Apache TLS/SSL Acceleration at 100GbE

Chelsio T6 vs. Intel AES-NI vs. Software Enabled Encryption

Executive Summary

Chelsio Crypto Accelerator is a co-processor designed specifically to perform computationally intensive cryptographic operations more efficiently than general-purpose CPUs. Servers with system load, comprising of cryptographic operations, see great performance improvement by offloading crypto operations on to the Chelsio Unified Wire adapter. Chelsio's solution uses the standard crypto API framework provided by the operating system and enables the offloading of crypto operations to the adapter.

This paper showcases the Apache TLS/SSL acceleration capabilities of Chelsio T6 adapters. The paper compares Chelsio crypto accelerator's performance with Intel AES-NI and software encryption. The results showcase Chelsio crypto solution's superior throughput and CPU Utilization when an Apache serves web content to a client with multiple requests.

Chelsio Encryption Offload

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 offers crypto offload capability for AES and SHA variants. Transport Layer Security (TLS) and its predecessor Secure Socket Layer (SSL), provide network security and find widespread use in applications such as content delivery networks (CDN), web servers and Virtual Private Networks (VPN). TLS provides both privacy and integrity for data exchanged over a network. Chelsio Unified Wire adapters provide accelerated TLS/SSL solution which is well suited for site-to-site security over WAN.

Chelsio crypto accelerator secures data using AES (Advanced Encryption Standard) - the strongest encryption algorithm available. Encryption and decryption processing for TLS/SSL is offloaded on to the T6 adapter, freeing CPU resources for other tasks.

Chelsio crypto driver registers with the kernel crypto framework with high priority and ensures that encryption request is offloaded and processed by T6. SSL protocol is available as OpenSSL library or other standard implementation of SSL/TLS protocol. The *libcrypto* interface of OpenSSL uses the EVP API interface to transform crypto API into Chelsio crypto API and encrypt/decrypt the payload.

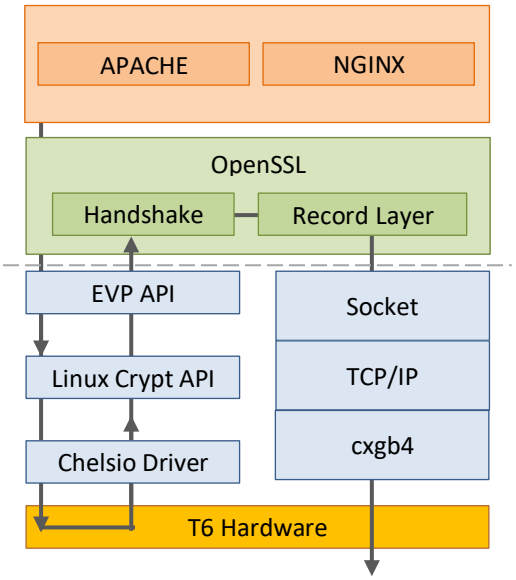

Figure 1 – T6 Apache TLS/SSL Encryption

Test Results

The following graph compares the throughput and CPU Usage in Chelsio crypto (offload), Intel AES-NI and Software (non-offload) modes using the **apache benchmark** tool varying the number of instances.

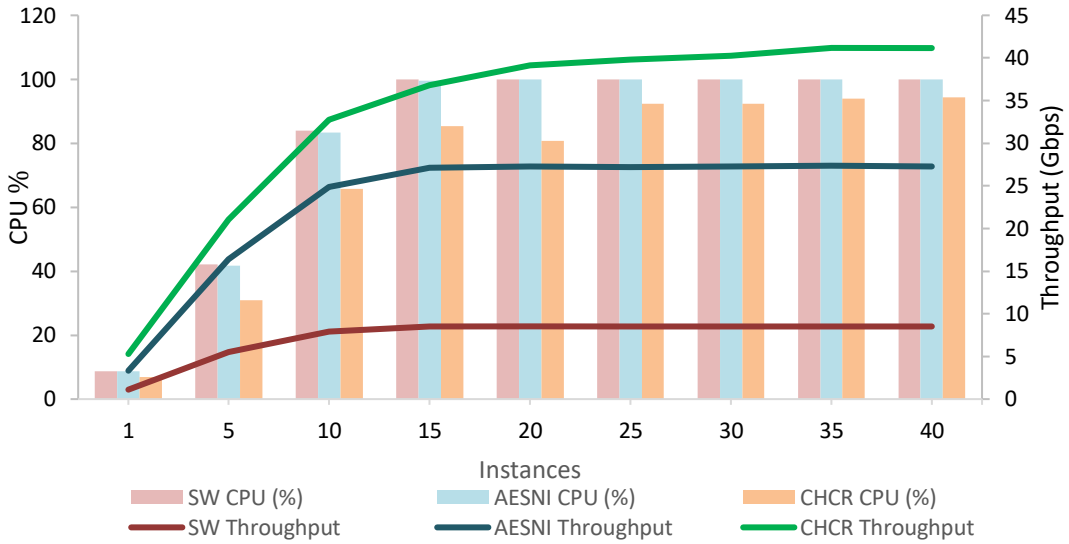

Figure 2 - Throughput and CPU% of Chelsio crypto vs. Intel AES-NI vs. Software Encryption

