

مقدمة

لجكاشم او (ASA) فيكتل لباقال نامال زاهج يلع ددعتملا ثبل هيچوت دنتسملا اذه فصلي
ةعئاشل.

ةزيملا تامولعم

لباقال نامال زاهج يلع ددعتملا ثبل هيچوت لوح شدم يوتحم يلع لوصحلل: ةظحال
ةيامحل راج ديهت نع عافدل" و " (FTD) ةيرانلا ةقائل ديهت نع عافدل" و (ASA) فيكتل
تالاقملا هذه يلع عجر، " (FTD) نمال:

[ددعتملا ثبل تالوكوتوربو \(IGMP\) تنرتنالا تاعومجم ةرادا لوكوتورب عاڤخأ فاشكتسأ](#)

[اهالصل او FirePOWER ديهت نع عافدل اب ةصاخلا](#)

[اهالصل او ASA ددعتملا ثبل او FirePOWER ديهت نع عافدل عاڤخأ فاشكتسأ](#)

تارصتخملا/تارصتخملا

تارصتخال	حرضل
رآ شتا فإ	رورم ةكرح ردصمب ةرشابم ةلصتم ةوطخ - يلوالا ةوطخل هجوم ددعتملا ثبل.
رل	ةرشابم ةلصتم لوصو ةطقن - ةريخالا ةوطخل هجوم ددعتملا ثبل رورم ةكرح تالبق تسمب.
ي ب رآ	ءاقتلالا ةطقن
روتكد	نيعم هجوم
SPT	راسم رصقأ ةرجش
RPT	ةكراشملا ةرجش، (RP) ءاقتلالا ةطقن ةرجش
يسكعلا راسملا هيچوت ةداعإ	يسكعلا راسملا هيچوت ةداعإ
تيز	ةرداصللا ةهاولا ةمئاق
برأم	ددعتملا ثبل هيچوت تامولعم ةدعاق

MFIB	ددعتملا ثبلا هي جوت ةداع! تامولعم ةدعاق
ASM	ردصم يأل ددعتملا ثبلا
رأ سا يب	هجوم Bootstrap
SSM	ردصملا ددعتملا ثبلا
عزوم	عيرس راسم
SP	ءيطب راسم
CP	مكحتلا ةطقن
PPS	ةيناثلا يف ةمزالا

نبيعضولا دحأ يف ASA لىل ددعتملا ثبلا نبيوكت نكمي:

- لوكوتوربلا نع لقتسملا ددعتملا ثبلا (PIM) ل رثانتملا عضولا ([RFC 4601](#)): لوكوتوربلا نع لقتسملا ددعتملا ثبلا
- تاعومجم ةرادا لوكوتورب (IGMP Stub-mode) تنرتنالا تاعومجم ةرادا لوكوتورب عضو ([RFC 2236](#)): تنرتنالا

لوكوتورب ربع ناريجلاب لصت يف ASA نأل لصفملا رايختالا وه PIM ل رثانتملا عضولا ددعتملا ثبلا نبيوكت رايخ وه IGMP Stub عضو ناك. (PIM) ددعتملا ثبلا لىل يقي قح هي جوت ريراقت هي جوت ةداعا قيرط نع ةطاسبب هليغشت متي و، 7.0 رادصلا ASA رادصلا لبق ديحوللا يلولوالا ثبلا تاهجوم هاجت عالمعلال نم اهلابقتسا متي يتال IGMP.

ددعتملا ثبلا تانوكم

تانوكملا هذه نم ددعتملا ثبلا لىل ةيساسالا ةينبالا نوكتت، ماع لكشب

يه ةلثمألا. ددعتملا ثبلا قفد عاشناب موقبي يذلا ةكبشلا زاهج وأ فيضملا => لسرمل هي جوت لوكوتورب لغشت يتال ةكبشلا زهجاو توصلال وأ/و ويديفلا ثب لسري يذلا مداخل OSPF أو EIGRP لثم.

م تي ام ابلاغ. ددعتملا ثبلا قفدت لبق تسي يذلا زاهجالا وأ فيضملا => لبق تسملا IGMP لوكوتورب مادختساو رورملا ةكرب نيتمهملا ني فيضملا لىل حلطصملا اذه مادختسا اهاكرت وأ ةينعملال ددعتملا ثبلا ةعومجم لىل امامضنالل.

دعا و ددعتم ل ثب ل رورم ة كرح/ قفدت ة ج ل اع م نع ة لوؤس م ل ة ك ب ش ل ة زه ج أ => ASA / تاه جوم ل (عالمع ل) ل يم ع ل ل ر دص م ل نم ة ج ا ح ل دن ة ك ب ش ل نم ى ر خ أ ا ن ج أ ل ل ه ي جوت

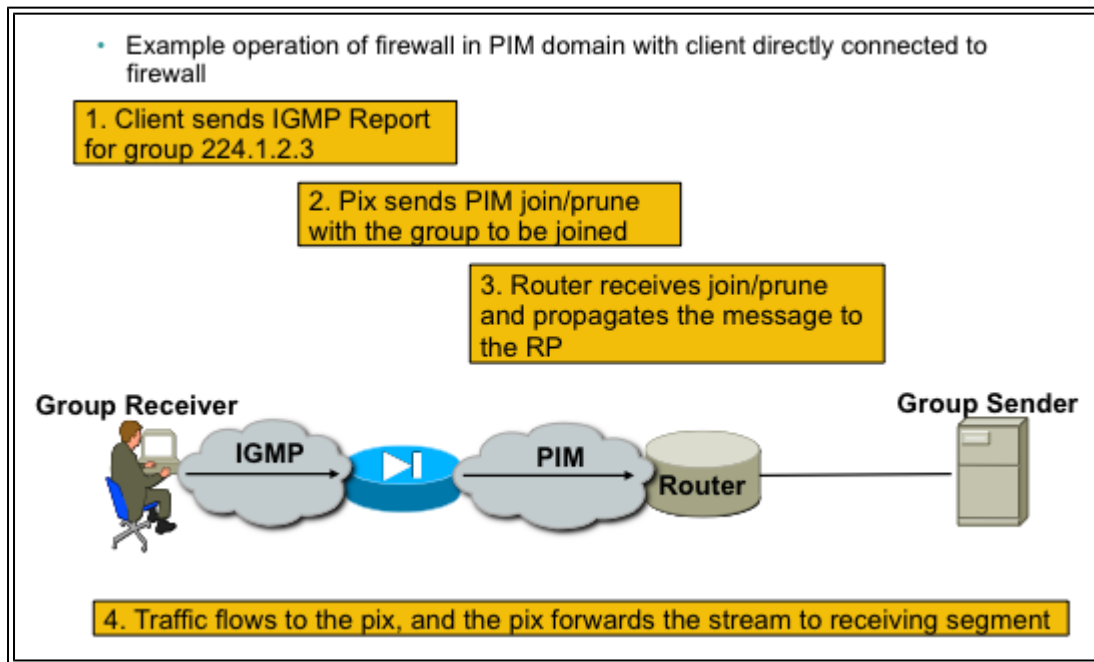
ددعتم ل ثب ل مزح ه ي جوت ة دعا ل نع لوؤس م ل لوكوت وورب ل => ددعتم ل ثب ل ه ي جوت لوكوت وورب ل لثم نور خ أ كانه نكلو (لوكوت وورب ل نع لقتس م ل ددعتم ل ثب ل) PIM وه اع و ي ش رث ك أ ل ل ا ث م ل ل ي ب س ل ع MOSPF.

ي ق ل ل ت ل عالمع ل اهم د خ ت س ي ي ت ل ة ل م ع ل => (IGMP) ت ن ر ت ن ل ا تاع و م ج م ة ر ا د ل لوكوت وورب ل ة. ن ع ي م ة و م ج م نم ددعتم ل ثب ق ف د ت

PIM رثان ت عضو ة ل م ع

- ه ا ج ت ا ل ا ي ئ ا ن ث PIM عضو و رثان ت م ل PIM عضو و ASA م ع د ي
- ت ق و ل ا س ف ن ي ف IGMP stub و رثان ت م ل PIM عضو و ر م ا و ا ن ي و ك ت م د ع ب ج ي
- ل ل ة ي ا د ب ل ا ي ف ددعتم ل ثب ل رورم ة ك ر ح ع ي م ج ق ف د ت م ت ي ، رثان ت م ل PIM عضو م ع م ض ع ب رورم د ع ب . ل ا ب ق ت س ا ل ا ة زه ج أ ل ل ا ه ي جوت ة دعا ل م ت م ث ، (RP) ا ق ت ل ا ل ا ة ط ق ن (RP زواج ت ي و) ي ق ل ل ت م ل ل ر دص م ل نم ة ر ش ا ب م ددعتم ل ثب ل ق ف د ت ل ق ت ن ي ، ت ق و ل ا

ة ه ج ا و ل ع ددعتم ل ثب عالمع ل ع ASA ي و ت ح ي ش ي ح ة ع ئ ا ش ر ش ن ة ل م ع ة ر و ص ل ا ه ذ ه ح ص و ت : ر خ أ ة ه ج ا و ل ع PIM ن ا ر ي ج و ة د ح ا و



PIM ل رثان ل عضو ة ن ي ع ن ي و ك ت

1. (ماع ل ا ن ي و ك ت ل ا عضو) ثب ل ا ددعتم ل ه ي جوت ل ا ن ي ك م ت ب م ق .

