Accelerated IPsec-VPN Communication with T6

Chelsio T6 vs. Intel AES-NI

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 on to the adapter.

This paper highlights Chelsio T6 Unified Wire adapters' unique accelerating capabilities for secure IPsec-based VPN connections by comparing its bandwidth and CPU usage with Intel AES-NI. T6 provides consistently higher throughput across the range of I/O sizes compared to Intel AES-NI. Furthermore, CPU usage was less than 5% across the board. Chelsio T6's IPsec-VPN solution provides enterprises with secure remote connection to access corporate applications and resources without sacrificing on performance and speed.

Chelsio VPN Acceleration

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. Internet Protocol Security (IPsec) is an end-to-end security scheme that provides protocols to ensure the authenticity, privacy and integrity of data in transit. Virtual Private Network (VPN) is a network connection that secures traffic between locations. Chelsio solution provides an accelerated IPsec-VPN tunnel 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 IPsec 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. IPsec protocol integrated in the kernel calls the crypto API framework which transforms the API into Chelsio supported crypto routines. The data is encrypted and decrypted in the loopback mode for both Tx and Rx paths.

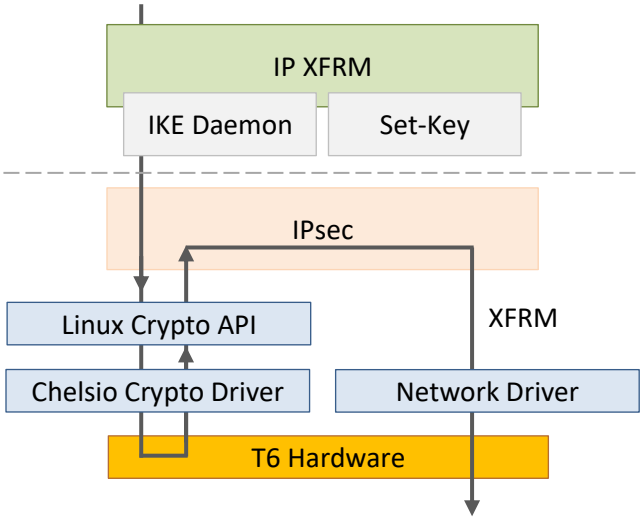

Figure 1 – T6 IPsec Acceleration

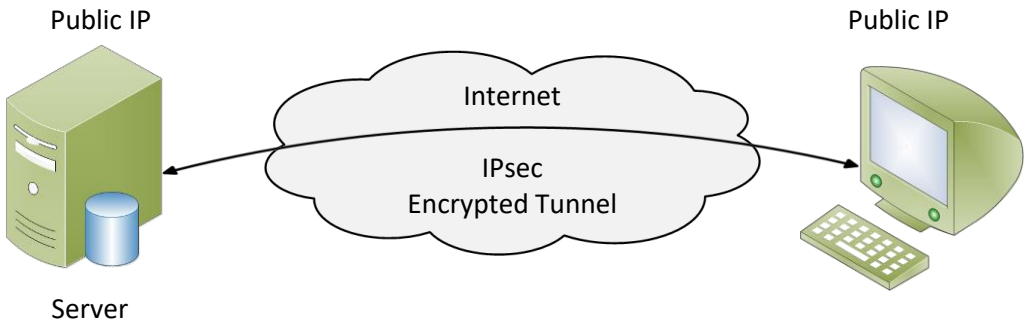

Figure 2 - IPsec Transport Mode

Test Results

The following graph compares the throughput and CPU Usage of Chelsio crypto (offload) and Intel AES-NI modes using the **iperf** tool.

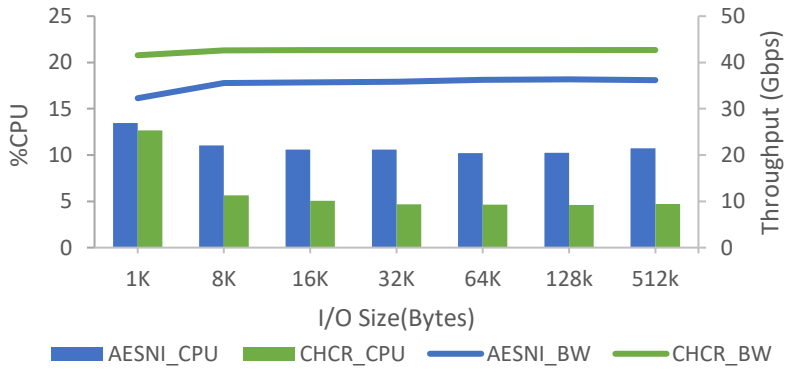

Figure 3 – Throughput and CPU % of Chelsio crypto vs. Intel AES-NI

Chelsio crypto solution delivers upto 15% higher throughput than Intel AES-NI across the range of I/O sizes. Also, evident from the graph is Chelsio's improved efficiency which is 50% less than Intel AES-NI from 8KB I/O size.

Test Configuration

The setup consists of two machines connected back-to-back using a single 100GbE port- a Server and a Client. Each system was configured with 2 Intel Xeon CPU E5-2687W v4 24-core processors clocked at 3.00GHz (HT enabled), 128GB of RAM and RHEL 7.3 operating system (kernel 4.9.13). Chelsio T62100-CR adapter was installed in each system and configured with latest Chelsio Unified Wire driver. MTU of 9000B was used.

