# Fehlerbehebung: Firepower Threat Defense - IGMP- und Multicast-Grundlagen

## Inhalt



## Einleitung

Dieses Dokument beschreibt die Grundlagen von Multicast und wie Firepower Threat Defense (FTD) das Internet Group Management Protocol (IGMP) implementiert.

## Voraussetzungen

### Anforderungen

Grundlegende Kenntnisse zu IP-Routing

### Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Der Inhalt dieses Artikels gilt auch für die Software der Adaptive Security Appliance (ASA).

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco FirePOWER 4125 Threat Defence Version 7.1.0
- FirePOWER Management Center (FMC) Version 7.1.0
- ASA Version 9.19.1.

# Hintergrundinformationen

### Definitionen

- Unicast = von einem einzelnen Host zu einem anderen Host (One-to-One).
- Broadcast = von einem einzelnen Host zu ALLEN möglichen Hosts (One-to-All).
- **Multicast = von einem Host einer Gruppe von Hosts zu einer Gruppe von Hosts (One-to-Many oder Many-to-Many).**
- Anycast = von einem Host zum nächsten Host einer Gruppe (One-to-One-of-Many).

### Grundlagen

- Multicast RFC 988 wurde 1986 von Steve Deering geschrieben.
- IPv4-Multicast verwendet den Bereich 224.0.0.0/4 (die ersten 4 Bit, 1110) - 224.0.0.0 - 239.255.255.255.
- Für IPv4 wird die L2-MAC-Adresse von der L3-Multicast-IP-Adresse abgeleitet: 01005e (24 Bit) + 25· Bit immer 0 + 23 niedrigere Bits der Multicast-IPv4-Adresse.
- IPv6-Multicast verwendet den Bereich FF00::/8 und ist flexibler als IPv4-Multicast, da Rendezvous Point (RP)-IP eingebettet werden kann.
- Für IPv6 wird die L2-MAC-Adresse aus dem L3-Multicast abgeleitet: 333 + 32 niedrigere Bits der Multicast-IPv6-Adresse.
- Multicast-Vorteile: Effizienz durch geringere Auslastung der Quelle. Leistung, da Datenverkehrsduplikate und -überflutungen vermieden werden.
- Multicast-Nachteile: Unzuverlässiger Transport (UDP-basiert), keine Vermeidung von Überlastung, Out-of-Sequence-Bereitstellung.
- Multicast wird im öffentlichen Internet nicht unterstützt, da hierfür alle Geräte im Pfad erforderlich sind. Wird in der Regel verwendet, wenn alle Geräte einer gemeinsamen administrativen Behörde unterstehen.
- Typische Multicast-Anwendungen: interner Video-Stream, Videokonferenz.

### Multicast und repliziertes Unicast

Bei repliziertem Unicast erstellt die Quelle mehrere Kopien desselben Unicast-Pakets (Replikate) und sendet sie an mehrere Ziel-Hosts. Multicast verlagert die Last vom Quell-Host zum Netzwerk, während bei Repliziertem Unicast die gesamte Arbeit auf dem Quell-Host ausgeführt wird.

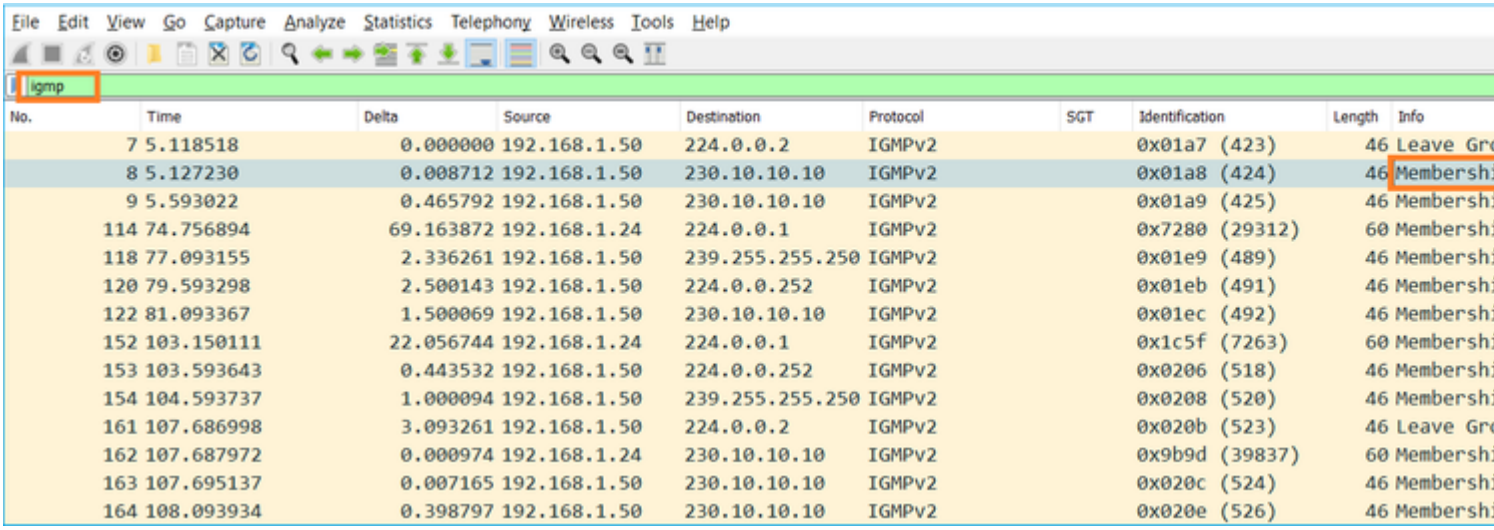
# Konfigurieren

### IGMP-Grundlagen

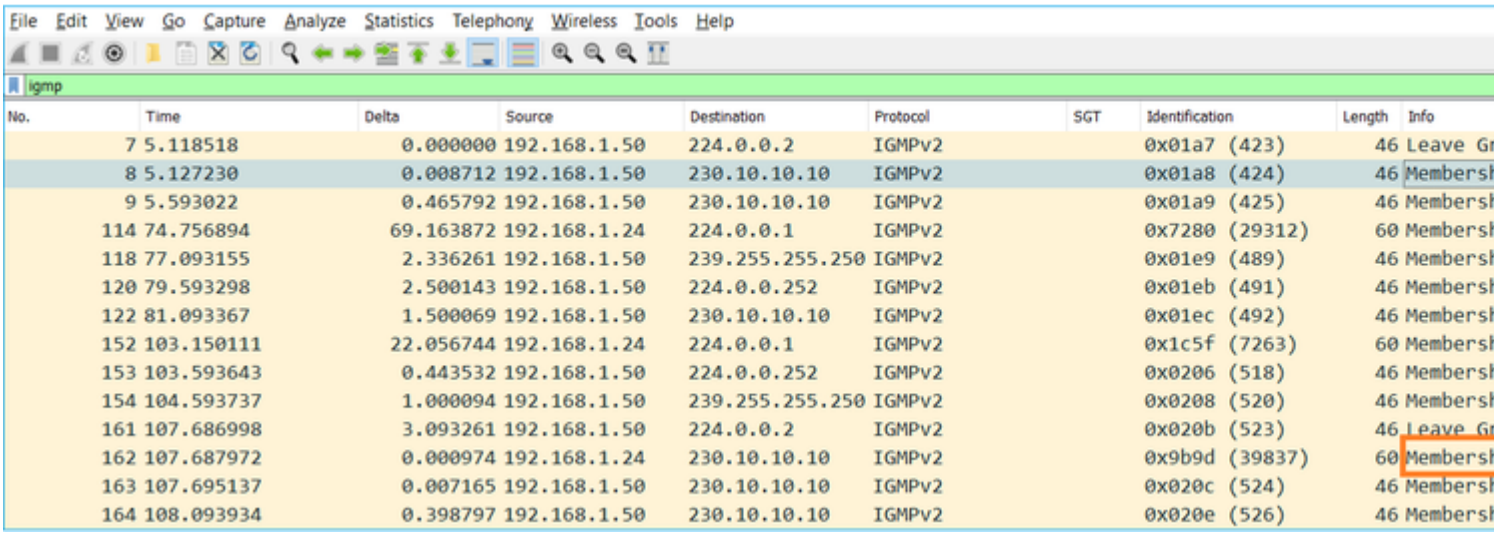
- IGMP ist die "Sprache", die zwischen den Multicast-Empfängern und dem lokalen L3-Gerät (in der Regel einem Router) gesprochen wird.
- IGMP ist ein Layer-3-Protokoll (wie ICMP) und verwendet das **IP-Protokoll Nummer 2.**
- Derzeit gibt es drei IGMP-Versionen. Die IGMP-Standardversion der Firewall ist Version 2. **Derzeit werden nur die Versionen 1 und 2 unterstützt.**
- Zwischen IGMPv1 und IGMPv2 bestehen die Hauptunterschiede in folgenden Bereichen:
    - IGMPv1 hat keine Nachricht "Leave Group" (Gruppe verlassen).
    - IGMPv1 verfügt über keine gruppenspezifische Abfrage (wird von der Firewall verwendet,

wenn ein Host eine Multicast-Gruppe verlässt).
  - IGMPv1 verfügt über keinen Abfrageauswahlprozess.

- **IGMPv3 wird derzeit** auf ASA/FTD **nicht unterstützt,** der wesentliche Unterschied zwischen IGMPv2 und IGMPv3 besteht jedoch in der Aufnahme einer gruppen- und quellenspezifischen Abfrage in IGMPv3, die in Source-Specific Multicast (SSM) verwendet wird.
- IGMPv1/IGMPv2/IGMPv3-Abfragen = **224.0.0.1**
  IGMPv2 Leave = **224,0.0,2**
  IGMPv3-Mitgliedsbericht = **224.0.0.22**
- Wenn ein Host beitreten möchte, kann er eine **nicht angeforderte IGMP**-Meldung senden:




- Vom Firewall-Standpunkt aus gibt es **zwei Arten von IGMP-Abfragen: Allgemeine Abfragen** und **gruppenspezifische Abfragen.**
- Wenn die Firewall die IGMP-Meldung "Leave Group" (Gruppe verlassen) empfängt, muss sie prüfen, ob sich andere Mitglieder dieser Gruppe im Subnetz befinden. Aus diesem Grund sendet die Firewall eine **gruppenspezifische Abfrage:**




- In Subnetzen mit mehreren Routern/Firewalls wird ein **Abfrager (**ein Gerät, das alle IGMP-Abfragen sendet) ausgewählt:

```
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
```

- Auf FTD können Sie, ähnlich wie bei klassischen ASA-Geräten, **IGMP** aktivieren**,** um IGMP-bezogene Meldungen anzuzeigen:

<#root>

```
firepower#
```

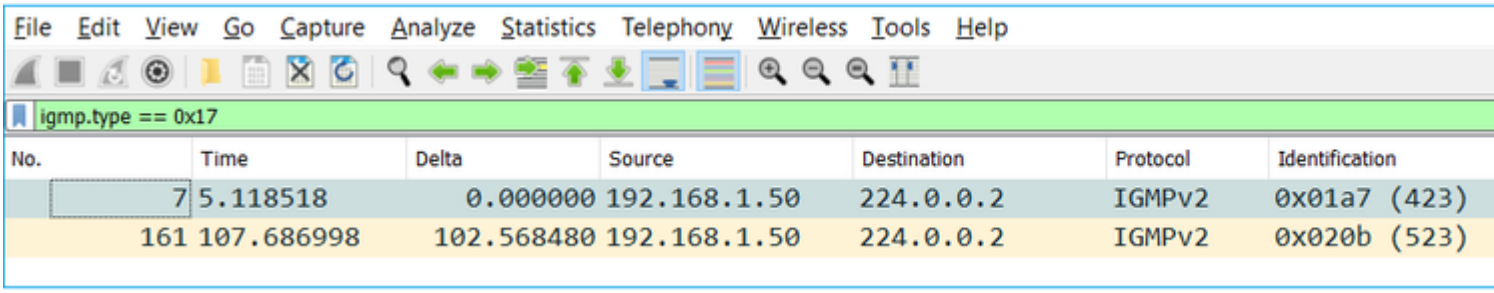
```
debug igmp
```

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

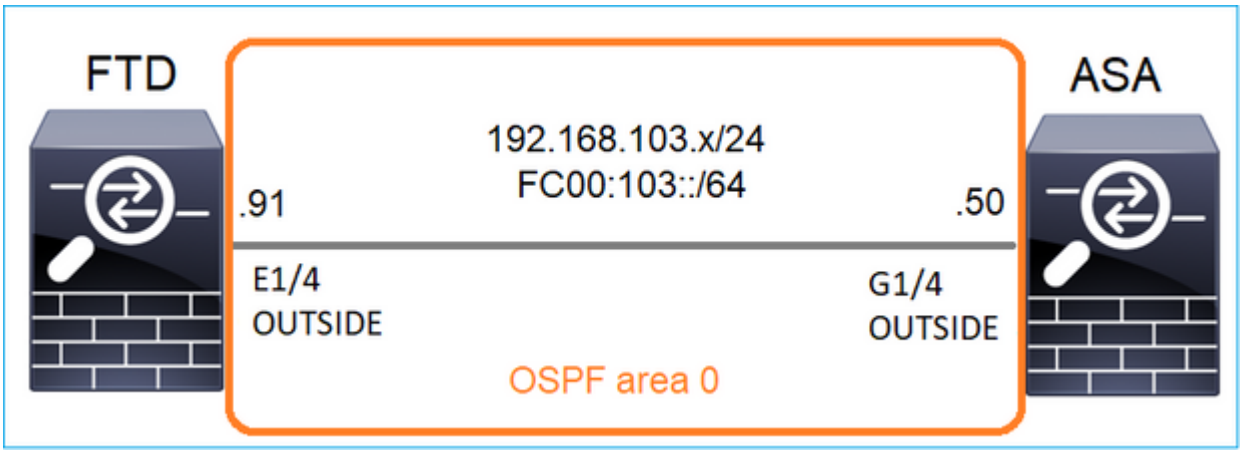
```
IGMP: Received v2 Report on INSIDE from 192.168.1.50 for 239.255.255.250
```

```
<-- 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
```

- Ein Host verlässt normalerweise eine Multicast-Gruppe mit einer **Leave Group**-Nachricht (IGMPv2).



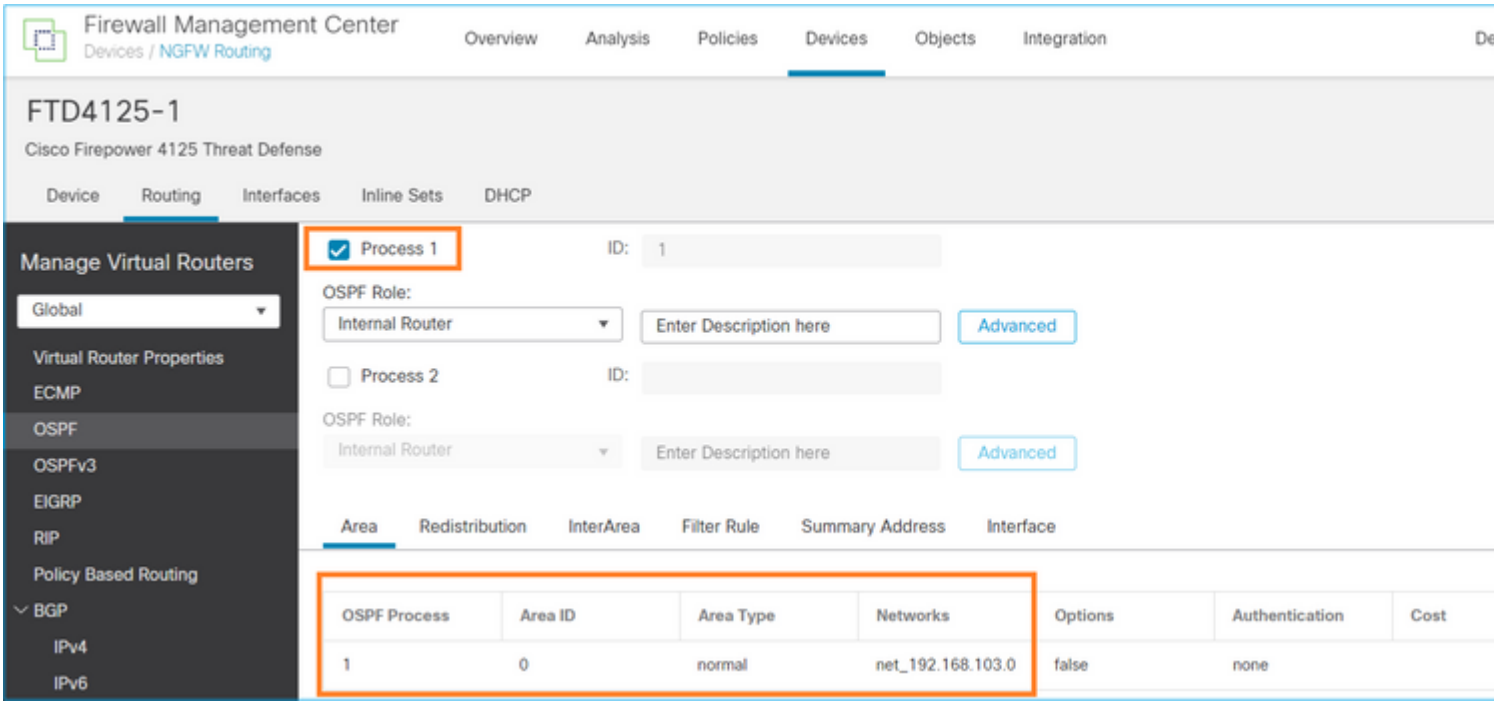

## Aufgabe 1: Multicast-Verkehr auf der Kontrollebene

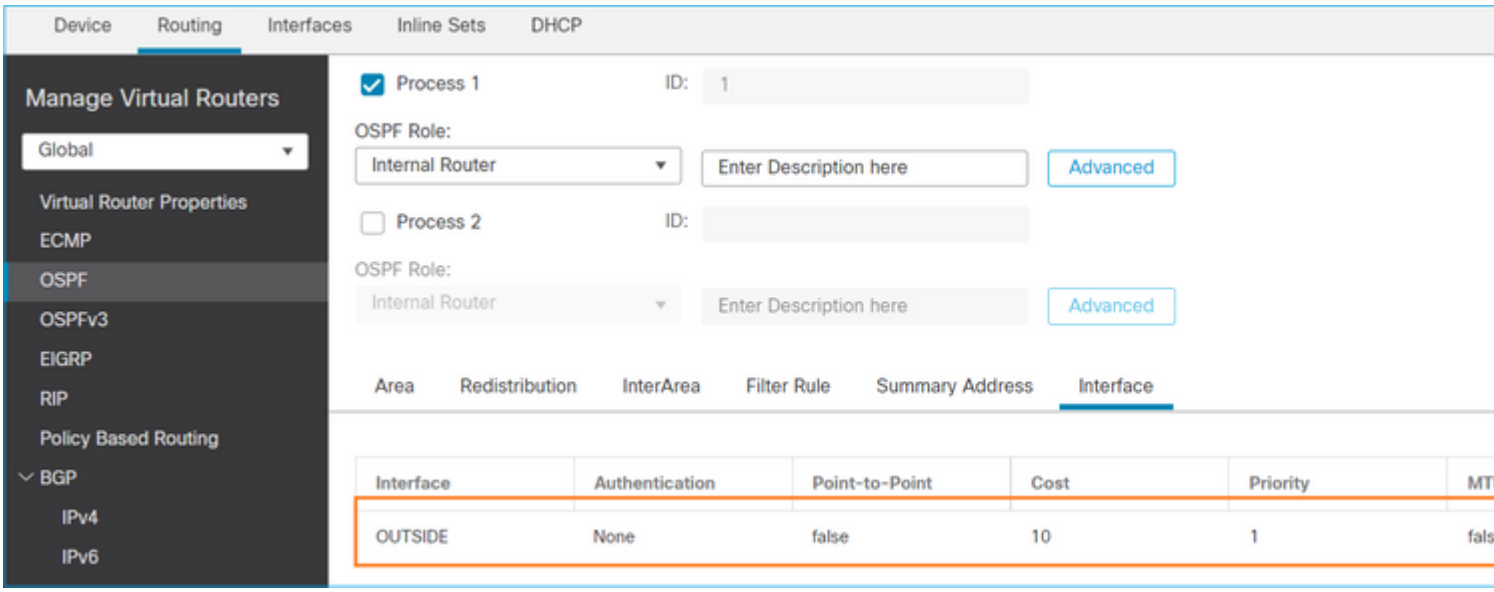



Konfigurieren Sie OSPFv2 und OSPFv3 zwischen dem FTD und der ASA. Prüfen Sie, wie die beiden Geräte den von OSPF generierten L2- und L3-Multicast-Datenverkehr verarbeiten.

**Lösung**

OSPFv2-Konfiguration






Ähnlich für OSPFv3

Konfiguration auf FTD CLI:

<#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
```

Bei der Konfiguration werden diese Einträge in den Erlaubnistabellen für den FTD Accelerated Security Path (ASP) erstellt, damit der eingehende Multicast-Datenverkehr nicht blockiert wird:

<#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
```

Für 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
...
```

Die OSPFv2- und OSPFv3-Adjacencies sind 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
```

Die folgenden Multicast-OSPF-Sitzungen werden an der Box terminiert:

```
<#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
```

Aktivieren Sie als Test die Erfassung für IPv4, und löschen Sie die Verbindungen zum Gerät:

```
<#root>

firepower#
```

```
capture CAP interface OUTSIDE trace

firepower#

clear conn all

12 connection(s) deleted.
firepower#

clear capture CAP

firepower# !
```

---

**Warnung**: Dies führt zu einem Ausfall! Das Beispiel dient nur zu Demonstrationszwecken.

---

Die erfassten OSPF-Pakete:

<#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]
```

So wird das OSPFv2-Multicast-Paket von der Firewall behandelt:

<#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

So wird das OSPFv3-Multicast-Paket von der Firewall behandelt:

<#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**

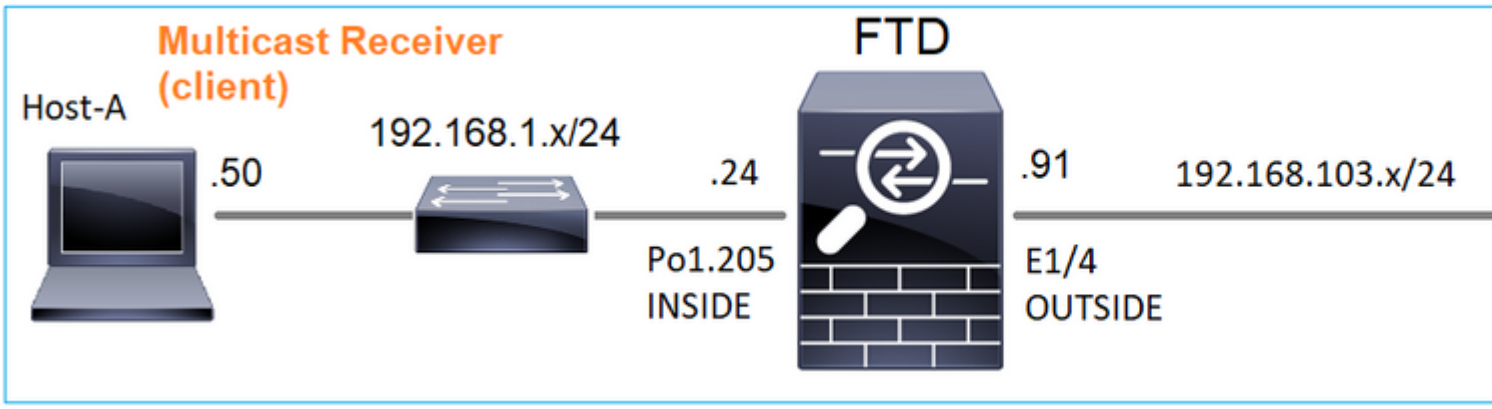
**Config:**

**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
```