Chelsio crypto solution delivers consistently higher throughput even as the number of instances increase. It achieves upto 5x the performance in Software mode, proving the worth of offload. It surpasses Intel AES-NI mode as well, delivering upto 50% higher throughput. Additionally, with lesser CPU utilization, Chelsio crypto solution indicates a more efficient processing path.

Test Configuration

The setup consists of an Apache Web Server machine connected to a client machine back-to-back. MTU of 9000B was configured. The machines were configured with 1 Intel Xeon CPU E5-1660 v2 6-core processor clocked at 3.70GHz (HT enabled), 64GB of RAM and RHEL 7.3 operating system (kernel 4.9.13). Chelsio T62100-CR adapter was installed in each system and configured with Co-processor driver v1.0.0.0.

Setup Configuration

Configure Networking between Web Server and Client:

i. Install the driver package.

```
[root@host ~]# ./install.sh -i
```

ii. Reboot the machine into newly installed kernel.
iii. Install Chelsio Co-processor driver.

```
[root@host ~]# ./install.sh -d
```

iv. Load Chelsio network driver and configure connectivity between Web Server and Client.

```
[root@host ~]# modprobe cxgb4
[root@host ~]# t4_perftune.sh
[root@host ~]# ifconfig ethX <IP address> mtu 9000 up
```

v. Perform NIC tuning.

```
Sysctl tunings:
sysctl -w net.ipv4.tcp_timestamps=0
sysctl -w net.core.netdev_max_backlog=250000
sysctl -w net.core.rmem_max=4194304
sysctl -w net.core.wmem_max=4194304
sysctl -w net.core.rmem_default=4194304
sysctl -w net.core.wmem_default=4194304
sysctl -w net.ipv4.tcp_rmem="4096       87380   4194304"
sysctl -w net.ipv4.tcp_wmem="4096       16384   4194304"

[root@host ~]# ethtool -C ethX adaptive-rx on
```

Apache Server configuration:

i. Configure httpd service with your required settings by updating */etc/httpd/conf/httpd.conf* file.

ii. Respective drivers were loaded for Chelsio crypto and Intel AES-NI modes. No drivers required for Software Crypto mode.

Chelsio crypto:

```
[root@host ~]# modprobe -v chcr
```

Intel AES-NI:

```
[root@host ~]# modprobe aesni_intel
```

iii. Create a file for the Apache Server to host:

```
[root@host ~]# modprobe brd rd_size=300000
[root@host ~]# mkfs.ext4 /dev/ram0
[root@host ~]# mkdir /var/www/html/host_dir
[root@host ~]# mount /dev/ram0 /var/www/html/host_dir/
[root@host ~]# cd /var/www/html/host_dir/
[root@host ~]# fallocate -l 100M <filename>
```

iv. Restart httpd service.

```
[root@host ~]# killall -9 httpd
[root@host ~]# httpd
```

Running the Tool:

i. From the client machine, run the apache benchmark tool using 100 requests, 512K Window Size varying the number of instances:

```
[root@host ~]# for i in {1..40}; do ab -n 100 -b 524288 https://<Server IP>/host_dir/filename & done
```

Conclusion

This paper presented performance comparison of Chelsio's T6 Apache TLS/SSL acceleration solution using T62100-CR adapter. With superior throughput and lesser CPU usage, Chelsio clearly outperforms both Intel AES-NI and software enabled encryption.

As more and more information is digitized and transmitted using computer networks, the need to safely store and transfer sensitive information has become the topmost priority for most datacenters. Chelsio's Terminator 6 (T6) Unified Wire adapters enable concurrent secure communication and secure storage with support for integrated TLS/SSL/DTLS and inline cryptographic functions, leveraging the proprietary TCP/IP offload engine for acceleration. Without the need for separate infrastructure and third-party software, Chelsio provides a low-power, low-cooling, low-cost encryption acceleration along with big savings on processing power and memory.

Related Links

Accelerated IPsec-VPN Communication with T6
Disk Encryption with 100GbE Crypto Accelerator
T6 100GbE Crypto Offload Performance
Chelsio Terminator 6 ASIC 100GE Crypto Offload
The Chelsio Terminator 6 ASIC
Chelsio T6 Crypto Offload Video