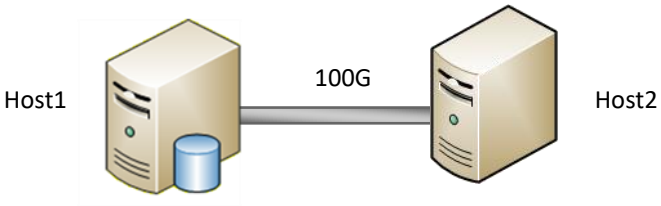

Figure 4 – Back to Back topology

Test Configuration

Following steps were executed on both the Hosts:

i. Install the 4.9 kernel with crypto components enabled.
ii. Reboot the machine into newly installed kernel.
iii. Download and install strongswan from https://www.strongswan.org/download.html
iv. Download the latest Chelsio Unified Wire package and install Chelsio Crypto accelerator driver.

```
[root@host~]# make crypto_install
```

v. Reboot the machine for changes to take effect.
vi. Chelsio network driver was loaded.

```
[root@host~]# modprobe cxgb4
```

vii. Respective drivers were loaded for Chelsio crypto and Intel AES-NI modes.

Chelsio crypto:

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

Intel AES-NI:

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

viii. IP alias was configured on Chelsio interfaces for 8 tunnels.

```
[root@host~]# for i in `seq 1 8`;do ifconfig ethX:$i $i.0.0.2/24 up;done
```

ix. CPU affinity was set.

```
[root@host~]# t4_perftune.sh -Q nic
[root@host~]# t4_perftune.sh -Q crypto
```

x. The following *sysctl* parameters were set:

```
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"
```

xi. Strongswan was configured using below steps.
   a. Remove the existing keys and certs on both hosts.

```
[root@host~]# rm -rf /usr/local/etc/ipsec.d/private/*
[root@host~]# rm -rf /usr/local/etc/swanctl/private/*
[root@host~]# rm -rf /usr/local/etc/ipsec.d/certs/*
[root@host~]# rm -rf /usr/local/etc/ipsec.d/cacerts/*
```

   b. Create keys on one host.

```
[root@host~]# cd /usr/local/sbin/
[root@host~]# ./ipsec pki --gen > caKey1.der
[root@host~]# ./ipsec pki --self --in caKey1.der --dn "C=CH, O=<domain>,
CN=<domain> CA1" --ca > caCert1.der

[root@host~]# ./ipsec pki --gen > host1Key1.der
[root@host~]# ./ipsec pki --pub --in host1Key1.der | ./ipsec pki --issue -
-cacert caCert1.der --cakey caKey1.der --dn "C=CH, O=<domain>, CN=host11"
> host1Cert1.der

[root@host~]# ./ipsec pki --gen > host2Key1.der
[root@host~]# ./ipsec pki --pub --in host2Key1.der | ./ipsec pki --issue -
-cacert caCert1.der --cakey caKey1.der --dn "C=CH, O=<domain>, CN=host21"
> host2Cert1.der
```

c. Copy the keys locally and to other host.

```
[root@host~]# cp host1Key*.der /usr/local/etc/ipsec.d/private/
[root@host~]# cp host1Cert*.der /usr/local/etc/ipsec.d/certs/
[root@host~]# cp caCert*.der /usr/local/etc/ipsec.d/cacerts/

[root@host~]# scp host2Key*.der host2:/usr/local/etc/ipsec.d/private/
[root@host~]# scp host2Cert*.der host2:/usr/local/etc/ipsec.d/certs/
[root@host~]# scp caCert*.der host2:/usr/local/etc/ipsec.d/cacerts/
```

d. Configure ipsec secrets on both hosts by updating */usr/local/etc/ipsec.secrets* file.

```
[root@host~]# cat /usr/local/etc/ipsec.secrets
# ipsec.secrets - strongSwan IPsec secrets file
include /usr/local/etc/ipsec.secrets
: RSA /usr/local/etc/ipsec.d/private/host1Key1.der
```

e. Configure *ipsec.conf* on both hosts.

```
[root@host~]# cat /usr/local/etc/ipsec.conf
config setup

conn %default
 ikelifetime=60m
 keylife=20m
 aggressive=yes
 rekeymargin=3m
 keyingtries=1
 keyexchange=ikev2

conn host1-host2-p1
    left=1.0.0.2
    leftcert=host1Cert1.der
    leftid="C=CH, O=<domain>, CN=host11"
    leftfirewall=yes
    right=1.0.0.3
    rightid="C=CH, O=<domain>, CN=host21"
    type=tunnel
    esp=aes256-sha256!
    auto=add
```

f. Start the IPsec tunnel.

```
[root@host~]# cd /usr/local/sbin/
[root@host~]# ./ipsec start
[root@host~]# ./ipsec up conn host1-host2-p1
```

xii. Strongswan was configured for 8 tunnels using the Steps in (xi).

xiii. iperf servers with 8 different IP alias were started on Host1.

```
[root@host~]# for i in `seq 1 8`; do taskset -c 0-23 iperf -s -w 512k -p 500$i
& done
```

xiv. Connections to the listening servers were established from the Host2.

```
[root@host~]# for i in `seq 1 8`; do taskset -c $i iperf -c $i.0.0.2 -p 500$i
-w 512K -l <I/O size> -t 30 & done
```

Conclusion

This paper presented performance comparison of Chelsio's T6 IPsec-VPN solution and Intel's AES-NI using T62100-CR adapter in Linux. Chelsio outperformed Intel AES-NI with a consistently higher throughput across the range of study. In addition, Chelsio's CPU usage was half of Intel's indicative of a more efficient processing path. Chelsio's T6 low-cost IPsec-based VPN solution provides data transfer with high accuracy and speed without affecting integrity and confidentiality.

Related Links

Apache TLS/SSL Acceleration at 100GbE
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