Содержание

Введение

Этот документ descibes проблема с пропускной способностью на платформе ASR1002 с Видимостью Приложения и Контролем (AVC) настроен наряду с функцией IPSec на маршрутизаторе.

Общие сведения

Согласно документации CCO, ASR10002 предоставляет пропускную способность на 10 Гбит/с для нормального трафика данных, 4 Гбит/с с активированной опцией IPSec. Но существует предупреждение, подключенное к пропускной способности на платформе ASR1002. Netflow и NBAR являются двумя функциями, который использует много ресурсов от процессора Quantum Flow (QFP) и таким образом уменьшает cabability карты Безопасного закрытия полезной нагрузки (ESP) для обработки большего количества трафика и таким образом сокращения пропускной способности глобальной системы. С конфигурацией AVC наряду с IPSec полная пропускная способность платформы может быть сильно ухудшена и может стоять перед огромной потерей трафика.

Ограничение Problem: ASR1002 платформы с IPSec, Netflow, NBAR

Проблема была начальной, заметил, когда пропускная способность была обновлена с поставщиком, и тестирование пропускной способности было, выполняют. Первоначально 1000 байтовых пакетов передавались, который пошел превосходный, тогда тестирование было выполнено с 512 пакетами в 1 байт, после которых они почти заметили 80%-ю потерю трафика. См. эту топологию лабораторного испытания:

Выполните эти функции:

- DMVPN по IPSec
- Netflow
- NBAR (как часть сообщения о совпадении политики QoS)

!--- конфигурацию

```
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
!
```

Динамическая многоточечная VPN (DMVPN) между двумя маршрутизаторами ASR1k. Трафик генерировался от IXIA до IXIA через облако DMVPN с размером пакета 512 байтов 50000 pps. Другой поток настроен для трафика Ускоренной пересылки (EF) от IXIA до IXIA

С вышеупомянутым потоком мы заметили потерю трафика в обоих потоках для почти до 30000 pps.

Наблюдения

Не было большого приращения отбрасываний выходных данных, и не много понижается замеченный в классе EF или других классах кроме от класса по умолчанию стратегии обслуживания.

Найденные падения QFP использование **show platform hardware qfp активные отбрасывания статистики** и замеченный те отбрасывания инкрементно увеличивались быстро.

```
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#
```

Дальнейшие отбрасывания IPSec были проверены для QFP использование команды **show platform hardware qfp активные отбрасывания данных ipsec функции**

```
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#
```

Было замечено, что счетчик сбросов для счетчика **IN_PSTATE_CHUNK_ALLOC_FAIL** совпадал со значением счетчик **IpsecInput** в отбрасываниях QFP и том же с **IpsecOutput**, совпадающим со счетчиком **OUT_PSTATE_CHUNK_ALLOC_FAIL.**

Эта проблема замечена из-за программного обеспечения defect# CSCuf25027.

Решение

Обходной путь к этой проблеме должен отключить опцию Netflow и Сетевого распознавания приложений (NBAR) на маршрутизаторе. Если вы хотите выполнить все функции и иметь лучшую пропускную способность, то лучшая опция должна обновить к ASR1002-X или ASR1006 с ESP 100.