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 VPC-DI

The pre tunnel fragmentation feature and its maximal MTU size will be defined under WSG service. This MTU size is stored with other WSG service parameters. During IPsec SA creation, the MTU is passed to crypto driver subsystem. The crypto driver will calculate the crypto overhead to determine the effective MTU size for plaintext based on given MTU size and SA information. When crypto driver receives a packet for encryption and packet length is longer than effective MTU, the packet will be fragmented before deliver to crypto chip.

MTU range is between intiger 576 to 2048, default is 1400.

Configuring IPsec Pre tunnel fragmentation

Use the below configuration to configure Pre-tunnel Fragmentation:

```
   config
      context context_name
        pre_fragment mtu mtu_size
        [ default | no ] pre_fragment
exit
```