Limitation de la plate-forme ASR1002 avec IPSec, Netflow, NBAR

Contenu

Introduction

Ce document décrit le problème de débit sur la plate-forme ASR1002 avec AVC (Application Visibility and Control) configuré avec la fonctionnalité IPSec sur le routeur.

Informations générales

Selon la documentation CCO, ASR10002 fournit un débit de 10 gbits/s pour le trafic de données normal, 4 Gbits/s avec la fonctionnalité IPSec activée. Mais une mise en garde est associée au débit de la plate-forme ASR1002. Netflow et NBAR sont deux fonctionnalités qui consomment beaucoup de ressources du processeur de flux Quantum (QFP) et réduisent ainsi la capacité de la carte ESP (Encapsulating Security Payload) à traiter davantage de trafic et donc à réduire le débit global du système. Grâce à la configuration d'AVC et à IPSec, le débit global de la plate-forme peut être gravement dégradé et peut entraîner d'énormes pertes de trafic.

Problème : Limitation de la plate-forme ASR1002 avec IPSec, Netflow, NBAR

Le problème a été détecté au début lorsque la bande passante a été mise à niveau avec le fournisseur et que les tests de bande passante étaient en cours. Initialement, un paquet de 1000 octets a été envoyé, ce qui s'est très bien passé, puis le test a été effectué avec des paquets de 512 octets, après quoi ils ont presque remarqué une perte de trafic de 80 %. Référez-vous à cette topologie de test de TP :

Exécutez ces fonctions :

- DMVPN sur IPSec
- Netflow
- NBAR (dans le cadre de l'instruction de correspondance de stratégie QoS)

Configuration

```
crypto isakmp policy 1
encr 3des
group 2
crypto isakmp policy 2
encr 3des
authentication pre-share
group 2
crypto isakmp key cisco123 address 0.0.0.0
crypto ipsec security-association replay disable
crypto ipsec transform-set remoteoffice-vpn esp-3des esp-sha-hmac
mode tunnel
crypto ipsec transform-set IPTerm-TransSet esp-3des esp-sha-hmac
mode tunnel
crypto ipsec profile IPTerminals-VPN
set transform-set IPTerm-TransSet
crypto ipsec profile vpn-dmvpn
set transform-set remoteoffice-vpn
!
<snip>
class-map match-any Test
match ip precedence 2
match ip dscp af21
match ip dscp af22
match ip dscp af23
match access-group name test1
 match protocol ftp
 match protocol secure-ftp
!
policy-map test
<snip>
!
interface Tunnel0
bandwidth 512000
ip vrf forwarding CorpnetVPN
ip address 10.1.1.1 255.255.255.0
no ip redirects
ip mtu 1350
```

```
 ip flow ingress
ip nhrp authentication 1dcBb
ip nhrp map multicast dynamic
ip nhrp network-id 1000
ip nhrp holdtime 600
ip nhrp shortcut
ip nhrp redirect
ip virtual-reassembly max-reassemblies 256
ip tcp adjust-mss 1310
ip ospf network point-to-multipoint
ip ospf hello-interval 3
ip ospf prefix-suppression
load-interval 30
qos pre-classify
tunnel source Loopback0
tunnel mode gre multipoint
tunnel key 1234
tunnel protection ipsec profile vpn-dmvpn
!
int gi 0/1/0
bandwidth 400000
ip address 12.12.12.1 255.255.255.252
load-interval 30
negotiation auto
ip flow ingress
service-policy output PM-1DC-AGGREGATE
!
```

Le DMVPN (Dynamic Multipoint VPN) se situe entre les deux routeurs ASR1K. Le trafic a été généré entre IXIA et IXIA sur le cloud DMVPN avec une taille de paquet de 512 octets à 50 000 pps. Un autre flux est configuré pour le trafic de transfert accéléré (EF) entre IXIA et IXIA

Avec le flux ci-dessus, nous avons remarqué une perte de trafic dans les deux flux pour près de 30 000 pps.

Observations

Il n'y a pas eu beaucoup de chutes de sortie incrémentant et pas beaucoup de chutes vues dans la classe EF ou d'autres classes sauf de la classe par défaut de la stratégie de service.

Des baisses ont été détectées dans QFP à l'aide de **la commande show platform hardware qfp active statistics baisses** et ont remarqué que ces baisses augmentaient rapidement.

```
RTR-1#show platform hardware qfp active statistics drop
------------------------------------------------------------------------------
Global Drop Stats Packets Octets
------------------------------------------------------------------------------
IpsecInput 300010 175636790
IpsecOutput 45739945 23690171340
TailDrop 552830109 326169749399

RTR-1#
RTR-1#show platform hardware qfp active statistics drop
------------------------------------------------------------------------------
Global Drop Stats Packets Octets
------------------------------------------------------------------------------
```

```
IpsecInput 307182 179835230
IpsecOutput 46883064 24282257670
TailDrop 552830109 326169749399

RTR-1#
```

D'autres pertes IPSec ont été vérifiées pour QFP à l'aide de la commande **show platform hardware qfp active feature ipsec data drops**

```
RTR-1#show platform hardware qfp active feature ipsec data drops
----------------------------------------------------------------------
Drop Type Name Packets
----------------------------------------------------------------------

28 IN_PSTATE_CHUNK_ALLOC_FAIL 357317


54 OUT_PSTATE_CHUNK_ALLOC_FAIL 51497757
66 N2_GEN_NOTIFY_SOFT_EXPIRY 4023610

RTR-1#
```

Il a été remarqué que le compteur de dépôt pour **IN_PSTATE_CHUNK_ALLOC_FAIL** correspondait à la valeur du compteur **IpsecInput** dans les pertes QFP et identique avec **IpsecOutput** correspondant au compteur **OUT_PSTATE_CHUNK_ALLOC_FAIL.**

Ce problème est détecté en raison du défaut logiciel n° CSCuf25027 .

Solution

Pour résoudre ce problème, désactivez la fonction NBAR (Network Based Application Recognition) et Netflow sur le routeur. Si vous voulez exécuter toutes les fonctionnalités et obtenir un meilleur débit, alors la meilleure option consiste à mettre à niveau vers ASR1002-X ou ASR1006 avec ESP-100.