Problemen oplossen Multicast Packet Drops op Firewall met Bidir PIM-configuratie

Inhoud

uitgeven

Deze symptomen worden waargenomen op Secure Firewall Threat Defense (FTD) dat deelneemt als intermediaire hop in het multicast-routeringsdomein met de Bidirectional Protocol Independent Multicast (BIDIR-PIM), een variant van PIM Sparse-Mode (PIM-SM):

1. De route voor de specifieke multicastgroep 232.4.4.4 ontbreekt:

<#root>

```
device#

show mroute 232.4.4.4



No mroute entries found.
```

2. De "Other drops"-teller voor het 232.0.0.0/8-groepsbereik in de uitvoer van de opdracht show mfib count verhoogt:

<#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. Multicast-pakketten worden verwijderd als de puntsnelheidslimiet is overschreden (puntsnelheidslimiet) en de reden voor de val in het versnelde beveiligingspad (ASP) is overschreden. De valteller neemt voortdurend toe:

<#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. De buitengrensinterfaceopnames tonen geen uitgaande multicastpakketten:

<#root>

```
device#
```

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

```
device#
```

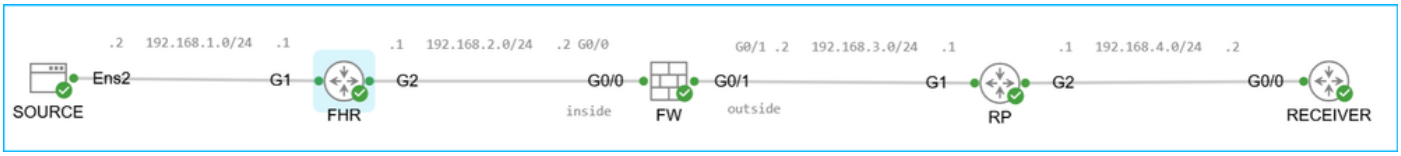
show cap capo

0 packet captured

0 packet shown

milieu

Topologie:



topologie.png

Belangrijkste punten:

- De peers in het multicast-domein gebruiken BIDIR-PIM.
- De "router" in dit artikel verwijst naar een Cisco-router zoals CSR of ASR.
- Rendezvous Point (RP) is ASR1001-X met Cisco IOS XE Software, versie 17.09.08. Ook

andere platforms en softwareversies kunnen worden beïnvloed.

- First Hop Router (FHR) is C9200L-48T-4G met Cisco IOS XE Software, versie 16.12.04. Ook andere platforms en softwareversies kunnen worden beïnvloed.
- RP-adres (Rendezvous Point) 10.4.4.4 op de Loopback0-interface voor het volledige multicastbereik 224.0.0.0/8 wordt dynamisch verspreid in het multicastdomein met behulp van de PIM Bootstrap router (BSR). Implementaties met de statische PIM RP-adresconfiguratie kunnen ook worden beïnvloed.

  PIM-configuratie op 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
  ```

- Eenvoudigheidshalve wordt in dit geval de RP weergegeven als verbonden met de ontvanger, dat wil zeggen dat het ook de laatste hoprouter (LHR) is. Dit is optioneel.
- De firewall is Secure Firewall 3110 met versie 7.6.4. Andere firewallplatforms, softwareversies en Adaptive Security Appliance (ASA)-software kunnen ook worden beïnvloed.
- Op de firewall is multicast-routering ingeschakeld en is er PIM-nabijheid met de First Hop Router (FHR) en RP met de PIM BIDIR-mogelijkheid:

  ```
  <#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
```

- Ondanks het gebruik van PIM BSR wordt het PIM RP-adres 10.4.4.4 handmatig geconfigureerd. Dit is een redundante configuratie. Als gevolg hiervan zijn er 2 RP-to-group mappings tussen de groep 224.0.0.0/4 en het RP-adres 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
```

resolutie

Voordat u doorgaat, moet u ervoor zorgen dat u de sectie Oorzaak bekijkt.

