Risoluzione dei problemi comuni del multicast ASA

Sommario

Introduzione

Questo documento descrive il routing multicast su Adaptive Security Appliance (ASA) e i problemi comuni.

Informazioni sulle funzionalità

Nota: per un contenuto aggiornato sul routing multicast su ASA (Adaptive Security Appliance), FTD (Firepower Threat Defense) o FTD (Secure Firewall Threat Defense), fare riferimento a questi articoli:
Risoluzione dei problemi di base di Firepower Threat Defense per IGMP e multicast
Risoluzione dei problemi di Firepower Threat Defense e ASA Multicast PIM

Abbreviazioni/Acronimi

Acronimi	Spiegazione
FHR	Router del primo hop: hop connesso direttamente all'origine del traffico multicast.
LHR	Router dell'ultimo hop: hop collegato direttamente ai destinatari del traffico multicast.
RP	Rendezvous-Point
DR.	Router designato
SPT	Albero del percorso più breve
RPT	Struttura ad albero di Rendezvous-Point (RP), albero condiviso
RPF	Inoltro percorso inverso
PETROLIO	Elenco interfacce in uscita
MRIB	Base informazioni routing multicast

MFIB	Base informazioni inoltro multicast
ASM	Multicast Any-Source
BSR	Bootstrap Router
SSM	Multicast specifico dell'origine
FP	Percorso rapido
SP	Percorso lento
PC	Punto di controllo
PPS	Frequenza pacchetti al secondo

Il multicast sull'appliance ASA può essere configurato in una di due modalità:

- PIM in modalità sparse (multicast indipendente dal protocollo: RFC 4601)
- Modalità stub IGMP (Internet Group Management Protocol: RFC 2236)

La modalità sparse del PIM è la scelta preferita perché l'ASA comunica con i router adiacenti tramite un vero protocollo PIM (Multicast Routing Protocol). La modalità Stub IGMP era l'unica opzione di configurazione multicast prima del rilascio di ASA versione 7.0 e funzionava semplicemente inoltrando i report IGMP ricevuti dai client verso i router upstream.

Componenti del multicast

In generale, un'infrastruttura multicast è composta dai seguenti componenti:

Mittente => Host o dispositivo di rete da cui proviene il flusso multicast. Ad esempio, un server che invia flussi video e/o audio e dispositivi di rete che eseguono un protocollo di routing, quale EIGRP o OSPF.

Receiver => Host o dispositivo che riceve il flusso multicast. Questo termine viene utilizzato più di frequente per gli host attivamente interessati al traffico e utilizza IGMP per unirsi o uscire dal gruppo multicast in questione.

Router / ASA => Dispositivi di rete responsabili dell'elaborazione e dell'inoltro del traffico/flusso

multicast ad altri segmenti della rete quando necessario, dall'origine ai client.

Protocollo di routing multicast => Protocollo responsabile dell'inoltro dei pacchetti multicast. Il più comune è PIM (Protocol Independent Multicast), ma ce ne sono altri come MOSPF per esempio.

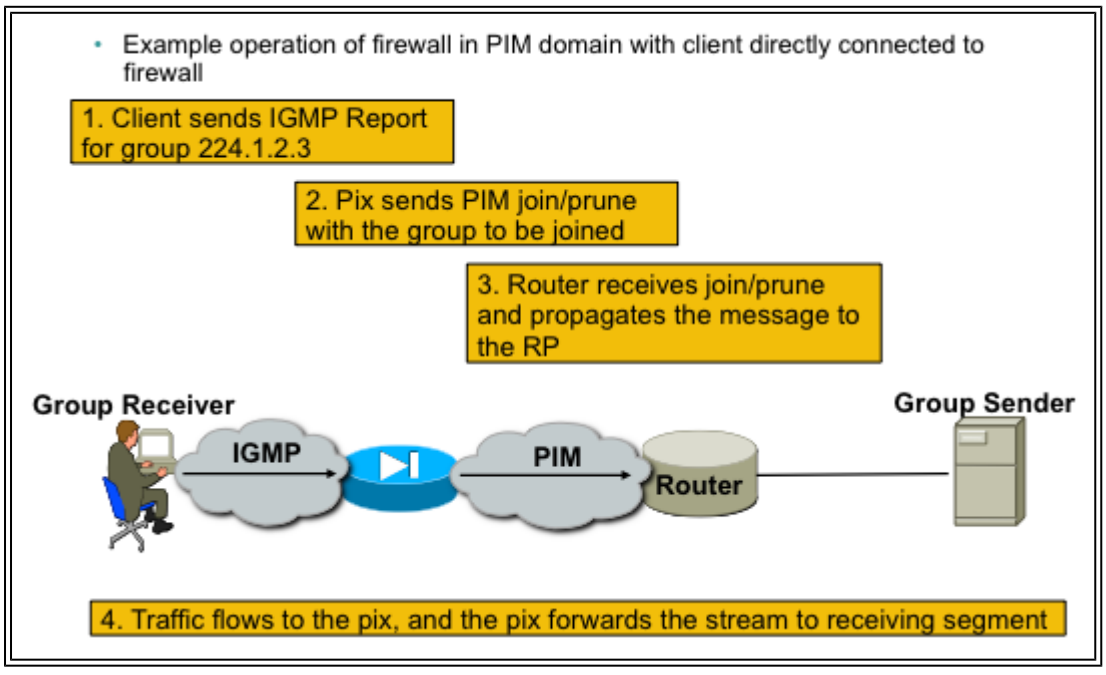
IGMP (Internet Group Management Protocol) => Processo utilizzato dai client per ricevere un flusso multicast da un determinato gruppo.

Funzionamento in modalità sparse PIM

- L'ASA supporta la modalità sparse PIM e la modalità bidirezionale PIM.
- I comandi PIM in modalità sparse e IGMP in modalità stub non devono essere configurati contemporaneamente.

- Con la modalità sparse del PIM tutto il traffico multicast inizialmente fluisce verso il punto di rendering (RP), quindi viene inoltrato verso i ricevitori. Dopo qualche tempo il flusso multicast passa direttamente dalla sorgente ai ricevitori (e bypassa l'RP).

