Fehlerbehebung bei Multicast-Paketverlusten auf der Firewall mit Bidir PIM-Konfiguration

Inhalt

Problem

Diese Symptome wurden bei Secure Firewall Threat Defense (FTD) beobachtet, die als intermediärer Hop in der damaligen Multicast-Routing-Domäne mit Bidirectional Protocol Independent Multicast (BIDIR-PIM), einer Variante des PIM Sparse-Mode (PIM-SM), agiert:

1. Die Route für die spezifische Multicast-Gruppe 232.4.4.4 fehlt:

<#root>

device#

show mroute 232.4.4.4

No mroute entries found.

2. Der Zähler "Other drops" für den Gruppenbereich 232.0.0.0/8 in der Ausgabe des Befehls show mfib count erhöht sich:

<#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-Pakete werden verworfen, wenn der Grenzwert für die Punt-Rate im Accelerated Security Path (ASP) den Verwerfungsgrund überschritten hat. Der Tropfenzähler erhöht sich kontinuierlich:

<#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. Die externen Schnittstellenerfassungen zeigen keine ausgehenden Multicast-Pakete an:

<#root>

```
device#
```

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

```
device#
```

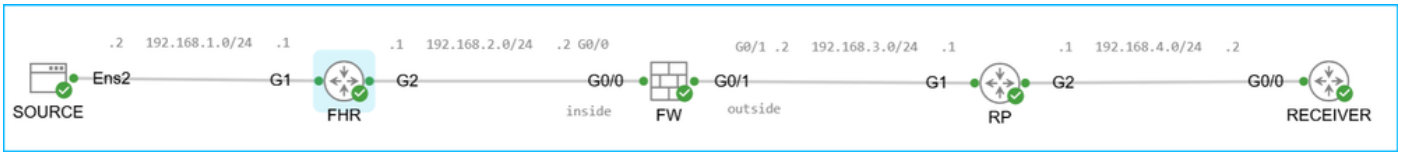
show cap capo

0 packet captured

0 packet shown

Umwelt

Topologie:



topology.png

Wichtigste Punkte:

- Die Peers in der Multicast-Domäne verwenden BIDIR-PIM.
- Der "Router" in diesem Artikel bezieht sich auf einen Cisco Router wie CSR oder ASR.
- Rendezvous Point (RP) ist ein ASR1001-X mit Cisco IOS XE Software, Version 17.09.08.

Andere Plattformen und Softwareversionen können ebenfalls betroffen sein.

- First Hop Router (FHR) ist ein C9200L-48T-4G mit Cisco IOS XE Software, Version 16.12.04. Andere Plattformen und Softwareversionen können ebenfalls betroffen sein.
- Die Rendezvous Point (RP)-Adresse 10.4.4.4 an der Loopback0-Schnittstelle für den gesamten Multicast-Bereich 224.0.0.0/8 wird mithilfe des PIM-Bootstrap-Routers (BSR) dynamisch in der Multicast-Domäne propagiert. Bereitstellungen mit statischer PIM RP-Adresskonfiguration können ebenfalls betroffen sein.

  PIM-Konfiguration auf 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

- Der Einfachheit halber ist in diesem Fall der RP als mit dem Empfänger verbunden dargestellt, d.h. er ist auch der Last Hop Router (LHR).
- Die Firewall ist eine sichere Firewall 3110 mit Version 7.6.4. Andere Firewall-Plattformen, Softwareversionen und die Adaptive Security Appliance (ASA)-Software können ebenfalls betroffen sein.
- Auf der Firewall ist Multicast-Routing aktiviert, und es besteht PIM-Adjacency mit dem First Hop Router (FHR) und RP mit der PIM BIDIR-Funktion:

  <#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
```

- Auf der Firewall wird die PIM RP-Adresse 10.4.4.4 trotz PIM BSR manuell konfiguriert. Diese Konfiguration ist redundant. Daher gibt es 2 RP-Gruppen-Zuordnungen zwischen der Gruppe 224.0.0.0/4 und der RP-Adresse 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
```

Auflösung

Überprüfen Sie vor dem Fortfahren unbedingt den Abschnitt mit der Ursache.

Die Paketverluste auf der Firewall werden aufgrund der Inkompatibilität zwischen der beabsichtigten Konfiguration (BIDIR-PIM) und dem Datenverkehr erwartet, der mithilfe von PIM SSM verarbeitet werden muss.

