Problemen met hoog QFP-gebruik oplossen vanwege NAT Gatekeeper-standaardconfiguratie

Inhoud

Inleiding

In dit document wordt beschreven hoe het gebruik van High Quantum Flow Processor (QFP) op routeringsplatforms kan worden geïdentificeerd en opgelost als gevolg van een combinatie van NATed- en niet-NATed-verkeer.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van Cisco IOS® XE packet forwarding architectuur
- Basiservaring met Packet Trace-functie

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies. Het is van toepassing op elk Cisco IOS XE-routeringsplatform met fysieke/gevirtualiseerde QFP zoals ASR1000, ISR4000, ISR1000, Cat8000 of Cat8000v.

Dit document is gebaseerd op Cisco IOS XE-apparaten in autonome modus, SDWAN (controller) of SD-routering kan een vergelijkbare logica volgen, maar de specificaties kunnen anders zijn.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Problemen met hoge benutting en prestaties op de Cisco Quantum Flow Processor (QFP) kunnen worden waargenomen op een Cisco-router wanneer er een mix van NATed- en Non-NAT-verkeersstromen aanwezig is op dezelfde interface. Dit kan ook leiden tot andere prestatieproblemen zoals interfacefouten of traagheid.

Opmerking: De QFP bevindt zich op de Embedded Services Processor (ESP) en is verantwoordelijk voor het gegevensvlak en de pakketverwerking voor alle inkomende en uitgaande verkeersstromen, dit kan fysiek of gevirtualiseerd zijn, afhankelijk van het platform.

Symptomen

Het is belangrijk om deze symptomen van de router te valideren en te bevestigen om dit gedrag te identificeren:

1. Waarschuwingen voor hoge QFP-belasting. Deze waarschuwingen worden weergegeven wanneer de belasting de drempel van 80% overschrijdt.

```
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.
```

Opmerking: U kunt ook de opdracht show platform hardware qfp active datapath utilization summary uitvoeren om de belasting op de QFP en de verkeerssnelheden weer te geven.

```
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. Interfacefouten. Pakketten kunnen worden weggelaten als gevolg van tegendruk als er een hoog QFP-gebruik is. In dergelijke gevallen worden Overruns en Input Drops vaak waargenomen op de interfaces. Als u deze informatie wilt weergeven, kunt u de opdracht interfaces weergeven uitvoeren.

```
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. In sommige scenario's kunnen gebruikers klagen over traagheid op het netwerk.

Packet Trace-functie

- Packet Trace is een tool die gedetailleerde informatie biedt over hoe gegevenspakketten worden verwerkt door de Cisco IOS XE-platforms.
- Het heeft 3 niveaus van inspectie die boekhouding, samenvatting en gegevenspad zijn. Het inspectieniveau is gebaseerd op de foutopsporingsstatus van het platform.

- U kunt informatie verkrijgen zoals:
    - In- en uitvoerinterface
    - Packet-status
    - tijdstempels
    - Packet Trace

Opmerking: het gegevenspad configureren verbruikt meer bronnen voor pakketverwerking, wat alleen wordt weergegeven op de pakketten die overeenkomen met de filtervoorwaarde.

Meer informatie over Packet Trace bij het oplossen van problemen met de Cisco IOS XE Datapath Packet Trace-functie

Basic Packet Trace Configuration

Dit is een voorbeeld van een eenvoudige Packet Trace-configuratie met gegevenspadniveaucontrole. Het verzamelt 8192 pakketten op een cirkelvormige manier (overschrijft oude pakketten), maakt een kopie van elk pakket van Layer 3 dat aankomt en verlaat 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
```

U kunt de resultaten van Packet Trace controleren met deze opdrachten.

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

Bij Packet Trace-vastlegging kunt u zien dat de NAT-functie meer bronnen verbruikt dan verwacht. In het volgende voorbeeld kunt u zien dat de verstreken tijd voor de IPV4_NAT_INPUT_FIA-functie aanzienlijk groter is dan de verstreken tijd van andere functies. Dit gedrag geeft meestal aan dat het QFP meer tijd kost om deze functie te verwerken en dat als gevolg daarvan meer middelen uit het QFP worden gebruikt voor 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
```

