WHITE PAPER

Mellanox Innova™ IPsec:

Achieve Groundbreaking Security for VPN, Data Privacy & Data-in-Motion, while Reducing Total Cost of Ownership (TCO)

THE DATA CENTER ENCRYPTION CHALLENGE

As cyber-attacks increase in sophistication and effectiveness, the once popular perimeter security scheme can no longer be relied upon to effectively protect the data center from such threats.

Growing concerns over traffic interception, as well as the collection and use of unencrypted information, have kindled a global desire for privacy protection. This has led to a massive increase in the use of encryption to protect data-in-motion and data-at-rest in the data center, not to mention the additional security functionality now being implemented at the server access layer (such as firewall, load balancing, virtual switching, and virtual routing) and the exponential growth in network communication processing. Indeed, encryption is the new standard for cloud-based applications where it protects the confidentiality and integrity of data passed between locations. Encryption is also progressively used to protect lateral traffic inside the data center.

KEY USE CASES

- Site-to-Site VPN Tunnel
- VPN Tunnel Aggregation
- Host-to-Host Encryption

This paper introduces an advanced, high performance network controller that addresses multiple encryption needs and architectures. The network controller provides up to 6X more throughput than software-only solutions, using fewer CPU cores, while dramatically reducing Total Cost of Ownership (TCO).

Today's Server CPU Cannot Cope with the Growth in Encryption Needs

As encryption is a compute intensive application, software / CPU-based encryption solutions cannot scale to meet modern data center needs. Consequently, fewer CPU resources are being allocated for application execution while more are being allocated for crypto operations.

Mellanox Innova™ IPsec adapter offloads the processing of the IPsec encryption algorithm, freeing up valuable CPU resources, and easing network bottlenecks. IPsec is a protocol suite for secure Internet Protocol (IP) communications that authenticates and encrypts each IP packet of a communication session. The Mellanox Innova IPsec adapter card delivers 40Gb/s IPsec traffic with lower CPU utilization, enabling the efficient use of CPU resources to be dedicated to application execution.

The combination of encryption offload with advanced network capabilities in a single adapter maintains the adapter's network offloads, contributing to a decrease in CPU utilization and a better Total Cost of Ownership (TCO) compared to discrete encryption acceleration solutions.

INTRODUCTION TO MELLANOX INNOVA™ IPsec

Mellanox Innova IPsec network adapter provides transparent security acceleration for IPsec-enabled networks. Leveraging the Mellanox ConnectX® family of network controllers' best-in-class performance, unmatched scalability, and efficiency, Innova IPsec adapter is a versatile solution based on Mellanox ConnectX-4 Lx network adapter and Xilinx Kintex UltraScale FPGA. The adapter integrates advanced network capabilities and encryption offloading in one card, while utilizing only a single PCIe slot for both networking and crypto to provide a wide range of CPU offloads and advanced network capabilities, including:

- Cloud (e.g. virtual switching, overlay networks), HPC, and storage offloads
- Hardware-based I/O virtualization
- Ethernet stateless offloads
- AES-GCM, AES-CBC encryption/ decryption and authentication algorithm offloads
- IPsec HMAC-SHA1 and HMAC-SHA2 (224, 256, 384, 512 key length) authentication
- Native low-latency RDMA over converged Ethernet (RoCE)
- End-to-end QoS and congestion control

Use Cases

Mellanox Innova IPsec addresses multiple encryption needs and architectures as described in the following use cases:

- **Site-to-Site VPN Tunnel**
  In site-to-site scenarios, VPN gateways are used in order to encrypt traffic between two, or more, locations protecting the confidentiality and integrity of the data passed between the locations. Mellanox Innova IPsec can be deployed as an IPsec accelerator on the gateways at each site of the communication link. The VPN gateways can then offload the encryption of network traffic to the Innova IPsec card, relieving the CPU to perform other tasks. Using one, or multiple, Innova adapters per VPN gateway increases the IPsec bandwidth supported, and thus reduces the TCO of such solutions as fewer VPN gateways will be required.

- **Client-to-Site VPN**
  Mellanox Innova IPsec can be deployed as an aggregation point for incoming VPN connections. Similar to the previous scenario, it offloads the encryption task and frees up CPU cycles on the VPN gateway. A typical VPN tunnel aggregator will support a few thousands of VPN tunnels, with each connected to a different client device. Although the traversed data rate in each tunnel is not high, the total bandwidth and large number of tunnels require a high-end server to manage the task. Mellanox Innova IPsec is capable of connecting up to 50K tunnels per server, per Mellanox Innova IPsec card, while maintaining high bandwidth for each tunnel.

- **Host-to-Host Encryption**
  Many of today's datacenter administrators no longer rely only on perimeter security. Encryption, serving as an increasingly popular means to secure the internal network from unauthorized access and eavesdropping, also has high performance impact. Moreover, as the CPUs on the datacenter hosts have been purchased to perform application and not security tasks, every CPU cycle used for encryption is done so at the cost of revenue-creating application cycles. Mellanox Innova IPsec significantly eases this burden by enabling up to 40GbE of encrypted data, freeing up the CPU to accelerate application performance.

