Solucionar problemas de alta utilização de QFP devido à configuração padrão do gatekeeper NAT

Contents

[Introdução](#)

[Pré-requisitos](#)

- [Requisitos](#)
- [Componentes Utilizados](#)

[Informações de Apoio](#)

[Sintomas](#)

[Recurso Packet Trace](#)

- [Configuração básica do Packet Trace](#)

[O que é o Gatekeeper NAT?](#)

[Verifique o Gatekeeper NAT](#)

[Solução alternativa/correção](#)

- [Solução 1](#)
- [Solução 2](#)

[Summary](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como identificar e resolver a utilização do QFP (High Quantum Flow Processor) em plataformas de roteamento causada pela combinação de tráfego NAT e não NAT.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico da arquitetura de encaminhamento de pacotes do Cisco IOS® XE
- Experiência básica com o recurso Packet Trace

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas. Ele se aplica a qualquer plataforma de roteamento Cisco IOS XE com QFP físico/virtualizado como ASR1000, ISR4000, ISR1000, Cat8000 ou Cat8000v.

Este documento é baseado nos dispositivos Cisco IOS XE em modo autônomo, SDWAN (controlador) ou roteamento SD pode seguir uma lógica semelhante, mas os detalhes podem ser diferentes.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Problemas de alta utilização e desempenho no Cisco Quantum Flow Processor (QFP) podem ser observados em um roteador Cisco quando há uma combinação de fluxos de tráfego NAT e não NAT presentes na mesma interface. Isso também pode levar a outros problemas de desempenho, como erros de interface ou lentidão.

Note: O QFP está localizado no Embedded Services Processor (ESP) e é responsável pelo plano de dados e processamento de pacotes para todos os fluxos de entrada e saída de tráfego, que pode ser físico ou virtualizado, dependendo da plataforma.

Sintomas

É importante validar e confirmar esses sintomas a partir do roteador para identificar esse comportamento:

1. Alertas de carga QFP alta. Esses alertas aparecem quando a carga excede o limite de 80%.

```
Feb 8 08:02:25.147 mst: %IOSXE_QFP-2-LOAD_EXCEED: Slot: 0, QFP:0, Load 81% exceeds the setting threshol
Feb 8 08:04:15.149 mst: %IOSXE_QFP-2-LOAD_RECOVER: Slot: 0, QFP:0, Load 59% recovered.
```

Note: Você também pode executar o comando show platform hardware qfp ative datapath usage summary para revelar a carga no QFP e as taxas de tráfego.

```
Router# show platform hardware qfp active datapath utilization summary
  CPP 0: Subdev 0            5 secs        1 min        5 min       60 min
Input:  Priority (pps)            0            0            0            0
                 (bps)           96           32           32           32
    Non-Priority (pps)       327503       526605       552898       594269
                 (bps)   1225600520   2664222472   2867573720   2960588728
           Total (pps)       327503       526605       552898       594269
                 (bps)   1225600616   2664222504   2867573752   2960588760
Output: Priority (pps)            6            7            7            7
                 (bps)         8576         9992         9320         9344
```

```
    Non-Priority (pps)       327715       526839       553128       594506
                 (bps)   1257522072   2714335584   2920005904   3016943800
           Total (pps)       327721       526846       553135       594513
                 (bps)   1257530648   2714345576   2920015224   3016953144
Processing: Load (pct)           99           72           34           19
```

