

Risoluzione dei problemi relativi al traffico multicast che non passa attraverso il firewall FTD con configurazione PIM Bidir

Sommario

Problema

Si manifestano tutti i seguenti sintomi:

- Il traffico multicast ha smesso di funzionare su Firewall Threat Defense (FTD) per un gruppo multicast specifico.
- Non ci sono route multicast (route) nell'FTD per il gruppo (nell'esempio 224.2.2.2).

```
<#root>
```

```
device#
```

```
show mroute 224.2.2.2
```

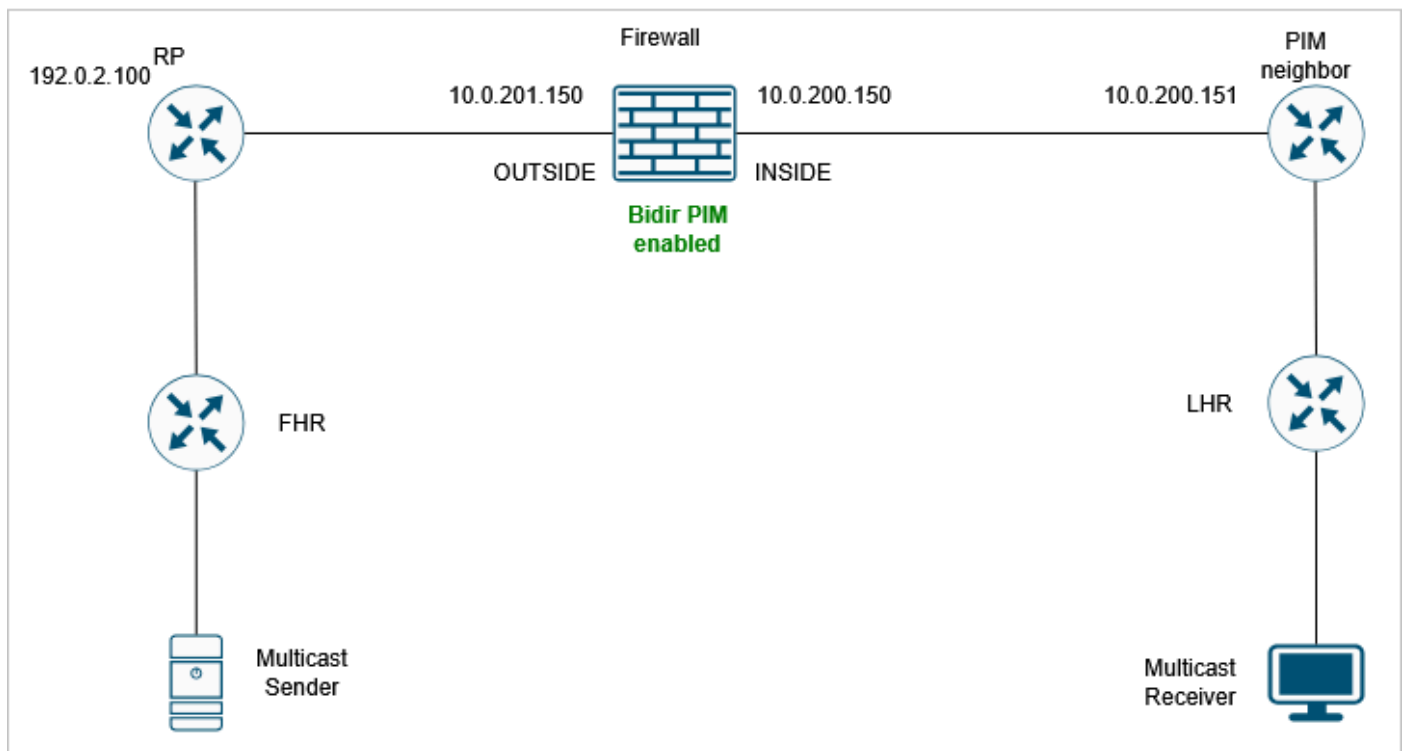
```
No mroute entries found.
```

```
device#
```

Ambiente

- Visualizzato per la prima volta nella versione 7.4. Il problema può riguardare anche altre versioni software, tra cui Adaptive Security Appliance (ASA).
- PIM (Bidirectional Protocol Independent Multicast) abilitato sul firewall.

Topologia



inline_image_0.png

Risoluzione

Passaggio 1: Controllare la configurazione multicast corrente.

Esaminare la configurazione del routing multicast esistente su tutti i dispositivi nel percorso di rete per identificare eventuali configurazioni errate o impostazioni mancanti che potrebbero impedire al traffico multicast di attraversare il firewall.

Sul firewall è presente una configurazione PIM bidirezionale:

```
<#root>
```

```
device#
```

```
show run pim
```

```
pim rp-address 192.0.2.100 bidir
```

Passaggio 2: Verificare i vicini PIM.

