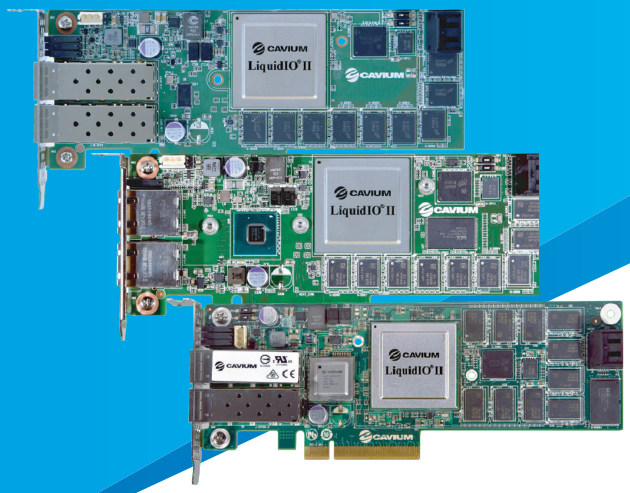
LiquidIO®II IPsec for Data Center Security



Secure Data Center Traffic with High Performance Security Adapter with Data Encryption and Data Privacy while reducing TCO

SECURITY IN THE DATA CENTER

With the increasing data security breaches, encrypting and protecting data-in-flight and data-at-rest in data centers has gained the highest priority for data center security. To address the challenges of securing the perimeter and within the data center from unlawful intercepts, protect data integrity and confidentiality, Cloud Data Centers are increasingly encrypting data within and across data centers, adding strict security policies by deploying firewalls at the network edge and at server access.

HOST BASED ENCRYPTION IS CPU INTENSIVE

As data centers encrypt network and storage traffic, the traditional host-based encryption model cannot scale in performance. With the increased adoption of virtualization, SDN, and multi-tenancy in data centers, computing resources are in high demand.

Encryption is a very compute intensive application using up a lot of host CPU cores. There are fewer CPU cores left to execute applications as more CPU cores are allocated for encrypting data. This makes it cost prohibitive, with increasing TCO and inadequate performance.

LiquidIO II offloads IPsec packet processing from the host, freeing up CPU resources for application execution. LiquidIO Smart NIC efficiently encrypts the packet at line-rate (10G/25G) without burdening the host CPU cores. In addition, its multi-core architecture can offload additional network features onto the smart NIC efficiently while maintaining optimal performance, overall compute resource scalability, and reducing the overall TCO.

ABOUT LIQUIDIO II SMART NIC

LiquidIO II 10G and 25G Smart NIC leverages Cavium's industry leading security expertise offering line-rate performance with zero host CPU utilization, delivering the most efficient IPsec offload solution with end-to-end data protection. LiquidIO IPsec solution supports both Tunnel and Transport modes of operation and with the multi-core programmable architecture allows data centers to develop new custom network and security features for an evolving Software Defined Data Center.

This product family integrates security, encryption and advanced networking capabilities with on to a single adapter including:

- Stateless Offloads - RSS, TSO, LRO and checksum offloads
- Overlay Offloads - VXLAN, NVGRE, GENEVE
- Hardware based I/O Virtualization
- IPsec Offload (AH and ESP)
  - Tunnel and Transport mode
  - Encryption Algorithms: NULL, DES-CBC, 3DES-CBC, AES (128, 192, 256)-CBC & AES (128, 192, 256)-CTR
  - Authentication Algorithms: NULL, HMAC-MD5, HMAC-AES-XCBC, HMAC-SHA1, HMAC-SHA (256, 384, 512)
  - AEAD Algorithms: AES (128, 192, 256)-GCM
  - IKE Compliance: v1 and v2
- Open Virtual Switch Offload and Acceleration
  - OVS 2.8 full offload with NAT and Connection Tracking
- OVS Full offload with IPsec encryption
  Fully programmable architecture for additional custom offloads with mature toolchain support

Offloading and Accelerating IPsec with LiquidIO® Smart NICs

USE CASES

- LiquidIO II IPsec solution encrypts data and secures the traffic for these scenarios:

1. Site-To-Site VPN: LiquidIO is used to encrypt and secure traffic across two or more sites, acting as a gateway at each location and encrypting and securing data across these locations. The VPN gateway acts as an aggregator encrypting data coming from different clients (tunnels) within a site. Similarly, on the other end of this VPN connection, a LiquidIO based VPN gateway decrypts the network traffic to be delivered to the destination clients. Multiple LiquidIO can be deployed to increase the overall IPsec bandwidth without burdening the CPU, hence reducing the TCO.

2. Client(s) to Gateway: In this scenario, LiquidIO is deployed as a VPN gateway point accepting incoming traffic from clients. Here also, the packet encryption is done on LiquidIO, without burdening the host CPU, hence reducing the TCO.

3. Host-To-Host: With Virtualization, SDN, virtual switching and routing, data centers need to maintain confidentiality even for east-west traffic within the datacenter, between hosts and the VMs on each host. Using the IPsec Transport mode where the host initiates encryption. LiquidIO IPsec Transport mode encrypts the traffic and forwards the encrypted packet to the specific host.

BEST-IN-CLASS PERFORMANCE FOR IPSEC OFFLOAD PROCESSING

In the benchmarking tests, two servers were directly connected to each other with one adapter in each server. While measuring throughput and CPU utilization in both servers, an IPsec tunnel was established between two servers. Three scenarios were tested.