IPSEC OFFLOAD PERFORMANCE GAINS

The figure below compares a typical CPU-based encryption solution (on the left side) to an encryption solution based on Mellanox Innova IPsec (right side). It highlights the performance gains when using Mellanox Innova IPsec adapter cards.ing Mellanox Innova IPsec adapter cards.

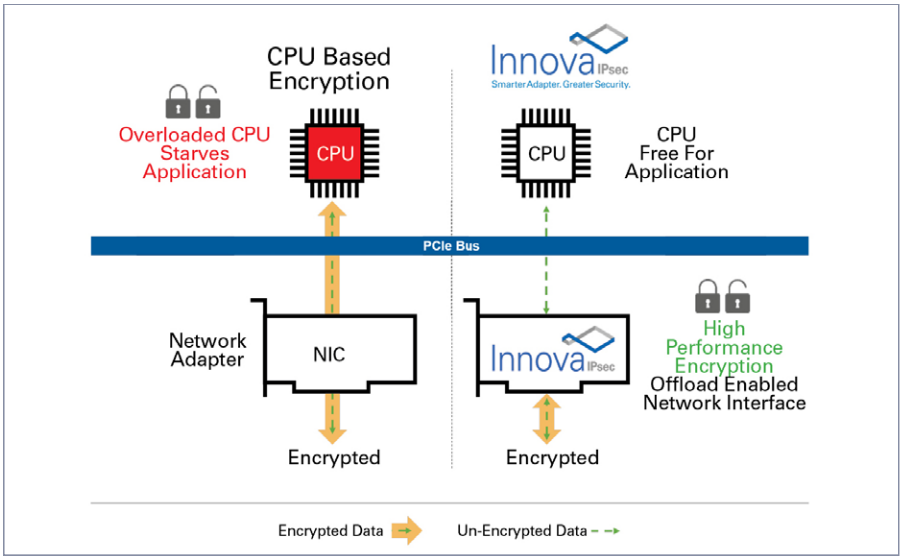

Figure 1. CPU-based Encryption Solution vs Innova IPsec Offload

Up to 6X Throughput Gains

In the following tests, two servers were directly connected to each other. An IPsec tunnel was opened between the servers, while traffic and CPU utilization were measured. In one case, software was used to perform IPsec-based encryption (noted as "CPU-based crypto" in red). In a second case, the encryption offload was performed by Mellanox Innova IPsec (dotted green). A third scenario involved measuring standard unencrypted traffic (blue).

Figure 2 represents the throughput comparison results: Mellanox Innova IPsec-based encryption achieves up to 6X higher throughput - nearly matching the throughput in the scenario where no encryption was used.

A single stream of encryption is problematic as it has lower bandwidth and higher latency, and thus requires more compute resources from CPUs/hosts. Mellanox Innova IPsec goes beyond competing offerings to mitigate this limitation by hardware-offloading the encryption-decryption operations that otherwise the CPU would have to perform.

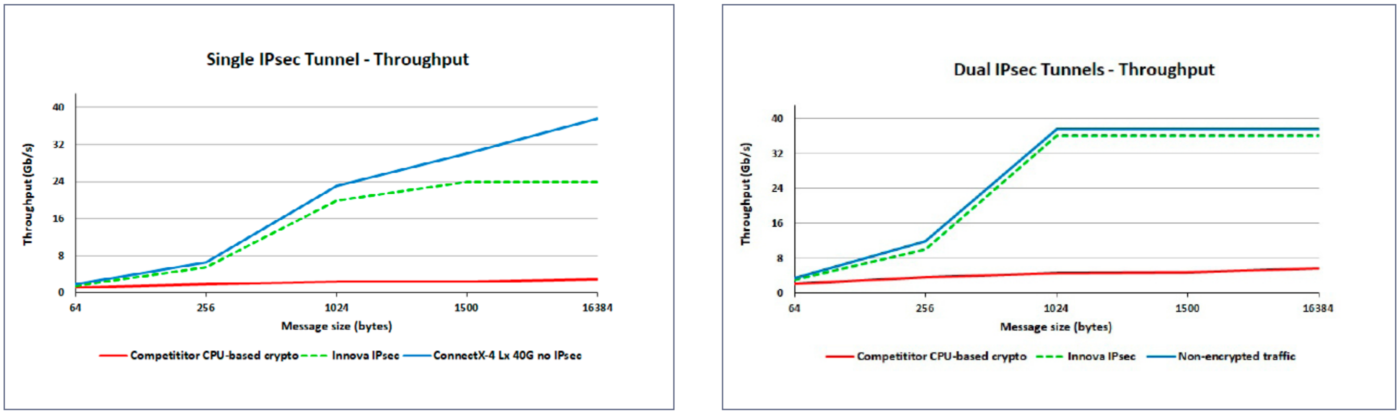

Figure 2. IPsec Throughput: Innova IPsec versus CPU-based Crypto

Up to 10X CPU Savings

Figure 3 shows the CPU resources needed to establish IPsec tunnels (calculated per 1Gb/s of IPsec traffic). As indicated in the chart below, Innova IPsec solution is 10X more efficient than CPU-based encryption.

