Contenido

Introducción

Este documento describe el problema con la producción en la plataforma ASR1002 con la visibilidad y el control (AVC) de la aplicación configurados junto con la característica del IPSec en el router.

Antecedentes

Según la documentación CCO, ASR10002 proporciona la producción del 10 gbps para el tráfico de datos normales, 4 Gbps con la característica del IPSec habilitada. Pero hay una advertencia asociada a la producción en la plataforma ASR1002. El Netflow y el NBAR son dos características que consume muchos recursos del procesador del flujo de Quantum (QFP) y reduce así el cabability del indicador luminoso LED amarillo de la placa muestra gravedad menor del Encapsulating Security Payload (ESP) para procesar más tráfico y así la reducción de la producción de general del sistema. Con la configuración AVC junto con el IPSec, la producción total de la plataforma se puede degradar seriamente y puede hacer frente a la pérdida de tráfico enorme.

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

El problema era inicial notada cuando el ancho de banda fue actualizado con el proveedor y prueba era del ancho de banda se realiza. El paquete de bytes 1000 fue enviado inicialmente, que fue perfectamente multa, después la prueba fue realizada con 512 paquetes de bytes después de lo cual él notó casi la pérdida de tráfico del 80%. Refiera a esta topología de la prueba de laboratorio:

Funcione con estas características:

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

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
!
```

El Dynamic Multipoint VPN (DMVPN) está entre el dos Routers ASR1k. El tráfico fue generado del IXIA al IXIA a través de la nube DMVPN con el tamaño de paquetes de 512 bytes @ 50000 pps. Otra secuencia se configura para el tráfico del expedited forwarding (EF) del IXIA al IXIA

Con la secuencia antedicha, notamos la pérdida de tráfico en ambas secuencias para hasta casi 30000 pps.

'Observaciones'

No había mucho las caídas de resultados que incrementaban y no mucho cae visto en la clase EF u otras clases excepto de la clase predeterminada de la servicio-directiva.

Los descensos encontrados en QFP usando los **descensos de las estadísticas activas del qfp del hardware de plataforma de la demostración** y notado esos descensos incrementaban 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#
```

Descensos más futuros del IPSec fueron marcados para saber si hay QFP usando los **descensos activos de los datos del IPSec de la característica del qfp del hardware del** comando show platform

```
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#
```

Fue notado que el contador de caídas para **IN_PSTATE_CHUNK_ALLOC_FAIL** contrario correspondía con el contador de **IpsecInput del** valor en los descensos QFP y lo mismo con **IpsecOutput** que correspondía con con **OUT_PSTATE_CHUNK_ALLOC_FAIL** al revés.

Este problema es considerado debido al defect# CSCuf25027 del software.

Solución

El Workaround a este problema es inhabilitar la característica del Netflow y del Reconocimiento de aplicaciones basadas en la red (NBAR) en el router. Si usted quiere funcionar con todas las características y tener mejor producción, después la opción es mejor actualizar a ASR1002-X o a ASR1006 con el ESP-100.