IPSec、Netflow、NBARによるASR1002プラットフォームの制限

内容

概要

このドキュメントでは、ルータのIPSec機能とともにApplication Visibility and Control(AVC)が設定されたASR1002プラットフォームのスループットに関する問題について説明します。

背景説明

CCOのドキュメントによると、ASR10002は通常のデータトラフィックに対して10 gbpsのスループットを提供し、IPSec機能が有効な4 Gbpsを実現します。ただし、ASR1002プラットフォームのスループットには注意が必要です。NetflowとNBARは、Quantum Flow Processor(QFP)から大量のリソースを消費する2つの機能であり、Encapsulating Security Payload(ESP)カードがより多くのトラフィックを処理し、システム全体のスループットが低下します。IPSecとともにAVCを設定すると、プラットフォーム全体のスループットが著しく低下し、トラフィックの損失が大きくなる可能性があります。

問題：IPSec、Netflow、NBARによるASR1002プラットフォームの制限

この問題は、プロバイダーで帯域幅がアップグレードされ、帯域幅テストが実行されたときに最初に認識されました。最初に1000バイトのパケットが送信されましたが、これは完全に正常に終了しました。その後、512バイトのパケットを使用してテストが実行され、その後、トラフィックの損失が80 %に近づきました。次のラボテストトポロジを参照してください。

次の機能を実行します。

- IPSec上のDMVPN
- NetFlow
- NBAR（QoSポリシー照合文の一部として）

コンフィギュレーション

```
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
!
```

Dynamic Multipoint VPN(DMVPN)は、2つのASR1kルータ間にあります。トラフィックは、DMVPNクラウド全体でIXIAからIXIAに生成され、パケットサイズは512バイト@ 50000 ppsでした。IXIAからIXIAへのExpedited Forwarding(EF)トラフィック用に別のストリームが設定されています

上記のストリームでは、最大30000 ppsの両方のストリームのトラフィック損失に気付きました。

観察

サービスポリシーのデフォルトクラスを除き、EFクラスやその他のクラスで表示される出力ドロップの数は多くありませんでした。

show platform hardware qfp active statistics dropsを使用してQFPでドロップが見つかり、**それらのドロップが急速に増え**ていることに気付きました。

```
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#
```

さらに、**show platform hardware qfp active feature ipsec data dropsコマンド**を使用して、QFPに関するIPSecのドロップ**を確認しました**

```
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カウンタのドロップカウンタが、QFPドロップの値 **IpsecInputカウンタと一致し、OUT_PSTATE_CHUNK_ALLOC_FAIL**カウンタと同じであることがわかりました。

この問題は、ソフトウェア不具合番号CSCuf25027（登録ユーザ専用）が原因で発生します。

解決方法

この問題の回避策は、ルータでNetflowおよびNetwork Based Application Recognition(NBAR)機能を無効にすることです。すべての機能を実行し、スループットを向上させる場合は、ESP-100を使用してASR1002-XまたはASR1006にアップグレードする方法が適しています。