ASR1002-Plattformbeschränkung mit IPSec, Netflow, NBAR

Inhalt

Einführung

Dieses Dokument beschreibt das Problem mit dem Durchsatz auf der ASR1002-Plattform mit AVC (Application Visibility and Control), die zusammen mit der IPSec-Funktion auf dem Router konfiguriert wurde.

Hintergrundinformationen

Laut CCO-Dokumentation bietet der ASR10002 einen Durchsatz von 10 Gbit/s für den normalen Datenverkehr, 4 Gbit/s bei aktivierter IPSec-Funktion. Beim Durchsatz der ASR1002-Plattform besteht jedoch ein Problem. NetFlow und NBAR sind zwei Funktionen, die eine Menge Ressourcen vom Quantum Flow Processor (QFP) benötigen und so die Verkabelung der Encapsulating Security Payload (ESP)-Karte zur Verarbeitung von mehr Datenverkehr und somit zur Verringerung des Gesamtsystemdurchsatzes reduzieren. Bei der AVC-Konfiguration in Verbindung mit IPSec kann der Gesamtdurchsatz der Plattform erheblich reduziert werden und kann zu enormen Datenverkehrsverlusten führen.

Problem: ASR1002-Plattformbeschränkung mit IPSec, Netflow, NBAR

Das Problem wurde zunächst bemerkt, als die Bandbreite mit dem Anbieter aktualisiert wurde und Bandbreitentests durchgeführt wurden. Ursprünglich wurden 1000-Byte-Pakete gesendet, was perfekt lief. Anschließend wurden die Tests mit 512-Byte-Paketen durchgeführt, nach denen fast 80 % Datenverkehrsverluste auftraten. Weitere Informationen finden Sie in dieser Testtopologie:

Führen Sie folgende Funktionen aus:

- DMVPN über IPSec
- NetFlow
- NBAR (als Teil der QoS-Richtlinie-Match-Anweisung)

Konfiguration

```
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
!
```

Das Dynamic Multipoint VPN (DMVPN) befindet sich zwischen den beiden ASR1k-Routern. Der Datenverkehr wurde von IXIA nach IXIA über die DMVPN-Cloud mit einer Paketgröße von 512 Byte bei 50.000 pps generiert. Ein weiterer Stream ist für Expedited Forwarding (EF)-Datenverkehr von IXIA nach IXIA konfiguriert.

Mit dem oben genannten Stream wurden Datenverkehrsverluste in beiden Datenströmen für bis zu 30.000 pps festgestellt.

Beobachtungen

Außer in der Standardklasse der Dienstrichtlinie gab es nur wenige inkrementelle Ausgabeverwerbe und nicht viel Verwerfungen in der EF-Klasse oder anderen Klassen.

Bei QFP wurden Verwerfungen mithilfe von **show platform hardware qfp active statistics festgestellt** und diese Verwerfungen stiegen schnell an.

```
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#
```

Weitere IPSec-Verwerfen wurden mithilfe des Befehls **show platform hardware qfp active feature ipsec data drop** auf QFP überprüft.

```
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#
```

Es wurde festgestellt, dass der Drop-Zähler für den Zähler **IN_PSTATE_CHUNK_ALLOC_FAIL** mit dem Wert **IpsecInput**-Zähler im QFP-Drops und dem mit dem Zähler **IpsecOutput** übereinstimmenden Wert **OUT_PSTATE_CHUNK_ALLOC_FAIL_** übereinstimmt**.**

Dieses Problem ist auf den Softwarefehler# CSCuf25027 zurückzuführen.

Lösung

Als Problemumgehung gilt die Deaktivierung der Funktion "NetFlow" und "Network Based Application Recognition" (NBAR) auf dem Router. Wenn Sie alle Funktionen ausführen und einen besseren Durchsatz erzielen möchten, empfiehlt sich ein Upgrade auf ASR1002-X oder ASR1006 mit ESP-100.