Contents

Introduction

This document descibes the problem with throughput on ASR1002 platform with Application Visibility and Control (AVC) configured along with IPSec feature on the router.

Background Information

As per CCO documentation, ASR10002 provides 10 gbps throughput for normal data traffic, 4 Gbps with IPSec feature enabled. But there is a caveat attached to the throughput on ASR1002 platform. Netflow and NBAR are two features which consumes a lot of resources from Quantum Flow Processor (QFP) and thus reduces the cabability of the Encapsulating Security Payload (ESP) card to process more traffic and thus reducing the overall system throughput. With AVC configuration along with IPSec, the overall platform throughput can be severely degraded and can face huge traffic loss.

Problem: ASR1002 platform limitation with IPSec, Netflow, NBAR

The problem was initial noticed when the bandwidth was upgraded with the provider and bandwidth testing was being perform. Initially 1000 bytes packet was sent, which went perfectly fine, then the testing was performed with 512 byte packets after which they nearly noticed 80% traffic loss. Refer to this lab testing topology:

Run these features:

- DMVPN over IPSec
- Netflow
- NBAR (as part of QoS policy match statement)

Configuration

```
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
!
```

The Dynamic Multipoint VPN (DMVPN) is between the two ASR1k routers. Traffic was generated from IXIA to IXIA across the DMVPN cloud with packet size of 512 bytes @ 50000 pps. Another stream is configured for Expedited Forwarding (EF) traffic from IXIA to IXIA

With the above stream, we noticed traffic loss in both streams for upto nearly 30000 pps.

Observations

There were not much output drops incrementing and not much drops seen in the EF class or other classes except from default class of the service-policy.

Found drops in QFP using **show platform hardware qfp active statistics drops** and noticed those drops were incrementing rapidly.

```
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#
```

Further IPSec drops were checked for QFP using command **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#
```

It was noticed that drop counter for **IN_PSTATE_CHUNK_ALLOC_FAIL** counter was matching the value **IpsecInput** counter in the QFP drops and same with **IpsecOutput** matching with **OUT_PSTATE_CHUNK_ALLOC_FAIL** counter**.**

This issue is seen due to the software defect# CSCuf25027 .

Solution

Workaround to this problem is to disable Netflow and Network Based Application Recognition (NBAR) feature on the router. If you want to run all the features and have better throughput, then better option is to upgrade to ASR1002-X or ASR1006 with ESP-100.