Resolución de problemas de uso elevado de QFP debido a la configuración predeterminada del gatekeeper NAT

Contenido

Introducción

Este documento describe cómo identificar y resolver la utilización del procesador de flujo cuántico alto (QFP) en las plataformas de ruteo causada por la mezcla de tráfico NATed y no NATed.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos de la arquitectura de reenvío de paquetes Cisco IOS® XE
- Experiencia básica con la función de seguimiento de paquetes

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware. Se aplica a cualquier plataforma de routing Cisco IOS XE con QFP físico/virtualizado como ASR1000, ISR4000, ISR1000, Cat8000 o Cat8000v.

Este documento se basa en los dispositivos Cisco IOS XE en modo autónomo, SDWAN (controlador) o el ruteo SD puede seguir una lógica similar pero los aspectos específicos pueden ser diferentes.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Se pueden observar problemas de alto uso y rendimiento en el procesador Quantum Flow Processor (QFP) de Cisco en un router de Cisco cuando hay una mezcla de flujos de tráfico NAT y no NAT presentes en la misma interfaz. Esto también puede ocasionar otros problemas de rendimiento, como errores de interfaz o lentitud.

Nota: El QFP se encuentra en el procesador de servicios integrados (ESP) y se encarga del plano de datos y del procesamiento de paquetes para todos los flujos de tráfico entrante y saliente, que pueden ser físicos o virtualizados en función de la plataforma.

Síntomas

Es importante validar y confirmar estos síntomas desde el router para identificar este comportamiento:

1. Alertas de carga QFP alta. Estas alertas aparecen cuando la carga supera el umbral del 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.
```

Nota: También puede ejecutar el comando show platform hardware qfp active datapath utilization summary para revelar la carga en el QFP y las velocidades de tráfico.

```
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. Errores de interfaz. Los paquetes se pueden perder debido a la contrapresión si hay una alta utilización de QFP. En tales casos, se observan con frecuencia desbordamientos y caídas de entrada en las interfaces. Para mostrar esta información, puede ejecutar el 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. En algunos escenarios, los usuarios pueden quejarse de la lentitud en la red.

Característica de seguimiento de paquetes

- Packet Trace es una herramienta que proporciona información detallada sobre cómo las plataformas Cisco IOS XE procesan los paquetes de datos.
- Tiene 3 niveles de inspección que son contabilidad, resumen y ruta de datos. El nivel de inspección se basa en el estado de la condición de la plataforma de depuración.

- Puede obtener información como:

- Interfaz de entrada y salida
- Estado del paquete
- Marcas de tiempo
- Seguimiento de paquetes

Nota: La ruta de datos de configuración consume más recursos de procesamiento de paquetes, lo que sólo se refleja en los paquetes que coinciden con la condición de filtro.

Más detalles sobre Packet Trace en Troubleshooting con la Función Datapath Packet Trace de Cisco IOS XE

Configuración básica de seguimiento de paquetes

Este es un ejemplo de una configuración básica de Rastreo de paquetes con inspección de nivel de Trayectoria de datos. Recopila paquetes 8192 de forma circular (sobrescribe paquetes antiguos), crea una copia de cada paquete de la capa 3 que llega y sale de la interfaz 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
```

Puede verificar los resultados de Rastreo de paquetes con estos comandos.

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

En la captura de seguimiento de paquetes, puede observar que la función NAT consume más recursos de los esperados. En el siguiente ejemplo, puede ver que el tiempo transcurrido para la función IPV4_NAT_INPUT_FIA es significativamente mayor que el tiempo transcurrido de otras funciones. Este comportamiento suele indicar que el QFP tarda más tiempo en procesar esta función y, como resultado, se utilizan más recursos del QFP 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
```

¿Qué es el Gatekeeper NAT?

En las plataformas de routing de Cisco IOS XE, la función NAT (Network Address Translation) Gatekeeper está habilitada de forma predeterminada. NAT Gatekeeper se creó originalmente para evitar que los flujos que no son de NAT utilicen recursos de procesamiento excesivos para crear una traducción NAT. NAT Gatekeeper crea dos pequeñas memorias caché para la dirección interna a la dirección externa y para otra dirección basada en la dirección de origen. Cada entrada de caché consta de una dirección de origen, un ID de reenvío y routing virtual (VRF), un valor de temporizador (utilizado para invalidar la entrada) y un contador de tramas.

El alto volumen de tráfico no NATed en una interfaz NATed consume una gran cantidad de recursos y provoca picos de utilización QFP. Cisco recomienda que los clientes no tengan flujos NAT-ed y no NAT-ed en la misma interfaz siempre que sea posible.

Verifique el Gatekeeper NAT

Las estadísticas de NAT Gatekeeper se pueden verificar con los comandos show platform hardware qfp active feature nat datapath { gatein | gateout }activity. Muestra el tamaño de la

caché, el número de aciertos, faltas, entradas antiguas, agregadas y activas en la caché. Normalmente, si hay un gran número de faltas y este número aumenta rápidamente en un breve período de tiempo, esto indica que un gran número de flujos no desatendidos no se agregan a la caché. Este comportamiento hace que estos flujos sean procesados por el QFP dentro del flujo de trabajo de NAT, y esto puede aumentar en una alta utilización de 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
```

Solución/Solución

En la mayoría de los entornos, la funcionalidad del gatekeeper NAT funciona bien y no causa problemas. Sin embargo, si se encuentra con este problema, hay algunas maneras de resolverlo.

Solución 1

Para este tipo de problemas, Cisco recomienda separar el tráfico NATed y el tráfico no NATed de la misma interfaz. Se puede utilizar en diferentes interfaces o dispositivos de red.

Solución 2

Aumente el tamaño de la memoria caché en la función de control de acceso NAT para reducir el número de errores del control de acceso.

El siguiente ejemplo muestra cómo ajustar el Gatekeeper en un router Cisco. Tenga en cuenta que este valor debe representarse en potencias de 2. De lo contrario, el valor se establece automáticamente en el siguiente tamaño inferior.

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

Nota: Ajustar el tamaño de la memoria caché puede costar memoria exmem dentro del QFP, por lo que debe optimizar su uso. Intente ajustar este valor gradualmente y comience con el valor más cercano posible al valor predeterminado.

Después de realizar una de las soluciones descritas, se recomienda monitorear estos dos parámetros para confirmar que el problema se ha resuelto:

1. Verifique que la utilización de QFP haya disminuido.
2. Verifique que el número de errores no siga aumentando.

Summary

La función NAT Gatekeeper puede mejorar el rendimiento del router cuando hay flujos no NATed en una interfaz NATed. Esto suele suceder cuando NAT traduce algunos flujos NATed cuando, al mismo tiempo, los flujos no NATed pasan a través de la misma interfaz. En la mayoría de los entornos, la función NAT Gatekeeper no causa ningún impacto en el router. Sin embargo, es importante ajustar esta función si es necesario, con cuidado para evitar efectos secundarios.

Información Relacionada

- ASR1K NAT falla intermitentemente al traducir algunos paquetes
- Resolución de Problemas con la Función Cisco IOS XE Datapath Packet Trace
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).