أستكشاف أخطاء الدفاع عن تهديد FirePOWER والبث المتعدد ASA وإصلاحها

المحتويات

المقدمة

يوضح هذا المستند كيفية تنفيذ الدفاع ضد تهديد الطاقة النارية (FTD) وتطبيق جهاز الأمان القابل للتكيف (ASA) للبث المتعدد المستقل عن البروتوكول (PIM).

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.

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.
- برنامج جهاز الأمان القابل للتكيف من Cisco، الإصدار 9.17(1)9.

معلومات أساسية

أساسيات توجيه البث المتعدد

- إعادة توجيه الحزم الأحادي نحو الوجهة أثناء إعادة توجيه البث المتعدد للحزم بعيدا عن المصدر.
- تقوم أجهزة شبكة البث المتعدد (جدران الحماية/الموجهات، وما إلى ذلك) بإعادة توجيه الحزم عبر إعادة توجيه المسار العكسي (RPF). لاحظ أن إعادة توجيه المسار العكسي (RPF) ليست هي نفسها إعادة توجيه المسار العكسي (uRPF) التي يتم إستخدامها في البث الأحادي لمنع أنواع معينة من الهجمات. يمكن تحديد إعادة توجيه المسار العكسي (RPF) كآلية تقوم بإعادة توجيه حزم البث المتعدد بعيدا عن المصدر من الواجهات التي تؤدي إلى مستقبلات البث المتعدد. ودوره الأساسي هو منع حلقات مرور البيانات وضمان تصحيح مسارات حركة المرور.
- يحتوي بروتوكول البث المتعدد مثل PIM على 3 وظائف رئيسية:

1. العثور على واجهة الخادم (الواجهة الأقرب للمصدر).

2. العثور على واجهات تدفق البيانات من الخادم المرتبطة بتدفق بث متعدد محدد (واجهات تجاه أجهزة الاستقبال).

3. الاحتفاظ بشجرة البث المتعدد (إضافة أو إزالة فروع الشجرة).

- يمكن إنشاء شجرة بث متعدد وصيانتها باستخدام إحدى الطريقتين التاليتين: الوصلات الضمنية (الفيضان والتفتيت) أو الوصلات الصريحة (نموذج السحب). يستخدم وضع PIM المكثف (PIM-DM) وصلات ضمنية بينما يستخدم وضع PIM المتناثر (PIM-SM) وصلات صريحة.
- يمكن أن تكون شجرة البث المتعدد مشتركة أو مستندة إلى مصدر:
  - تستخدم الأشجار المشتركة مفهوم نقطة الالتقاء (RP) ويشار إليها على أنها (*، G) حيث G = مجموعة البث المتعدد IP.
  - تتأصل الأشجار المعتمدة على المصدر في المصدر، ولا تستخدم بروتوكول RP، وتتم الملاحظة ك (s، g) حيث S = عنوان IP لمصدر/خادم البث المتعدد.
- نماذج إعادة توجيه البث المتعدد:
  - يستخدم وضع تسليم البث المتعدد لأي مصدر (ASM) الأشجار المشتركة (*، G) حيث يمكن لأي مصدر إرسال تدفق البث المتعدد.
  - يستخدم البث المتعدد محدد المصدر (SSM) الأشجار القائمة على المصدر (S، G)

ونطاق IP 232/8.
  - ثنائي الإتجاه (BiDir) هو نوع من الشجرة المشتركة (*، G) حيث تمر حركة مرور كل من مستوى التحكم ومستوى البيانات عبر RP.
- يمكن تكوين نقطة االلتقاء أو إختيارها باستخدام إحدى الطريقتين التاليتين:
  - RP الثابت
  - Auto-RP
  - الموجه bootstrap (BSR)

ملخص أوضاع PIM

وضع PIM	آر بي	شجرة مشتركة	تدوين	IGMP	دعم ASA/FTD
الوضع المتناثر ل PIM	نعم	نعم	(* و (ز) و(ز)	الإصدار الأول/الإصدار الثاني/الثالث	نعم
وضع PIM المكثف	ال	ال	(س، ز)	الإصدار الأول/الإصدار الثاني/الثالث	ال*
وضع PIM ثنائي الإتجاه	نعم	نعم	(*، زاي)	الإصدار الأول/الإصدار الثاني/الثالث	نعم
وضع البث المتعدد محدد المصدر (SSM) ل PIM	ال	ال	(س، ز)	الإصدار الثالث	ال**

*Auto-RP = يمكن لحركة مرور بيانات Auto-RP المرور

** ال يمكن أن يكون ASA/FTD جهاز من المرحلة الأخيرة

ملخص تكوين RP

تكوين نقطة االلتقاء	ASA/FTD
RP الثابت	نعم

Auto-RP	ال، ولكن يمكن لحركة مرور مستوى التحكم في RP التلقائي المرور
بي إس آر	نعم، ولكن ليس دعم C-RP

ملاحظة: قبل البدء في أستكشاف أخطاء البث المتعدد وإصلاحها، من المهم للغاية الحصول على نظرة واضحة على مخطط البث المتعدد. على وجه التحديد، في الحد الأدنى، يجب أن تعرف:
- ما هو دور جدار الحماية في مخطط البث المتعدد؟
- من هو نائب الرئيس؟
- من هو مرسل دفق البث المتعدد (IP المصدر ومجموعة البث المتعدد IP)؟
- من هو مستقبل تدفق البث المتعدد؟
- هل لديك مشاكل مع مستوى التحكم (IGMP/PIM) أو مستوى البيانات (دفق البث المتعدد) نفسه؟

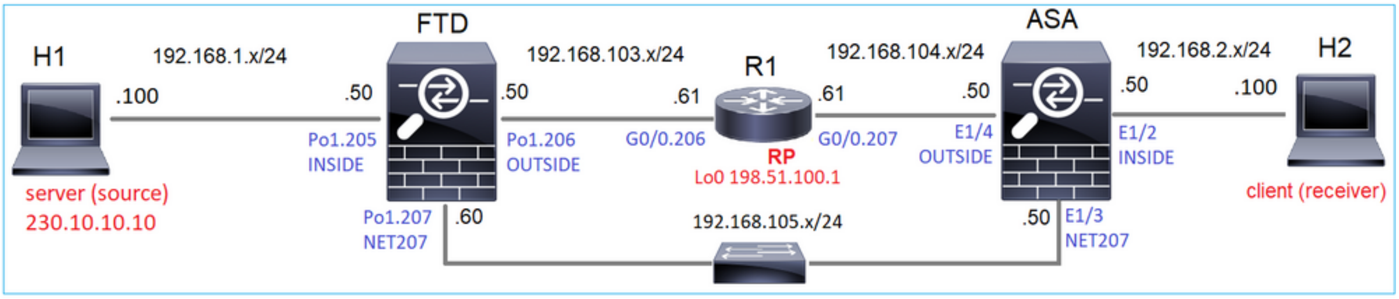
المختصرات/المختصرات

الاختصارات	الشرح
إف اتش آر	موجه الخطوة الأولى - خطوة متصلة مباشرة بمصدر حركة مرور البث المتعدد.
ل.ر	موجه الخطوة الأخيرة - نقطة وصول متصلة مباشرة بمستقبلات حركة مرور البث المتعدد.
آر بي	نقطة الالتقاء
دكتور	موجه معين
SPT	شجرة أقصر مسار
RPT	شجرة نقطة الالتقاء (RP)، شجرة المشاركة
إعادة توجيه المسار العكسي	إعادة توجيه المسار العكسي
زيت	قائمة الواجهة الصادرة

مأرب	قاعدة معلومات توجيه البث المتعدد
MFIB	قاعدة معلومات إعادة توجيه البث المتعدد
ASM	البث المتعدد لأي مصدر
بي إس آر	موجه Bootstrap
SSM	البث المتعدد محدد المصدر
موزع	مسار سريع
SP	مسار بطيء
CP	نقطة التحكم
PPS	الحزمة في الثانية

المهمة 1 - وضع PIM المتناثر (RP الثابت)

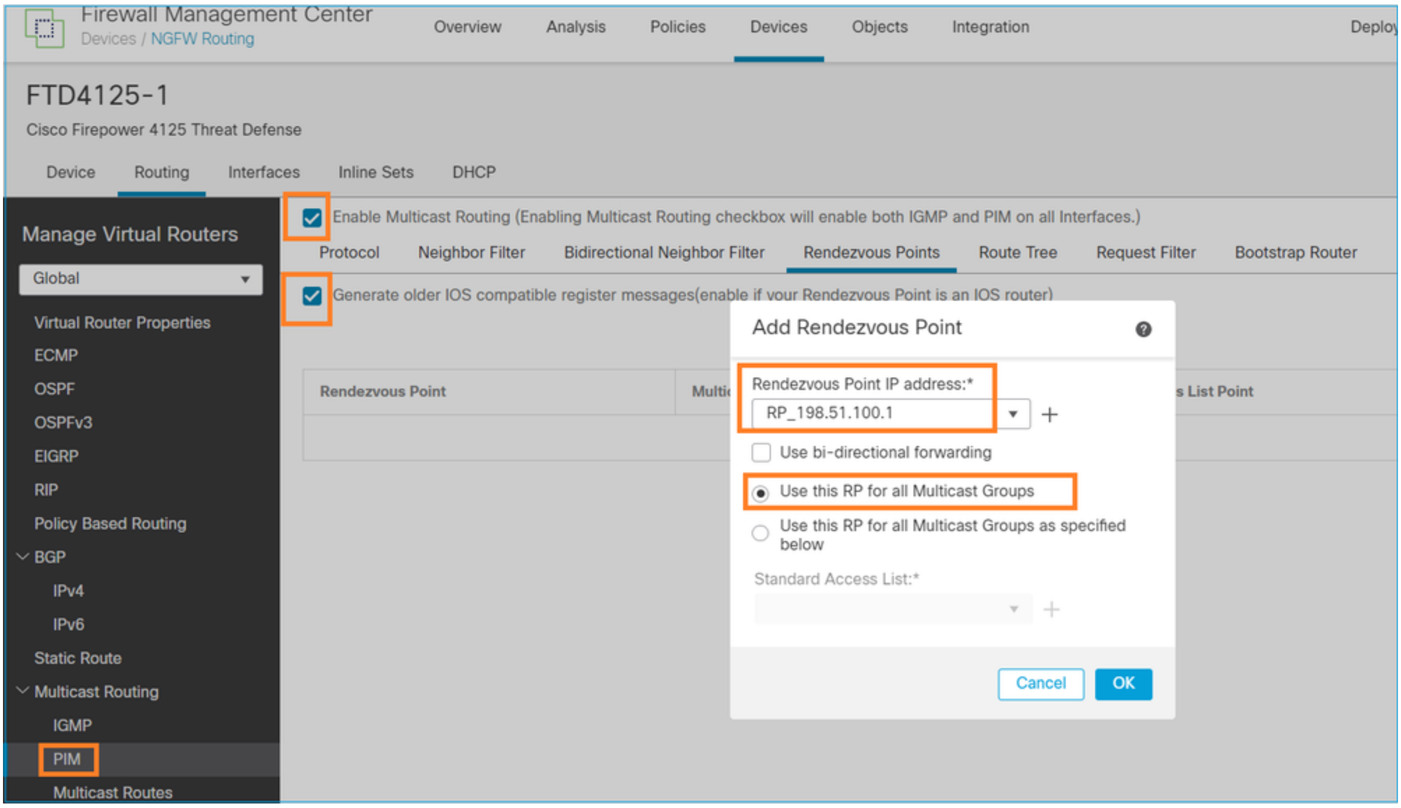
المخطط



قم بتكوين الوضع المتناثر ل PIM للبث المتعدد في المخطط مع R1 (198.51.100.1) ك RP.

الحل

تكوين FTD:



FTD4125-1

Cisco Firepower 4125 Threat Defense

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

☑ Generate older IOS compatible register messages(enable if your Rendezvous Point is an IOS router)

Add Rendezvous Point

Rendezvous Point IP address:* RP_198.51.100.1

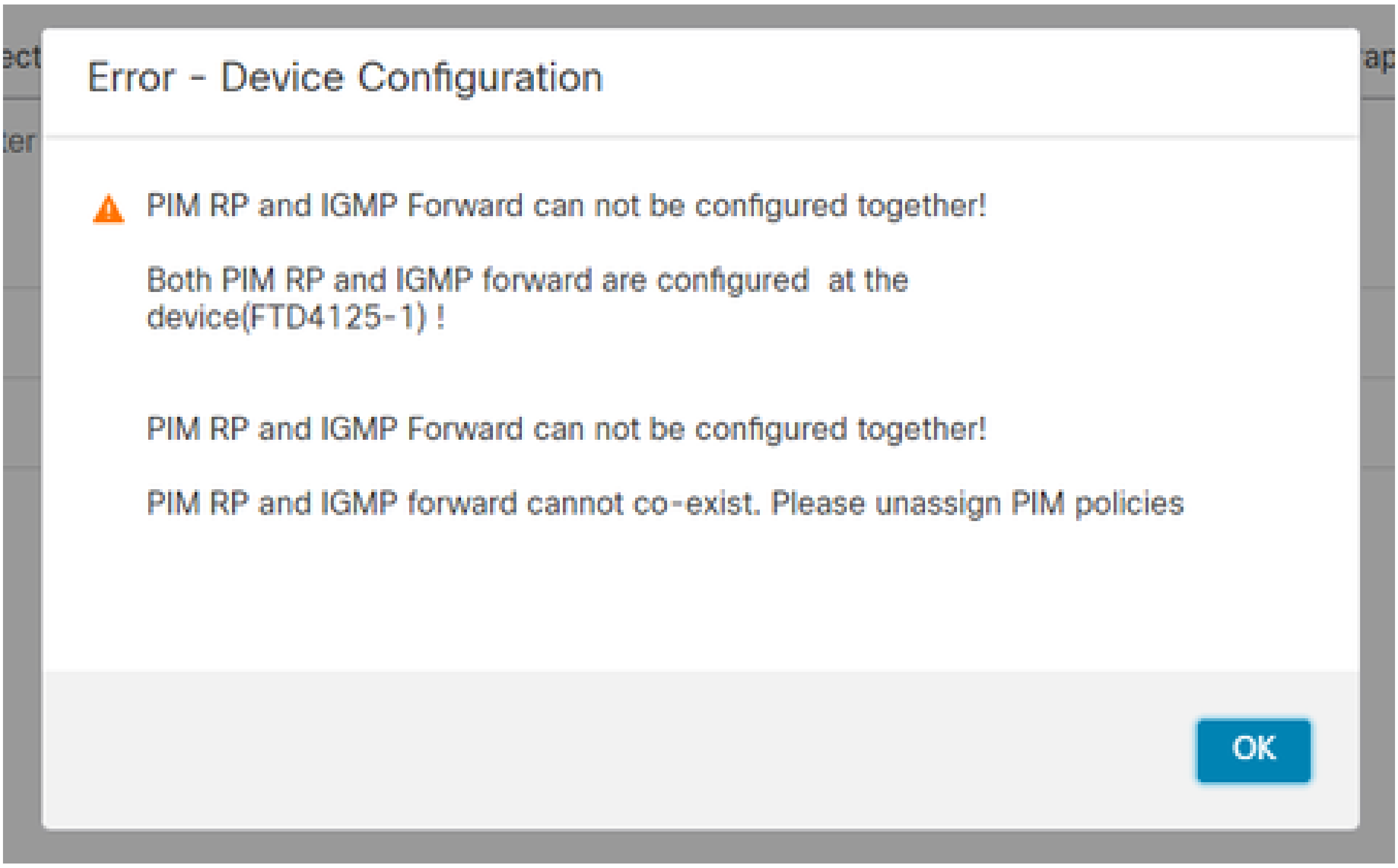
□ Use bi-directional forwarding

● Use this RP for all Multicast Groups

○ Use this RP for all Multicast Groups as specified below

Standard Access List:*

لا يمكن تكوين ASA/FTD لتوجيه كعب بروتوكول IGMP و PIM في نفس الوقت:



Error - Device Configuration

PIM RP and IGMP Forward can not be configured together!

Both PIM RP and IGMP forward are configured at the device(FTD4125-1) !

PIM RP and IGMP Forward can not be configured together!

PIM RP and IGMP forward cannot co-exist. Please unassign PIM policies

التكوين الناتج على FTD:

<#root>

```
firepower#
show running-config multicast-routing


multicast-routing


<-- Multicast routing is enabled globally on the device


firepower#
show running-config pim


pim rp-address 198.51.100.1              <-- Static RP is configured on the firewall



firepower#
ping 198.51.100.1


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.51.100.1, timeout is 2 seconds:
!!!!!                                    <-- The RP is reachable


Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

على جدار حماية ASA، هناك تكوين مماثل:

```
<#root>
asa(config)#
multicast-routing


asa(config)#
pim rp-address 198.51.100.1
```

تكوين RP (موجه Cisco):

```
<#root>
ip multicast-routing
ip pim rp-address 198.51.100.1           <-- The router is the RP
```

```
!
interface GigabitEthernet0/0.206
 encapsulation dot1Q 206
 ip address 192.168.103.61 255.255.255.0

 ip pim sparse-dense-mode                <-- The interface participates in multicast routing

 ip ospf 1 area 0
!
interface GigabitEthernet0/0.207
 encapsulation dot1Q 207
 ip address 192.168.104.61 255.255.255.0

 ip pim sparse-dense-mode                <-- The interface participates in multicast routing

 ip ospf 1 area 0
!
interface Loopback0


ip address 198.51.100.1 255.255.255.255

<-- The router is the RP


ip pim sparse-dense-mode                <-- The interface participates in multicast routing

 ip ospf 1 area 0
```

التحقق

تحقق من مستوى التحكم في البث المتعدد على FTD عند عدم وجود حركة مرور للبث المتعدد (المرسلون أو المستقبلون):

<#root>

```
firepower#

show pim interface

Address            Interface        PIM  Nbr   Hello  DR          DR
                                         Count Intvl  Prior

192.168.105.60     NET207           on   1     30     1           this system


<-- PIM enabled on the interface. There is 1 PIM neighbor

192.168.1.50       INSIDE           on   0     30     1           this system        <-- PIM enabled on t

0.0.0.0            diagnostic       off  0     30     1           not elected

192.168.103.50     OUTSIDE          on   1     30     1           192.168.103.61     <-- PIM enabled on t
```

التحقق من جيران PIM:

<#root>

```
firepower#

show pim neighbor

Neighbor Address    Interface          Uptime    Expires DR pri Bidir
192.168.105.50      NET207             00:05:41  00:01:28 1      B
192.168.103.61      OUTSIDE            00:05:39  00:01:32 1 (DR)
```

يعلن RP عن نطاق مجموعة البث المتعدد بأكمله:

<#root>

```
firepower#

show pim group-map

Group Range         Proto   Client   Groups RP address      Info
224.0.1.39/32*      DM      static   0      0.0.0.0
224.0.1.40/32*      DM      static   0      0.0.0.0
224.0.0.0/24*       L-Local static   1      0.0.0.0
232.0.0.0/8*        SSM     config   0      0.0.0.0

224.0.0.0/4*        SM      config   2      198.51.100.1    RPF: OUTSIDE,192.168.103.61     <-- The mult

224.0.0.0/4         SM      static   0      0.0.0.0         RPF: ,0.0.0.0
```

يحتوي جدول مسار جدار الحماية على بعض الإدخالات غير ذات الصلة (239.255.255.250 وه بروتوكول اكتشاف الخدمة البسيط (SSDP) المستخدم من قبل الموردين مثل Mac OS و Microsoft Windows):

<#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), 00:17:35/never, RP 198.51.100.1, flags: SCJ
  Incoming interface: OUTSIDE
  RPF nbr: 192.168.103.61
  Immediate Outgoing interface list:
    INSIDE, Forward, 00:17:35/never
```

يوجد نفق PIM بين جدران الحماية و RP:

<#root>

```
firepower#

show pim tunnel

Interface           RP Address        Source Address

Tunnel0             198.51.100.1      192.168.103.50


<-- PIM tunnel between the FTD and the RP
```

كما يمكن رؤية نفق PIM على جدول اتصال جدار الحماية:

<#root>

```
firepower#

 show conn all detail address 198.51.100.1
...
PIM OUTSIDE: 198.51.100.1/0 NP Identity Ifc: 192.168.103.50/0,


<-- PIM tunnel between the FTD and the RP
, flags , idle 16s, uptime 3m8s, timeout 2m0s, bytes 6350
Connection lookup keyid: 153426246
```

التحقق من جدار حماية ASA:

<#root>

```
asa#

show pim neighbor


Neighbor Address   Interface      Uptime     Expires DR pri Bidir
192.168.105.60     NET207         2d21h      00:01:29 1 (DR) B
192.168.104.61     OUTSIDE        00:00:18   00:01:37 1 (DR)
```

<#root>

```
asa#

show pim tunnel

Interface           RP Address        Source Address

Tunnel0             198.51.100.1      192.168.104.50
```

```
<-- PIM tunnel between the ASA and the RP
```

RP (موجه Cisco) التحقق من RP. هناك بعض مجموعات البث المتعدد ل SSDP و Auto-RP:

<#root>

```
Router1#

show ip pim rp

Group: 239.255.255.250, RP: 198.51.100.1, next RP-reachable in 00:01:04
Group: 224.0.1.40, RP: 198.51.100.1, next RP-reachable in 00:00:54
```

التحقق بمجرد إعلان المستلم عن وجوده

ملاحظة: أوامر جدار الحماية الموضحة في هذا القسم قابلة للتطبيق الكامل على ASA و FTD.

