Risoluzione dei problemi relativi alla perdita di pacchetti multicast sul firewall con configurazione PIM Bidir

Sommario

Problema

Questi sintomi vengono osservati su Secure Firewall Threat Defense (FTD) che partecipa come hop intermedio nel dominio di routing multicast con il protocollo bidirezionale Independent Multicast (BIDIR-PIM), una variante di PIM Sparse-Mode (PIM-SM):

1. Il percorso per lo specifico gruppo multicast 232.4.4.4 è assente:

<#root>

device#

show mroute 232.4.4.4

No mroute entries found.

2. Il contatore "Altre perdite" per l'intervallo di gruppi 232.0.0.0/8 nell'output del comando show mfib count aumenta:

<#root>

device#

show mfib count

IP Multicast Statistics

6 routes, 3 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: 224.0.1.39
  RP-tree:
   Forwarding: 0/0/0/0, Other: 0/0/0
Group: 224.0.1.40
  RP-tree:
   Forwarding: 0/0/0/0, Other: 0/0/0

Group: 232.0.0.0/8

  RP-tree:
   Forwarding: 0/0/0/0,

Other: 2551

/0/

2551 <----

device#

show mfib count

IP Multicast Statistics
6 routes, 3 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: 224.0.1.39
  RP-tree:
   Forwarding: 0/0/0/0, Other: 0/0/0
Group: 224.0.1.40
  RP-tree:
   Forwarding: 0/0/0/0, Other: 0/0/0

```
Group: 232.0.0.0/8


  RP-tree:
   Forwarding: 0/0/0/0,

Other: 2864

/0/

2864

<----
```

3. I pacchetti multicast vengono scartati quando il limite di velocità Punt è stato superato (limite di velocità Punt) nel percorso di sicurezza accelerato (ASP). Il contatore aumenta continuamente:

```
<#root>
device#

cap capi trace interface inside match udp any host 232.4.4.4


device#

show cap capi trace


   2: 19:36:08.509205

192.168.1.2.12345 > 232.4.4.4.12345

:  udp 0
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 13056 ns
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 13056 ns
Config:
Implicit Rule
```

```
Additional Information:
MAC Access list

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Elapsed time: 2560 ns
Config:
Additional Information:
Found flow with id 4876, using existing flow

Result:
input-interface: inside
input-status: up
input-line-status: up
Action: drop
Time Taken: 28672 ns

Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (NA



device#

show asp drop



Frame drop:

  Punt rate limit exceeded (punt-rate-limit)                                    142


  FP L2 rule drop (l2_acl)                                                        6

Last clearing: 19:38:00 UTC Apr 29 2026 by admin

Flow drop:

Last clearing: 19:38:00 UTC Apr 29 2026 by admin
…
device#

show asp drop



Frame drop:

  Punt rate limit exceeded (punt-rate-limit)                                    780


  FP L2 rule drop (l2_acl)                                                       37
```

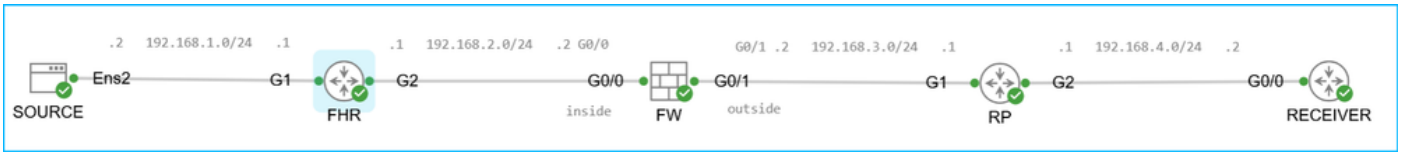
4. Le clip dell'interfaccia esterna non mostrano alcun pacchetto multicast in uscita:

<#root>

```
device#

capture capo type raw-data interface outside match udp any host 232.4.4.4


device#

show cap capo



0 packet captured



0 packet shown
```

Ambiente

Topologia:



topologia.png

Considerazioni principali:

- I peer nel dominio multicast utilizzano BIDIR-PIM.
- Il termine "router" in questo articolo si riferisce a un router Cisco come CSR o ASR.

- Rendezvous Point (RP) è un ASR 1001-X con software Cisco IOS XE, versione 17.09.08. Il problema può riguardare anche altre piattaforme e versioni software.
- Il router primo hop (FHR) è lo switch C9200L-48T-4G con software Cisco IOS XE, versione 16.12.04. Il problema può riguardare anche altre piattaforme e versioni software.
- L'indirizzo 10.4.4.4 di Rendezvous Point (RP) sull'interfaccia Loopback0 per l'intero intervallo multicast 224.0.0.0/8 viene propagato dinamicamente nel dominio multicast utilizzando il router di bootstrap PIM (BSR). Possono essere interessate anche le distribuzioni con la configurazione statica dell'indirizzo PIM RP.