2. Erros de interface. Os pacotes podem ser descartados devido à pressão contrária Se houver alta utilização de QFP. Nesses casos, Overruns e Quedas de Entrada são comumente observados nas interfaces. Para exibir essas informações, você pode executar o comando show interfaces.

```
Router# show interface gigabitEthernet 0/0/1
GigabitEthernet0/0/1 is up, line protocol is up
  Hardware is ISR4351-3x1GE, address is e41f.7b59.cba1 (bia e41f.7b59.cba1)
  Description: ### LAN Interface ###
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 2/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  1., loopback not set
  Keepalive not supported
  Full Duplex, 1000Mbps, link type is force-up, media type is LX
  output flow-control is on, input flow-control is on
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:02, output 00:06:47, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  30 second input rate 9390000 bits/sec, 2551 packets/sec
  30 second output rate 1402000 bits/sec, 1323 packets/sec
     368345166434 packets input, 199203081647360 bytes, 0 no buffer
     Received 159964 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     2884115457 input errors, 0 CRC, 0 frame, 2884115457 overrun, 0 ignored
     0 watchdog, 3691484 multicast, 0 pause input
     220286824008 packets output, 32398293188401 bytes, 0 underruns
     0 output errors, 0 collisions, 4 interface resets
     3682606 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     21 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

3. Em alguns cenários, os usuários podem reclamar da lentidão na rede.

Recurso Packet Trace

- O Packet Trace é uma ferramenta que fornece informações detalhadas de como os pacotes de dados são processados pelas plataformas Cisco IOS XE.
- Ele tem 3 níveis de inspeção, que são contabilidade, resumo e caminho de dados. O nível de inspeção é baseado no estado de condição da plataforma de depuração.

- Você pode obter informações como:

- Interface de entrada e saída
- Estado do pacote
- Carimbos de data/hora
- Rastreamento de pacotes

Note: Configurar o caminho de dados consome mais recursos de processamento de pacotes, que são refletidos apenas nos pacotes que correspondem à condição do filtro.

Mais detalhes sobre o Rastreamento de Pacotes na Solução de Problemas com o Recurso de Rastreamento de Pacotes do Datapath do Cisco IOS XE

Configuração básica do Packet Trace

Este é um exemplo de uma configuração básica do Packet Trace com inspeção no nível do Caminho de Dados. Ele coleta 8.192 pacotes de forma circular (substitui pacotes antigos), cria uma cópia de cada pacote da Camada 3 que chega e deixa a interface GigabitEthernet 0/0/1.

```
Router# debug platform packet-trace packet 8192 circular fia-trace data-size 2048
Router# debug platform packet-trace copy packet both L3 size 64
Router# debug platform condition interface gigabitEthernet 0/0/1 both
Router# debug platform condition start
Router# debug platform condition stop
```

Você pode verificar os resultados do Packet Trace com esses comandos.

```
Router# show platform packet-trace summary
Router# show platform packet-trace packet all
```

Na captura do Packet Trace, você pode observar que o recurso NAT consome mais recursos do que o esperado. No próximo exemplo, você pode ver que o tempo decorrido para o recurso IPV4_NAT_INPUT_FIA é significativamente maior do que o tempo decorrido de outros recursos. Esse comportamento geralmente indica que o QFP leva mais tempo para processar esse recurso e, como resultado, mais recursos do QFP são usados para NAT.

```
Packet: 161         CBUG ID: 161
Summary
  Input     : GigabitEthernet0/0/1
  Output    : GigabitEthernet0/0/2.1730
  State     : FWD
  Timestamp
    Start   : 25136781447706429 ns (02/10/2024 00:25:49.584050 UTC)
```

```
    Stop    : 25136781447993237 ns (02/10/2024 00:25:49.584337 UTC)



Feature: IPV4_NAT_INPUT_FIA   <<<<<<<<<<<<
  Entry       : Input - 0x700162ac
  Input       : GigabitEthernet0/0/1
  Output      :



