Risoluzione dei problemi di utilizzo QFP elevato dovuto alla configurazione predefinita Gatekeeper NAT

Sommario

Introduzione

Questo documento descrive come identificare e risolvere l'utilizzo di High Quantum Flow Processor (QFP) sulle piattaforme di routing causato dalla combinazione di traffico NAT e non NAT.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base dell'architettura di inoltro pacchetti Cisco IOS® XE
- Funzionalità di base con Packet Trace

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware. Si applica a tutte le piattaforme Cisco IOS XE di routing con QFP fisico/virtualizzato come ASR1000, ISR4000,

ISR1000, Cat8000 o Cat8000v.

Questo documento si basa sui dispositivi Cisco IOS XE in modalità autonoma, mentre SDWAN (controller) o SD-routing possono seguire una logica simile, ma le specifiche potrebbero essere diverse.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

È possibile rilevare problemi di utilizzo e prestazioni elevati sul Cisco Quantum Flow Processor (QFP) su un router Cisco quando sulla stessa interfaccia è presente una combinazione di flussi di traffico NAT e non NAT. Ciò può inoltre causare altri problemi di prestazioni, ad esempio errori dell'interfaccia o lentezza.

Nota: QFP si trova su ESP (Embedded Services Processor) ed è responsabile dell'elaborazione del piano dati e dei pacchetti per tutti i flussi di traffico in entrata e in uscita, che possono essere fisici o virtualizzati a seconda della piattaforma.

Sintomi

È importante convalidare e confermare questi sintomi dal router per identificare questo comportamento:

1. Avvisi di caricamento QFP elevati. Questi avvisi vengono visualizzati quando il carico supera la soglia dell'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: È inoltre possibile eseguire il comando show platform hardware qfp active datapath usage summary per visualizzare il carico sul QFP e le velocità del traffico.

```
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. Errori di interfaccia. I pacchetti possono essere scartati a causa della contropressione in caso di utilizzo QFP elevato. In questi casi, gli overrun e le perdite di input vengono in genere osservati sulle interfacce. Per visualizzare queste informazioni, è possibile eseguire il 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. In alcuni casi, gli utenti possono lamentarsi della lentezza della rete.

Funzione Packet Trace

- Packet Trace è uno strumento che fornisce informazioni dettagliate su come i pacchetti di dati vengono elaborati dalle piattaforme Cisco IOS XE.

- Dispone di 3 livelli di ispezione, ovvero contabilità, riepilogo e percorso dati. Il livello di ispezione è basato sullo stato della condizione della piattaforma di debug.
- È possibile ottenere informazioni quali:
    - Interfaccia di input e output
    - Stato pacchetto
    - Timestamp
    - Traccia pacchetto

Nota: La configurazione del percorso dati comporta l'utilizzo di una maggiore quantità di risorse di elaborazione, che si riflette solo sui pacchetti che soddisfano la condizione del filtro.

Ulteriori dettagli su Packet Trace in Risoluzione dei problemi con Cisco IOS XE Datapath Packet Trace Feature

Configurazione di base della traccia del pacchetto

Questo è un esempio di configurazione di base di Packet Trace con ispezione a livello di percorso dati. Raccoglie 8192 pacchetti in modo circolare (sovrascrive i pacchetti precedenti), crea una copia di ciascun pacchetto dal layer 3 che arriva e lascia l'interfaccia Gigabit Ethernet 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
```

È possibile controllare i risultati di Packet Trace con questi comandi.

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

Dall'acquisizione di Packet Trace, è possibile osservare che la funzionalità NAT utilizza più risorse del previsto. Nell'esempio seguente, il tempo di inattività della funzione IPV4_NAT_INPUT_FIA è notevolmente superiore a quello di altre funzionalità. Questo comportamento in genere indica che il QFP impiega più tempo per elaborare questa funzione e, di conseguenza, vengono utilizzate più risorse dal QFP per 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
```

Che cos'è NAT Gatekeeper

Nelle piattaforme di routing Cisco IOS XE, la funzione Network Address Translation (NAT) Gatekeeper è abilitata per impostazione predefinita. Il Gatekeeper NAT è stato originariamente creato per impedire a flussi non NAT di utilizzare risorse di elaborazione eccessive per creare una traduzione NAT. Gatekeeper NAT crea due piccole cache per la direzione interna-esterna e per l'altra direzione in base all'indirizzo di origine. Ogni voce della cache è costituita da un indirizzo di origine, un ID VRF (Virtual Routing and Forwarding), un valore del timer (utilizzato per invalidare la voce) e un contatore di frame.

Un volume elevato di traffico non NAT su un'interfaccia NAT consuma una quantità elevata di risorse e causa i picchi di utilizzo QFP. Cisco consiglia di non utilizzare flussi NAT e non NAT sulla stessa interfaccia, se possibile.

Controlla il Gatekeeper NAT

Le statistiche Gatekeeper NAT possono essere verificate con i comandi show platform hardware qfp active feature nat datapath { gateway | uscita }attività. Mostra la dimensione della cache, il numero di accessi riusciti, non riusciti, l'età, le voci aggiunte e le voci attive nella cache.In genere, se il numero di accessi non riusciti è elevato e aumenta rapidamente in un breve periodo di tempo, significa che alla cache non viene aggiunto un numero elevato di flussi non specificati. Questo comportamento causa l'elaborazione di questi flussi da parte di QFP all'interno del flusso di lavoro NAT e può determinare un elevato utilizzo di 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
```

Soluzione/correzione

Nella maggior parte degli ambienti, la funzionalità Gatekeeper NAT funziona correttamente e non causa problemi. Tuttavia, se si incontra questo problema, ci sono alcuni modi per risolverlo.

Soluzione 1

Per questi tipi di problemi, Cisco consiglia di separare il traffico NAT e il traffico non NAT dalla stessa interfaccia. Può essere utilizzato in interfacce o dispositivi di rete diversi.

Soluzione 2

Aumentare le dimensioni della cache sulla funzionalità Gatekeeper NAT per ridurre il numero di mancati riscontri da parte del gatekeeper.

Nell'esempio successivo viene mostrato come regolare il Gatekeeper su un router Cisco. Si noti che questo valore deve essere rappresentato in potenze di 2. In caso contrario, il valore viene automaticamente impostato sulla dimensione immediatamente inferiore.

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

Nota: La regolazione delle dimensioni della cache può comportare un costo eccessivo per la memoria all'interno di QFP, ottimizzandone l'utilizzo. Provare a regolare questo valore

gradualmente e iniziare con il valore più vicino possibile all'impostazione predefinita.

Dopo aver eseguito una delle soluzioni descritte, si consiglia di monitorare questi due parametri per verificare che il problema sia stato risolto:

1. Verificare che l'utilizzo di QFP sia diminuito.
2. Verificare che il numero di mancati riscontri non continui ad aumentare.

Riepilogo

La funzionalità Gatekeeper NAT può migliorare le prestazioni del router in caso di flussi non NAT su un'interfaccia NAT. Ciò si verifica in genere quando NAT converte alcuni flussi NATed quando, allo stesso tempo, i flussi non NAT passano attraverso la stessa interfaccia. Nella maggior parte degli ambienti, la funzione NAT Gatekeeper non causa alcun impatto sul router. Tuttavia, se necessario, è importante regolare questa funzione con attenzione per evitare effetti collaterali.

Informazioni correlate

- ASR1K NAT non riesce a tradurre alcuni pacchetti in modo intermittente
- Risoluzione dei problemi con la funzionalità Cisco IOS XE Datapath Packet Trace
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).