Wat is de NAT Gatekeeper

In Cisco IOS XE Routing Platforms is de functie Network Address Translation (NAT) Gatekeeper standaard ingeschakeld. NAT Gatekeeper is oorspronkelijk gemaakt om te voorkomen dat niet-NAT-ed stromen te veel verwerkingsbronnen gebruiken om een NAT-vertaling te maken. NAT Gatekeeper maakt twee kleine caches voor de binnen- naar buitenrichting en voor andere richting op basis van het bronadres. Elk cacheitem bestaat uit een bronadres, een Virtual Routing and Forwarding (VRF)-ID, een timerwaarde (die wordt gebruikt om het item ongeldig te maken) en een frameteller.

Een groot volume niet-NATed-verkeer op een NATed-interface verbruikt een grote hoeveelheid middelen en veroorzaakt pieken in het gebruik van QFP. Cisco raadt klanten aan om waar mogelijk geen NAT-ed en niet-NAT-ed stromen op dezelfde interface te hebben.

Controleer de NAT Gatekeeper

De NAT Gatekeeper Statistics kan worden gecontroleerd met de opdrachten tonen platform

hardware qfp actieve functie nat datapath { gatein | gateout } activiteit. Dit toont de grootte van de cache, het aantal hits, missers, verouderde, toegevoegde en actieve items in de cache.Meestal, als er een hoog aantal missers is en als dit aantal snel toeneemt in een korte periode van tijd, geeft dit aan dat een enorm aantal niet-Natted-stromen niet aan de cache worden toegevoegd. Dit gedrag zorgt ervoor dat deze stromen worden verwerkt door de QFP binnen de NAT-workflow, en dit kan oplopen bij een hoog QFP-gebruik.

```
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
```

Oplossing/oplossing

In de meeste omgevingen werkt de NAT-poortwachterfunctionaliteit prima en veroorzaakt deze geen problemen. Als u echter tegen dit probleem aanloopt, zijn er een paar manieren om het op te lossen.

Oplossing 1

Voor dit soort problemen beveelt Cisco aan om het NATed- en niet-NATed-verkeer van dezelfde interface te scheiden. Het kan worden gebruikt in verschillende interfaces of netwerkapparaten.

Oplossing 2

Verhoog de grootte van de cache op de NAT Gatekeeper-functie om het aantal missers van de poortwachter te verminderen.

In het volgende voorbeeld wordt getoond hoe u de Gatekeeper op een Cisco-router kunt aanpassen. Let op: deze waarde moet worden weergegeven in machten van 2. Anders wordt de waarde automatisch ingesteld op de volgende lagere grootte.

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

Opmerking: het aanpassen van de cachegrootte kan het geheugen binnen de QFP kosten, zodat het gebruik ervan wordt geoptimaliseerd. Probeer deze waarde geleidelijk aan te passen en begin met de dichtstbijzijnde mogelijke waarde bij de standaardinstelling.

Nadat een van de beschreven oplossingen is uitgevoerd, wordt aanbevolen deze twee parameters te controleren om te bevestigen dat het probleem is opgelost:

1. Controleer of het gebruik van het QFP is afgenomen.
2. Controleer of het aantal missers niet blijft toenemen.

Samenvatting

De NAT Gatekeeper-functie kan de prestaties van de router verbeteren wanneer er niet-NATed-stromen op een NATed-interface zijn. Dit gebeurt meestal wanneer NAT sommige NATed-stromen vertaalt wanneer tegelijkertijd niet-NATed-stromen door dezelfde interface gaan. In de meeste omgevingen heeft de NAT Gatekeeper-functie geen invloed op de router. Het is echter belangrijk om deze functie indien nodig zorgvuldig aan te passen om bijwerkingen te voorkomen.

Gerelateerde informatie

- ASR1K NAT slaagt er met tussenpozen niet in om sommige pakketten te vertalen
- Problemen oplossen met de Cisco IOS XE Datapath Packet Trace-functie
- Cisco Technical Support en downloads

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.