  Lapsed time : 1873376 ns     <<<<<<<<<<<<



Feature: IPV4_INPUT_IPOPTIONS_PROCESS
  Entry       : Input - 0x70016344
  Input       : GigabitEthernet0/0/1
  Output      : GigabitEthernet0/0/2.1730
  Lapsed time : 64 ns
```

O que é o Gatekeeper NAT?

Nas plataformas de roteamento Cisco IOS XE, o recurso Network Address Translation (NAT) Gatekeeper é ativado por padrão. O NAT Gatekeeper foi originalmente criado para impedir fluxos não-NAT-ed para usar recursos de processamento excessivos para criar uma conversão NAT. O NAT Gatekeeper cria dois caches pequenos para a direção de dentro para fora e para outra direção com base no endereço de origem. Cada entrada de cache consiste em um endereço de origem, um ID de roteamento e encaminhamento virtual (VRF), um valor de temporizador (usado para invalidar a entrada) e um contador de quadros.

O alto volume de tráfego não NAT em uma interface NAT consome uma grande quantidade de recursos e causa picos de utilização de QFP. A Cisco recomenda que os clientes não devem ter fluxos NAT e não NAT na mesma interface sempre que possível.

Verifique o Gatekeeper NAT

As estatísticas do gatekeeper NAT podem ser verificadas com os comandos show platform hardware qfp ative feature nat datapath { gatein | atividade de gateway }. Mostra o tamanho do cache, o número de acertos, erros, entradas antigas, adicionadas e ativas no cache.Normalmente, se houver um número alto de erros e se esse número aumentar

rapidamente em um curto período de tempo, isso indica que um grande número de fluxos Não Nacionados não é adicionado ao cache. Esse comportamento faz com que esses fluxos sejam processados pelo QFP dentro do fluxo de trabalho de NAT, e isso pode aumentar em alta utilização do QFP.

```
Router# show platform hardware qfp active feature nat datapath gatein activity
Gatekeeper on
def mode Size 8192, Hits 191540578459, Miss 3196566091, Aged 1365537 Added 9 Active 7

Router# show platform hardware qfp active feature nat datapath gateout activity
Gatekeeper on
def mode Size 8192, Hits 448492109001, Miss 53295038401, Aged 149941327 Added 603614728 Active 1899
```

Solução alternativa/correção

Na maioria dos ambientes, a funcionalidade do gatekeeper do NAT funciona bem e não causa problemas. No entanto, se você tiver esse problema, há algumas maneiras de resolvê-lo.

Solução 1

Para esses tipos de problemas, a Cisco recomenda separar o tráfego NATed e não NATed da mesma interface. Ele pode ser usado em diferentes interfaces ou dispositivos de rede.

Solução 2

Aumente o tamanho do cache no recurso NAT Gatekeeper para reduzir o número de erros do gatekeeper.

O próximo exemplo mostra como ajustar o Gatekeeper em um roteador Cisco. Observe que esse valor deve ser representado em potências de 2. Caso contrário, o valor será automaticamente definido para o próximo tamanho inferior.

```
Router(config)# ip nat service gatekeeper
Router(config)# ip nat settings gatekeeper-size 65536
```

Note: Ajustar o tamanho do cache pode custar memória suficiente dentro do QFP, portanto, otimize seu uso. Tente ajustar esse valor gradualmente e comece com o valor mais próximo possível da configuração padrão.

Após executar uma das soluções descritas, é recomendável monitorar esses dois parâmetros para confirmar se o problema foi resolvido:

1. Verifique se a utilização do QFP diminuiu.

2. Verifique se o número de erros não continua a aumentar.

Summary

O recurso NAT Gatekeeper pode melhorar o desempenho do roteador quando há fluxos não NAT em uma interface NAT. Isso geralmente acontece quando o NAT converte alguns fluxos NAT quando, ao mesmo tempo, fluxos não NAT passam pela mesma interface. Na maioria dos ambientes, o recurso NAT Gatekeeper não causa nenhum impacto no roteador. No entanto, é importante ajustar essa característica se necessário, cuidadosamente a fim de evitar efeitos colaterais.

Informações Relacionadas

- O NAT ASR1K falha intermitentemente ao converter alguns pacotes
- Solucionar problemas com o recurso de rastreamento de pacote de caminho de dados do Cisco IOS XE
- Suporte técnico e downloads da Cisco

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.