يتلقى ال ASA رسالة تقرير عضوية IGMP وينشئ إدخالات (*، g) لبروتوكول IGMP وخط المسار:

<#root>

```
asa#

show igmp group 230.10.10.10

IGMP Connected Group Membership
Group Address    Interface          Uptime    Expires   Last Reporter

230.10.10.10     INSIDE             00:01:15  00:03:22  192.168.2.100     <-- Host 192.168.2.100 repor
```

يقوم جدار حماية ASA بإنشاء مسار لمجموعة البث المتعدد:

<#root>

```
asa#

show mroute 230.10.10.10


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)

, 00:00:17/never,

RP 198.51.100.1

, flags: SCJ

<-- The mroute for group 230.10.10.10


Incoming interface: OUTSIDE


<-- Expected interface for a multicast packet from the source. If the packet is not received on this int

  RPF nbr: 192.168.104.61

 Immediate Outgoing interface list:                                 <-- The OIL points towards the recei
    INSIDE, Forward, 00:01:17/never
```

تتمثل عملية تحقق أخرى من جدار الحماية في إخراج مخطط PIM:

<#root>

```
asa#

show pim topology 230.10.10.10

...

(*,230.10.10.10) SM Up: 00:07:15 RP: 198.51.100.1                    <-- An entry for multicast group 23

JP: Join(00:00:33) RPF: OUTSIDE,192.168.104.61 Flags: LH
  INSIDE             00:03:15  fwd LI LH
```

ملاحظة: إذا لم يكن لجدار الحماية مسار نحو RP، يظهر إخراج تصحيح الأخطاء PIM فشل البحث عن RPF

فشل بحث RPF في إخراج تصحيح الأخطاء PIM:

<#root>

```
asa#

debug pim


IPv4 PIM: RPF lookup failed for root 198.51.100.1                    <-- The RPF look fails because ther

IPv4 PIM: RPF lookup failed for root 198.51.100.1
```

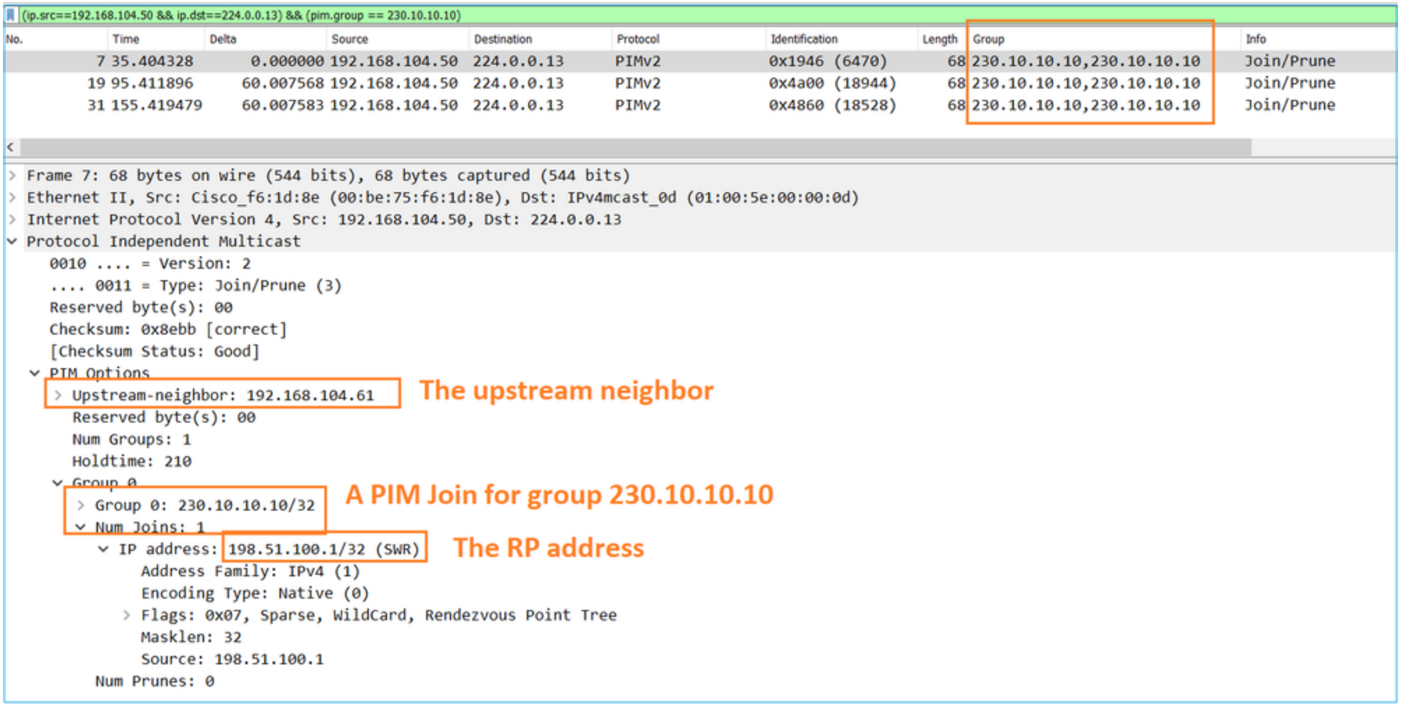
```
IPv4 PIM: (*,230.10.10.10) Processing Periodic Join-Prune timer
IPv4 PIM: (*,230.10.10.10) J/P processing
IPv4 PIM: (*,230.10.10.10) Periodic J/P scheduled in 50 secs
IPv4 PIM: (*,230.10.10.10) No RPF neighbor to send J/P
```

في حالة الموافقة على كل شيء، يرسل جدار الحماية رسالة PIM Join-Prune إلى RP:

<#root>

```
asa#

debug pim group 230.10.10.10


IPv4 PIM group debugging is on
for group 230.10.10.10

IPv4 PIM: (*,230.10.10.10) J/P scheduled in 0.0 secs
IPv4 PIM: [0] (*,230.10.10.10/32) MRIB modify A NS
IPv4 PIM: [0] (*,230.10.10.10/32) NULLIF-skip MRIB modify !A !NS
IPv4 PIM: [0] (*,230.10.10.10/32) OUTSIDE MRIB modify A NS
IPv4 PIM: (*,230.10.10.10) Processing timers
IPv4 PIM: (*,230.10.10.10) J/P processing
IPv4 PIM: (*,230.10.10.10) Periodic J/P scheduled in 50 secs

IPv4 PIM: (*,230.10.10.10) J/P adding Join on OUTSIDE
```

يظهر الالتقاط أن رسائل PIM Join يتم إرسالها كل 1 دقيقة ودقيقة PIM Hellos كل 30 ثانية. يستخدم PIM بروتوكول IP 224.0.0.13:



```
(ip.src==192.168.104.50 && ip.dst==224.0.0.13) && (pim.group == 230.10.10.10)
No.     Time        Delta     Source          Destination  Protocol  Identification   Length Group                      Info
      7 35.404328   0.000000  192.168.104.50  224.0.0.13   PIMv2     0x1946 (6470)        68 230.10.10.10,230.10.10.10  Join/Prune
     19 95.411896  60.007568  192.168.104.50  224.0.0.13   PIMv2     0x4a00 (18944)       68 230.10.10.10,230.10.10.10  Join/Prune
     31 155.419479 60.007583  192.168.104.50  224.0.0.13   PIMv2     0x4860 (18528)       68 230.10.10.10,230.10.10.10  Join/Prune

> Frame 7: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
> Ethernet II, Src: Cisco_f6:1d:8e (00:be:75:f6:1d:8e), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
> Internet Protocol Version 4, Src: 192.168.104.50, Dst: 224.0.0.13
v Protocol Independent Multicast
    0010 .... = Version: 2
    .... 0011 = Type: Join/Prune (3)
    Reserved byte(s): 00
    Checksum: 0x8ebb [correct]
    [Checksum Status: Good]
  v PIM Options
    > Upstream-neighbor: 192.168.104.61
      Reserved byte(s): 00
      Num Groups: 1
      Holdtime: 210
    v Group 0
      > Group 0: 230.10.10.10/32
      v Num Joins: 1
        v IP address: 198.51.100.1/32 (SWR)
            Address Family: IPv4 (1)
            Encoding Type: Native (0)
          > Flags: 0x07, Sparse, WildCard, Rendezvous Point Tree
            Masklen: 32
            Source: 198.51.100.1
        Num Prunes: 0
```

The upstream neighbor

A PIM Join for group 230.10.10.10

The RP address

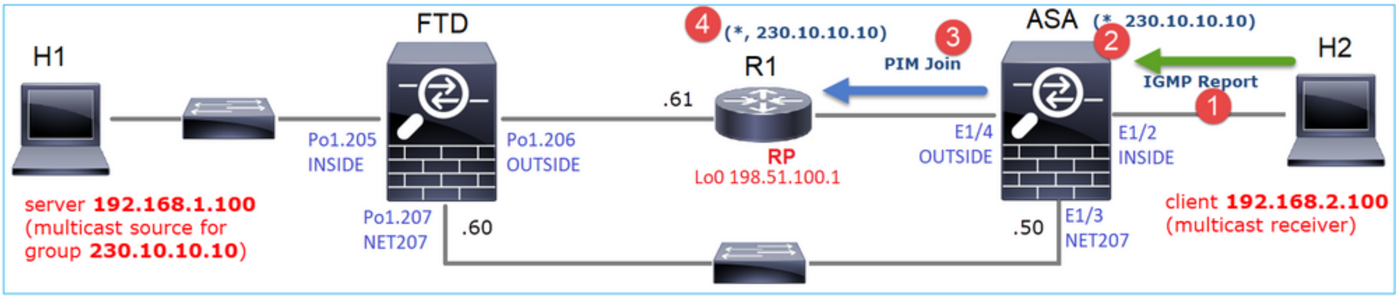
تلميح: عامل تصفية عرض Wireshark: (ip.src==192.168.104.50 & ip.dst==224.0.0.13) & & (pim.group = 230.10.10.10)
- 192.168.104.50 هو جدار الحماية IP الخاص بواجهة الخروج (نحو جار PIM للتدفق)
- 224.0.0.13 هي مجموعة البث المتعدد ل PIM حيث يتم إرسال وصلات PIM وتقسيماتها
- 230.10.10.10 هي مجموعة البث المتعدد التي نرسل لها PIM Join/Prune

يقوم RP بإنشاء مسار (*، g). لاحظ أنه نظرا لعدم وجود أي خوادم بعد، فإن الواجهة الواردة خالية:

<#root>

```
Router1#

show ip mroute 230.10.10.10 | b \(


(*, 230.10.10.10), 00:00:27/00:03:02, RP 198.51.100.1, flags: S          <-- The mroute for the multicas



Incoming interface: Null

, RPF nbr 0.0.0.0        <-- No incoming multicast stream


Outgoing interface list:



GigabitEthernet0/0.207

, Forward/Sparse-Dense, 00:00:27/00:03:02

<-- There was a PIM Join on this interface
```

ويمكن تمثيل ذلك على النحو التالي:



1. تم إستلام تقرير IGMP على ASA.
2. تتم إضافة مسار (*، G).
3. يرسل ال ASA PIM ربط رسالة إلى ال RP (198.51.100.1).
4. يستقبل RP رسالة الانضمام ويضيف مسار (*، G).

في الوقت نفسه، لا توجد طرق في برنامج الإرسال فائق السرعة (FTD) نظرا لعدم وجود

تقرير IGMP أو PIM Join:

<#root>

```
firepower#

show mroute 230.10.10.10

No mroute entries found.
```

التحقق من الصحة عند إرسال الخادم لتدفق البث المتعدد

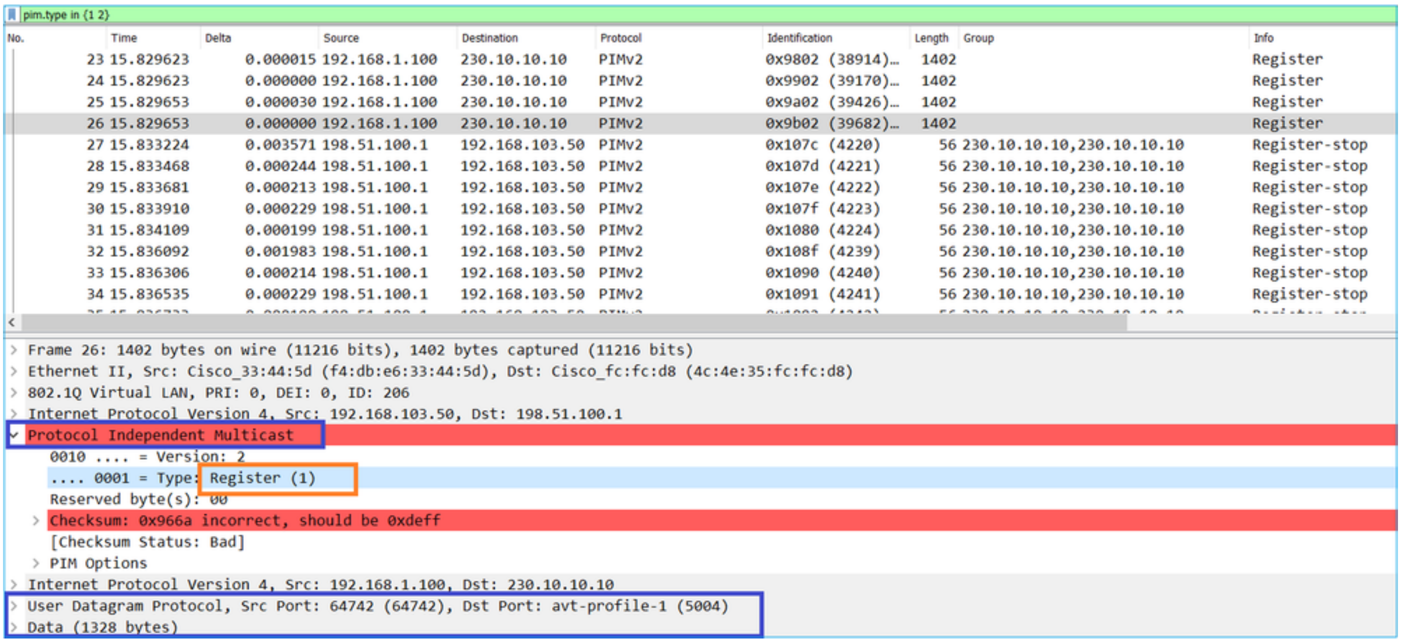
يحصل FTD على تدفق البث المتعدد من H1 ويبدأ عملية تسجيل PIM باستخدام RP. يرسل FTD رسالة سجل PIM للبث الأحادي إلى RP. يرسل RP رسالة انضمام PIM إلى موجه الخطوة الأولى (FHR)، وهو FTD في هذه الحالة، للانضمام إلى شجرة البث المتعدد. ثم يرسل رسالة إيقاف تسجيل.

<#root>

```
firepower#

debug pim group 230.10.10.10


IPv4 PIM group debugging is on
for group 230.10.10.10
firepower#
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB update (f=20,c=20)
IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on INSIDE
IPv4 PIM: (192.168.1.100,230.10.10.10) Create entry

IPv4 PIM: (192.168.1.100,230.10.10.10) RPF changed from 0.0.0.0/- to 192.168.1.100/INSIDE



<-- The FTD receives a multicast stream on INSIDE interface for group 230.10.10.10


IPv4 PIM: (192.168.1.100,230.10.10.10) Connected status changed from off to on
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify NS
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) MRIB modify DC
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify A NS
IPv4 PIM: (192.168.1.100,230.10.10.10) Set alive timer to 210 sec
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify !NS
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) MRIB modify !DC

IPv4 PIM: (192.168.1.100,230.10.10.10) Start registering to 198.51.100.1                <-- The FTD


IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 J/P state changed from Null to Join
IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 FWD state change from Prune to Forward
IPv4 PIM: (192.168.1.100,230.10.10.10) Updating J/P status from Null to Join
IPv4 PIM: (192.168.1.100,230.10.10.10) J/P scheduled in 0.0 secs
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB modify NS
IPv4 PIM: (192.168.1.100,230.10.10.10) Set SPT bit
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) MRIB modify NS
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify !A
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB modify A !NS
```

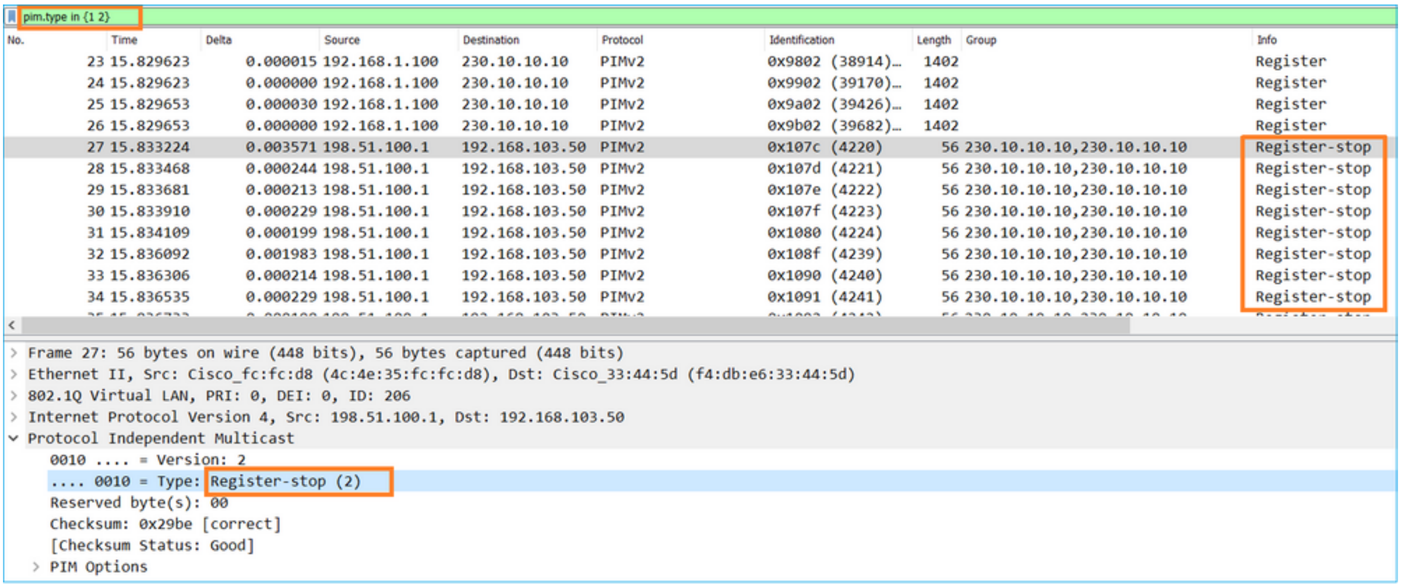
```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) Tunnel0 MRIB modify F NS
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB modify !SP
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB update (f=2,c=20)

IPv4 PIM: J/P entry: Join root: 192.168.1.100 group: 230.10.10.10 flags: S                  <-- The FTD


IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE J/P state changed from Null to Join
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE FWD state change from Prune to Forward
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify F NS
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE Raise J/P expiration timer to 210 seconds
IPv4 PIM: J/P entry: Join root: 192.168.1.100 group: 230.10.10.10 flags: S
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE Raise J/P expiration timer to 210 seconds
IPv4 PIM: (192.168.1.100,230.10.10.10) Processing timers
IPv4 PIM: (192.168.1.100,230.10.10.10) J/P processing
IPv4 PIM: (192.168.1.100,230.10.10.10) Suppress J/P to connected source
IPv4 PIM: (192.168.1.100,230.10.10.10) Suppress J/P to connected source
IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 Processing timers
IPv4 PIM: J/P entry: Join root: 192.168.1.100 group: 230.10.10.10 flags: S
IPv4 PIM: (192.168.1.100,230.10.10.10) NET207 J/P state changed from Null to Join
IPv4 PIM: (192.168.1.100,230.10.10.10) NET207 FWD state change from Prune to Forward
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify F NS
IPv4 PIM: (192.168.1.100,230.10.10.10) NET207 Raise J/P expiration timer to 210 seconds
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=29,c=20)
IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on NET207
IPv4 PIM: (192.168.1.100,230.10.10.10) Send [0/0] Assert on NET207
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify !SP
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=9,c=20)
IPv4 PIM: J/P entry: Prune root: 192.168.1.100 group: 230.10.10.10 flags: S
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE J/P state changed from Join to Null
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE FWD state change from Forward to Prune
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify !F !NS
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=29,c=20)
IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on NET207
IPv4 PIM: (192.168.1.100,230.10.10.10) Send [0/0] Assert on NET207
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify !SP
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=9,c=20)
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE Processing timers

IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop                              <-- The RP s



IPv4 PIM: (192.168.1.100,230.10.10.10) Stop registering


IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 J/P state changed from Join to Null
IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 FWD state change from Forward to Prune
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) Tunnel0 MRIB modify !F !NS
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 Processing timers
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB update (f=22,c=20)
IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on INSIDE
IPv4 PIM: (192.168.1.100,230.10.10.10) Set alive timer to 210 sec
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB modify !SP
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB update (f=2,c=20)
```

رسالة سجل PIM هي رسالة PIM تحمل بيانات UDP مع معلومات سجل PIM:



```
pim.type in {1 2}
No.  Time       Delta     Source        Destination     Protocol  Identification    Length  Group                     Info
  23 15.829623  0.000015 192.168.1.100  230.10.10.10    PIMv2     0x9802 (38914)…   1402                              Register
  24 15.829623  0.000000 192.168.1.100  230.10.10.10    PIMv2     0x9902 (39170)…   1402                              Register
  25 15.829653  0.000030 192.168.1.100  230.10.10.10    PIMv2     0x9a02 (39426)…   1402                              Register
  26 15.829653  0.000000 192.168.1.100  230.10.10.10    PIMv2     0x9b02 (39682)…   1402                              Register
  27 15.833224  0.003571 198.51.100.1   192.168.103.50  PIMv2     0x107c (4220)       56 230.10.10.10,230.10.10.10   Register-stop
  28 15.833468  0.000244 198.51.100.1   192.168.103.50  PIMv2     0x107d (4221)       56 230.10.10.10,230.10.10.10   Register-stop
  29 15.833681  0.000213 198.51.100.1   192.168.103.50  PIMv2     0x107e (4222)       56 230.10.10.10,230.10.10.10   Register-stop
  30 15.833910  0.000229 198.51.100.1   192.168.103.50  PIMv2     0x107f (4223)       56 230.10.10.10,230.10.10.10   Register-stop
  31 15.834109  0.000199 198.51.100.1   192.168.103.50  PIMv2     0x1080 (4224)       56 230.10.10.10,230.10.10.10   Register-stop
  32 15.836092  0.001983 198.51.100.1   192.168.103.50  PIMv2     0x108f (4239)       56 230.10.10.10,230.10.10.10   Register-stop
  33 15.836306  0.000214 198.51.100.1   192.168.103.50  PIMv2     0x1090 (4240)       56 230.10.10.10,230.10.10.10   Register-stop
  34 15.836535  0.000229 198.51.100.1   192.168.103.50  PIMv2     0x1091 (4241)       56 230.10.10.10,230.10.10.10   Register-stop

> Frame 26: 1402 bytes on wire (11216 bits), 1402 bytes captured (11216 bits)
> Ethernet II, Src: Cisco_33:44:5d (f4:db:e6:33:44:5d), Dst: Cisco_fc:fc:d8 (4c:4e:35:fc:fc:d8)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 206
> Internet Protocol Version 4, Src: 192.168.103.50, Dst: 198.51.100.1
v Protocol Independent Multicast
    0010 .... = Version: 2
    .... 0001 = Type: Register (1)
    Reserved byte(s): 00
  > Checksum: 0x966a incorrect, should be 0xdeff
    [Checksum Status: Bad]
  > PIM Options
> Internet Protocol Version 4, Src: 192.168.1.100, Dst: 230.10.10.10
> User Datagram Protocol, Src Port: 64742 (64742), Dst Port: avt-profile-1 (5004)
> Data (1328 bytes)
```

رسالة إيقاف تسجيل PIM:



```
pim.type in {1 2}
No.  Time       Delta     Source        Destination     Protocol  Identification    Length  Group                     Info
  23 15.829623  0.000015 192.168.1.100  230.10.10.10    PIMv2     0x9802 (38914)…   1402                              Register
  24 15.829623  0.000000 192.168.1.100  230.10.10.10    PIMv2     0x9902 (39170)…   1402                              Register
  25 15.829653  0.000030 192.168.1.100  230.10.10.10    PIMv2     0x9a02 (39426)…   1402                              Register
  26 15.829653  0.000000 192.168.1.100  230.10.10.10    PIMv2     0x9b02 (39682)…   1402                              Register
  27 15.833224  0.003571 198.51.100.1   192.168.103.50  PIMv2     0x107c (4220)       56 230.10.10.10,230.10.10.10   Register-stop
  28 15.833468  0.000244 198.51.100.1   192.168.103.50  PIMv2     0x107d (4221)       56 230.10.10.10,230.10.10.10   Register-stop
  29 15.833681  0.000213 198.51.100.1   192.168.103.50  PIMv2     0x107e (4222)       56 230.10.10.10,230.10.10.10   Register-stop
  30 15.833910  0.000229 198.51.100.1   192.168.103.50  PIMv2     0x107f (4223)       56 230.10.10.10,230.10.10.10   Register-stop
  31 15.834109  0.000199 198.51.100.1   192.168.103.50  PIMv2     0x1080 (4224)       56 230.10.10.10,230.10.10.10   Register-stop
  32 15.836092  0.001983 198.51.100.1   192.168.103.50  PIMv2     0x108f (4239)       56 230.10.10.10,230.10.10.10   Register-stop
  33 15.836306  0.000214 198.51.100.1   192.168.103.50  PIMv2     0x1090 (4240)       56 230.10.10.10,230.10.10.10   Register-stop
  34 15.836535  0.000229 198.51.100.1   192.168.103.50  PIMv2     0x1091 (4241)       56 230.10.10.10,230.10.10.10   Register-stop

> Frame 27: 56 bytes on wire (448 bits), 56 bytes captured (448 bits)
> Ethernet II, Src: Cisco_fc:fc:d8 (4c:4e:35:fc:fc:d8), Dst: Cisco_33:44:5d (f4:db:e6:33:44:5d)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 206
> Internet Protocol Version 4, Src: 198.51.100.1, Dst: 192.168.103.50
v Protocol Independent Multicast
    0010 .... = Version: 2
    .... 0010 = Type: Register-stop (2)
    Reserved byte(s): 00
    Checksum: 0x29be [correct]
    [Checksum Status: Good]
  > PIM Options
```