In questa immagine viene illustrata una distribuzione comune in cui l'ASA ha client multicast su un'interfaccia e vicini PIM su un'altra interfaccia:



Configurazione di esempio in modalità sparsa PIM

1. Abilitare il routing multicast (modalità di configurazione globale).

<#root>

```
ASA(config)#
```

multicast-routing

2. Definire l'indirizzo del punto di rendering PIM.

<#root>

```
ASA(config)#
```

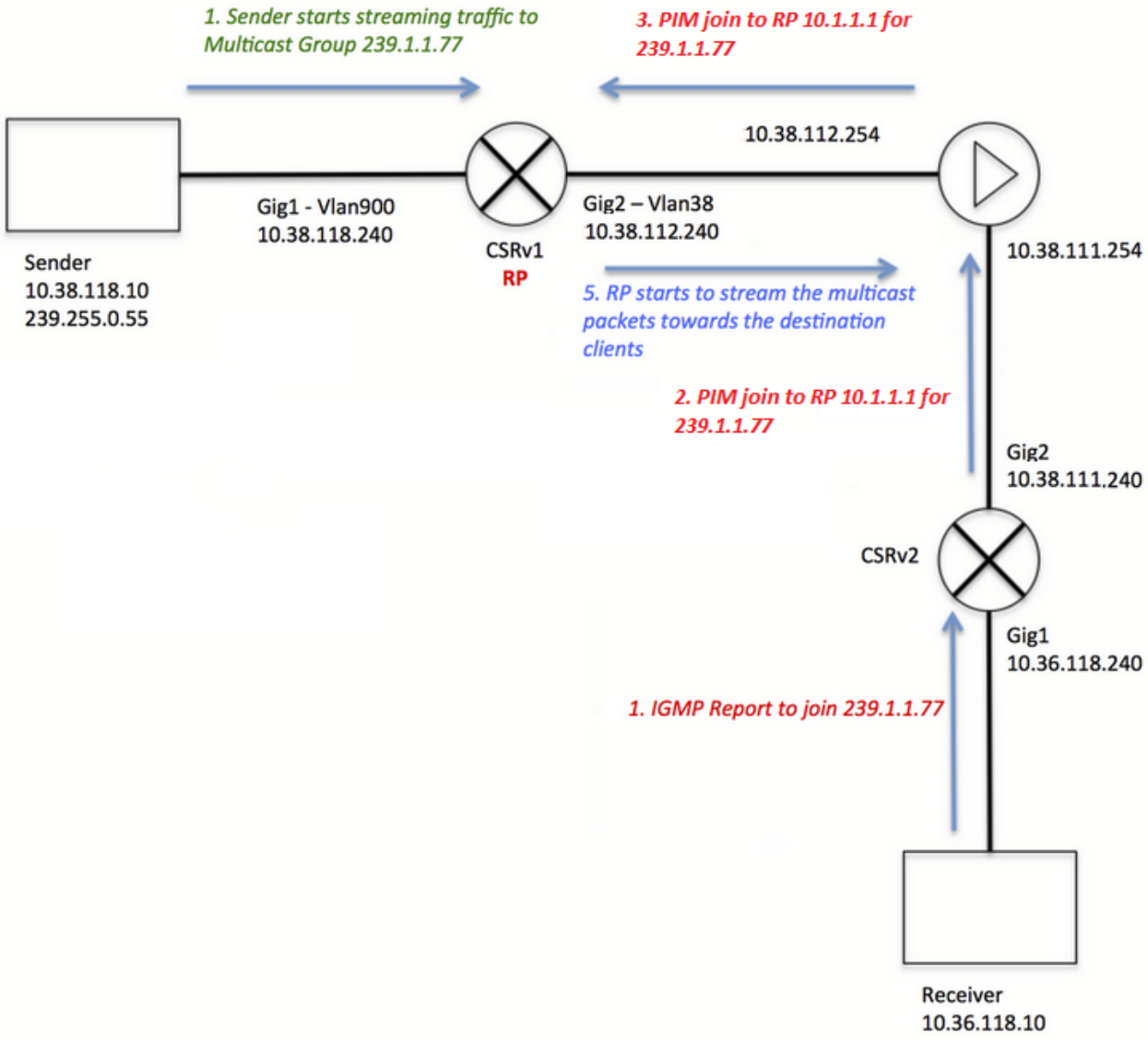
pim rp-address 172.18.123.3

3. Consentire l'ingresso dei pacchetti multicast sull'interfaccia appropriata (necessario solo se i pacchetti multicast in entrata sono bloccati dai criteri di sicurezza dell'ASA).

<#root>

access-list 105 extended permit ip any host 224.1.2.3
access-group 105 in interface outside

Esempio di modalità sparsa PIM:



Si noti che la registrazione IGMP del client (passaggi in rosso) e il flusso ricevuto dal server (passaggi in verde) sono stati colorati in modo diverso, e questo è stato fatto in questo modo per dimostrare che entrambi i processi possono verificarsi in modo indipendente.

Fasi della registrazione del client (fasi rosse):

1. Il client invia un report IGMP per il gruppo 239.1.1.77

2. Il router invia un messaggio di unione PIM all'RP statica configurata (10.1.1.1) per il gruppo 239.1.1.77.

3. L'ASA invia all'RP un messaggio di unione PIM per il gruppo 239.1.1.77.

ASA visualizza la voce PIM *,G sull'output del comando show mroute:

```
<#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
```

Tuttavia, poiché il server di origine non ha avviato alcun flusso, l'output "show mfib" sull'appliance ASA non visualizza i pacchetti ricevuti:

<#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
```

Prima che il server inizi a inviare traffico al gruppo multicast, nell'RP viene visualizzata solo una voce "*.G" senza alcuna interfaccia in ingresso nell'elenco, ad esempio:

<#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
```

Quando il server inizia a inviare lo streaming al gruppo multicast, l'RP crea una voce "S,G" e inserisce l'interfaccia rivolta al mittente nell'elenco delle interfacce in arrivo e inizia a inviare il traffico a valle all'ASA:

<#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
```

Utilizzare i seguenti comandi per le verifiche:

- show mroute visualizza una voce "S,G"

- show mfib, comando visualizza i contatori dei pacchetti in avanti

- il comando show conn visualizza la connessione correlata all'ip del gruppo multicast

<#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 -
```

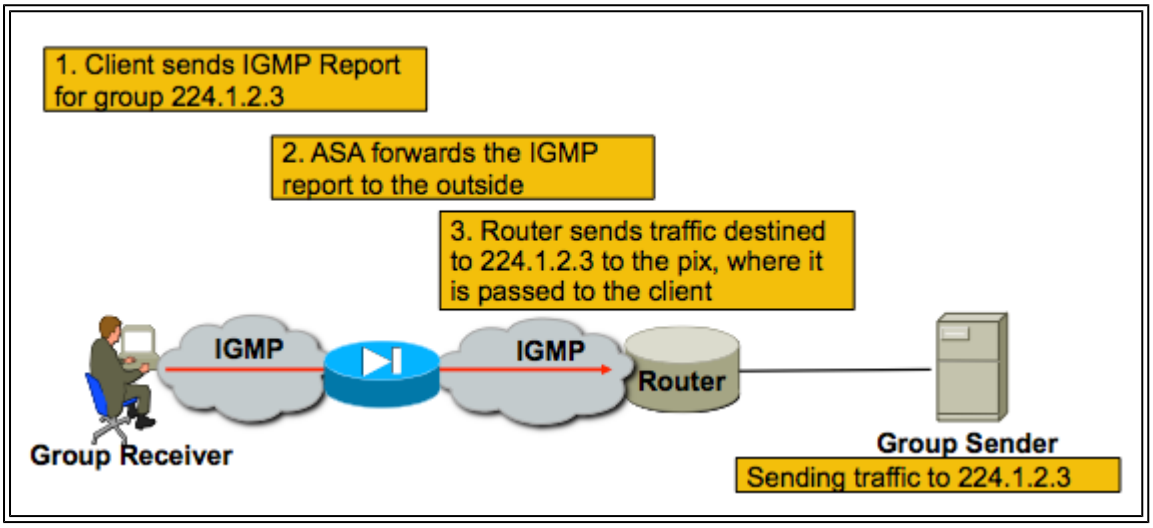
Nota: dopo che il client ha chiuso l'applicazione client multicast, l'host invia un messaggio di query IGMP.