Wenn die beabsichtigte Konfiguration BIDIR-PIM ist, dann sollten Sie folgende Optionen in Betracht ziehen:

- Nur Nicht-PIM SSM-Gruppen verwenden.
- Wenn PIM SSM-Gruppen verwendet werden müssen, stellen Sie sicher, dass die Firewall Multicast-Gruppen aus dem PIM SSM-Bereich als Nicht-SSM-Gruppenadressen behandelt. Weitere Informationen finden Sie im Abschnitt "Fragen und Antworten".
- Berücksichtigen Sie die Cisco Bug-ID CSCwt9960.

Ursache

Die Adresse 232.4.4.4 gehört zum SSM-Gruppenbereich (Source Specific Multicast), der von der IANA (Internet Assigned Numbers Authority) reserviert ist. Die Firewall reserviert automatisch den Bereich 232.0.0.0/8 für 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
```

Wichtige Punkte zu PIM SSM:

- Es erstellt quellenbasierte Trees und verwendet (S,G) mroute.
- Eine RP-basierte Shared-Tree-Infrastruktur des PIM-SM-Protokolls ist nicht erforderlich. Mit anderen Worten, RP- oder (*,G)-Routen werden nicht verwendet.
- Empfänger treten dem Multicast-Tree in der Regel über das Internet Group Management Protocol Version 3 (IGMPv3) mit "Quellfilterung" bei, d. h. die Möglichkeit für ein System, Interesse am Empfang von Paketen zu melden, die nur von bestimmten Quelladressen oder von allen, mit Ausnahme bestimmter Quelladressen, an eine bestimmte Multicast-Adresse gesendet werden.

Wichtige Punkte zu BIDIR-PIM:

- Er erstellt bidirektionale Shared Trees, die Multicast-Quellen und -Empfänger miteinander verbinden.
- Bidirektionale Trees werden mithilfe eines ausfallsicheren Designated Forwarder (DF)-Auswahlmechanismus erstellt, der auf jeder Verbindung einer Multicast-Topologie funktioniert.
- Mithilfe des DF werden Multicast-Daten nativ von Quellen an den RP und damit entlang des Shared Tree an Empfänger weitergeleitet, ohne dass ein quellenspezifischer Status erforderlich ist.
- BIDIR-PIM verwendet keine SPT- (Shortest Path Trees) und G-Einträge (S, G).
- BIDIR-PIM-Peers erstellen Shared Trees mithilfe von (*,G)-Einträgen. Dieser Eintrag für eine bestimmte Multicast-Gruppe muss in der mroute-Tabelle vorhanden sein.

Im Gegensatz zu den Schlüsselpunkten für PIM SSM und BIDIR-PIM zeigt sich, dass PIM SSM und BIDIR-PIM sich gegenseitig ausschließende Funktionen aufweisen.

In diesem Fall ist die Multicast-Domäne für die Verwendung von BIDIR-PIM konfiguriert, während die Multicast-Gruppe zu dem von IANA und der Firewall für PIM SSM reservierten Bereich gehört. Da die Multicast-Domäne BIDIR-PIM verwendet, sind für PIM SSM erforderliche Routen (S,G) auf der Firewall nicht verfügbar. Aufgrund fehlender Routen sind die ausgehenden/ausgehenden Schnittstellen für den Multicast-Verkehr nicht verfügbar. Das Fehlen einer ausgehenden/ausgehenden Schnittstelle führt zu Paketverlusten in der Multicast Forwarding Information Base (MFIB). Die Drops können mit den Befehlen show mfib oder show mfib count überprüft werden:

<#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

Die Firewall versucht, die ausgehende/ausgehende Schnittstelle durch Anwenden des Kontrollpunkts (CP) zu lösen. Dies ist die kritische Firewall-Komponente, die hauptsächlich für

Funktionen der Management- und Kontrollebene verantwortlich ist, wie Routing-Protokolle, Managementzugriff, Failover-/Cluster-Management, Verarbeitung von Paketen, die an die Firewall-Schnittstelle gerichtet sind, Multicast- oder Broadcast-IP-Adressen usw.

Um eine Überlastung des Kontrollpunkts zu vermeiden, verfügt die Firewall über integrierte Schutzmechanismen. Beispielsweise begrenzt eine Firewall die Rate der Pakete, die von der Datenebene (DP) an den Kontrollpunkt gesendet werden. Pakete, die die Rate überschreiten, werden verworfen, wenn der Grenzwert für die Paketrate überschritten wird (Grenzwert für die Paketrate), weil ASP verworfen wurde. Die Punktrate kann in der Ausgabe des show asp event dp-cp punt verifiziert werden | Befehl "begin EVENT-TYPE":

<#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
```