تلميح: لعرض تسجيل PIM ورسائل إيقاف تسجيل PIM فقط على Wireshark، يمكنك إستخدام عامل تصفية العرض: PIM.type في {1 2}

يحصل جدار الحماية (موجه الخطوة الأخيرة) على تدفق البث المتعدد على الواجهة في الخارج، ويبدأ تبديل شجرة المسار الأقصر (SPT) إلى واجهة NET207:

<#root>

asa#

debug pim group 230.10.10.10

```
IPv4 PIM group debugging is on
for group 230.10.10.10

IPv4 PIM: (*,230.10.10.10) Processing Periodic Join-Prune timer
IPv4 PIM: (*,230.10.10.10) J/P processing
IPv4 PIM: (*,230.10.10.10) Periodic J/P scheduled in 50 secs
IPv4 PIM: (*,230.10.10.10) J/P adding Join on OUTSIDE
```

<-- A PIM Join message is sent from the interface OUTSIDE

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB update (f=20,c=20)
```

IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on OUTSIDE <-- The m

```
IPv4 PIM: (192.168.1.100,230.10.10.10) Create entry
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify NS
```

IPv4 PIM: (192.168.1.100,230.10.10.10) RPF changed from 0.0.0.0/- to 192.168.105.60/NET207

<-- The SPT switchover starts from the interface OUTSIDE to the interface NET207

```
IPv4 PIM: (192.168.1.100,230.10.10.10) Source metric changed from [0/0] to [110/20]
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) MRIB modify DC
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify A NS
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB modify F NS
IPv4 PIM: (192.168.1.100,230.10.10.10) Set alive timer to 210 sec
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify !NS
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) MRIB modify !DC
IPv4 PIM: (192.168.1.100,230.10.10.10) Updating J/P status from Null to Join
IPv4 PIM: (192.168.1.100,230.10.10.10) J/P scheduled in 0.0 secs
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify NS
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify !SP
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB update (f=2,c=20)
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=28,c=20)
IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on NET207
IPv4 PIM: (192.168.1.100,230.10.10.10)
```

Set SPT bit <-- The SPT bit is set

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) MRIB modify !SP
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify !A
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify A !NS
IPv4 PIM: (192.168.1.100,230.10.10.10)RPT Updating J/P status from Null to Prune
IPv4 PIM: (192.168.1.100,230.10.10.10)RPT Create entry
IPv4 PIM: (192.168.1.100,230.10.10.10)RPT J/P scheduled in 0.0 secs
IPv4 PIM: (192.168.1.100,230.10.10.10) Set alive timer to 210 sec
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify !SP
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=2,c=20)
IPv4 PIM: (192.168.1.100,230.10.10.10)RPT Processing timers
IPv4 PIM: (192.168.1.100,230.10.10.10)RPT J/P processing
```

IPv4 PIM: (192.168.1.100,230.10.10.10)RPT J/P adding Prune on OUTSIDE

<-- A PIM Prune message is sent from the interface OUTSIDE

```
IPv4 PIM: (192.168.1.100,230.10.10.10)RPT Delete entry
IPv4 PIM: (192.168.1.100,230.10.10.10) Processing timers
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10) J/P processing
IPv4 PIM: (192.168.1.100,230.10.10.10) Periodic J/P scheduled in 50 secs

IPv4 PIM: (192.168.1.100,230.10.10.10) J/P adding Join on NET207


<-- A PIM Join message is sent from the interface NET207


IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=22,c=20)
IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on NET207
IPv4 PIM: (192.168.1.100,230.10.10.10) Set alive timer to 210 sec
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify !SP
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=2,c=20)
```

تصحيح أخطاء PIM على FTD عند حدوث المحول:

<#root>

```
IPv4 PIM: J/P entry: Join root: 192.168.1.100 group: 230.10.10.10 flags: S

IPv4 PIM: (192.168.1.100,230.10.10.10) NET207 J/P state changed from Null to Join


<-- A PIM Join message is sent from the interface NET207


IPv4 PIM: (192.168.1.100,230.10.10.10) NET207 FWD state change from Prune to Forward


<-- The packets are sent from the interface NET207


IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify F NS
IPv4 PIM: (192.168.1.100,230.10.10.10) NET207 Raise J/P expiration timer to 210 seconds
IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 Processing timers
...
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=9,c=20)
IPv4 PIM: J/P entry: Prune root: 192.168.1.100 group: 230.10.10.10 flags: S
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE J/P state changed from Join to Null

IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE FWD state change from Forward to Prune


<-- A PIM Prune message is sent from the interface OUTSIDE
```

مسار FTD بمجرد بدء تبديل SPT:

<#root>

```
firepower#

show mroute 230.10.10.10


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

(192.168.1.100, 230.10.10.10), 00:00:06/00:03:23, flags: SF

T                <-- SPT-bit is set when the switchover occurs


  Incoming interface: INSIDE
  RPF nbr: 192.168.1.100, Registering
  Immediate Outgoing interface list:


NET207, Forward, 00:00:06/00:03:23                                     <-- Both interfaces are shown ir




OUTSIDE, Forward, 00:00:06/00:03:23                                    <-- Both interfaces are shown ir


    Tunnel0, Forward, 00:00:06/never
```

في ةياهن لوحم SPT، متي ضرع ةهجاو NET207 طقف يف زيت FTD:

<#root>

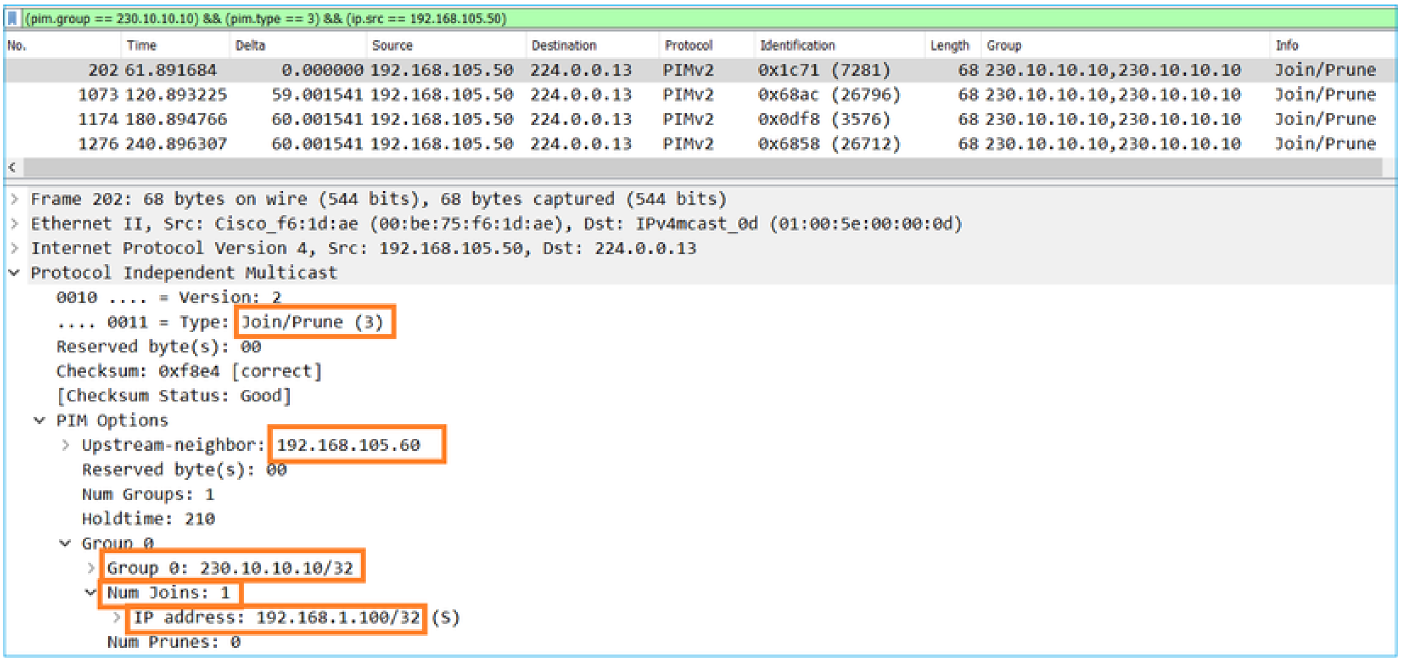
```
firepower#

show mroute 230.10.10.10



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

(192.168.1.100, 230.10.10.10), 00:00:28/00:03:01, flags: SFT
  Incoming interface: INSIDE
  RPF nbr: 192.168.1.100
  Immediate Outgoing interface list:


NET207, Forward

, 00:00:28/00:03:01
```

```
<-- The interface NET207 forwards the multicast stream after the SPT switchover
```

على موجه الخطوة الأخيرة (ASA)، يتم تعيين وحدة بت SPT أيضا:

```
<#root>

asa#

show mroute 230.10.10.10


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), 01:43:09/never, RP 198.51.100.1, flags: SCJ
  Incoming interface: OUTSIDE
  RPF nbr: 192.168.104.61
  Immediate Outgoing interface list:
    INSIDE, Forward, 01:43:09/never


(192.168.1.100, 230.10.10.10)

, 00:00:03/00:03:27, flags: SJ

T        <-- SPT switchover for group 230.10.10.10



Incoming interface:



NET207                                             <-- The multicast packets arrive on interface NET207


  RPF nbr: 192.168.105.60
  Inherited Outgoing interface list:
    INSIDE, Forward, 01:43:09/never
```

المحول من واجهة ASA NET207 (الموجه من الخطوة الأولى الذي قام بالتحويل). يتم إرسال رسالة ربط PIM إلى جهاز البث (FTD):

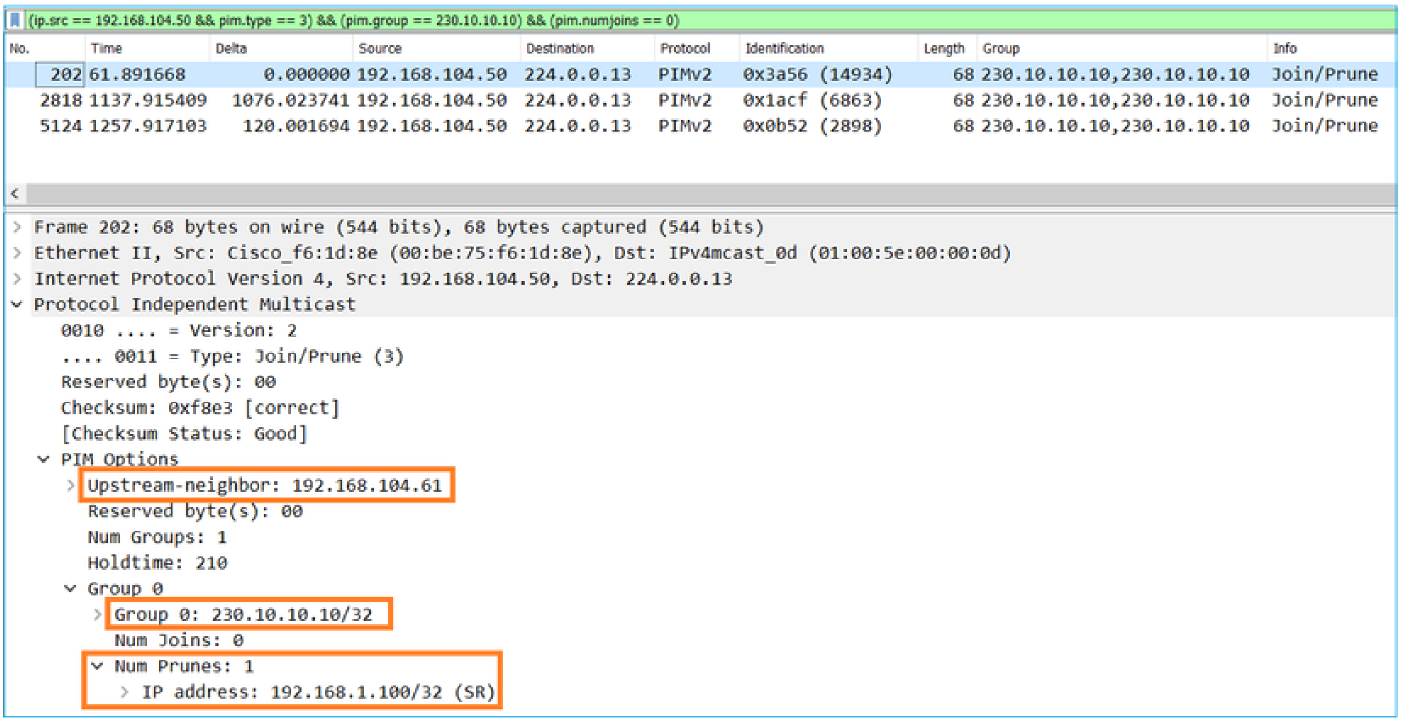


```
(pim.group == 230.10.10.10) && (pim.type == 3) && (ip.src == 192.168.105.50)
```

No.	Time	Delta	Source	Destination	Protocol	Identification	Length	Group	Info
202	61.891684	0.000000	192.168.105.50	224.0.0.13	PIMv2	0x1c71 (7281)	68	230.10.10.10,230.10.10.10	Join/Prune
1073	120.893225	59.001541	192.168.105.50	224.0.0.13	PIMv2	0x68ac (26796)	68	230.10.10.10,230.10.10.10	Join/Prune
1174	180.894766	60.001541	192.168.105.50	224.0.0.13	PIMv2	0x0df8 (3576)	68	230.10.10.10,230.10.10.10	Join/Prune
1276	240.896307	60.001541	192.168.105.50	224.0.0.13	PIMv2	0x6858 (26712)	68	230.10.10.10,230.10.10.10	Join/Prune

```
> Frame 202: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
> Ethernet II, Src: Cisco_f6:1d:ae (00:be:75:f6:1d:ae), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
> Internet Protocol Version 4, Src: 192.168.105.50, Dst: 224.0.0.13
v Protocol Independent Multicast
    0010 .... = Version: 2
    .... 0011 = Type: Join/Prune (3)
    Reserved byte(s): 00
    Checksum: 0xf8e4 [correct]
    [Checksum Status: Good]
  v PIM Options
    > Upstream-neighbor: 192.168.105.60
      Reserved byte(s): 00
      Num Groups: 1
      Holdtime: 210
    v Group 0
      > Group 0: 230.10.10.10/32
      v Num Joins: 1
        > IP address: 192.168.1.100/32 (S)
        Num Prunes: 0
```

على الواجهة الخارجية، يتم إرسال رسالة تنقيح PIM إلى RP لإيقاف تدفق البث المتعدد:



```
(ip.src == 192.168.104.50 && pim.type == 3) && (pim.group == 230.10.10.10) && (pim.numjoins == 0)
```

No.	Time	Delta	Source	Destination	Protocol	Identification	Length	Group	Info
202	61.891668	0.000000	192.168.104.50	224.0.0.13	PIMv2	0x3a56 (14934)	68	230.10.10.10,230.10.10.10	Join/Prune
2818	1137.915409	1076.023741	192.168.104.50	224.0.0.13	PIMv2	0x1acf (6863)	68	230.10.10.10,230.10.10.10	Join/Prune
5124	1257.917103	120.001694	192.168.104.50	224.0.0.13	PIMv2	0x0b52 (2898)	68	230.10.10.10,230.10.10.10	Join/Prune

```
> Frame 202: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
> Ethernet II, Src: Cisco_f6:1d:8e (00:be:75:f6:1d:8e), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
> Internet Protocol Version 4, Src: 192.168.104.50, Dst: 224.0.0.13
v Protocol Independent Multicast
    0010 .... = Version: 2
    .... 0011 = Type: Join/Prune (3)
    Reserved byte(s): 00
    Checksum: 0xf8e3 [correct]
    [Checksum Status: Good]
  v PIM Options
    > Upstream-neighbor: 192.168.104.61
      Reserved byte(s): 00
      Num Groups: 1
      Holdtime: 210
    v Group 0
      > Group 0: 230.10.10.10/32
        Num Joins: 0
      v Num Prunes: 1
        > IP address: 192.168.1.100/32 (SR)
```

التحقق من حركة مرور PIM:

<#root>

```
firepower#
```

`show pim traffic`

```
PIM Traffic Counters
Elapsed time since counters cleared: 1w2d
```

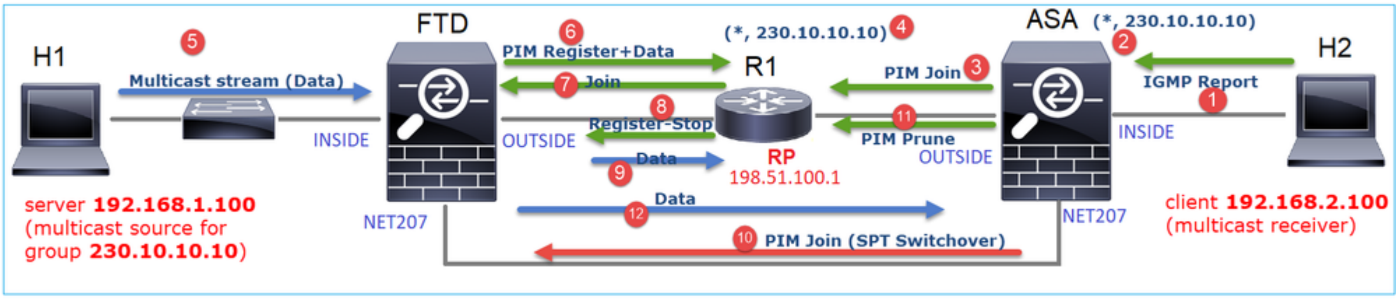
```
                              Received     Sent
Valid PIM Packets             53934        63983
Hello                         36905        77023

Join-Prune                    6495         494          <-- PIM Join/Prune messages



Register                      0            2052         <-- PIM Register messages



Register Stop                 1501         0            <-- PIM Register Stop messages


Assert                        289          362
Bidir DF Election             0            0

Errors:
Malformed Packets                            0
Bad Checksums                                0
Send Errors                                  0
Packet Sent on Loopback Errors               0
Packets Received on PIM-disabled Interface   0
Packets Received with Unknown PIM Version    0
Packets Received with Incorrect Addressing   0
```

للتحقق من عدد الحزم التي تمت معالجتها في المسار البطيء مقابل المسار السريع مقابل نقطة التحكم:

<#root>

```
firepower#

show asp cluster counter



Global dp-counters:


Context specific dp-counters:
MCAST_FP_FROM_PUNT                       2712    Number of multicast packets punted from CP to FP
MCAST_FP_FORWARDED                       94901   Number of multicast packets forwarded in FP
MCAST_FP_TO_SP                           1105138 Number of multicast packets punted from FP to SP
MCAST_SP_TOTAL                           1107850 Number of total multicast packets processed in SP
MCAST_SP_FROM_PUNT                       2712    Number of multicast packets punted from CP to SP
MCAST_SP_FROM_PUNT_FORWARD               2712    Number of multicast packets coming from CP that are for
MCAST_SP_PKTS                            537562  Number of multicast packets that require slow-path atte
MCAST_SP_PKTS_TO_FP_FWD                  109     Number of multicast packets that skip over punt rule and
MCAST_SP_PKTS_TO_CP                      166981  Number of multicast packets punted to CP from SP
MCAST_FP_CHK_FAIL_NO_HANDLE              567576  Number of multicast packets failed with no flow mcast_ha
MCAST_FP_CHK_FAIL_NO_ACCEPT_IFC          223847  Number of multicast packets failed with no accept inter
MCAST_FP_CHK_FAIL_NO_SEQ_NO_MATCH        131     Number of multicast packets failed with no matched seque
MCAST_FP_CHK_FAIL_NO_FP_FWD              313584  Number of multicast packets that cannot be fast-path fo
MCAST_FP_UPD_FOR_UNMATCH_IFC             91      Number of times that multicast flow's ifc_out  cannot be
```

رسم بياني يوضح ما يحدث خطوة بخطوة:



1. يرسل المضيف النهائي (H2) تقرير IGMP للانضمام إلى تدفق البث المتعدد 230.10.10.10.
2. يقوم موجه الخطوة الأخيرة (ASA) الذي هو PIM DR بإنشاء إدخال (*، 230.10.10.10).
3. يرسل ASA رسالة PIM Join نحو RP للمجموعة 230.10.10.10.
4. يقوم RP بإنشاء الإدخال (*، 230.10.10.10).
5. يرسل الخادم بيانات تدفق البث المتعدد.
6. يقوم FTD بتضمين حزم البث المتعدد في رسائل سجل PIM ويرسلها (البث الأحادي) إلى RP. عند هذه النقطة، يرى RP أن لديه جهاز إستقبال نشط، ويزيل كبسلة حزم البث المتعدد، ويرسلها إلى المستقبل.
7. يرسل RP رسالة انضمام PIM إلى FTD للانضمام إلى شجرة البث المتعدد.
8. يرسل RP رسالة إيقاف سجل PIM إلى FTD.
9. يرسل FTD تدفق بث متعدد أصلي (لا يوجد تضمين PIM) نحو RP.
10. يرى موجه الخطوة الأخيرة (ASA) أن المصدر (192.168.1.100) لديه مسار أفضل من واجهة NET207 ويبدأ عملية تحويل. إنه يرسل رسالة ربط PIM إلى جهاز البث (FTD).
11. يرسل الموجه من الخطوة الأخيرة رسالة تنقيح PIM إلى RP.
12. يقوم FTD بإعادة توجيه تدفق البث المتعدد نحو واجهة NET207. ينتقل ASA من الشجرة المشتركة (شجرة RP) إلى الشجرة المصدر (SPT).