<#root>

ASA(config)#

multicast-routing

2. PIM ءاقتلا ةطقن ناونع دي دحت .

<#root>

ASA(config)#

pim rp-address 172.18.123.3

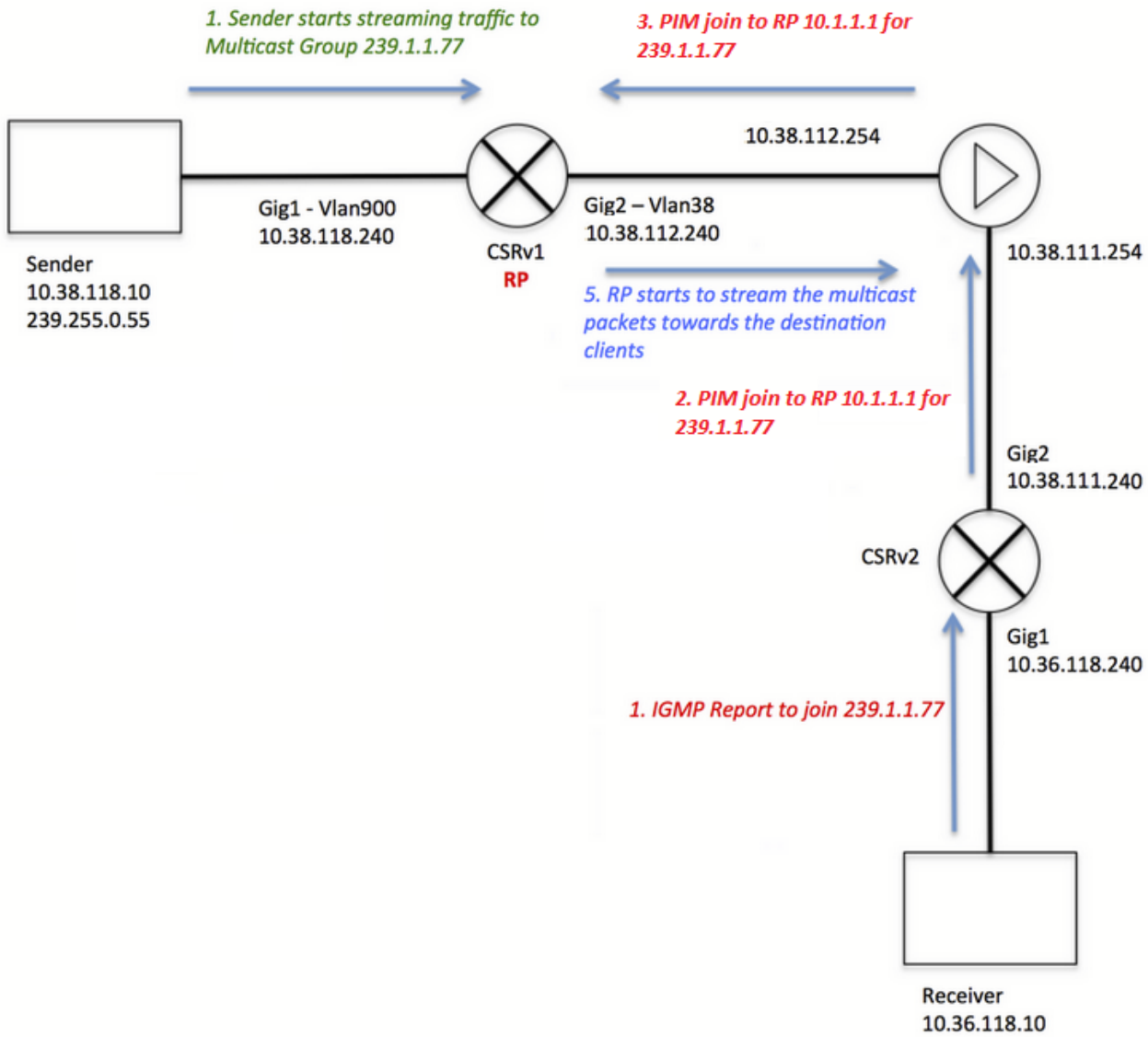
3. نامألا ةسايس ماق اذا طقف يوررض) ةبسانملا ةهجاولا يف ددعتملا ثبلا مزح ب حم سا .
(ةدراولا ددعتملا ثبلا مزح رطح ب ASA ب ةصاخلا

<#root>

access-list 105 extended permit ip any host 224.1.2.3

access-group 105 in interface outside

رثانتملا PIM عضو لاثم:



يذلل قفدتلالو (رمحلأال نوللاب تاوطلال) ليمعلااب صاخالل IGMP لوكوتورب ليجست نأ ظحال لدت ةقيرطال هذهو، فللخمل لكشب هنيولت مت دق (رضألأال نوللاب تاوطلال) مداخل هملتسي مظتنم ريغل لكشب ثدحت نأ نكمي نيتمعلاالك نأ لىل

(ءارمحلأال تاوطلال) ليمعلاال ليجست تاوطلال:

1. ةومحملل IGMP ريرقت ليمعلاال لسري 239.1.1.77
2. ةومحملل (10.1.1.1) نوكمل تابثالل RP لىل PIM طبر ةلاسرهومال لسري 239.1.1.77.
3. ةومحملل PIM Join ةلاسرهومال RP لىل ASA لسري 239.1.1.77.

show mroute: رمألأال جارل لىل G*, PIM لخالل ASA ضرعي

<#root>

ciscoasa#

show mroute 239.1.1.77

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

(* , 239.1.1.77), 00:03:43/00:02:41, RP 10.1.1.1, flags: S

Incoming interface: outside

RPF nbr: 10.38.111.240

Immediate Outgoing interface list:

inside, Forward, 00:03:43/00:02:41

مزح ي أضرعي ال ASA لى لع "show mfib" جارخا نإف، قفدت ي أدي مل ردصم ال مداخل نأ امب نكلو
ةم لتسم:

<#root>

ciscoasa#

show mfib 239.1.1.77

Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,

AR - Activity Required, K - Keepalive

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

Other counts: Total/RPF failed/Other drops

Interface Flags: A - Accept, F - Forward, NS - Negate Signalling

IC - Internal Copy, NP - Not platform switched

SP - Signal Present

Interface Counts: FS Pkt Count/PS Pkt Count

(* ,239.1.1.77) Flags: C K

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

outside Flags: A

inside Flags: F NS

Pkts: 0/0

لاخدإ طقف RP ضرعي، ددعتم ال ثبل الة ومجم لى لإ رورم ةكرح ي لاسرا ي ف مداخل أدي نأ لبق
لا ثم ال لى بس لى لع، ةم ئاق لى ف ة دراو ةه جاو نوب "G".

<#root>

CRSV#

show ip mroute 239.1.1.77

IP Multicast Routing Table

Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,

L - Local, P - Pruned, R - RP-bit set, F - Register flag,

T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,

X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,

U - URD, I - Received Source Specific Host Report,

Z - Multicast Tunnel, z - MDT-data group sender,
 Y - Joined MDT-data group, y - Sending to MDT-data group,
 G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
 N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
 Q - Received BGP S-A Route, q - Sent BGP S-A Route,
 V - RD & Vector, v - Vector, p - PIM Joins on route,
 x - VxLAN group
 Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
 (*, 239.1.1.77), 00:00:02/00:03:27, RP 10.1.1.1, flags: S
 Incoming interface: Null, RPF nbr 0.0.0.0
 Outgoing interface list:
 GigabitEthernet2, Forward/Sparse-Dense, 00:00:02/00:03:27

عضي و "S,G" لاخدا عاشن اب RP موقى ،ددعتم ل ثبل اة وومجم لى ل ق ف دل ا ي ف م داخ ل ا ادب درجم ب
 تانا ي بل ا رورم اة كرح ل اسرا ي ف ا د ب ي و ا درا و ال ا ه ج ا و ال ا م ئ ا ق ي ف ل س ر م ل ا ه ج ا و ت ي ت ل ا ه ج ا و ال
 ل ا س A : م داخ ل ل ا ل ا

<#root>

CRSv#

show ip mroute 239.1.1.77

...

(*, 239.1.1.77), 00:03:29/stopped, RP 10.1.1.1, flags: SF
 Incoming interface: Null, RPF nbr 0.0.0.0
 Outgoing interface list:
 GigabitEthernet2, Forward/Sparse-Dense, 00:03:29/00:02:58
 (10.38.118.10, 239.1.1.77), 00:00:07/00:02:52, flags: FT
 Incoming interface: GigabitEthernet1, RPF nbr 0.0.0.0
 Outgoing interface list:
 GigabitEthernet2, Forward/Sparse-Dense, 00:00:07/00:03:22

ق ق ح ت ل ل ر م ا و ال ا ه ذ ه م د خ ت س ا :

- "S,G" لاخدا ا ض ر ع ي م rroute ر م ال ا ض ر ع -

ة ي م ا م ال ا م ز ح ل ا ت ا د ا د ع -show mfib ر م ال ا ض ر ع ي

- ip د د ع ت م ل ا ث ب ل ا ه و و م ج م ب ق ل ع ت م ل ا ل ا ص ت ال ا show conn ر م ال ا ض ر ع ي -

<#root>

ciscoasa#

show mroute 239.1.1.77

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

(* , 239.1.1.77), 00:06:22/00:02:50, RP 10.1.1.1, flags: S

Incoming interface: outside

RPF nbr: 10.38.111.240

Immediate Outgoing interface list:

inside, Forward, 00:06:22/00:02:50

(10.38.118.10, 239.1.1.77), 00:03:00/00:03:28, flags: ST

Incoming interface: outside

RPF nbr: 10.38.111.240

Immediate Outgoing interface list:

inside, Forward, 00:03:00/00:03:26

ciscoasa#

show mfib 239.1.1.77

Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,

AR - Activity Required, K - Keepalive

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

Other counts: Total/RPF failed/Other drops

Interface Flags: A - Accept, F - Forward, NS - Negate Signalling

IC - Internal Copy, NP - Not platform switched

SP - Signal Present

Interface Counts: FS Pkt Count/PS Pkt Count

(* , 239.1.1.77) Flags: C K

Forwarding: 15/0/1271/0, Other: 0/0/0

outside Flags: A

inside Flags: F NS

Pkts: 0/15

(10.38.118.10, 239.1.1.77) Flags: K

Forwarding: 7159/34/1349/360, Other: 0/0/0

outside Flags: A

inside Flags: F NS

Pkts: 7159/5

ciscoasa#

show conn all | i 239.1.1.77

UDP outside 10.38.118.10:58944 inside 239.1.1.77:5004, idle 0:00:00, bytes 10732896, flags -

UDP outside 10.38.118.10:58945 inside 239.1.1.77:5005, idle 0:00:01, bytes 2752, flags -

UDP outside 10.38.118.10:58944 NP Identity Ifc 239.1.1.77:5004, idle 0:00:00, bytes 0, flags -

UDP outside 10.38.118.10:58945 NP Identity Ifc 239.1.1.77:5005, idle 0:00:01, bytes 0, flags -

