أستكشاف أخطاء بروتوكول إدارة مجموعات الإنترنت (IGMP) وبروتوكولات البث المتعدد الخاصة بالدفاع عن تهديد FirePOWER وإصلاحها

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

معلومات أساسية

التكوين

أساسيات IGMP

المهمة 1 - حركة مرور البث المتعدد لمستوى التحكم

المهمة 2 - تكوين البث المتعدد الأساسي

استطلاع بروتوكول إدارة مجموعات الإنترنت (IGMP)

المهمة 3 - المجموعة الثابتة لبروتوكول إدارة مجموعات الإنترنت (IGMP) مقابل مجموعة الانضمام إلى بروتوكول إدارة مجموعات الإنترنت (IGMP)

مجموعة IGMP الثابتة

مجموعة انضمام IGMP

المهمة 4 - تكوين التوجيه متعدد البث لبروتوكول IGMP الجذري

مشكلات معروفة

تصفية حركة مرور البث المتعدد على مناطق الوجهة

يتم رفض تقارير IGMP بواسطة جدار الحماية عند تجاوز حد واجهة IGMP

يتجاهل جدار الحماية تقارير IGMP لنطاق العناوين 232.x.x/8

معلومات ذات صلة

المقدمة

يصف هذا المستند أساسيات البث المتعدد وكيفية تنفيذ الدفاع ضد تهديد FirePOWER (FTD) لبروتوكول إدارة مجموعة الإنترنت (IGMP).

المتطلبات الأساسية

المتطلبات

معرفة توجيه IP الأساسية.

المكونات المستخدمة

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

ينطبق محتوى هذه المقالة أيضا على برنامج أجهزة الأمان المعدلة (ASA).

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- الدفاع ضد التهديد Cisco Firepower 4125، الإصدار 7.1.0.
- مركز إدارة Firepower (FMC)، الإصدار 7.1.0.
- ASA الإصدار 9.19.1.

معلومات أساسية

التعاريف

- Unicast = من مضيف واحد إلى مضيف آخر (واحد إلى واحد).
- Broadcast = من مضيف واحد إلى جميع البيئات المضيفة المحتملة (واحد إلى الكل).
- البث المتعدد = من مضيف مجموعة من الأجهزة المضيفة إلى مجموعة من الأجهزة المضيفة (واحد إلى كثير وأ كثير إلى كثير).
- AnyCast = من مضيف إلى أقرب مضيف لمجموعة (واحد إلى واحد من عدة).

أساسيات

- تمت كتابة RFC 988 للبث المتعدد في عام 1986 بواسطة ستيف ديرينج.
- يستخدم البث المتعدد ل IPv4 النطاق 224.0.0.0/4 (أول 4 وحدات بت 1110) - 224.0.0.0 - 239.255.255.255.
- بالنسبة ل IPv4، يستمد عنوان MAC من L2 بروتوكول IP للبث المتعدد من L3: 01005e (24 وحدة بت) + 25وحدة بت دائما 0 + 23 وحدة بت أقل من عنوان IPv4 للبث المتعدد.
- يستخدم البث المتعدد ل IPv6 النطاق FF00:/8 وهو أكثر مرونة من البث المتعدد ل IPv4 نظرا لأنه يمكن تضمين بروتوكول الإنترنت لنقطة الالتقاء (RP).
- بالنسبة ل IPv6، يستمد عنوان MAC من البث المتعدد للمستوى 3: 3333 + 32 بت أقل من عنوان IPv6 للبث المتعدد.
- ميزات البث المتعدد: الكفاءة الناتجة عن انخفاض الحمل على المصدر. الأداء، نظرا لأنه يجنبان إزدواجية حركة المرور وأ فيضانها.
- عيوب البث المتعدد: نقل غير موثوق به (يستند إلى UDP)، عدم تجنب الازدحام، التسليم خارج التسلسل.
- ال يتم دعم البث المتعدد على الإنترنت العام لأنه يتطلب جميع الأجهزة الموجودة في المسار لتمكينه. يستخدم عادة عندما تكون جميع الأجهزة تحت سلطة إدارية مشتركة.
- تطبيقات البث المتعدد النموذجية: بث فيديو داخلي وعقد مؤتمرات فيديو.

البث المتعدد مقابل البث الأحادي المنسوخ

في Unicast منسوخ نسخا متماثلا يشيء المصدر نسخ متعددة من نفس حزمة البث الأحادي (نسخة طبق الأصل) ويرسلها إلى مضيف وجهة متعددة. يعمل البث المتعدد على

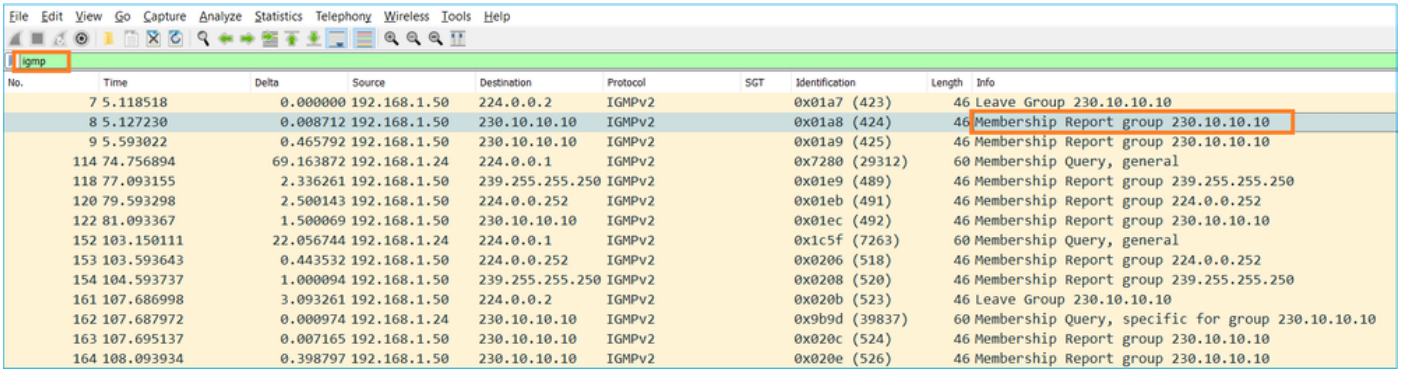
نقل العبء من المضيف المصدر إلى الشبكة، بينما في البث الأحادي المنسوخ نسخا متماثلا يتم تنفيذ كل العمل على المضيف المصدر.

التكوين

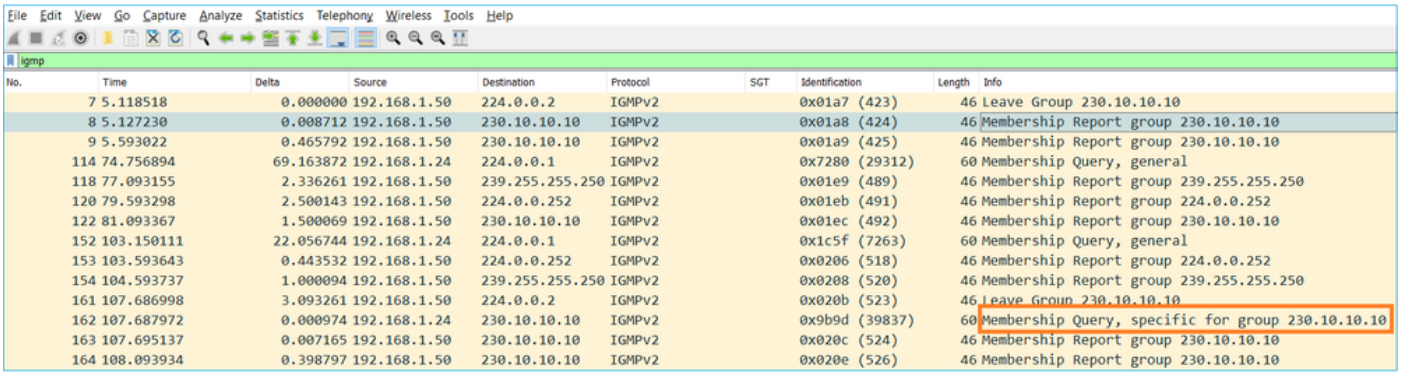
أساسيات IGMP

- IGMP هي "اللغة" التي يتم التحدث بها بين أجهزة إستقبال البث المتعدد وجهاز L3 المحلي (عادة ما يكون موجها).
- IGMP هو بروتوكول من الطبقة 3 (مثل ICMP) ويستخدم بروتوكول IP رقم 2.
- هناك حاليا 3 إصدارات IGMP. إصدار IGMP الافتراضي على جدار الحماية هو الإصدار 2. يتم دعم الإصدارين 1 و 2 فقط حاليا.
- بين IGMPv1 و IGMPv2 الفروق الرئيسية هي:
    - لا يحتوي IGMPv1 على رسالة Leave Group.
    - لا يحتوي IGMPv1 على استعلام خاص بالمجموعة (يتم إستخدامه بواسطة جدار الحماية عندما يترك مضيف مجموعة بث متعدد).
    - لا يحتوي IGMPv1 على أي عملية إختيار للاستعلام.

- لا يتم حاليا دعم IGMPv3 على ASA/FTD، ولكن كمرجع، يكمن الاختلاف المهم بين IGMPv2 و IGMPv3 في تضمين استعلام خاص بالمجموعة والمصدر في IGMPv3 الذي يتم إستخدامه في البث المتعدد محدد المصدر (SSM).
- استعلامات IGMPv1/IGMPv2/IGMPv3 = 224.0.0.1
  إجازة IGMPv2 = 224.0.0.2
  تقرير عضوية IGMPv3 = 224.0.0.22
- إذا أراد المضيف الانضمام، فيمكنه إرسال رسالة تقرير عضوية IGMP غير المرغوب فيها:



- من وجهة نظر جدار الحماية، يوجد نوعان من استعلامات IGMP: استعلامات عامة واستعلامات خاصة بالمجموعة
- عندما يستقبل جدار الحماية رسالة IGMP Leave Group، يجب التحقق مما إذا كان هناك أعضاء آخرون في هذه المجموعة على الشبكة الفرعية. لهذا السبب، يرسل جدار الحماية استعلاما خاصا بالمجموعة:



- على الشبكات الفرعية التي يوجد بها العديد من المومجهات/جدران الحماية، يتم إختيار مستعلم (جهاز يرسل جميع استعلامات 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
```

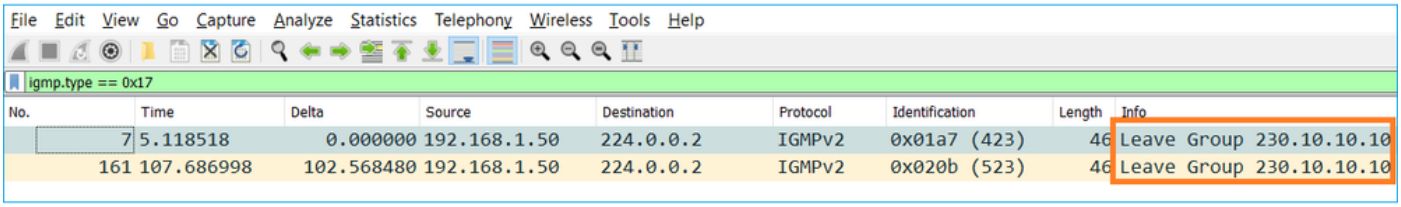
- في FTD، على غرار ASA التقليدي، يمكنك تمكين debug igmp لعرض الرسائل المتعلقة ب IGMP:

<#root>

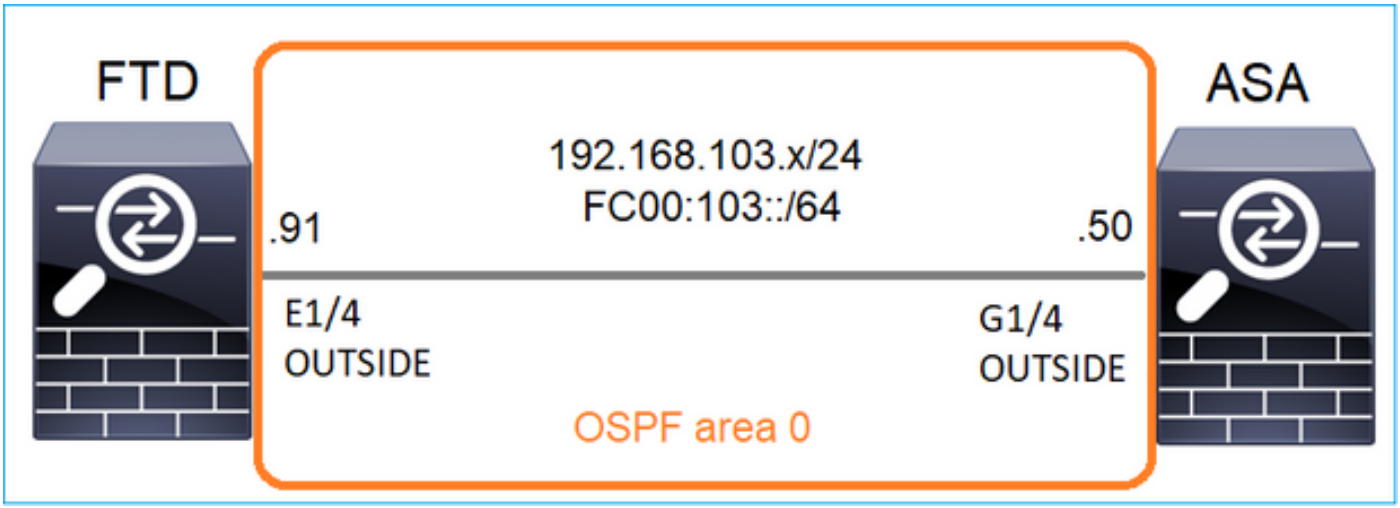
```
firepower#