المهمة 2 - تكوين موجه بروتوكول PIM (BSR) التمهيد

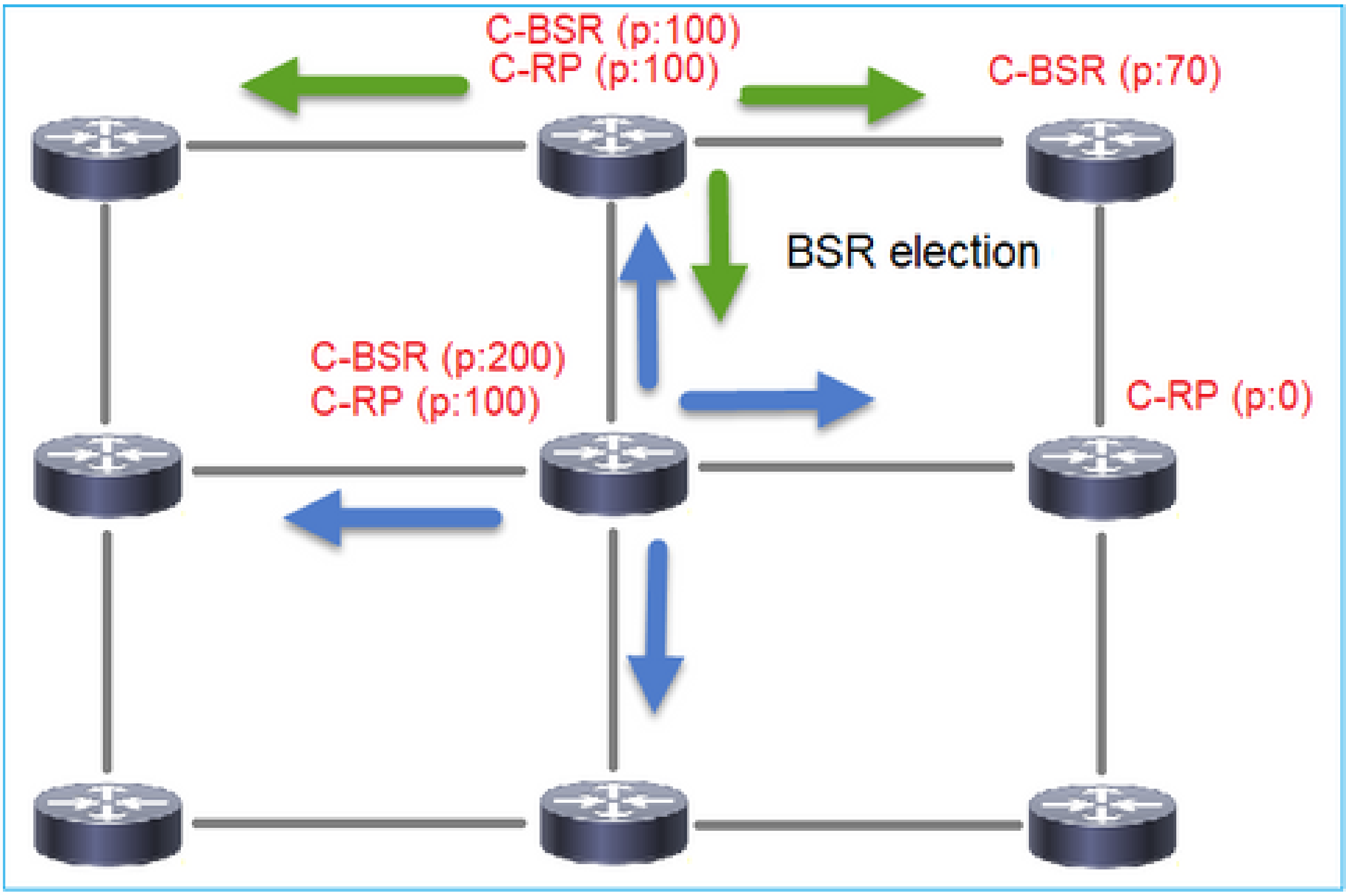
أساسيات BSR

- BSR (RFC 5059) هو آلية بث متعدد لمستوى التحكم تستخدم بروتوكول PIM وتسمح للأجهزة بتعلم معلومات RP بشكل ديناميكي.
- تعريفات BSR:
  - RP المرشح (C-RP): جهاز يريد أن يكون RP.
  - مرشح BSR (C-BSR): جهاز يريد أن يكون BSR ويعلن عن مجموعات RP لأجهزة أخرى.
  - BSR: جهاز ينتخب BSR من بين العديد من C-BSRs. وتفوز الانتخابات بأعلى أولوية في قانون المقاصة.
  - مجموعة البرامج الإقليمية: قائمة بجميع البرامج الإقليمية وأولوياتها.
  - rp: يفوز بالاختيار الجهاز صاحب أدنى أولوية في بروتوكول التوجيه الملاحي.
  - رسالة BSR PIM (فارغة): رسالة PIM المستخدمة في إختيار BSR.
  - رسالة BSR PIM (عادية): رسالة PIM يتم إرسالها إلى IP 224.0.0.13 وتحتوي على معلومات RP و BSR.

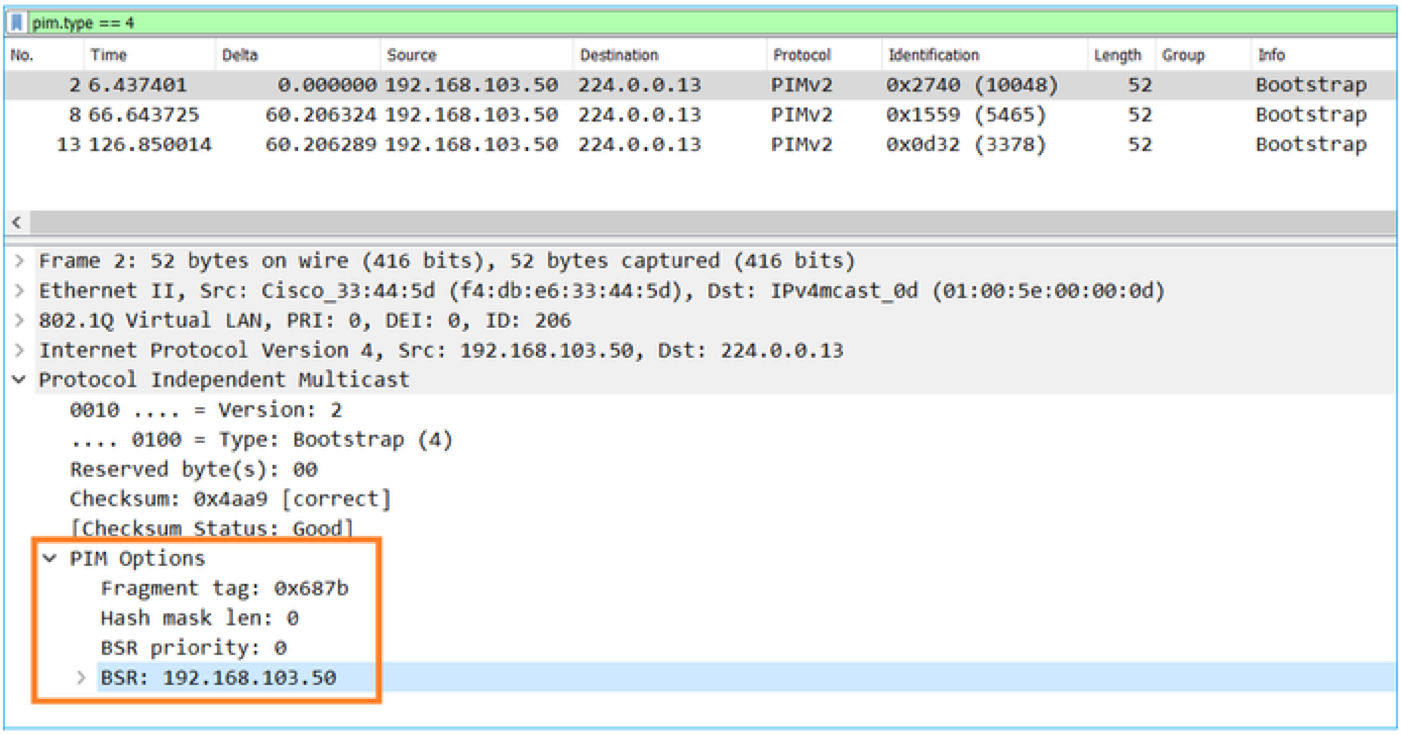
كيفية عمل BSR

1. آلية انتخاب bsr.

يرسل كل C-BSR رسائل PIM BSR فارغة تحتوي على أولوية. فيفوز الجهاز صاحب الأولوية العليا (قيمة الجهاز الاحتياطية هي أعلى عنوان IP) بالانتخابات ويصبح هو BSR. لا تقوم باقي الأجهزة بإرسال رسائل BSR فارغة مرة أخرى.



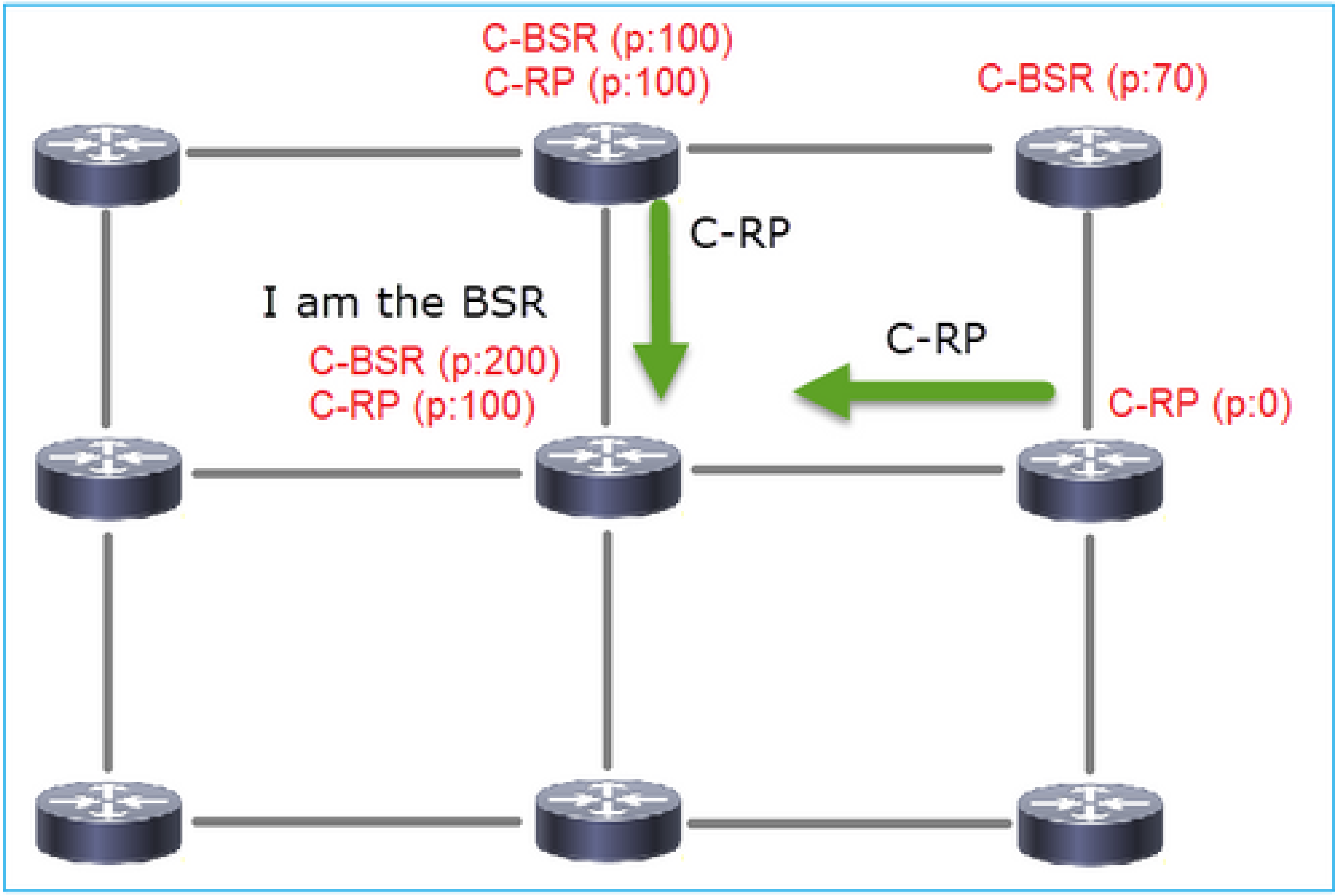
تحتوي رسالة BSR المستخدمة في العملية الإنتخابية على معلومات أولوية C-BSR فقط:



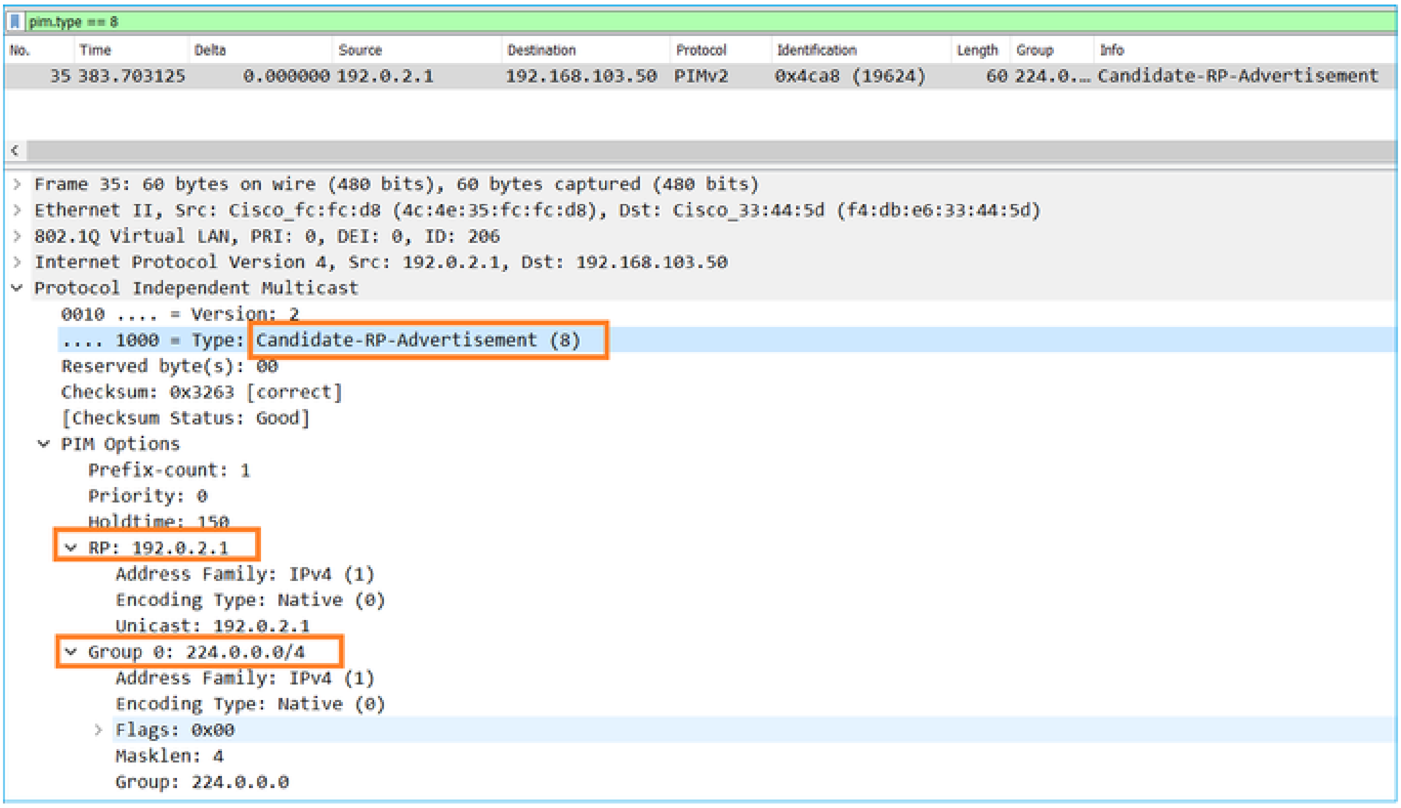
```
pim.type == 4
No.   Time        Delta      Source          Destination  Protocol  Identification  Length  Group  Info
    2 6.437401     0.000000 192.168.103.50  224.0.0.13   PIMv2     0x2740 (10048)    52           Bootstrap
    8 66.643725   60.206324 192.168.103.50  224.0.0.13   PIMv2     0x1559 (5465)     52           Bootstrap
   13 126.850014  60.206289 192.168.103.50  224.0.0.13   PIMv2     0x0d32 (3378)     52           Bootstrap

> Frame 2: 52 bytes on wire (416 bits), 52 bytes captured (416 bits)
> Ethernet II, Src: Cisco_33:44:5d (f4:db:e6:33:44:5d), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 206
> Internet Protocol Version 4, Src: 192.168.103.50, Dst: 224.0.0.13
v Protocol Independent Multicast
    0010 .... = Version: 2
    .... 0100 = Type: Bootstrap (4)
    Reserved byte(s): 00
    Checksum: 0x4aa9 [correct]
    [Checksum Status: Good]
  v PIM Options
      Fragment tag: 0x687b
      Hash mask len: 0
      BSR priority: 0
    > BSR: 192.168.103.50
```

لعرض رسائل BSR في Wireshark، أستخدم عامل تصفية العرض هذا: pim.type == 4

2. تقوم C-RPs بإرسال رسائل BSR للبث الأحادي إلى BSR التي تحتوي على أولوية C-RP الخاصة بها:



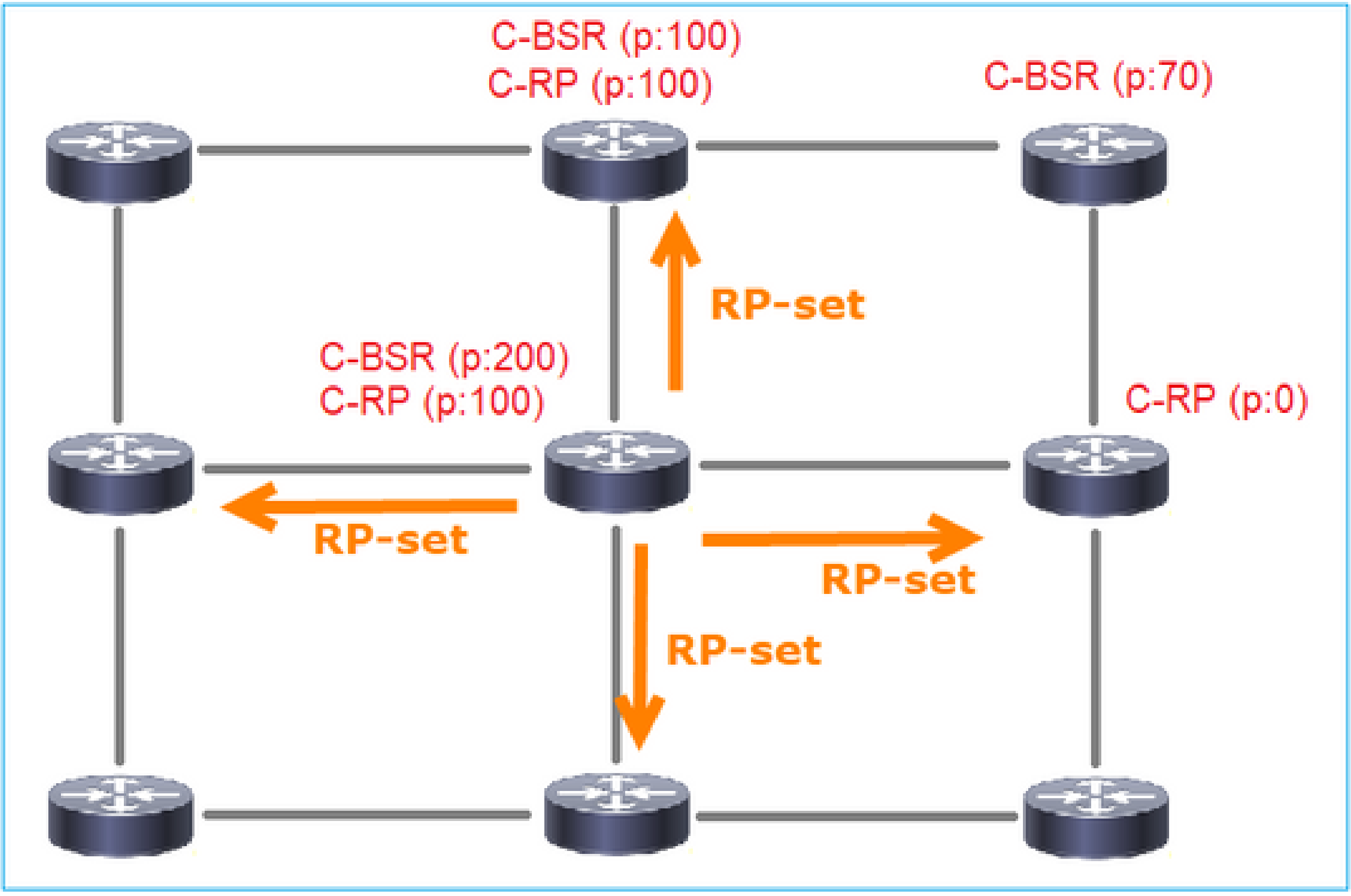
رسالة RP للمرشح:

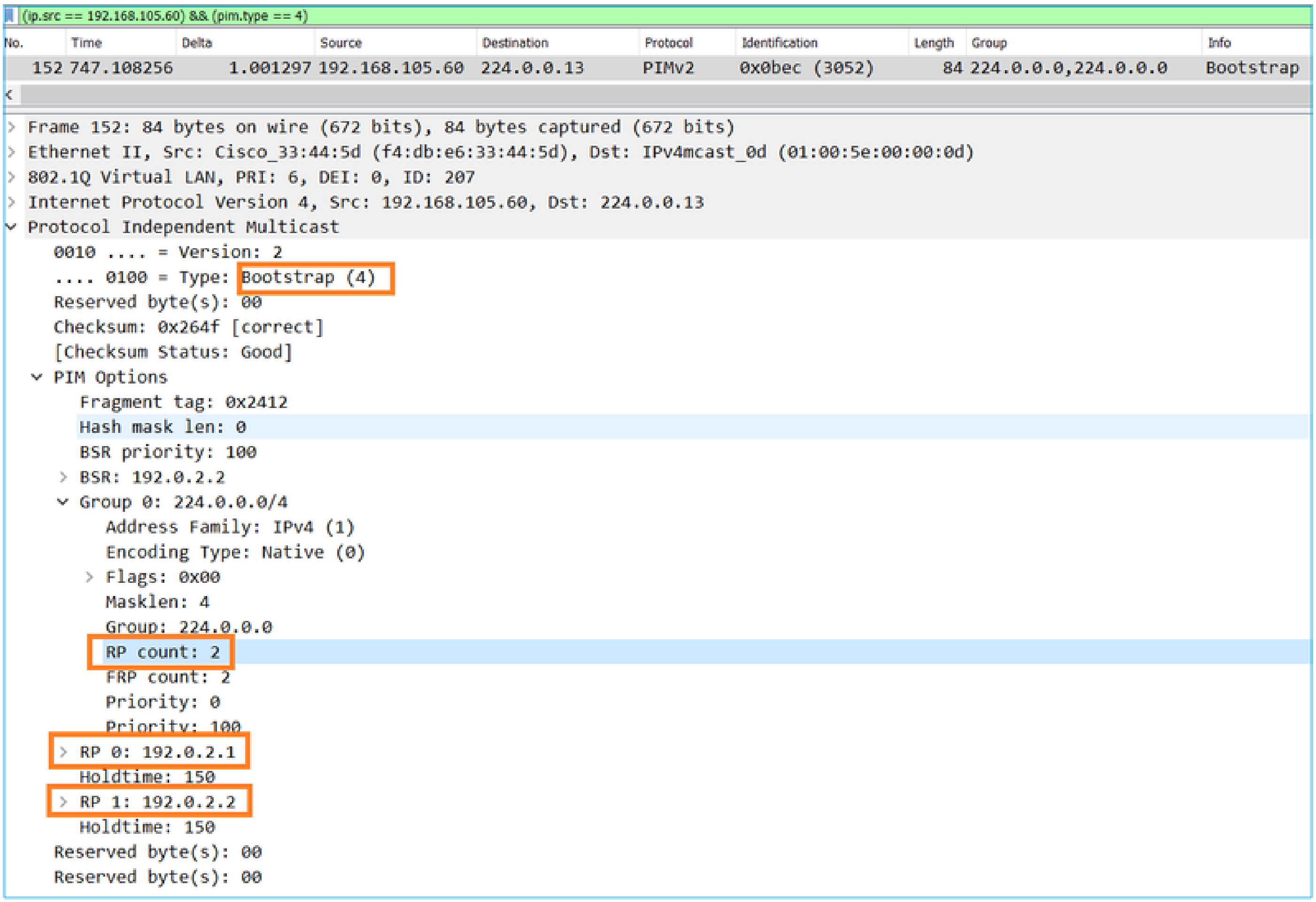


```
pim.type == 8
No.  Time          Delta     Source      Destination     Protocol  Identification  Length  Group     Info
  35 383.703125    0.000000  192.0.2.1   192.168.103.50  PIMv2     0x4ca8 (19624)      60  224.0.…  Candidate-RP-Advertisement

> Frame 35: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: Cisco_fc:fc:d8 (4c:4e:35:fc:fc:d8), Dst: Cisco_33:44:5d (f4:db:e6:33:44:5d)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 206
> Internet Protocol Version 4, Src: 192.0.2.1, Dst: 192.168.103.50
v Protocol Independent Multicast
    0010 .... = Version: 2
    .... 1000 = Type: Candidate-RP-Advertisement (8)
    Reserved byte(s): 00
    Checksum: 0x3263 [correct]
    [Checksum Status: Good]
  v PIM Options
      Prefix-count: 1
      Priority: 0
      Holdtime: 150
    v RP: 192.0.2.1
        Address Family: IPv4 (1)
        Encoding Type: Native (0)
        Unicast: 192.0.2.1
    v Group 0: 224.0.0.0/4
        Address Family: IPv4 (1)
        Encoding Type: Native (0)
      > Flags: 0x00
        Masklen: 4
        Group: 224.0.0.0
```

