Limitação de plataforma ASR1002 com IPSec, Netflow, NBAR

Contents

Introduction

Este documento descreve o problema com o throughput na plataforma ASR1002 com Application Visibility and Control (AVC) configurado junto com o recurso IPSec no roteador.

Informações de Apoio

De acordo com a documentação do CCO, o ASR10002 oferece throughput de 10 gbps para tráfego de dados normal, 4 Gbps com recurso IPSec habilitado. Mas há uma advertência relacionada ao throughput na plataforma ASR1002. O Netflow e o NBAR são dois recursos que consomem muitos recursos do Quantum Flow Processor (QFP) e, portanto, reduzem a capacidade da placa ESP (Encapsulating Security Payload) para processar mais tráfego e, assim, reduzir o throughput geral do sistema. Com a configuração do AVC junto com o IPSec, o throughput geral da plataforma pode ser severamente degradado e pode enfrentar uma enorme perda de tráfego.

Problema: Limitação de plataforma ASR1002 com IPSec, Netflow, NBAR

O problema foi observado inicialmente quando a largura de banda foi atualizada com o provedor e o teste de largura de banda estava sendo executado. Inicialmente, um pacote de 1.000 bytes foi enviado, o que correu perfeitamente bem, então o teste foi realizado com pacotes de 512 bytes, após os quais quase perceberam uma perda de tráfego de 80%. Consulte esta topologia de teste de laboratório:

Execute estes recursos:

- DMVPN sobre IPSec
- Netflow
- NBAR (como parte da instrução de correspondência de política de QoS)

Configuração

```
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
!
```

O Dynamic Multipoint VPN (DMVPN) está entre os dois roteadores ASR1k. O tráfego foi gerado do IXIA para o IXIA na nuvem DMVPN com tamanho de pacote de 512 bytes a 50.000 pps. Outro fluxo é configurado para tráfego de encaminhamento expresso (EF - Expedited Forwarding) de IXIA para IXIA

Com o fluxo acima, percebemos perda de tráfego em ambos os fluxos para até quase 30.000 pps.

Observações

Não houve muitas quedas de saída incrementando e poucas quedas foram vistas na classe EF ou em outras classes, exceto da classe padrão da política de serviço.

Foram encontradas quedas no QFP usando **quedas de estatísticas ativas de qfp de hardware de plataforma** e essas quedas aumentaram rapidamente.

```
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#
```

Outras quedas de IPSec foram verificadas para QFP usando o comando **show platform hardware qfp ative 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#
```

Foi observado que o contador de queda para o contador **IN_PSTATE_CHUNK_ALLOC_FAIL** correspondia ao valor **IpsecInput** no QFP drops e o mesmo com **IpsecOutput** correspondente ao **OUT_PSTATE_CHUNK_ALLOC_FAIL** contador.

Esse problema é observado devido ao defeito de software# CSCuf25027 .

Solução

A solução para esse problema é desabilitar o recurso Netflow e Network Based Application Recognition (NBAR) no roteador. Se você quiser executar todos os recursos e ter um throughput melhor, a melhor opção é atualizar para ASR1002-X ou ASR1006 com ESP-100.