Limitazione della piattaforma ASR1002 con IPSec, Netflow, NBAR

Sommario

Introduzione

In questo documento viene descritto il problema della velocità effettiva sulla piattaforma ASR1002 con Application Visibility and Control (AVC) configurato insieme alla funzionalità IPSec sul router.

Premesse

Come indicato nella documentazione CCO, ASR10002 fornisce un throughput di 10 Gb/s per il normale traffico dati e di 4 Gb/s con la funzionalità IPSec abilitata. Tuttavia, esiste una nota aggiuntiva relativa al throughput sulla piattaforma ASR1002. Netflow e NBAR sono due funzioni che consumano molte risorse da Quantum Flow Processor (QFP) e che quindi riducono la cablabilità della scheda Encapsulating Security Payload (ESP) per elaborare più traffico e quindi ridurre la velocità di trasmissione complessiva del sistema. Con la configurazione AVC e IPSec, il throughput complessivo della piattaforma può subire un grave peggioramento e può subire un'enorme perdita di traffico.

Problema: Limitazione della piattaforma ASR1002 con IPSec, Netflow, NBAR

Il problema è stato inizialmente rilevato durante l'aggiornamento della larghezza di banda con il provider e durante l'esecuzione dei test della larghezza di banda. Inizialmente è stato inviato un pacchetto da 1000 byte, che è andato perfettamente bene, poi il test è stato eseguito con pacchetti da 512 byte, dopo di che hanno quasi notato una perdita dell'80% del traffico. Fare riferimento a questa topologia di test di laboratorio:

Esegui le seguenti funzionalità:

- DMVPN over IPSec
- NetFlow
- NBAR (come parte dell'istruzione match dei criteri QoS)

Configurazione

```
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 DMVPN (Dynamic Multipoint VPN) è situata tra i due router ASR1k. Il traffico è stato generato da IXIA a IXIA attraverso il cloud DMVPN con dimensioni del pacchetto di 512 byte a 50000 bps. È configurato un altro flusso per il traffico di inoltro accelerato (EF) da IXIA a IXIA

Con il flusso sopra riportato, abbiamo notato una perdita di traffico in entrambi i flussi fino a quasi 30.000 pagine al secondo.

Osservazioni

Non sono state rilevate molte riduzioni dell'output in aumento e poche riduzioni nella classe EF o in altre classi, ad eccezione della classe predefinita della policy di servizio.

Sono stati rilevati cali di QFP che utilizzano **le statistiche attive qfp dell'hardware della piattaforma show** e sono stati notati cali in rapida crescita.

```
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#
```

Sono stati controllati ulteriori rilasci IPSec per QFP utilizzando il 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#
```

Èstato rilevato che il contatore di rilascio per il contatore **IN_PSTATE_CHUNK_ALLOC_FAIL** corrisponde al valore **IpsecInput** nel contatore QFP e corrisponde al valore **IpsecOutput** corrispondente al contatore **OUT_PSTATE_CHUNK_ALLOC_FAIL.**

Il problema è dovuto al problema software n. CSCuf25027 .

Soluzione

Per risolvere il problema, disabilitare la funzionalità Netflow e Network Based Application Recognition (NBAR) sul router. Se si desidera eseguire tutte le funzioni e avere un throughput migliore, un'opzione migliore è l'aggiornamento ad ASR1002-X o ASR1006 con ESP-100.