لعرض رسائل BSR في Wireshark، أستخدم عامل تصفية العرض هذا: PIM.type == 8

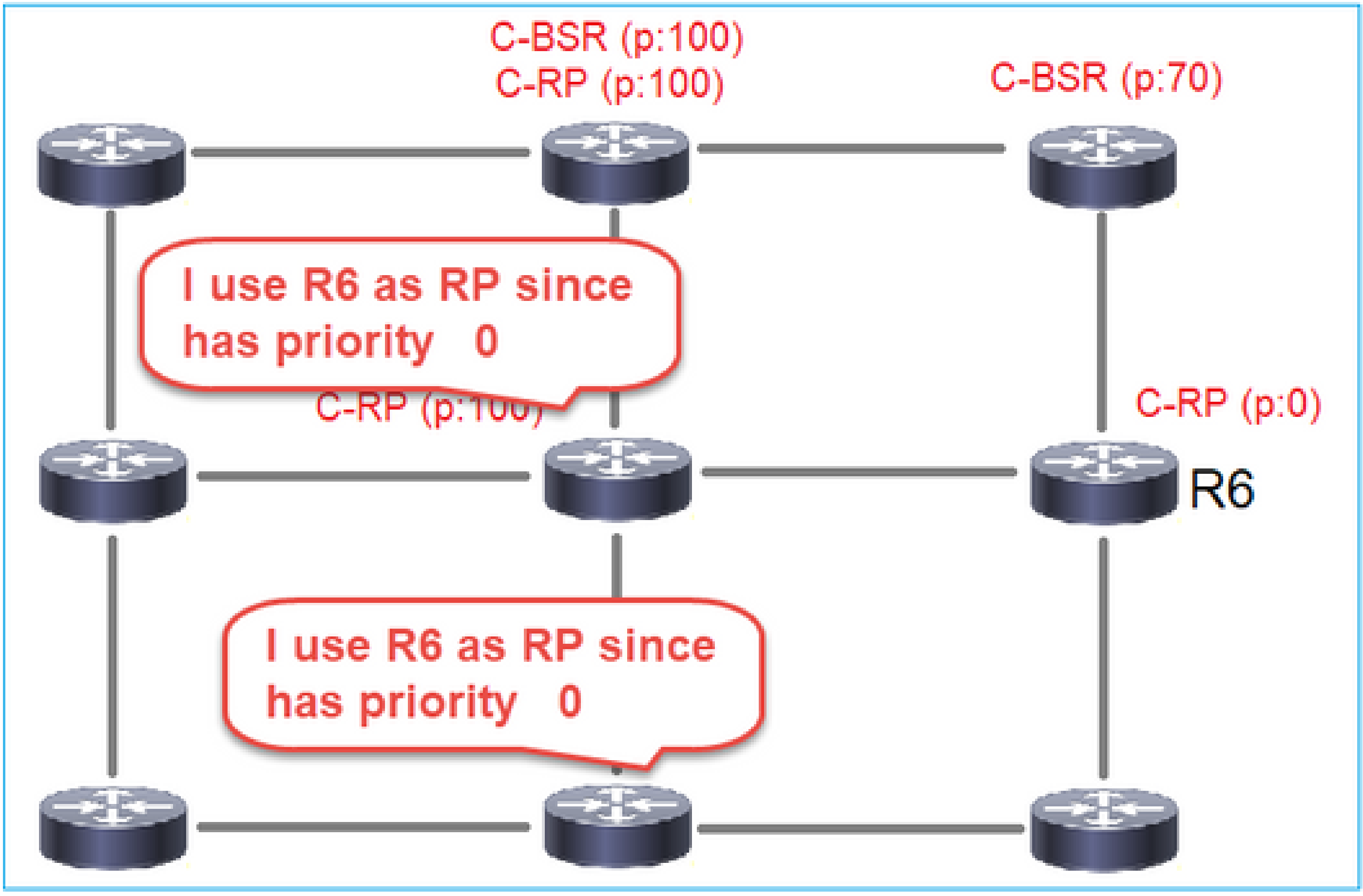
3. يقوم تقرير الأداء الفائق (BSR) بتكوين مجموعة برامج الأداء المطلوب (RP) والإعلان عنها لجميع الدول المجاورة لبروتوكول إدارة البنية الأساسية (PIM):





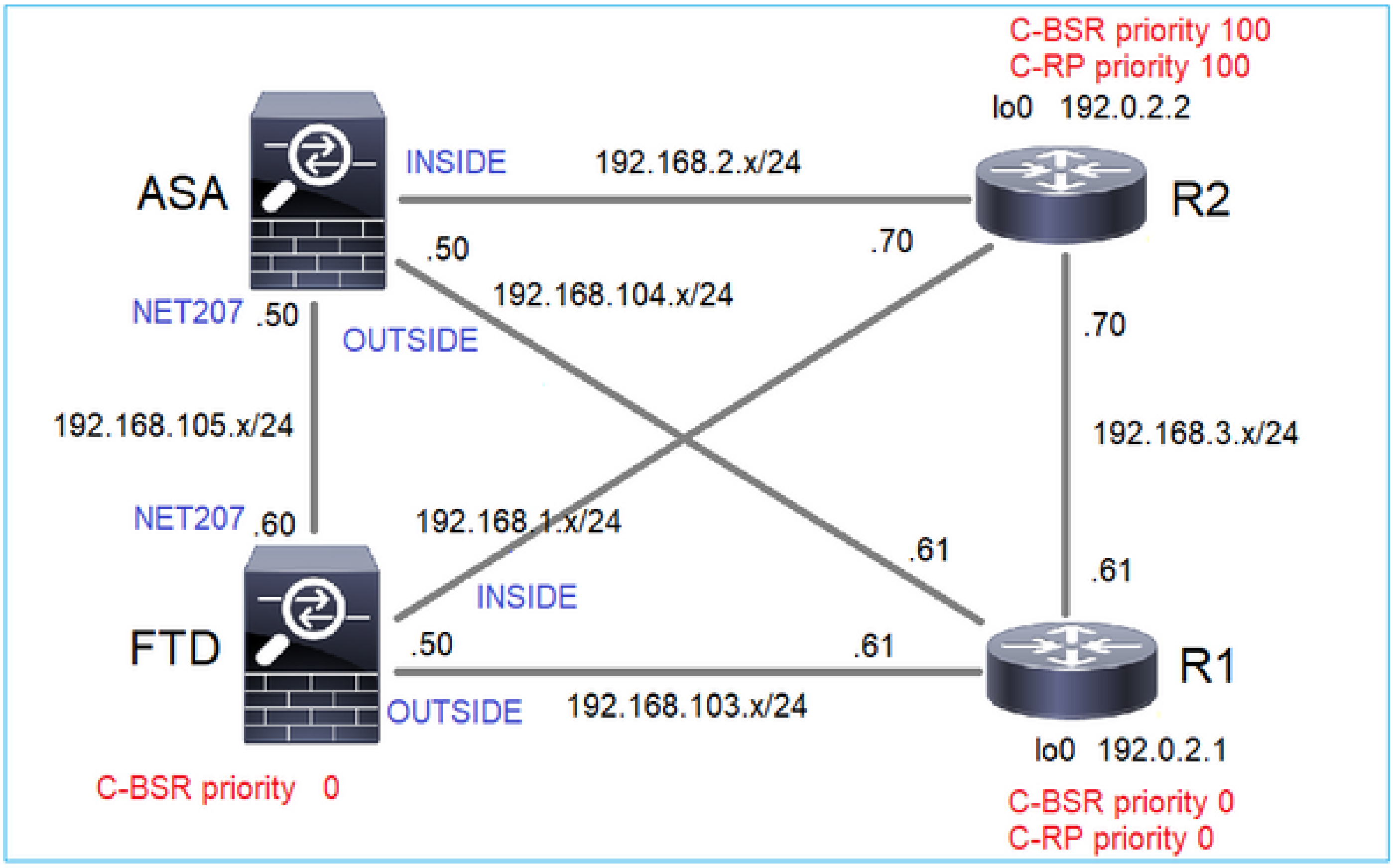
```
(ip.src == 192.168.105.60) && (pim.type == 4)
No.   Time        Delta     Source          Destination  Protocol  Identification  Length  Group                Info
  152 747.108256  1.001297  192.168.105.60  224.0.0.13   PIMv2     0x0bec (3052)       84  224.0.0.0,224.0.0.0  Bootstrap

> Frame 152: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
> Ethernet II, Src: Cisco_33:44:5d (f4:db:e6:33:44:5d), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
> 802.1Q Virtual LAN, PRI: 6, DEI: 0, ID: 207
> Internet Protocol Version 4, Src: 192.168.105.60, Dst: 224.0.0.13
v Protocol Independent Multicast
    0010 .... = Version: 2
    .... 0100 = Type: Bootstrap (4)
    Reserved byte(s): 00
    Checksum: 0x264f [correct]
    [Checksum Status: Good]
  v PIM Options
      Fragment tag: 0x2412
      Hash mask len: 0
      BSR priority: 100
    > BSR: 192.0.2.2
    v Group 0: 224.0.0.0/4
        Address Family: IPv4 (1)
        Encoding Type: Native (0)
      > Flags: 0x00
        Masklen: 4
        Group: 224.0.0.0
        RP count: 2
        FRP count: 2
        Priority: 0
        Priority: 100
    > RP 0: 192.0.2.1
      Holdtime: 150
    > RP 1: 192.0.2.2
      Holdtime: 150
    Reserved byte(s): 00
    Reserved byte(s): 00
```

4. تحصل الموجهات/جدران الحماية على مجموعة إجراءات الحماية (RP) وتنتخب RP استنادا إلى أقل الأولويات:


C-BSR (p:100)
C-RP (p:100)
C-BSR (p:70)
I use R6 as RP since has priority 0
C-RP (p:100)
C-RP (p:0)
R6
I use R6 as RP since has priority 0

متطلبات المهمة

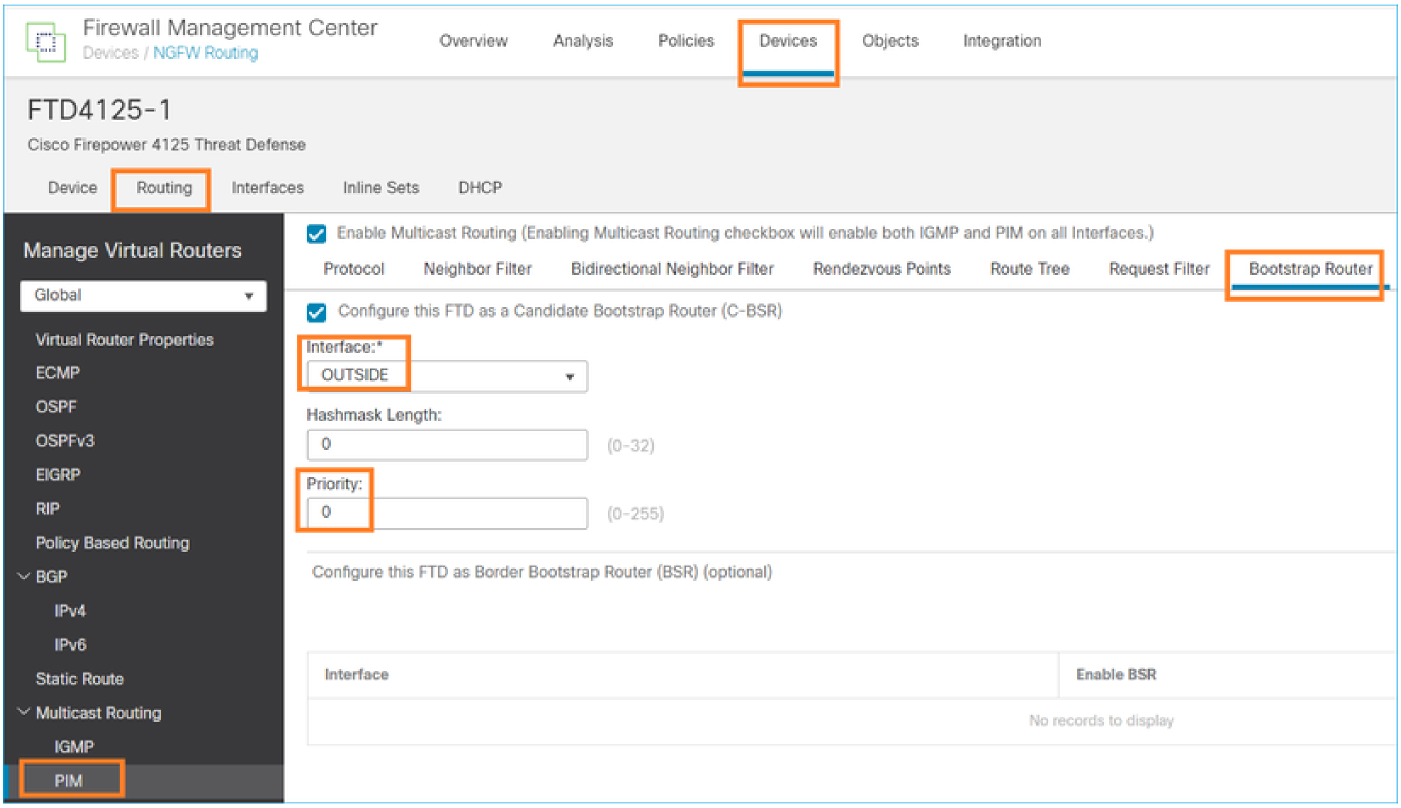
قم بتكوين C-BSRs و C-RPs لكل هذا المخطط:



لهذه المهمة، يجب أن يعلن FTD عن نفسه ك-BSR على الواجهة الخارجية بأولوية BSR 0.

الحل

تكوين FMC ل FTD:



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

☑ Configure this FTD as a Candidate Bootstrap Router (C-BSR)

Interface:* OUTSIDE

Hashmask Length: 0 (0-32)

Priority: 0 (0-255)

Configure this FTD as Border Bootstrap Router (BSR) (optional)

Interface	Enable BSR
No records to display	

التكوين الذي تم نشره:

```
multicast-routing
!
pim bsr-candidate OUTSIDE 0 0
```

التكوين على الأجهزة الأخرى:

R1

```
ip multicast-routing
ip pim bsr-candidate Loopback0 0
ip pim rp-candidate Loopback0
!
interface Loopback0
 ip address 192.0.2.1 255.255.255.255
 ip pim sparse-mode
!
! PIM is also enabled on the transit interfaces (e.g. G0/0.203, G0/0.207, G0/0.205)
```

نفس الشيء بالنسبة للخادم طراز R2، ولكن مع أولويات مختلفة للمكون C-BSR و C-RP

```
ip pim bsr-candidate Loopback0 0 100
ip pim rp-candidate Loopback0 priority 100
```

على ASA هناك فقط multicast بشكل عام يمكن. وهذا يمكن PIM على جميع الواجهات:

```
multicast-routing
```

التحقق

R2 هو BSR المنتخب انظر للأولوية العليا:

<#root>

```
firepower#

show pim bsr-router


PIMv2 BSR information

BSR Election Information

BSR Address: 192.0.2.2             <-- This is the IP of the BSR (R1 lo0)

     Uptime: 00:03:35, BSR Priority: 100

,

Hash mask length: 0
     RPF: 192.168.1.70,INSIDE

<-- The interface to the BSR

     BS Timer: 00:01:34
  This system is candidate BSR
      Candidate BSR address: 192.168.103.50, priority: 0, hash mask length: 0
```

يتم إختيار R1 ك RP انظر لأدنى أولوية:

<#root>

```
firepower#

show pim group-map
```

```
Group Range         Proto    Client    Groups RP address    Info

224.0.1.39/32*      DM       static    0      0.0.0.0
224.0.1.40/32*      DM       static    0      0.0.0.0
224.0.0.0/24*       L-Local  static    1      0.0.0.0
232.0.0.0/8*        SSM      config    0      0.0.0.0
224.0.0.0/4
```

*****

```
       SM
```

BSR

```
 0
```

192.0.2.1

```
     RPF: OUTSIDE,192.168.103.61
```

<-- The elected BSR

```
224.0.0.0/4         SM       BSR       0      192.0.2.2     RPF: INSIDE,192.168.1.70
224.0.0.0/4         SM       static    0      0.0.0.0       RPF: ,0.0.0.0
```

تخضع رسائل BSR للتحقق من إعادة توجيه المسار العكسي (RPF). يمكنك تمكين debug pim bsr للتحقق من ذلك:

<#root>

```
IPv4 BSR: Received BSR message from 192.168.105.50 for 192.0.2.2, BSR priority 100 hash mask length 0
IPv4 BSR:
```

BSR message

```
 from 192.168.105.50/
```

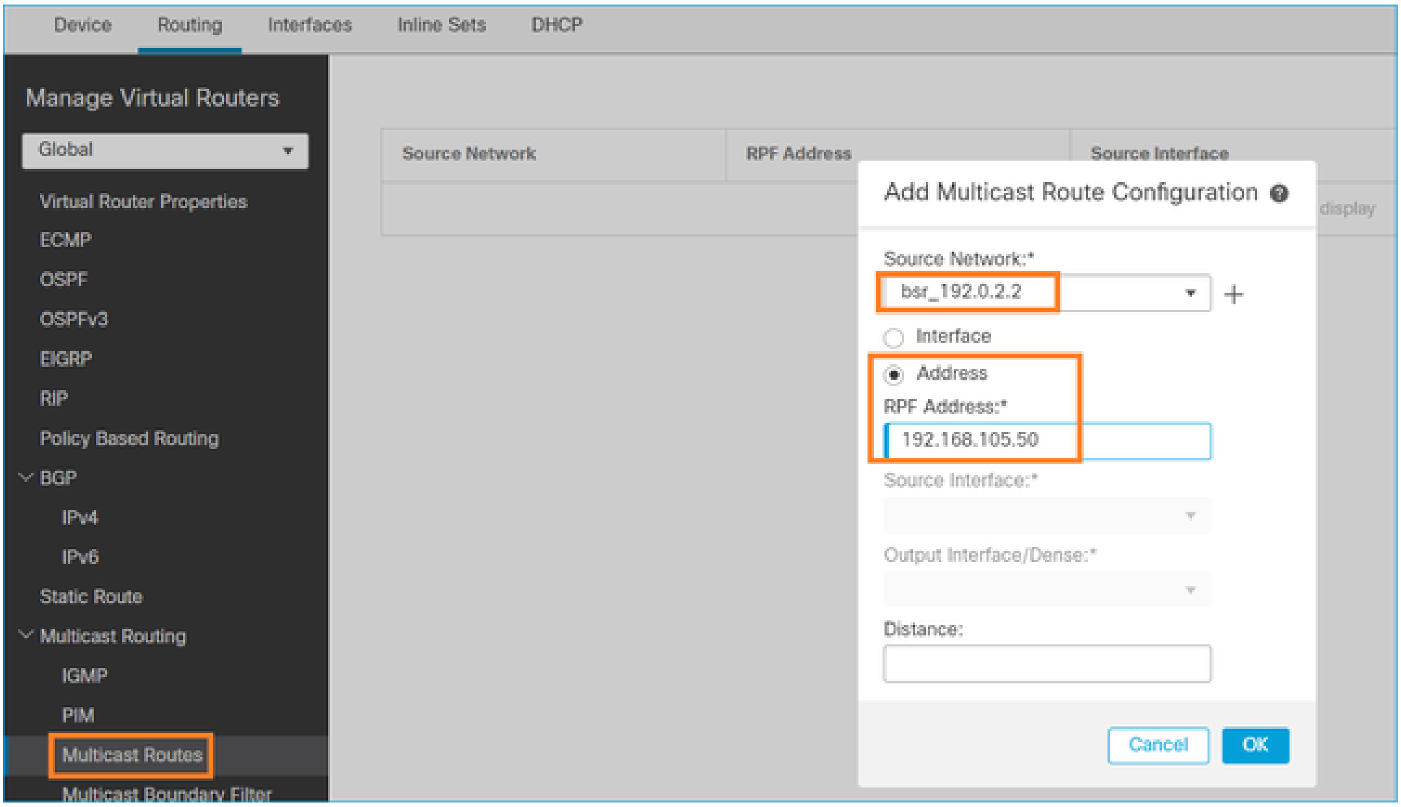
NET207

```
 for 192.0.2.2
```

RPF failed, dropped

<-- The RPF check for the received BSR message failed

إذا كنت ترغب في تغيير واجهة إعادة توجيه المسار العكسي (RPF)، فيمكنك تكوين مسار ثابت. في هذا المثال، يقبل جدار الحماية رسائل BSR من IP 192.168.105.50:



Source Network:* bsr_192.0.2.2

○ Interface

● Address

RPF Address:* 192.168.105.50

Source Interface:*

Output Interface/Dense:*

Distance:

```
<#root>
firepower#
show run mroute
mroute 192.0.2.2 255.255.255.255 192.168.105.50
```

```
<#root>
firepower#
show pim bsr-router

PIMv2 BSR information

BSR Election Information
     BSR Address: 192.0.2.2
     Uptime: 01:21:38, BSR Priority: 100, Hash mask length: 0

RPF: 192.168.105.50,NET207

<-- The RPF check points to the static mroute
     BS Timer: 00:01:37
This system is candidate BSR
      Candidate BSR address: 192.168.103.50, priority: 0, hash mask length: 0
```

الآن يتم قبول رسائل BSR على واجهة NET207، ولكن يتم إسقاط رسائل BSR على الداخل:

<#root>

```
IPv4 BSR: Received BSR message from 192.168.1.70 for 192.0.2.2, BSR priority 100 hash mask length 0


IPv4 BSR: BSR message from 192.168.1.70/INSIDE for 192.0.2.2 RPF failed, dropped


...

IPv4 BSR: Received BSR message from 192.168.105.50 for 192.0.2.2, BSR priority 100 hash mask length 0


<-- RPF check is OK
```

قم بتمكين االلتقاط باستخدام التتبع على جدار الحماية وتحقق من كيفية معالجة رسائل BSR:

<#root>

```
firepower#

show capture

capture CAPI type raw-data trace interface INSIDE [Capturing - 276 bytes]
  match pim any any
capture CAPO type raw-data trace interface OUTSIDE [Capturing - 176 bytes]
  match pim any any
```

يتم إنهاء إتصاالت PIM على جدار الحماية، لذا يلزم مسح االتصاالت بالمربع لكي يعرض التتبع معلومات مفيدة:

<#root>

```
firepower#

show conn all | i PIM

firepower# show conn all | include PIM
PIM OUTSIDE 192.168.103.61 NP Identity Ifc 224.0.0.13, idle 0:00:23, bytes 116802, flags
PIM NET207 192.168.104.50 NP Identity Ifc 224.0.0.13, idle 0:00:17, bytes 307296, flags
PIM NET207 192.168.104.61 NP Identity Ifc 224.0.0.13, idle 0:00:01, bytes 184544, flags
PIM NET207 192.168.105.50 NP Identity Ifc 224.0.0.13, idle 0:00:18, bytes 120248, flags
PIM INSIDE 192.168.1.70 NP Identity Ifc 224.0.0.13, idle 0:00:27, bytes 15334, flags
PIM OUTSIDE 224.0.0.13 NP Identity Ifc 192.168.103.50, idle 0:00:21, bytes 460834, flags
PIM INSIDE 224.0.0.13 NP Identity Ifc 192.168.1.50, idle 0:00:00, bytes 441106, flags
PIM NET207 224.0.0.13 NP Identity Ifc 192.168.105.60, idle 0:00:09, bytes 458462, flags

firepower#

clear conn all addr 224.0.0.13

8 connection(s) deleted.
firepower#
```

```
clear cap /all
```