1. For the first benchmarking test case, a standard NIC (competitor host-based NIC) was used in each server running host based IPsec Software for traffic encryption.

2. The next benchmark test case used an FPGA-based IPsec offload solution. The competitor FPGA-based Smart NIC offloaded the IPsec encryption to the FPGA.

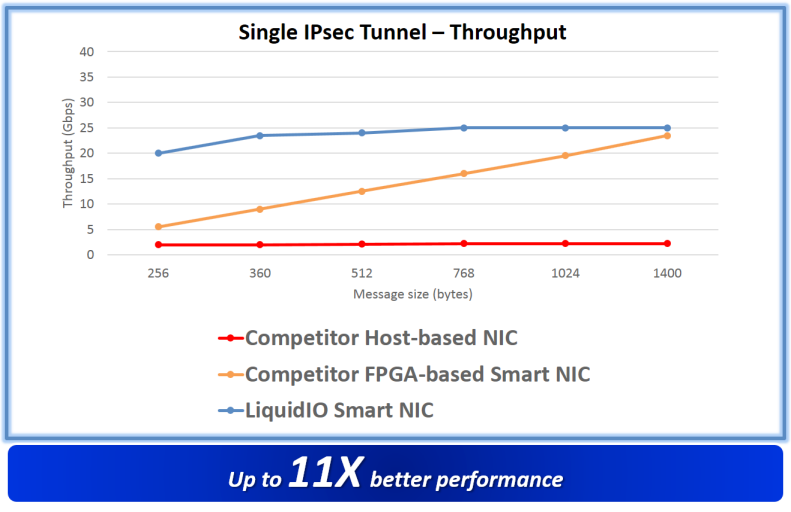
3. In the final benchmark test case, a LiquidIO Smart NIC was used to offload the IPsec encryption to its multi-core processor.

THROUGHPUT GAINS

Figure 1 shows the throughput comparison results: LiquidIO based IPsec encryption achieved up to 11X higher throughput compared to host-based IPsec encryption and up to 4.4X higher throughput compared to FPGA-based IPsec encryption at 256B packet size and maintains the performance at bigger message sizes.

Comparing the three solutions-

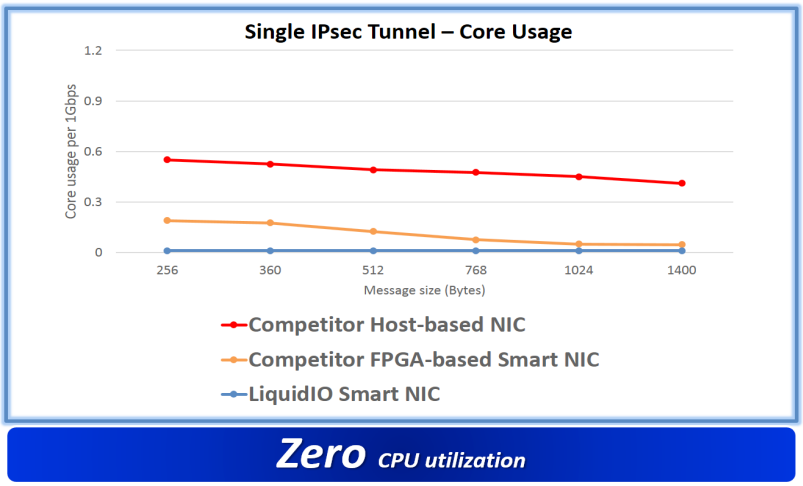
Liquid IPsec solution provides not only higher throughput (11x gain), but also eliminates the data processing burdens from the host CPU with its hardware-based encryption/decryption architecture. In the case of the FGPA-based IPsec Offload, the performance only increases with bigger message sizes. This clearly shows that LiquidIO IPsec offload provides the best-in-class performance.



[Figure 1: IPsec Throughput]

CPU SAVINGS

Figure 2 shows the host CPU resource used to establish IPsec tunnels with encryption. The chart shows the calculated host CPU usage per 1Gbps throughput. LiquidIO IPsec offload uses almost zero host CPU cores regardless of message sizes while other solutions use higher number of host CPU cores.



[Figure 2: CPU Utilization]

CONCLUSION

Cavium IPsec software provides the ability to accelerate the IPsec processing and encryption using LiquidIO Smart NIC. LiquidIO provides key benefits such as flexibility with different deployment scenarios, best-in-class performance, no CPU utilization, and securing data center traffic, while lowering the TCO significantly compared to the other two solutions.

ABOUT CAVIUM

Cavium, Inc. (NASDAQ: CAVM), offers a broad portfolio of infrastructure solutions for compute, security, storage, switching, connectivity and baseband processing. Cavium's highly integrated multi-core SoC products deliver software compatible solutions across low to high performance points enabling secure and intelligent functionality in Enterprise, Data Center and Service Provider Equipment. Cavium processors and solutions are supported by an extensive ecosystem of operating systems, tools, application stacks, hardware reference designs and other products. Cavium is headquartered in San Jose, CA with design centers in California, Massachusetts, India, Israel, China and Taiwan.

CAVIUM™

Follow us:

Corporate Headquarters Cavium, Inc. 2315 N. First Street San Jose, CA 95131 408-943-7100