Limitación de la plataforma ASR1002 con IPSec, Netflow, NBAR

Contenido

Introducción

Este documento describe el problema con el rendimiento en la plataforma ASR1002 con Application Visibility and Control (AVC) configurada junto con la función IPSec en el router.

Antecedentes

Según la documentación de CCO, ASR10002 proporciona un rendimiento de 10 gbps para el tráfico de datos normal, 4 Gbps con la función IPSec activada. Sin embargo, existe una advertencia relacionada con el rendimiento de la plataforma ASR1002. Netflow y NBAR son dos funciones que consumen muchos recursos del procesador Quantum Flow Processor (QFP) y, por lo tanto, reducen la capacidad de cableado de la tarjeta Encapsulating Security Payload (ESP) para procesar más tráfico y, por lo tanto, reducir el rendimiento general del sistema. Con la configuración de AVC junto con IPSec, el rendimiento general de la plataforma se puede degradar gravemente y puede enfrentarse a una enorme pérdida de tráfico.

Problema: Limitación de la plataforma ASR1002 con IPSec, Netflow, NBAR

El problema se notó inicialmente cuando se actualizó el ancho de banda con el proveedor y se estaban realizando pruebas de ancho de banda. Inicialmente, se envió un paquete de 1000 bytes, que salió perfectamente bien, y luego la prueba se realizó con paquetes de 512 bytes, después de lo cual casi notaron una pérdida de tráfico del 80%. Consulte esta topología de prueba de laboratorio:

Ejecute estas funciones:

- DMVPN sobre IPSec
- Netflow
- NBAR (como parte de la declaración de coincidencia de política de QoS)

Configuración

```
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
!
```

La VPN multipunto dinámica (DMVPN) se encuentra entre los dos routers ASR1k. El tráfico se generó de IXIA a IXIA a través de la nube DMVPN con un tamaño de paquete de 512 bytes a 50000 pps. Otra secuencia se configura para el tráfico de reenvío acelerado (EF) de IXIA a IXIA

Con el flujo anterior, observamos pérdidas de tráfico en ambos flujos durante casi 30000 pps.

'Observaciones'

No hubo demasiadas caídas de salida que aumentaran y no se observaron muchas caídas en la clase EF u otras clases, excepto en la clase predeterminada de service-policy.

Se encontraron caídas en QFP usando **show platform hardware qfp active statistics drop** y se dio cuenta de que esas caídas aumentaban rápidamente.

```
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#
```

Se comprobaron otras caídas de IPSec para QFP mediante el comando **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#
```

Se observó que el contador de caídas para el contador **IN_PSTATE_CHUNK_ALLOC_FAIL** coincidía con el contador de valor **IpsecInput** en las caídas de QFP y lo mismo con **IpsecOutput** que coincide con el contador **OUT_PSTATE_CHUNK_ALLOC_FAIL**.

Este problema se ve debido al defecto de software nº CSCuf25027 .

Solución

La solución alternativa a este problema es deshabilitar la función Netflow y Network Based Application Recognition (NBAR) en el router. Si desea ejecutar todas las funciones y tener un mejor rendimiento, la mejor opción es actualizar a ASR1002-X o ASR1006 con ESP-100.