Concurrent Offload & Encryption at 100GbE

Secure TCP/IP processing with T6 Inline-TLS/SSL Crypto Function

Executive Summary

T6 Cryptographic Offload solution produces record breaking TLS/SSL performance with inline cryptographic functions leveraging Chelsio's proprietary TCP/IP offload engine. Chelsio's full offload TLS/SSL is uniquely capable of 100Gb line rate performance. The solution supports TCP/IP and TLS/SSL AES/SHA processing in cut-through fashion to achieve optimal bandwidth and latency. An application writes Cleartext to a TLS/SSL socket and the T6 then adds the TLS/SSL PDU, encrypts and computes authentication codes. On receive, the T6 decrypts and authenticates the TLS/SSL PDU and sends Cleartext to the host.

This paper presents Chelsio T6 Inline-TLS/SSL performance, showing 100Gb line-rate bandwidth and minimal CPU usage on both Server as well as Client side. T6 delivers a consistent performance even with increasing numbers of connections while freeing up CPU resources. Hence, proving that Chelsio's T6 crypto solution is the best when it comes to delivering performance coupled with the highest data security.

Chelsio T6 Inline TLS/SSL Solution

The Terminator 6 (T6) ASIC from Chelsio Communications, Inc. is a sixth generation, high performance 1/10/25/40/50/100Gbps unified wire engine which enables concurrent secure communication and secure storage, all for the price and power of a typical NIC. T6 supports all the most popular AES/SHA cipher suites in TLS/SSL in-line mode with 100Gbps bandwidth and less than 2µs end-to-end latency. The typical T6 adapter supports 32K simultaneous TLS/SSL sessions.

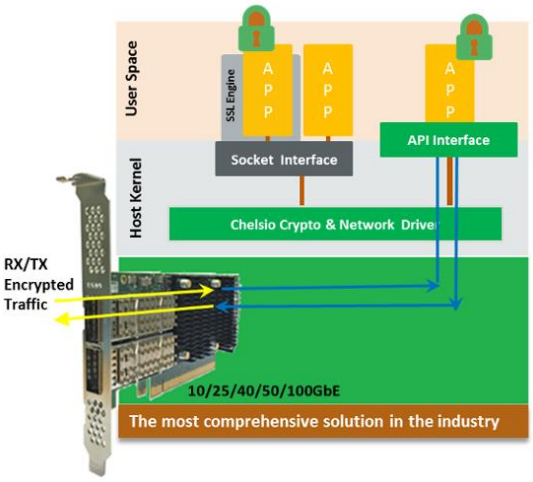

Figure 1 - Chelsio T6 Inline TLS/SSL

- T6 adapters offload the TLS/SSL PDU crypto, while handshake is still performed by the host.
- Chelsio OpenSSL modifies and provides hooks for data transmission, receive and key programming.
- Third party /customized TLS/SSL implementations are also supported.
- Supports crypto for all TLS/SSL ports.

Test Results

The following graph presents the throughput and CPU usage using Chelsio T6 crypto accelerator in Inline-TLS/SSL mode. The numbers are collected using **openssl** tool with connections ranging from 8 to 10000.

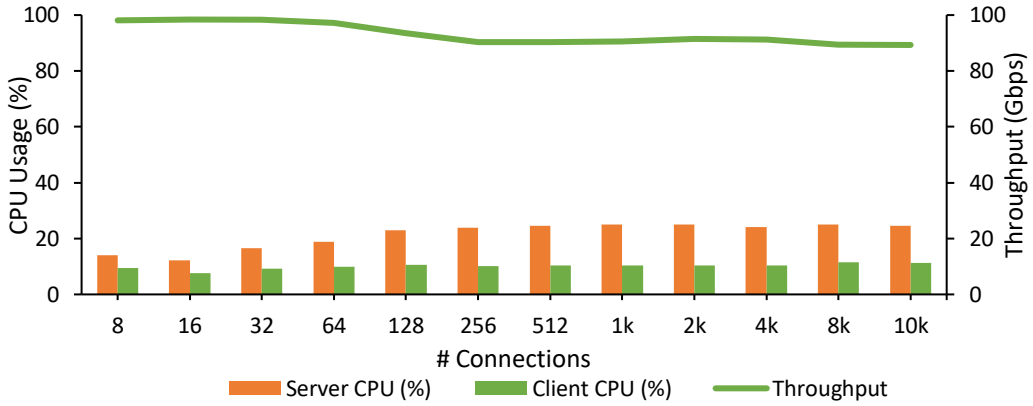

Figure 2 - Inline-TLS/SSL Throughput & CPU Usage vs. # Connections

Even with the increase in number of connections to 10000, Chelsio Inline-TLS/SSL solution maintains a flat throughput profile, delivering more than 90Gbps, while preserving the privacy and integrity of the data. The CPU usage on Server and Client never exceeded 25% even with 10000 connections, indicative of an efficient processing path. The freed-up CPU can be used for application processing.

Test Configuration

The setup consists of a server connected to a client back-to-back. MTU of 9000B was configured. Each of the machines were configured with 2 Intel Xeon CPU E5-2687W v4 12-core processors clocked at 3.00GHz (HT enabled), 128GB of RAM and RHEL 7.3 OS (kernel 4.9.13). Chelsio T62100-CR adapter was installed in each system and configured with latest Chelsio Unified Wire drivers.

Commands Used

Server

```
[root@host~]# openssl s_server -key <path_to_key> -cert <patch_to_cert> -accept
<port_num> -cipher AES128-GCM-SHA256  -WWW
```

Client

```
[root@host~]# openssl s_time -connect <IP>:<port_num>  -www /1.5G  -time 100
```

Conclusion

This paper presented performance of Chelsio's T6 Inline-TLS/SSL acceleration solution. With a consistent line-rate 100Gb performance and CPU savings even with 10000 connections, Chelsio's solutions proves to be the best choice for clients looking for highest level of data security and integrity, without compromising performance. T6 is currently the only secure engine capable of full TCP/IP Offload at 100Gbps. The in-line 100Gb encryption is achieved for an incremental latency of less than about 2µs. The introduction of integrated encryption within a NIC price and power envelope should further the migration towards secure cloud networks and storage.

Related Links

[Chelsio Terminator 6 ASIC 100GE Crypto Offload]
[The Chelsio Terminator 6 ASIC]