Dépannage de la forte utilisation due à la configuration par défaut du contrôleur d'accès NAT

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Symptômes

Fonctionnalité Packet Trace

- Configuration de base de Packet Trace

Qu'est-ce que NAT Gatekeeper ?

Vérifiez le contrôleur d'accès NAT

Solution/Correction

- Solution 1
- Solution 2

Résumé

Informations connexes

Introduction

Ce document décrit comment identifier et résoudre l'utilisation QFP élevée sur les plates-formes de routage causée par la combinaison du trafic NATed et non NATed.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de base de l'architecture de transfert de paquets Cisco IOS® XE
- Expérience de base avec la fonctionnalité Packet Trace

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques. Elle s'applique à toute plate-forme de routage Cisco IOS XE avec processeur physique/virtualisé à flux quantique élevé (QFP), comme ASR1000, ISR4000, ISR1000, Cat8000 ou Cat8000v.

Ce document est basé sur les périphériques Cisco IOS XE en mode autonome, SDWAN (contrôleur) ou le routage SD peut adhérer à une logique similaire, mais les spécificités peuvent être différentes.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Des problèmes d'utilisation et de performances élevés sur le processeur Cisco Quantum Flow Processor (QFP) peuvent être observés sur un routeur Cisco lorsqu'une combinaison de flux de trafic NAT et non NAT est présente sur la même interface. Cela peut également entraîner d'autres problèmes de performances, tels que des erreurs d'interface ou de la lenteur.

Remarque : Le QFP est situé sur le processeur de services intégrés (ESP) et il est chargé du plan de données et du traitement des paquets pour tous les flux de trafic entrant et sortant, qui peuvent être physiques ou virtualisés selon la plate-forme.

Symptômes

Il est important de valider et de confirmer ces symptômes à partir du routeur afin d'identifier ce comportement :

1.- Alertes de chargement QFP élevé. Ces alertes apparaissent lorsque la charge dépasse le seuil 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.
```

Remarque : Vous pouvez également exécuter la commande show platform hardware qfp active datapath use summary afin de révéler la charge sur le QFP et les débits de trafic.

```
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.- Erreurs d'interface. Les paquets peuvent être abandonnés en raison d'une contre-pression si l'utilisation du QFP est élevée. Dans ce cas, les dépassements et les pertes en entrée sont généralement observés sur les interfaces. Pour afficher ces informations, vous pouvez exécuter la commande 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.- Dans certains scénarios, les utilisateurs peuvent se plaindre de lenteur sur le réseau.

Fonctionnalité Packet Trace

Packet Trace est un outil qui fournit des informations détaillées sur la façon dont les paquets de données sont traités par les plates-formes Cisco IOS XE. Il possède 3 niveaux d'inspection qui sont la comptabilité, le résumé et le chemin des données. Le niveau d'inspection est basé sur l'état de la condition de la plate-forme de débogage.

Vous pouvez obtenir des informations telles que :

- Interface d'entrée et de sortie
- État du paquet
- Horodatages
- Suivi des paquets



Remarque : La configuration du chemin de données consomme davantage de ressources de traitement de paquets, ce qui n'est reflété que sur les paquets qui correspondent à la condition de filtre.

Plus de détails sur Packet Trace dans Dépannage avec la fonctionnalité Packet Trace de chemin de données de Cisco IOS XE.

Configuration de base de Packet Trace

Voici un exemple de configuration de base de Packet Trace avec inspection du niveau du chemin de données. Il collecte 8192 paquets de manière circulaire (remplace les anciens paquets), crée une copie de chaque paquet de la couche 3 qui arrive et quitte l'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
```

Vous pouvez vérifier les résultats de Packet Trace avec ces commandes.

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

À partir de la capture Packet Trace, vous pouvez observer que la fonctionnalité NAT consomme plus de ressources que prévu. Dans l'exemple suivant, vous pouvez voir que le temps écoulé pour la fonctionnalité IPV4_NAT_INPUT_FIA est beaucoup plus long que le temps écoulé pour les autres fonctionnalités. Ce comportement indique généralement que le QFP prend plus de temps pour traiter cette fonctionnalité et, par conséquent, que davantage de ressources du QFP sont utilisées pour la 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)
<snip>
  Feature: IPV4_NAT_INPUT_FIA   <<<<<<<<<<<<
    Entry       : Input - 0x700162ac
    Input       : GigabitEthernet0/0/1
    Output      : <unknown>
    Lapsed time : 1873376 ns     <<<<<<<<<<<<
<snip>
  Feature: IPV4_INPUT_IPOPTIONS_PROCESS
    Entry       : Input - 0x70016344
    Input       : GigabitEthernet0/0/1
    Output      : GigabitEthernet0/0/2.1730
    Lapsed time : 64 ns
```

Qu'est-ce que NAT Gatekeeper ?