  Configurazione PIM su RP:

  <#root>

  ```
  device#
  ```

  show run interface loopback0

  ```
  interface Loopback0
   description LOO
   ip address 10.4.4.4 255.255.255.255
   ip pim sparse-mode

  device(config)#
  ```

  ip pim bidir-enable

  ```
  device(config)#
  ```

  ip pim bsr-candidate Loopback0 0 1

  ```
  device(config)#
  ```

  ip pim rp-candidate Loopback0 interval 10 priority 1 bidir

- Per semplicità, in questo caso, l'RP viene mostrato come connesso al ricevitore, ossia è anche l'ultimo router hop (LHR). Questa condizione è facoltativa.
- Il firewall è Secure Firewall 3110 con versione 7.6.4. Il problema può riguardare anche altre piattaforme firewall, versioni software e software Adaptive Security Appliance (ASA).
- Sul firewall, il routing multicast è abilitato e il PIM è adiacente al First Hop Router (FHR) e al RP con la funzionalità PIM BIDIR:

  <#root>

  ```
  device#
  ```

  show run multicast-routing

```
multicast-routing


device#
show pim neighbor


Neighbor Address  Interface          Uptime    Expires DR pri Bidir
192.168.2.1       inside             1d12h     00:01:40 1
B

192.168.3.1       outside            1d12h     00:01:35 1
B
```

- Sul firewall, nonostante l'uso di PIM BSR, l'indirizzo PIM RP 10.4.4.4 è configurato manualmente. Si tratta di una configurazione ridondante. Di conseguenza, esistono 2 mapping RP a gruppo tra il gruppo 224.0.0.0/4 e l'indirizzo RP 10.4.4.4:

```
<#root>
device#
show run pim


pim rp-address 10.4.4.4 bidir


device#
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*        BD      BSR      0      10.4.4.4   RPF: outside,192.168.3.1 <-- * means the ma


224.0.0.0/4         BD      config   0      10.4.4.4   RPF: outside,192.168.3.1
```

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

Risoluzione

Prima di procedere, verificare la sezione relativa alla causa.

Le perdite di pacchetti sul firewall sono previste a causa dell'incompatibilità tra la configurazione desiderata (BIDIR-PIM) e il traffico che deve essere gestito utilizzando PIM SSM.

Se la configurazione desiderata è BIDIR-PIM, prendere in considerazione le seguenti opzioni:

- Utilizzare solo gruppi SSM non PIM.
- Se è necessario utilizzare gruppi SSM PIM, verificare che il firewall gestisca i gruppi multicast dell'intervallo SSM PIM come indirizzi di gruppi non SSM. Fare riferimento alla sezione Domande e risposte per ulteriori informazioni.
- Prendere in considerazione l'ID bug Cisco CSCwt9960.

Causa

L'indirizzo 232.4.4.4 appartiene all'intervallo del gruppo SSM (Source Specific Multicast) riservato dall'autorità IANA (Internet Assigned Numbers Authority). Il firewall riserva automaticamente l'intervallo 232.0.0.0/8 per PIM SSM:

<#root>

```
device#
```

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*        BD      BSR      0      10.4.4.4   RPF: outside,192.168.3.1
224.0.0.0/4         BD      config   0      10.4.4.4   RPF: outside,192.168.3.1
224.0.0.0/4         SM      static   0      0.0.0.0         RPF: ,0.0.0.0
```

Punti chiave di PIM SSM:

- Crea alberi basati sull'origine e utilizza percorsi (S, G).
- Infrastruttura ad albero condivisa basata su RP del protocollo PIM-SM non necessaria. In altre parole, non vengono utilizzate route RP o (*, G).
- In genere, i ricevitori si uniscono alla struttura multicast utilizzando il protocollo IGMPv3 (Internet Group Management Protocol versione 3) con il filtro dell'origine, ovvero la capacità di un sistema di segnalare l'interesse a ricevere pacchetti solo da indirizzi di origine specifici o da tutti gli indirizzi di origine tranne quelli specifici, inviati a un particolare indirizzo multicast.

Punti chiave su BIDIR-PIM:

- Crea alberi condivisi bidirezionali che connettono fonti e ricevitori multicast.
- Gli alberi bidirezionali vengono creati utilizzando un meccanismo di scelta DF (Designated Forwarder) a prova di errore che opera su ogni collegamento di una topologia multicast.
- Con l'assistenza del DF, i dati multicast vengono inoltrati in modo nativo dalle origini all'RP e quindi lungo la struttura condivisa ai ricevitori senza richiedere uno stato specifico dell'origine.
- BIDIR-PIM non utilizza voci SPT (Shortest Path Tree) e S, G (Shortest Path Tree).
- I peer BIDIR-PIM creano alberi condivisi utilizzando le voci (*, G). Questa voce per un gruppo multicast specifico deve essere presente nella tabella di route.

Il contrasto tra i punti chiave di PIM SSM e BIDIR-PIM indica che PIM SSM e BIDIR-PIM hanno funzionalità che si escludono a vicenda.

In questo caso, il dominio multicast è configurato per utilizzare BIDIR-PIM, mentre il gruppo multicast appartiene all'intervallo riservato da IANA e al firewall per PIM SSM. Poiché il dominio multicast utilizza BIDIR-PIM, le route (S, G) richieste per PIM SSM non sono disponibili sul firewall. A causa della mancanza di route, l'interfaccia in uscita/uscita per il traffico multicast non è disponibile. L'assenza dell'interfaccia in uscita/in uscita causa la perdita di pacchetti nel database

MFIB (Multicast Forwarding Information Base). I rilasci possono essere verificati usando i comandi show mfib o show mfib count:

<#root>

