Monitor SSL Hardware Acceleration

Use the show counters command in the CLI to evaluate TLS crypto acceleration behavior. This command lists a variety of metrics that inform you about normal activity, alerts, and potential fatal issues.

> **Note** Use the **show counters description** command to see explanations for each counter. To view only counters related to TLS crypto acceleration, use **show counters description | include TLS_TRK**.

Informational Counters

If a system under load is working well, you should see large counts for the following counters. Because there are 2 sides to the tracker process per connection, you can see these counters increase by 2 per connection. The PRIV_KEY_RECV and SECU_PARAM_RECV counters are the most important, and are highlighted. The CONTEXT_CREATED and CONTEXT_DESTROYED counters relate to the allocation of cryptographic chip memory.

```
> show counters
Protocol    Counter                       Value    Context
SSLENC      CONTEXT_CREATED               258225   Summary
SSLENC      CONTEXT_DESTROYED             258225   Summary
TLS_TRK     OPEN_SERVER_SESSION           258225   Summary
TLS_TRK     OPEN_CLIENT_SESSION           258225   Summary
TLS_TRK     UPSTREAM_CLOSE                516450   Summary
TLS_TRK     DOWNSTREAM_CLOSE              516450   Summary
TLS_TRK     FREE_SESSION                  516450   Summary
TLS_TRK     CACHE_FREE                    516450   Summary
TLS_TRK     PRIV_KEY_RECV                 258225   Summary
TLS_TRK     NO_KEY_ENABLE                 258225   Summary
TLS_TRK     SECU_PARAM_RECV               516446   Summary
TLS_TRK     DECRYPTED_ALERT               258222   Summary
TLS_TRK     DECRYPTED_APPLICATION       33568976   Summary
TLS_TRK     ALERT_RX_CNT                  258222   Summary
TLS_TRK     ALERT_RX_WARNING_ALERT        258222   Summary
TLS_TRK     ALERT_RX_CLOSE_NOTIFY         258222   Summary
```

```
TCP_PRX       OPEN_SESSION                      516450   Summary
TCP_PRX       FREE_SESSION                      516450   Summary
TCP_PRX       UPSTREAM_CLOSE                    516450   Summary
TCP_PRX       DOWNSTREAM_CLOSE                  516450   Summary
TCP_PRX       FREE_CONN                         258222   Summary
TCP_PRX       SERVER_CLEAN_UP                   258222   Summary
TCP_PRX       CLIENT_CLEAN_UP                   258222   Summary
```

Alert Counters

We implemented the following counters according to the TLS 1.2 specification. FATAL or BAD alerts could indicate issues; however, ALERT_RX_CLOSE_NOTIFY is normal.

For details, see RFC 5246 section 7.2.

```
TLS_TRK       ALERT_RX_CNT                          311   Summary
TLS_TRK       ALERT_TX_CNT                            2   Summary
TLS_TRK       ALERT_TX_IN_HANDSHAKE_CNT               2   Summary
TLS_TRK       ALERT_RX_IN_HANDSHAKE_CNT               2   Summary
TLS_TRK       ALERT_RX_WARNING_ALERT                308   Summary
TLS_TRK       ALERT_RX_FATAL_ALERT                    3   Summary
TLS_TRK       ALERT_TX_FATAL_ALERT                    2   Summary
TLS_TRK       ALERT_RX_CLOSE_NOTIFY                 308   Summary
TLS_TRK       ALERT_RX_BAD_RECORD_MAC                 2   Summary
TLS_TRK       ALERT_TX_BAD_RECORD_MAC                 2   Summary
TLS_TRK       ALERT_RX_BAD_CERTIFICATE                1   Summary
```

Error Counters

These counters indicate system errors. These counts should be low on a healthy system. The BY_PASS counters indicate packets that have been passed directly to or from the inspection engine (Snort) process (which runs in software) without decryption. The following example lists some of the bad counters.

Counters with a value of 0 are not displayed. To view a complete list of counters, use the command **show counters description | include TLS_TRK**

```
> show counters
Protocol      Counter                         Value    Context
TCP_PRX       BYPASS_NOT_ENOUGH_MEM            2134     Summary
TLS_TRK       CLOSED_WITH_INBOUND_PACKET          2     Summary
TLS_TRK       ENC_FAIL                           82     Summary
TLS_TRK       DEC_FAIL                          211     Summary
TLS_TRK       DEC_CKE_FAIL                    43194     Summary
TLS_TRK       ENC_CB_FAIL                      4335     Summary
TLS_TRK       DEC_CB_FAIL                       909     Summary
TLS_TRK       DEC_CKE_CB_FAIL                   818     Summary
TLS_TRK       RECORD_PARSE_ERR                  123     Summary
TLS_TRK       IN_ERROR                        44948     Summary
TLS_TRK       ERROR_UPSTREAM_RECORD           43194     Summary
TLS_TRK       INVALID_CONTENT_TYPE              123     Summary
TLS_TRK       DOWNSTREAM_REC_CHK_ERROR          123     Summary
TLS_TRK       DECRYPT_FAIL                    43194     Summary
TLS_TRK       UPSTREAM_BY_PASS                  127     Summary
TLS_TRK       DOWNSTREAM_BY_PASS                127     Summary
```

Fatal Counters

The fatal counters indicate serious errors. These counters should be at or near 0 on a healthy system. The following example lists the fatal counters.

```
> show counters
Protocol      Counter                           Value   Context
CRYPTO        RING_FULL                             1   Summary
CRYPTO        ACCELERATOR_CORE_TIMEOUT              1   Summary
CRYPTO        ACCELERATOR_RESET                    1   Summary
CRYPTO        RSA_PRIVATE_DECRYPT_FAILED            1   Summary
```

The RING_FULL counter is not a fatal counter, but indicates how often the system overloaded the cryptographic chip. The ACCELERATOR_RESET counter is the number of times the TLS crypto acceleration process failed unexpectedly, which also causes the failure of pending operations, which are the numbers you see in ACCELERATOR_CORE_TIMEOUT and RSA_PRIVATE_DECRYPT_FAILED.

If you have persistent problems, disable TLS crypto acceleration (or **config hwCrypto disable**) and work with Cisco TAC to resolve the issues.

Note   You can do additional troubleshooting using the **show snort tls-offload** and **debug snort tls-offload** commands. Use the **clear snort tls-offload** command to reset the counters displayed in the **show snort tls-offload** command to zero.

Fatal Counters