Dans les plates-formes de routage Cisco IOS XE, la fonctionnalité de contrôleur d'accès NAT (Network Address Translation) est activée par défaut. Le contrôleur d'accès NAT a été créé à l'origine pour empêcher les flux non-NAT d'utiliser des ressources de traitement excessives pour créer une traduction NAT. NAT Gatekeeper crée deux petits caches pour la direction interne vers externe et pour l'autre direction en fonction de l'adresse source. Chaque entrée de cache se compose d'une adresse source, d'un ID de routage et de transfert virtuel (VRF), d'une valeur de minuteur (utilisée pour invalider l'entrée) et d'un compteur de trames.

Un volume élevé de trafic non-NATed sur une interface NATed consomme une grande quantité de ressources et provoque des pics d'utilisation QFP. Cisco recommande que les clients ne doivent pas avoir de flux NAT-ed et non-NAT-ed sur la même interface chaque fois que possible.

Vérifiez le contrôleur d'accès NAT

Les statistiques du portier NAT peuvent être vérifiées avec les commandes show platform hardware qfp active feature nat datapath { gatein | gateout } activity. Indique la taille du cache, le nombre d'occurrences, d'échecs, d'entrées obsolètes, ajoutées et actives dans le cache.Généralement, si le nombre d'échecs est élevé et que ce nombre augmente rapidement en un court laps de temps, cela indique qu'un grand nombre de flux Non-Natted n'est pas ajouté au cache. Ce comportement entraîne le traitement de ces flux par le QFP dans le workflow NAT, ce qui peut augmenter dans une utilisation QFP élevée.

```
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
```

Solution/Correction

Dans la plupart des environnements, la fonctionnalité NAT gatekeeper fonctionne correctement et ne pose aucun problème. Cependant, si vous rencontrez ce problème, il existe plusieurs façons de le résoudre.

Solution 1

Pour ce type de problèmes, Cisco recommande de séparer le trafic NATed et non NATed de la même interface. Il peut être utilisé dans différentes interfaces ou sur différents périphériques réseau.

Solution 2

Augmentez la taille du cache sur la fonctionnalité NAT Gatekeeper afin de réduire le nombre d'échecs du gatekeeper.

L'exemple suivant montre comment régler le contrôleur d'accès sur un routeur Cisco. Veuillez noter que cette valeur doit être représentée par des puissances de 2. Sinon, la valeur est automatiquement définie sur la taille inférieure suivante.

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

Remarque : Le réglage de la taille du cache peut coûter cher en mémoire exemplaire dans le QFP, donc optimiser son utilisation. Essayez d'ajuster cette valeur progressivement et commencez par la valeur la plus proche possible du paramètre par défaut.

Après avoir appliqué l'une des solutions décrites, il est recommandé de surveiller ces deux paramètres afin de confirmer que le problème a été résolu :

1.- Vérifiez que l'utilisation du QFP a diminué.

2.- Vérifiez que le nombre d'échecs ne continue pas à augmenter.

Résumé

La fonctionnalité NAT Gatekeeper peut améliorer les performances du routeur quand il y a des flux non-NATed sur une interface NATed. Cela se produit généralement lorsque NAT traduit certains flux NATed lorsque, en même temps, des flux non NATed passent par la même interface. Dans la plupart des environnements, la fonctionnalité NAT Gatekeeper n'a aucun impact sur le routeur. Cependant, il est important d'ajuster cette fonction si nécessaire, avec précaution afin d'éviter les effets secondaires.

Informations connexes

- La NAT ASR1K ne parvient pas à traduire certains paquets par intermittence
- Dépannage avec la fonctionnalité de suivi des paquets de données Cisco IOS XE
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.