## Aufgabe 2: Konfigurieren von einfachem Multicast

### Topologie



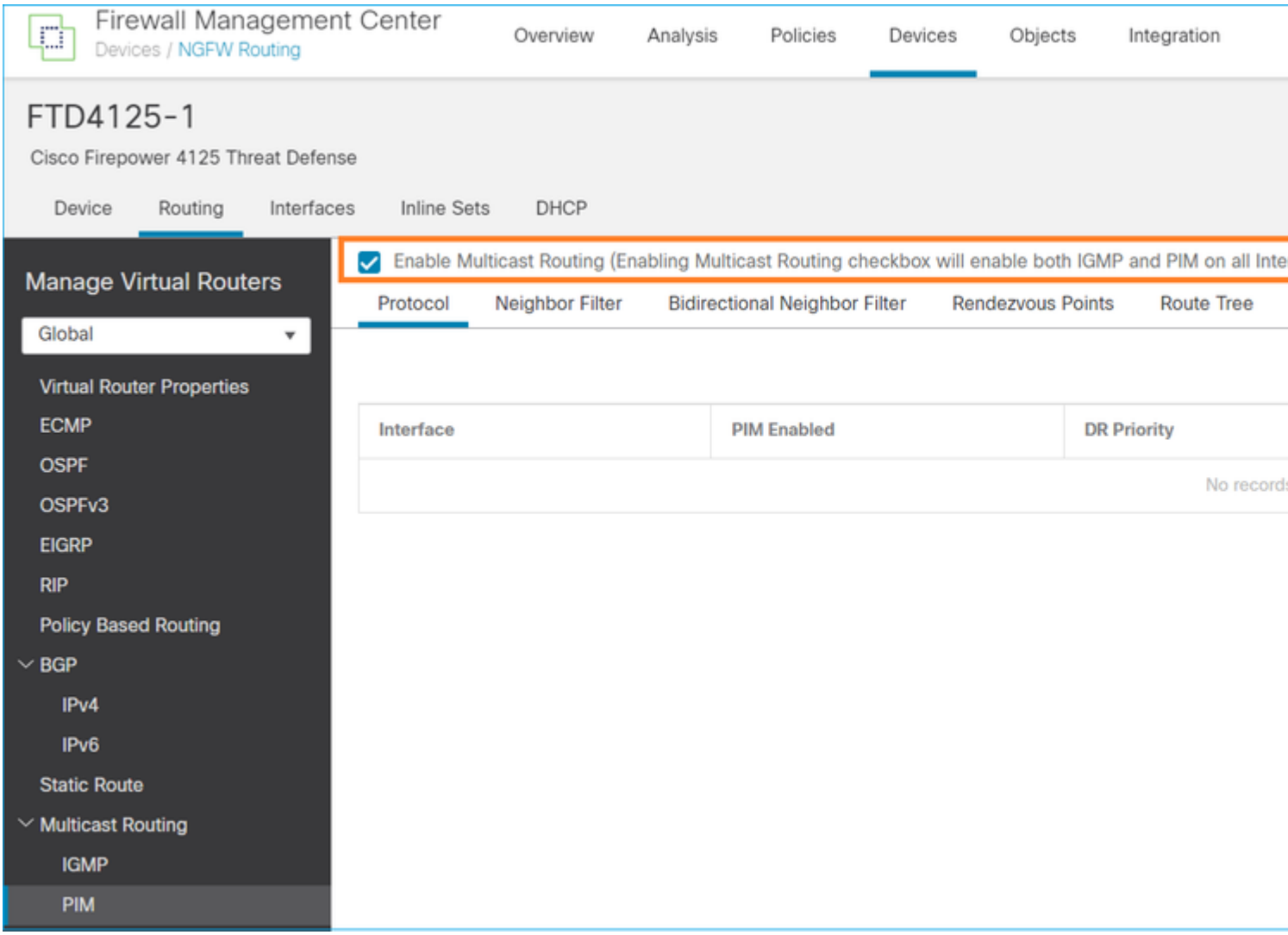

### Anforderung

Konfigurieren Sie die Firewall so, dass Multicast-Datenverkehr vom Server an den Multicast-Client unter IP 230.10.10.10 übertragen wird.

### Lösung

Aus Sicht der Firewall muss Multicast-Routing mindestens global aktiviert werden. Dadurch werden IGMP und PIM im Hintergrund auf allen Firewall-Schnittstellen aktiviert.

Auf der FMC-Benutzeroberfläche:




In der Firewall-CLI ist dies die Push-Konfiguration:

```
<#root>

firepower#

show run multicast-routing

multicast-routing

<-- Multicast routing is enabled
```

### IGMP-Verifizierung

```
<#root>

firepower#

 show igmp interface


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

**INSIDE is up, line protocol is up**

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

  **IGMP is enabled on interface**

<-- IGMP is enabled on the interface

  **Current IGMP version is 2**

<-- IGMP version
  IGMP query interval is 125 seconds
  IGMP querier timeout is 255 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1 seconds
  Inbound IGMP access group is:
  IGMP limit is 500, currently active joins: 1
  Cumulative IGMP activity: 4 joins, 3 leaves
  IGMP querying router is 192.168.1.24 (this system)

**OUTSIDE is up, line protocol is up**

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

  **IGMP is enabled on interface**

<-- IGMP is enabled on the interface

  **Current IGMP version is 2**

<-- IGMP version
  IGMP query interval is 125 seconds
  IGMP querier timeout is 255 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1 seconds
  Inbound IGMP access group is:
  IGMP limit is 500, currently active joins: 1
  Cumulative IGMP activity: 1 joins, 0 leaves
  IGMP querying router is 192.168.103.91 (this system)

<#root>

firepower#

**show igmp group**

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

<#root>

firepower#

**show igmp traffic**

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

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

Errors:
Malformed Packets           0
Martian source              0
Bad Checksums               0
```

## PIM-Verifizierung

<#root>

```
firepower#
```

**show pim interface**

```
Address          Interface          PIM  Nbr   Hello  DR         DR
                                       Count Intvl  Prior

0.0.0.0          diagnostic         off  0     30     1          not elected
192.168.1.24     INSIDE             on   0     30     1          this system
192.168.103.91   OUTSIDE            on   0     30     1          this system
```

## MFIB-Verifizierung

<#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
```

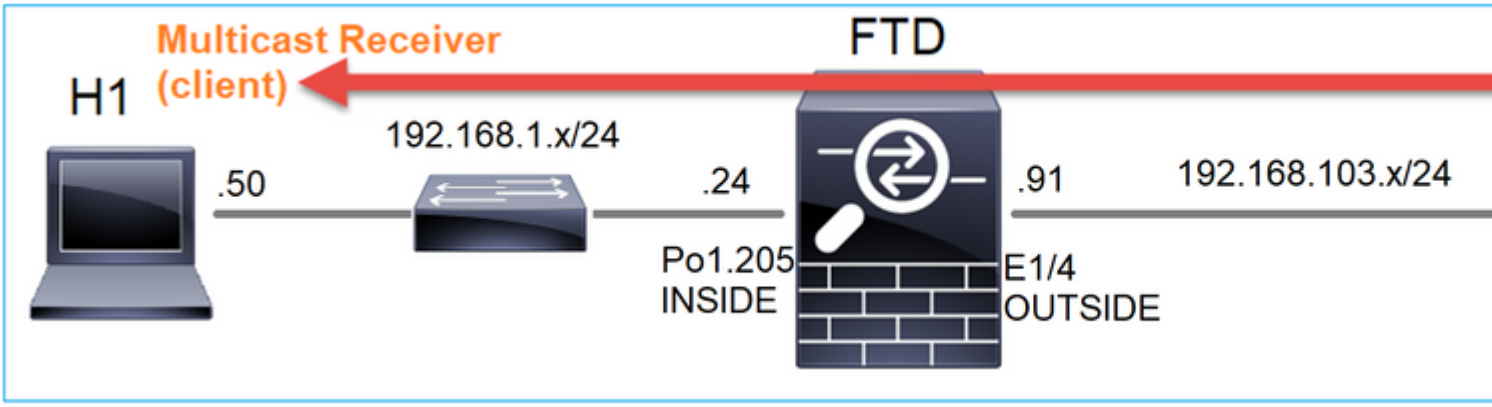
**Forwarding: 0/0/0/0**

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

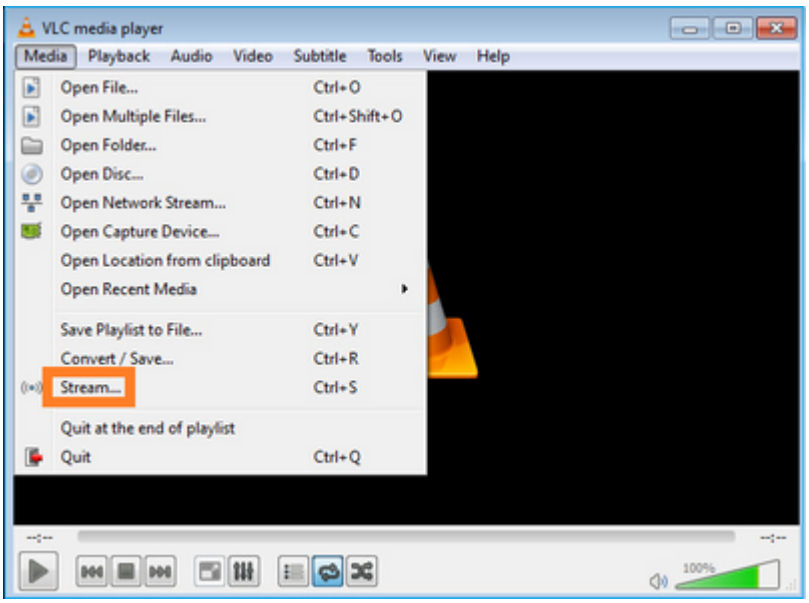
```
(*,224.0.1.40) Flags: S K
   Forwarding: 0/0/0/0,

