Contenu

Introduction

Ce document décrit le problème avec le débit sur la plate-forme ASR1002 avec la visibilité d'application et le contrôle (AVC) configurés avec la caractéristique d'IPSec sur le routeur.

Informations générales

Selon la documentation CCO, ASR10002 fournit au débit 10 GBP pour le trafic de données normal, 4 GBP la fonction activée d'IPSec. Mais il y a une mise en garde reliée au débit sur la plate-forme ASR1002. Le NetFlow et les NBAR sont deux caractéristiques qui consomment beaucoup de ressources du processeur d'écoulement de Quantum (QFP) et réduisent ainsi le cabability de la carte de Protocole ESP (Encapsulating Security Payload) pour traiter plus de trafic et réduire de ce fait le débit de système global. Avec la configuration AVC avec IPSec, le débit global de plate-forme peut être sévèrement dégradé et peut faire face à la perte énorme du trafic.

Problème : Limite de la plate-forme ASR1002 avec IPSec, NetFlow, NBAR

Le problème était initiale notée quand la bande passante a été mise à jour avec le fournisseur et test de bande passante était exécutent. Au commencement le paquet de 1000 octets a été envoyé, qui a disparu parfaitement correct, puis l'essai a été réalisé avec 512 paquets d'octet après quoi ils ont presque noté la perte du trafic de 80%. Référez-vous à cette topologie d'essai en laboratoire :

Exécutez ces caractéristiques :

- DMVPN au-dessus d'IPSec
- NetFlow
- NBAR (en tant qu'élément de la déclaration 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 VPN multipoint dynamique (DMVPN) est entre les deux Routeurs ASR1k. Le trafic a été généré de l'IXIA à l'IXIA à travers le nuage DMVPN avec la longueur de paquet de 512 octets @ 50000 PPS. Un autre flot est configuré pour le trafic (E-F) expédié d'expédition de l'IXIA à l'IXIA

Avec le flot ci-dessus, nous avons noté la perte du trafic dans les deux flots pour jusqu'à presque 30000 PPS.

Observations

Il n'y avait pas beaucoup des suppressions de sortie incrémentant et pas beaucoup relâche vu dans la classe E-F ou d'autres classes excepté de la classe par défaut de la service-stratégie.

Les baisses trouvées dans QFP utilisant des **baisses de statistiques actives de qfp de matériel de show platform** et noté ces baisses incrémentaient 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 baisses d'IPSec étaient QFP vérifiés utilisant des **baisses actives de données d'ipsec de caractéristique de qfp de matériel de show platform de** commande

```
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#
```

On l'a noté que la baisse contre- pour le compteur **IN_PSTATE_CHUNK_ALLOC_FAIL** appariait la valeur **IpsecInput** contre- dans les baisses et mêmes QFP avec **IpsecOutput** s'assortissant avec le compteur **OUT_PSTATE_CHUNK_ALLOC_FAIL.**

Cette question est due vu au defect# CSCuf25027 de logiciel.

Solution

Le contournement à ce problème est de désactiver la configuration de NetFlow et de Reconnaissance d'application fondée sur le réseau (NBAR) sur le routeur. Si vous voulez exécuter toutes les caractéristiques et avoir un meilleur débit, alors mieux l'option est d'améliorer à ASR1002-X ou à ASR1006 avec ESP-100.