Fehlerbehebung bei hoher QFP-Auslastung aufgrund der NAT Gatekeeper-Standardkonfiguration

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie die QFP-Auslastung (High Quantum Flow Processor) auf Routing-Plattformen identifiziert und behoben werden kann, die durch eine Kombination aus NAT- und Nicht-NAT-Datenverkehr verursacht wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundkenntnisse der Paketweiterleitungsarchitektur Cisco IOS® XE
- Grundlegende Funktionen der Packet Trace-Funktion

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt. Sie gilt für alle Cisco IOS XE Routing-Plattformen mit physischem/virtualisiertem QFP, wie ASR1000,

ISR4000, ISR1000, Cat8000 oder Cat8000v.

Dieses Dokument basiert auf Cisco IOS XE-Geräten im Autonomous-Mode, SDWAN (Controller) oder SD-Routing kann einer ähnlichen Logik folgen, die Details können jedoch unterschiedlich sein.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Hohe Auslastungs- und Leistungsprobleme beim Cisco Quantum Flow Processor (QFP) können auf einem Cisco Router beobachtet werden, wenn auf derselben Schnittstelle eine Mischung aus NAT- und Nicht-NAT-Datenverkehrsflüssen vorhanden ist. Dies kann auch zu anderen Leistungsproblemen wie Schnittstellenfehlern oder einer Verlangsamung führen.

Anmerkung: Der QFP befindet sich auf dem Embedded Services Processor (ESP) und ist für die Datenebene und die Paketverarbeitung für den gesamten ein- und ausgehenden Datenverkehr zuständig. Dieser kann je nach Plattform entweder physisch oder virtualisiert sein.

Symptome

Um dieses Verhalten zu identifizieren, müssen diese Symptome vom Router validiert und bestätigt werden:

1. Hochwertige QFP-Lastwarnungen. Diese Warnungen werden angezeigt, wenn die Last den Schwellenwert von 80 % überschreitet.

```
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.
```

Anmerkung: Sie können auch den Befehl show platform hardware qfp active datapath usage summary ausführen, um die Auslastung des QFP und die Datenverkehrsraten anzuzeigen.

```
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. Schnittstellenfehler. Bei hoher QFP-Auslastung können Pakete aufgrund von Gegendruck verworfen werden. In diesen Fällen werden Überläufe und Eingabetropfen häufig an den Schnittstellen beobachtet. Um diese Informationen anzuzeigen, können Sie den Befehl show interfaces ausführen.

```
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 einigen Szenarien können sich Benutzer über die Langsamkeit des Netzwerks beschweren.

Packet Trace-Funktion

- Packet Trace ist ein Tool, das detaillierte Informationen darüber bereitstellt, wie Datenpakete von den Cisco IOS XE-Plattformen verarbeitet werden.

- Es verfügt über drei Inspektionsebenen: Buchhaltung, Zusammenfassung und Datenpfad. Die Inspektionsebene basiert auf dem Zustand der Debugplattform.
- Sie können folgende Informationen erhalten:
    - Eingabe- und Ausgabeschnittstelle
    - Paketstatus
    - Zeitstempel
    - Paketnachverfolgung

Anmerkung: Der konfigurierte Datenpfad benötigt mehr Paketverarbeitungsressourcen, was sich nur in den Paketen widerspiegelt, die mit der Filterbedingung übereinstimmen.

Weitere Details zu Packet Trace bei der Fehlerbehebung mit der Cisco IOS XE DataPath Packet Trace-Funktion

Grundlegende Paketablaufverfolgungskonfiguration

Dies ist ein Beispiel für eine grundlegende Packet Trace-Konfiguration mit Prüfung auf Datenpfadebene. Er sammelt 8.192 Pakete in einem Rundlauf (überschreibt alte Pakete), erstellt eine Kopie jedes Pakets von Layer 3, das die Schnittstelle GigabitEthernet 0/0/1 erreicht und verlässt.

```
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
```

Sie können die Ergebnisse von Packet Trace mit diesen Befehlen überprüfen.

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

Bei der Pakettetrace-Erfassung können Sie beobachten, dass die NAT-Funktion mehr Ressourcen verbraucht als erwartet. Im nächsten Beispiel können Sie sehen, dass die verstrichene Zeit für die IPV4_NAT_INPUT_FIA-Funktion wesentlich größer ist als die verstrichene Zeit für andere Funktionen. Dieses Verhalten zeigt in der Regel an, dass der QFP mehr Zeit benötigt, um diese Funktion zu verarbeiten, und dass daher mehr Ressourcen aus dem QFP für NAT verwendet werden.

```
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
```

Was ist der NAT Gatekeeper?