De pakketdruppels op de firewall worden verwacht als gevolg van incompatibiliteit tussen de beoogde configuratie (BIDIR-PIM) en verkeer dat moet worden afgehandeld met behulp van PIM SSM.

Als de beoogde configuratie BIDIR-PIM is, overweeg dan deze opties:

- Gebruik alleen niet-PIM SSM-groepen.
- Als PIM SSM-groepen moeten worden gebruikt, moet u ervoor zorgen dat de firewall multicast-groepen uit het PIM SSM-bereik als niet-SSM-groepsadressen behandelt. Raadpleeg de Q&A sectie voor meer informatie.
- Neem bijvoorbeeld Cisco bug ID CSCwt99960.

Oorzaak

Het adres 232.4.4.4 behoort tot het Source Specific Multicast (SSM)-groepsbereik dat is gereserveerd door de Internet Assigned Numbers Authority (IANA). De firewall reserveert automatisch het bereik 232.0.0.0/8 voor 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
```

Belangrijkste punten over PIM SSM:

- Het bouwt brongebaseerde bomen en gebruikt (S, G) mroutes.
- RP-gebaseerde gedeelde boominfrastructuur van het PIM-SM-protocol is niet vereist. Met andere woorden, RP- of (*, G)-routes worden niet gebruikt.
- Ontvangers sluiten zich meestal aan bij de multicaststructuur door gebruik te maken van het Internet Group Management Protocol Version 3 (IGMPv3) met "bronfiltering", dat wil zeggen de mogelijkheid voor een systeem om interesse te melden in het ontvangen van pakketten alleen vanaf specifieke bronadressen, of van alle maar specifieke bronadressen, verzonden naar een bepaald multicastadres.

Belangrijkste punten over BIDIR-PIM:

- Het bouwt bidirectionele gedeelde bomen die multicast-bronnen en ontvangers verbinden.
- Bidirectionele bomen zijn gebouwd met behulp van een fail-safe Designated Forwarder (DF) verkiezingsmechanisme dat werkt op elke link van een multicast topologie.
- Met de hulp van de DF worden multicast-gegevens native doorgestuurd van bronnen naar de RP en dus langs de gedeelde boom naar ontvangers zonder bronspecifieke status te vereisen.
- BIDIR-PIM maakt geen gebruik van de vermeldingen voor de kortste paden (SPT) en (S, G).
- BIDIR-PIM-peers bouwen gedeelde bomen met behulp van (*, G) vermeldingen. Deze vermelding voor een bepaalde multicastgroep moet in de mroutetabel staan.

Uit het contrast tussen de belangrijkste punten voor PIM SSM en BIDIR-PIM blijkt dat PIM SSM en BIDIR-PIM elkaar uitsluitende functionaliteit hebben.

In dit geval is het multicast-domein geconfigureerd voor het gebruik van BIDIR-PIM, terwijl de multicast-groep behoort tot het bereik dat is gereserveerd door IANA en de firewall voor PIM SSM. Aangezien het multicast-domein gebruik maakt van BIDIR-PIM, zijn (S, G)-routes die vereist zijn

voor PIM SSM niet beschikbaar op de firewall. Vanwege het ontbreken van mroutes zijn de uitgaande/uitgaande interface voor het multicast-verkeer niet beschikbaar. De afwezigheid van uitgang/uitgaande interface resulteert in pakketdalingen in de multicast forwarding information base (MFIB). De druppels kunnen worden geverifieerd met behulp van de opdrachten show mfib of 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
```

De firewall probeert de uitgaande/uitgaande interface op te lossen door het besturingspunt (CP) in te schakelen. Dit is de kritieke firewallcomponent die voornamelijk verantwoordelijk is voor het beheer en de controle van vliegtuigfuncties, zoals routeringsprotocollen, beheertoegang, failover-/clusterbeheer, het afhandelen van pakketten die bestemd zijn voor de firewall-interface, multicast- of broadcast-IP-adressen, enzovoort.

