ASR1002 platform beperking met IPSec, NetFlow, NBAR

Inhoud

Inleiding

Dit document beschrijft het probleem met de doorvoersnelheid op ASR1002-platform met Application Visibility and Control (AVC) die samen met IPSec-functie op de router is geconfigureerd.

Achtergrondinformatie

Overeenkomstig CCO-documentatie biedt ASR1002 10 Gbps doorvoersnelheid voor normaal gegevensverkeer en 4 Gbps met IPSec-optie. Maar er is een voorbehoud verbonden aan de doorvoersnelheid op het ASR1002-platform. NetFlow en NBAR zijn twee functies die veel resources gebruiken voor Quantum Flow Processor (QFP) en zo de mogelijkheid van de Encapsulating Security Payload-kaart (ESP) verminderen om meer verkeer te verwerken en zo de totale systeemdoorvoersnelheid te reduceren. Dankzij de AVC-configuratie in combinatie met IPSec kan de algemene doorvoersnelheid van het platform ernstig worden aangetast en kan deze bij groot verkeersverlies worden geconfronteerd.

Probleem: ASR1002 platform beperking met IPSec, NetFlow, NBAR

Het probleem werd aanvankelijk opgemerkt toen de bandbreedte met de leverancier werd bijgewerkt en de bandbreedte test werd uitgevoerd. Eerst werd 1000 bytes-pakket verzonden, dat perfect goed ging, toen de test werd uitgevoerd met 512 byte-pakketten waarna ze bijna 80% verkeersverlies zagen. Raadpleeg deze topologie voor laboratoriumtests:

Draai deze functies:

- DMVPN via IPSec
- NetFlow
- NBAR (als onderdeel van een QoS-beleidsmatchverklaring)

Configuratie

```
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
!
```

Dynamic Multipoint VPN (DMVPN) is tussen de twee ASR1k routers. Er is verkeer gegenereerd van IXIA naar IXIA over de DMVPN-cloud met een pakketgrootte van 512 bytes @ 50000 pps. Een andere stroom is ingesteld voor FEF-verkeer (Fast Forwarding) van IXIA naar IXIA

Met de bovenstaande stroom zagen we verkeersverlies in beide stromen tot bijna 30.000 pps.

Opmerkingen

Er waren niet veel output druppels meer, en er waren niet veel druppels te zien in de EF-klasse of andere klassen behalve uit de standaardklasse van het service-beleid.

Gevonden dalingen in QFP met behulp van **tonen platform hardware qfp actieve statistieken dalen** en merkten dat die druppels snel toenamen.

```
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#
```

Andere IPSec-druppels werden voor QFP gecontroleerd met behulp van **een** commando **show platform hardware qfp actieve optie ipsec-gegevensdruppels**

```
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#
```

Het werd opgemerkt dat de druppelteller voor **IN_PSTATE_CHUNK_ALLOC_FAIL** bij de waarde **IpsecInput** teller in de QFP druppels lag en hetzelfde was met **IPsecOutput** matching met **OUT_PSTATE_CHUNK_ALLOC_FAIL** teller.

Dit probleem wordt gezien vanwege de softwarefout# CSCuf25027.

Oplossing

Werkruimte voor dit probleem is om NetFlow en Network-Based Application Recognition (NBAR) optie op de router uit te schakelen. Als u alle functies wilt uitvoeren en een betere doorvoersnelheid wilt hebben, is het beter om naar ASR 1002-X of ASR 1006 te upgraden met ESP-100.