Auf Cisco IOS XE Routing-Plattformen ist die Funktion Network Address Translation (NAT) Gatekeeper standardmäßig aktiviert. NAT Gatekeeper wurde ursprünglich entwickelt, um zu verhindern, dass Datenflüsse ohne NAT übermäßige Verarbeitungsressourcen für die NAT-Übersetzung nutzen. NAT Gatekeeper erstellt auf Basis der Quelladresse zwei kleine Caches für die Innen- zur Außenrichtung und für die andere Richtung. Jeder Cache-Eintrag besteht aus einer Quelladresse, einer VRF-ID (Virtual Routing and Forwarding), einem Timer-Wert (mit dem der Eintrag ungültig gemacht wird) und einem Frame-Zähler.

Ein hohes Volumen an Datenverkehr ohne NAT auf einer NAT-Schnittstelle belegt einen hohen Ressourcenaufwand und verursacht QFP-Auslastungsspitzen. Cisco empfiehlt, NAT- und Nicht-NAT-Flows möglichst nicht auf derselben Schnittstelle zu verwenden.

NAT Gatekeeper überprüfen

Die NAT-Gatekeeper-Statistik kann mithilfe der Befehle show platform hardware qfp active feature nat datapath { gatein | Gateway-Aktivität. Dies zeigt die Größe des Caches, die Anzahl von Treffern, Fehlschlägen, veralteten, hinzugefügten und aktiven Einträgen im Cache.Normalerweise, wenn es eine hohe Anzahl von Fehlschlägen gibt und wenn diese Anzahl schnell in einem kurzen Zeitraum zunimmt, weist dies darauf hin, dass eine große Anzahl von Not-Natted-Flüssen nicht zum Cache hinzugefügt wird. Dieses Verhalten führt dazu, dass diese Datenflüsse vom QFP innerhalb des NAT-Workflows verarbeitet werden. Dies kann zu einer hohen QFP-Auslastung führen.

```
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
```

Problemumgehung/Fehlerbehebung

In den meisten Umgebungen funktioniert die NAT-Gatekeeper-Funktion einwandfrei und verursacht keine Probleme. Wenn Sie jedoch auf dieses Problem stoßen, gibt es einige Möglichkeiten, es zu beheben.

Lösung 1

Für diese Art von Problemen empfiehlt Cisco, den NAT-basierten und den nicht-NAT-basierten Datenverkehr von derselben Schnittstelle zu trennen. Es kann entweder in verschiedenen Schnittstellen oder Netzwerkgeräten verwendet werden.

Lösung 2

Vergrößern Sie den Cache der NAT Gatekeeper-Funktion, um die Anzahl der Fehlschläge vom Gatekeeper zu verringern.

Das nächste Beispiel zeigt, wie der Gatekeeper auf einem Cisco-Router angepasst wird. Beachten Sie, dass dieser Wert in Potenzen von 2 dargestellt werden muss. Andernfalls wird der Wert automatisch auf die nächstkleinere Größe gesetzt.

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

Anmerkung: Die Anpassung der Cache-Größe kann extrem viel Speicher innerhalb des QFP kosten, sodass seine Nutzung optimiert wird. Versuchen Sie, diesen Wert schrittweise anzupassen, und beginnen Sie mit dem nächstmöglichen Wert, um die Standardeinstellung einzustellen.

Nach der Durchführung einer der beschriebenen Lösungen wird empfohlen, die folgenden beiden Parameter zu überwachen, um sicherzustellen, dass das Problem behoben wurde:

1. Überprüfen Sie, ob die QFP-Auslastung abgenommen hat.
2. Stellen Sie sicher, dass die Anzahl der Fehlschläge nicht weiter zunimmt.

Zusammenfassung

Die NAT-Gatekeeper-Funktion kann die Leistung des Routers verbessern, wenn auf einer NAT-Schnittstelle Datenflüsse ohne NAT vorliegen. Dies geschieht normalerweise, wenn NAT einige NATed-Flows übersetzt, wenn gleichzeitig Nicht-NATed-Flows durch dieselbe Schnittstelle fließen. In den meisten Umgebungen hat die NAT Gatekeeper-Funktion keine Auswirkungen auf den Router. Es ist jedoch wichtig, diese Funktion bei Bedarf anzupassen, um Nebenwirkungen zu vermeiden.

Zugehörige Informationen

- ASR1K NAT übersetzt gelegentlich einige Pakete nicht
- Fehlerbehebung mit der Packet Trace-Funktion von Cisco IOS XE
- Technischer Support und Downloads von Cisco

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.