Nel caso in cui questo sia l'unico host conosciuto dal router come il client desideri ricevere il flusso, il router invia un messaggio IGMP Prune all'RP.

Funzionamento in modalità stub IGMP

- In modalità stub IGMP, l'ASA agisce come client multicast e genera o inoltra report IGMP (noti anche come "join" IGMP) verso router adiacenti, per attivare la ricezione del traffico multicast
- I router inviano periodicamente query agli host per verificare se un nodo della rete desidera continuare a ricevere il traffico multicast.
- La modalità stub IGMP non è consigliata perché la modalità sparse PIM offre molti vantaggi rispetto alla modalità stub (con flussi di traffico multicast più efficienti, possibilità di partecipare a PIM, ecc.).

L'immagine mostra il funzionamento di base di un'appliance ASA configurata per la modalità stub IGMP:



Configurazione modalità stub IGMP

1. Abilitare il routing multicast (modalità di configurazione globale).

<#root>

```
ASA(config)#
```

multicast-routing

2. Configurare il comando igmp forward-interface sull'interfaccia su cui il firewall riceve i rapporti igmp. Inoltra i pacchetti dall'interfaccia verso l'origine del flusso. In questo esempio, i ricevitori multicast sono collegati direttamente all'interfaccia interna e la sorgente multicast è esterna.

<#root>

```
!
interface Ethernet0
 nameif outside
 security-level 0
```

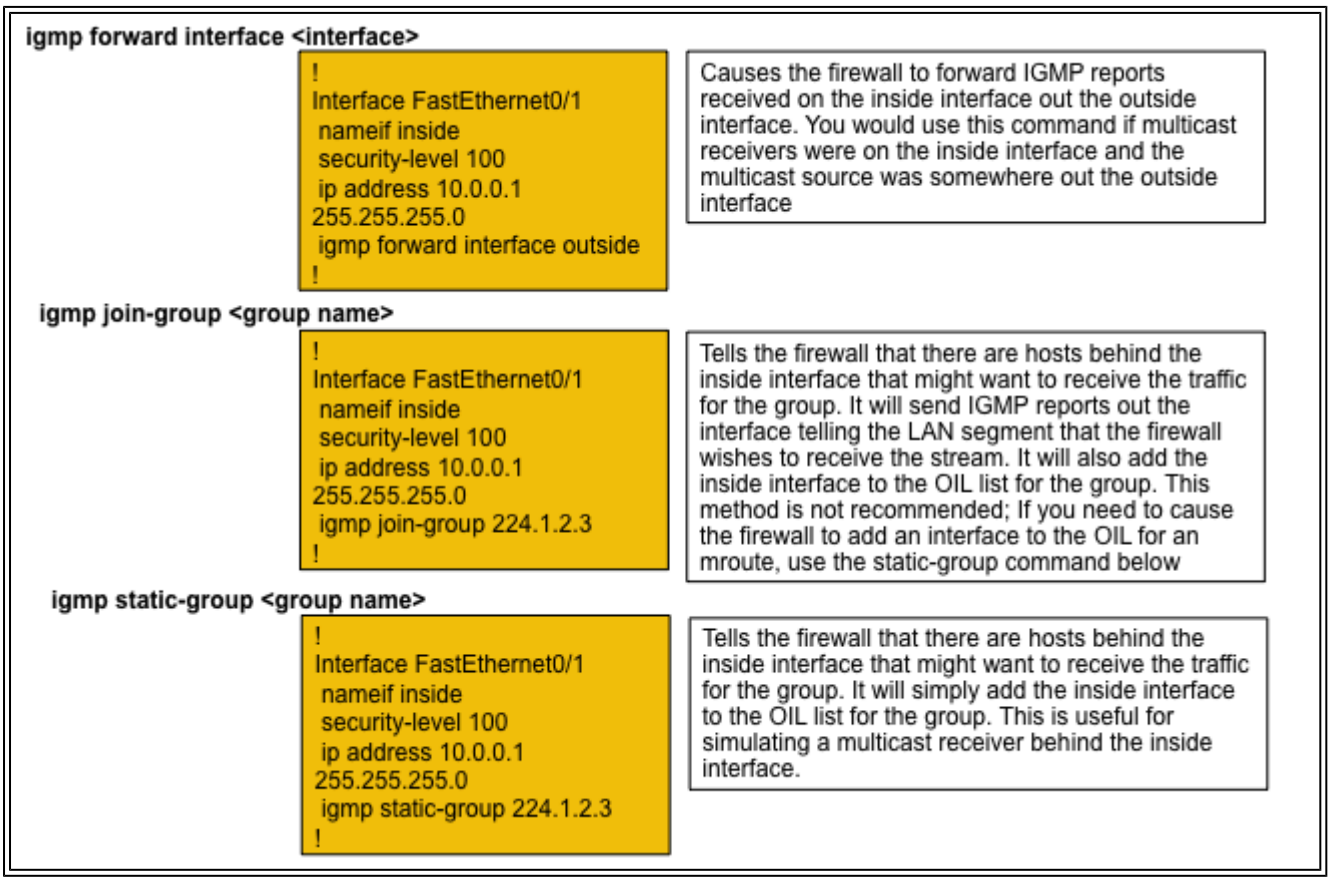
```
 ip address 172.16.1.1 255.255.255.0
 no pim
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.0.0.1 255.255.255.0
 no pim


igmp forward interface outside

!
```

3. Consentire l'ingresso dei pacchetti multicast sull'interfaccia appropriata (solo se i criteri di sicurezza dell'ASA negano il traffico multicast in entrata).

<#root>

```
ASA(config)#

access-list 105 extended permit ip any host 224.1.2.3

ASA(config)#

access-group 105 in interface outside
```

Spesso i diversi comandi dell'interfaccia igmp in modalità secondaria sono confusi e questo diagramma descrive quando utilizzarli:



Bidir PIM

Nel PIM bidirezionale non è presente alcun albero condiviso (SPT). Questo significa tre cose:

1. Il primo router hop (collegato al mittente) non invia i pacchetti del registro PIM al punto di ripristino.

2. L'RP non invia messaggi di JOIN PIM per unirsi all'albero di origine.

3. I router nel percorso verso il destinatario inviano messaggi di join PIM all'RP per unirsi all'RPT.

Ciò significa che l'ASA non genera un (S,G) in quanto i dispositivi non si uniscono all'SPT. Tutto il traffico multicast passa attraverso il RP. L'ASA inoltra tutto il traffico multicast finché è presente un (*,G). Se non c'è (*,G), l'ASA non ha mai ricevuto un pacchetto di unione PIM. In questo caso, l'ASA non deve inoltrare pacchetti multicast.

