目录

简介

本文描述与吞吐量的问题在ASR1002平台用与在路由器的IPSec功能一起和控制(AVC)配置的应用程序可见性。

背景信息

根据CCO文档， ASR10002提供正常数据流的10 gbps吞吐量，与启用的IPSec功能的4 Gbps。但是有警告附加对在ASR1002平台的吞吐量。浪费从Quantum流处理器的Netflow和NBAR是两个功能(QFP)的很多资源和因而减少封装安全有效载荷(ESP)卡cabability处理更多流量和因而降低整个系统吞吐量。使用与IPSec一起的AVC配置，整体平台吞吐量严重降低并且能受巨大的数据流损失。

问题：ASR1002与IPSec的平台限制， Netflow， NBAR

问题是被注意的初始，当带宽升级与供应商，并且带宽测试是实行。最初1000字节信息包发送，完全去罚款，然后测试用512个字节信息包执行，在后他们接近注意了80%数据流损失。参考此实验室测试拓扑：

运行这些功能：

- 在IPSec的DMVPN
- Netflow
- NBAR (作为QoS策略匹配语句一部分)

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)在两ASR1k路由器之间。流量从鸢尾属生成到在DMVPN网云间的鸢尾属与数据包大小512个字节@ 50000 pps。另一数据流为紧急转发(EF)流量配置从鸢尾属到鸢尾属

使用上述数据流，我们注意了在两数据流的数据流损失接近30000 pps的。

观察

没有增加的输出丢弃，并且并非从服务策略的默认组丢弃看到在E-F类或其他类除了。

在QFP的被找到的丢包使用**显示平台硬件qfp活动统计信息丢包**并且注意那些丢包迅速地增加。

```
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show platform命令**硬件qfp活动功能ipsec数据丢包，更加**进一步的IPSec丢包被检查了QFP

```
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#
```

被注意IN_PSTATE_CHUNK_ALLOC_FAIL计数器的丢弃计数器匹配在QFP丢包的值IpsecInput计数器和同样与匹配与OUT_PSTATE_CHUNK_ALLOC_FAIL计数器的IpsecOutput。

此问题被看到的归结于软件defect# CSCuf25027。

解决方案

对此问题的应急方案是禁用在路由器的Netflow和基于网络的应用程序识别(NBAR)功能。如果要运行所有功能和有更加好的吞吐量，则更加好的选项是升级对ASR1002-X或ASR1006与ESP-100。