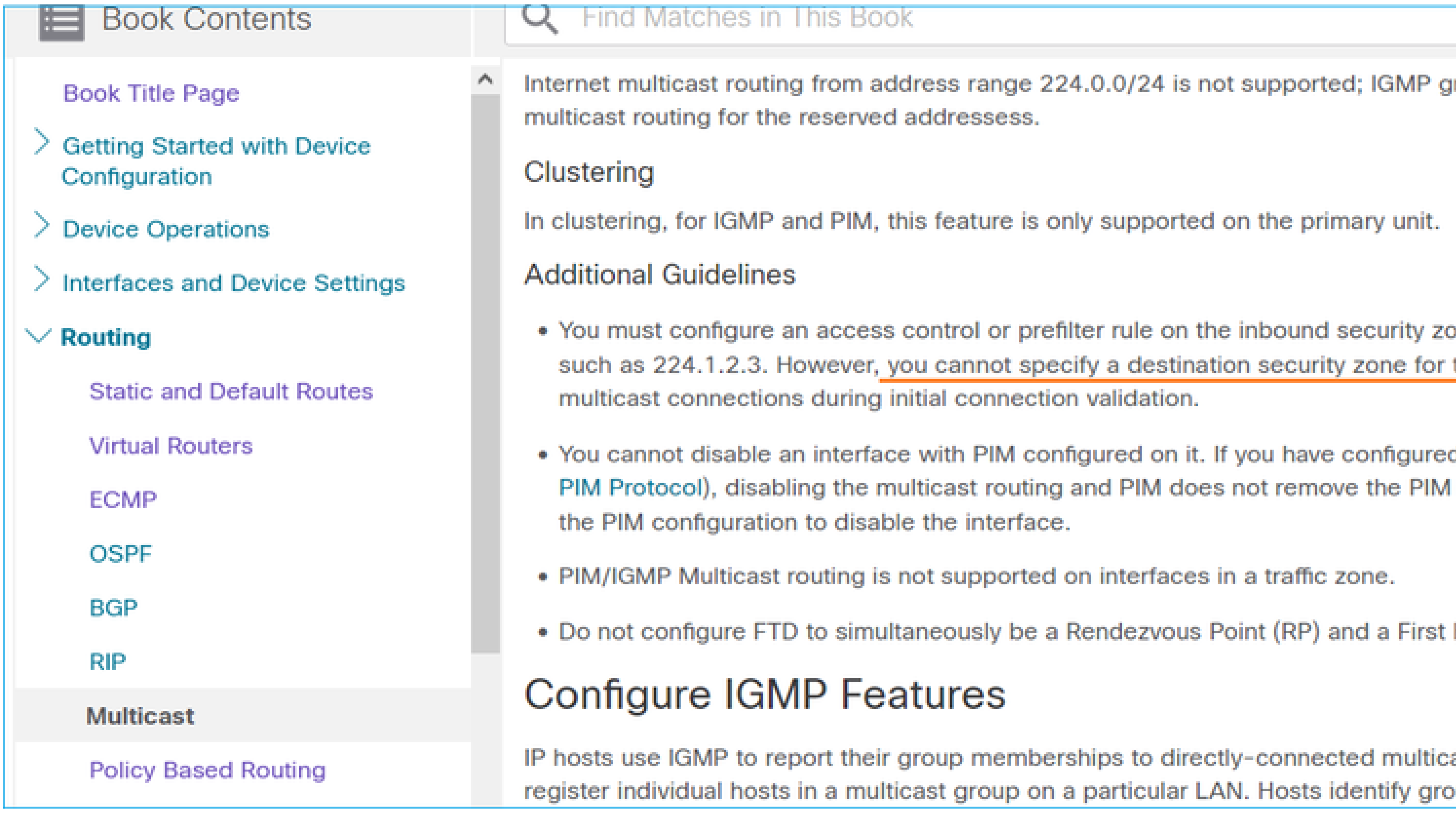
No puede especificar una zona de seguridad de destino para la regla de directiva de control de acceso que coincida con el tráfico de multidifusión:



Misconfiguration! The Dest Zones must be empty!

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source Ports	Dest Ports	URLs	Source Dynami Attribut
Mandatory - FTD_Access_Control_Policy (1-1)												
1	allow_multicast	INSIDE_ZONE	OUTSIDE_ZONE	Any	224.1.2.3	Any	Any	Any	Any	Any	Any	Any
Default - FTD_Access_Control_Policy (-)												
There are no rules in this section. Add Rule or Add Category												

Esto también se documenta en la guía del usuario de FMC:


Book Contents
Find Matches in This Book
Book Title Page
Getting Started with Device Configuration
Device Operations
Interfaces and Device Settings
Routing
Static and Default Routes
Virtual Routers
ECMP
OSPF
BGP
RIP
Multicast
Policy Based Routing

Internet multicast routing from address range 224.0.0/24 is not supported; IGMP g
multicast routing for the reserved addressess.

Clustering

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

Additional Guidelines

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

Configure IGMP Features

IP hosts use IGMP to report their group memberships to directly-connected multica
register individual hosts in a multicast group on a particular LAN. Hosts identify gro

El firewall deniega los informes IGMP cuando se supera el límite de la interfaz IGMP

De forma predeterminada, el firewall permite un máximo de 500 uniones activas actuales (informes) en una interfaz. Si se excede este umbral, el firewall ignora los informes IGMP entrantes adicionales de los receptores multicast.

Para verificar el límite IGMP y las uniones activas, ejecute el comando **show igmp interface nameif**:

<#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)
```

El comando de depuración IGMP **debug igmp** muestra este resultado:

<#root>

```
asa#

debug igmp


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

ID de bug de Cisco CSCuw84390 realiza un seguimiento de la mejora para aumentar el límite IGMP.

El firewall ignora los informes IGMP para el rango de direcciones 232.x.x.x/8

El rango de direcciones 232.x.x.x/8 se utiliza con Source Specific Multicast (SSM). El firewall no admite la funcionalidad de multidifusión específica de origen (SSM) de PIM ni la configuración relacionada.

El comando de depuración IGMP **debug igmp** muestra este resultado:

<#root>

```
asa#

debug igmp


Apr 20 2023 09:37:10: %ASA-7-711001: IGMP: Received v2 Report on inside from 10.10.10.11 for 232.179.89.
Apr 20 2023 09:37:10: %ASA-7-711001: IGMP: group_db: add new group 232.179.89.253 on inside

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

ID de bug de Cisco CSCsr53916 realiza un seguimiento de la mejora para admitir el intervalo SSM.

Información Relacionada

- Routing multidifusión para Firepower Threat Defence
- Solución de problemas de Firepower Threat Defense y ASA Multicast PIM