```
device#

show mfib count



IP Multicast Statistics
6 routes, 3 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: 224.0.1.39
  RP-tree:
   Forwarding: 0/0/0/0, Other: 0/0/0
Group: 224.0.1.40
  RP-tree:
   Forwarding: 0/0/0/0, Other: 0/0/0

Group: 232.0.0.0/8



  RP-tree:
   Forwarding: 0/0/0/0, Other:

333797

/0/

333797
```

Il firewall tenta di risolvere l'interfaccia in uscita/uscita attivando il punto di controllo (CP). Si tratta del componente critico del firewall, responsabile principalmente delle funzioni di gestione e control plane, come i protocolli di routing, l'accesso di gestione, la gestione di failover/cluster, la gestione di pacchetti destinati all'interfaccia del firewall, gli indirizzi IP multicast o broadcast e così via.

Per evitare di sovraccaricare il punto di controllo, il firewall dispone di meccanismi di protezione integrati. Ad esempio, il firewall limita la velocità dei pacchetti inviati dal piano dati (DP) al punto di controllo. I pacchetti che superano la velocità vengono scartati con il limite di velocità massima

superato (limite di velocità massima) motivo di rilascio ASP. La velocità di punt può essere verificata nell'output dell'evento show asp dp-cp punt | begin EVENT-TYPE, comando:

<#root>

```
device#

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


EVENT-TYPE          ALLOC ALLOC-FAIL ENQUEUED ENQ-FAIL  RETIRED 15SEC-RATE

punt              1264746          0  1264746        0  1264746         44

<-- 15-second punt rate

  multicast       1250020          0  1250020        0  1250020         44



  pim               14726          0    14726        0    14726          0
```

Per riepilogare, la conclusione è che ci si aspetta che il pacchetto cada sul firewall a causa dell'incompatibilità tra la configurazione prevista (BIDIR-PIM) e il traffico che deve essere gestito utilizzando PIM SSM.

Domande e risposte

In questa sezione, il termine "router" si riferisce a un router Cisco come CSR e il termine "firewall" si riferisce ai firewall Cisco che eseguono ASA o FTD.

1. D: Il firewall riserva automaticamente 232.0.0.0/8 per PIM SSM?

A: Sì. A differenza, ad esempio, dei router come CSR, non è richiesta alcuna configurazione specifica. Sui router, l'intervallo PIM SSM richiede una configurazione esplicita:

<#root>

```
device(config)#
```

```
ip pim ssm ?

  default  Use 232/8 group range for SSM

  range    ACL for group range to be used for SSM
```

2. D: Il contatore MFIB "Other drops" è specifico del firewall?

A: No. Contatore simile esiste sui router Cisco con routing multicast.

3. D: I pacchetti inviati al gruppo 232.4.4.4 potrebbero essere ignorati anche da un altro dispositivo, ad esempio un router, anziché un firewall?

A: Dipende da come il router tratta l'indirizzo 232.4.4.4. A differenza dei firewall, per impostazione predefinita i router non riservano l'intervallo 232.0.0.0/8 per PIM SSM. Tuttavia, se sia PIM SSM che BIDIR-PIM sono abilitati e il router è un RP con visibilità BIDIR-PIM o riceve un mapping RP-to-group con il flag Bidir e riceve pacchetti multicast inviati all'intervallo PIM SSM, i pacchetti vengono scartati e il contatore MFIB "Other" aumenta:

<#root>

```
device#

show run | i pim

ip pim bidir-enable

no ip pim autorp

ip pim ssm default

device#
```

show ip pim rp mapping

```
Auto-RP is not enabled
PIM Group-to-RP Mappings

Group(s) 224.0.0.0/4
  RP 10.4.4.4 (?), v2,
```

bidir <-- mapping has the bidir flag