Configurazione PIM Bidir

1. Abilitare il routing multicast (modalità di configurazione globale).

```
<#root>

ASA(config)#

 multicast-routing
```

2. Definire l'indirizzo del punto di rendering PIM.

```
<#root>

ASA(config)#

pim rp-address 172.18.123.3 bidir
```

3. Consentire l'ingresso dei pacchetti multicast sull'interfaccia appropriata (necessario solo se i pacchetti multicast in entrata sono bloccati dai criteri di sicurezza dell'ASA).

```
<#root>

access-list 105 extended permit ip any host 224.1.2.3
access-group 105 in interface outside
```

Metodologia di risoluzione dei problemi

Informazioni Da Raccogliere Per La Risoluzione Dei Problemi Relativi Al Multicast

Per comprendere e diagnosticare completamente un problema di inoltro multicast sull'appliance ASA, è necessario fornire alcune o tutte le informazioni seguenti:

· Una descrizione della topologia di rete, la posizione dei mittenti multicast, dei riceventi e del punto di rendering.
· L'indirizzo IP del gruppo specifico, nonché le porte e i protocolli utilizzati.
· Syslog generati dall'ASA quando il flusso multicast ha un problema.
· Output specifico del comando show dall'interfaccia della riga di comando ASA:

<#root>

```
show mroute
show mfib
show pim neighbor
show route
show tech-support
```

· Il pacchetto viene acquisito per mostrare se i dati multicast arrivano all'appliance ASA e se i pacchetti vengono inoltrati tramite l'appliance ASA (prendere nota del valore TTL (Time to Live) IP del pacchetto. Questa condizione può essere rilevata con il comando 'show capture x detail')
· Acquisizioni di pacchetti per pacchetti IGMP e/o PIM. Esempio:

<#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
```

· Informazioni da dispositivi multicast adiacenti (router) quali "show mroute" e "show mfib".
· Il pacchetto acquisisce e/o mostra comandi per determinare se l'ASA rifiuta i pacchetti multicast. Il comando "show asp drop" può essere usato per determinare se l'ASA scarta i pacchetti. Inoltre, le acquisizioni dei pacchetti di tipo 'asp-drop' possono essere usate per acquisire tutti i pacchetti scartati dall'ASA, quindi esaminate per verificare se i pacchetti multicast sono presenti nell'acquisizione dei pacchetti scartati.

Output utile del comando Show

L'output del comando show mroute visualizza i vari gruppi e le informazioni di inoltro ed è molto simile al comando show mroute di IOS. Il comando show mfib visualizza lo stato di inoltro dei vari gruppi multicast. È particolarmente importante osservare il contatore del pacchetto di inoltro, nonché Altro (che indica le cadute):

<#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#
```

Il comando clear mfib counters può essere usato per cancellare i contatori, il che è molto utile durante il test:

<#root>

```
ciscoasa#
```

clear mfib counters

Acquisizioni pacchetti

L'utilità di acquisizione pacchetti integrata è molto utile per risolvere i problemi relativi al multicast. Nell'esempio, vengono acquisiti tutti i pacchetti in entrata sull'interfaccia DMZ destinati alla versione 239.17.17.17:

<#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
....
```

L'output del comando show capture x detail visualizza il valore TTL dei pacchetti, che è abbastanza utile. In questo output, il valore TTL del pacchetto è 1 (e l'ASA trasmette il pacchetto poiché non diminuisce il valore TTL dei pacchetti IP per impostazione predefinita), ma un router downstream scarta i pacchetti:

```
<#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 P0 10.4.2.95.1806 > 239.255.2.195.5000:  [udp sum ok] udp 1316 (DF) [ttl 1] (id
```

Le acquisizioni dei pacchetti sono utili anche per acquisire il traffico PIM e IGMP. Questa acquisizione mostra che l'interfaccia interna ha ricevuto un pacchetto IGMP (protocollo IP 2) proveniente da 10.0.0.2:

```
<#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 P0 10.0.0.2 > 224.1.2.3:  ip-proto-2, length 8
ciscoasa#
```

Il valore TTL dei pacchetti può essere visualizzato con il comando "show capture x detail".

Qui è possibile vedere le clip acquisite da ASP che mostrano i pacchetti multicast scartati e il motivo per cui sono stati scartati (punt-rate-limit):

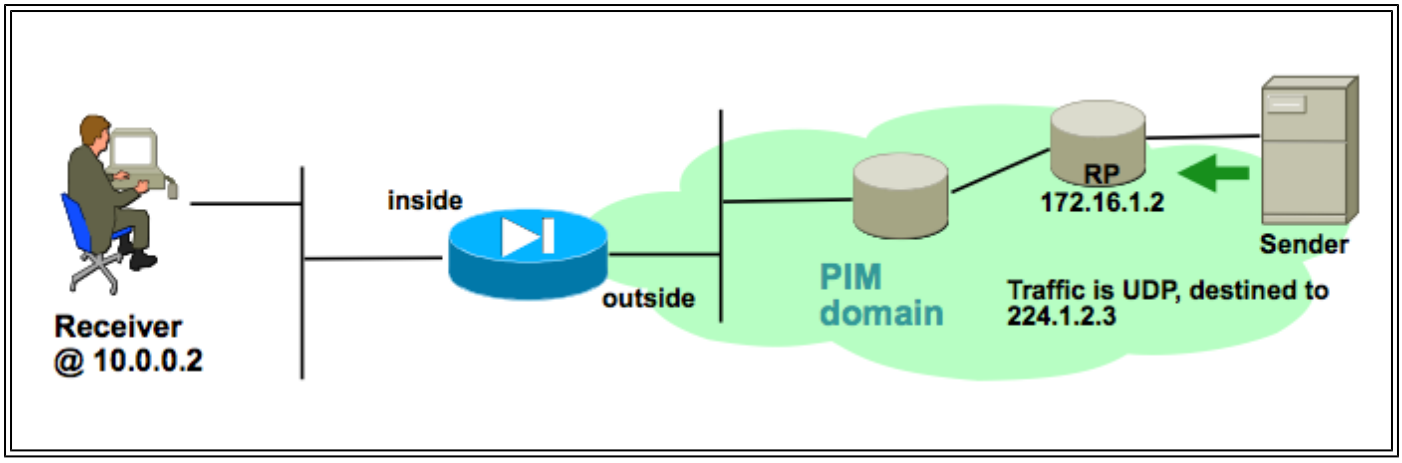
```
<#root>

