ASR1002平台限制，带IPSec、Netflow、NBAR

目录

简介

本文档介绍在ASR1002平台上配置了应用可视性与可控性(AVC)以及路由器上的IPSec功能的吞吐量问题。

背景信息

根据CCO文档，ASR10002为正常数据流量提供10 gbps的吞吐量，4 Gbps，并启用IPSec功能。但是，ASR1002平台上的吞吐量附加了警告。Netflow和NBAR是两个功能，它们消耗了量子流处理器(QFP)的大量资源，从而降低了封装安全负载(ESP)卡处理更多流量的电缆能力，从而降低了整体系统吞吐量。使用AVC配置和IPSec，整个平台吞吐量可能严重降低，并可能面临巨大的流量丢失。

问题：ASR1002平台限制，带IPSec、Netflow、NBAR

最初，在向提供商升级带宽并执行带宽测试时，就注意到了问题。最初发送了1000字节的数据包，这个数据包非常正常，然后对512字节的数据包执行测试，之后他们几乎注意到80%的流量丢失。请参阅本实验测试拓扑：

运行以下功能：

- 基于IPSec的DMVPN

- Netflow
- NBAR（作为QoS策略匹配语句的一部分）

配置

```
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
!
```

动态多点VPN(DMVPN)位于两台ASR1k路由器之间。数据包大小为512字节(50000 pps)，通过DMVPN云从IXIA生成到IXIA的流量。另一个流配置为从IXIA到IXIA的加速转发(EF)流量

通过上述流，我们注意到两个流中的流量丢失高达近30000 pps。

观察结果

EF类或除服务策略的默认类外，没有多少输出丢包递增，在EF类或其他类中也没有多少丢包。

使用show platform hardware qfp active statistics drops**发现QFP中的丢包，**并注意到这些丢包正在快速增加。

```
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#
```

使用命令show platform hardware qfp active feature ipsec data drops检查QFP的**进一步IPSec丢弃**

```
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#
```

注意到IN_PSTATE_CHUNK_ALLOC_FAIL计数器的丢弃计数器与QFP丢包中的值**IpsecInput**计数器匹配，与**OUT_PSTATE_CHUNK_ALLOC_FAIL** 计数器的**IpsecOutput**匹配。

出现此问题是由于软件缺陷# CSCuf25027 。

解决方案

此问题的解决方法是在路由器上禁用Netflow和基于网络的应用识别(NBAR)功能。如果您希望运行所有功能并获得更好的吞吐量，则更好的选择是升级到带ESP-100的ASR1002-X或ASR1006。