Zusammenfassend lässt sich feststellen, dass Paketverluste auf der Firewall aufgrund von Inkompatibilität zwischen der beabsichtigten Konfiguration (BIDIR-PIM) und Datenverkehr, der mit PIM SSM verarbeitet werden muss, zu erwarten sind.

Fragen und Antworten

In diesem Abschnitt bezieht sich "Router" auf einen Cisco Router wie CSR und "Firewall" auf Cisco Firewalls mit ASA oder FTD.

1. F: Reserviert die Firewall automatisch 232.0.0.0/8 für PIM SSM?

A : Ja. Im Gegensatz zu Routern wie CSR ist keine spezifische Konfiguration erforderlich. Auf Routern muss der PIM SSM-Bereich explizit konfiguriert werden:

<#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. F: Ist der MFIB-Zähler "Other Drops" (Sonstige Drops) spezifisch für die Firewall?

A : Nein. Ein ähnlicher Zähler ist auf Cisco Routern mit Multicast-Routing vorhanden.

3. F: Würde ein anderes Gerät wie ein Router anstelle einer Firewall auch Pakete verwerfen, die an die Gruppe 232.4.4.4 gesendet wurden?

A : Dies hängt davon ab, wie der Router die Adresse 232.4.4.4 behandelt. Im Gegensatz zu Firewalls reservieren Router standardmäßig den Bereich 232.0.0.0/8 nicht für PIM SSM. Wenn jedoch sowohl PIM SSM als auch BIDIR-PIM aktiviert sind und der Router entweder einen BIDIR-PIM-fähigen RP aufweist oder eine RP-Gruppen-Zuordnung mit dem Bidir-Flag empfängt und an den PIM SSM-Bereich gesendete Multicast-Pakete empfängt, werden die Pakete verworfen, und der MFIB-Zähler "Sonstige" erhöht sich:

<#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
```

Beachten Sie, dass der Zähler für den Anstieg im Gegensatz zur Firewall mit dem Zähler für den Anstieg der "Sonstige Drops" auf dem Router "RPF fehlgeschlagen" ist.

4. F: Wie werden Firewalls dazu gezwungen, eine Gruppe aus dem PIM SSM-Bereich als Nicht-SSM-Gruppenadresse zu behandeln?

A : Stellen Sie sicher, dass entweder der RP die Zuordnung von RP zu Gruppen für Gruppen ankündigt, die spezifischer sind als 232.0.0.0/8 (längeres Präfix), oder dass Sie die RP-Adresse für bestimmte Gruppen manuell auf der Firewall konfigurieren.

Option 1. Konfiguration auf 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
```

Überprüfung auf der 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
```

Option 2. Konfiguration der 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
```

Beachten Sie, dass die Zugriffsliste keine Hosteinträge oder -einträge mit der Maske 255.255.255.255 verwenden darf.

5. F: Was passiert, wenn die Firewall eine Gruppe aus dem PIM SSM-Bereich als Nicht-SSM-Gruppenadresse behandelt?

A : Angenommen, die Gruppe 232.4.4.4 wird als Nicht-SSM-Adresse behandelt (siehe Frage 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
```

Wenn die Softwareversion von der Cisco Bug-ID CSCwt9960 betroffen ist, fehlt die (*,G)-Route, und der Multicast-Fluss ist mit einer Rate von ca. 50 Paketen pro Sekunde begrenzt. Übermäßige Pakete werden verworfen, wenn der Grenzwert für die Punktrate überschritten wird (Grenzwert für die Punktrate). ASP-Verwerfungsgrund:

<#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/
…
```

Weitere Informationen finden Sie unter der Cisco Bug-ID CSCwt99960.

Verwandte Inhalte

- Quellspezifischer Multicast-Block
- Cisco Bug-ID CSCwt99960

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.