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
```

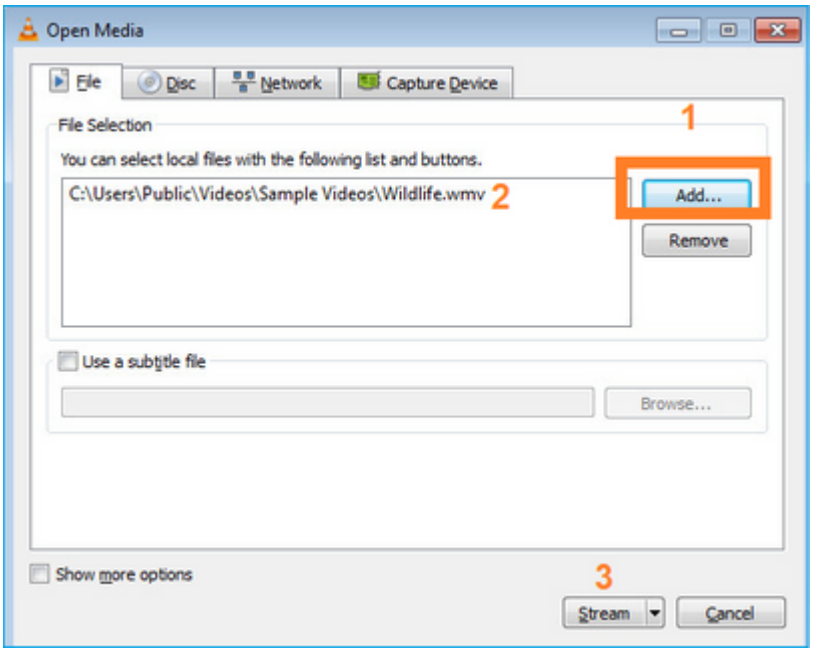
### Multicast-Verkehr durch die Firewall

In diesem Fall wird die VLC Media Player-Anwendung als Multicast-Server und Client zum Testen des Multicast-Datenverkehrs verwendet:



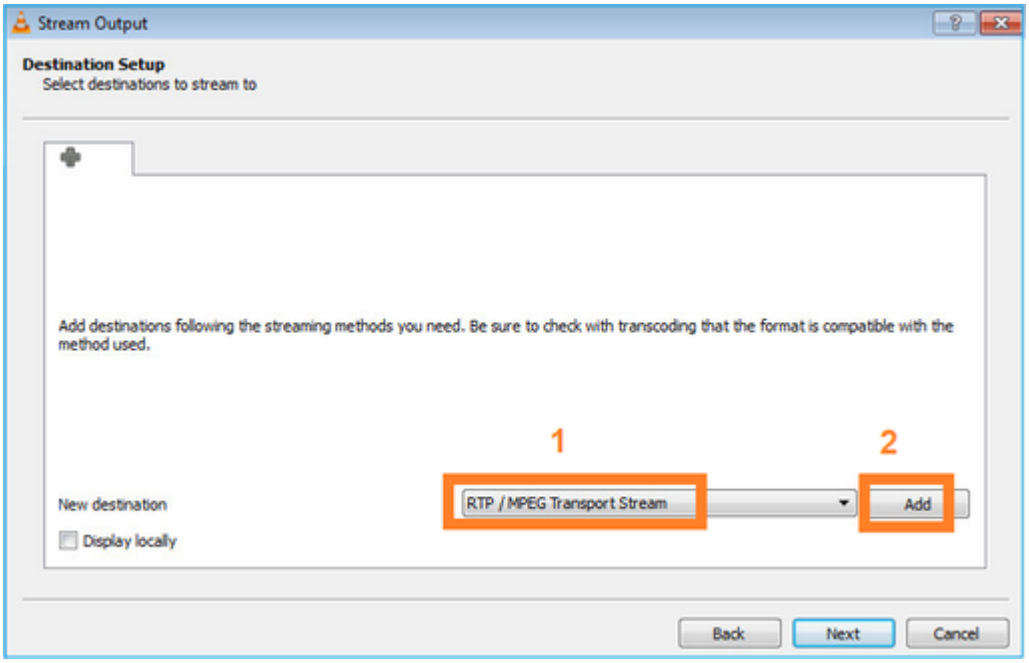

Konfiguration des VLC-Multicast-Servers:



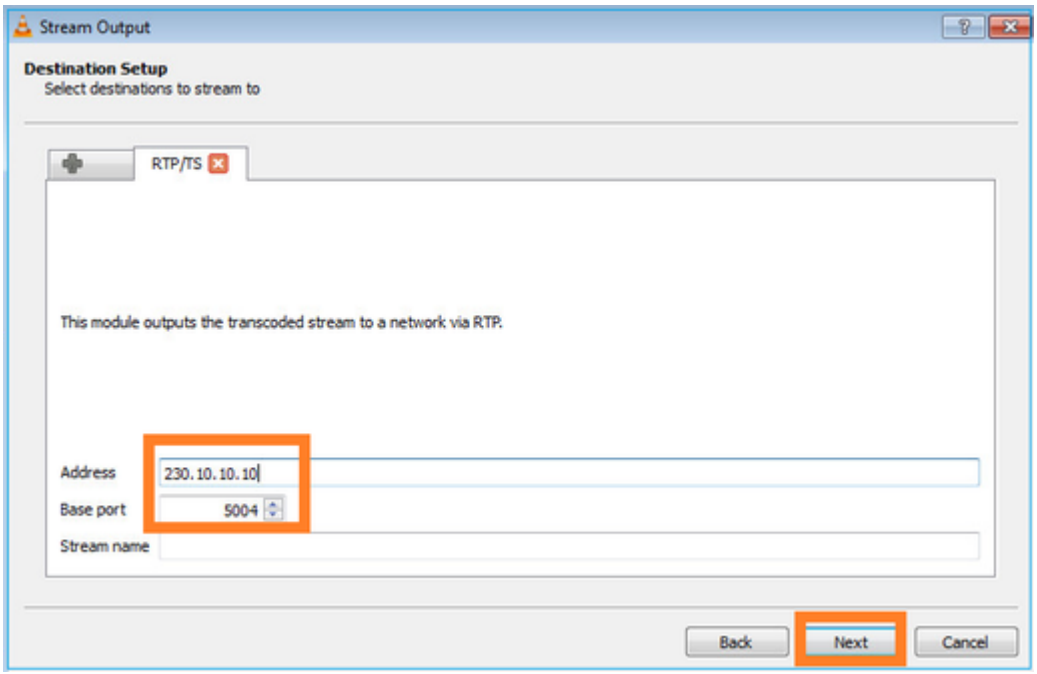


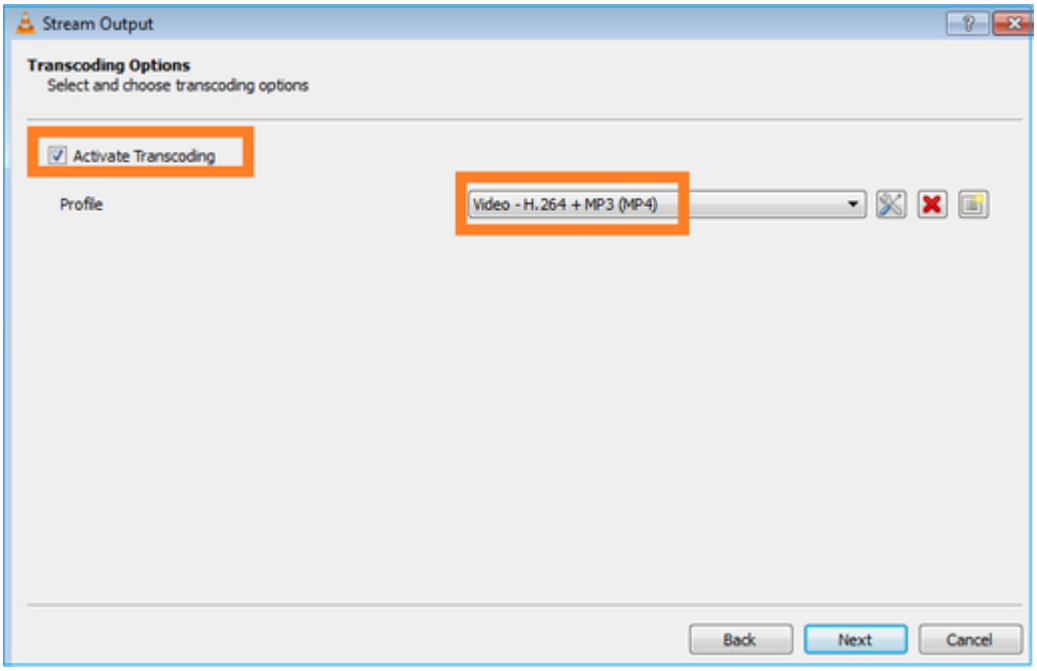

Wählen Sie auf dem nächsten Bildschirm einfach **Weiter.**

Format auswählen:




Geben Sie die Multicast-IP und den Multicast-Port an:



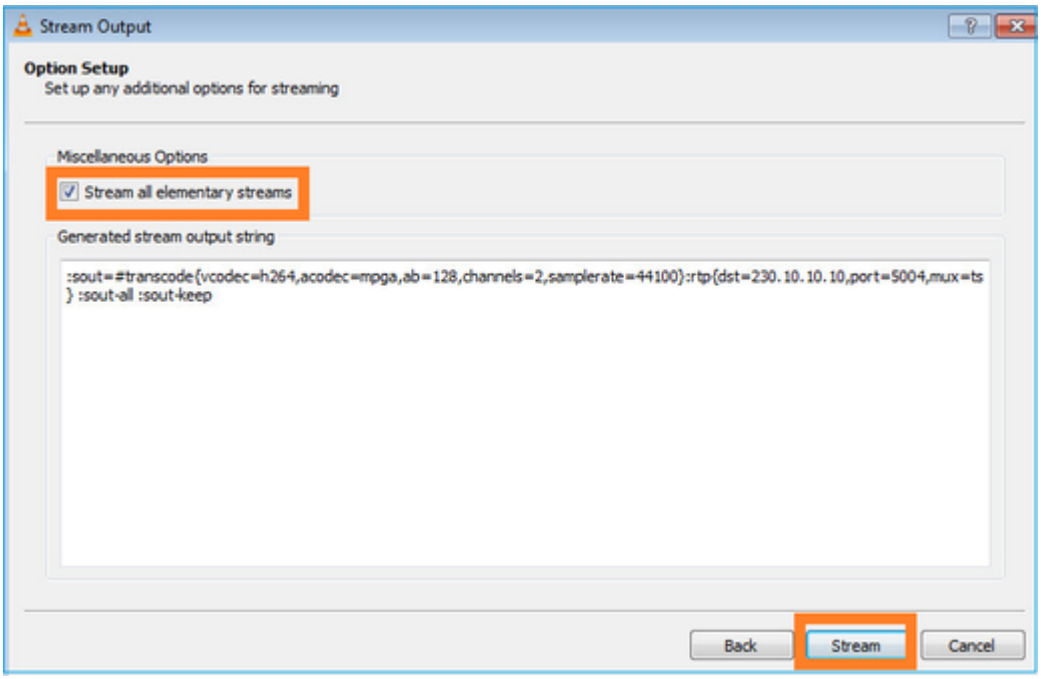




Aktivieren Sie LINA-Aufzeichnungen auf der FTD-Firewall:

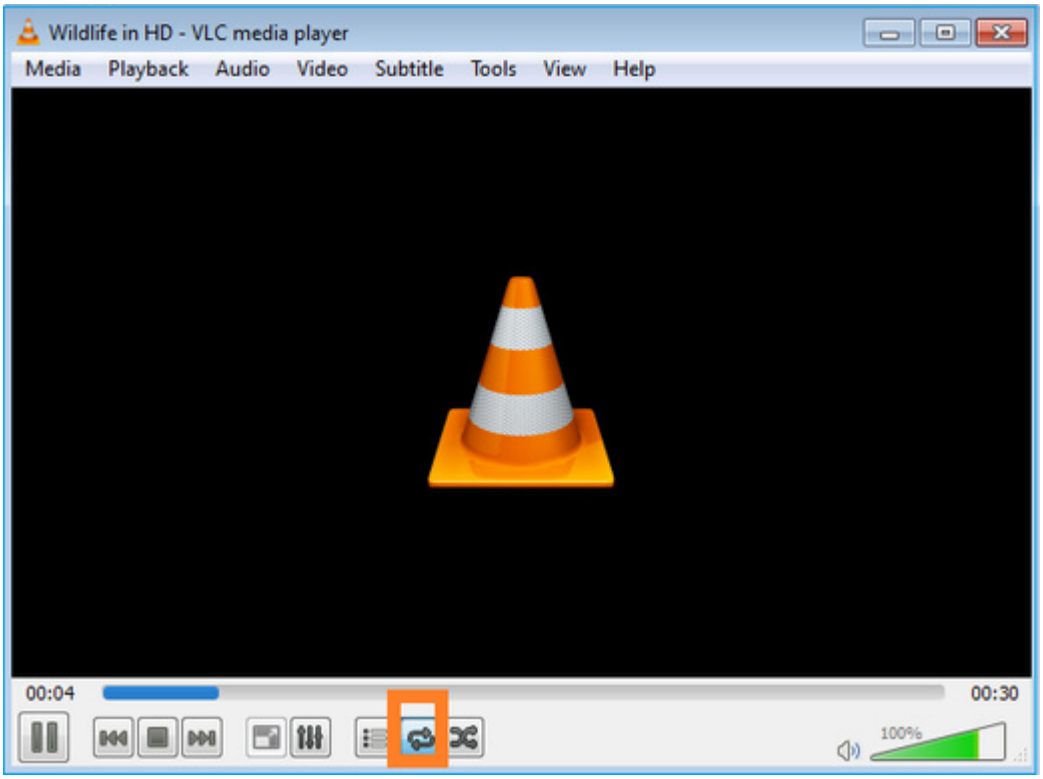
<#root>

