IPSec, Netflow, NBAR가 포함된 ASR1002 플랫폼 제한

목차

소개

이 문서에서는 라우터의 IPSec 기능과 함께 AVC(Application Visibility and Control)가 구성된 ASR1002 플랫폼의 처리량 문제를 설명합니다.

배경 정보

CCO 설명서에 따라 ASR1002는 일반 데이터 트래픽에 10gbps의 처리량을 제공하며, IPSec 기능이 활성화된 경우 4Gbps를 제공합니다.그러나 ASR1002 플랫폼의 처리량에 유의해야 합니다.Netflow와 NBAR는 QFP(Quantum Flow Processor)의 많은 리소스를 소비하여 더 많은 트래픽을 처리하고 전체 시스템 처리량을 줄이기 위해 ESP(Encapsulating Security Payload) 카드의 케이블 기능을 줄여주는 두 가지 기능입니다.IPSec과 함께 AVC 컨피그레이션을 사용하면 전반적인 플랫폼 처리량이 크게 저하될 수 있으며 트래픽 손실이 커질 수 있습니다.

문제/장애:IPSec, Netflow, NBAR가 포함된 ASR1002 플랫폼 제한

공급자와 함께 대역폭을 업그레이드하고 대역폭 테스트를 수행할 때 문제가 처음 발견되었습니다.처음에는 1000바이트 패킷이 전송되었지만, 완벽하게 잘 작동한 다음 512바이트 패킷으로 테스트를 수행했으며, 그 후 트래픽이 80% 손실되는 것을 거의 확인했습니다.다음 실습 테스트 토폴로지를 참조하십시오.

다음 기능을 실행합니다.

- IPSec을 통한 DMVPN
- Netflow
- NBAR(QoS 정책 일치 문의 일부로)

구성

```
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
!
```

DMVPN(Dynamic Multipoint VPN)은 두 ASR1k 라우터 사이에 있습니다.패킷 크기가 512바이트인 50000pps인 DMVPN 클라우드에서 IXIA에서 IXIA로 트래픽이 생성되었습니다.IXIA에서 IXIA로의 빠른 전달(EF) 트래픽을 위해 다른 스트림이 구성되었습니다.

위의 스트림에서는 두 스트림에서 거의 30000pps까지 트래픽 손실을 발견했습니다.

관찰

서비스 정책의 기본 클래스를 제외하고 EF 클래스나 기타 클래스에 표시되는 출력 삭제는 많지 않고 많이 감소되지 않았습니다.

QFP에서 **show platform hardware qfp active statistics drops**를 사용하여 드롭이 발견되었으며 이러한 드롭이 빠르게 증가하고 있음을 확인했습니다.

```
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#
```

show platform hardware qfp active feature ipsec **데이터 삭제** 명령을 사용하여 QFP에 대한 추가 IPSec 삭제**를 확인했습니다.**

```
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#
```

IN_PSTATE_CHUNK_ALLOC_FAIL 카운터에 대한 드롭 카운터가 QFP **삭제**의 IpsecInput 카운터와 일치하고 OUT_PSTATE_CHUNK_ALLOC_FAIL 카운터와 일치하는 **IpsecOutput과 일치한다는 것을** 발견했습니다.

이 문제는 소프트웨어 결함 번호 CSCuf25027으로 인해 나타납니다.

솔루션

이 문제를 해결하려면 라우터에서 Netflow 및 NBAR(Network Based Application Recognition) 기능을 비활성화해야 합니다.모든 기능을 실행하고 처리량을 높이려면 ESP-100을 사용하여 ASR1002-X 또는 ASR1006으로 업그레이드하는 것이 좋습니다.