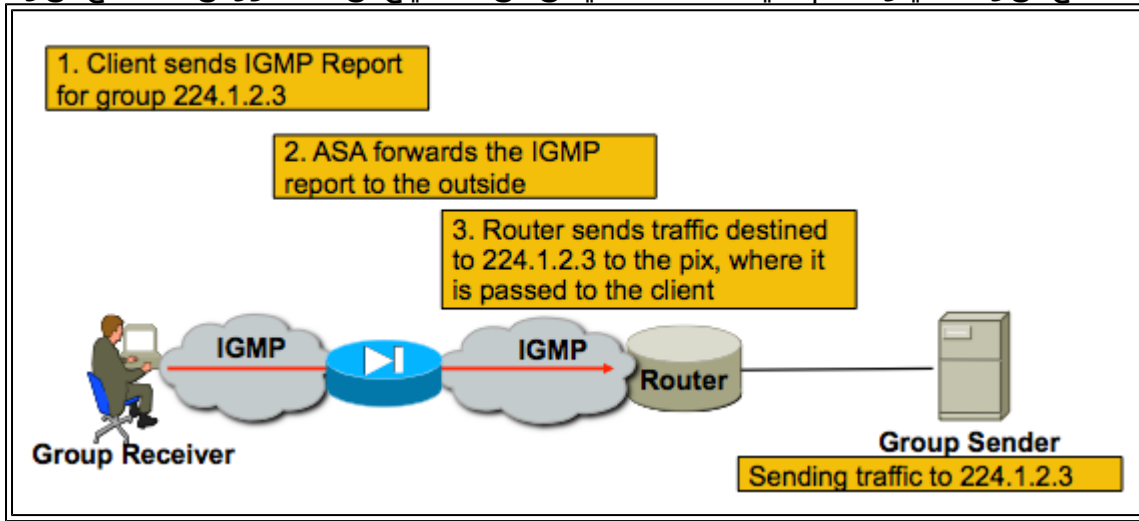
الاسر فيض الم لسري، ددعت الم ثبلا ليمع قي ببطت ق ال غاب ليمع الم موق ي نأ درجم ب: ةظحالم
IGMP م ال عتسا

لابقتسا دير ليمعك هجوم الم ةطساوب فورعمل ديحول فيض الم وه اذه ناك اذا ام ةلاحي في
RP لى لى IGMP ةانق ةالاسر هجوم الم لسري، ق فدل

يولوال IGMP عضو لي غشت

- ليمعك ASA لوكوتورب لمعي، (IGMP) تنرتنإل تاومجم ةرادا لوكوتورب بعبك عضو ي ف "تالصولا" مساب اضيأ ةفورعمل (IGMP) ريراقت عاشنإب موقيو، ددعتمال ثبلل ةرواجملا تاومجملا وحن اههيجوت ةداعا و (IGMP) تنرتنإل تاومجم ةرادا لوكوتورب ل ددعتمال ثبلل رورم ةكرح لابقتسا لي غشتل
- يأ تناك اذا ام ةفرعمل ةفيضملا ةزهجالا يلا تامالعتسا يروء لكشب تاومجملا لسرت ددعتمال ثبلل رورم ةكرح لابقتسا ي ف رارمتسالا ديرت ةكبشلا يلع ةدقع
- ربع دئاوللا نم ديدعل رفو ي ردانل PIM عضو نأل IGMP Stub-mode عضو ي صوي ال ةكراشملا يلع ةردقلاو، ةيلالاعف رثكال ددعتمال ثبلل رورم ةكرح تاقتدتم (Stub عضو ي ف PIM، امو يلا).

IGMP Stub: عضو هنيوكت مت يذلا ASA ل ياساسال لي غشتلا ةروصللا هذه حضوت



IGMP Stub عضو نيوكت

1. (ماعال نيوكتال عضو) ثبلل ددعتم هيجوتال نيوكمت.

<#root>

```
ASA(config)#
```

```
multicast-routing
```

2. ةيمامألا ةهجالا رمأ نيوكتب مق، IGMP ريراقت ةيماحل رادج لبقتسي يتلا ةهجالا يلع ل لصتت، لاثملا اذه ي ف. قفدللا نم رصملا يلا نراقلا جراح طبرلا تلسرا. IGMP لوكوتورب ل جراح ددعتمال ثبلل رصم نوكيو، ةيلخاللا ةهجالا ةرشابم ددعتمال ثبلل لابقتسا ةزهجالا ةي جراحال ةهجالا.

<#root>

```
!  
interface Ethernet0  
nameif outside
```

```
security-level 0
ip address 172.16.1.1 255.255.255.0
no pim
!
interface Ethernet1
nameif inside
security-level 100
ip address 10.0.0.1 255.255.255.0
no pim

igmp forward interface outside

!
```

3. نام ألسايس تضفر اذإ طقف یرورض) ةبسانملا ةهجالا یف ددعتملا ثبلا مزحب حمسا . (ةدراولا ددعتملا ثبلا رورم ةكرح ASA ب ةصاخلا

<#root>

```
ASA(config)#
access-list 105 extended permit ip any host 224.1.2.3

ASA(config)#
access-group 105 in interface outside
```

تاعومجم ةرادإ لوكوتورب ةهجالا یعرفلا عضولا رماوا لوح شیشوشت كانه نوكی ام ابلاغ لك مادختسا هیف مئی ذللا تقولا ططخملا اذه فصیو، ةفلتخمل (IGMP) تنرتنإلا

igmp forward interface <interface>	<pre>! Interface FastEthernet0/1 nameif inside security-level 100 ip address 10.0.0.1 255.255.255.0 igmp forward interface outside !</pre>	<p>Causes the firewall to forward IGMP reports received on the inside interface out the outside interface. You would use this command if multicast receivers were on the inside interface and the multicast source was somewhere out the outside interface</p>
igmp join-group <group name>	<pre>! Interface FastEthernet0/1 nameif inside security-level 100 ip address 10.0.0.1 255.255.255.0 igmp join-group 224.1.2.3 !</pre>	<p>Tells the firewall that there are hosts behind the inside interface that might want to receive the traffic for the group. It will send IGMP reports out the interface telling the LAN segment that the firewall wishes to receive the stream. It will also add the inside interface to the OIL list for the group. This method is not recommended; If you need to cause the firewall to add an interface to the OIL for an mroute, use the static-group command below</p>
igmp static-group <group name>	<pre>! Interface FastEthernet0/1 nameif inside security-level 100 ip address 10.0.0.1 255.255.255.0 igmp static-group 224.1.2.3 !</pre>	<p>Tells the firewall that there are hosts behind the inside interface that might want to receive the traffic for the group. It will simply add the inside interface to the OIL list for the group. This is useful for simulating a multicast receiver behind the inside interface.</p>

مې ب ري دي ب

روم ا ةثال ث ين عي اذهو . (SPT) ةكرتشم ةرجش دجوت ال ،هاجت ال ا ئئانث PIM ي ف

1. RP ال ا PIM ل ج س مزح ل اسراب (ل سر رمل اب ل صتم ال) ال و ال ا ةوطخل ال هجوم موق ي ال .
2. ردصم ال ةرجش ال ا مامضن ال ال PIM Join لئ اسر RP ل سري ال .
3. RP هاجت اب PIM Join لئ اسر ل اسراب ل بقت سمل ال ال ا سمل ال ي ف ةدوجوم ال ا هاجوم ال موقت . RPT ال ا مامضن ال ال .

ث بل ا رورم ةكر ل ك . SPT ال ا مضمنت ال ةزهج ال ال ن ال (S,G) ءاشن اب موق ي ال ASA ن ا ين عي اذهو ك انه ن ك ي مل اذ ا . (*,G) ك انه امل اط رورم ةكر multicast ل ك ال ASA ل سري . RP ربع رمت ددتم ال ل سري ال ن ا ب ج ي ف ، ةل ا ج ال وه اذه ن ا ك اذ ا . PIM Join ةمزح ا د ب ا ق ل تي مل ال ASA ن ا ين عي اذهف ، (*,G) ددتم ال ا ث بل ا مزح ال ASA .

Bidir PIM ني وكت

1. (م ا ل ال ني وكت ال ا عضو) ث بل ا ددتم ه ي جوت ال ني ك م تب مق .

<#root>

ASA(config)#

multicast-routing

2. PIM. ءاقتلال ةطقن ناوئع دي دحت .

<#root>

```
ASA(config)#
```

```
pim rp-address 172.18.123.3 bidir
```

3. نامألا ةسايس ماق اذا طقف يرورض) ةبسانملا ةهجالولا يف ددعتملا ثبلما مزح ب حم سا . (ةدراولا ددعتملا ثبلما مزح رظح ب ASA ب ةصاخلا

<#root>

```
access-list 105 extended permit ip any host 224.1.2.3
```

```
access-group 105 in interface outside
```

اهحالصإو ءاطخالأ فاشك تسأ ةيجه نم

ثبلما ءاطخالأ فاشك تسأ دنع اهعيميحت متي يتلا تامولعمل ا هحالصإو ددعتملا

مزلي، ASA، لعل لماك لكشب اهصخيشتو ددعتملا ثبلل هيچوت ةداعإ ةلكشم مهف لجأ نم اهللك وأ تامولعمل هذه ضعب

- ءاقتلالا ةطقنو، نيملتسملاو، ددعتملا ثبللا يلسرم عقومو، ةكبشلا ططخم فصو .
- ةمدختسملا تالوكوتوربلاو ذفانملا لىل ةفاضلاب، ةومجملاب صاخلا IP ناوئع .
- ددعتملا ثبللا قفدت هي ف هجاو يذلا تقولا يف ASA ةطساوب اهؤاشنإ مت يتلا Syslog ةلكشم .