Verificare che i router adiacenti multicast siano visualizzati correttamente sul firewall:

```
<#root>
```

```
device#
```

```
show pim neighbor
```

Neighbor Address	Interface	Uptime	Expires	DR	pri	Bidir
10.0.200.151	INSIDE	19:13:30	00:01:24	1	(DR)	
10.0.201.200	OUTSIDE	00:01:31	00:01:42	1	(DR)	B

```
B
```

Nell'output si noti che il router adiacente 10.0.201.200 ha il flag Bidir B, mentre il router adiacente 10.0.200.151 non lo ha.

Passaggio 3: Abilita debug PIM per il gruppo multicast 24.2.2.2:

```
<#root>
```

```
FPR3100-14#
```

```
debug pim group 224.2.2.2
```

```
IPv4 PIM group debugging is on  
for group 224.2.2.2
```

Il debug mostra che è presente un pacchetto di aggiunta/eliminazione PIM che viene scartato a causa della mancata scelta di un file df bidir:

```
<#root>
```

```
IPv4 PIM: J/P entry: Join root: 192.0.2.100 group: 224.2.2.2 flags: RPT WC S
IPv4 PIM: (*,224.2.2.2) J/P with RP 192.0.2.100 on INSIDE
```

```
discarded, no bidir df election-state on this intf
```

Passaggio 4: Abilita le acquisizioni PIM verso la risorsa adiacente PIM 10.0.200.151. L'obiettivo è ottenere una maggiore visibilità sul contenuto del pacchetto:

```
<#root>
```

```
device#
```

```
capture CAPI interface INSIDE trace match pim host 10.0.200.151 any
```

Passaggio 5: Raccogli l'acquisizione del firewall dal dispositivo FTD:

```
<#root>
```

```
device#
```

```
copy /pcap capture:CAPI CAPI.pcap
```

```
Source capture name [CAPI]?
Destination filename [CAPI.pcap]?
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
!
28 packets copied in 0.0 secs
```

Raccogliere il file pcap da FMC seguendo la procedura descritta all'indirizzo <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html>

Passaggio 6: Analisi delle acquisizioni.

Il pacchetto PIM Hello contiene queste opzioni:

```
19 2026/114 08:36:29.103983 1.552086 10.0.200.151 224.0.0.13 PIMv2 72 58 0x4e2c (20012) Hello
Frame 19: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
Ethernet II, Src: Cisco_71:ab:c0 (b8:38:61:71:ab:c0), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
Internet Protocol Version 4, Src: 10.0.200.151, Dst: 224.0.0.13
Protocol Independent Multicast
  0010 .... = Version: 2
  ... 0000 = Type: Hello (0)
  Reserved byte(s): 00
  Checksum: 0x6fa0 [correct]
  [Checksum Status: Good]
  PIM Options: 5
    > Option 1: Hold Time: 105
    > Option 20: Generation ID: 165045991
    > Option 19: DR Priority: 1
    > Option 21: State-Refresh: Version = 1, Interval = 0s
    > Option 65004: RPF Proxy Vector (Cisco proprietary)
```

PIM_Hello_Options_no-bidir-capabilities.png

Si noti l'assenza del flag Bidir.

Passaggio 7: Abilitare il PIM bidirezionale sulla porta adiacente 10.0.200.151.

A questo punto, il flag PIM Bidir B viene visualizzato per entrambi i vicini:

<#root>

device#

show pim neighbor

Neighbor Address	Interface	Uptime	Expires	DR pri	Bidir
10.0.200.151	INSIDE	19:34:26	00:01:38	1 (DR)	

B

10.0.201.200	OUTSIDE	00:22:27	00:01:23	1 (DR)	B
--------------	---------	----------	----------	--------	---

Passaggio 8: Raccogliere una nuova acquisizione e controllare le opzioni di PIM Hello per il router adiacente 10.0.200.151. Viene visualizzata l'opzione PIM 22 (capacità bidirezionale):

```
77 2026/114 08:50:19.459952 5.000031 10.0.200.151 224.0.0.13 PIMv2 76 62 0x4f65 (20325) Hello
> Frame 77: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
> Ethernet II, Src: Cisco_71:ab:c0 (b8:38:61:71:ab:c0), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
> Internet Protocol Version 4, Src: 10.0.200.151, Dst: 224.0.0.13
> Protocol Independent Multicast
  0010 .... = Version: 2
  .... 0000 = Type: Hello (0)
  Reserved byte(s): 00
  Checksum: 0x6f8a [correct]
  [Checksum Status: Good]
  > PIM Options: 6
    > Option 1: Hold Time: 105
    > Option 20: Generation ID: 165045991
    > Option 22: Bidirectional Capable
    > Option 19: DR Priority: 1
    > Option 21: State-Refresh: Version = 1, Interval = 0s
    > Option 65004: RPF Proxy Vector (Cisco proprietary)
```

PIM_Hello_Options_option2.png

Passaggio 9: Verificare che il percorso per il gruppo multicast 24.2.2.2 sia visualizzato:

<#root>

device#

show mroute

Multicast Routing Table

Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
C - Connected, L - Local, I - Received Source Specific Host Report,
P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
J - Join SPT

Timers: Uptime/Expires

Interface state: Interface, State

(* , 224.0.1.40), 19:41:44/never, RP 0.0.0.0, flags: DPC

Incoming interface: Null

RPF nbr: 0.0.0.0

Immediate Outgoing interface list:

INSIDE, Null, 19:41:44/never

(* , 224.2.2.2)

, 00:06:29/00:02:53, RP 192.0.2.100, flags: B

Bidir-Upstream: OUTSIDE

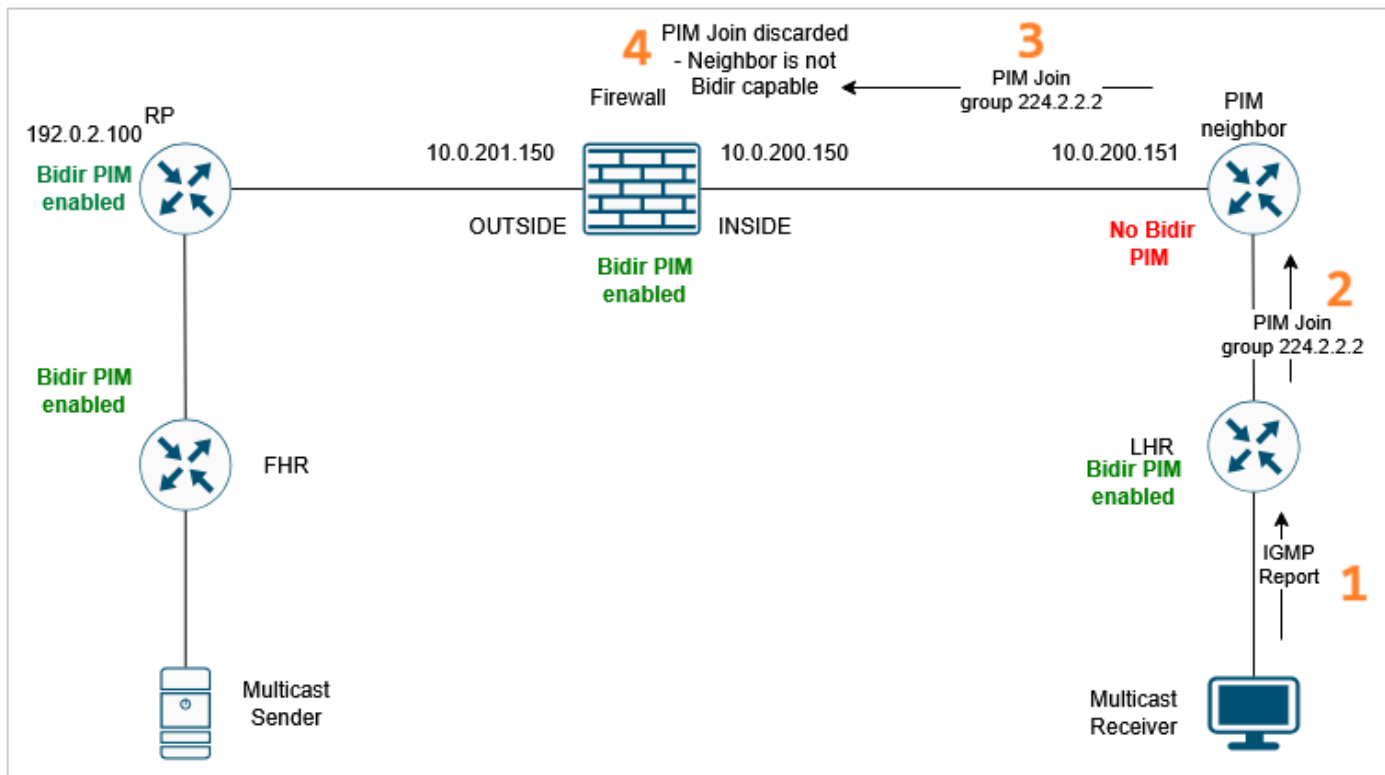
RPF nbr: 10.0.201.200

Immediate Outgoing interface list:

INSIDE, Forward, 00:06:29/00:02:53

Causa

L'errore relativo al traffico multicast è stato causato da una configurazione PIM multicast e bidirezionale errata o incompleta nel dispositivo di rete adiacente. A causa del problema di configurazione specifico, FTD ha eliminato il messaggio di aggiunta/eliminazione PIM per il gruppo multicast specifico. Di conseguenza, il firewall non è in grado di creare il percorso per il traffico multicast. Affinché il traffico di dati multicast passi attraverso il piano dati del firewall, il control plane (PIM) deve stabilire il percorso corretto.



Causa.png

Contenuto correlato

- <https://datatracker.ietf.org/doc/html/rfc5015#section-3.7.4>

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).