ASA#

show cap capasp det

 12: 14:37:26.538332 c062.6baf.8dc3 0100.5e7f.02c3 0x8100 Length: 1362
      802.1Q vlan#1007 P0 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 P0 10.76.4.95.1806 > 239.255.2.195.5000:  [udp sum ok] udp 1316 (DF) [ttl 1] (id
```

Esempio di distribuzione multicast in modalità sparse di ASA PIM

Nei diagrammi viene mostrata l'interazione dell'ASA con i dispositivi adiacenti in modalità sparse PIM.

Informazioni sulla topologia di rete

Determina esattamente la posizione dei mittenti e dei destinatari del flusso multicast specifico. Determinare inoltre l'indirizzo IP del gruppo multicast e la posizione del punto di rendering.



In questo caso, i dati possono essere ricevuti sull'interfaccia esterna dell'appliance ASA e inoltrati al ricevitore multicast sull'interfaccia interna. Poiché il ricevitore si trova nella stessa subnet IP

dell'interfaccia interna dell'ASA, quando il client richiede di ricevere il flusso, deve essere visualizzato un report IGMP ricevuto sull'interfaccia interna. L'indirizzo IP del mittente è 192.168.1.50.

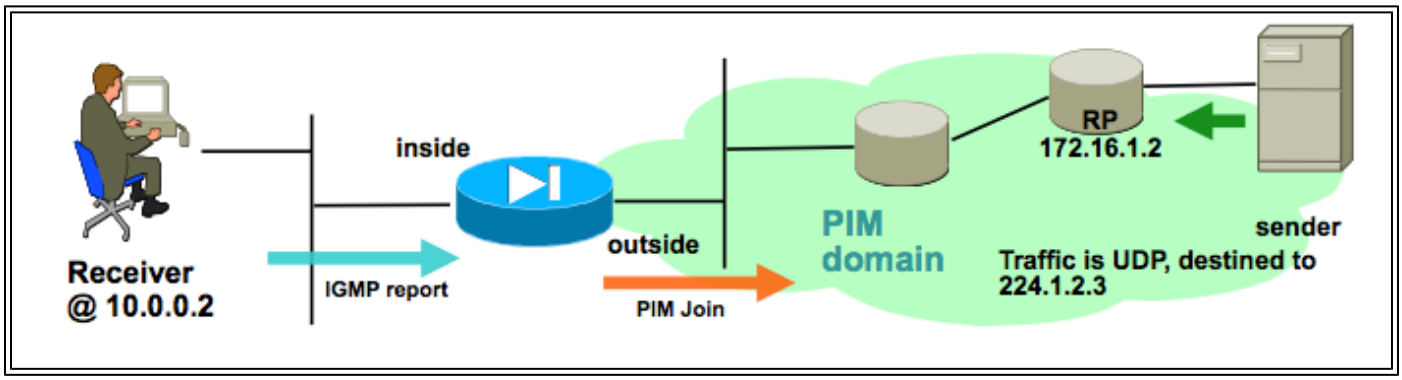
Verificare che l'appliance ASA riceva il report IGMP dal destinatario

In questo esempio, il report IGMP viene generato dal destinatario ed elaborato dall'ASA.

Le acquisizioni dei pacchetti e l'output del comando debug igmp possono essere usati per verificare che l'appliance ASA abbia ricevuto ed elaborato correttamente il messaggio IGMP.

Verificare che l'ASA invii un messaggio di join PIM verso il punto di rendering

L'ASA interpreta il report IGMP e genera un messaggio di join PIM, quindi lo invia all'interfaccia verso l'RP.

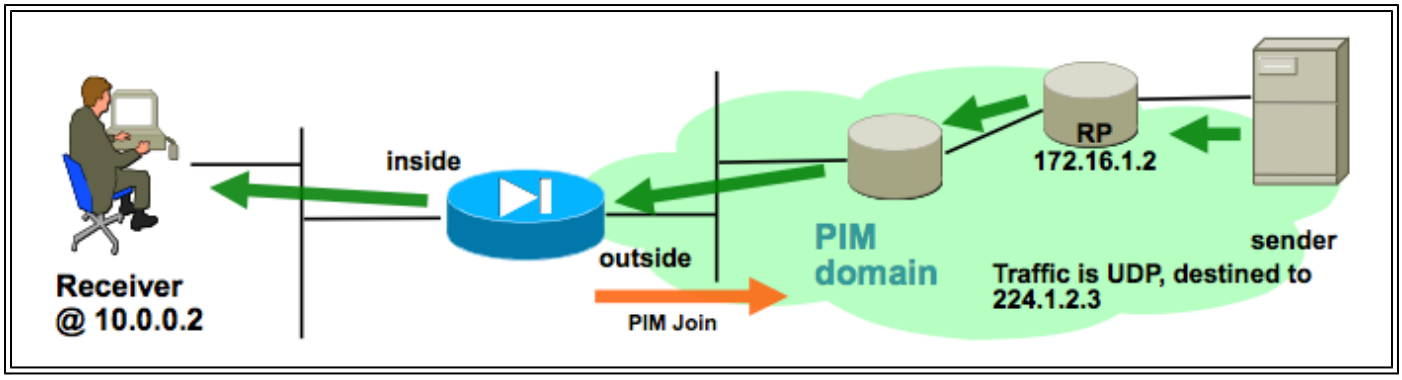


Questo output viene generato dal gruppo pim di debug 24.1.2.3 e mostra che l'ASA ha inviato correttamente il messaggio di join PIM. Il mittente del flusso multicast è 192.168.1.50.

```
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
```

Verificare che l'appliance ASA riceva e inoltri il flusso multicast

L'ASA inizia a ricevere il traffico multicast sull'interfaccia esterna (illustrata dalle frecce verdi) e a inoltrarlo ai ricevitori all'interno.



I comandi show mroute e show mfib e le acquisizioni dei pacchetti possono essere usati per verificare che l'ASA riceva e inoltri i pacchetti multicast.

Nella tabella delle connessioni viene creata una connessione per rappresentare il flusso multicast:

<#root>