<#root>

```
firepower#

show capture CAPI packet-number 2 trace


6 packets captured

2: 11:31:44.390421 802.1Q vlan#205 P6

192.168.1.70 > 224.0.0.13

 ip-proto-103, length 38

<-- Ingress PIM packet


Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 4880 ns
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 4880 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 192.168.1.70 using egress ifc INSIDE(vrfid:0)

Phase: 4
Type: CLUSTER-DROP-ON-SLAVE
Subtype: cluster-drop-on-slave
Result: ALLOW
Elapsed time: 4392 ns
Config:
Additional Information:

Phase: 5
Type: ACCESS-LIST
Subtype:
Result: ALLOW
```

```
Elapsed time: 4392 ns
Config:
Implicit Rule
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Elapsed time: 4392 ns
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Elapsed time: 4392 ns
Config:
Additional Information:

Phase: 8
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Elapsed time: 18056 ns
Config:
Additional Information:

Phase: 9

Type: MULTICAST             <-- The multicast process



Subtype: pim


Result: ALLOW
Elapsed time: 976 ns
Config:
Additional Information:

Phase: 10
Type: MULTICAST
Subtype:
Result: ALLOW
Elapsed time: 488 ns
Config:
Additional Information:

Phase: 11
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 20008 ns
Config:
Additional Information:
New flow created with id 25630, packet dispatched to next module

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: 76616 ns
```

إذا تم إسقاط حزمة PIM بسبب فشل إعادة توجيه المسار العكسي (RPF)، فإن التتبع يوضح:

<#root>

```
firepower#

show capture NET207 packet-number 4 trace


85 packets captured

4: 11:31:42.385951 802.1Q vlan#207 P6

192.168.104.61 > 224.0.0.13 ip-proto-103

, length 38

<-- Ingress PIM packet


Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 5368 ns
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 5368 ns
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: INPUT-ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Elapsed time: 11224 ns
Config:
Additional Information:
Found next-hop 192.168.103.61 using egress ifc OUTSIDE(vrfid:0)

Phase: 4
```

```
Type: INPUT-ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Elapsed time: 3416 ns
Config:
Additional Information:
Found next-hop 192.168.103.61 using egress ifc OUTSIDE(vrfid:0)

Result:
input-interface: NET207(vrfid:0)
input-status: up
input-line-status: up
output-interface: OUTSIDE(vrfid:0)
output-status: up
output-line-status: up
Action: drop
Time Taken: 25376 ns

Drop-reason: (rpf-violated) Reverse-path verify failed, Drop-location: frame 0x0000558f240d6e15 flow (NA


<-- the packet is dropped due to RPF check failure
```

تعرض عمليات إسقاط وتالتقاط لودج ASP مزح RPF الفاشلة:

```
<#root>

firepower#

show asp drop


Frame drop:


 Reverse-path verify failed (rpf-violated)                                  122

 <-- Multicast RPF drops
  Flow is denied by configured rule (acl-drop)                               256
  FP L2 rule drop (l2_acl)                                                   768
```

االلتقاط الحزم التي يتم إسقاطها بسبب فشل RPF:

```
<#root>

firepower#

capture ASP type asp-drop rpf-violated



<#root>

firepower#
```

```
show capture ASP | include 224.0.0.13


2: 11:36:20.445960 802.1Q vlan#207 P6 192.168.104.50 > 224.0.0.13 ip-proto-103, length 38
10: 11:36:38.787846 802.1Q vlan#207 P6 192.168.104.61 > 224.0.0.13 ip-proto-103, length 38
15: 11:36:48.299743 802.1Q vlan#207 P6 192.168.104.50 > 224.0.0.13 ip-proto-103, length 46
16: 11:36:48.300063 802.1Q vlan#207 P6 192.168.104.61 > 224.0.0.13 ip-proto-103, length 46
```

منهجية أستكشاف الأخطاء وإصلاحها

تعتمد منهجية أستكشاف أخطاء جدار الحماية وإصلاحها بشكل رئيسي على دور جدار الحماية في مخطط البث المتعدد. هذه قائمة بالخطوات الموصى بها لاستكشاف الأخطاء وإصلاحها:

1. قم بتوضيح تفاصيل وصف المشكلة وأعراضها. حاول تضييق النطاق إلى مشاكل مستوى التحكم (IGMP/PIM) أو مستوى البيانات (دفق البث المتعدد).
2. إن المتطلبات الأساسية الإلزامية لاستكشاف أخطاء البث المتعدد وإصلاحها على جدار الحماية هي توضيح مخطط البث المتعدد. على أقل تقدير، تحتاج إلى تعريف:
   - دور جدار الحماية في مخطط البث المتعدد - FHR أو LHR أو RP أو دور وسيط آخر.
   - واجهات الدخول والخروج للبث المتعدد المتوقعة على جدار الحماية.
   - أر بي.
   - عناوين IP لمصدر المرسل.
   - عناوين IP الخاصة بمجموعات البث المتعدد ومنافذ الوجهة.
   - مستقبلات تدفق البث المتعدد.

3. تحديد نوع التوجيه للبث المتعدد - التوجيه الجذري أو متعدد البث ل PIM:

- التوجيه متعدد البث للجزء الأولي - يوفر التسجيل الديناميكي للمضيف وييسر التوجيه متعدد البث. عند تكوين التوجيه متعدد البث للجزء الأولي، يعمل ASA كوكيل لبروتوكول IGMP. بدلا من المشاركة الكاملة في توجيه البث المتعدد، يقوم ASA بإعادة توجيه رسائل IGMP إلى موجه البث المتعدد للتدفق، والذي يقوم بإعداد تسليم بيانات البث المتعدد. لتحديد توجيه وضع الكعب، أستخدم الأمر show igmp interface وفحص تكوين بروتوكول إدارة مجموعات الإنترنت (IGMP) للأمام:

<#root>

```
firepower#

show igmp interface


inside is up, line protocol is up
  Internet address is 192.168.2.2/24
  IGMP is disabled on interface
outside is up, line protocol is up
  Internet address is 192.168.3.1/24
  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: 0
  Cumulative IGMP activity: 0 joins, 0 leaves

IGMP forwarding on interface inside

  IGMP querying router is 192.168.3.1 (this system)
```

تم تمكين PIM على الواجهات، ومع ذلك لم يتم تأسيس علاقات الجوار:

<#root>

```
firepower#

show pim interface

Address          Interface          PIM  Nbr   Hello  DR          DR
                                         Count Intvl  Prior

192.168.2.2      inside             on   0     30     1           this system
192.168.3.1      outside            on   0     30     1           this system

firepower# show pim neighbor

No neighbors found.
```

ال يتم دعم إعادة توجيه PIM-SM/Bidir و IGMP في نفس الوقت.

أنت يستطيع ال يشكل خيار مثل العنوان:

<#root>

```
%Error: PIM-SM/Bidir and IGMP forwarding are not supported concurrently
```

- التوجيه متعدد البث ل PIM - يعد التوجيه متعدد البث ل PIM هو النشر الأكثر شيوعا. يدعم جدار الحماية كل من PIM-SM و PIM ثنائي الإتجاه. PIM-SM هو بروتوكول توجيه للبث المتعدد يستخدم قاعدة معلومات توجيه البث الأحادي الأساسية أو قاعدة معلومات توجيه منفصلة تدعم البث المتعدد. يقوم بإنشاء شجرة مشتركة أحادية الإتجاه متجذرة في نقطة تجميع (RP) واحدة لكل مجموعة بث متعدد ويقوم إختياريا بإنشاء أشجار أقصر مسار لكل مصدر بث متعدد. في وضع النشر هذا، وعلى عكس وضع STUB، يقوم المستخدمون عادة بتكوين تكوين عنوان RP، وينشئ جدار الحماية عمليات تجاور PIM مع الأجهزة النظيرة:

<#root>

```
firepower#

show run pim
```

```
pim rp-address 10.10.10.1

firepower#

show pim group-map


Group Range         Proto   Client   Groups RP address      Info
224.0.1.39/32*      DM      static   0      0.0.0.0
224.0.1.40/32*      DM      static   0      0.0.0.0
224.0.0.0/24*       L-Local static   1      0.0.0.0
232.0.0.0/8*        SSM     config   0      0.0.0.0

224.0.0.0/4*        SM      config   1      10.10.10.1     RPF: inside,192.168.2.1 <--- RP address is 10


224.0.0.0/4         SM      static   0      0.0.0.0         RPF: ,0.0.0.0

firepower#

show pim neighbor


Neighbor Address  Interface          Uptime    Expires DR pri Bidir
192.168.2.1       inside             00:02:52  00:01:19 1
192.168.3.100     outside            00:03:03  00:01:39 1 (DR)
```

4. تحقق من تكوين عنوان IP الخاص ب RP وإمكانية الوصول:

<#root>

```
firepower#

show run pim


pim rp-address 10.10.10.1

firepower#

show pim group-map



Group Range         Proto   Client   Groups RP address      Info
224.0.1.39/32*      DM      static   0      0.0.0.0
224.0.1.40/32*      DM      static   0      0.0.0.0
224.0.0.0/24*       L-Local static   1      0.0.0.0
232.0.0.0/8*        SSM     config   0      0.0.0.0

224.0.0.0/4*        SM      config   1      10.10.10.1     RPF: inside,192.168.2.1 <--- RP is 10.10.10.1


224.0.0.0/4         SM      static   0      0.0.0.0         RPF: ,0.0.0.0
```

<#root>

```
firepower#
```

```
show pim group-map



Group Range         Proto   Client   Groups RP address      Info
224.0.1.39/32*      DM      static   0      0.0.0.0
224.0.1.40/32*      DM      static   0      0.0.0.0
224.0.0.0/24*       L-Local static   1      0.0.0.0
232.0.0.0/8*        SSM     config   0      0.0.0.0

224.0.0.0/4*        SM      config   1      192.168.2.2     RPF: Tunnel0,192.168.2.2 (us) <--- “us” mear


224.0.0.0/4         SM      static   0      0.0.0.0         RPF: ,0.0.0.0
```

تحذير: ال يمكن أن يكون جدار الحماية RP وFHR في آن واحد.

5. التحقق من النواتج الإضافية وفقا لدور جدار الحماية في مخطط البث المتعدد وأعراض المشكلة.

إف ات ش آر

- تحقق من حالة النفق0 للواجهة. يتم إستخدام هذه الواجهة لتضمين حركة مرور البث المتعدد الخام داخل حمولة PIM وإرسال حزمة البث الأحادي إلى RP ل مع مجموعة بت PIM-register:

<#root>

```
firepower#

show interface detail  | b Interface Tunnel0



Interface Tunnel0 "", is up, line protocol is up


  Hardware is   Available but not configured via nameif
        MAC address 0000.0000.0000, MTU not set
        IP address unassigned
  Control Point Interface States:
        Interface number is un-assigned
        Interface config status is active
        Interface state is active

firepower#

show pim tunnel


Interface          RP Address        Source Address
Tunnel0            10.10.10.1       192.168.2.2
```

- فحص المسارات:

<#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

(192.168.2.1, 230.1.1.1), 00:00:07/00:03:22, flags: SFT
  Incoming interface: inside

  RPF nbr: 192.168.2.1, Registering <--- Registering state


  Immediate Outgoing interface list:
    outside, Forward, 00:00:07/00:03:26

    Tunnel0, Forward, 00:00:07/never <--- Tunnel0 is in OIL, that indicates raw traffic is encapsulated.
```

عندما يستلم جدار الحماية حزمة PIM مع بت إيقاف التسجيل، تتم إزالة Tunnel0 من النفط. وبعد ذلك يوقف جدار الحماية عملية الكبسلة ويرسل حركة مرور أولية للبث المتعدد عبر واجهة الخروج:

<#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

(192.168.2.1, 230.1.1.1), 00:07:26/00:02:59, flags: SFT
  Incoming interface: inside
  RPF nbr: 192.168.2.1
  Immediate Outgoing interface list:


outside, Forward, 00:07:26/00:02:59
```

- التحقق من عدادات سجل PIM:

<#root>

```
firepower#

show pim traffic



PIM Traffic Counters
Elapsed time since counters cleared: 00:13:13

                              Received     Sent
Valid PIM Packets             42           58
Hello                         27           53
Join-Prune                    9            0

Register                      0            8  <--- Sent to the RP



Register Stop                 6            0  <--- Received from the RP


Assert                        0            0
Bidir DF Election             0            0

Errors:
Malformed Packets                           0
Bad Checksums                               0
Send Errors                                 0
Packet Sent on Loopback Errors              0
Packets Received on PIM-disabled Interface  0
Packets Received with Unknown PIM Version   0
Packets Received with Incorrect Addressing  0
```

- التحقق من التقاط حزمة PIM للبث الأحادي بين جدار الحماية و RP:

<#root>

```
firepower#

capture capo interface outside match pim any host 10.10.10.1 <--- RP IP


firepower#

show capture  capi



4 packets captured


  1: 09:53:28.097559       192.168.3.1 > 10.10.10.1  ip-proto-103, length 50     <--- Unicast to RP


  2: 09:53:32.089167       192.168.3.1 > 10.10.10.1  ip-proto-103, length 50
  3: 09:53:37.092890       192.168.3.1 > 10.10.10.1  ip-proto-103, length 50

  4: 09:53:37.095850       10.10.10.1 > 192.168.3.1  ip-proto-103, length 18     <--- Unicast from RP
```

- تجميع المخرجات الإضافية (x.x.x.x هي مجموعة البث المتعدد، y.y.y هو rp ip). ويوصى بجمع النواتج مرات قليلة:

<#root>

```
show conn all protocol udp address x.x.x.x



show local-host x.x.x.x



show asp event dp-cp



show asp drop



show asp cluster counter



show asp table routing y.y.y.y



show route y.y.y.y



show mroute



show pim interface



show pim neighbor
show pim traffic



show igmp interface



show mfib count
```

- تجميع حزمة واجهة البث المتعدد الخام وقرب إسقاط ASP.

<#root>

```
capture capi interface
```

```
      buffer 32000000 match udp host X host Z <--- (ingress capture for multicast UDP traffic from host
```

```
capture capo interface
```

```
      buffer 32000000 match udp host X host Z <--- (egress capture for multicast UDP traffic from host X
```

```
capture asp type asp-drop buffer 32000000 match udp host X host Z <--- (ASP drop capture for multicast U
```

- رسائل syslog - المعرفات الشائعة هي 302015 و 302016 و 710005.

آر بي

- تحقق من حالة النفق0 للواجهة. يتم إستخدام هذه الواجهة لتضمين حركة مرور البث المتعدد الخام داخل حمولة PIM وإرسال حزمة البث الأحادي إلى FHR ل مع تعيين بت إيقاف PIM:

<#root>

```
firepower#
show interface detail  | b Interface Tunnel0


Interface Tunnel0 "", is up, line protocol is up


  Hardware is   Available but not configured via nameif
        MAC address 0000.0000.0000, MTU not set
        IP address unassigned
  Control Point Interface States:
        Interface number is un-assigned
        Interface config status is active
        Interface state is active

firepower#

 show pim tunnel


Interface          RP Address       Source Address


Tunnel0            192.168.2.2      192.168.2.2


Tunnel0            192.168.2.2       -
```

- فحص المسارات:

<#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


(*, 230.1.1.1), 01:04:30/00:02:50, RP 192.168.2.2, flags: S <--- *,G entry




Incoming interface: Tunnel0


  RPF nbr: 192.168.2.2
  Immediate Outgoing interface list:


outside

, Forward, 01:04:30/00:02:50


(192.168.1.100, 230.1.1.1), 00:00:04/00:03:28, flags: ST S <--- S,G entry


  Incoming interface:

inside


  RPF nbr: 192.168.2.1
  Immediate Outgoing interface list:
```

```
outside, Forward, 00:00:03/00:03:25
```

- التحقق من عدادات PIM:

<#root>

```
firepower #

show pim traffic


PIM Traffic Counters
Elapsed time since counters cleared: 02:24:37

                              Received     Sent

Valid PIM Packets             948          755



Hello                         467          584



Join-Prune                    125          32



Register                      344          16



Register Stop                 12           129


Assert                        0            0
Bidir DF Election             0            0

Errors:
Malformed Packets                           0
Bad Checksums                               0
Send Errors                                 0
Packet Sent on Loopback Errors              0
Packets Received on PIM-disabled Interface  0
Packets Received with Unknown PIM Version   0
Packets Received with Incorrect Addressing  0
```

- تجميع المخرجات الإضافية (x.x.x.x هي مجموعة البث المتعدد، y.y.y هو rp ip). ويوصى بجمع النواتج مرات قليلة:

<#root>

```
show conn all protocol udp address x.x.x.x
show conn all | i PIM

show local-host x.x.x.x

show asp event dp-cp

show asp drop

show asp cluster counter

show asp table routing y.y.y.y

show route y.y.y.y

show mroute

show pim interface

show pim neighbor

show igmp interface

show mfib count
```

- تجميع حزمة واجهة البث المتعدد الخام وقرب إسقاط ASP:

<#root>

```
capture capi interface



      buffer 32000000 match udp host X host Z <--- (ingress capture for multicast UDP traffic from host
capture capo interface
```

```
      buffer 32000000 match udp host X host Z <--- (egress capture for multicast UDP traffic from host X
```

```
capture asp type asp-drop buffer 32000000 match udp host X host Z <--- (ASP drop capture for multicast U
```

- Syslog - المعرفات الشائعة هي 302015 و 302016 و 710005.

ل.ر

خذ بعين الإعتبار الخطوات المذكورة في القسم الخاص ب إجراء العملية الإفتراضية وعمليات الفحص الإضافية التالية:

- المسارات:

<#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


(*, 230.1.1.1), 00:23:30/never, RP 10.10.10.1, flags: SCJ <--- C flag means connected receiver


  Incoming interface:

inside
```

```
  RPF nbr: 192.168.2.1
  Immediate Outgoing interface list:

outside

, Forward, 00:23:30/never

(192.168.1.100, 230.1.1.1), 00:00:36/00:03:04, flags: SJT <--- J flag indicates switchover to SPT, T fla

  Incoming interface:
inside

  RPF nbr: 192.168.2.1
  Inherited Outgoing interface list:

outside

, Forward, 00:23:30/never

(*, 230.1.1.2), 00:01:50/never, RP 10.10.10.1, flags: SCJ <--- C flag means connected receiver

  Incoming interface:
inside

  RPF nbr: 192.168.2.1
  Immediate Outgoing interface list:

outside

, Forward, 00:01:50/never

(192.168.1.100, 230.1.1.2), 00:00:10/00:03:29, flags: SJT <--- <--- J flag indicates switchover to SPT,

  Incoming interface:
inside

  RPF nbr: 192.168.2.1
  Inherited Outgoing interface list:

outside

, Forward, 00:01:50/never
```

- مجموعات IGMP:

<#root>

```
firepower#

show igmp groups detail <--- The list of IGMP groups


Interface:      outside

Group:          230.1.1.1


Uptime:         00:21:42
Router mode:    EXCLUDE (Expires: 00:03:17)
Host mode:      INCLUDE

Last reporter:  192.168.3.100 <--- Host joined group 230.1.1.1


Source list is empty
Interface:      outside


Group:          230.1.1.2


Uptime:         00:00:02
Router mode:    EXCLUDE (Expires: 00:04:17)
Host mode:      INCLUDE

Last reporter:  192.168.3.101 <--- Host joined group 230.1.1.2


Source list is empty
```

- إحصائيات حركة مرور IGMP:

<#root>

```
firepower#

show igmp traffic



IGMP Traffic Counters
Elapsed time since counters cleared: 1d04h

                              Received     Sent
Valid IGMP Packets            2468         856
Queries                       2448         856
Reports                       20           0
Leaves                        0            0
Mtrace packets                0            0
DVMRP packets                 0            0
PIM packets                   0            0

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

أوامر أستكشاف أخطاء PIM وإصلاحها (ورقة الشحن)

	الوصف
show running-config multicast-routing	لمعرفة ما إذا تم تمكين توجيه البث المتعدد على جدار الحماية
عرض مسار التشغيل	للاطلاع على المسارات الثابتة التي تم تكوينها على جدار الحماية
show running-config pim	للاطلاع على تكوين PIM على جدار الحماية
show pim interface	لمعرفة واجهات جدار الحماية التي تم تمكين PIM عليها وجيران PIM.
إظهار جار PIM	لرؤية جيران ال PIM
show pim group-map	لترى مجموعات البث المتعدد المعينة إلى RP
show mroute	للاطلاع على جدول توجيه البث المتعدد الكامل
show mroute 230.10.10.10	للاطلاع على جدول البث المتعدد لمجموعة بث متعدد معينة
نفق show pim	لمعرفة ما إذا كان هناك نفق PIM تم إنشاؤه بين جدار الحماية و RP
عرض كافة عناوين التفاصيل rp_ip_address	لمعرفة ما إذا كان هناك اتصال (نفق PIM) تم إنشاؤه بين جدار الحماية و RP
عرض طبولوجيا pim	لعرض إخراج طبولوجيا PIM لجدار الحماية
debug pim	يعرض تصحيح الأخطاء هذا جميع رسائل PIM من جدار الحماية وإليه

debug pim group 230.10.10.10	يعرض تصحيح الأخطاء هذا جميع رسائل PIM من وإلى جدار الحماية لمجموعة البث المتعدد المحددة
عرض حركة مرور PIM	للاطلاع على إحصائيات حول رسائل PIM المستلمة والمرسلة
إظهار عداد نظام المجموعة ASP	للتحقق من عدد الحزم التي تمت معالجتها في المسار البطيء مقابل المسار السريع مقابل نقطة التحكم
إظهار إسقاط ASP	لمشاهدة كافة حالات السقوط على مستوى البرامج على جدار الحماية
على قبض CAP قارن داخلي تتبع مطابقة أي	لالتقاط حزم البث المتعدد ل PIM وتعقبها الخاصة بالمدخل على جدار الحماية
التقاط واجهة CAP لخاد تتبع مطابقة UDP مضيف 224.1.2.3 أي	لالتقاط دفق البث المتعدد المدخل وتعقبه
show pim bsr-router	للتحقق من من هو موجه BSR المنتخب
إظهار كافة العناوين 224.1.2.3	لإظهار اتصال البث المتعدد الأصل
show local-host 224.1.2.3	لإظهار إتصالات البث المتعدد التابع/الجذري

لمزيد من المعلومات حول التقاط جدار الحماية، قم بالعمل مع لصاقات الدفاع ضد تهديد FirePOWER وتتبع الحزمة

مشكلات معروفة

قيود البث المتعدد Firepower:

- لا يدعم IPv6.
- البث المتعدد PIM/IGMP غير مدعوم على الواجهات في منطقة حركة المرور (EMCP).
- لا يمكن أن يكون جدار الحماية مماثلا لبروتوكول RP وبروتوكول FHR.
- يعرض الأمر show conn all إتصالات الهوية للبث المتعدد فقط. لإظهار اتصال البث المتعدد الجذري/الثانوي أستخدم الأمر show local-host <group ip>.

PIM غير معتمد على Nexus الخاص بالكمبيوتر الشخصي vPC

إذا حاولت نشر تجاور PIM بين Nexus vPC وجدار الحماية، فسيكون هناك حد Nexus كما هو موضح هنا:

[الهياكل المدعومة للتوجيه عبر قناة المنفذ الافتراضية على أنظمة Nexus الأساسية]

من وجهة نظر NGFW، ترى في الالتقاط مع تتبع هذا الإسقاط:

<#root>