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
```

- يترك المضيف عادة مجموعة البث المتعدد مع رسالة ترك مجموعة (IGMPv2).



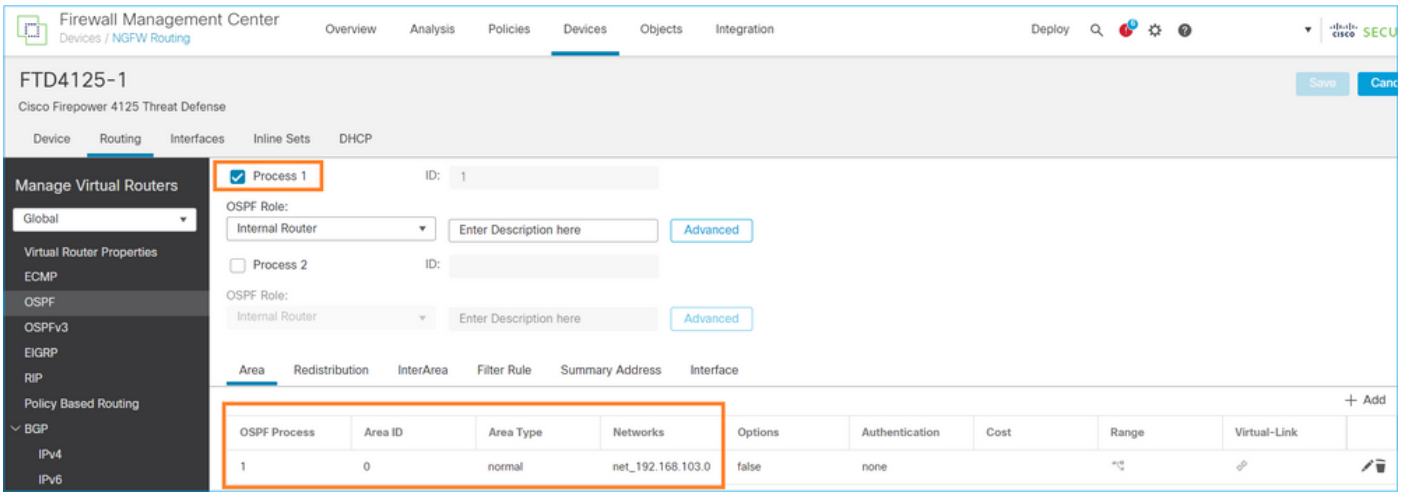
المهمة 1 - حركة مرور البث المتعدد لمستوى التحكم

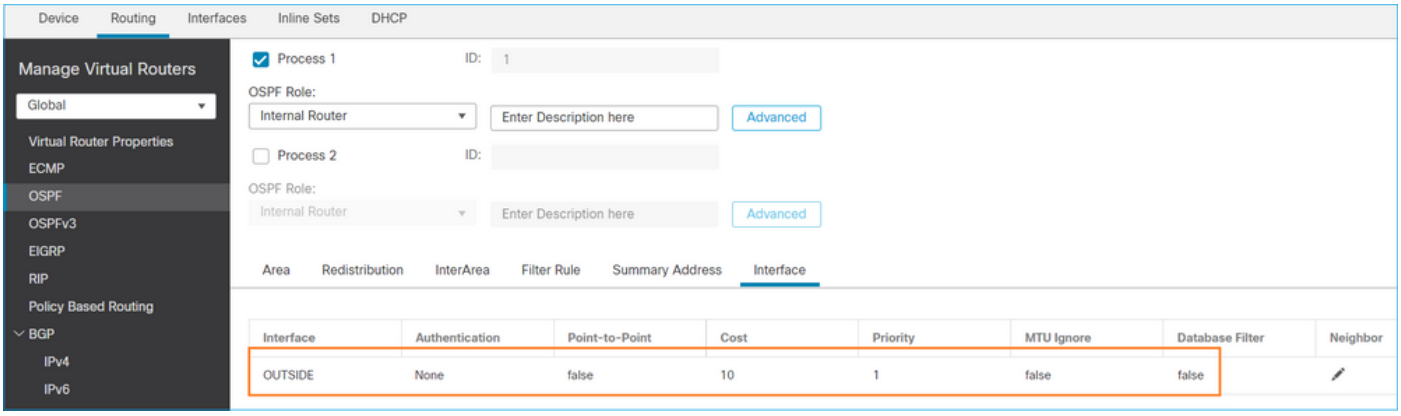


تكوين OSPFv2 و OSPFv3 بين FTD و ASA. تحقق من كيفية معالجة الجهازين ل L2 وحركة مرور البث المتعدد ل L3 التي تم إنشاؤها بواسطة OSPF.

الحل

تكوين OSPFv2





وبالمثل، بالنسبة ل OSPFv3

التكوين على واجهة سطر الأوامر (CLI) ل 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
```

يقوم التكوين بإنشاء هذه الإدخالات في جداول السماح لمسار الأمان السريع (ASP) ل FTD

حتى ال يتم حظر حركة مرور البث المتعدد للمدخل:

```
<#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
```

بالنسبة للإصدار السادس من بروتوكول الإنترنت (IP):

```
<#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
...
```

تكون عمليات تجاور OSPFv2 و OSPFv3 قيد التشغيل:

```
<#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
```

هذه هي جلسات عمل OSPF للبث المتعدد التي تم إنهاؤها إلى المربع:

```
<#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
```

إختبار، قم بتمكين الالتقاط ل IPv4 ومسح الاتصالات بالجهاز:

<#root>

```
firepower#

capture CAP interface OUTSIDE trace

firepower#

clear conn all

12 connection(s) deleted.
firepower#

clear capture CAP

firepower# !
```

تحذير: يسبب هذا انقطاع! يتم عرض المثال لأغراض العرض التوضيحي فقط!

حزم OSPF الملتقطة:

<#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]
```

فيما يلي كيفية معالجة حزمة البث المتعدد OSPFv2 بواسطة جدار الحماية:

<#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
```

هذه هي الطريقة التي يتم بها معالجة حزمة البث المتعدد OSPFv3 بواسطة جدار الحماية:

<#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:

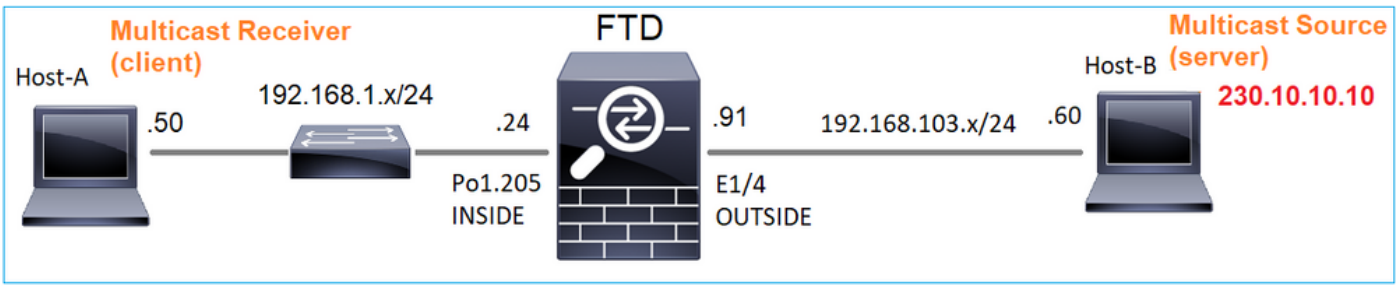
Additional Information:

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

المهمة 2 - تكوين البث المتعدد الأساسي

المخطط



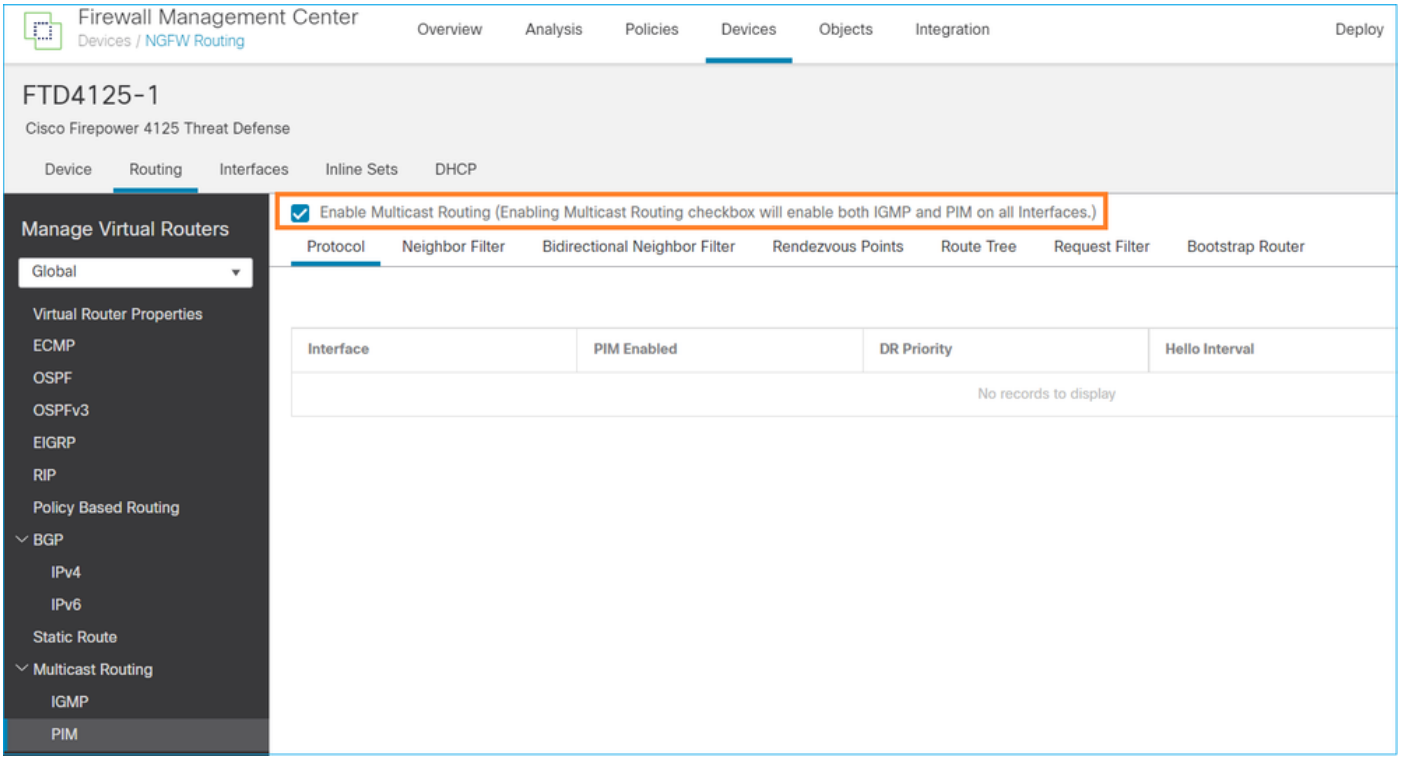
المتطلبات

قم بتكوين جدار الحماية بحيث يتم تدفق حركة مرور البث المتعدد من الخادم إلى عميل البث المتعدد على IP 230.10.10.10

الحل

من وجهة نظر جدار الحماية، فإن التكوين الأدنى هو تمكين توجيه البث المتعدد بشكل عام. وهذا يمكن في الخلفية IGMP و PIM على جميع واجهات جدار الحماية.