· ASA رماو رطس ةهجالو نم ددحم show رما جارخإ :

<#root>

```
show mroute
```

```
show mfib
```

```
show pim neighbor
```

```
show route
```

```
show tech-support
```

- مزحلا تناك اذا امو، ASA لىل لصت ددعتملا ثبللا تانايب تناك اذا ام راهظال ةمزحلا طاقتلا .
- ةظحالم نكميو . ةمزحلاب صاخلا (TTL) ثبلل IP تقو ظحال (ASA لالخنم اههچوت ةداعإ متت 'show capture x detail' رمال مادختساب لك لذ
- لاثم . PIM. وأ IGMP مزحل مزحلا طاقتلا :

<#root>

```
capture cap1 interface outside match ip any host 239.1.1.77
```

>>> This captures the multicast traffic itself

```
capture cappim1 interface inside match pim any any
```

>>> This captures PIM Join/Prune messages

```
capture capigmp interface inside match igmp any any
```

>>> This captures IGMP Report/Query messages

· "show mroute" و "show mfib" لثم (تاهجومل) ةرواجملا ددعتملا ثبللا ةزهجأ نم تامولعم .
· ددعتملا ثبللا مزح طاقسإب موقيسي ASA ناك اذا ام ديدحتل ضرعل رماوأ وأ/و ةمزحل طاقتللا .
ةفاضإلاب .مزحل طاقسإب موقيسي ASA ناك اذا ام ديدحتل "show asp drop" رمال مادختسإ نكمي
يتلا مزحلل عيمج طاقتلل "asp-drop" عونلا نم مزحل طاقتلل مادختسإ نكمي ،كلذىلى
طاقتلل في ةدوجوم ددعتملا ثبللا مزح ناك اذا ام ةفرعمل اهصحف متي م ث ASA طقس
طاقسإلاب .

ديفم راهظإ رما جارخإ

ادج لثامم وهو ،هيجوتلا ةداعإ تامولعمو ةفلتخملا تاعومجمل show mroute رمال جارخإ ضرعي
ددعتملا ثبللا تاعومجمل ةصاخلا هيجوتلا ةداعإ ةلاح show mfib رمال ضرعي . show mroute رمال
يذلا) ىرخأ لىلى ةفاضإلاب ،هيجوتلا ةداعإ مزح دادع ةظحالم صاخ لكشب مهملا نم . ةفلتخملا
(طوقسللا تالاح لىلى ريشي :

```
<#root>
```

```
ciscoasa#
```

```
show mfib
```

```
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,  
AR - Activity Required, K - Keepalive  
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second  
Other counts: Total/RPF failed/Other drops  
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling  
IC - Internal Copy, NP - Not platform switched  
SP - Signal Present  
Interface Counts: FS Pkt Count/PS Pkt Count  
(* ,224.1.2.3) Flags: S K  
Forwarding: 0/0/0/0, Other: 0/0/0  
inside Flags: F  
Pkts: 0/0  
(192.168.1.100,224.1.2.3) Flags: K  
Forwarding: 6749/18/1300/182, Other: 690/0/690  
outside Flags: A  
inside Flags: F  
Pkts: 6619/8  
(* ,232.0.0.0/8) Flags: K  
Forwarding: 0/0/0/0, Other: 0/0/0  
ciscoasa#
```

رابط خال انثا ةي اغلل دي فم رمأ وهو ، تاداعل ا حسم ل clear mfib counters رمأ ل مادختسا نكمي :

```
<#root>
ciscoasa#
clear mfib counters
```

مزحل طاقتل

في احوال صا و ددعتم ل ثبل ا عا طخأ فاشكتسال ادج ةدي فم ةجمدم ل مزحل طاقتل ةدعاسم ةادأ 239.17.17.17 ل ةهجوم ل ، DMZ ةهجاو في لوخل مزح عي مج طاقتل متي ، لاثم ل اذه :

```
<#root>
ciscoasa#
capture dmzcap interface dmz

ciscoasa#
capture dmzcap match ip any host 239.17.17.17

ciscoasa#
show cap dmzcap
```

324 packets captured

```
1: 17:13:30.976618      802.1Q vlan#301 P0 10.1.123.129.2000 > 239.17.17.17.16384:  udp 172
2: 17:13:30.976679      802.1Q vlan#301 P0 10.1.123.129.2000 > 239.17.17.17.16384:  udp 172
3: 17:13:30.996606      802.1Q vlan#301 P0 10.1.123.129.2000 > 239.17.17.17.16384:  udp 172
4: 17:13:30.996652      802.1Q vlan#301 P0 10.1.123.129.2000 > 239.17.17.17.16384:  udp 172
5: 17:13:31.016676      802.1Q vlan#301 P0 10.1.123.129.2000 > 239.17.17.17.16384:  udp 172
6: 17:13:31.016722      802.1Q vlan#301 P0 10.1.123.129.2000 > 239.17.17.17.16384:  udp 172
....
```

اذه في ا. ادج دي فم نوكي ي ، طبرل نم TTL ل رمأ لي صفت x capture ضرع ل نم جات نإل ي دبي ةدم للقت ال اهنأل ارطن ةمزحل ا هذه ASA ررمي و) 1 ةمزحل ل (TTL) عاقبل ةدم نوكت ، جارخإل ا طقسيس مداخل نم تانايب ل قفدت هجوم نكل و (يضا رتفا لك شب IP مزحل (TTL) عاقبل ا مزحل :

```
<#root>
ASA#
show cap capout detail
```

453 packets captured

...

```
1: 14:40:39.427147 c062.6baf.8dc3 0100.5e7f.02c3 0x8100 Length: 1362
   802.1Q vlan#1007 PO 10.4.2.95.1806 > 239.255.2.195.5000: [udp sum ok] udp 1316 (DF) [ttl 1] (id
```

هنا نرى أن طاقته الال اذه حضوي. IGMP و PIM رورم ة كرح طاقته الال دي فم مزح ال طاقته الال نأ امك
10.0.0.2: اهردصم (2 IP لو كوتورب) IGMP ة مزح تقلت ة ي لخال الال

<#root>

ciscoasa#

```
capture capin interface inside
```

ciscoasa#

```
capture capin match igmp any any
```

ciscoasa#

```
show cap capin
```

1 packets captured

```
1: 10:47:53.540346 802.1Q vlan#15 PO 10.0.0.2 > 224.1.2.3: ip-proto-2, length 8
```

ciscoasa#

'show capture x detail' رم الال مادخت ساب مزحلل TTL ة يور نكمي هنا طحال

ببس و ة طقس م الال ددعت م الال ثبل مزح ره ظي يذال ذخت م الال ASP طاقس الال طاقته الال ة يور ان نكمي انه
(دحل-عاطق الال لدعم) طاقس الال تاي لمع

<#root>

ASA#

```
show cap capasp det
```

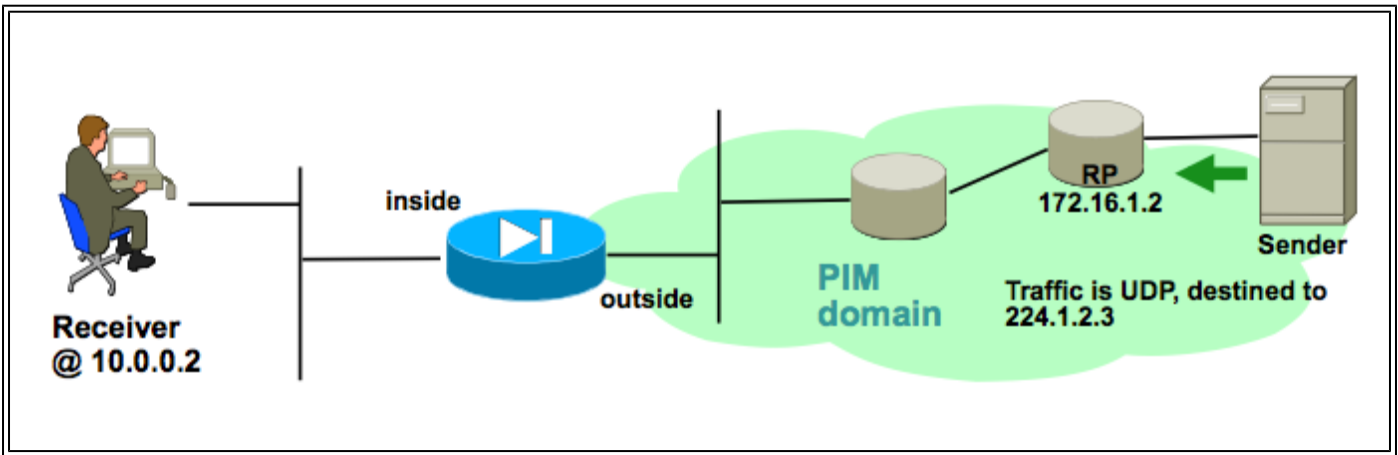
```
12: 14:37:26.538332 c062.6baf.8dc3 0100.5e7f.02c3 0x8100 Length: 1362
   802.1Q vlan#1007 PO 10.76.4.95.1806 > 239.255.2.195.5000: [udp sum ok] udp 1316 (DF) [ttl 1] (id
13: 14:37:26.538439 c062.6baf.8dc3 0100.5e7f.02c3 0x8100 Length: 1362
   802.1Q vlan#1007 PO 10.76.4.95.1806 > 239.255.2.195.5000: [udp sum ok] udp 1316 (DF) [ttl 1] (id
```

ASA PIM رثان م الال عضولال ي ف ددعت م الال ثبلال رشن

قرفت م الال PIM عضوي ف ة رواج م الال ة زه الال عم ASA لعافت ة ي ف ي ك تاططخ م الال هذه حضوت

ة ك بشلال طاطخ م هه

ناونع دح، اضيأ. ةق د ب ددح م ل ا ددع م ل ا ث ب ل ا ق ف د ت ل ن ي م ل ت س م ل ا و ن ي ل س ر م ل ا ع ق و م د ي د ح ت
 عا ق ت ل ا ل ا ة ط ق ن ع ق و م ي ل ا ة ف ا ض ا ل ا ب ، د د ع م ل ا ث ب ل ا ة ع و م ح م ل IP



ي ل ا ا ه ي ج و ت ة د ا ع و ، ASA ل ة ي ج ر ا خ ل ا ة ه ج ا و ل ا ي ل ع ت ا ن ا ي ب ل ا ي ق ل ت ن ك م ي ، ة ل ا ح ل ا ه ذ ه ي ف
 IP ة ك ب ش ي ف د و ج و م ل ا ب ق ت س ا ل ا ز ا ه ج ن ا ل ا ر ط ن . ة ي ل خ ا د ل ا ة ه ج ا و ل ا ي ل ع د د ع م ل ا ث ب ل ا ل ب ق ت س م
 م ت ي IGMP ر ي ر ق ت ة ي و ر ع ق و ت ك ي ل ع ف ، ASA ل ة ي ل خ ا د ل ا ة ه ج ا و ل ا ب ة ص ا خ ل ا ا ه س ف ن ة ي ع ر ف ل ا
 ص ا خ ل ا IP ن ا و ن ع . ق ف د ل ا ي ق ل ت ل ي م ع ل ا ب ل ط ي ا م د ن ع ة ي ل خ ا د ل ا ة ه ج ا و ل ا ي ل ع ه ل ا ب ق ت س ا
 و ه ل س ر م ل ا ب 192.168.1.50.