```
Result:
input-interface: NET102
input-status: up
input-line-status: up
output-interface: NET102
output-status: up
output-line-status: up
Action: drop

Drop-reason: (no-mcast-intrf) FP no mcast output intrf      <-- The ingress multicast packet is dropped
```

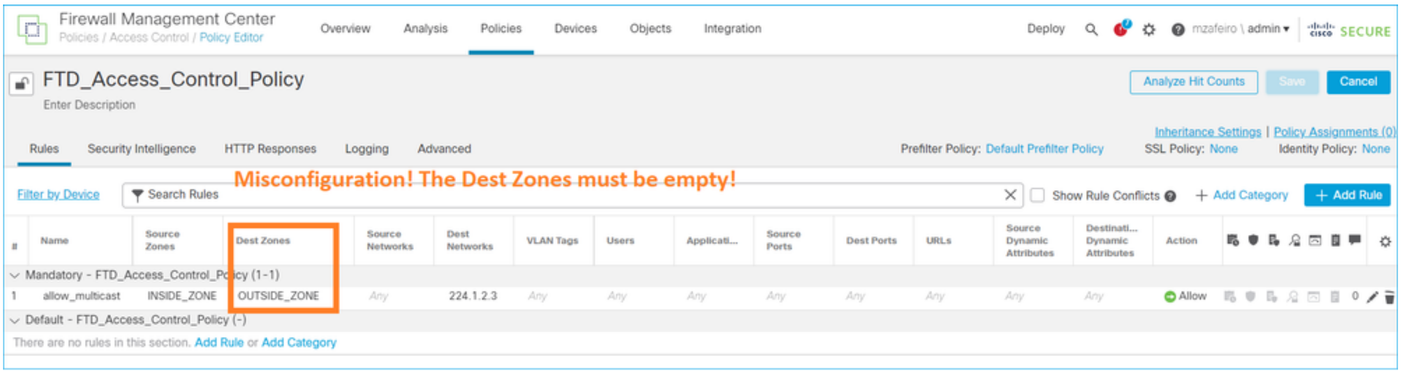
يتعذر على جدار الحماية إكمال تسجيل RP:

<#root>

```
firepower#

show mroute 224.1.2.3


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

(*, 224.1.2.3), 01:05:21/never, RP 10.1.0.209, flags: SCJ
  Incoming interface: OUTSIDE
  RPF nbr: 10.1.104.10
  Immediate Outgoing interface list:
    Server_102, Forward, 01:05:21/never

(10.1.1.48, 224.1.2.3), 00:39:15/00:00:04, flags: SFJT
  Incoming interface: NET102

  RPF nbr: 10.1.1.48, Registering         <-- The RP Registration is stuck

  Immediate Outgoing interface list:
    Tunnel0, Forward, 00:39:15/never
```

مناطق الوجهة غير مدعومة

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



Firewall Management Center
Policies / Access Control / Policy Editor

Overview | Analysis | Policies | Devices | Objects | Integration | Deploy | mzafeiro \ admin ▾ | SECURE

FTD_Access_Control_Policy
Enter Description

Analyze Hit Counts | Save | Cancel

Rules | Security Intelligence | HTTP Responses | Logging | Advanced

Inheritance Settings | Policy Assignments (0)
Prefilter Policy: Default Prefilter Policy   SSL Policy: None   Identity Policy: None

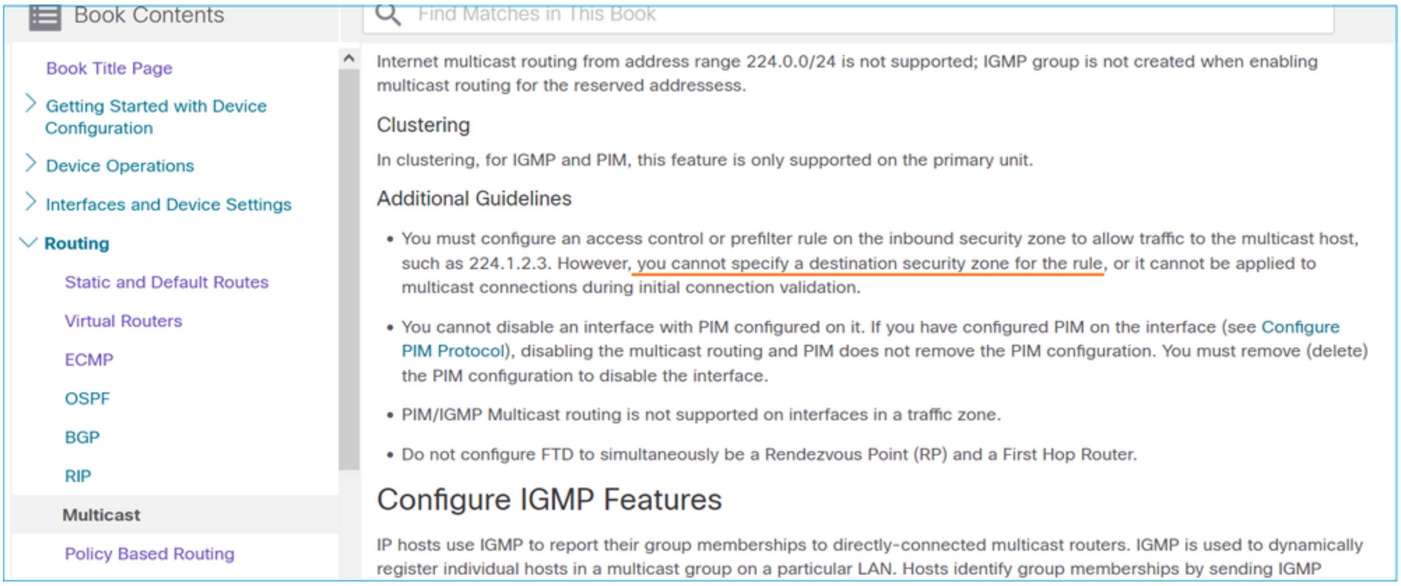
Misconfiguration! The Dest Zones must be empty!

Filter by Device | Search Rules | □ Show Rule Conflicts | + Add Category | + Add Rule

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destinati... Dynamic Attributes	Action
Mandatory - FTD_Access_Control_Policy (1-1)														
1	allow_multicast	INSIDE_ZONE	OUTSIDE_ZONE	Any	224.1.2.3	Any	Any	Any	Any	Any	Any	Any	Any	Allow
Default - FTD_Access_Control_Policy (-)														

There are no rules in this section. Add Rule or Add Category

وهذا موثق أيضا في دليل مستخدم FMC:



Book Contents | Find Matches in This Book

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

Internet multicast routing from address range 224.0.0/24 is not supported; IGMP group is not created when enabling multicast routing for the reserved addressess.

Clustering

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

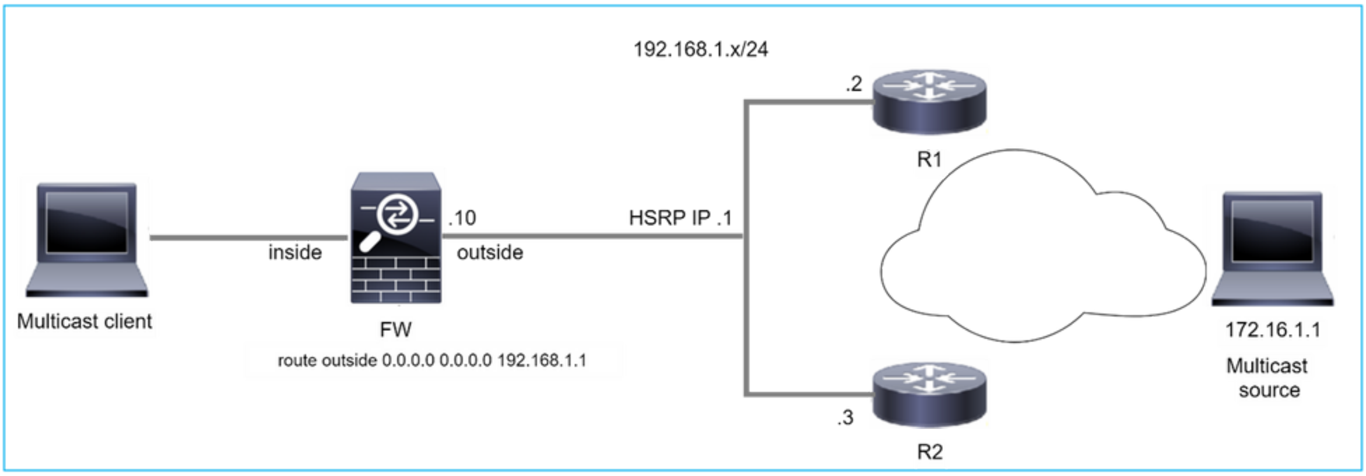
Additional Guidelines

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

Configure IGMP Features

IP hosts use IGMP to report their group memberships to directly-connected multicast routers. IGMP is used to dynamically register individual hosts in a multicast group on a particular LAN. Hosts identify group memberships by sending IGMP

لا يتضمن جدار الحماية رسائل PIM تجاه موجهات الخادم بسبب HSRP



في هذه الحالة، يكون لجدار الحماية مسار افتراضي عبر بروتوكول تكرار الاستعداد السريع

(HSRP) IP 192.168.1.1 وجارة PIM مع الموجهين R1 و R2:

<#root>

```
firepower#

show run route

route outside 0.0.0.0 0.0.0.0 192.168.1.1 1
```

يحتوي جدار الحماية على تجاور PIM بين الخارج والواجهة المادية IP على R1 و R2:

<#root>

```
firepower#

show pim neighbor


Neighbor Address  Interface          Uptime    Expires DR pri Bidir
192.168.1.1       outside            01:18:27  00:01:25 1
192.168.1.2       outside            01:18:03  00:01:29 1 (DR)
```

لا يقوم جدار الحماية بإرسال رسالة PIM Join إلى شبكة البث. يعرض أمر تصحيح أخطاء PIM debug pim هذا الإخراج:

<#root>

```
firepower#

debug pim
...

IPv4 PIM: Sending J/P to an invalid neighbor: outside 192.168.1.1
```

يشير RFC 2362 إلى أن "الموجه يرسل رسالة ربط/تنقيح دورية إلى كل مجاور مميز لإعادة توجيه المسار العكسي (RPF) مرتبط بكل إدخال (S،G) و(*،G) و(*،*،RP)". يتم إرسال رسائل الانضمام/النسخ فقط إذا كان جار إعادة توجيه المسار العكسي (RPF) جار PIM.

للحد من المشكلة، يمكن للمستخدم إضافة إدخال مسار ثابت على جدار الحماية. يجب أن يشير الموجه إلى أحد عنواني IP لواجهة الموجه، 192.168.1.2 أو 192.168.1.3، وعادة ما يكون HSRP هو الموجه النشط IP.

مثال:

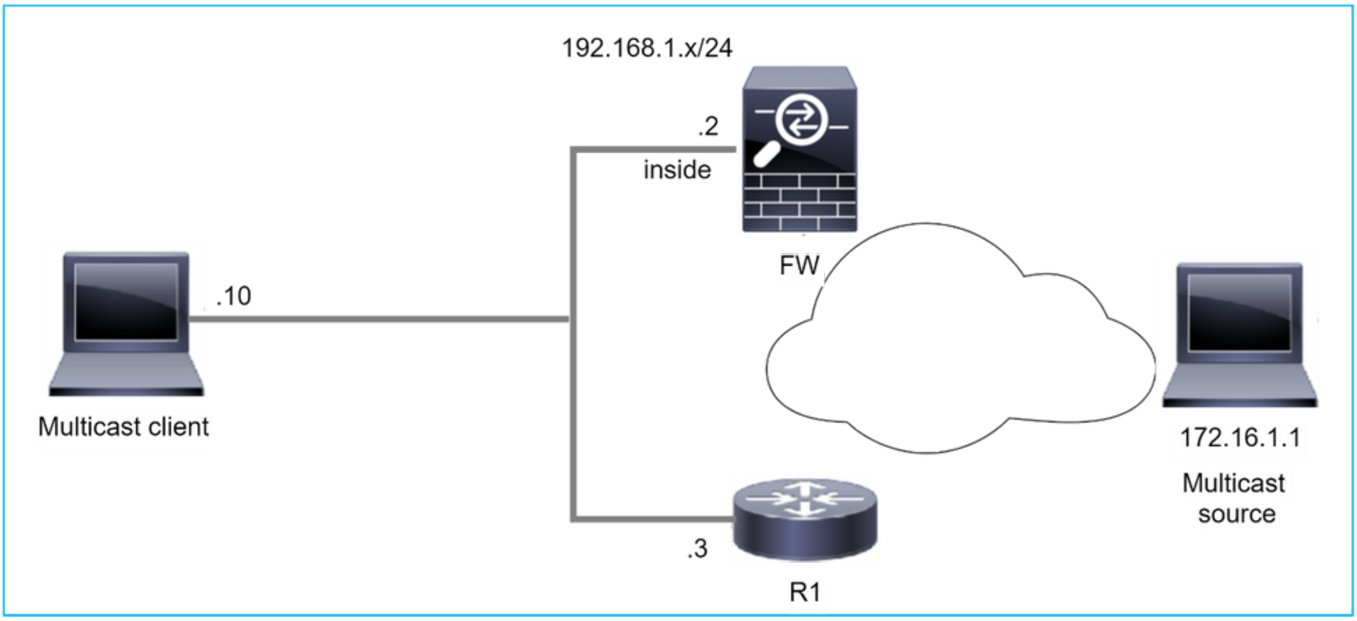
<#root>

```
firepower#

show run mroute


firepower#

mroute 172.16.1.1 255.255.255.255 192.168.1.2
```

ما إن ال ساكن إستاتيكي مسحاج تخديد تشكيل يكون في مكان، ل ال RPF بحث، يعطي جدار الحماية الأفضلية إلى ال multicast تحشد طاولة instead of unicast تحشد طاولة من ال ASA ويرسل ال PIM رسالة مباشرة إلى مجاور 192.168.1.2.

ملاحظة: المسار الثابت إلى حد ما يتجاوز فائدة تكرار HSRP، نظرا لأن المسار يقبل خطوة تالية واحدة فقط لكل مجموعة عنوان/قناع الشبكة. إذا فشلت الخطوة التالية المحددة في الأمر route أو أصبح يتعذر الوصول إليها، فلن يرجع جدار الحماية إلى الموجه الآخر.

ال يعتبر جدار الحماية LHR عندما ال يكون DR في مقطع الشبكة المحلية (LAN)



يحتوي جدار الحماية على R1 كجيران PIM في مقطع الشبكة المحلية (LAN). R1 هو PIM DR:

<#root>

```
firepower#

show pim neighbor


Neighbor Address  Interface          Uptime    Expires DR pri Bidir

192.168.1.3       inside             00:12:50  00:01:38 1 (DR)
```

إذا تم تلقي طلب انضمام IGMP من العميل، فلن يصبح جدار الحماية هو LHR.

يظهر المسار قيمة خالية إضافية كالنفط وبها علامة تنقيح:

```
<#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


(*, 230.1.1.1), 00:06:30/never, RP 0.0.0.0,

flags

: S

P

C
  Incoming interface: Null
  RPF nbr: 0.0.0.0
  Immediate Outgoing interface list:


inside, Null, 00:06:30/never <--- OIL has inside and Null
```

لجعل جدار الحماية LHR، يمكن زيادة أولوية الواجهة DR.

```
<#root>

firepower#

interface GigabitEthernet0/0


firepower#

pim dr-priority 2



firepower#

show pim neighbor


Neighbor Address  Interface          Uptime    Expires DR pri Bidir
```

```
192.168.1.3       inside            17:05:28  00:01:41 1
```

يعرض أمر تصحيح أخطاء PIM debug pim هذا الإخراج:

<#root>

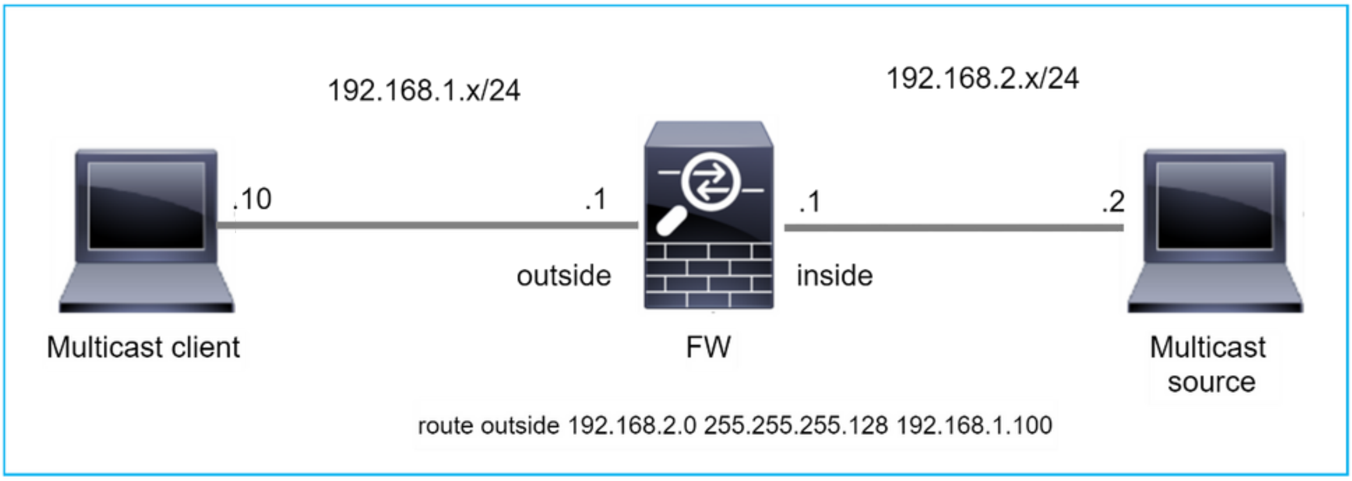
```
firepower#

debug pim

firepower#

IPv4 PIM: (*,230.1.1.1) inside Start being last hop <--- Firewall considers itself as the lasp hop


IPv4 PIM: (*,230.1.1.1) Start being last hop


IPv4 PIM: (*,230.1.1.1) Start signaling sources
IPv4 PIM: [0] (*,230.1.1.1/32) NULLIF-skip MRIB modify NS
IPv4 PIM: (*,230.1.1.1) inside FWD state change from Prune to Forward
IPv4 PIM: [0] (*,230.1.1.1/32) inside MRIB modify F NS
IPv4 PIM: (*,230.1.1.1) Updating J/P status from Null to Join
IPv4 PIM: (*,230.1.1.1) J/P scheduled in 0.0 secs
IPv4 PIM: (*,230.1.1.1) Processing timers
IPv4 PIM: (*,230.1.1.1) J/P processing
IPv4 PIM: (*,230.1.1.1) Periodic J/P scheduled in 50 secs
IPv4 PIM: (*,230.1.1.1) No RPF interface to send J/P
```

تتم إزالة العلامة التي تم تشفيرها و Null من المسار:

<#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

(*, 230.1.1.1), 16:48:23/never, RP 0.0.0.0, flags:

SCJ


  Incoming interface: Null
  RPF nbr: 0.0.0.0
  Immediate Outgoing interface list:
    inside, Forward, 16:48:23/never
```

جدار الحماية يسقط حزم البث المتعدد بسبب فشل التحقق من إعادة توجيه المسار العكسي



في هذه الحالة، يتم إسقاط حزم UDP للبث المتعدد بسبب فشل RPF، حيث يحتوي جدار الحماية على مسار أكثر تحديدا مع القناع 255.255.255.128 عبر الواجهة الخارجية.

<#root>

```
firepower#

capture capi type raw-data trace interface inside match udp any any


firepower#

show captureture capi packet-number 1 trace



106 packets captured
   1: 08:57:18.867234       192.168.2.2.12345 > 230.1.1.1.12354:  udp 500
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 2684 ns
Config:
Additional Information:
MAC Access list


Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
```

```
Elapsed time: 2684 ns
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: INPUT-ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Elapsed time: 13664 ns
Config:
Additional Information:
Found next-hop 192.168.1.100 using egress ifc  outside

Phase: 4
Type: INPUT-ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Elapsed time: 8296 ns
Config:
Additional Information:
Found next-hop 192.168.1.100 using egress ifc  outside

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: drop
Time Taken: 27328 ns

Drop-reason: (rpf-violated) Reverse-path verify failed, Drop-location: frame 0x0000556bcb1069dd flow

(NA)/NA

firepower#

show route static


Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is not set

S        192.168.2.0 255.255.255.128 [1/0] via 192.168.1.100, outside
```

تظهر عمليات التقاط إسقاط ASP سبب الإسقاط الذي تم انتهاكه من قبل RPF:

<#root>

```
firepower#

show capture asp


Target:     OTHER
Hardware:   ASAv
Cisco Adaptive Security Appliance Software Version 9.19(1)
ASLR enabled, text region 556bc9390000-556bcd0603dd

21 packets captured



1: 09:00:53.608290       192.168.2.2.12345 > 230.1.1.1.12354:  udp 500 Drop-reason: (rpf-violated) Rever


   2: 09:00:53.708032       192.168.2.2.12345 > 230.1.1.1.12354:  udp 500 Drop-reason: (rpf-violated) R
   3: 09:00:53.812152       192.168.2.2.12345 > 230.1.1.1.12354:  udp 500 Drop-reason: (rpf-violated) R
   4: 09:00:53.908613       192.168.2.2.12345 > 230.1.1.1.12354:  udp 500 Drop-reason: (rpf-violated) R
```

عدادات فشل إعادة توجيه المسار العكسي (RPF) في زيادة إخراج MFIB:

<#root>

```
firepower#

show mfib 230.1.1.1 count


IP Multicast Statistics
7 routes, 4 groups, 0.00 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: 230.1.1.1


  RP-tree:

   Forwarding: 0/0/0/0, Other: 6788/6788/0




...
firepower#

show mfib 230.1.1.1 count


IP Multicast Statistics
7 routes, 4 groups, 0.00 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: 230.1.1.1
  RP-tree:


Forwarding: 0/0/0/0, Other: 6812/6812/0 <--- RPF failed counter increased
```

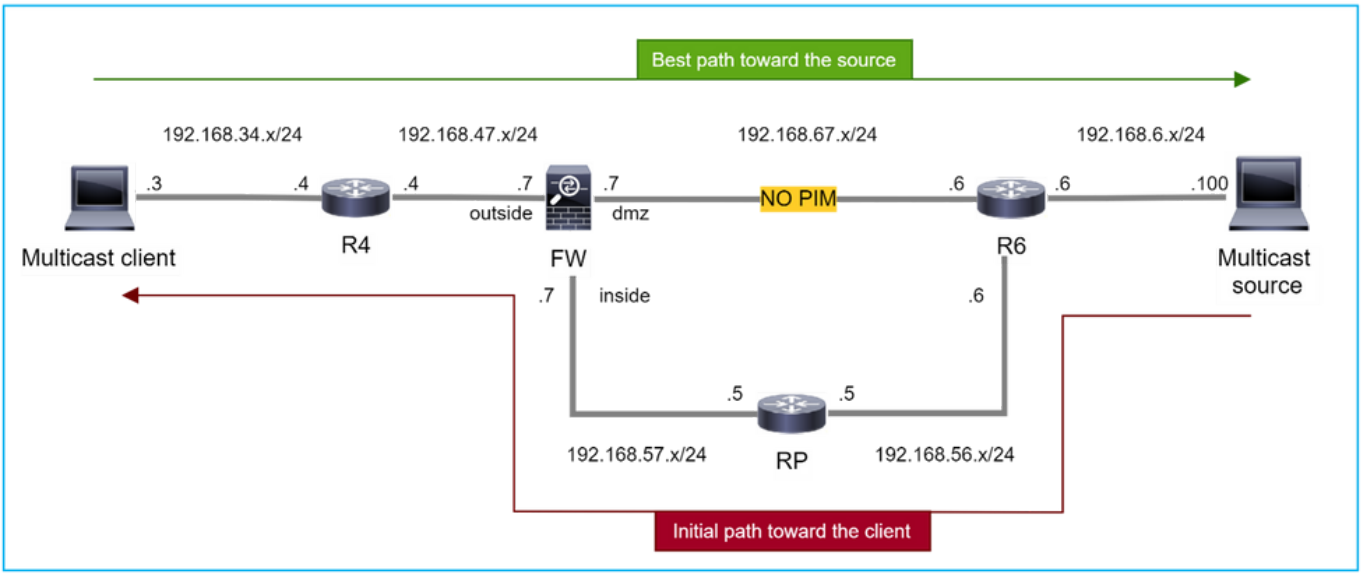
يكمن الحل في إصلاح فشل التحقق من إعادة توجيه المسار العكسي (RPF). أحد الخيارات هو إزالة المسار الثابت.