في واجهة مستخدم FMC:



على واجهة سطر أوامر (CLI) جدار الحماية هذا هو التكوين الذي تم دفعه:

```
<#root>

firepower#

show run multicast-routing

multicast-routing

<-- Multicast routing is enabled
```

التحقق من 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
```

التحقق من 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
```

التحقق من MFIB

<#root>

```
firepower#
```

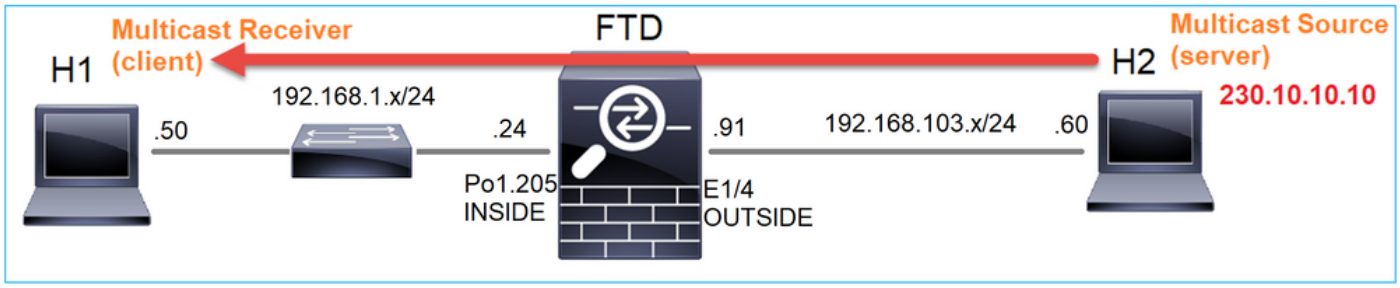
show mfib

```
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
```

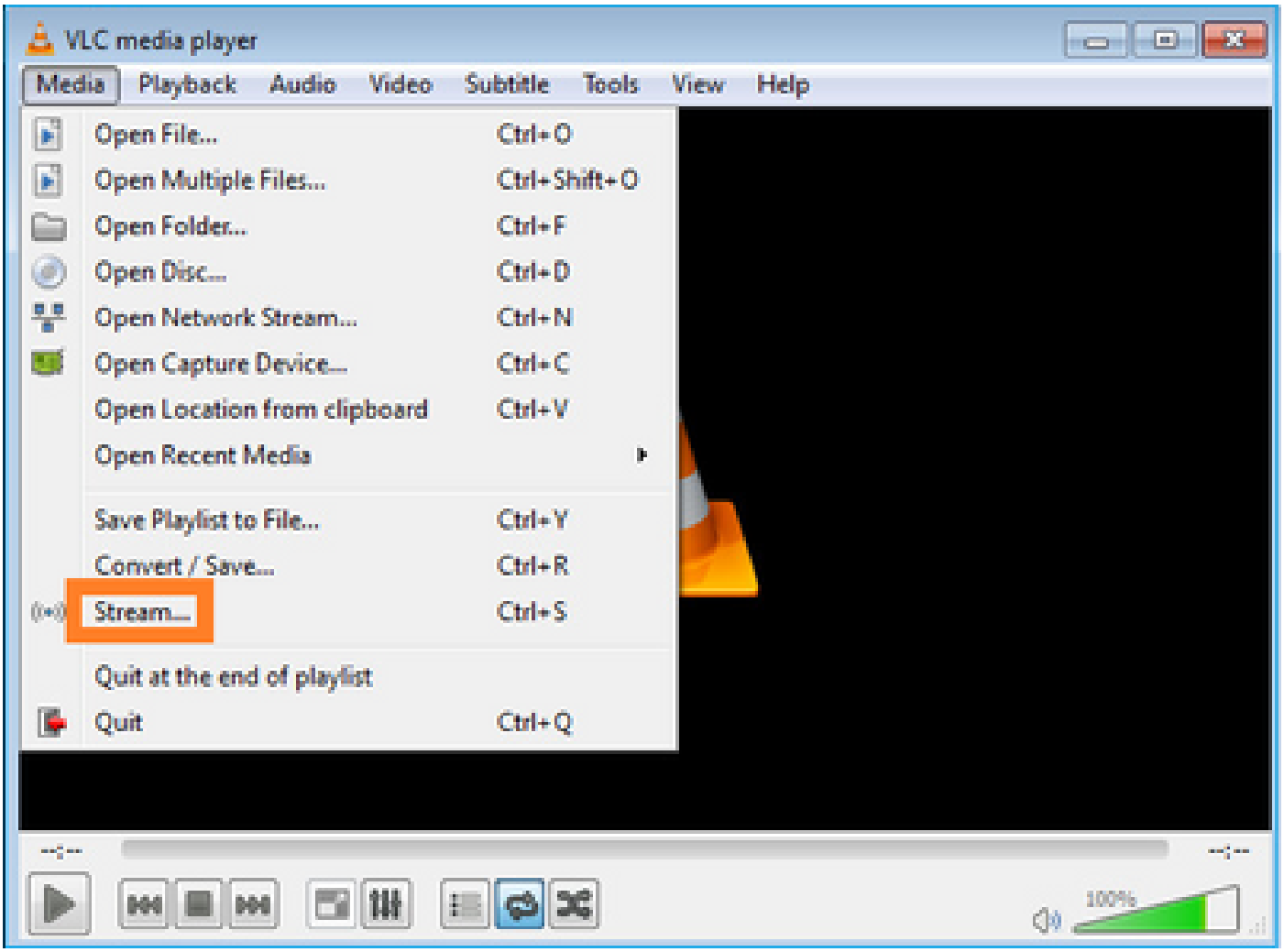
```
Interface Counts: FS Pkt Count/PS Pkt Count

(*,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 seco
(*,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
```

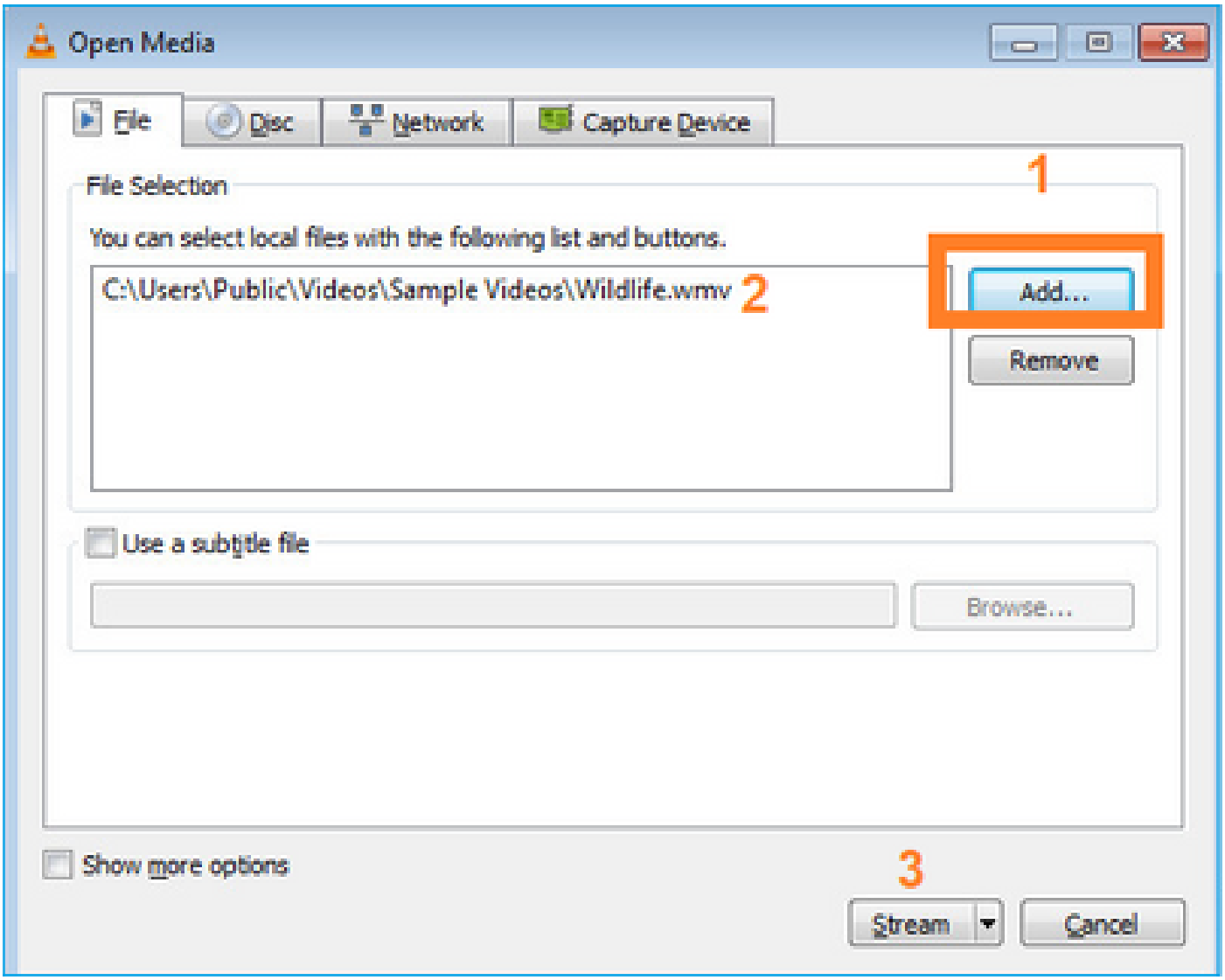
حركة مرور البث المتعدد من خلال جدار الحماية

في هذه الحالة، ال VLC وسائط مشغل استعملت تطبيق كندل multicast وزبون أن يختبر multicast حركة مرور:



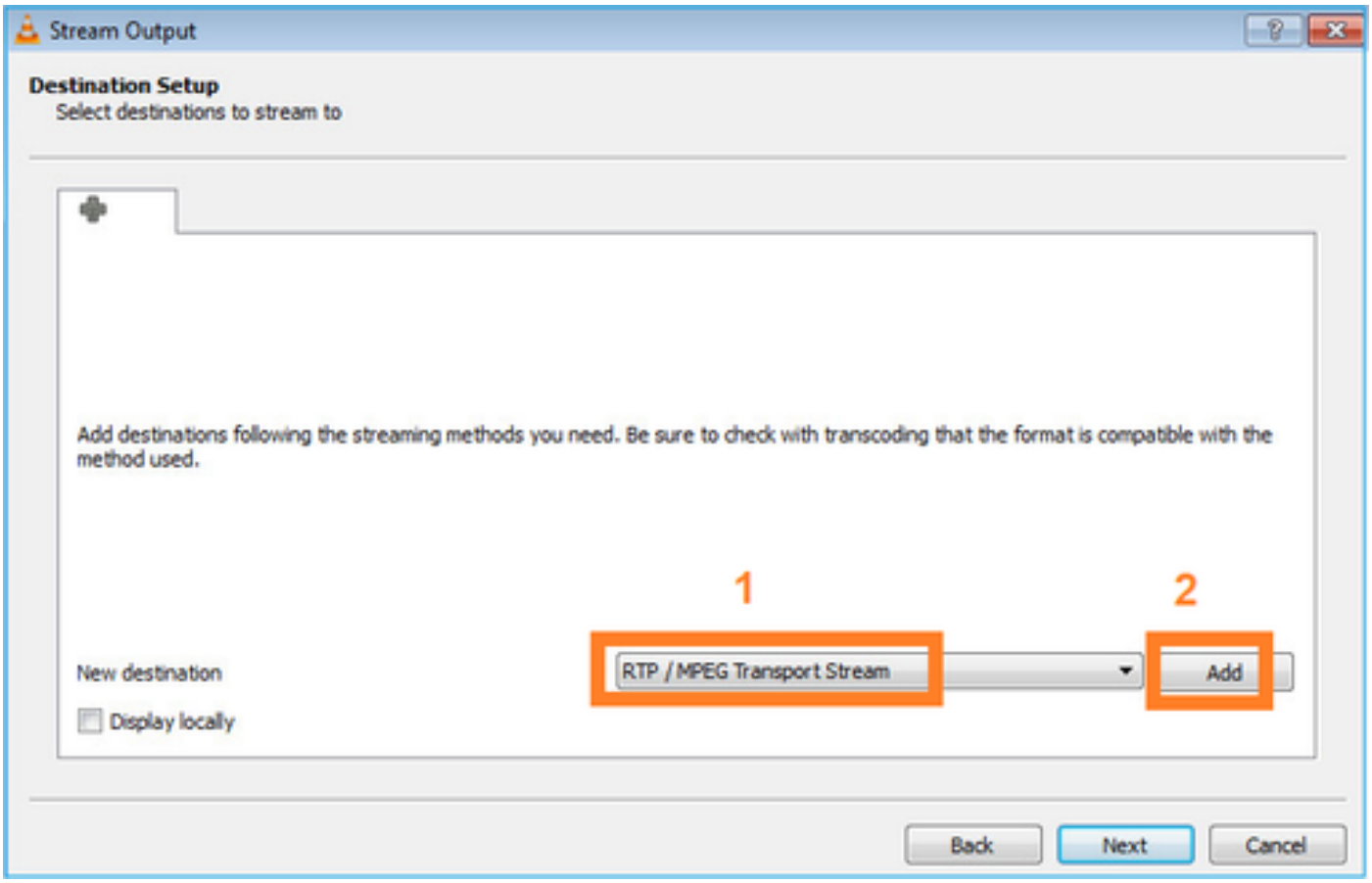
تكوين خادم البث المتعدد VLC:


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
--:--
--:--
100%

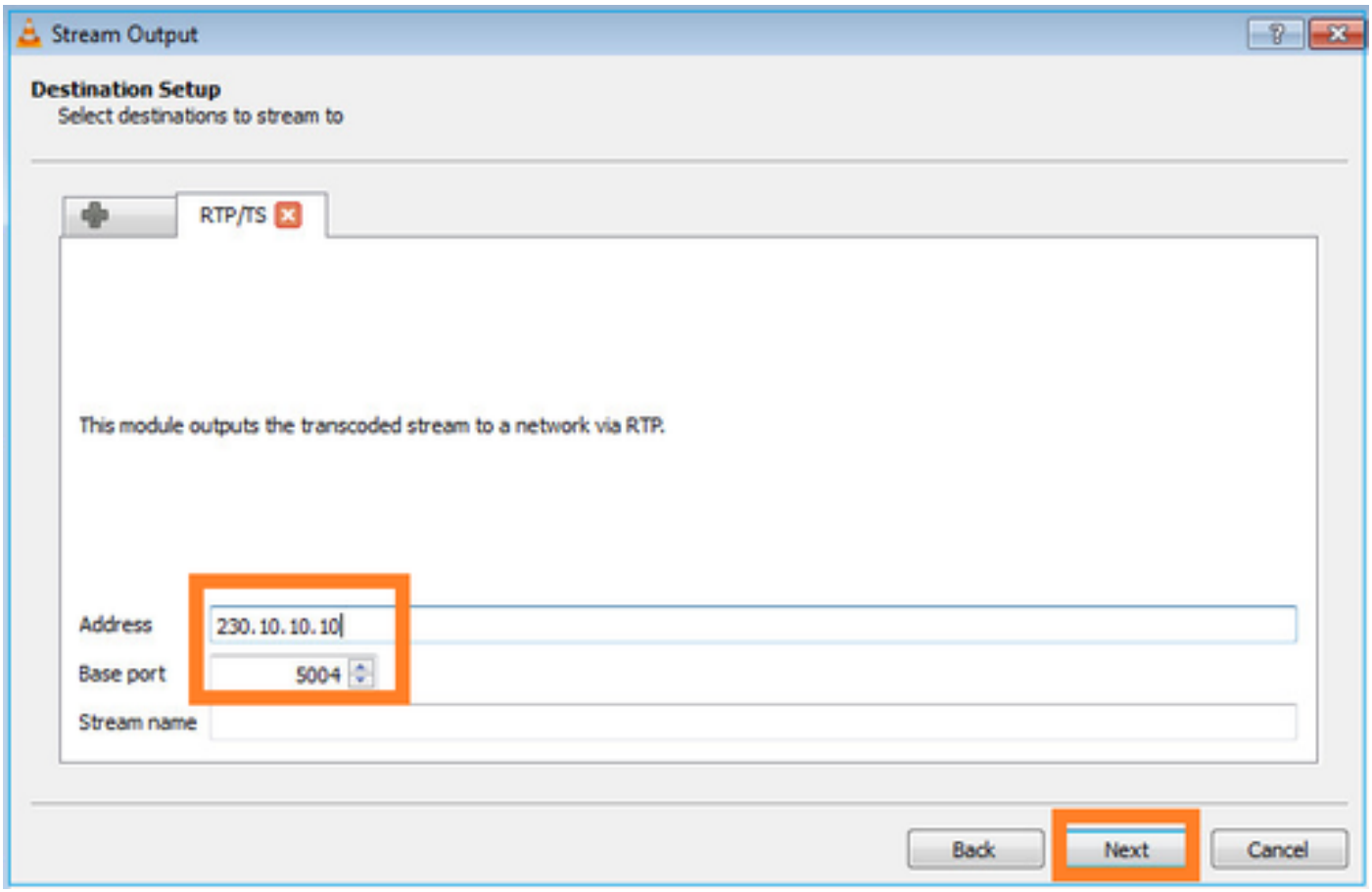


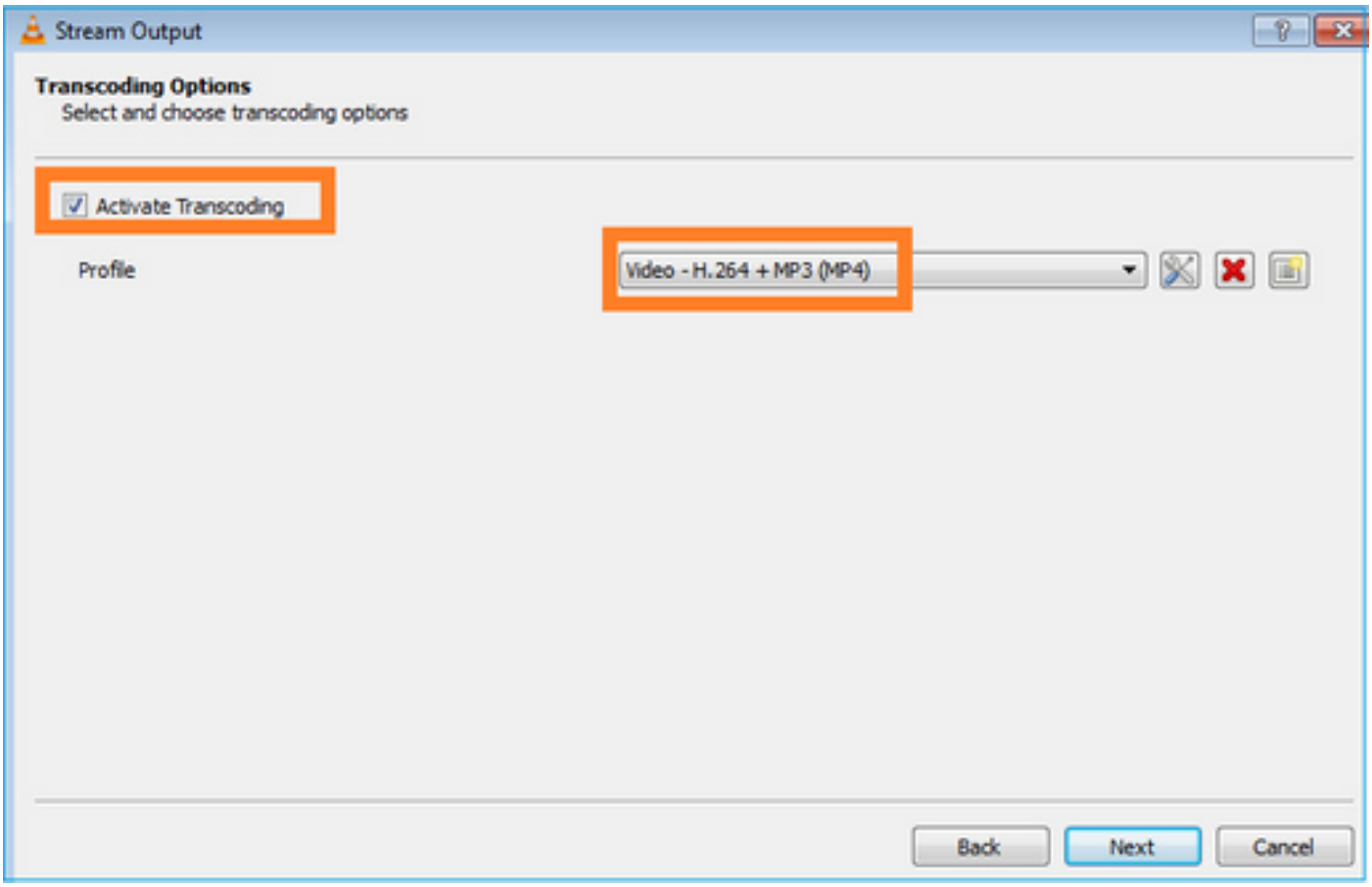
في الشاشة التالية، حدد التالي فقط.

حدد التنسيق:



عينت الـ multicast IP وميناء:



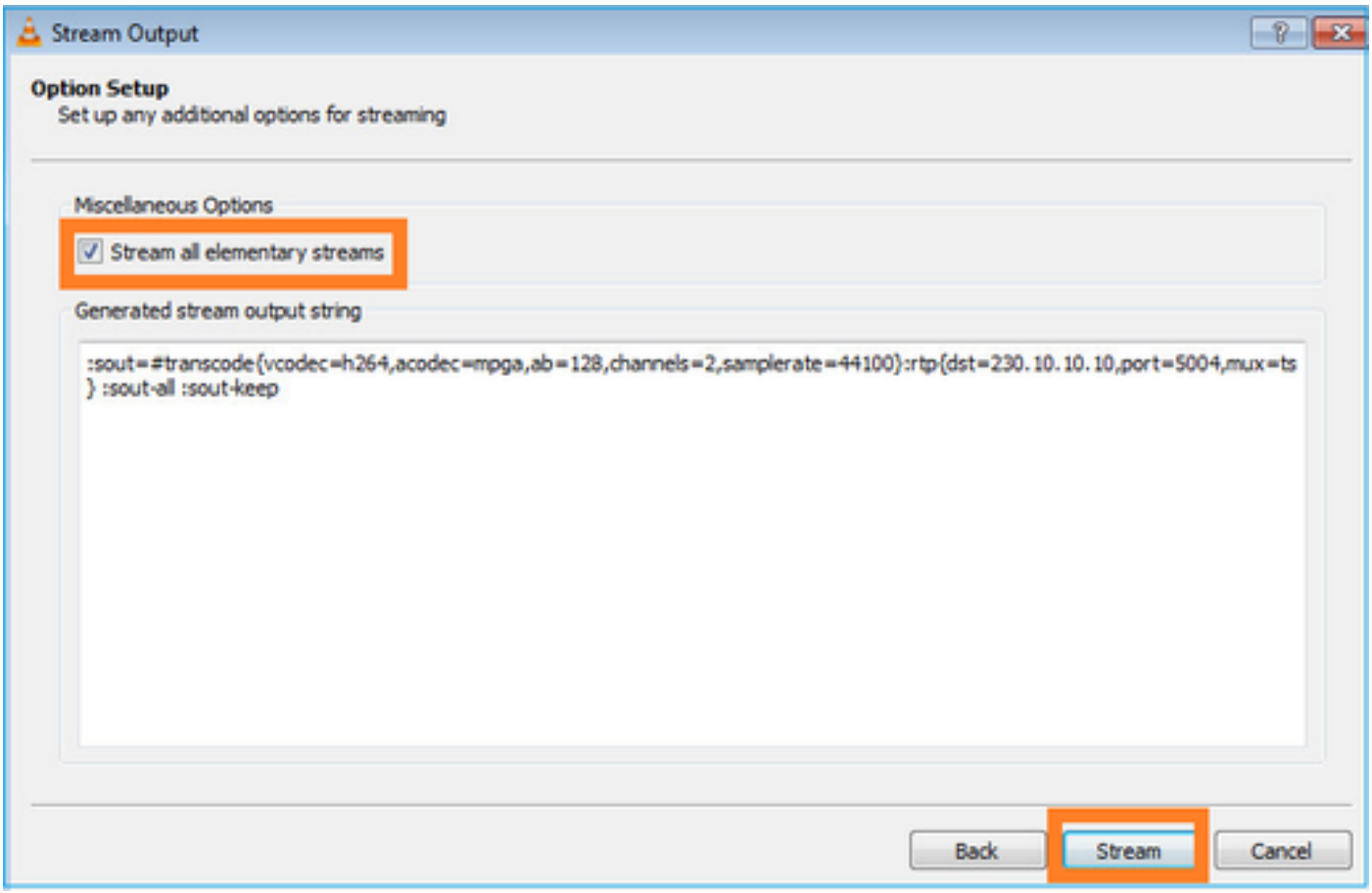


تمكين التقاط LINA على جدار حماية FTD:

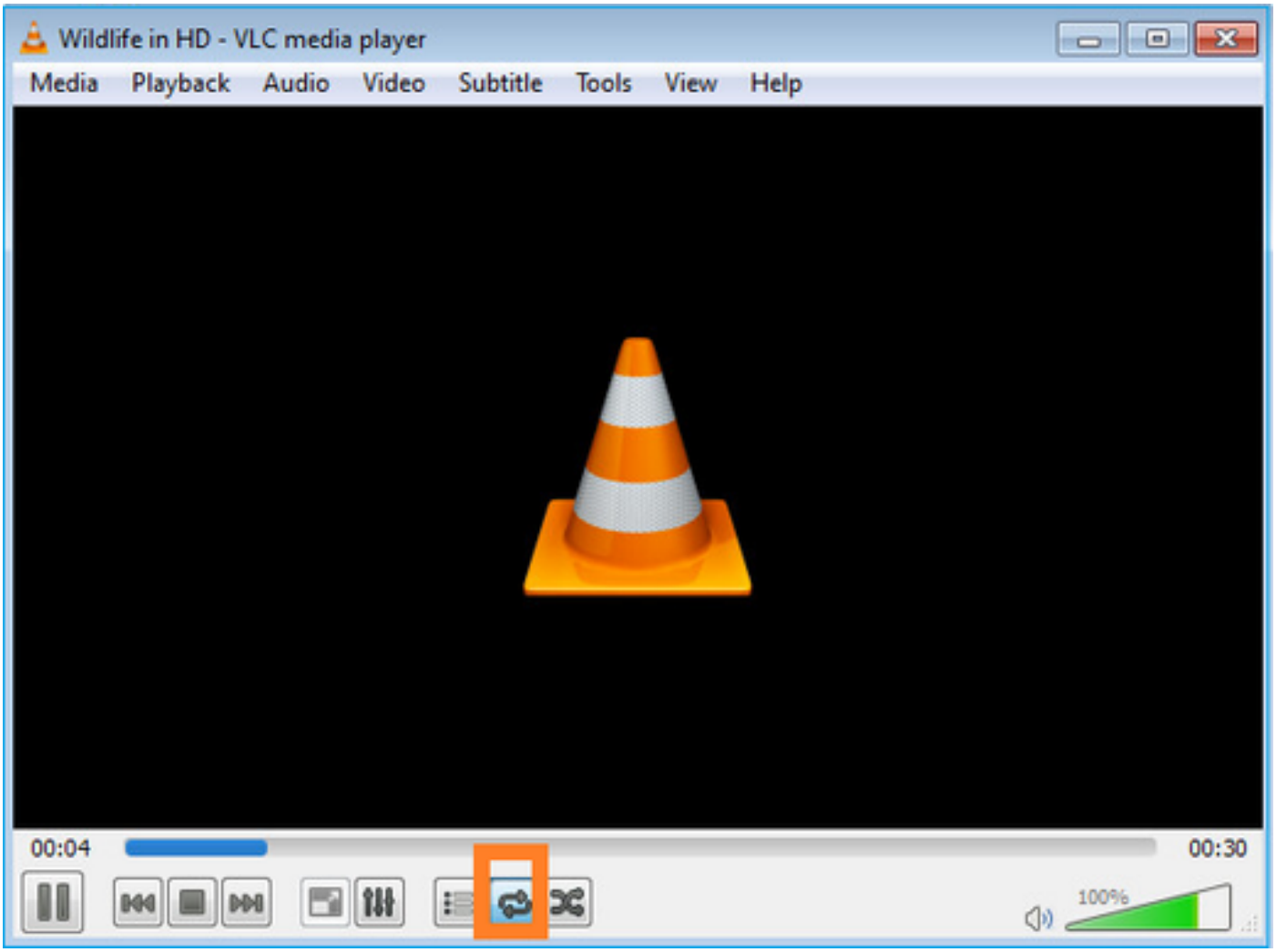
<#root>

```
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
```

حدد زر الدفق للجهاز لبدء دفق البث المتعدد:



مكن خيار "التكرار الحلقي" بحيث يتم إرسال الدفق باستمرار:



التحقق (سيناريو غير تشغيلي)

وهذا السيناريو دليل على سيناريو غير عملي. الهدف هو إثبات سلوك جدار الحماية.