```
ciscoasa#
```

show conn

```
59 in use, 29089 most used
...
UDP outside:192.168.1.50/52075 inside:224.1.2.3/1234 flags -
...
```

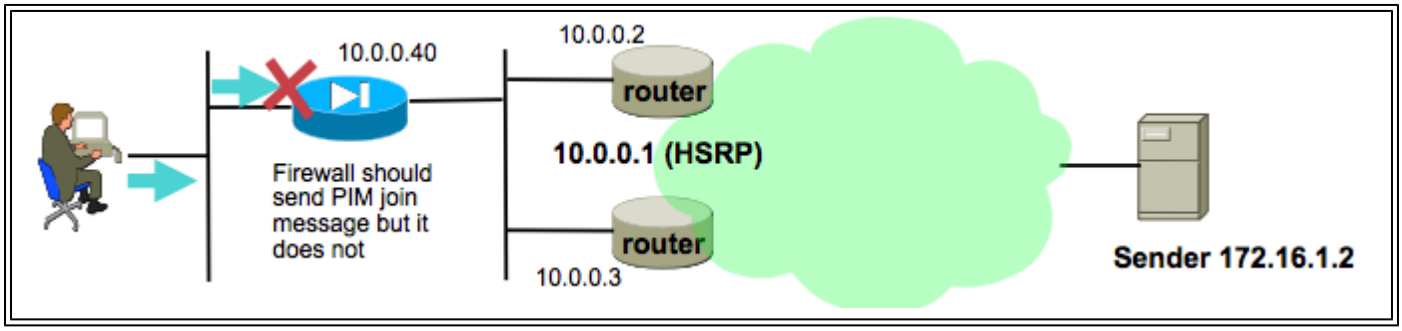
Analisi dei dati

Problemi comuni

Questa sezione fornisce una serie di problemi correlati al multicast ASA reali

L'ASA non riesce a inviare messaggi PIM verso i router a monte a causa dell'HSRP

Quando si verifica questo problema, l'ASA non riesce a inviare alcun messaggio PIM all'esterno di un'interfaccia. Il diagramma mostra che l'ASA non può inviare messaggi PIM al mittente, ma lo stesso problema si verifica quando l'ASA deve inviare un messaggio PIM all'RP.



L'output del comando debug pim mostra che l'ASA non può inviare il messaggio PIM al router

upstream dell'hop successivo:

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

Questo problema non riguarda solo l'appliance ASA, ma anche i router. Il problema viene attivato dalla combinazione della configurazione della tabella di routing e della configurazione HSRP utilizzata dai vicini PIM.

La tabella di routing punta all'IP 10.0.0.1 dell'HSRP come dispositivo dell'hop successivo:

<#root>

```
ciscoasa#
```

show run route

```
route outside 0.0.0.0 0.0.0.0 10.0.0.1 1
```

Tuttavia, tra gli indirizzi IP dell'interfaccia fisica dei router e non tra l'indirizzo IP dell'HSRP si forma la relazione PIM adiacente:

<#root>

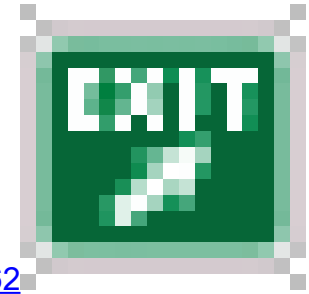
```
ciscoasa#
```

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)
```

Per ulteriori informazioni, vedere "Perché la modalità sparse del PIM non funziona con un percorso statico a un indirizzo HSRP?".

Ecco un estratto del documento:



Perché il router non invia il messaggio di aggiunta/eliminazione? La RFC 2362 afferma che "un router invia un messaggio di join/eliminazione periodico a ogni singolo router adiacente RPF associato a ciascuna voce (S,G), (*,G) e (*,*,RP). I messaggi di

unione/eliminazione vengono inviati solo se il router adiacente RPF è un router adiacente PIM."

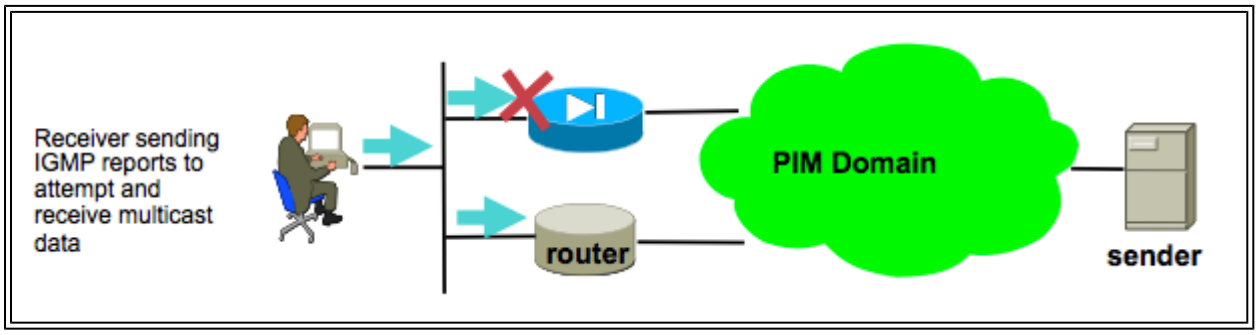
Per risolvere il problema, aggiungere una voce relativa al percorso statico sull'appliance ASA per il traffico in questione. Accertarsi che punti a uno dei due indirizzi IP dell'interfaccia del router (10.0.0.2 o 10.0.0.3). In questo caso, il comando permette all'ASA di inviare messaggi PIM diretti al mittente multicast all'indirizzo 172.16.1.2:

```
<#root>

ciscoasa(config)#

mroute 172.16.1.2 255.255.255.255 10.0.0.3
```

Al termine, la tabella di routing multicast sostituisce la tabella di routing unicast dell'ASA e l'ASA invia i messaggi PIM direttamente alla versione adiacente 10.0.0.3.

L'ASA Ignora i report IGMP perché non è il router designato sul segmento LAN

Per questo problema, l'ASA riceve un report IGMP da un ricevitore multicast connesso direttamente, ma lo ignora. Non viene generato alcun output di debug e il pacchetto viene semplicemente scartato e la ricezione del flusso non riesce.



Per questo problema, l'ASA ignora il pacchetto perché non è il router PIM scelto sul segmento LAN in cui risiedono i client.

Questo output dell'ASA CLI mostra che un dispositivo diverso è il router designato (indicato da "DR") sulla rete dell'interfaccia interna:

```
<#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)
```

per impostazione predefinita, quando si aggiunge il comando multicast-routing alla configurazione, il protocollo PIM è abilitato su tutte le interfacce ASA. Se sull'interfaccia interna dell'ASA (dove risiedono i client) sono presenti altri router PIM adiacenti (altri router o appliance ASA) e uno di questi router adiacenti è stato scelto a causa del DR per il segmento in questione, gli altri router non DR eliminano i report IGMP. La soluzione è disabilitare il protocollo PIM sull'interfaccia (con il comando no pim sull'interfaccia interessata) o fare in modo che l'ASA venga usata come DR per il segmento tramite il comando pim dr-priority dell'interfaccia.

I report IGMP vengono rifiutati dal firewall quando viene superato il limite dell'interfaccia IGMP

Per impostazione predefinita, l'ASA supporta 500 join attivi correnti (report) tracciati su un'interfaccia. Questo è il valore massimo configurabile. Se i client richiedono un numero elevato di flussi multicast da un'interfaccia, è possibile rilevare un massimo di 500 join attivi e l'ASA potrebbe ignorare altri report IGMP in arrivo dai ricevitori multicast.

