SSL/TLS with ToE Engine

Xilinx Alveo powers SSL/TLS Acceleration

VVDN TECHNOLOGIES

XILINX

SOLUTION BRIEF

XILINX ALVEO™

INTRODUCTION

Secure Socket Layer (SSL) or Transport Layer Security (TLS) with a full TCP offload Engine (ToE) on Xilinx® Alveo™ Card is ideal for improving system level performance as it provides a complete offload of TCP and Crypto operations.

Transmission Control Protocol/Internet Protocol (TCP/IP) and SSL/TLS network communication imposes significant overhead on the CPU, so in order to improve performance over CPU based implementation, the network accelerator processes the entire TCP/IP stack and crypto operations on Alveo card.

KEY BENEFITS

- Offloads the SSL/TLS and ToE to FPGA
- Saving CPU cores by offloading the L2-L5 packet processing tasks
- Ideal platform for acceleration of secure network functions
- High performance hardware based cryptography
- Lesser RAM and CPU core requirement for the FPGA supported software Framework.

- Industry proven TCP Offload Engine (ToE) and Crypto engine
- Maximum bandwidth delivered with low latency
- Having L2-L5 layer processing on FPGA, CPU is available for other critical tasks.

SOLUTION OVERVIEW

- TCP offload engine processes ARP, ICMP, IGMP Packets without host involvement
- 32 bit AXI 4 lite slave control interface for MAC and TCP configuration
- DMA operations are performed by using Xilinx ® QDMA IP
- The FPGA crypto block work inline with the Host CPU
- TLS application data inline support
- The TLS control plane is handled by host stack which require details for data-plane. This will be offloaded to the HW solution from the software during the TLS handshake process
- The inbuilt solution helps any insecure application to work on a secure environment without application over heads for TLS packet processing
- Support available over Open SSL package
- QSFP28 cages are used for 25G Ethernet support

XILINX

Adaptable. Intelligent.

SECURE SOCKET LAYER (SSL)

VVDN TECHNOLOGIES XILINX

Xilinx Alveo powers SSL Acceleration

SOLUTION DETAILS

- Supports Symmetric and Asymmetric operations
- Supports Look-aside and Inline mode
- Multiple connection support by TCP offload engine
- 25 /10G Full duplex throughput
- Up to 2K simultaneous TCP connections or TLS sessions
- 45-50% Logic utilization (includes 10/25G MAC and PCIe DMA)
- Supports RSA2K/4K, AES128/256-GCM operations
- Off chip memory of 64 GB
- Internal SRAM capacity 35 MB

RESULTS

in Gbps	10G Solution	25G Solution
TX Throughput (TOE alone)	8.8	18.2
RX Throughput (TOE alone)	8.8	22
HTTPS Throughput	8	18

RSA-4K			
in ops/sec	SW	FPGA	Gain
Sign	364	2852.5	7.84
Verify	23441	108961	4.65

AES-GCM			
in Gbps	SW	FPGA	Gain
Encryption	2.18	17.43	7.99x
Decryption	2.18	17.08	7.84x

TAKE THE NEXT STEP

Learn more about Xilinx Alveo accelerator cards
Learn more about Partner: https://www.vvdntech.com/
Reach out to VVDN sales:
Vinod Soman: vinod.soman@vvdntech.com (US Sales)
Nitin Jain: nitin.jain@vvdntech.com (India Sales)

XILINX

Adaptable. Intelligent.