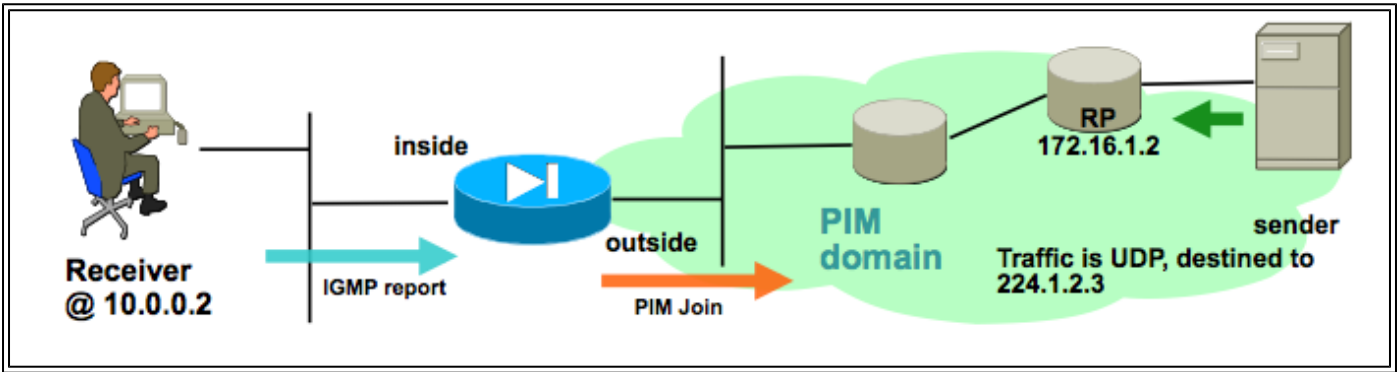
ل ب ق ت س م ل ا ن م IGMP ر ي ر ق ت ASA ي ق ل ت ن م ق ق ح ت ل ا

ASA. ة ط س ا و ب ه ت ج ل ا ع م م ت ي و م ل ت س م ل ا ة ط س ا و ب IGMP ر ي ر ق ت ء ا ش ن ا م ت ي ، ل ا ث م ل ا ا ذ ه ي ف

ن م ق ق ح ت ل ل ة ي ل خ ا د ل ا ة ر ا ب ع ل ا ل و ك و ت و ر ب ء ا ط خ ا ح ي ح ص ت ت ا ج ر خ م و م ز ح ل ا ط ا ق ت ل ا م ا د خ ت س ا ن ك م ي
 ج ا ج ن ب IGMP ة ل ا س ر ة ج ل ا ع م و ، ASA ي ق ل ت

عا ق ت ل ا ل ا ة ط ق ن ي ل ا PIM Join ة ل ا س ر ل س ر ي ASA ن ا ن م ق ق ح ت ل ا

RP. و ح ن ة ه ج ا و ل ا ج ر ا خ ا ه ل س ر ي م ث ، PIM م ا م ض ن ا ة ل ا س ر د ل و ي و IGMP ر ي ر ق ت ASA ر س ف ي



PIM م ا م ض ن ا ة ل ا س ر ل س ر ي ASA ن ا ر ه ظ ي و PIM 224.1.2.3 ء ا ط خ ا ل ا ح ي ح ص ت ة ع و م ح م ن م ج ا ر خ ا ل ا ا ذ ه
 192.168.1.50. و ه د د ع م ل ا ث ب ل ا ق ف د ل س ر م . ج ا ج ن ب

```
IPv4 PIM: (*,224.1.2.3) J/P processing
IPv4 PIM: (*,224.1.2.3) Periodic J/P scheduled in 50 secs
IPv4 PIM: (*,224.1.2.3) J/P adding Join on outside
IPv4 PIM: (*,224.1.2.3) inside Processing timers
```

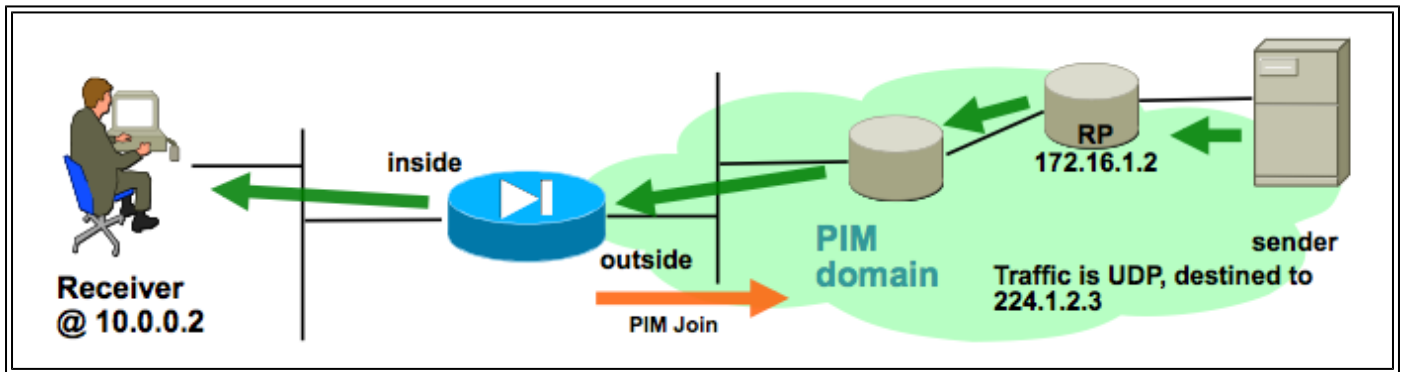
```

IPv4 PIM: Sending J/P message for neighbor 10.2.3.2 on outside for 1 groups
IPv4 PIM: [0] (192.168.1.50,224.1.2.3/32) MRIB update (a=0,f=0,t=1)
IPv4 PIM: [0] (192.168.1.50,224.1.2.3/32) outside MRIB update (f=20,c=20)
IPv4 PIM: [0] (192.168.1.50,224.1.2.3) Signal present on outside
IPv4 PIM: (192.168.1.50,224.1.2.3) Create entry
IPv4 PIM: [0] (192.168.1.50,224.1.2.3/32) outside MRIB modify NS
IPv4 PIM: Adding monitor for 192.168.1.50

```

هه جيوت ةداع او ددعت الما ثبلا قفدتل ASA يقلت نم ققحتل

ديعيو، (رضخأ مهسلا كلذ يدي) يجراخ نراقلا ىلع multicast رورم ةكرح يقلتب ASA لا ادبي لخداللا ىلع يقلت الما ىلا اهه جيوت.



نم ققحتلل، مزحلا طاقتلا ىلا ةفاضلاب، show mroute و show mfib رماو مادختسا نكمي اهه جيوت ةداع او ددعت الما ثبلا مزحل ASA يقلت.

ددعت الما ثبلا قفدت ليثمتل لاصتالا لودج ي ف لاصتاءاشن امتي:

```

<#root>
ciscoasa#
show conn
59 in use, 29089 most used
...
UDP outside:192.168.1.50/52075 inside:224.1.2.3/1234 flags -
...

```

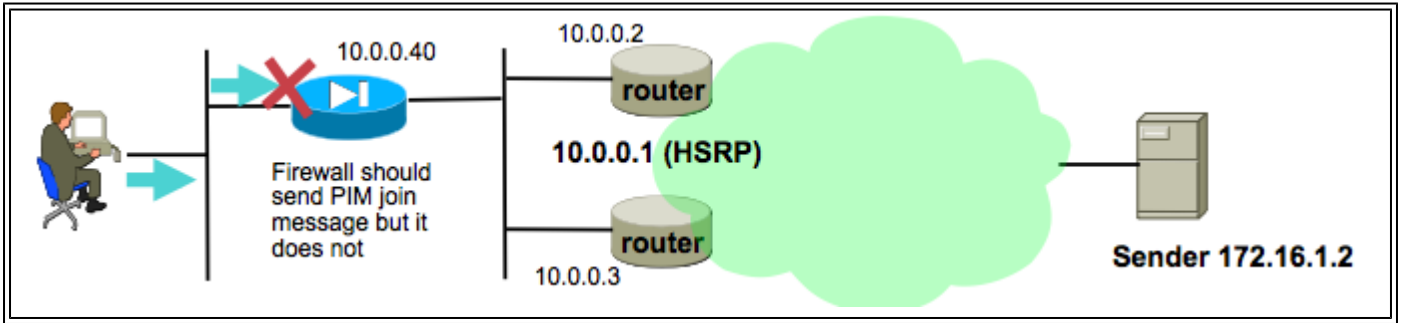
تانايبلا ليحت

ةكرتشم لكاشم

ملاعلا ي ف ASA ددعت الما ثبلا ةصللا تا ذ لكاشم الما نم ةلسلس مسقلا اذه رفوي يقي قحلا

HSRP ببسب مداخل تاهجوم وحن PIM لئاسر لاسرا ي ف ASA لشف

طبخملا اذه حضوي .ةهجاو نم PIM لئاسرر ي لاسررا في ASA لش في ،ةلكشملا هذه ةهجاوم دنع ام دنع ةلكشملا سفن ةيؤر نمك مي نكلو ،لسررملال لىل PIM لئاسرر لاسررا هنكمي ال ASA نأ RP. لىل PIM ةلاسرر لاسررا لىل ASA جاتحي



ةيلاللا ةوطخلال هجاوم لىل PIM ةلاسرر لاسررا هنكمي ال ASA نأ debug pim رمالا جارخا حضوي قفدتلل:

```
IPv4 PIM: Sending J/P to an invalid neighbor: outside 10.0.0.1
```

