Solucione problemas de quedas de pacotes multicast no firewall com a configuração PIM do Bidir

Contents

Problema

Esses sintomas são observados no Secure Firewall Threat Defense (FTD) que participa como um salto intermediário no domínio de roteamento multicast com o Bidirectional Protocol Independent Multicast (BIDIR-PIM), uma variante do PIM Sparse-Mode (PIM-SM):

1. A mroute para o grupo multicast específico 232.4.4.4 está ausente:

<#root>

device#

show mroute 232.4.4.4

No mroute entries found.

2. O contador "Other drops" para o intervalo do grupo 232.0.0.0/8 na saída da saída do 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. Os pacotes multicast são descartados com a razão de queda Limite de taxa punt excedido (limite de taxa punt) no Caminho de Segurança Acelerado (ASP). O contador de queda 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. As capturas de interface externa não mostram nenhum pacote multicast de saída:

<#root>

device#

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

device#

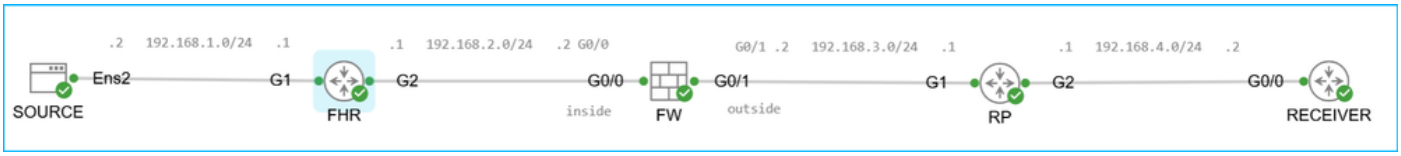
show cap capo

0 packet captured

0 packet shown

Ambiente

Topologia:



topology.png

Pontos principais:

- Os peers no domínio multicast usam BIDIR-PIM.
- O "roteador" neste artigo refere-se a um roteador Cisco como CSR ou ASR.

- O Rendezvous Point (RP) é o ASR1001-X executando o software Cisco IOS XE, versão 17.09.08. Outras plataformas e versões de software também podem ser afetadas.
- O First Hop Router (FHR) é C9200L-48T-4G executando o software Cisco IOS XE, versão 16.12.04. Outras plataformas e versões de software também podem ser afetadas.
- O endereço do ponto de rendezvous (RP) 10.4.4.4 na interface Loopback0 para todo o intervalo de multicast 224.0.0.0/8 é propagado dinamicamente no domínio de multicast usando o roteador de bootstrap PIM (BSR). As implantações com a configuração de endereço RP PIM estático também podem ser afetadas.

  Configuração PIM no RP:

  ```
  <#root>

  device#

  show run interface loopback0


  interface Loopback0
   description LO0
   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
  ```

- Por uma questão de simplicidade, nesse caso, o RP é mostrado como conectado ao receptor, ou seja, também é o roteador de último salto (LHR). Isso é opcional.
- O firewall é o Secure Firewall 3110 executando a versão 7.6.4. Outras plataformas de firewall, versões de software e software Adaptive Security Appliance (ASA) também podem ser afetados.
- No firewall, o roteamento multicast é ativado e há adjacência de PIM com o First Hop Router (FHR) e RP com o recurso 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
```

- No firewall, apesar de usar o PIM BSR, o endereço 10.4.4.4 do PIM RP é configurado manualmente. Essa é uma configuração redundante. Como resultado, há 2 mapeamentos RP-para-grupo entre o grupo 224.0.0.0/4 e o endereço 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
```

Resolução

Antes de continuar, certifique-se de revisar a seção Causa.

Os descartes de pacotes no firewall são esperados devido à incompatibilidade entre a configuração pretendida (BIDIR-PIM) e o tráfego que precisa ser tratado usando o PIM SSM.

Se a configuração pretendida for BIDIR-PIM, considere estas opções:

- Use somente grupos SSM não PIM.
- Se for necessário usar grupos PIM SSM, certifique-se de que o firewall manipule grupos multicast do intervalo PIM SSM como endereços de grupo não SSM. Consulte a seção de PerguntaseRespostas para obter mais informações.
- Considere a ID de bug da Cisco CSCwt9960.

