Fast Path Stats Counters

This appendix describes the Fast Path stats counters.

Table B-1 and Table B-2lists the Fast Path Stats supported by the WSG:

Table B-1   Global IPsec Fast Path Stats Supported by the WSG

Stats	Source	Description
ceipSecGlobalInDrops	NPU	The total number of packets dropped during receive processing by all current and previous IPsec Phase-2 Tunnels. This count does NOT include packets dropped due to Anti-Replay processing. Possible causes of this error: • Incorrect IP version • TTL field is zero • ESP packet's Next Header field does not match the IP protocol of the encapsulated packet
ceipSecGlobalOutDrops	NPU	The total number of packets dropped during send processing by all current and previous IPsec Phase-2 Tunnels Possible cause of this error: • Fragmentation errors; E.g., packet larger than the WSG's configured pre-framentation MTU with DF bit set.
ceipSecGlobalInReplayDrops	Crypto chip	The total number of packets dropped during receive processing due to Anti-Replay processing by all current and previous IPsec Phase-2 Tunnels Possible causes of this error: • WSG recives an ESP packet with sequence number out of the replay window. • Simulated by capturing and reply the ESP packet.

Table B-1   Global IPsec Fast Path Stats Supported by the WSG (continued)

Stats	Source	Description
ceipSecGlobalInAuthFails	Crypto chip	The total number of decrypt packet authentications which ended in failure by all current and previous IPsec Phase-2 Tunnels.
ceipSecGlobalOutAuthFails	NPU	The total number of encrypt packet authentications which ended in failure by all current and previous IPsec Phase-2 Tunnels. Possible cause of this error: • Failures during encryption of the packets for any tunnel on the card.

Table B-2   IPsec Tunnel Fast Path Stats Supported by the WSG

Stats	Source	Description
ceipSecTunInDropPkts	NPU	The total number of packets dropped during receive processing by this IPsec Phase-2 Tunnel. This count does NOT include packets dropped due to Anti-Replay processing. Possible causes of this error: • Incorrect IP version • TTL field is zero • ESP packet's Next Header field does not match the IP protocol of the encapsulated packet
ceipSecTunOutDropPkts	NPU	The total number of packets dropped during send processing by this IPsec Phase-2 Tunnel. Possible cause of this error: • Fragmentation errors; E.g., packet larger than the WSG's configured pre-framentation MTU with DF bit set.
ceipSecTunInAuthFails	NPU	The total number of inbound authentication's which ended in failure by this IPsec Phase-2 Tunnel. Possible cause of this error: • Failures during decryption of the packet because of mis-comparison in the hash mac.
ceipSecTunOutAuthFails	NPU	The total number of outbound authentication's which ended in failure by this IPsec Phase-2 Tunnel.

Table B-2   IPsec Tunnel Fast Path Stats Supported by the WSG (continued)

Stats	Source	Description
ceipSecTunInDecryptFails	NPU	The total number of inbound decryption's which ended in failure by this IPsec Phase-2 Tunnel. Possible causes of this error: • Tunnel decryption failed due to next header mismatch in the decrypted packet • Bad IP version • Bad IP checksum • TTL expiry
ceipSecTunOutEncryptFails	NPU	The total number of outbound encryption's which ended in failure by this IPsec Phase-2 Tunnel. Possible cause of this error: • Badly formed IP packet getting encrypted; e.g. wrong checksum, bad IP version, etc.
ceipSecTunInReplayDropPkts	NPU	The total number of packets dropped during receive processing due to Anti-Replay processing by this IPsec Phase-2 Tunnel. Possible cause of this error: • Receiving packets with ESP sequence numbers within the replay window.