نم ةلكشملا ليغشت متي .تاهجوملا لىل اضيأ رثؤتو ،ASA لىل ةلكشملا هذه رصتقت ال PIM ناريج لبق نم مدختسملال HSRP نيوكتو هيجوتلال لودج نيوكت ني ب عمجال لالخال

ةيلاللا ةوطخلال زاهاك IP 10.0.0.1 HSRP لىل هيجوتلال لودج ريشي:

```
<#root>
ciscoasa#
show run route
route outside 0.0.0.0 0.0.0.0 10.0.0.1 1
```

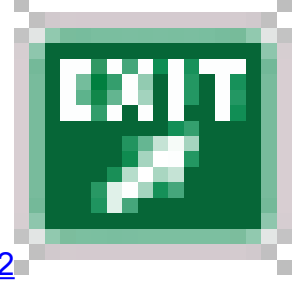
س يلو ،تاهجوملل ةيداملال ةهجاولل IP نيوانع ني ب PIM راولع نيوكت متي ،كلذ عم و IP HSRP ناونع:

```
<#root>
ciscoasa#
show pim neighbor
Neighbor Address Interface Uptime Expires DR pri Bidir
10.0.0.2 outside 01:18:27 00:01:25 1
10.0.0.3 outside 01:18:03 00:01:29 1 (DR)
```

نم ديزم لىل لوصحلل "HSRP؟ ناونع لىل اثبات راسم عم ردانللا PIM عضو لمعي ال اذامل" عجار

ت.امولعمل.

ة:قثولانم فطتقم



مئلقتل/مامضنالا ةلسرلسراب هوملالموقئال اذامل
راسملا هئوت ةءاعلال زئم روم لك لئ ةئود هئقننن/مامضنالا ةلسرلسرئ هوملانا لئ
خسنننل/مامضنالا لئاسرلسرا مئئ. (*،*،RP) و (*،G) و (S،G) لئءل لك ب طبترم (RPF) لئسكعلا
PIM. راج (RPF) لئسكعلا راسملا هئوت ةءاعلال راج ناك اءل طقف

اهنا نم دكأت. ةئنعمل رورملا ةكرحل ASA لئسكعلا راسم لئءل فضا، ةلكشملا لئلقتل
ل رمالا اءه حمسئ، ةلءال هءه ف. (10.0.0.2 و 10.0.0.3) هوملا ةءاول IP لئناونع دءا لئ رئشئ
172.16.1.2 لئسكعلا ءلءل لئسرم لئ ةءوملالم PIM لئاسرلسراب ASA

<#root>

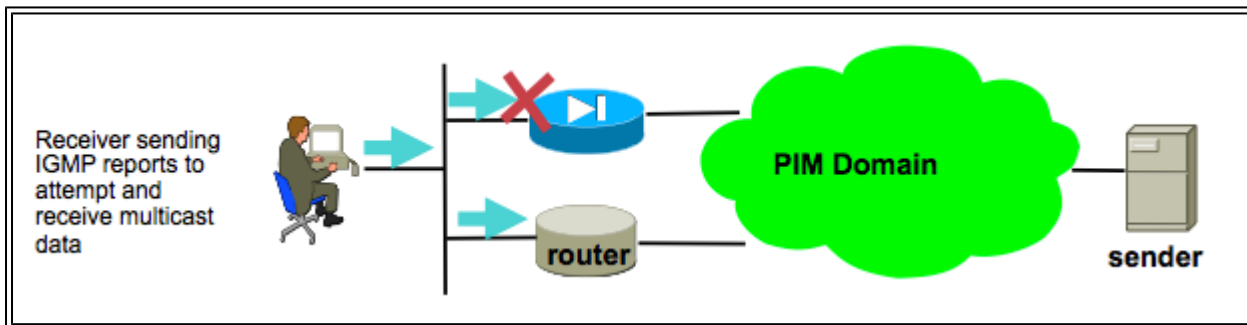
```
ciscoasa(config)#
```

```
mroute 172.16.1.2 255.255.255.255 10.0.0.3
```

ب صاءلا لئءالءال ءلءال هئوت لوءء دءءملا ءلءال هئوت لوءء زواءئئ، لكءب مائلالاءءءم ب
روءملا 10.0.0.3 زاه لئ ةرءشابم PIM لئاسرلسراب ASA لئسري و ASA.

ءكءبشلال عطقم لئسكعلا هوملالم سئل هنال IGMP رئراقء ASA لهاءئئ
(LAN) ةئلءملا

لصءم دءءم ءلءل بقاءءسم نم IGMP رئرقء ASA لئسكعلا هءل ءبسننلاب
ءمءللا طاقسلا مئئ و ءاطءالاءءل هئصءءارءل ءاشنل مئئال. لكءل لهاءئئ هنكلو، ةرءشابم
قفءللا لئسكعلا لئسكعلا، ءطاسبب



ل هباءءنل مئئ لئسكعلا هوملالم سئل هنال ءمءللا ASA لهاءئئ، ءكءبشلال هءل ءبسننلاب
ءالءملاءءاوءئئ ءئء (LAN) ةئلءملا عطقم لئسكعلا PIM

هه لراشملا) نيعملا هوملا وه رخآ ازاهج نأ ASA اذه (CLI) رمأوالا رطس ههجاو جارجا حضوي
ةيلخادلا ههجاو لةكبش ىلع ("DR" ةطساوب

```
<#root>
```

```
ciscoasa#
```

```
show pim neighbor
```

Neighbor Address	Interface	Uptime	Expires	DR	pri	Bidir
192.168.1.2	outside	01:18:27	00:01:25	N/A		
10.0.0.2	inside	01:18:03	00:01:29	1		

```
(DR)
```

multicast-routing رمأال ةفاضل دنع ASA تاهجاو عيمج ىلع PIM نيكم متي ،يضارتفا لكشب
ASA ل ةيلخادلا ههجاو لىلع (ASA وأ رخآ تاهجوم) PIM ل نورخآ ناريج كانه ناك اذا .نيوكتلا ىل
تاهجوم موقت ذئدنع ،عزجلا كذلذ DR نأل ناريجال ءالؤه دحأ رايخ متو (ءالمعال ميق ي شيح)
no pim رمأال مادختساب) ههجاو لىلع PIM ليطعت وه لجال .IGMP ريراقت طاقساوب DR ريغ رخآ
PIM dr-priority ههجاو لرمأ ربع عطقم لل DR وه ASA لجع وأ ،(ةينعملا ههجاو لىلع

IGMP ههجاو دح زواجت دنع ةياملال رادج ةطساوب IGMP ريراقت ضفر متي

وه اذه .ههجاو لىلع هبقت متي ي لاج (ريراقت) طشن طبار 500 ب ASA حمسي ،يضارتفا لكشب
ثبلا تاقفدت نم اريبك ادعء الملال بلط اذا .نيوكتلل ةلباقلا ةميقلل ىصقأال دجال
لهاجتي نأ نكمي و ،ةطشن ةلصو 500 ددعل ىصقأال دجال ههجاوم نكمي ،ههجاو ل جراخ ددعتمال
ددعتمال ثبلا لابقساوب ءزهجا نم ةيفاضلا ءدراول IGMP ريراقت ASA

show igmp interface رمأال رادصاوب مق ،ددعتمال ثبلا لشف ببس وه اذه ناك اذا ام ديكأتل
ههجاو ل "IGMP دح" تامولعم نع ثحباو 'interface interface'

```
<#root>
```

```
ASA#
```

```
show igmp interface inside
```

```
Hosting-DMZ is up, line protocol is up
Internet address is 10.11.27.13/24
IGMP is enabled on interface
Current IGMP version is 2
IGMP query interval is 125 seconds
IGMP querier timeout is 255 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1 seconds
Inbound IGMP access group is:
```

```
IGMP limit is 500, currently active joins: 500
```

```
Cumulative IGMP activity: 7018 joins, 6219 leaves
IGMP querying router is 10.11.27.13 (this system)
```

DEBUG - IGMP: Group x.x.x.x limit denied on outside

يتم 232.x.x/8 لـ في رورم multicast لـ سرى نـ ASA لـ لـ شـ في

هم عدي الـ يـ ذـ لـ (SSM) ردصم لـ ددعتم لـ ثـ بـ لـ عم مادختس لـ صـ صـ مـ اذـه نيوانع لـ قاطن
ASA لـ لـ اـ.

أطخ لـ اذـه debug igmp رم لـ اـ جـ اـ رـ عـ يـ

IGMP: Exclude report on inside ignored for SSM group 232.179.89.253

راسم لـ هـ يـ جـ وـ تـ ةـ دـ اـ عـ نـ م قـ قـ حـ تـ لـ بـ بـ سـ بـ ددعتم لـ ثـ بـ لـ مـ زـ حـ ASA طـ قـ سـ يـ
يـ سـ كـ عـ لـ

يـ لـ عـ لـ سـ رـ يـ الـ وـه نـ اـ رـ يـ غـ ، نـ رـ اـ قـ يـ لـ عـ multicast رورم ةـ كـ حـ ASA لـ مـ لـ تـ سـ يـ ، ةـ لـ اـ حـ لـ هـ ذـه يـ في
هـ يـ جـ وـ تـ ةـ دـ اـ عـ نـ م قـ قـ حـ تـ لـ يـ فـ لـ شـ فـ تـ اـ هـ نـ اـ لـ ASA ةـ طـ سـ اـ وـ بـ مـ زـ حـ لـ طـ اـ قـ سـ اـ مـ تـ يـ . يـ قـ لـ تـ مـ لـ
تـ اـ هـ جـ اـ وـ لـ اـ عـ يـ مـ جـ يـ لـ عـ (RPF) يـ سـ كـ عـ لـ راسم لـ هـ يـ جـ وـ تـ ةـ دـ اـ عـ نـ م قـ قـ حـ تـ لـ مـ تـ يـ . (RPF) يـ سـ كـ عـ لـ راسم لـ
قـ قـ حـ تـ لـ مـ تـ يـ الـ ، يـ دـ اـ حـ اـ لـ ثـ بـ لـ مـ زـ حـ لـ ةـ بـ سـ نـ لـ اـ بـ) اـ هـ لـ يـ طـ عـ تـ نـ كـ مـ يـ الـ وـ ددعتم لـ ثـ بـ لـ رورم ةـ كـ حـ لـ
(ip verify reverse-path interface) رم اـ مادختس اـ بـ هـ نـ يـ كـ مـ تـ مـ تـ يـ وـ ، يـ ضـ اـ رـ تـ فـ اـ لـ كـ شـ بـ