```
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
```

Wählen Sie die **Stream**-Taste für das Gerät aus, um den Multicast-Stream zu starten:




Aktivieren Sie die Option "loop" (Schleife), damit der Stream kontinuierlich gesendet wird:




**Überprüfung (nicht betriebsbereites Szenario)**

Dieses Szenario ist eine Demonstration eines nicht betriebsbereiten Szenarios. Ziel ist es, das Verhalten der Firewall zu demonstrieren.

Das Firewall-Gerät empfängt den Multicast-Stream, leitet ihn aber nicht weiter:

<#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 zeigen:

```
<#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
```

Um ein Paket zu verfolgen, muss das erste Paket des Multicast-Flusses erfasst werden. Aus diesem Grund löschen Sie die aktuellen Ströme:

```
<#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
...
```

Die Detailoption gibt die Multicast-MAC-Adresse an:

<#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)
...
```

Die Ablaufverfolgung eines echten Pakets zeigt, dass das Paket zulässig ist. Dies ist jedoch nicht der Fall:

<#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
```

Basierend auf den mroute- und mfib-Zählern werden die Pakete verworfen, da die OIL (Outgoing Interface List) leer ist:

<#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
```

Die MFIB-Zähler zeigen RPF-Fehler an, die in diesem Fall nicht das sind, was wirklich passiert:

<#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

Ähnliche RPF-Fehler in der Ausgabe von "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

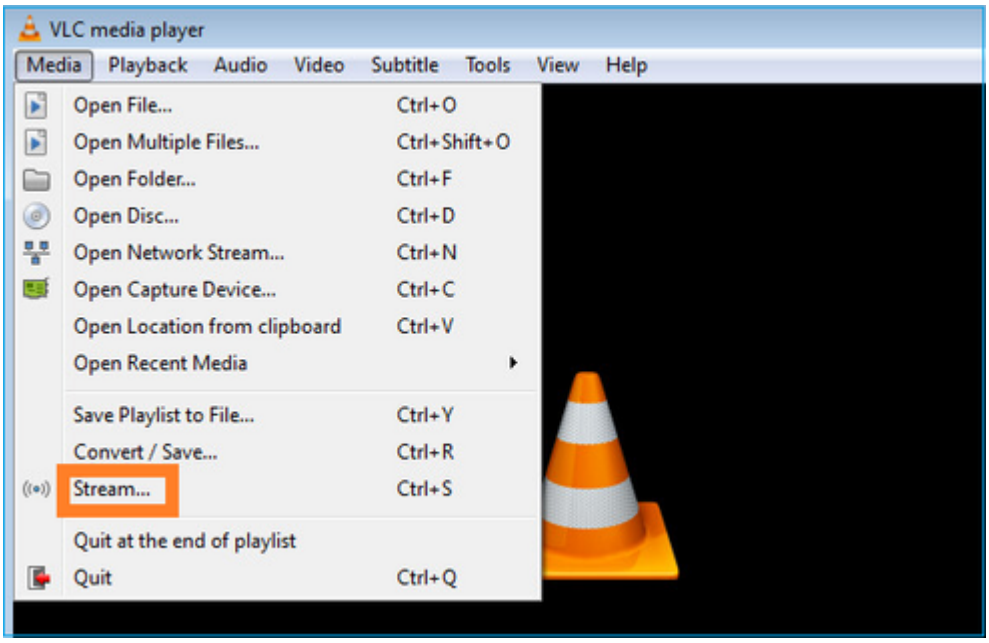
**Group: 230.10.10.10**

  Source: 192.168.103.60,
    Forwarding: 0/0/0/0,

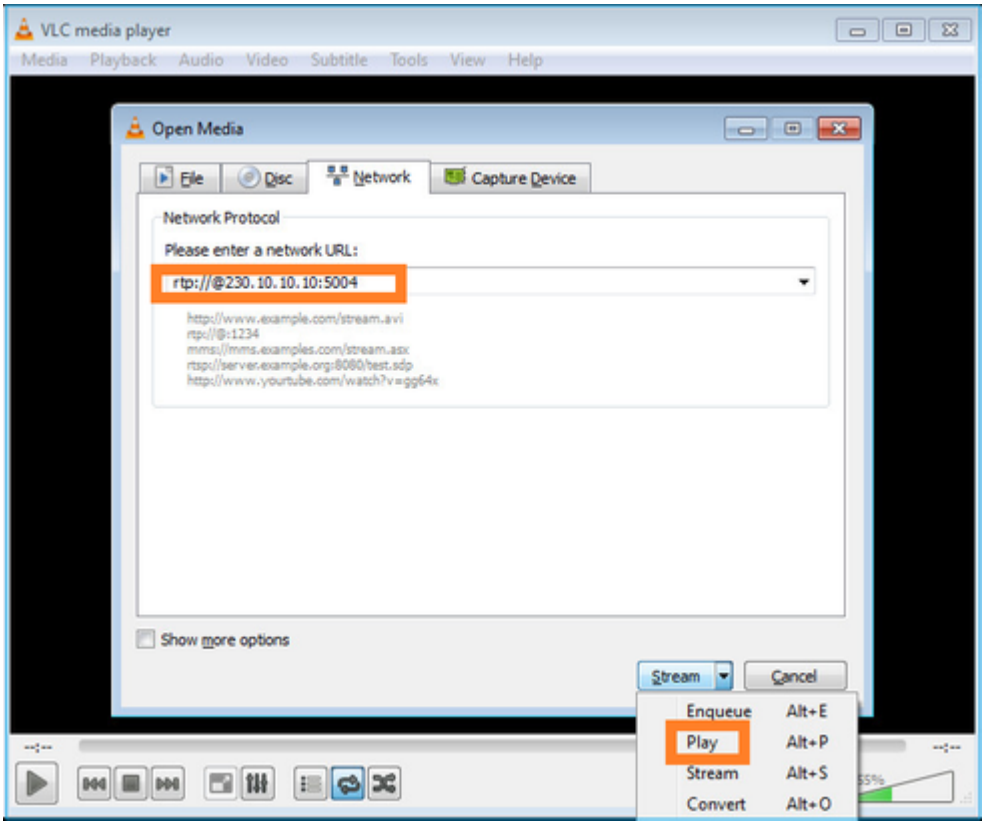
**Other: 1115/1115**

/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

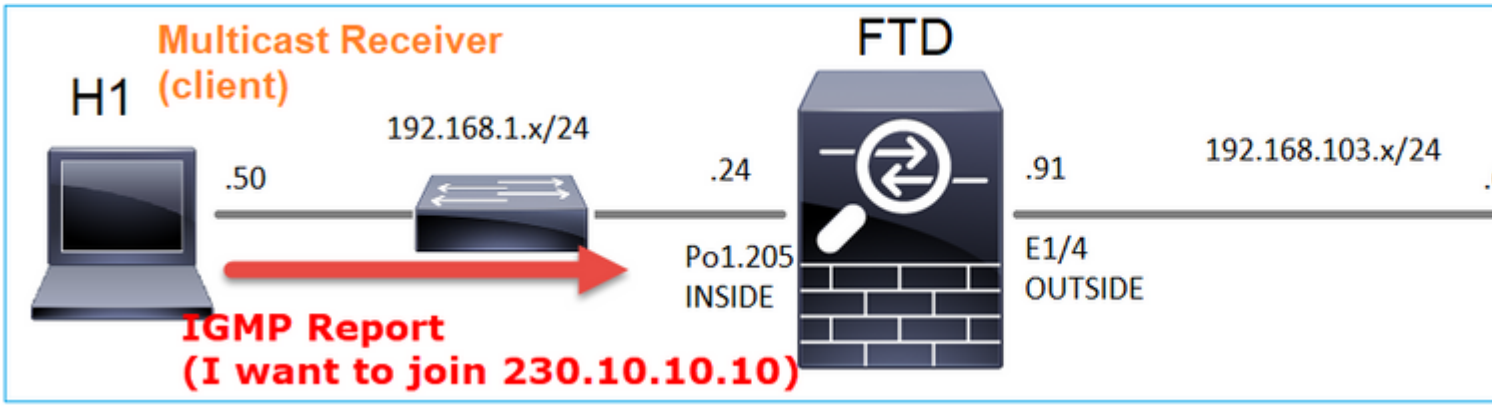
Konfigurieren Sie den VLC-Multicast-Empfänger:




Geben Sie die Multicast-Quell-IP an, und wählen Sie **Wiedergabe:**




Sobald Sie im Backend **Play** (**Wiedergabe)** auswählen, kündigt der Host seine Bereitschaft an, der spezifischen Multicast-Gruppe beizutreten, und sendet eine **IGMP-Bericht-**Nachricht:




Wenn Sie ein Debugging aktivieren, werden die IGMP-Berichtsmeldungen angezeigt:

<#root>

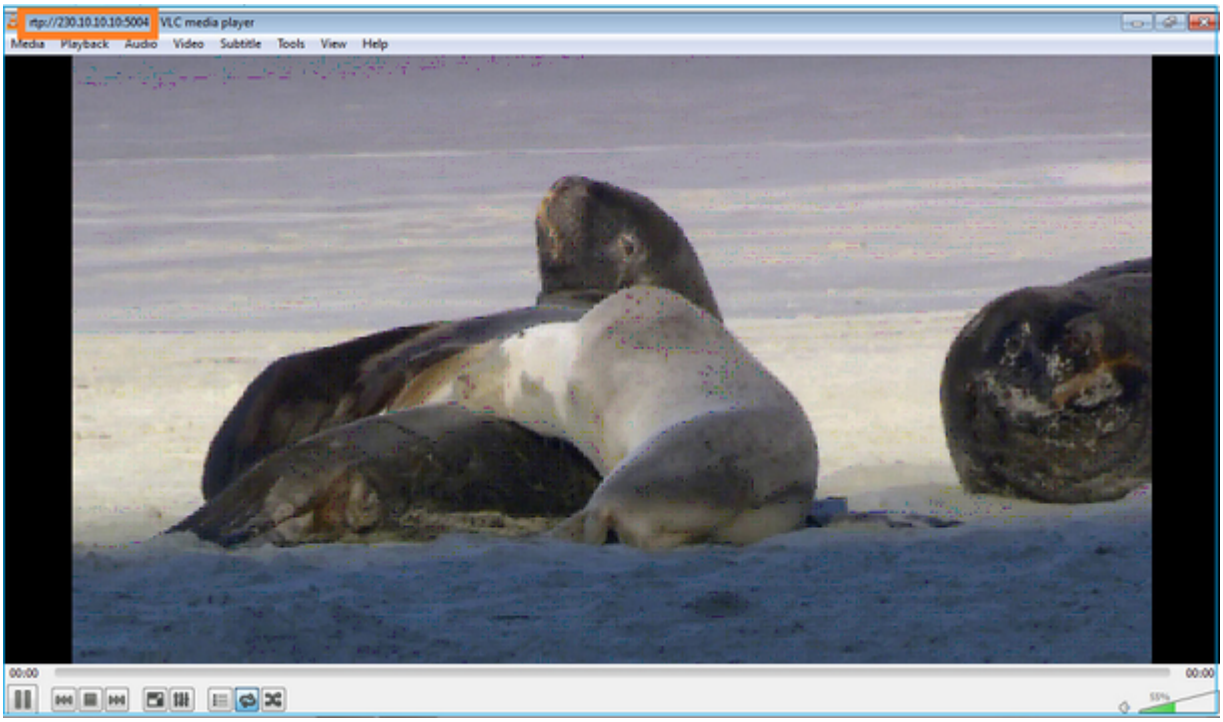
```
firepower#
```

**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
```

Der Datenstrom wird gestartet:




**Überprüfung (Betriebsszenario)**

<#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
```