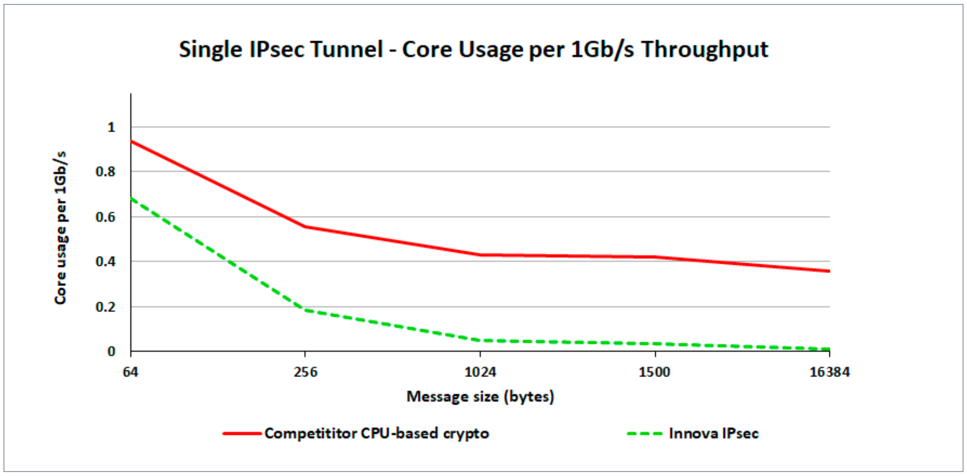

Figure 3. CPU Cores for IPsec Encryption (per 1Gb/s of IPsec traffic)

MELLANOX INNOVA'S ARCHITECTURE ADVANTAGE

Alternative IPsec solutions are comprised of a CPU with a PCI accelerator for encryption, built into a look-aside architecture. In such an architecture, the data is moved from the CPU to the accelerator ("on the side") for encryption and then back to the CPU before being transmitted to the network. Alternatively Mellanox Innova IPec offers a simple and efficient inline architecture as network traffic is encrypted/decrypted as it passed through the card.

Improved CPU Utilization

Compared to the look-aside approach, the Mellanox inline approach provides better performance and flexibility, and is more transparent to the user as it encrypts the data on its way to the network. The inline acceleration architecture handles all encryption tasks in the Mellanox Innova IPsec card as the data traverses through the network controller; thus offloading the compute heavy datapath crypto activities from the CPU.

Networking Offloads Enabled

Encryption/decryption is performed as a bump-on-the-wire; as such the offloads supported by ConnectX 4-Lx can also be used. Heavy networking operations such as virtual networking (e.g. Open vSwitch), VXLAN and others can be offloaded, significantly improving performance and further reducing the load from the CPU. In alternative solutions, where all encrypted data is passed from the network to the CPU, the adapter is mostly "blind" and cannot perform many of its offloads against the passing network traffic as it is encrypted, overloading the CPU with additional network-related tasks.

Minimized PCIe Traffic

With the inline acceleration architecture of Innova IPsec, the encryption is done at the same data pass, without additional PCIe requests as opposed to the alternative solution in which data traverses over the PCIe three (3) times. This reduces latency and prevents overloading the PCIe bus.

Efficient PCIe Lane and Slot Utilization

Mellanox Innova IPsec combines networking and encryption acceleration in a single adapter card. Contrary to the look-aside solution, it uses only one PCIe slot and 8 PCIe lanes; there's no need for additional slots nor dedicated lanes.

CONCLUSION

The Mellanox Innova IPsec Adapter Card lowers the overall TCO of server clusters by providing an efficient IPsec encryption offload from the CPU, freeing up valuable CPU cycles for application processing. Taking advantage of the ConnectX network controller combined with a Xilinx™ FPGA accelerator, Mellanox Innova IPsec takes accelerates security for IPsec-enabled networks, with best-in-class performance and efficiency. Moreover, Mellanox Innova IPsec inline architecture delivers the benefits of full CPU offload, without requiring additional PCIe resources. The offload provides significant performance gains and over 6X more throughput, with lower CPU utilization.

About Mellanox

Mellanox Technologies (NASDAQ: MLNX) is a leading supplier of end-to-end Ethernet and InfiniBand intelligent interconnect solutions and services for servers, storage, and hyper-converged infrastructure. Mellanox intelligent interconnect solutions increase data center efficiency by providing the highest throughput and lowest latency, delivering data faster to applications and unlocking system performance. Mellanox offers a choice of high performance solutions: network and multi-core processors, network adapters, switches, cables, software and silicon, that accelerate application runtime and maximize business results for a wide range of markets including high performance computing, enterprise data centers, Web 2.0, cloud, storage, network security, telecom and financial services.
More information is available at www.mellanox.com.

350 Oakmead Parkway, Suite 100, Sunnyvale, CA 94085
Tel: 408-970-3400 • Fax: 408-970-3403
www.mellanox.com