يحصل جهاز جدار الحماية على تدفق البث المتعدد، ولكنه لا يقوم بإعادة توجيهه:

<#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
```

إظهار عمليات إسقاط ASP لجدار الحماية Lina:

```
<#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
```

لتتبع حزمة هناك حاجة إلى التقاط الحزمة الأولى من تدفق البث المتعدد. لهذا السبب قم بمسح التدفقات الحالية:

```
<#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
...
```

يكشف خيار "التفاصيل" عنوان MAC للبث المتعدد:

```
<#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)
...
```

يظهر تتبع الحزمة الحقيقية أن الحزمة مسموح بها، ولكن هذا ليس ما يحدث حقا:

```
<#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
```

استنادا إلى عدادات المسار و mfib، يتم إسقاط الحزم لأن قائمة الواجهة الصادرة (OIL) فارغة:

```
<#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

تظهر عدادات MFIB حالات فشل RPF والتي في هذه الحالة ليست ما يحدث حقا:

<#root>

firepower#

show mfib 230.10.10.10

Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
AR - Activity Required, K - Keepalive
firepower# show mfib 230.10.10.10
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
AR - Activity Required, K - Keepalive

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

<-- Multicast forwarding counters

Other counts: Total/RPF failed

/Other drops <-- Multicast drop counters
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
IC - Internal Copy, NP - Not platform switched
SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count

(192.168.103.60,230.10.10.10) Flags: K

Forwarding: 0/0/0/0

,

Other: 650/650

/0 <-- Allowed and dropped multicast packets

'show mfib count' إخراج في مماثلة RPF فشل حالات:

<#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
```

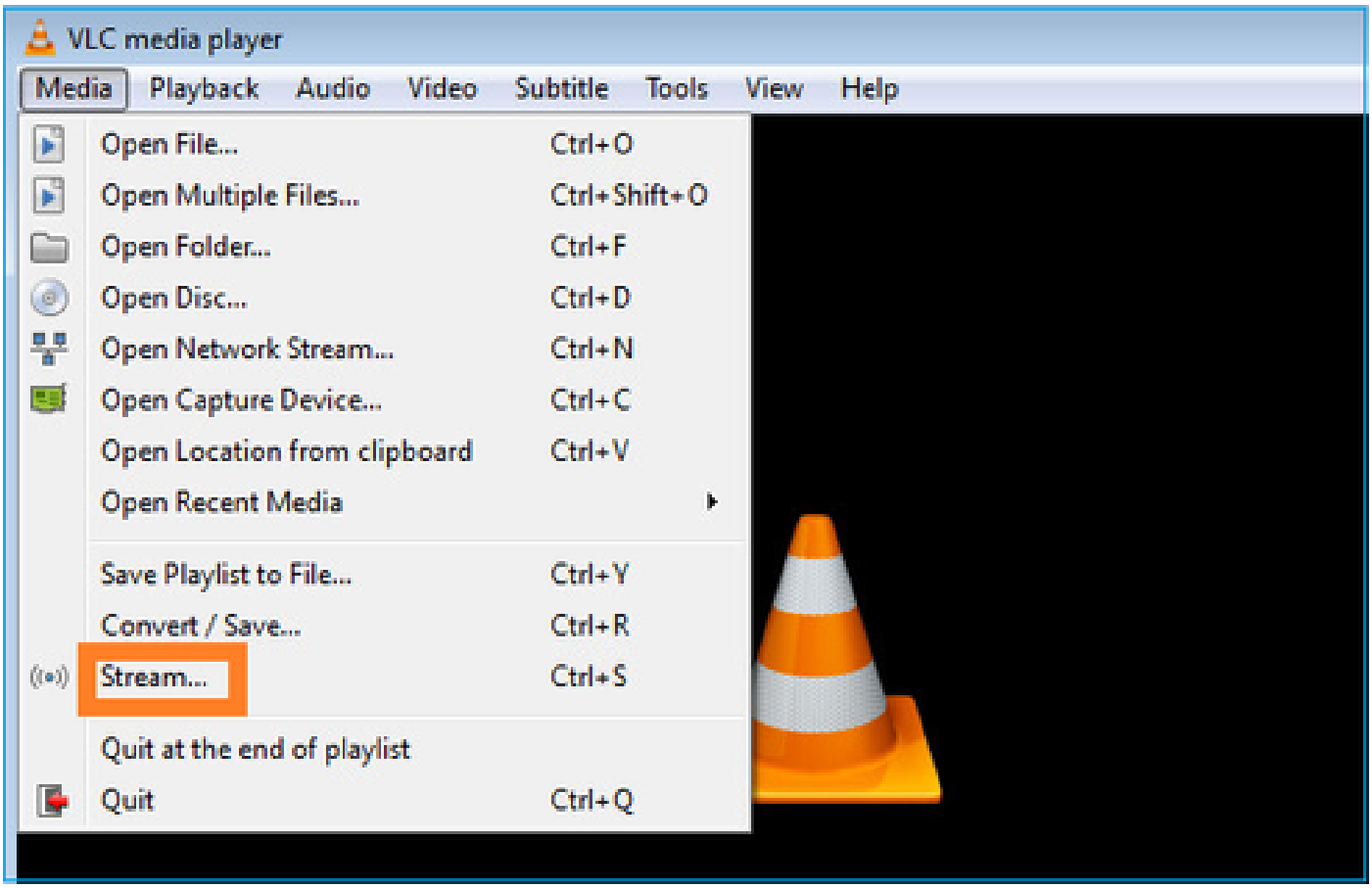
Group: 230.10.10.10

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

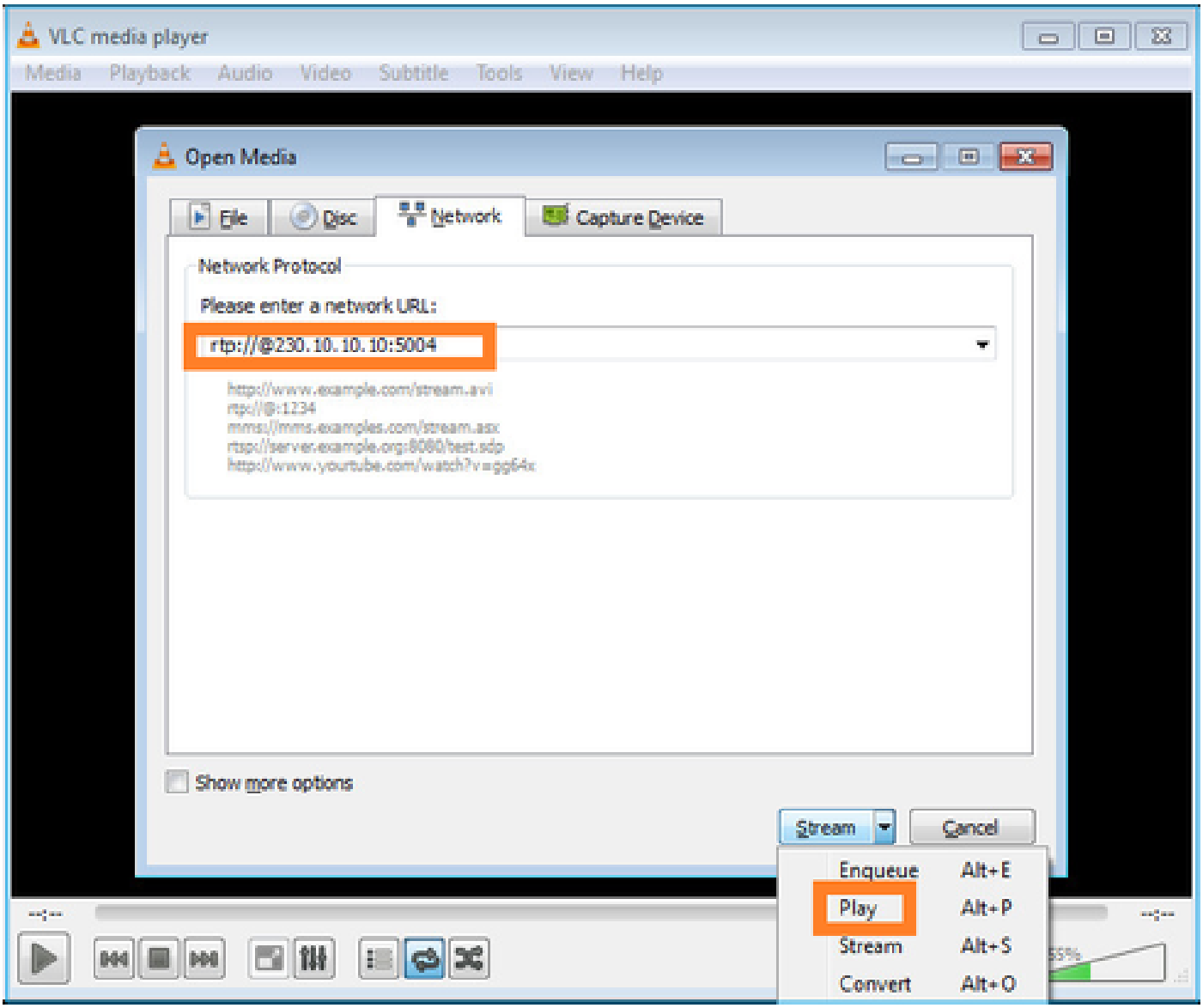
Other: 1115/1115

```
/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
```

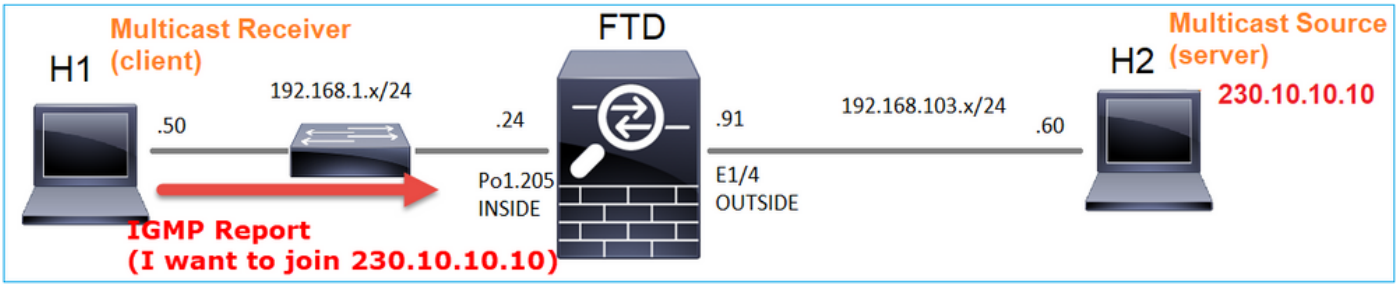
تكوين مستقبل VLC للبث المتعدد:



حدد IP مصدر البث المتعدد وحدد تشغيل:



في النهاية الخلفية، بمجرد تحديد تشغيل يعلن المضيف عن إستعداده للانضمام إلى مجموعة البث المتعدد المحددة ويرسل رسالة تقرير IGMP:

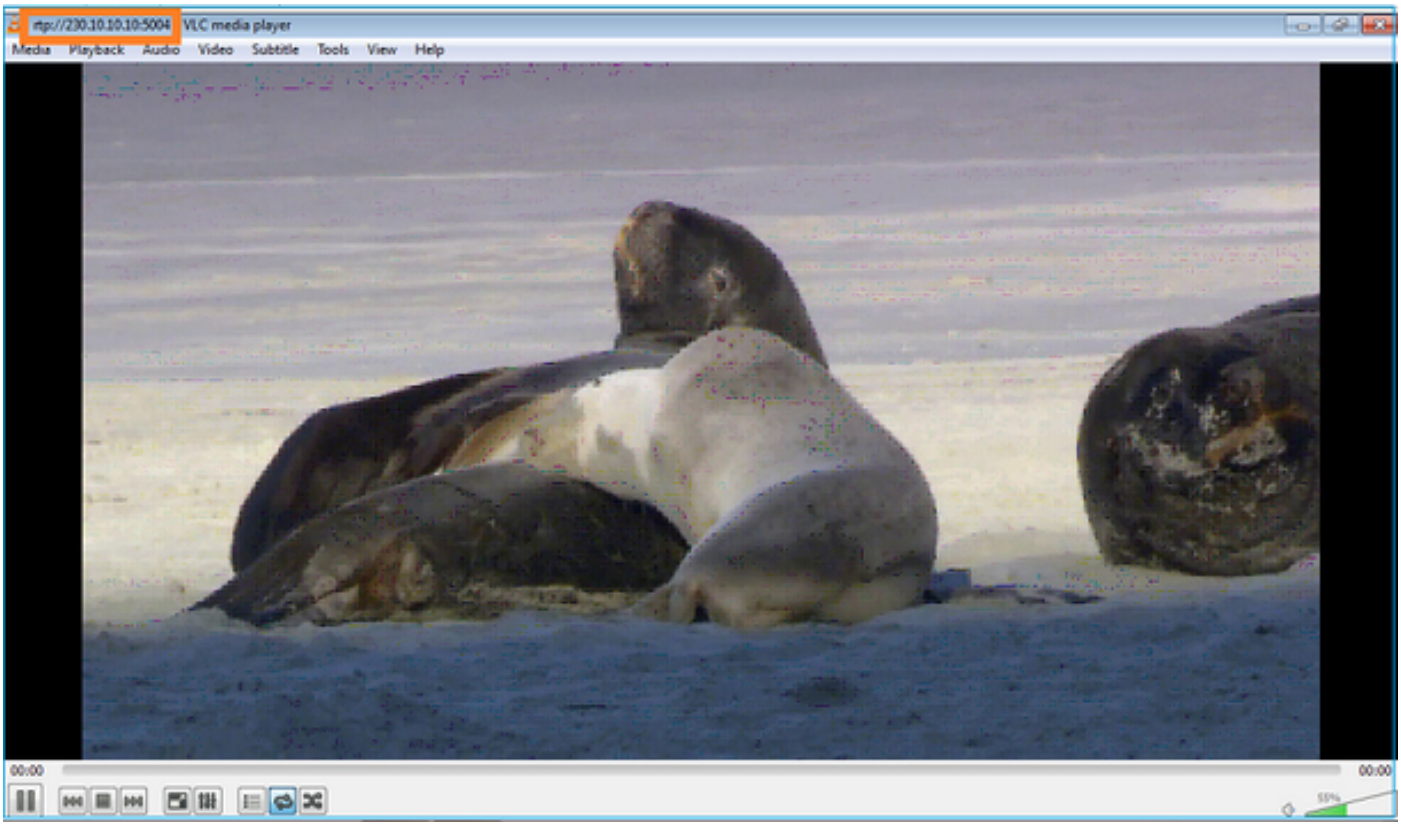


إذا قمت بتمكين تصحيح أخطاء، فيمكنك رؤية رسائل تقرير IGMP:

```
<#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
```

يبدأ الدفق:



التحقق (السيناريو التشغيلي)

<#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
```

جدول مسار جدار الحماية:

<#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

عدادات 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
```

إستطلاع بروتوكول إدارة مجموعات الإنترنت (IGMP)

- إستطلاع IGMP هي آلية تستخدم على المحولات لمنع غمر البث المتعدد.
- يراقب المحول تقارير IGMP لتحديد مكان الأجهزة المضيفة (أجهزة الاستقبال) الموجودة.
- يراقب المحول استعلامات IGMP لتحديد مكان وجود الموجهات/جدران الحماية (المرسلين).
- يتم تمكين التطفل على بروتوكول IGMP بشكل افتراضي على معظم محولات Cisco. راجع أدلة التحويل ذات الصلة للحصول على مزيد من التفاصيل. هنا العينة إنتاج من L3 مادة حفازة مفتاح:

<#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
```

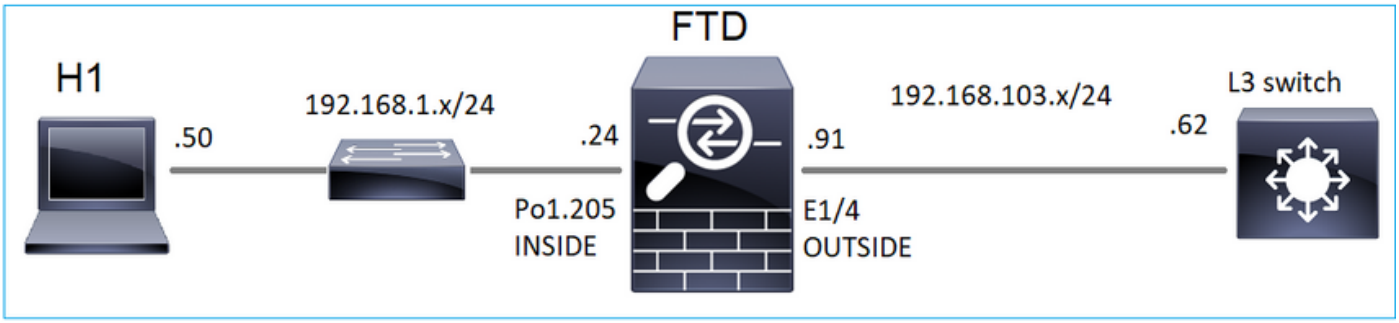
المهمة 3 - المجموعة الثابتة لبروتوكول إدارة مجموعات الإنترنت (IGMP) مقابل مجموعة الانضمام إلى بروتوكول إدارة مجموعات الإنترنت (IGMP)

نظرة عامة

	ip igmp static-group	ip igmp join-group
هل تم التطبيق على واجهة FTD؟	نعم	نعم
هل يجذب "برنامج الإرسال فائق السرعة (FTD)" تيار البث المتعدد؟	نعم، يتم إرسال "انضمام PIM" تجاه جهاز الخادم. المصدر أو نحو نقطة الالتقاء (RP). اذه يحدث إلا إذا كان FTD به اذه الأمر وه الموجه المعين ل PIM (DR) على هذه الواجهة.	نعم، يتم إرسال "انضمام PIM" تجاه جهاز الخادم. المصدر أو نحو نقطة الالتقاء (RP). اذه يحدث إلا إذا كان FTD به اذه الأمر وه الموجه المعين ل PIM (DR) على هذه الواجهة.
هل يقوم FTD بإعادة توجيه حركة مرور البث المتعدد خارج الواجهة؟	نعم	نعم
هل يستهلك FTD حركة مرور البث المتعدد ويرد عليها	لا	نعم، يقوم FTD بفك تشفير البث المتعدد إلى وحدة المعالجة المركزية (CPU) واستهلاك الموارد على المصدر.
تأثير وحدة المعالجة المركزية	الحد الأدنى حيث إن الحزمة لا يتم انتقالها إلى وحدة المعالجة المركزية.	يمكن التأثير على وحدة المعالجة المركزية (CPU) الخاصة ب FTD نظرًا لأن كل حزمة من حزم البث المتعدد التي تنتمي إلى المجموعة يتم انتقالها إلى وحدة المعالجة المركزية (CPU) الخاصة ب FTD.

متطلبات المهمة

خذ بعين الاعتبار هذا الهيكل:



عل جدار الحماية قم بتمكين عمليات الالتقاط التالية:

<#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. أستخدم إختبار اتصال ICMP من محول L3 لإرسال حركة مرور البث المتعدد إلى IP 230.11.11.11 وفحص كيفية معالجة هذه الأمر بواسطة جدار الحماية.
2. قم بتمكين الأمر igmp static-group على جدار الحماية داخل الواجهة وفحص كيفية معالجة تدفق البث المتعدد (IP 230.11.11.11) بواسطة جدار الحماية.
3. قم بتمكين الأمر igmp static-group على جدار الحماية داخل الواجهة وفحص كيفية معالجة تدفق البث المتعدد (IP 230.11.11.11) بواسطة جدار الحماية.

الحل

ال يحتوي جدار الحماية عل أي مسارات ل 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
```

هناك طريقة بسيطة لاختبار البث المتعدد وهي إستخدام أداة إختبار اتصال ICMP. في هذه الحالة، ابدأ إختبار اتصال من R2 إلى عنوان IP للبث المتعدد 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:
.............................
```

على جدار الحماية، يتم إنشاء مسار ديناميكي والنفط فارغ:

```
<#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
```

يظهر الالتقاط على جدار الحماية:

```
<#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
```

يقوم جدار الحماية بإنشاء إتصالات لكل إختبار اتصال، ولكنه يقوم بإسقاط الحزم بصمت:

```
<#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 230.1
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.
May 17 2022 11:05:49: %FTD-6-302021: Teardown ICMP connection for faddr 192.168.103.62/6 gaddr 230.11.1
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 230.1
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.
May 17 2022 11:05:53: %FTD-6-302021: Teardown ICMP connection for faddr 192.168.103.62/6 gaddr 230.11.1
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
```

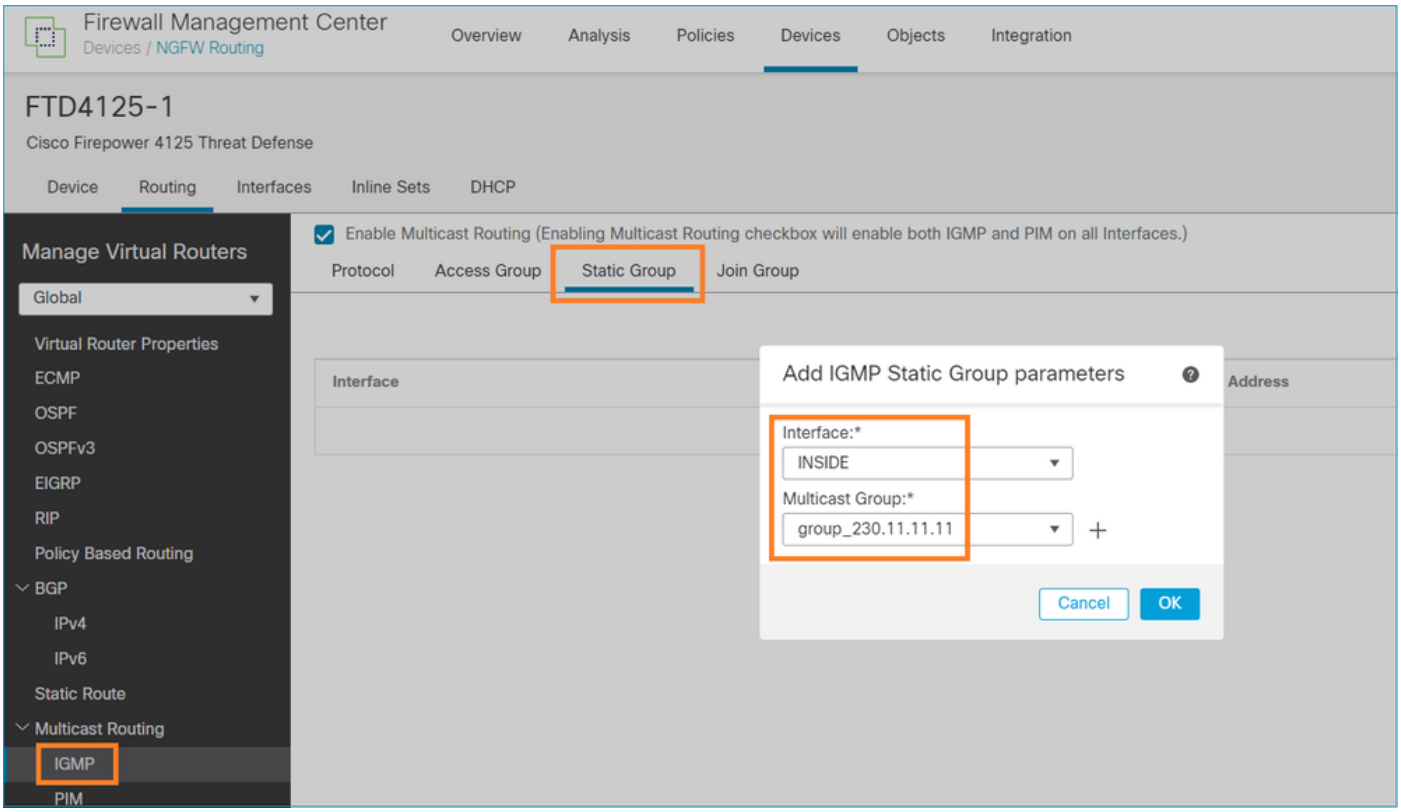
ملاحظة: لا يعرض التقاط LINA ASP الإسقاط الحزم التي تم إسقاطها

المؤشر الرئيسي لعمليات إسقاط حزمة البث المتعدد هو:

```
<#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
```

مجموعة IGMP الثابتة

على FMC قم بتكوين مجموعة IGMP ثابتة:



هذا ما يتم نشره في الخلفية:

```
<#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
```

فشل إختبار الاتصال، ولكن تتم إعادة توجيه حركة مرور بث ICMP المتعدد الآن من خلال جدار الحماية:

```
<#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
```