في حال عدم وجود المزيد من فشل التحقق من إعادة توجيه المسار العكسي (RPF)، تتم إعادة توجيه الحزم ويزداد عداد إعادة التوجيه في إخراج MFIB:

<#root>

```
firepower#

show mfib 230.1.1.1 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: 230.1.1.1
  RP-tree:
   Forwarding: 0/0/0/0, Other: 9342/9342/0

  Source: 192.168.2.2,



   Forwarding: 1033/9/528/39

, Other: 0/0/0
  Tot. shown: Source count: 1, pkt count: 0
...
firepower#

show mfib 230.1.1.1 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: 230.1.1.1
  RP-tree:
   Forwarding: 0/0/0/0, Other: 9342/9342/0

  Source: 192.168.2.2,



   Forwarding: 1044/10/528/41

, Other: 0/0/0

<--- Forward counter increased


  Tot. shown: Source count: 1, pkt count: 0
```

لا يقوم جدار الحماية بإنشاء PIM Join عند تبديل PIM إلى شجرة المصدر



في هذه الحالة، يعلم جدار الحماية المسار نحو مصدر البث المتعدد عبر واجهة DMZ R4 > FW > R6، بينما يكون مسار حركة المرور الأولية من المصدر إلى العميل هو R6 > RP > DW > R4:

<#root>

```
firepower#

show route 192.168.6.100



Routing entry for 192.168.6.0 255.255.255.0
  Known via "ospf 1", distance 110, metric 11, type intra area


Last update from 192.168.67.6 on dmz, 0:36:22 ago


  Routing Descriptor Blocks:


* 192.168.67.6, from 192.168.67.6, 0:36:22 ago, via dmz


      Route metric is 11, traffic share count is 1
```

يقوم R4 ببدء تبديل SPT وإرسال رسالة ربط PIM الخاصة بالمصدر بمجرد الوصول إلى عتبة تبديل SPT. في جدار الحماية لا يتم تبديل SPT، لا يحتوي المسار (S،G) على علامة T:

<#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

(*, 230.1.1.1), 00:00:05/00:03:24, RP 10.5.5.5, flags: S
  Incoming interface: inside
  RPF nbr: 192.168.57.5
  Immediate Outgoing interface list:
    outside, Forward, 00:00:05/00:03:24


(192.168.6.100, 230.1.1.1), 00:00:05/00:03:24, flags: S


  Incoming interface: dmz
  RPF nbr: 192.168.67.6
  Immediate Outgoing interface list:
    outside, Forward, 00:00:05/00:03:2
```

يعرض أمر تصحيح أخطاء PIM debug PIM طلب انضمام PIM 2 الذي تم تلقيه من النظير R4 - ل (*،G) و(S،G). أرسل جدار الحماية طلب PIM Join للتحميل (*،G)، وفشل في إرسال طلب خاص بالمصدر بسبب الجوار غير الصالح 192.168.67.6:

<#root>

```
firepower#

debug pim



IPv4 PIM: Received J/P on outside from 192.168.47.4 target: 192.168.47.7 (to us) <--- 1st PIM join to th


IPv4 PIM: J/P entry: Join root: 10.5.5.5 group: 230.1.1.1 flags:  RPT WC S <--- 1st PIM join with root a


IPv4 PIM: (*,230.1.1.1) Create entry
IPv4 PIM: [0] (*,230.1.1.1/32) MRIB modify DC
IPv4 PIM: [0] (*,230.1.1.1/32) inside MRIB modify A
IPv4 PIM: (*,230.1.1.1) outside J/P state changed from Null to Join
IPv4 PIM: (*,230.1.1.1) outside Raise J/P expiration timer to 210 seconds
IPv4 PIM: (*,230.1.1.1) outside FWD state change from Prune to Forward
IPv4 PIM: [0] (*,230.1.1.1/32) outside MRIB modify F NS
IPv4 PIM: (*,230.1.1.1) Updating J/P status from Null to Join
IPv4 PIM: (*,230.1.1.1) J/P scheduled in 0.0 secs
IPv4 PIM: (*,230.1.1.1) Processing timers
IPv4 PIM: (*,230.1.1.1) J/P processing
IPv4 PIM: (*,230.1.1.1) Periodic J/P scheduled in 50 secs
IPv4 PIM: (*,230.1.1.1) J/P adding Join on inside

IPv4 PIM: Sending J/P message for neighbor 192.168.57.5 on inside for 1 groups   <--- PIM Join sent from


IPv4 PIM: Received J/P on outside from 192.168.47.4 target: 192.168.47.7 (to us) <--- 1st PIM join to th
```

```
IPv4 PIM: J/P entry: Join root: 192.168.6.100 group: 230.1.1.1 flags:  S        <--- 1st PIM join with
```

```
IPv4 PIM: (192.168.6.100,230.1.1.1) Create entry
IPv4 PIM: Adding monitor for 192.168.6.100
IPv4 PIM: RPF lookup for root 192.168.6.100: nbr 192.168.67.6, dmz via the rib
IPv4 PIM: (192.168.6.100,230.1.1.1) RPF changed from 0.0.0.0/- to 192.168.67.6/dmz
IPv4 PIM: (192.168.6.100,230.1.1.1) Source metric changed from [0/0] to [110/11]
IPv4 PIM: [0] (192.168.6.100,230.1.1.1/32) MRIB modify DC
IPv4 PIM: [0] (192.168.6.100,230.1.1.1/32) inside MRIB modify A
IPv4 PIM: [0] (192.168.6.100,230.1.1.1/32) outside MRIB modify F NS
IPv4 PIM: (192.168.6.100,230.1.1.1) outside J/P state changed from Null to Join
IPv4 PIM: (192.168.6.100,230.1.1.1) outside Imm FWD state change from Prune to Forward
IPv4 PIM: (192.168.6.100,230.1.1.1) Updating J/P status from Null to Join
IPv4 PIM: (192.168.6.100,230.1.1.1) J/P scheduled in 0.0 secs
IPv4 PIM: [0] (192.168.6.100,230.1.1.1/32) dmz MRIB modify NS
IPv4 PIM: (192.168.6.100,230.1.1.1) outside Raise J/P expiration timer to 210 seconds
IPv4 PIM: (192.168.6.100,230.1.1.1) Processing timers
IPv4 PIM: (192.168.6.100,230.1.1.1) J/P processing
IPv4 PIM: (192.168.6.100,230.1.1.1) Periodic J/P scheduled in 50 secs
IPv4 PIM: (192.168.6.100,230.1.1.1) J/P adding Join on dmz
```

```
IPv4 PIM: Sending J/P to an invalid neighbor: dmz 192.168.67.6


<--- Invalid neighbor
```

يفتقر إخراج أوامر show pim neigbour إلى R6:

<#root>

```
firepower#

show pim neighbor



Neighbor Address  Interface          Uptime    Expires DR pri Bidir
192.168.47.4      outside            00:21:12  00:01:44 1
192.168.57.5      inside             02:43:43  00:01:15 1
```

تم تمكين PIM على واجهة جدار الحماية dmz:

<#root>

```
firepower#

show pim interface


Address          Interface          PIM  Nbr   Hello  DR          DR
                                         Count Intvl  Prior

192.168.47.7     outside            on   1     30     1           this system
```

```
192.168.67.7     dmz                on    0     30     1          this system

192.168.57.7     inside             on    1     30     1          this system
```

تم تعطيل PIM على واجهة R6:

<#root>

```
R6#

show ip interface brief

Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         192.168.6.1     YES manual up                    up
GigabitEthernet0/1         192.168.56.6    YES manual up                    up
GigabitEthernet0/2         unassigned      YES unset  administratively down down

GigabitEthernet0/3         192.168.67.6    YES manual up                    up

Tunnel0                    192.168.56.6    YES unset  up                    up

R6#

show ip pim interface GigabitEthernet0/3 detail

GigabitEthernet0/3 is up, line protocol is up
  Internet address is 192.168.67.6/24
  Multicast switching: fast
  Multicast packets in/out: 0/123628
  Multicast TTL threshold: 0

PIM: disabled <--- PIM is disabled

  Multicast Tagswitching: disabled
```

الحل هو تمكين PIM على الواجهة GigabitEthernet0/3 على R6:

<#root>

```
R6(config-if)#

interface GigabitEthernet0/3

R6(config-if)#

ip pim sparse-mode

R6(config-if)#
*Apr 21 13:17:14.575: %PIM-5-NBRCHG: neighbor 192.168.67.7 UP on interface GigabitEthernet0/3
```

```
*Apr 21 13:17:14.577: %PIM-5-DRCHG: DR change from neighbor 0.0.0.0 to 192.168.67.7 on interface Gigabit
```

يقوم جدار الحماية بتثبيت علامة T، التي تشير إلى تبديل SPT:

<#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

(*, 230.1.1.1), 00:26:30/00:02:50, RP 10.5.5.5, flags: S
  Incoming interface: inside
  RPF nbr: 192.168.57.5
  Immediate Outgoing interface list:
    outside, Forward, 00:26:30/00:02:50


(192.168.6.100, 230.1.1.1), 00:26:30/00:03:29, flags: ST


  Incoming interface: dmz
  RPF nbr: 192.168.67.6
  Immediate Outgoing interface list:
    outside, Forward, 00:26:30/00:02:39
```

جدار الحماية يسقط الحزم القليلة الأولى التي تستحق حد معدل النفاد

عندما يستلم جدار الحماية الربط الأول من جديد multicast تيار في FP، معالجة إضافي ب ال cp يستطيع كنت تطلبت. في هذه الحالة، يلكم ال FP الربط إلى ال cp عن طريق SP (FP > SP > CP) للعمليات الإضافية:

- خلق أصل توصيل في FP بين المدخل قارن والهوية قارن.
- عمليات تحقق إضافية خاصة بالبث المتعدد، مثل التحقق من صحة إعادة توجيه المسار العكسي (RPF) وتغليف PIM (في حالة ما إذا كان جدار الحماية هو FHR) وفحص النفط وما إلى ذلك.
- إنشاء إدخال (S،G) باستخدام الواجهات الواردة والصادرة في جدول المسار.
- إنشاء اتصال تابع/كعب في FP بين الواجهات الواردة والصادرة.

كجزء من حماية مستوى التحكم، يحدد جدار الحماية داخليا معدل الحزم التي يتم انتقاؤها إلى cp.

يتم إسقاط الحزم التي تتجاوز المعدل باستخدام سبب إسقاط معدل التخفيض:

<#root>

```
firepower#

show asp drop


Frame drop:


Punt rate limit exceeded (punt-rate-limit) 2062
```

أستخدم الأمر show asp cluster counter للتحقق من عدد حزم البث المتعدد التي يتم توجيهها إلى CP من SP:

<#root>

```
firepower#

show asp cluster counter


Global dp-counters:

Context specific dp-counters:

MCAST_FP_FROM_PUNT              30       Number of multicast packets punted from CP to FP
MCAST_FP_TO_SP                  2680     Number of multicast packets punted from FP to SP
MCAST_SP_TOTAL                  2710     Number of total multicast packets processed in SP

MCAST_SP_FROM_PUNT              30       Number of multicast packets punted from CP to SP <--- Number of


MCAST_SP_FROM_PUNT_FORWARD      30       Number of multicast packets coming from CP that are forwarded
MCAST_SP_PKTS                   30       Number of multicast packets that require slow-path attention
MCAST_SP_PKTS_TO_CP             30       Number of multicast packets punted to CP from SP
MCAST_FP_CHK_FAIL_NO_HANDLE     2650     Number of multicast packets failed with no flow mcast_handle
MCAST_FP_CHK_FAIL_NO_FP_FWD     30       Number of multicast packets that cannot be fast-path forwarded
```

أستخدم الأمر show asp event dp-cp punt للتحقق من عدد الحزم في قائمة انتظار FP > CP، ومعدل 15 ثانية:

<#root>

```
firepower#

show asp event dp-cp punt | begin EVENT-TYPE


EVENT-TYPE           ALLOC ALLOC-FAIL ENQUEUED ENQ-FAIL  RETIRED 15SEC-RATE
punt                   24452         0    24452        0     10852     1402


multicast

           23800        0
```

```
23800

     0      10200

1402


  pim                 652          0      652        0      652          0
```

عندما يتم تعبئة المسار وإنشاء الاتصالات الأصل/التابع في FP، تتم إعادة توجيه الحزم في FP كجزء من الاتصالات الموجودة. في هذه الحالة، لا يلصق FP الربط إلى ال cp.

كيف يقوم جدار الحماية بمعالجة الحزم الأولى لتدفق البث المتعدد الجديد؟

عندما يستقبل جدار الحماية الحزم الأولى لتدفق جديد للبث المتعدد في DataPath، يقوم جدار الحماية باتخاذ هذه الإجراءات:

1. التحقق مما إذا كان نهج الأمان يسمح بالحزم.
2. يلكم الربط إلى ال cp عن طريق ممر fp.
3. ينشئ اتصال أصلي بين واجهات المدخل وواجهات الهوية:

```
<#root>

firepower#

show capture capi packet-number 1 trace


10 packets captured

   1: 08:54:15.007003       192.168.1.100.12345 > 230.1.1.1.12345:  udp 400


Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: INPUT-ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 192.168.2.1 using egress ifc  inside
```

```
Phase: 4
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:

Phase: 5
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: QOS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 9

Type: MULTICAST


Subtype:
Result: ALLOW
Config:
Additional Information:


Phase: 10

Type: FLOW-CREATION


Subtype:
Result: ALLOW
Config:
Additional Information:

New flow created with id 19, packet dispatched to next module <--- New flow



Result:
input-interface: inside
```

```
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
```

Action: allow

Syslogs:

<#root>

```
firepower# Apr 24 2023 08:54:15: %ASA-7-609001: Built local-host inside:192.168.1.100
Apr 24 2023 08:54:15: %FTD-7-609001: Built local-host identity:230.1.1.1
```

Apr 24 2023 08:54:15: %FTD-6-302015: Built inbound UDP connection 19 for inside:192.168.1.100/12345 (192

يكون اذه الاتصال مرئيا في مخرجات الأمر show conn all:

<#root>

```
firepower#
```

show conn all protocol udp

```
13 in use, 17 most used
```

UDP inside 192.168.1.100:12345 NP Identity Ifc 230.1.1.1:12345, idle 0:00:02, bytes 0, flags -

4. يشرك ال cp العملية multicast عملية ل إضافي multicast خاص تدقيق، مثل ال RPF صحة، PIM عملية كبسلة (في الحالة إن جدار الحماية هو FHR)، زيتي تدقيق، وهكذا.
5. يخلق ال cp (S،G) مدخل مع القادم والصادر قارن في المسار:

<#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

(*, 230.1.1.1), 00:19:28/00:03:13, RP 192.168.192.168, flags: S
```

```
  Incoming interface: inside
  RPF nbr: 192.168.2.1
  Immediate Outgoing interface list:
    outside, Forward, 00:19:28/00:03:13


(192.168.1.100, 230.1.1.1), 00:08:50/00:03:09, flags: ST



  Incoming interface: inside


  RPF nbr: 192.168.2.1
  Immediate Outgoing interface list:

    outside, Forward, 00:00:32/00:02:57
```

6. يرشد ال cp ال FP عن طريق cp > SP > FP ممر أن يخلق بذرة/فرع توصيل بين القارن قادم وصادر:

يكون هذا الاتصال مرئيا فقط في إخراج الأمر show local-host:

<#root>

```
firepower#

show local-host



Interface outside: 5 active, 5 maximum active
local host: <224.0.0.13>,
local host: <192.168.3.100>,
local host: <230.1.1.1>,

  Conn:



    UDP outside  230.1.1.1:12345 inside  192.168.1.100:12345, idle

 0:00:04, bytes 4000, flags -
local host: <224.0.0.5>,
local host: <224.0.0.1>,
Interface inside: 4 active, 5 maximum active
local host: <192.168.1.100>,


  Conn:



    UDP outside  230.1.1.1:12345 inside  192.168.1.100:12345, idle

 0:00:04, bytes 4000, flags -
local host: <224.0.0.13>,
local host: <192.168.2.1>,
local host: <224.0.0.5>,
Interface nlp_int_tap: 0 active, 2 maximum active
Interface any: 0 active, 0 maximum active
```

في إصدارات البرامج مع إصلاح معرف تصحيح الأخطاء من Cisco CSCwe21280
، يتم أيضا إنشاء رسالة syslog 302015 لاتصال الطفل/كعب:

```
<#root>

Apr 24 2023 08:54:15: %FTD-6-302015:

Built outbound UDP connection 20 for outside:230.1.1.1/12345 (230.1.1.1/12345) to inside:192.168.1.100/1
```

عندما يتم إنشاء كل من إتصالات الأصل والتابع/الكعب، فإن حزم المدخل تطابق الاتصال الموجود وتتم إعادة توجيهها في FP:

```
<#root>

firepower#

show capture capi trace packet-number 2


10 packets captured
   2: 08:54:15.020567       192.168.1.100.12345 > 230.1.1.1.12345:  udp 400
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list


Phase: 3


Type: FLOW-LOOKUP


Subtype:
Result: ALLOW
Config:
```

```
Additional Information:

Found flow with id 19, using existing flow <--- Existing flow



Result:
input-interface: inside
input-status: up
input-line-status: up
Action: allow
```

تصفية حركة مرور بث ICMP المتعدد

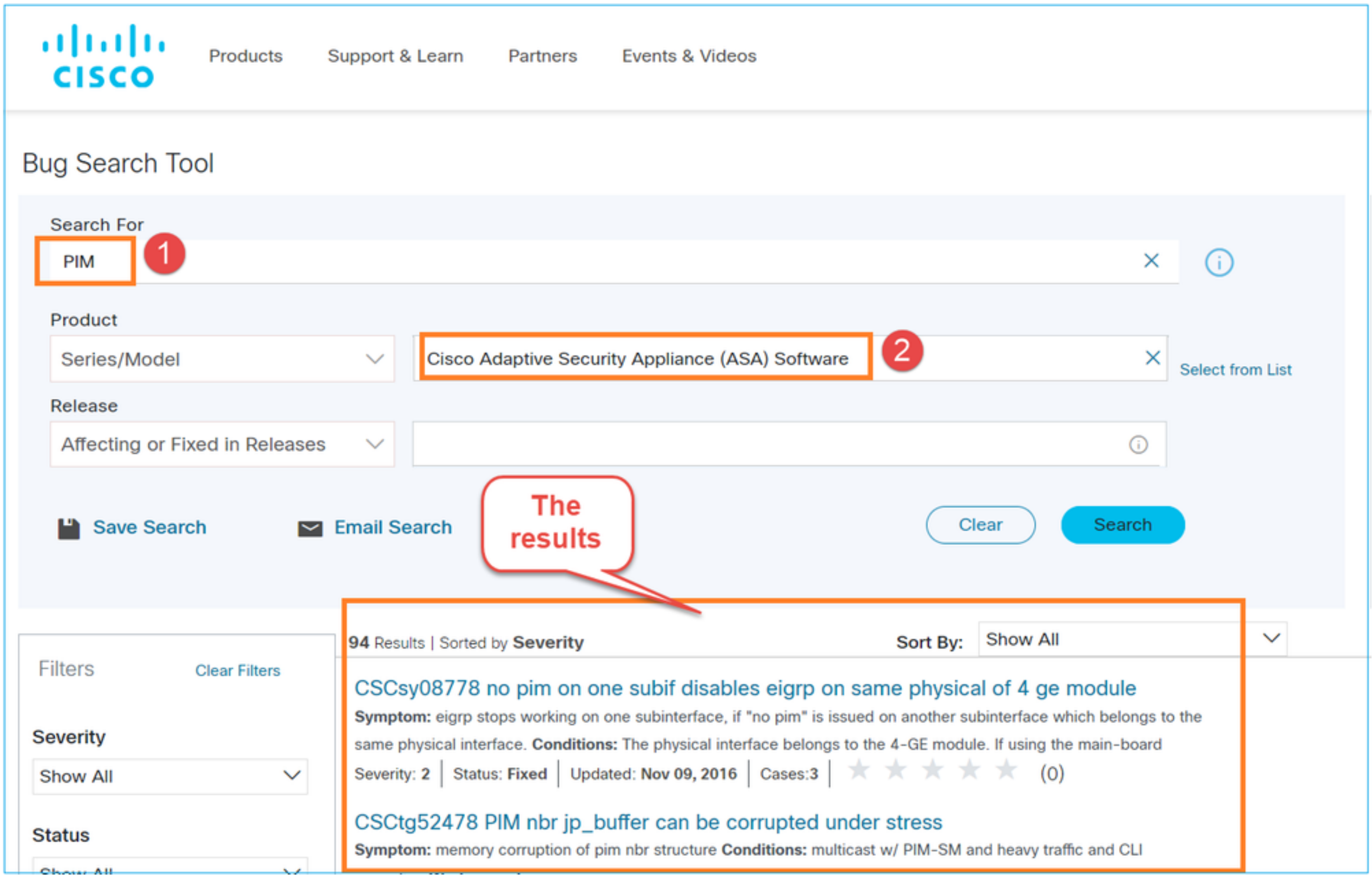
لا يمكنك تصفية حركة مرور ICMP للبث المتعدد باستخدام قائمة التحكم في الوصول (ACL). يجب إستخدام سياسة مستوى التحكم (ICMP):

لا يقوم معرف تصحيح الأخطاء من Cisco [CSCsl26860](https://tools.cisco.com/bugsearch/bug/CSCsl26860) ASA بتصفية حزم ICMP للبث المتعدد

عيوب البث المتعدد المعروفة ل PIM

يمكنك إستخدام أداة البحث عن الأخطاء للعيوب المعروفة:
https://bst.cloudapps.cisco.com/bugsearch

يتم سرد معظم عيوب ASA و FTD ضمن منتج "جهاز الأمان القابل للتكيف (ASA) من Cisco":



Bug Search Tool

Search For: PIM

Product: Series/Model — Cisco Adaptive Security Appliance (ASA) Software

Release: Affecting or Fixed in Releases

94 Results | Sorted by Severity

CSCsy08778 no pim on one subif disables eigrp on same physical of 4 ge module
Symptom: eigrp stops working on one subinterface, if "no pim" is issued on another subinterface which belongs to the same physical interface. **Conditions:** The physical interface belongs to the 4-GE module. If using the main-board
Severity: 2 | Status: Fixed | Updated: Nov 09, 2016 | Cases:3 | ☆ ☆ ☆ ☆ ☆ (0)

CSCtg52478 PIM nbr jp_buffer can be corrupted under stress
Symptom: memory corruption of pim nbr structure **Conditions:** multicast w/ PIM-SM and heavy traffic and CLI

معلومات ذات صلة

- أستكشاف أخطاء البث المتعدد ل ASA وإصلاحها والمشاكل الشائعة
- البث المتعدد لمركز إدارة Firepower
- ملخص علامات البث المتعدد ل Firepower

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).