Om overbelasting van het controlepunt te voorkomen, heeft de firewall ingebouwde beveiligingsmechanismen. Firewall beperkt bijvoorbeeld de snelheid van pakketten die van het gegevensvlak (DP) naar het besturingspunt worden verzonden. Pakket dat het tarief overschrijdt, wordt verwijderd met de puntsnelheidslimiet overschreden (puntsnelheidslimiet) ASP-valreden. De puntfrequentie kan worden geverifieerd in de uitvoer van de show asp event dp-cp punt | begin EVENT-TYPE opdracht:

```
<#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
```

Samenvattend is de conclusie dat pakketdruppels op de firewall worden verwacht als gevolg van incompatibiliteit tussen de beoogde configuratie (BIDIR-PIM) en verkeer dat moet worden afgehandeld met behulp van PIM SSM.

V&A

In deze sectie verwijst "router" naar een Cisco-router zoals CSR en "firewall" verwijst naar Cisco-firewalls die ASA of FTD uitvoeren.

1. V: reserveert de firewall automatisch 232.0.0.0/8 voor PIM SSM?

A: Ja. In tegenstelling tot bijvoorbeeld routers zoals CSR, is er geen specifieke configuratie vereist. Op routers moet het PIM SSM-bereik expliciet worden geconfigureerd:

<#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. Q: Is de MFIB "Andere druppels" teller specifiek voor firewall?

A: Nee. Een soortgelijke teller bestaat op Cisco-routers met multicast-routering.

3. V: Zou een ander apparaat zoals een router in plaats van een firewall ook pakketten laten vallen die naar de groep 232.4.4.4 zijn verzonden?

A: Het hangt af van hoe de router het adres behandelt 232.4.4.4. In tegenstelling tot firewalls reserveren routers standaard het bereik 232.0.0.0/8 niet voor PIM SSM. Als echter zowel PIM SSM als BIDIR-PIM zijn ingeschakeld en de router ofwel BIDIR-PIM-aware RP is of RP-to-group mapping ontvangt met de Bidir-vlag en multicast-pakketten ontvangt die naar het PIM SSM-bereik worden verzonden, worden de pakketten verwijderd en neemt de MFIB "Other"-teller toe:

<#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
```

Merk op dat in tegenstelling tot de firewall met de toenemende "Andere druppels" teller op de router de toenemende teller is "RPF mislukt".

4. V: Hoe kan ik firewalls dwingen om een groep uit het PIM SSM-bereik als een niet-SSM-groepsadres te behandelen?

A: Zorg ervoor dat RP RP-to-group mapping adverteert voor groepen die specifieker zijn dan 232.0.0.0/8 (langer voorvoegsel) of configureer het RP-adres handmatig in de firewall voor specifieke groepen.

Optie 1. Configuratie op 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
```

Verificatie op 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
```

Optie 2. Configuratie op 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
```

Merk op dat de toegangslijst geen hostvermeldingen of -vermeldingen met het masker 255.255.255.255 mag gebruiken.

5. V: Wat gebeurt er als de firewall een groep uit het PIM SSM-bereik behandelt als een niet-SSM-groepsadres?

A: Stel dat groep 232.4.4.4 wordt behandeld als een niet-SSM-adres (zie vraag 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
```

Als de softwareversie wordt beïnvloed door Cisco bug-ID CSCwt99960, ontbreekt de (*, G) mroute en is de multicast-stroomsnelheid beperkt tot ongeveer 50 pakketten per seconde. Excessieve pakketten worden verwijderd met overschrijding van de puntsnelheidslimiet (puntsnelheidslimiet) ASP-dropreden:

```
<#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/
…
```

Raadpleeg voor meer informatie de Cisco bug ID CSCwt99960.

Verwante inhoud

- bronspecifiek multicastblok
- Cisco bug ID CSCwt99960

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.