Causa

O endereço 232.4.4.4 pertence ao intervalo de grupos do SSM (Source Specific Multicast, envio específico da origem) reservado pela IANA (Internet Assigned Numbers Authority, autoridade para números atribuídos à Internet). O firewall reserva automaticamente o intervalo 232.0.0.0/8 para o 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
```

Pontos principais sobre o PIM SSM:

- Ele constrói árvores baseadas na fonte e usa mroutes (S, G).
- A infraestrutura de árvore compartilhada baseada em RP do protocolo PIM-SM não é necessária. Em outras palavras, as rotas RP ou (*, G) não são usadas.
- Os receptores tipicamente unem-se à árvore multicast usando o Internet Group Management Protocol Versão 3 (IGMPv3) com "filtragem de origem", isto é, a capacidade de um sistema relatar o interesse em receber pacotes somente de endereços de origem específicos, ou de todos os endereços de origem, exceto os específicos, enviados para um endereço multicast particular.

Pontos principais sobre BIDIR-PIM:

- Ela cria árvores compartilhadas bidirecionais conectando fontes e receptores multicast.
- Árvores bidirecionais são criadas usando um mecanismo de eleição de encaminhador designado (DF) à prova de falhas operando em cada link de uma topologia multicast.
- Com a ajuda do DF, os dados multicast são encaminhados nativamente das fontes para o RP e, portanto, ao longo da árvore compartilhada para os receptores sem exigir o estado específico da fonte.
- O BIDIR-PIM não usa as entradas Shortest Path Trees (SPT) e (S, G).
- Os peers BIDIR-PIM constroem árvores compartilhadas usando entradas (*, G). Essa entrada para um grupo multicast específico deve existir na tabela mroute.

O contraste dos pontos principais para o PIM SSM e o BIDIR-PIM mostra que o PIM SSM e o BIDIR-PIM têm funcionalidade mutuamente exclusiva.

Nesse caso, o domínio multicast é configurado para usar BIDIR-PIM, enquanto o grupo multicast pertence ao intervalo reservado pela IANA e o firewall para o PIM SSM. Como o domínio multicast está usando BIDIR-PIM, as rotas (S, G) necessárias para SSM PIM não estão

disponíveis no firewall. Devido à falta de mroutes, a interface de saída/saída para o tráfego multicast não está disponível. A ausência de interface de saída/saída resulta em quedas de pacotes no Multicast Forwarding Information Base (MFIB). As quedas podem ser verificadas usando os comandos show mfib ou 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
```

O firewall tenta resolver a interface de saída/saída ativando o ponto de controle (CP). Esse é o componente crítico de firewall responsável principalmente pelas funções do plano de gerenciamento e controle, como protocolos de roteamento, acesso de gerenciamento, gerenciamento de failover/cluster, tratamento de pacotes destinados à interface de firewall, endereços IP multicast ou de broadcast e assim por diante.

Para evitar a sobrecarga do ponto de controle, o firewall tem mecanismos de proteção integrados. Por exemplo, o firewall limita a taxa de pacotes enviados do plano de dados (DP) para o ponto de controle. Os pacotes que excederem a taxa serão descartados com o limite de taxa de punt excedido (limite de taxa de punt) motivo de queda do ASP. A taxa de punt pode ser verificada na saída do comando show asp event dp-cp punt | begin EVENT-TYPE command:

```
<#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
```

Resumindo, a conclusão é que os descartes de pacotes no firewall são esperados devido à incompatibilidade entre a configuração pretendida (BIDIR-PIM) e o tráfego que precisa ser tratado usando o PIM SSM.

Perguntas e respostas

Nesta seção, "roteador" refere-se a um roteador Cisco como CSR e "firewall" refere-se a firewalls Cisco que executam ASA ou FTD.

1. P: O firewall reserva automaticamente 232.0.0.0/8 para o PIM SSM?

R: Yes. Ao contrário de, por exemplo, roteadores como CSR, nenhuma configuração específica é necessária. Nos roteadores, o intervalo de SSM PIM precisa de configuração explícita:

<#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: O contador de "Outras quedas" do MFIB é específico do firewall?

R: Não. Existe um contador semelhante nos roteadores Cisco com roteamento multicast.

3. Q: Um outro dispositivo como um roteador no lugar de um firewall também descartaria pacotes enviados para o grupo 232.4.4.4?

R: Depende de como o roteador trata o endereço 232.4.4.4. Ao contrário dos firewalls, por padrão os roteadores não reservam o intervalo 232.0.0.0/8 para o PIM SSM. No entanto, se o PIM SSM e o BIDIR-PIM estiverem ativados, e o roteador for RP BIDIR-PIM ciente ou receber o mapeamento RP-para-grupo com a flag Bidir e receber pacotes multicast enviados ao intervalo PIM SSM, os pacotes serão descartados e o contador "Outro" MFIB aumentará:

<#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
```

Observe que, ao contrário do firewall, com o contador crescente de "Outras quedas" no roteador, o contador crescente é "RPF falhou".

4. P: Como forçar os firewalls a lidar com um grupo do intervalo do PIM SSM como um endereço de grupo não SSM?

R: Certifique-se de que o RP anuncie o mapeamento RP-para-grupo para grupos que são mais específicos do que 232.0.0.0/8 (prefixo mais longo) ou no firewall configure manualmente o endereço RP para grupos específicos.

Opção 1. Configuração no 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
```

Verificação no 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
```

Opção 2. Configuração no 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
```

Observe que a lista de acesso não deve usar entradas de host ou entradas com a máscara 255.255.255.255.

5. Q: O que acontece se o firewall tratar um grupo do intervalo de SSM PIM como um endereço de grupo não SSM?

R: Suponha que o grupo 232.4.4.4 seja tratado como um endereço não SSM (consulte a pergunta 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 a versão do software for afetada pelo bug da Cisco ID CSCwt9960, o mroute (*, G) está ausente e o fluxo multicast é limitado por taxa em torno de 50 pacotes por segundo. Pacotes excessivos são descartados com o limite de taxa de punt excedido (limite de taxa de punt) motivo de queda do 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/
…
```

Para obter mais informações, consulte o bug da Cisco ID CSCwt9960.

Conteúdo relacionado

- Bloco Multicast Específico da Origem
- ID de bug da Cisco CSCwt99960

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.