ددعتم لـ ثـ بـ لـ رورم ةـ كـ حـ مـ aـ lـ تـ سـ اـ دـ نـ عـ ، (RPF) يـ سـ كـ عـ لـ راسم لـ هـ يـ جـ وـ تـ ةـ دـ اـ عـ نـ م قـ قـ حـ تـ لـ بـ بـ سـ بـ
هـ نـ اـ فـ) ددعتم لـ ثـ بـ لـ رورم ةـ كـ حـ ردصم يـ لـ اـ رـ خـ اـ ةـ رـ مـ راسم هـ يـ دـ لـ نـ اـ مـ ASA قـ قـ حـ تـ يـ ، ةـ هـ جـ اـ وـ يـ لـ عـ
راسم هـ يـ دـ لـ نـ كـ يـ مـ لـ اـ ذـ اـ . ةـ هـ جـ اـ وـ لـ كـ لـ تـ يـ لـ عـ (ددعتم لـ ثـ بـ لـ وـ يـ دـ اـ حـ اـ لـ ثـ بـ لـ هـ يـ جـ وـ تـ لـ وـ دـ جـ نـ م قـ قـ حـ تـ يـ
جـ اـ رـ خـ اـ يـ فـ دـ aـ دـ عـ كـ طـ وـ قـ سـ لـ تـ aـ يـ لـ مـ عـ هـ ذـه رابـ تـ عـ نـ كـ مـ يـ . ةـ مـ زـ حـ لـ طـ aـ قـ سـ اـ بـ مـ وـ قـ يـ هـ نـ اـ فـ ، لـ سـ رـ مـ لـ يـ لـ
show asp drop:

<#root>

ciscoasa(config)#

show asp drop

Frame drop:

Invalid UDP Length	2
No valid adjacency	36
No route to host	4469
Reverse-path verify failed	121012

route رم لـ اـ مادختس اـ مـ تـ يـ ، لـ اـ ثـ مـ لـ اـ ذـه يـ فـ . رورم لـ ةـ كـ حـ لـ سـ رـ مـ لـ راسم ةـ فـ اـ ضـ اـ وـه تـ اـ رـ aـ يـ خـ لـ دـ حـ
172.16.1.2 نـ م ةـ مـ لـ تـ سـ مـ لـ ددعتم لـ ثـ بـ لـ رورم ةـ كـ حـ لـ (RPF) راسم لـ هـ يـ جـ وـ تـ ةـ دـ اـ عـ نـ م قـ قـ حـ تـ يـ صـ حـ فـ اـ ضـ رـ aـ لـ
ةـ يـ جـ aـ رـ خـ aـ لـ ةـ هـ جـ aـ وـ lـ يـ لـ عـ

<#root>

```
ciscoasa(config)#
```

```
mroute 172.16.1.2 255.255.255.255 outside
```

ردصملا ةرجش ىلإ PIM ليدبت ىلع PIM Join ءاشنإب ASA موقى ال

ددعتملا ثبلا لسرم نم PIM ل رثانتملا عضولا يف ددعتملا ثبلا مزح قفدتت، ةيادبلا يف لوصو درجمب، كلذ عمو. ةكرتشم ددعتم ثب ةرجش ربع لبقتسملا ىلإ RP نم م، RP ىلإ ددعتملا ثبلا لبقتسم ىلإ برقألا هجوملا لواحي، ني عم دح ىلإ يلامجالا ثبلا لدعم ءاشنإب هجوملا اذه موقى. ردصملا ب ةصاخلا ةرجشلا لوط ىلع تانايبلا رورم ةكرح لابقتسا امك، RP هاجت سي لو) ددعتملا ثبلا قفدت لسرم ىلإ هلاسراو ةومجملل ديدج PIM مامضنا (لبق نم ناك).

امدنع RP. نعة فلتخم ASA ةهجاو ىلع ددعتملا ثبلا رورم ةكرح لسرم موقى نأ نكمي راسم ASA ل نوكى نأ بجي، ردصملا ددحمللا ةرجشلا ىلإ ليدبتلل PIM Join ASA لبقتسي مامضنا ةمزح طاقسا متي، راسملا اذه ىلع روثعلا متي مل اذا. لسرملا ب صاخلا IP ناو نع ىلإ PIM ءاطخأ حيحصت جارخا يف ةلاسرا هذو ةيؤر متي و PIM

```
NO RPF Neighbor to send J/P
```

ASA ةهجاو ىلإ ري شي، قفدلا لسرملا ثبات راسم لاخدا ةفاضلا وه ةلكشملا هذو صاخلا لجالا لسرملا اهنم دجاوتي يتلا.

(TTL) ءاقبلا ةدم زواجت ببسب ددعتملا ثبلا مزح ASA طاقست

ببستى اذهو. ادج ضفخنم طبرلا نم TTL ل نأل رورم ةكرح multicast لش في، ةلالا هذو يف اءاطاقسا ب، ةكبشلا يف ىرخألا ةزهجالا ضعب وأ، ASA مايق يف

ادج ةضفخنم اهنىي عت مت يتلا TTL IP ةميقى ىلع ددعتملا ثبلا مزح يتوتحت ام ابلاغ يضارتفا لكش ب كلذب مايقلا متي، ناىجالا ضعب يف. اهل سرأ يذلا قي بطلتلا ةطساوب لببس ىلع. ةكبشلا نع اديعب ددعتملا ثبلا رورم ةكرح لاقتنا مدع نامض يف ةدعاسملا ثبلا ددعتم لاسرا زاىج) ليمعلا قي بطلت لمعي LAN ويديفلا يضارتفا لكش ب، لاثملا يضارتفا لكش ب 1 ىلع IP ةمزح يف (TTL) ءاقبلا ةدم نيي عت ىلع (رابتخا ةادأو عئاش

مزحلا طاقسا و يلالا (CPU) ةيزكرملا ةجالاعملا ةدحو مادختسا ASA ربتخي ةددحمللا ددعتملا ثبلا ايجولوبط ببسب

ددعتملا ثبلا قفدت هجاوي نأ نكمى و ةيالا (CPU) ةيزكرم ةجالاعم ةدحو ASA هجاوي نأ نكمى ددعتملا ثبلا ططخم لوح ةحيحصتالا هذو عيمجتناك اذا مزحلا طاقسا تالاح:

1. RP ل اءافصب ASA ل لمعي و.
2. ددعتملا ثبلا لسرم نأ ينعى اذه. راي ت multicast ل نم لابقتسا ةوطخ لوأ وه ASA ل.

ASA ههجاووا هسفن ةعرفال IP ةكبش يف دوجوم

ثبلال لبقتسم نأ يفنعي اذه .ددعتمال ثبلال قفدت نم ةريخأال ةوطخال هجوم وه ASA .3
ASA ههجاوب ةصاخال هسفن ةعرفال IP ةكبش يف دوجوم ددعتمال

الجاتفمال جلاعي نأ ربحم نوكي ASA ل ديحت ميمصت لمع بجاو ةروكذمال ضارعال ترهظ اذإ
عفترم تانايب لقن لدعم تاذا ددعتمال ثبلال تاقفدت لىل يدؤي اذهو .رورم ةكرح multicast
وه مزحل هذه طاقس دنع ديزي يذل show asp طاقس دادع نوكي .مزحل طاقس ايلمع ةبرجتل
punt-rate-limit.

steps: اذه ،ةلكشم اذه ىقلتي ASA ن اددح in order to تمتأ

RP: وه ASA ناك اذإ امم ققحت 1: ةوطخال

```
<#root>
```

```
show run pim  
show pim tunnel
```

ةريخأال ةوطخال هجوم وه ASA ناك اذإ امم ققحت 2: ةوطخال

```
<#root>
```

```
show igmp group  
<mcast_group_IP>
```

ىلوال ةوطخال هجوم وه ASA ناك اذإ امم ققحت 3: ةوطخال

```
<#root>
```

```
show mroute  
<mcast_group_IP>
```

ةلكشمال هذه نم فيفختلل ةيلاتل تاوطخال ذاخت ا نكمي

ةرشابم لصتم ريغ ملتسمال وأ لسرمل لعج ،وأ RP. وه ASA نوكي ال شيحب ططخمال ليدعت -
ع ASA

- ددعتمال ثبلال هيجوت ةداعإل IGMP stub عضو مدختسأ ،PIM نم ال دب -

الو ا ددعتمال ثبلال قفدت ادب دنع لىلوال ةللىل مال مزحل طاقس اب ASA موقوي

لاصتا انايب ASA موقوي نأ بجي ،ASA لىل ددعتمال ثبلال قفدت نم لىلوال مزحل لوصو دنع
يف لاخداال نوكي امنيب .مزحل هيجوت ةداعإل طبترممال راسمال لاخداو اذه ددحمال ددعتمال ثبلال

تالاصتالاوراسملا ءاشنإ متي ىتح ددعتملا ثبلا مزح ضعب طاقسإ نكمي، ءاشنإل ءي لمع مزحلا دعت مل، ددعتملا ثبلا قفدت دادعإ لامتكأ درجمب. (ةيناث نم لقلأ كلذ قرغتسي ام ءداع) لدملا ءددم.

