Pre-Tunnel Fragmentation

SecGW supports post-tunnel fragmentation for IPsec ESP data packets. If an encrypted packet exceeds an interface MTU size the packet is fragmented. Post-tunnel fragmentation can cause performance degradation and pre-tunnel fragmentation has better packet processing rate.

The following sections provide more detailed information:

Pre-Tunnel fragmentation at ASR 9000 XR

XR already supports fragmentation at interface level. SecGW in ASR 9000 has the advantage of using the XR functionality because the packets are always forwarded via XR.

The MTU size can be configured at the VSM interface used for clear traffic. The MTU size should be the PMTU of the encrypted network subtracted by the outer IP header size and crypto overhead (which is up to 100 bytes). If PMTU of the encrypted network is 1400 then the VSM clear interface MTU size must be 1300 for pre-tunnel fragmentation to work.

Configuration

The below configuration at XR enables Pre-Tunnel Fragmentation feature.

To enable the feature configure the MTU size in VSM interface used for clear traffic in XR. The MTU size is calculated by subtracting 100 bytes (overhead for encryption) from the PMTU size of the encrypted network.

```
interface TenGigE0/1/1/1
 description "CLEAR Interface"
 mtu 500    ----------------------- if PMTU is 600
 ipv4 address 79.79.79.14 255.255.255.0
 ipv6 address 2001:79:79:79::14/64
 !
```