```
    Info source: 10.4.4.4 (?), via bootstrap, priority 1, holdtime 150
         Uptime: 17:32:39, expires: 00:02:05

device#
```

show ip mfib count

```
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)
Default
 9 routes, 6 (*,G)s, 3 (*,G/m)s
Group: 224.0.0.0/4
  RP-tree,
   SW Forwarding: 1/0/28/0, Other: 41037/41037/0
   HW Forwarding:   3428217/0/64/0, Other: 0/0/0
```

Group: 232.0.0.0/8

```
  RP-tree,
```

SW Forwarding: 0/0/0/0, Other: 97/97

```
/0 <----
   HW Forwarding:   0/0/0/0, Other: 0/0/0

device#
```

show ip mfib count

```
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)
Default
 9 routes, 6 (*,G)s, 3 (*,G/m)s
```

```
Group: 224.0.0.0/4
  RP-tree,
   SW Forwarding: 1/0/28/0, Other: 41037/41037/0
   HW Forwarding:   3428217/0/64/0, Other: 0/0/0

Group: 232.0.0.0/8


  RP-tree,



SW Forwarding: 0/0/0/0,

 Other: 106/106

/0 <----
   HW Forwarding:   0/0/0/0, Other: 0/0/0
```

Si noti che, a differenza del firewall con il contatore crescente "Altre perdite" sul router, il contatore crescente è "RPF failed".

4. D: Come forzare i firewall a gestire un gruppo dall'intervallo SSM PIM come indirizzo di gruppo non SSM?

A: Verificare che RP annunci il mapping da RP a gruppo per i gruppi più specifici di 232.0.0.0/8 (prefisso più lungo) o che nel firewall configuri manualmente l'indirizzo RP per gruppi specifici.

Opzione 1. Configurazione su RP:

```
<#root>
device(config)#

access-list 1 permit host 232.4.4.4


device(config)#

ip pim rp-candidate Loopback0 group 1 interval 10 priority 1 bidir

<-- group refers to the access-list
```

Verifica sul firewall:

<#root>

device#

show pim group-map 232.4.4.4

Group Range Proto Client Groups RP address Info

232.4.4.4/32* BD

BSR 0 10.4.4.4 RPF: outside,192.168.3.1 <-- Proto is BD, not SSM

Opzione 2. Configurazione sul firewall:

<#root>

device(config)#

access-list mcast standard permit 232.4.4.4 255.255.255.254

device(config)#

pim rp-address 10.4.4.4 mcast bidir

device(config)#

show pim group-map 232.4.4.4

Group Range Proto Client Groups RP address Info

232.4.4.4/31*

BD

config 0 10.4.4.4 RPF: outside,192.168.3.1 <-- Proto is BD, not SSM

Notare che l'elenco degli accessi non deve usare voci host o voci con la maschera 255.255.255.255.

5. D: Cosa succede se il firewall gestisce un gruppo dell'intervallo SSM PIM come indirizzo di gruppo non SSM?

A: Si supponga che il gruppo 232.4.4.4 sia gestito come un indirizzo non SSM (fare riferimento alla domanda 4):

<#root>

```
device#

show pim group-map 232.4.4.4



Group Range         Proto   Client   Groups RP address      Info


232.4.4.4/32*       BD

      BSR      0      10.4.4.4   RPF: outside,192.168.3.1
```

Se la versione software è interessata dall'ID bug Cisco CSCwt9960, il percorso (*, G) risulta mancante e la velocità del flusso multicast è limitata a circa 50 pacchetti al secondo. I pacchetti in eccesso vengono scartati con il limite della velocità di punt superato (limite della velocità di punt) Motivo del rilascio di ASP:

<#root>

```
device#

show mroute 232.4.4.4



No mroute entries found.



device#

show mfib 232.4.4.4 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: 232.4.4.4
  RP-tree:
   Forwarding: 23317/
```

50

```
/28/10, Other: 0/0/0


device#
```

show mfib 232.4.4.4 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: 232.4.4.4
  RP-tree:
   Forwarding: 23540/
```

49

```
/28/10, Other: 0/0/0

device#
```

capture capi interface inside trace match udp any host 232.4.4.4

```


device#
```

show capture capi trace | i Drop-reason

```
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (N/
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (N/
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (N/
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (N/
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (N/
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (N/
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (N/
Drop-reason: (punt-rate-limit) Punt rate limit exceeded, Drop-location: frame snp_sp_mcast:4898 flow (N/
…
```

Per ulteriori informazioni, fare riferimento all'ID bug Cisco CSCwt9960.

Contenuto correlato

- Blocco Multicast Specifico Dell'Origine
- ID bug Cisco CSCwt9960

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).