ملاحظة: يظهر تتبع الحزمة مخرجات غير صحيحة (واجهة الدخول هي نفسها مثل مخرج. لمزيد من التفاصيل، راجع معرف تصحيح الأخطاء من 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
```

تلميح: يمكنك إختبار الاتصال باستخدام المهلة 0 من المضيف المصدر ويمكنك التحقق من عدادات mfib لجدار الحماية:

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

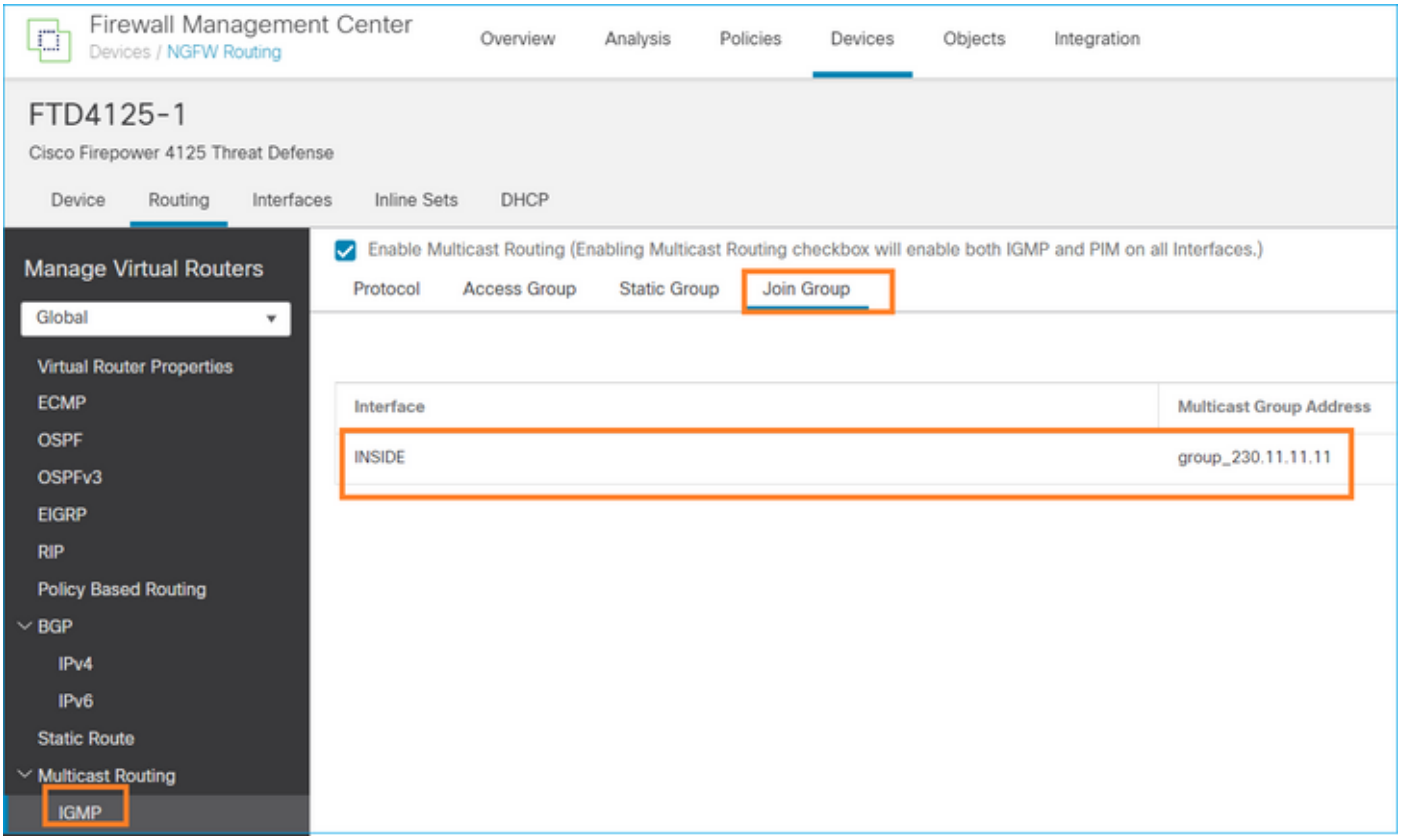
<#root>

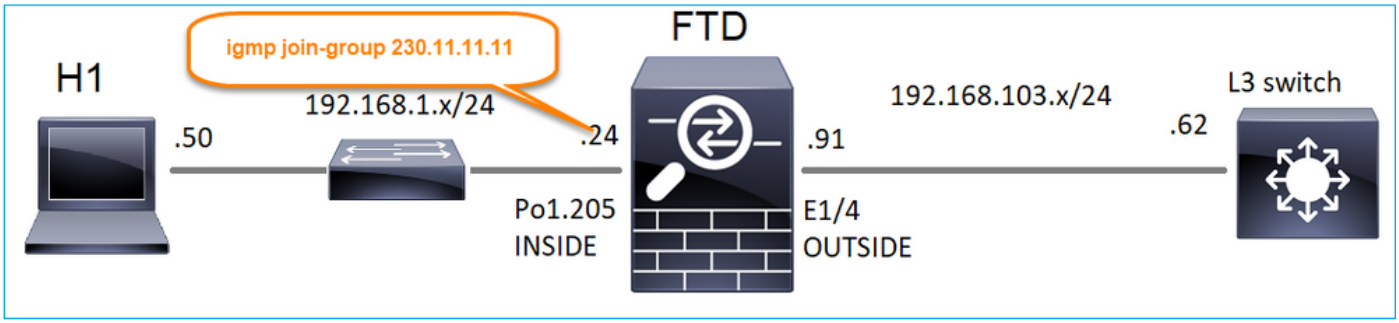
```
firepower# clear mfib counters

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
```

مجموعة انضمام IGMP

على وحدة التحكم في إدارة اللوحة الأساسية (FMC) عن بعد، تم تكوين تكوين المجموعة الثابتة التي تم تكوينها مسبقا وتكوين مجموعة انضمام إلى بروتوكول إدارة مجموعات الإنترنت (IGMP):





التكوين الذي تم نشره:

```
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
```

مجموعة 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
```

من مضيف المصدر، جرب إختبار ICMP للبث المتعدد الألول نحو 230.11.11.11 IP:

<#root>

```
L3-Switch#
```

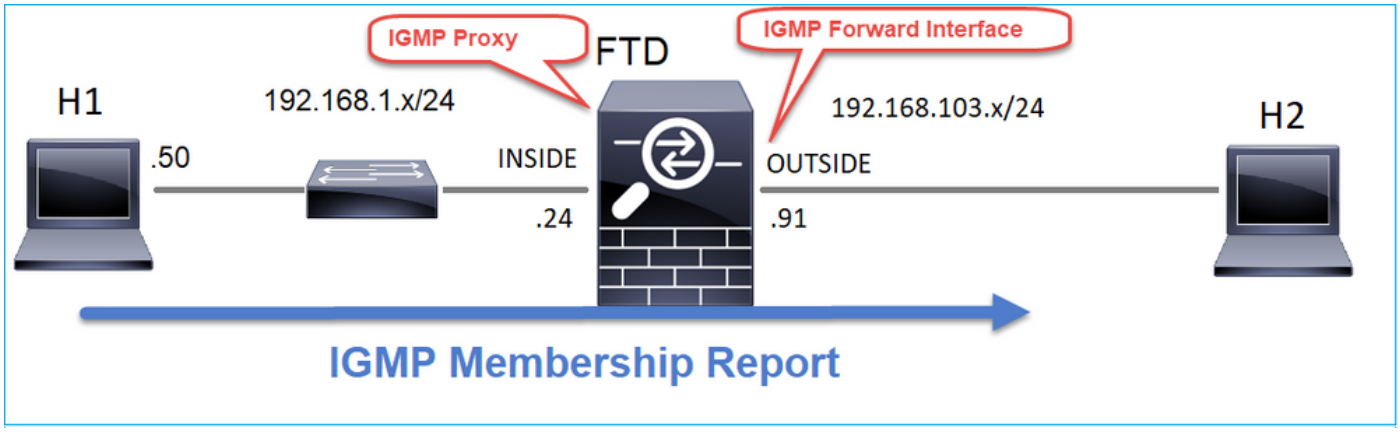
ping 230.11.11.11 repeat 10

```
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
```

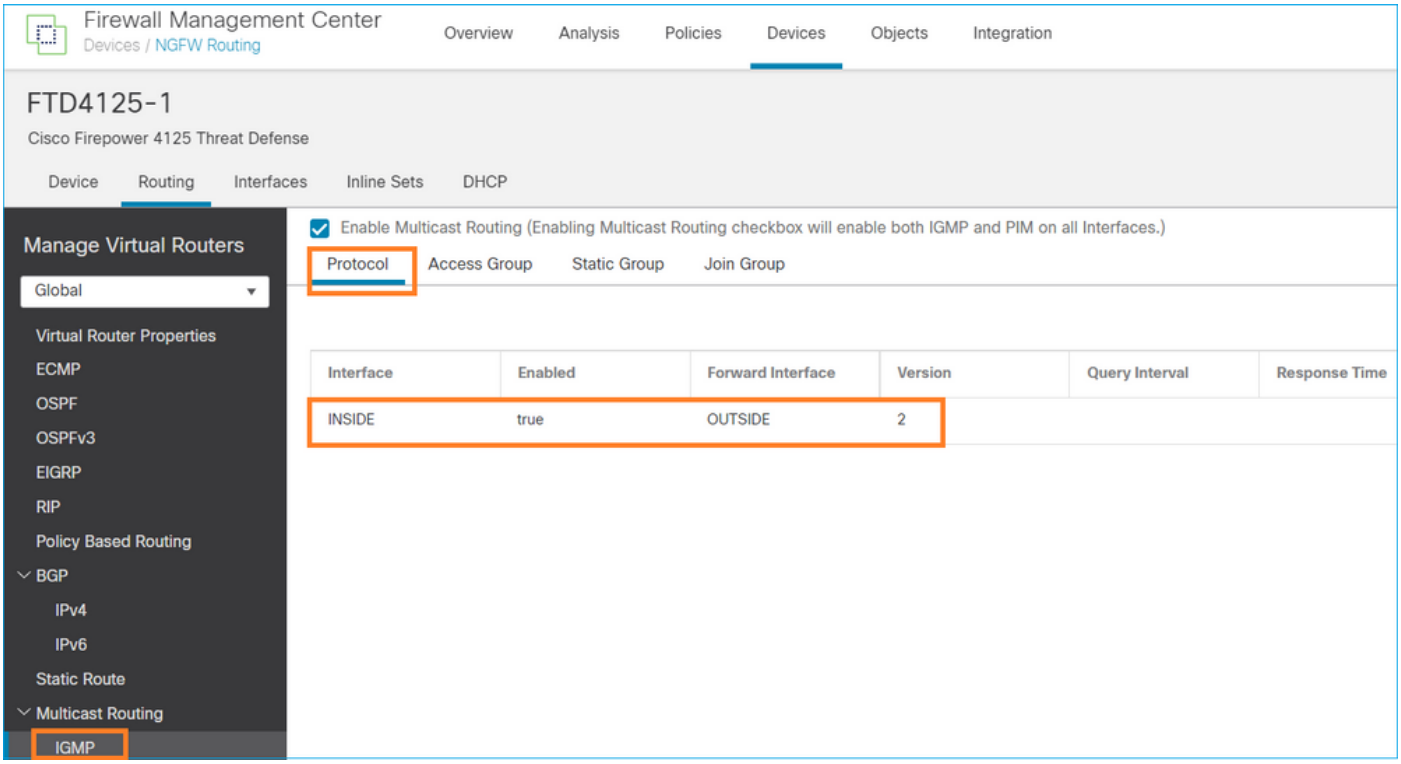
ملاحظة: إذا لم تشاهد جميع الردود، فتحقق من معرفة تصحيح الأخطاء من Cisco CSCvm90069.

المهمة 4 - تكوين التوجيه متعدد البث لبروتوكول IGMP الجذري



قم بتكوين توجيه البث المتعدد لبروتوكول الجذع على FTD حتى تتم إعادة توجيه رسائل تقرير عضوية IGMP التي يتم استقبالها على الواجهة الداخلية إلى الواجهة الخارجية.