Per verificare se questa è la causa di un errore multicast, usare il comando 'show igmp interface interface name' e cercare le informazioni 'IGMP limit' per l'interfaccia.

<#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
```

L'ASA non riesce ad inoltrare il traffico multicast nell'intervallo 232.x.x.x/8

Questo intervallo di indirizzi deve essere usato con il multicast (SSM) specifico dell'origine che attualmente non è supportato dall'ASA.

L'output del comando debug igmp visualizza questo errore:

```
IGMP: Exclude report on inside ignored for SSM group 232.179.89.253
```

L'ASA Rifiuta I Pacchetti Multicast A Causa Del Controllo Dell'Inoltro Inverso Del Percorso

In questo caso, l'ASA riceve il traffico multicast su un'interfaccia, ma non viene inoltrata al destinatario. I pacchetti vengono scartati dall'ASA perché non superano il controllo di sicurezza RPF (Reverse Path Forwarding). L'RPF è abilitato su tutte le interfacce per il traffico multicast e non può essere disabilitato (per i pacchetti unicast il controllo non è abilitato per impostazione predefinita ed è abilitato con il comando ip verify-path interface).

A causa del controllo RPF, quando il traffico multicast viene ricevuto su un'interfaccia, l'ASA controlla che disponga di una route verso l'origine del traffico multicast (controlla la tabella di routing unicast e multicast) su quell'interfaccia. Se non ha un percorso verso il mittente, scarta il pacchetto. Queste gocce possono essere viste come un contatore nell'output di 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
```

Un'opzione consiste nell'aggiungere una route per il mittente del traffico. Nell'esempio, il comando mroute viene usato per verificare che RPF abbia generato traffico multicast proveniente da 172.16.1.2 ricevuto sull'interfaccia esterna:

```
<#root>

ciscoasa(config)#

mroute 172.16.1.2 255.255.255.255 outside
```

L'ASA non genera l'aggiunta PIM quando il PIM viene trasferito alla struttura origine

Inizialmente, i pacchetti multicast in modalità sparse del PIM passano dal mittente multicast all'RP,

quindi dall'RP al destinatario tramite una struttura multicast condivisa. Tuttavia, quando la velocità in bit aggregata raggiunge una determinata soglia, il router più vicino al ricevitore multicast cerca di ricevere il traffico lungo la struttura specifica dell'origine. Questo router genera un nuovo join PIM per il gruppo e lo invia al mittente del flusso multicast (e non verso l'RP, come prima).

Il mittente del traffico multicast può risiedere su un'interfaccia ASA diversa da quella dell'RP. Quando l'ASA riceve il join PIM per passare all'albero specifico dell'origine, deve avere una route all'indirizzo IP del mittente. Se la route non viene trovata, il pacchetto di unione PIM viene scartato e questo messaggio viene visualizzato nell'output del pim di debug

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

Per risolvere questo problema, aggiungere una voce di route statica per il mittente del flusso che indichi l'interfaccia ASA da cui risiede il mittente.

L'ASA Rifiuta I Pacchetti Multicast A Causa Del Superamento Del Valore TTL (Time To Live)

In questo caso, il traffico multicast non riesce perché il valore TTL dei pacchetti è troppo basso. In questo modo, l'ASA, o un altro dispositivo della rete, li scarta.

Spesso i pacchetti multicast hanno un valore TTL IP impostato molto basso dall'applicazione che li ha inviati. A volte questa operazione viene eseguita per impostazione predefinita per evitare che il traffico multicast passi troppo lontano attraverso la rete. Per impostazione predefinita, ad esempio, la scheda Video LAN Per impostazione predefinita, l'applicazione client (un comune trasmettitore e strumento di prova multicast) imposta il valore TTL nel pacchetto IP su 1.

L'ASA Sfrutta Un Utilizzo Elevato Della CPU E Perde I Pacchetti A Causa Di Una Topologia Multicast Specifica

L'ASA può sperimentare una CPU elevata e il flusso multicast può sperimentare perdite di pacchetti se tutte le seguenti affermazioni sulla topologia multicast sono vere:

1. L'ASA svolge il ruolo di RP.
2. L'ASA è il primo ricevitore hop del flusso multicast. Ciò significa che il mittente multicast si trova nella stessa subnet IP di un'interfaccia ASA.
3. L'ASA è l'ultimo router hop del flusso multicast. Ciò significa che un ricevitore multicast si trova nella stessa subnet IP di un'interfaccia ASA.

Se si riscontrano tutti i sintomi menzionati, A causa di una limitazione della progettazione, l'ASA è costretta a elaborare lo switch per il traffico multicast. Il risultato sono flussi multicast ad alta velocità di trasmissione dei dati che causano la perdita dei pacchetti. Il contatore show asp drop che aumenta quando questi pacchetti vengono scartati è punt-rate-limit.

Per stabilire se un'appliance ASA ha questo problema, attenersi alla seguente procedura:

Passaggio 1: verificare se l'ASA è l'RP:

<#root>

show run pim
show pim tunnel

Passaggio 2: verificare che l'ASA sia l'ultimo router hop:

<#root>

show igmp group

<mcast_group_IP>

Passaggio 3: verificare che l'ASA sia il router del primo hop:

<#root>

show mroute

<mcast_group_IP>

Per risolvere il problema, è possibile effettuare le seguenti operazioni:

- Modificare la topologia in modo che l'ASA non sia l'RP. In alternativa, verificare che il mittente o il destinatario non siano collegati direttamente all'appliance ASA

- Anziché PIM, utilizzare la modalità stub IGMP per l'inoltro multicast.

L'ASA Elimina I Primi Pacchetti Quando Si Avvia Un Flusso Multicast

Quando i primi pacchetti di un flusso multicast arrivano all'appliance ASA, questa deve creare la connessione multicast e la voce del percorso associata per inoltrare i pacchetti. Mentre la voce è in fase di creazione, alcuni pacchetti multicast possono essere scartati fino a quando il routing e le connessioni non sono stati stabiliti (generalmente questa operazione richiede meno di un secondo). Una volta completata la configurazione del flusso multicast, i pacchetti non hanno più limiti di velocità.