Die Routing-Tabelle der 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**

MFIB-Zähler:

<#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

- IGMP-Snooping wird auf Switches verwendet, um Multicast-Flooding zu verhindern.
- Der Switch überwacht IGMP-Berichte, um festzustellen, wo sich Hosts (Empfänger) befinden.
- Der Switch überwacht IGMP-Abfragen, um festzustellen, wo sich Router/Firewalls (Absender) befinden.
- IGMP-Snooping ist auf den meisten Cisco Switches standardmäßig aktiviert. Weitere Informationen finden Sie in den entsprechenden Switching-Leitfäden. Dies ist die Beispielausgabe eines L3 Catalyst Switches:

<#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
```

## Schritt 3: IGMP static-group und IGMP join-group

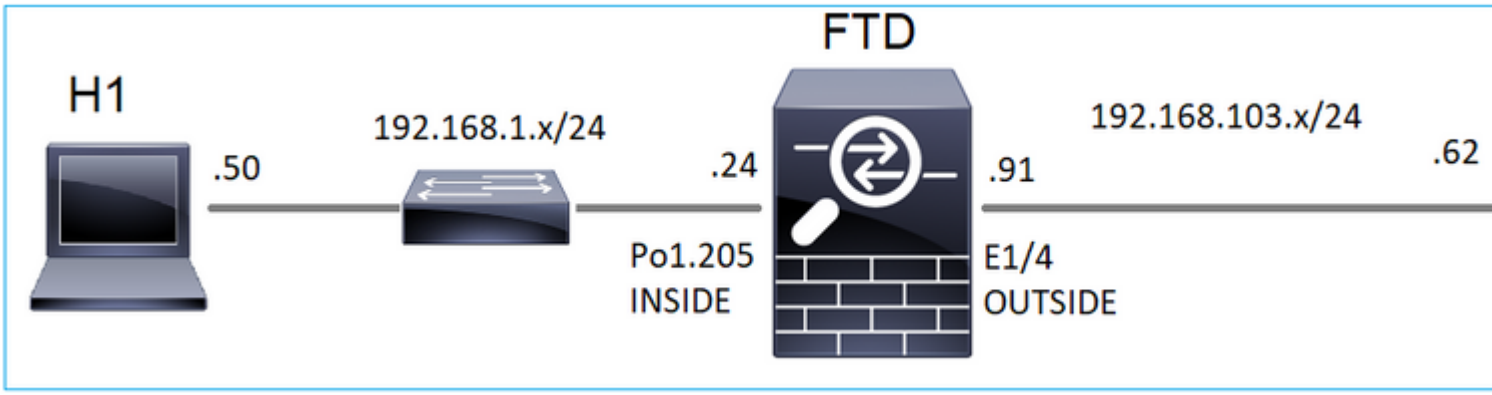
### Überblick

| | **ip igmp static-group** | **ip igmp join-group** |
|---|---|---|
| **Auf FTD-Schnittstelle angewendet?** | Ja | Ja |
| **Zieht die FTD einen Multicast-Stream an?** | Ja, eine PIM-Join wird an das Upstream-Gerät, die Quelle oder an den Rendezvous Point (RP) gesendet. Dies ist nur der Fall, wenn es sich bei dem FTD mit diesem Befehl um den PIM Designated Router (DR) an dieser Schnittstelle handelt. | Ja, eine PIM-Join wird an das Upstream-Gerät, die Quelle oder an den Rendezvous Point (RP) gesendet. Dies ist nur der Fall, wenn es sich bei dem FTD mit diesem Befehl um den PIM Designated Router (DR) an dieser Schnittstelle handelt. |
| **Leitet das FTD Multicast-Datenverkehr von der Schnittstelle weiter?** | Ja | Ja |
| **Nutzt die FTD den Multicast-Datenverkehr und antwortet sie darauf?** | Nein | Ja, die FTD analysiert den Multicast-Stream an die CPU, nutzt ihn und antwortet an die Quelle. |

| | | |
|---|---|---|
| **CPU-Auswirkung** | Minimal, da das Paket nicht an die CPU gesendet wird. | Kann die FTD-CPU beeinflussen, da jedes Multicast-Paket, das zu der Gruppe gehört, an die FTD-CPU gesendet wird. |

**Voraussetzung für diese Aufgabe**

Betrachten Sie diese Topologie:




Aktivieren Sie auf der Firewall die folgenden Funktionen:

```
<#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. Verwenden Sie den ICMP-Ping vom L3-Switch, um Multicast-Datenverkehr an die IP 230.11.11.11 zu senden und zu überprüfen, wie die Firewall damit umgeht.
2. Aktivieren Sie den Befehl **igmp static-group** an der Firewall INSIDE-Schnittstelle, und überprüfen Sie, wie der Multicast-Stream (IP 230.11.11.11) von der Firewall verarbeitet wird.
3. Aktivieren Sie den Befehl **igmp static-group** an der Firewall INSIDE-Schnittstelle, und überprüfen Sie, wie der Multicast-Stream (IP 230.11.11.11) von der Firewall verarbeitet wird.

**Lösung**

Die Firewall verfügt über keine Routen für die 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
```

Eine einfache Möglichkeit zum Testen von Multicast ist die Verwendung des ICMP-Ping-Tools. Starten Sie in diesem Fall einen Ping vom R2 zur Multicast-IP-Adresse 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:
.............................
```

Auf der Firewall wird dynamisch eine Route erstellt, und das OIL ist leer:

<#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
```

Die Erfassung auf der Firewall zeigt Folgendes:

<#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

Die Firewall erstellt für jeden Ping eine Verbindung, verwirft jedoch die Pakete unbeaufsichtigt:

<#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

---

**Hinweis:** Bei der LINA ASP-Abwurfaufzeichnung werden die verworfenen Pakete nicht angezeigt.

---

Der Hauptindikator für das Verwerfen von Multicast-Paketen ist:

<#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)**

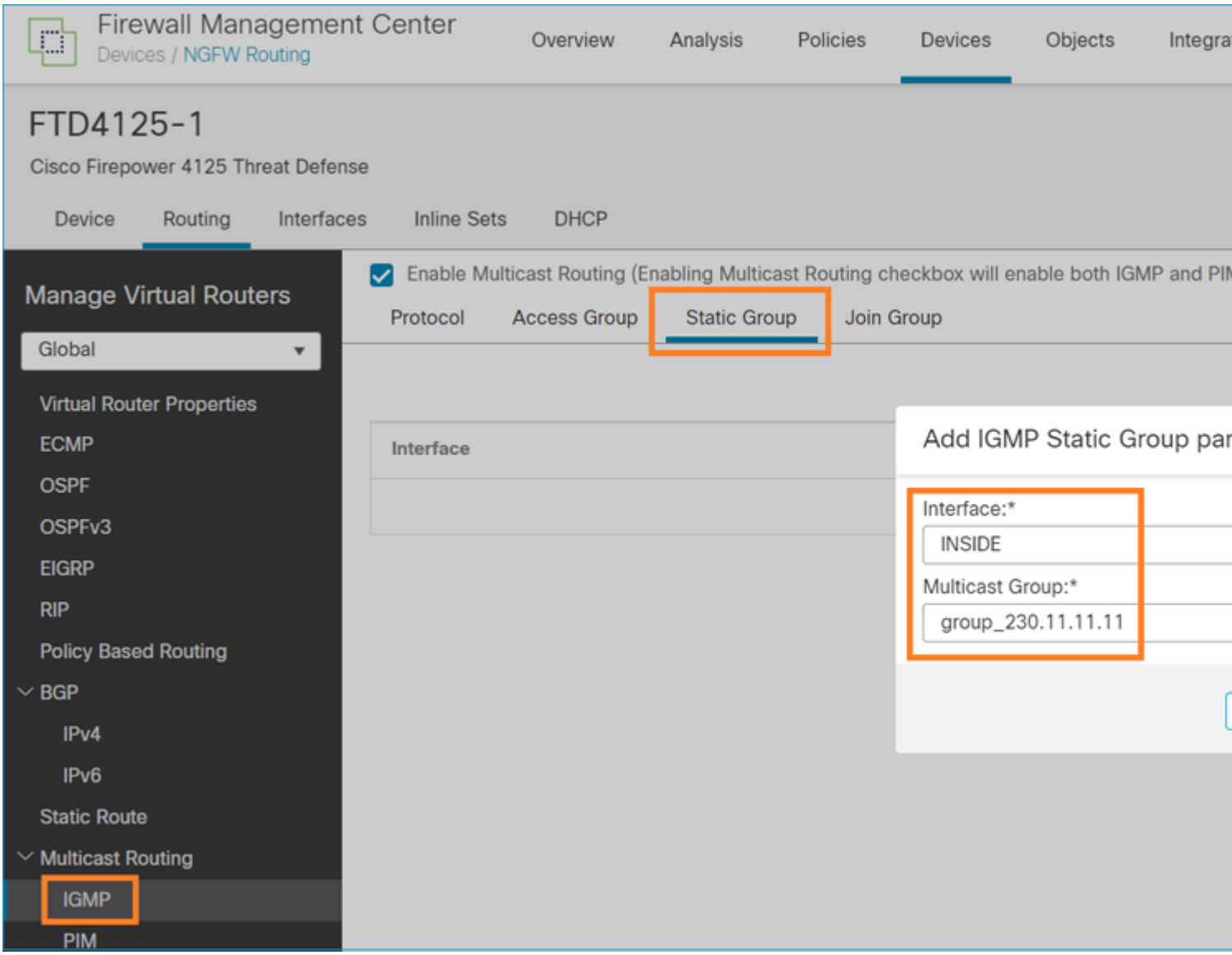
```
 Flags: K         <-- The multicast stream
  Forwarding: 0/0/0/0,
```

**Other: 27/27/0**

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

### igmp static-group

Konfigurieren Sie auf FMC eine statische IGMP-Gruppe:




Im Hintergrund wird Folgendes bereitgestellt:

<#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
```

Der Ping schlägt fehl, aber der ICMP-Multicast-Verkehr wird nun durch die Firewall weitergeleitet:

<#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
```

---

**Hinweis**: Die Ablaufverfolgung des Pakets zeigt eine falsche Ausgabe an (die Eingangsschnittstelle ist mit der Ausgangsschnittstelle identisch). Weitere Informationen finden Sie unter Cisco Bug ID 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

---

**Tipp:** Sie können einen Ping mit Timeout 0 vom Quellhost senden und die Firewall-Konfigurationszähler überprüfen:

---

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

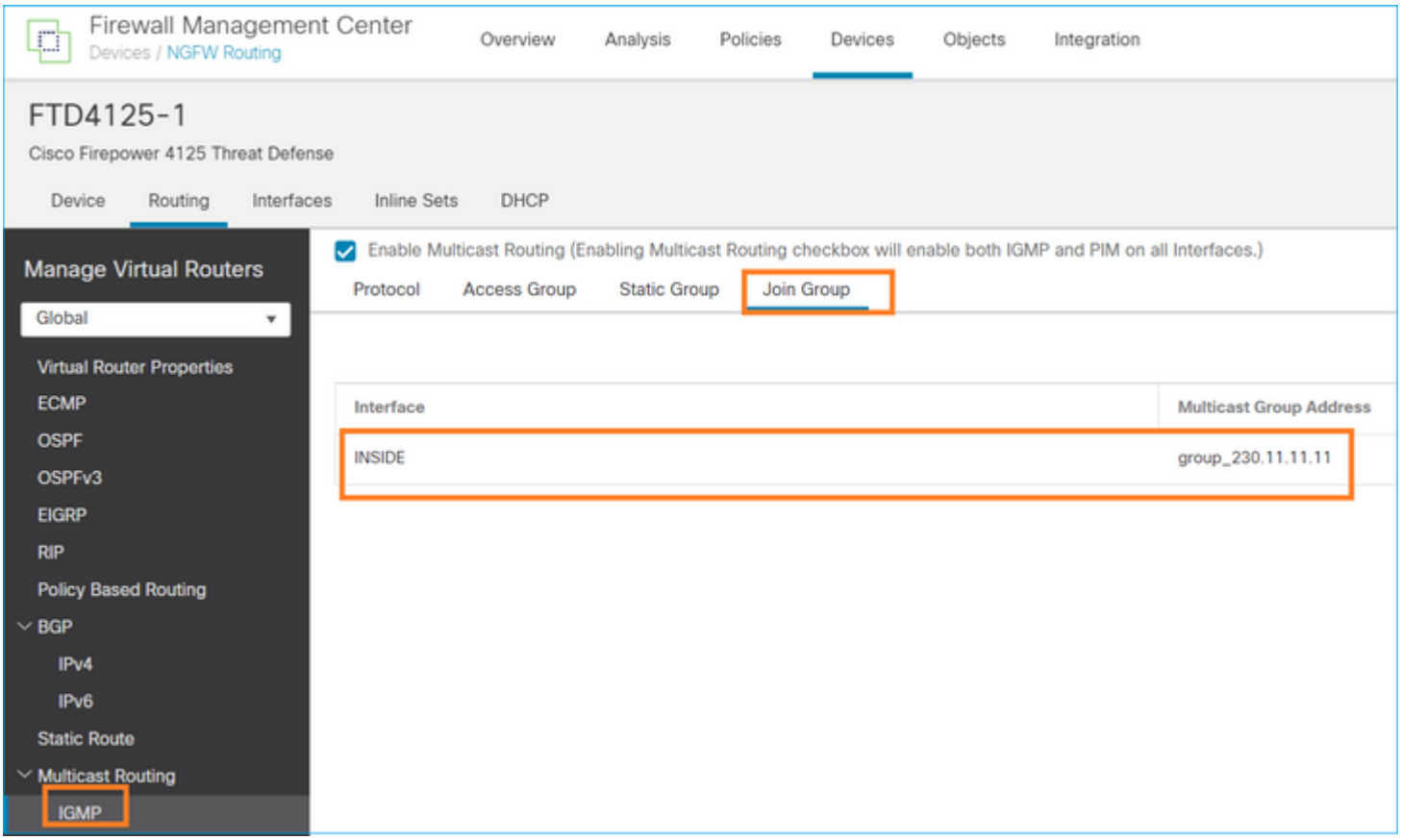
```
.....................
```

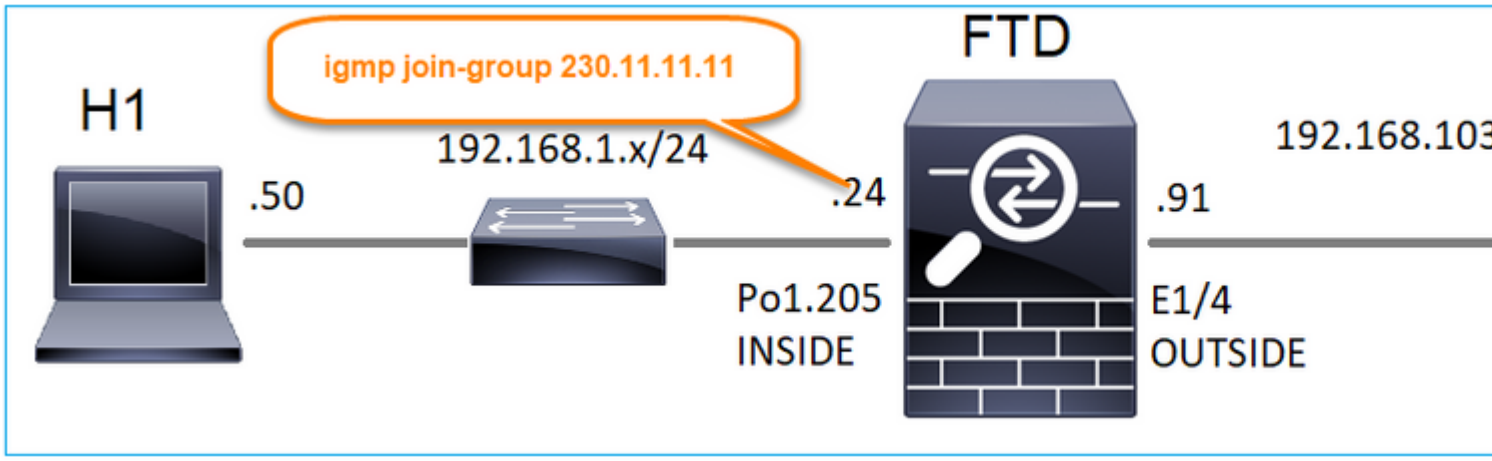
<#root>

```
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-Gruppe

Auf FMC-Remote-Server die zuvor konfigurierte statische Gruppe konfigurieren und eine IGMP-Beitrittsgruppe konfigurieren:




Die bereitgestellte Konfiguration:

<#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
```

Die IGMP-Gruppe:

<#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
```

Testen Sie vom Quellhost aus den ersten ICMP-Multicast-Test in Richtung 230.11.11.11 IP:

<#root>

```
L3-Switch#
```

**ping 230.11.11.11 repeat 10**

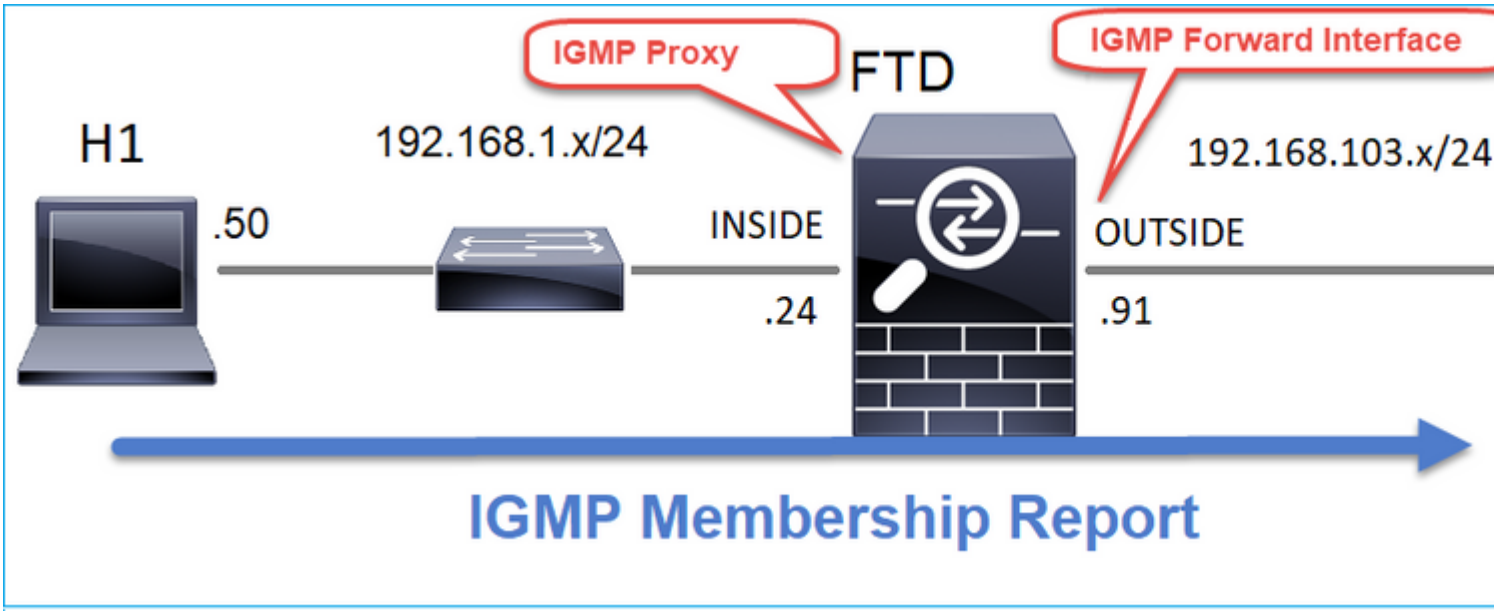
```
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 230.11.11.11, timeout is 2 seconds:

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
```

---

**Hinweis**: Wenn nicht alle Antworten angezeigt werden, überprüfen Sie die Cisco Bug-ID CSCvm90069.

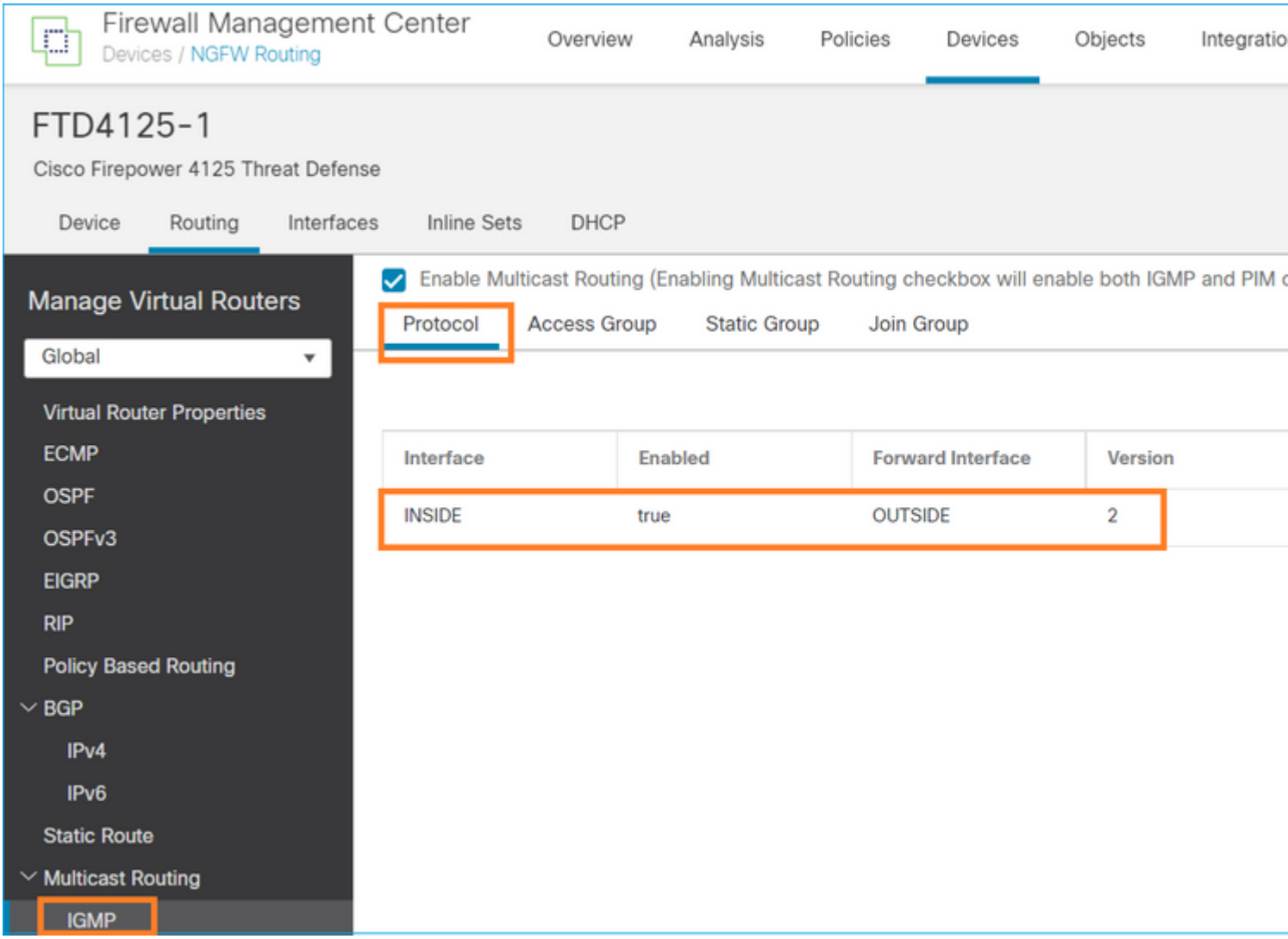
---

## Schritt 4: Konfigurieren von IGMP-Stub-Multicast-Routing




Konfigurieren Sie das Stub-Multicast-Routing auf FTD so, dass auf der INSIDE-Schnittstelle empfangene IGMP-Membership-Report-Meldungen an die OUTSIDE-Schnittstelle weitergeleitet werden.