هنيوكت مت ASP طاقسإ طاقسإ ل ASP (Punt-rate-limit) "Punt-rate-limit) Limit". اذه 'show capture asp' جرخم وه اذه مت يتيلا مزحلا نوكي (اهطاقسإ مت يتيلا مزحلا طاقسإ ل ASA ىلع بابسلا اذهل اهطاقسإ):

```
<#root>
```

```
ASA #
```

```
show capture asp
```

```
2 packets captured
```

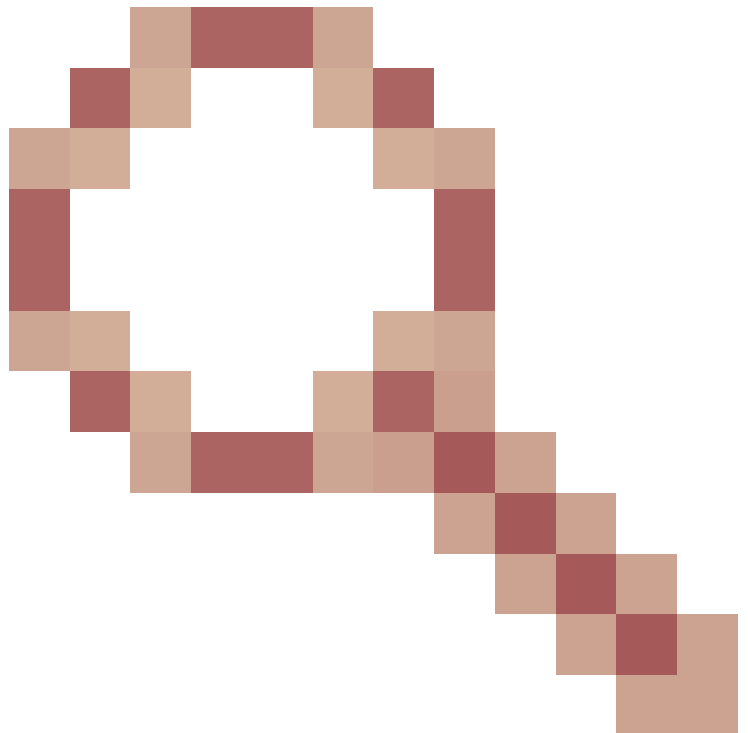
```
1: 16:14:49.419091 10.23.2.2.810 > 239.255.123.123.890: udp 32 Drop-reason: (punt-rate-limit) Punt
```

```
2: 16:14:49.919172 10.23.2.2.810 > 239.255.123.123.890: udp 32 Drop-reason: (punt-rate-limit) Punt
```

```
2 packets shown
```

ةومجم لابقتسإ ءةطاقمب لصتملا ريغ ثبلا ددعتم لابقتسإ زاغ موقبي ىرخألا تاهجاولا ىلع ددعتملا ثبلا

ASA تادحورثأتت ال. ءلكشملا هذه نم يناعت IGMP Stub عضوي لمعت يتيلا ASAs طقف PIM ل ددعتملا ثبلا هيجوت ي ف كراشت يتيلا.



ع رادصإل تنبي Cisco ب id [CSCeg48235](#)

نراق رخآ ىلع ددعتملا ثبلا رورم ءكرح عطاقي نراق دحاو ىلع ءزاج IGMP.

ةلكشملا حرشت يتيلا، أطخل نم رادصإل ءظالم يه هذه:

ASA(config)#

show mfib 239.255.2.1195

Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
AR - Activity Required, K - Keepalive
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
IC - Internal Copy, NP - Not platform switched
SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count

(* ,239.255.2.195) Flags: C K
Forwarding: 4278/50/1341/521, Other: 0/0/0
Outside-1007 Flags: A
RDEQ-to-Corporate Flags: F NS
Pkts: 0/4278 <---- HERE

(S,G) ال نكلو (*,G) ددعتملا ثبلا هي جوت لودج رهظي

<#root>

ASA(config)#

show mroute 239.255.2.1195

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

(* , 239.255.2.195), 00:44:03/00:02:44, RP 10.1.135.10, flags: S
Incoming interface: Outside-1007
RPF nbr: 10.100.254.18
Immediate Outgoing interface list:
RDEQ-to-Corporate, Forward, 00:44:03/00:02:44

ASA موقوي 1. وه ASA لى لى لصي نأ طبر تاي طعم multicast طبر لى نأ انه ةلكشملا موقوي نكلو، (TTL للقي ال هنأل) مداخل لى لى تاناي بى قفدت زاه لى لى مزحلا هذه هي جوت ةداعاب مداخل لى نأ تاناي بى قفدت هجوم موقوي ال، كذل ةجيتنو. مزحلا طاقساب مداخل لى لى هجوم ال ASA موقوي ال. لسررمل هاجت ASA لى لى (ردصملا ددجم مامضنا) (S,G) PIM لى لى مامضنا لاسراب رورم ةكرح لك نإف، هؤانب متي مل (S,G) نأل. اذه PIM مامضنا ملتسي يتح (S,G) لخدإ عاشناب لى لى ددعتملا دح هنع جتني امم اهلي وحت متي ددعتملا ثبلا

زاهج لحمست يتلاو، 1 تسي ل مزحلل (TTL) عاقبلا ةدم نأ نم دكأتلا وه ةلكشملا هذه لى لى لى ف بىستى اذهو؛ لسررمل وحن ردصملا لى لى مامضنالا لاسراب مداخل لى نأ تاناي بى قفدت ةعرسب مزحلا عي مج لي دبب متي م، لودجلا يى ردصملا لى لى صاخ راسم تي بىببب ASA ماق ةلكشم ثودح نود ASA ربع رورملا ةكرح قفدت بجيو (هتجالع م تمت يذلا لودجلا نم ال دب)

PIM دي كأت ةلاسرب بسبب ددعتملا ثبلا قفدت فاقى مت

ةي عرفال ةكبشلا ىلإ اهسفن ددعتملا ثبلا مزح هي جوت ةداعإ ةكبشلا نازاهج ماق اذا
تايافنلا نم هنأل ارظن) مزحلا هي جوت ةداعإ فاقيا يلاثم لكشب امه دحأ ىلع بجيف ،اهسفن
يتلا اهسفن مزحلا ملتست اهنأ PIM لغشت يتلا تاهجوملا تفشتكا اذا .(ق فدل راركت
ىلع ديكأتلا لئاسر ءاشنإب موقت اهنإف ،اهسفن ةهجاو لا كلت ىلع اهئاشنإب اضيا موقت
ق فدل هي جوت ةداعإ نع فقوت يذلا ةكبشلا زاهج ديدحتل ةي لحملا ةكبشلا كلت

[ةي لمعب قلعتم RFC 4601 نم مسق](#) يف ةلاسرلا هذه لوح تامولعمل نم ديزم ةظحالم نكمي
[ديكأتلا](#).

ري رقتلا لهاجتي هنكلو ،239.1.1.227 ةومجملل IGMP ريرقت ملتسي ASA نأ ءاطخألا رهظت
رواجم هجوم نم اه اقلتي يتلا ةلاسرلا ديكأت ببسب

```
IPv4 PIM: (*,239.1.1.227) Periodic J/P scheduled in 50 secs
IPv4 PIM: (*,239.1.1.227) J/P adding Join on outside
IPv4 PIM: (10.99.41.205,239.1.1.227)RPT J/P adding Prune on outside
IPv4 PIM: (10.99.41.253,239.1.1.227)RPT J/P adding Prune on outside
IGMP: Received v2 Report on inside from 10.20.213.204 for 239.1.1.227
IGMP: Updating EXCLUDE group timer for 239.1.1.227
IPv4 PIM: (10.99.41.253,239.1.1.227) Received [15/110] Assert from 10.20.13.2 on inside
IPv4 PIM: (10.99.41.253,239.1.1.227) Assert processing message wins
IPv4 PIM: (10.99.41.253,239.1.1.227) inside Update assert timer (winner 10.20.13.2)
```

يف دوصقم ريغ لكشب ني عقوم رسج مت شي جاتنإ ةكبش يف ةلكشملا هذه ةظحالم تمت
نيزاهج هي دل ىلع ددعتملا ثبلا تالبقتسم ناك شي ةي لحملا ةكبشلا نأل لثم ،2-ةق بطلا
ASA ىلع رذعت ،ىرخأ ةكبش ةلكشم ثودحل ارظن .مهوحن ددعتملا ثبلا رورم ةكرح هي جوت ةداعإ
هجوملا رود امهنم لك ذخأ دق ف يلاتلابو ،PIM hellos ربع ضعبلا امهضعب نع فشكلا رخأ زاهجو
لشف مت ،ةرتفل ددعتملا ثبلا رورم ةكرح لمع ىلإ كلذ ىدا .(LAN) ةي لحملا ةكبشلا ني عمل
ريغ لاصتالا ليطعت مت ،ةلكشملا لحل .ةزهجال ةطساوب ديكأتلا لئاسر لاسرا دنع
ةلكشملا لح مت مت ،2 ةق بطلا يف ةزهجال رسجي يذلا حيحصلا

ةمزحلا مجح ببسب رواجملا ةطساوب هتجالعم متت ال نكلو ASA PIM Join لسري
MTU نم ربكألا

4900. زارطلا نيوكت متي ملو Jumbo تاراطإل ASA نيوكت مت .629575899 ماع يف كلذ ظحولو
قف دتاي لمع ضعب لمعت نل ،ددعتملا ثبلا قف ةي لمع 73 نم رثكأ ليمعلا بلطام دنع
MTU. 74SGs لخاد لازت ال يتلاو ،1494 مجح PIM Join ةلاسر ئشنيس 73 SGs .ددعتملا ثبلا
ةدراولا ةمزحلا طاقسإب 4900M مايق يف ببست امم ،1500 نم ربكأ PIM Join ةلاسر ئشنيس

ةلكشملا هذبه صاخلا حالصإلا ناك:

1. 4900m زارطلا ىلع ماع لكشب مجحلا ةريبك تاراطإل نيكم مت نم دكأت .

2. (MTU) لقنلل ىصقألا دحلا ءدحو مادختساب SVI و ةي داملا ءهجاو لا نم لك نيوكتب مق .
9216 غلبت

ةمچرتل هذه لوج

ةللأل تاي نقتلل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت
ملاعلاء انءمچم في نيمدختسمل معدى وتحم مي دقتل ةيرشبلاو
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئ. ةصاخل مهتغب
Cisco يلخت. فرتحم مچرتم اهمدقي يتلل ةيفارتحال ةمچرتلل عم لالحل وه
ىلإ أمئاد ةوچرلاب يصوت و تامچرتلل هذه ةقدنع اهتيلوئسم Cisco
Systems (رفوتم طبارلا) يلصلأل يزىلچنلإل دن تسمل