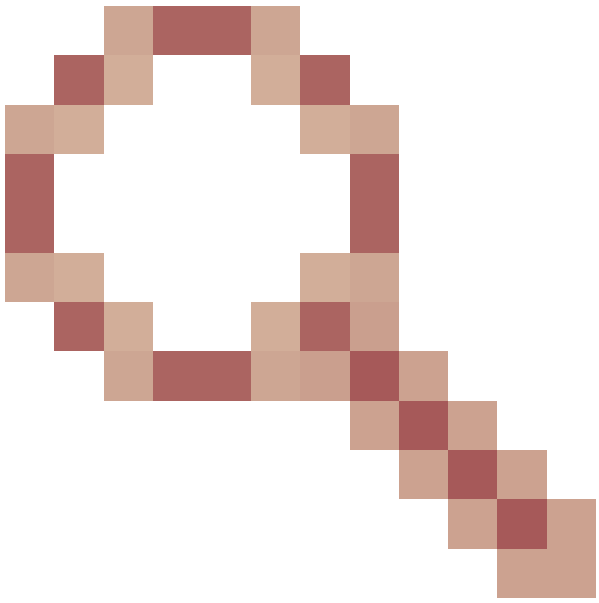
I pacchetti scartati per questo motivo hanno il motivo di rilascio ASP per il superamento del limite di velocità Punt (punt-rate-limit). Questo è l'output di 'show capture asp' (dove asp è un'operazione di drop capture ASP configurata sull'appliance ASA per acquisire i pacchetti scartati). È possibile visualizzare i pacchetti multicast scartati per questo motivo:

<#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
```

Un Ricevitore Multicast In Disconnessione Interrompe La Ricezione Di Gruppi Multicast Su Altre Interfacce

Questo problema si verifica solo per le appliance ASA in modalità stub IGMP. Le appliance ASA che partecipano al routing multicast PIM non sono interessate.



Il problema è identificato dall'ID bug Cisco CSCeg48235
Il comando IGMP Leave su un'interfaccia interrompe il traffico multicast su altre interfacce.

Questa è la nota sulla versione del bug, che spiega il problema:

```
Symptom:
When a PIX or ASA firewall is configured for IGMP stub mode multicast reception and traffic from a mult

The problem is triggered when the firewall forwards the IGMP leave for the group towards the upstream d

Conditions:
The PIX or ASA must be configured for IGMP stub mode multicast. IGMP stub mode is a legacy multicast fo

Workarounds:
1) Use PIM multicast routing instead of IGMP stub mode.
2) Decrease multicast IGMP query timers so that the receivers are queried more frequently, so their IGM
```

L'ASA rifiuta i pacchetti multicast a causa dei criteri di sicurezza dell'elenco degli

accessi in uscita

Con questo problema specifico, l'ASA scarta i pacchetti multicast (in base ai criteri di sicurezza configurati). Tuttavia, è difficile per l'amministratore di rete identificare il motivo per cui il pacchetto viene scartato. In questo caso, l'ASA scarta i pacchetti a causa dell'elenco degli accessi in uscita configurato per un'interfaccia. Per ovviare al problema, è necessario autorizzare il flusso multicast nell'elenco degli accessi in uscita.

In questo caso, i pacchetti multicast vengono scartati con il contatore di rilascio ASP "FP no mcast output intrf (no-mcast-intrf)".

L'ASA scarta continuamente alcuni pacchetti (ma non tutti) in un flusso multicast a causa della limitazione della velocità del punto di controllo

Il traffico è più probabile che la velocità sia limitata dal punto di controllo a causa del limite della velocità di punt. Osservare l'output del rilascio dell'asp e le acquisizioni per confermare:

```
<#root>

ASA#

show asp drop


Frame drop:
  Punt rate limit exceeded (punt-rate-limit)                                1492520




ASA#  show cap capasp det
 12: 14:37:26.538332 c062.6baf.8dc3 0100.5e7f.02c3 0x8100 Length: 1362
      802.1Q vlan#1007 P0 10.76.4.95.1806 > 239.255.2.195.5000:  [udp sum ok] udp 1316 (DF) [ttl 1] (id
```

La voce mfib mostra che tutto il traffico è commutato in base al processo:

```
<#root>

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
```

Nella tabella di routing multicast viene visualizzato un asterisco (*,G) ma no (S,G).

<#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
```

Il problema in questo caso è che il valore TTL dei pacchetti di dati multicast che arrivano all'appliance ASA è 1. L'ASA inoltra i pacchetti al dispositivo downstream (in quanto non riduce il valore TTL), ma il router downstream scarta i pacchetti. Di conseguenza, il router a valle non invia un join PIM (S,G) (un join specifico dell'origine) all'appliance ASA verso il mittente. L'ASA non crea una voce (S,G) finché non riceve questo join PIM. Poiché (S,G) non è generato, tutto il traffico multicast viene commutato in base al processo e ciò determina un limite di velocità.

Per risolvere questo problema, verificare che il valore TTL dei pacchetti non sia 1, in modo da consentire al dispositivo a valle di inviare il join specifico all'origine verso il mittente; in questo modo, l'ASA installa un percorso specifico all'origine nella tabella e tutti i pacchetti vengono commutati rapidamente (anziché commutati) e il traffico deve passare attraverso l'ASA senza alcun problema.

Il flusso multicast è stato interrotto a causa di un messaggio PIM ASSERT

Se due dispositivi di rete inoltrano gli stessi pacchetti multicast sulla stessa subnet, uno di essi deve interrompere l'inoltro dei pacchetti (in quanto la duplicazione del flusso costituisce uno spreco). Se i router che eseguono PIM rilevano di ricevere gli stessi pacchetti generati anche sulla stessa interfaccia, generano messaggi ASSERT sulla LAN per selezionare il dispositivo di rete che arresta l'inoltro del flusso.

Per ulteriori informazioni su questo messaggio, consultare una sezione della RFC 4601 relativa al processo ASSERT.

I debug mostrano che l'ASA riceve un report IGMP per il gruppo 239.1.1.227, ma ignora il report a causa del messaggio di asserzione che riceve da un router adiacente:

```
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)
```

Questo problema è stato osservato in una rete di produzione in cui due siti sono stati involontariamente collegati al layer 2, in modo che la LAN su cui si trovavano i ricevitori multicast disponesse di due dispositivi che inoltravano il traffico multicast verso di essi. A causa di un altro problema di rete, l'ASA e un altro dispositivo non sono stati in grado di rilevarsi a vicenda tramite gli helper PIM e quindi entrambi hanno assunto il ruolo di router designato per la LAN. Il traffico multicast è rimasto in funzione per un certo periodo di tempo, quindi non è riuscito quando i dispositivi hanno inviato i messaggi ASSERT. Per risolvere il problema, la connessione errata che collegava i dispositivi al layer 2 è stata disabilitata e quindi il problema è stato risolto.

L'ASA invia l'aggiunta PIM, ma il router adiacente non la elabora a causa delle dimensioni del pacchetto superiori all'MTU

Questo è stato osservato in 629575899. L'ASA era stata configurata per i frame jumbo, mentre la 4900 non lo era. Quando il client ha richiesto più di 73 flussi multicast, alcuni flussi multicast non funzionerebbero. 73 SG creavano un messaggio di unione PIM di dimensioni 1494, che era ancora all'interno dell'MTU. 74SG creavano un messaggio di unione PIM di dimensioni maggiori di 1500, che causava il rifiuto del pacchetto da parte del 4900M.

Correzione del problema:

1. Assicurarsi che i frame jumbo siano abilitati globalmente sullo switch 4900M

2. Configurare sia l'interfaccia fisica che la SVI con una MTU di 9216

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).