**Lösung**



Die bereitgestellte Konfiguration:

```
<#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
```

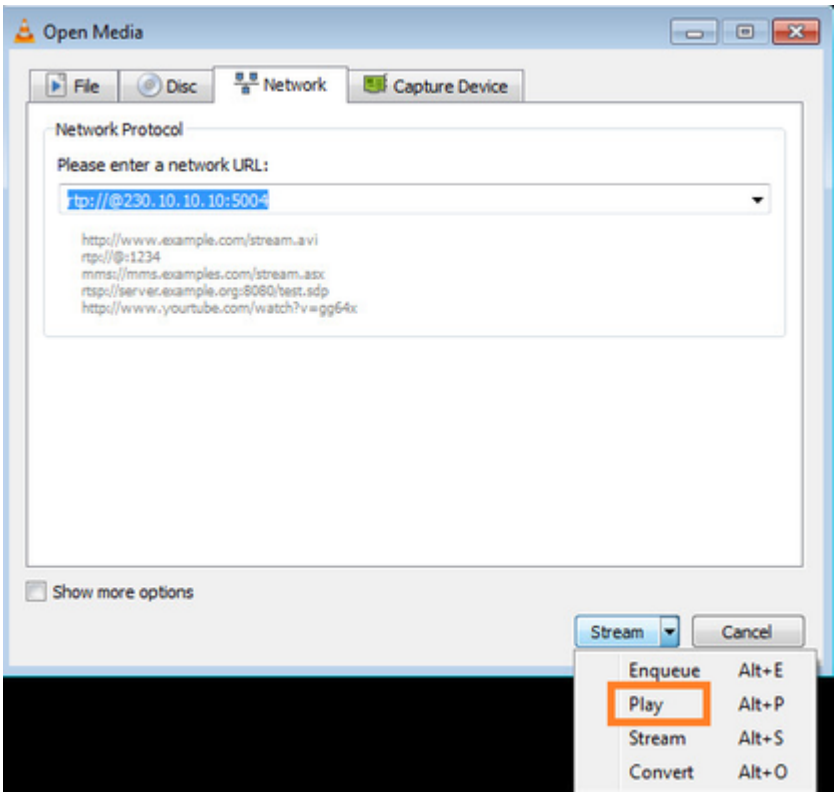
### Verifizierung

Erfassung auf FTD aktivieren:

```
<#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
```

### Verifizierung

Um einen IGMP-Mitgliedschaftsbericht zu erzwingen, können Sie eine Anwendung wie VLC verwenden:




Der FTD leitet die IGMP-Pakete weiter:

<#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
```

Die FTD ändert die Quell-IP:

<#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
```

Wenn Sie die pcap in Wireshark überprüfen, können Sie sehen, dass das Paket vollständig von der Firewall neu generiert wird (die IP-Identifikation ändert sich).

Ein Gruppeneintrag wird auf FTD erstellt:

<#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
```

Die FTD-Firewall erstellt zwei Verbindungen auf Kontrollebene:

<#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
```

Nachverfolgung des ersten Pakets:

<#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)

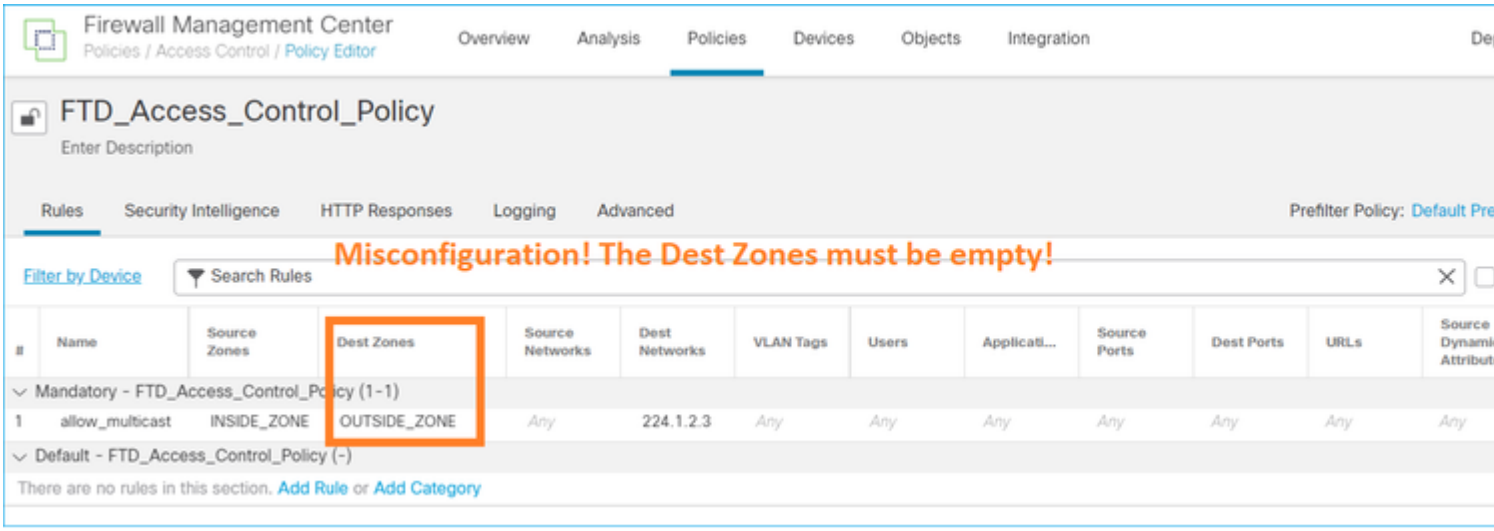
Phase: 13
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 9760 ns

```
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
```

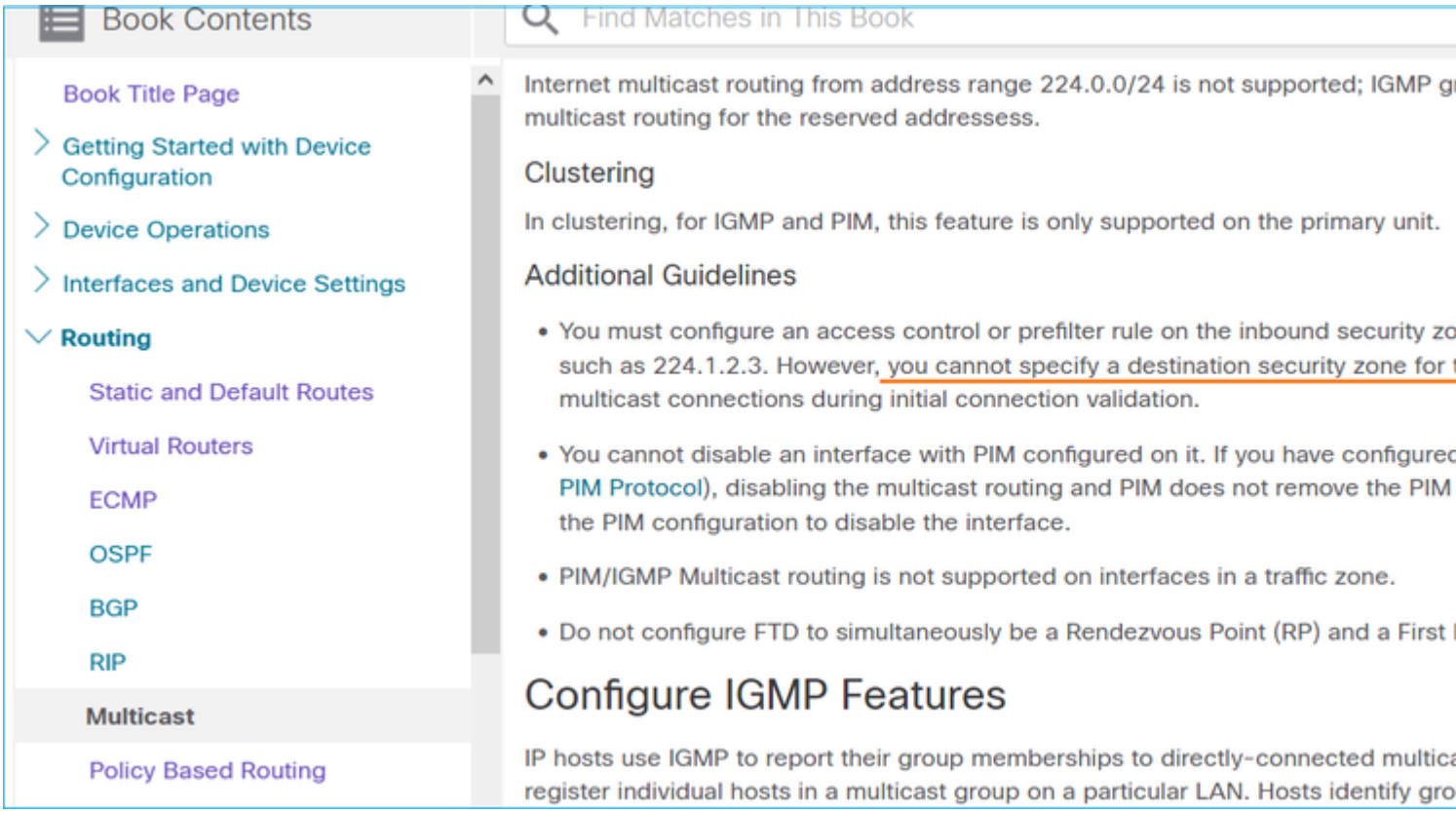
# Bekannte Probleme

## Filtern von Multicast-Datenverkehr in Zielzonen

Sie können keine Zielsicherheitszone für die Zugriffssteuerungsrichtlinienregel angeben, die mit dem Multicast-Verkehr übereinstimmt:




Dies wird auch im FMC-Benutzerhandbuch dokumentiert:




## IGMP-Berichte werden von der Firewall abgelehnt, wenn der IGMP-Schnittstellengrenzwert überschritten wird

Standardmäßig lässt die Firewall maximal 500 aktive Joins (Berichte) auf einer Schnittstelle zu. Wenn dieser Grenzwert überschritten wird, ignoriert die Firewall zusätzliche eingehende IGMP-Berichte von den Multicast-Empfängern.

Um die IGMP-Beschränkung und die aktiven Joins zu überprüfen, führen Sie den Befehl **show igmp interface *name* aus**:

```
<#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)
```

Der IGMP-Debug-Befehl **debug igmp** zeigt folgende Ausgabe an:

```
<#root>

asa#

debug igmp

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

Cisco Bug-ID CSCuw84390 verfolgt die Erweiterung, um den IGMP-Grenzwert zu erhöhen.

### Die Firewall ignoriert IGMP-Berichte für den Adressbereich 232.x.x.x/8.

Der Adressbereich 232.x.x.x/8 ist für Source Specific Multicast (SSM) vorgesehen. Die Firewall unterstützt weder die PIM Source Specific Multicast (SSM)-Funktion noch die zugehörige Konfiguration.

Der IGMP-Debug-Befehl **debug igmp** zeigt folgende Ausgabe an:

```
<#root>

asa#

debug igmp

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

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

Cisco Bug-ID CSCsr53916 verfolgt die Erweiterung zur Unterstützung des SSM-Bereichs.

## Zugehörige Informationen

- Multicast-Routing für Firepower Threat Defense
- Fehlerbehebung bei Firepower Threat Defense und ASA Multicast PIM

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.