الحل



التكوين الذي تم نشره:

```
<#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
```

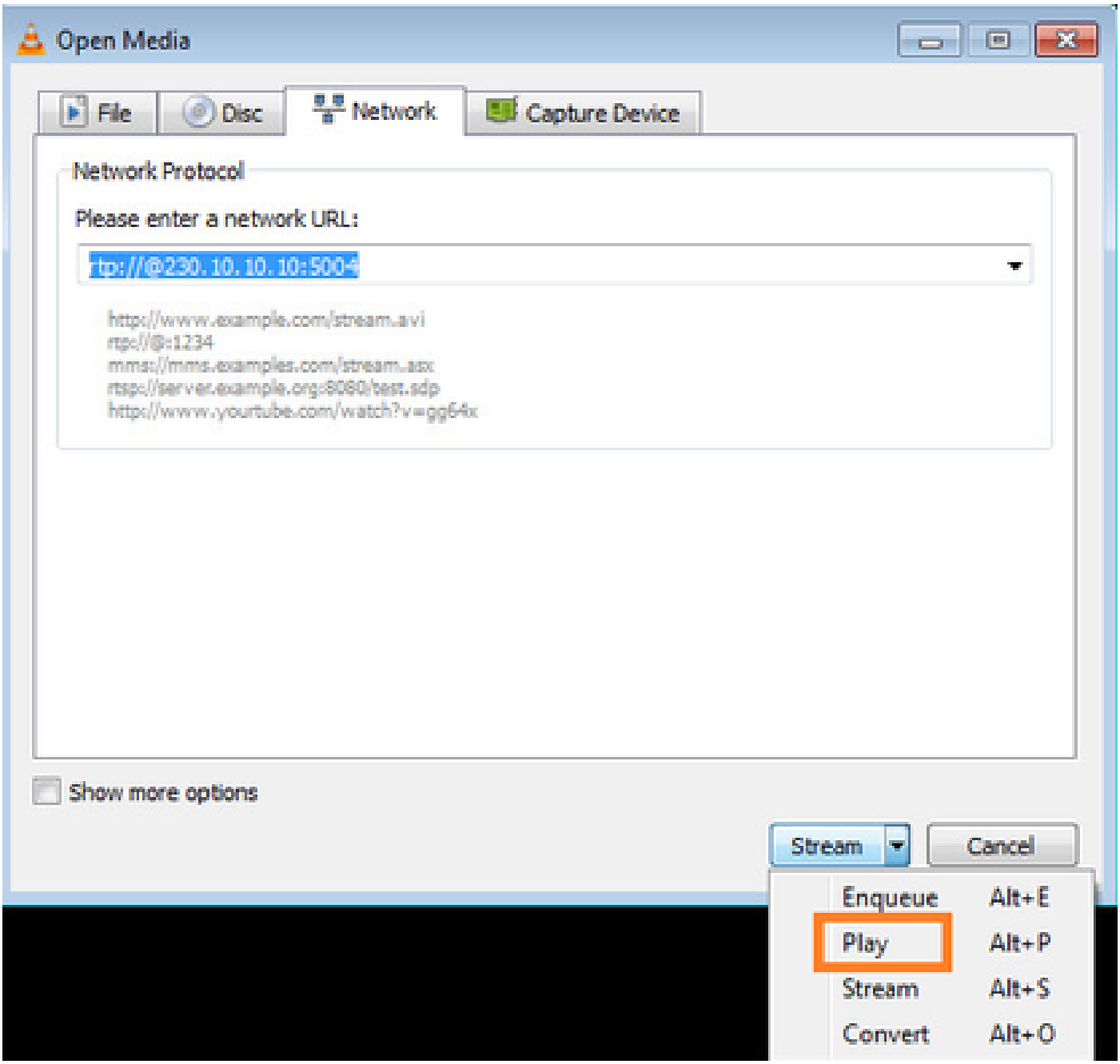
التحقق

تمكين عمليات الالتقاط على 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
```

التحقق

لفرض تقرير عضوية IGMP، يمكنك إستخدام تطبيق مثل VLC:



يقوم بروتوكول FTD بتوكيل حزم 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
```

يقوم FTD بتغيير IP المصدر:

```
<#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
```

إذا قمت بالتحقق من PCAP في Wireshark، يمكنك أن ترى أن الحزمة تم إنشاؤها بالكامل بواسطة جدار الحماية (تغييرات تعريف IP).

يتم إنشاء إدخال مجموعة في 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
```

يقوم جدار حماية FTD بإنشاء إتصالين لمستوى التحكم:

```
<#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
```

تتبع الحزمة الأولى:

```
<#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:

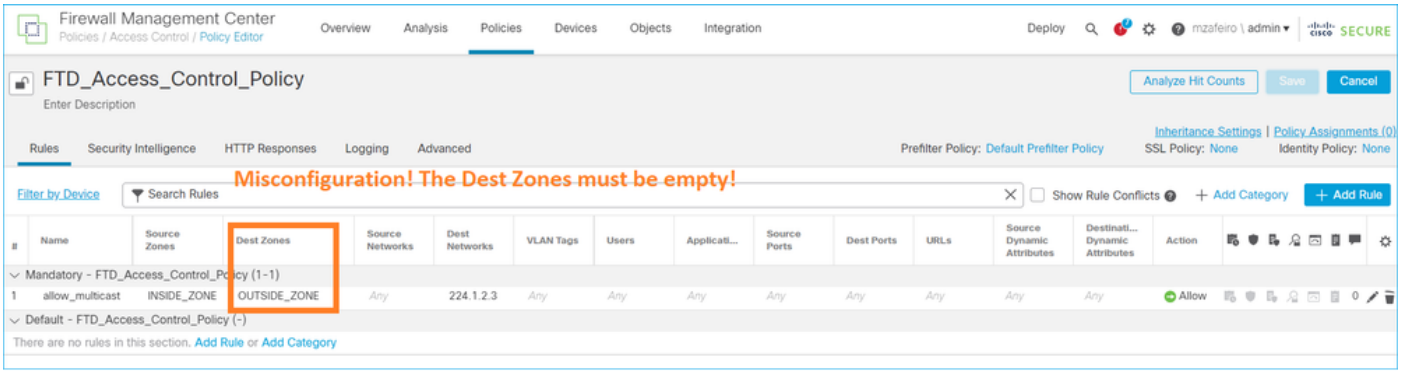
Additional Information:

```
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
```

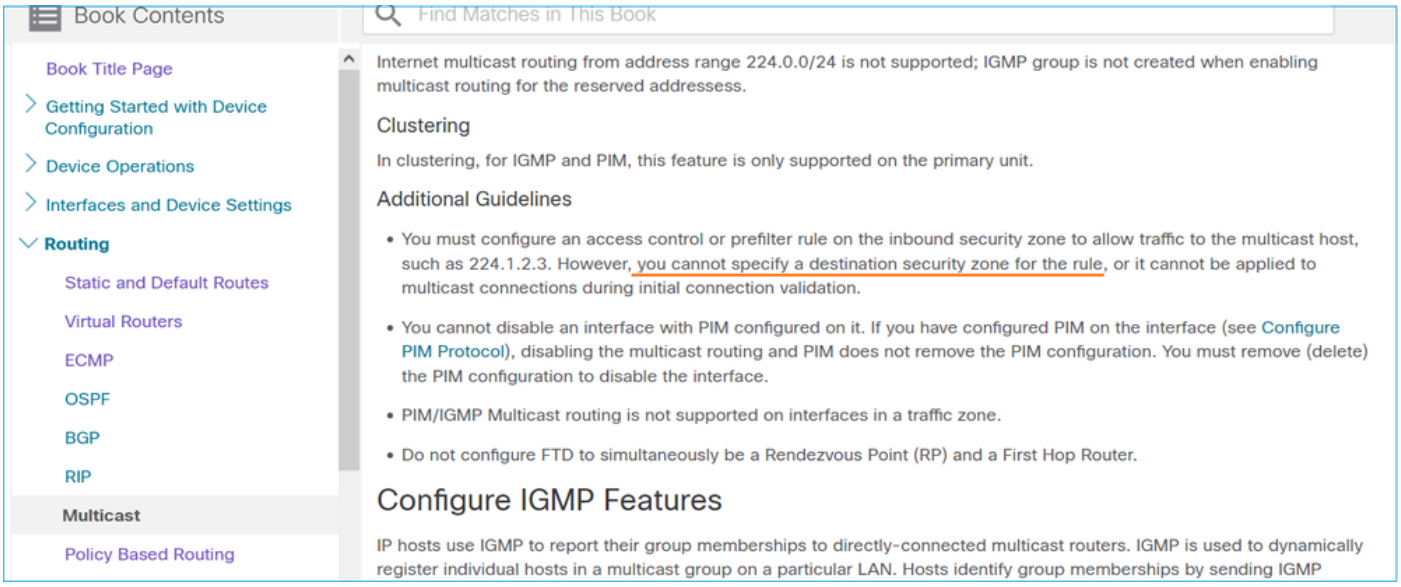
مشكلات معروفة

تصفية حركة مرور البث المتعدد على منطق الوجهة

ال يمكنك تحديد منطقة أمان وجهة لقاعدة نهج التحكم في الوصول التي تطابق حركة مرور البث المتعدد:



وهذا موثق أيضا في دليل مستخدم FMC:



يتم رفض تقارير IGMP بواسطة جدار الحماية عند تجاوز حد واجهة IGMP

يتيح جدار الحماية بشكل افتراضي الحد الأقصى لعدد 500 وصلة نشطة (تقارير) حالية على واجهة. إذا تم تجاوز هذا الحد، فإن جدار الحماية يتجاهل تقارير IGMP الواردة الإضافية من مستقبلات البث المتعدد.

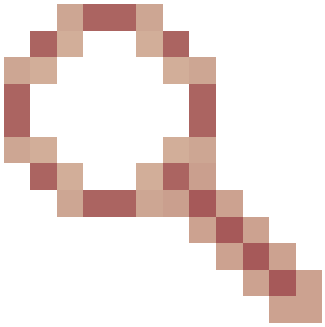
للتحقق من حد IGMP والروابط النشطة، قم بتشغيل الأمر show igmp interface name:

```
<#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)
```

يعرض أمر تصحيح أخطاء IGMP debug igmp هذا الإخراج:

```
<#root>

asa#
```

```
debug igmp

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



إصدارات البرامج مع إصلاح معرف تصحيح الأخطاء من Cisco CSCvw60976
السماح للمستخدمين بتكوين ما يصل إلى 5000 مجموعة لكل واجهة.

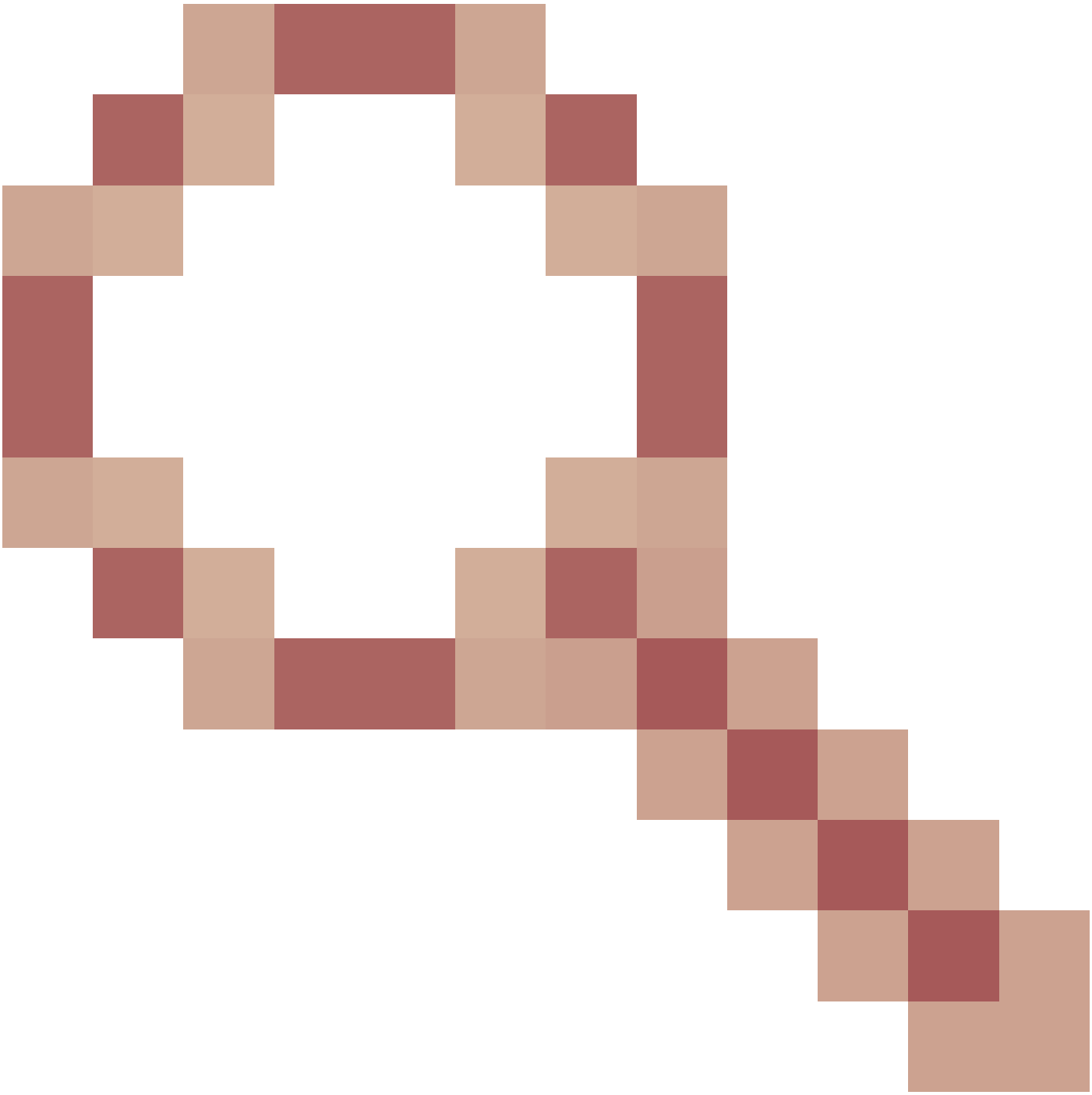
يتجاهل جدار الحماية تقارير IGMP لنطاق العناوين 232.x.x/8

يتم إستخدام نطاق العناوين 232.x.x.x/8 مع البث المتعدد محدد المصدر (SSM). الى يدعم جدار الحماية وظيفة البث المتعدد محدد المصدر (SSM) الخاص ب PIM والتكوين ذي الصلة.

يعرض أمر تصحيح أخطاء IGMP debug igmp هذا الإخراج:

```
<#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
```

معرف تصحيح الأخطاء من Cisco CSCsr53916



تعقب التحسين لدعم نطاق SSM.

معلومات ذات صلة

- توجيه البث المتعدد للدفاع عن تهديد الطاقة النارية
- أستكشاف أخطاء الدفاع عن تهديد FirePOWER والبث المتعدد ASA وإصلاحها

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).