SOLUTION BRIEF

Communications Service Providers
Network Security

Silicom* Boosts TLS Speed with Intel® QuickAssist Technology

Silicom and Intel test TLS handshakes performance on servers with Intel® Xeon® Platinum processors and find that the addition of Intel® QuickAssist Technology results in 3.92 times total speed up.[1]

Silicom Ltd.
Connectivity Solutions

Servers in data centers are being pushed to their limits by CPU-intensive workloads, virtualization overhead, and increased encryption/decryption requirements to secure data flows, especially for web applications. Specialized accelerator engines that are optimized to accelerate a particular function, such as virtualization, security, or network traffic processing, are one way to improve overall processing performance.

The impact of encryption on web and data center servers is significant as enterprises consider "encrypt everything" strategies and as new encrypted data flows from mobile and internet of things (IoT) systems add to the workload. Processing these data flows at 10 Gbps and faster network speeds consumes an increasing number of CPU cycles, impacting the processing of other workloads.

Intel offers its Intel® QuickAssist Technology (Intel® QAT) to accelerate encryption and decryption workloads. To test the impact of Intel QAT on servers powered by Intel® Xeon® Scalable processors, Intel worked with Silicom,* an Intel® Network Builders ecosystem member and expert in encryption acceleration technology, to demonstrate the performance advantage of Intel QAT in a web server application.

Intel® QuickAssist Technology

Intel QAT is a hardware accelerator for cryptographic and compression algorithms. Intel QAT can be added to a server via the Intel® C620 series chipsets, which can be implemented as an on-board accelerator or added as standalone accelerator plug-in cards. Intel QAT is also integrated in Intel® SoCs (system on a chip) such as the Intel Xeon processor D family, as well as the Intel Atom® processors C2000 and Intel Atom processors C3000. The Intel QAT accelerators for cryptography, public key, and compression enable users to develop high performance networking, storage, cloud, or big data applications while recapturing CPU cycles. Intel QAT supports the following algorithms:

- Symmetric cryptography functions such as: cipher operations (AES, DES, 3DES, ARC4); wireless (Kasumi, Snow, 3G); hash/authenticate operations (SHA-1, MD5, SHA-2 [SHA-224, SHA-256, SHA-384, SHA-512]); authentication (HMAC, AES-XCBC, AES-CCM); random number generation
- Public key functions such as: RSA operation; Diffie-Hellman operation; digital signature standard operation; key derivation operation; elliptic curve cryptography (ECDSA and ECDH) random number generation and price number testing
- Compression/decompression such as: DEFLATE (Lempel-Ziv 77)

Intel QAT has an application programming interface (API) that allows an application to interface with the Intel QAT hardware and access the features of the accelerator.

The API is independent of operating systems and can be used in either user or kernel space. Developers can leverage the API across different products, reducing software development efforts.

Measuring Intel QAT Performance

To measure the impact of Intel QAT on servers based on its latest processors, Intel worked with Silicom to test the performance of an Intel Xeon Platinum 8168 processor-based server with and without embedded Intel QAT capabilities. Silicom provided its high-performance network controller adapter and its expertise in Intel QAT.

Silicom's expertise in encryption acceleration comes from its development of Intel QAT-based acceleration add-on cards and network controllers, including the PE316ISLBEL, a PCIe* 3.0 crypto and compression acceleration server adapter, based on the Intel C620 series chipsets. The adapter is Silicom's third generation of adapters to integrate Intel QAT.

In setting up the test, Silicom chose its PE340G2QI71 dual-port, 40 GbE PCI Express network server adapter. The PE340G2QI71 is based on the Intel® Ethernet Controller XL710-BM2. While this controller supports Intel's hardware acceleration capabilities for TCP/UDP/IP checksum calculations and TCP segmentation, it doesn't include Intel QAT since this functionality is deployed on the server.

The server under test features the Intel Xeon Platinum 8168 processor, a CPU from the Intel Xeon processor Scalable family designed to offer extremely high performance. Intel Xeon Scalable processors are already optimized for encryption processing through the inclusion of Intel® Advanced Vector Extensions 512 (Intel® AVX-512), a new CPU instruction set designed for processing of encryption algorithms. Intel AVX-512 reduces the performance overhead for cryptography, enabling more data and services to be deployed with built-in security features.

The integrated Intel QAT technology in the server is designed for crypto and PKE workload acceleration at 100 Gbps utilizing Intel® Key Protection Technology (Intel® KPT), a new feature that provides efficient key and data protection for trusted digital service delivery. Increased platform security features come from Intel® Platform Trust Technology (Intel® PTT) and Intel® Trusted Execution Technology (Intel® TXT) with new One-Touch Activation capability, which eases the deployment of Intel TXT.

Test Results

Transport layer security (TLS) is a widely adopted encryption protocol in use by web servers to encrypt/decrypt data streams across the internet. Servers with accelerated TLS performance can process more encrypted data flows without impacting the performance of the CPU.

To see just how much more performance could be obtained with the use of Intel QAT, Intel and Silicom constructed a series of benchmark tests to measure asymmetric HTTPS RSA2048 connection establishment using an NGINX* web server using Intel QAT, with comparison to software-only NGINX performance. This TLS handshake process is the most CPU intensive part of the entire session.

The tests[1] compared a baseline server with dual 48-core Intel Xeon Platinum 8168 processors with 192 GB of memory with an equivalent server that also featured the Intel C628 chipset. Both servers featured turbo and HT on. The objective was to maximize processing of Open SSL (v1.1.0e) connections on a test web server powered by NGINX 1.10.3.

The testing showed several improvements in performance for the Intel QAT-equipped server. As shown in Figure 1, connections per second increased by 1.4 times, while concurrent session support doubled.[1]

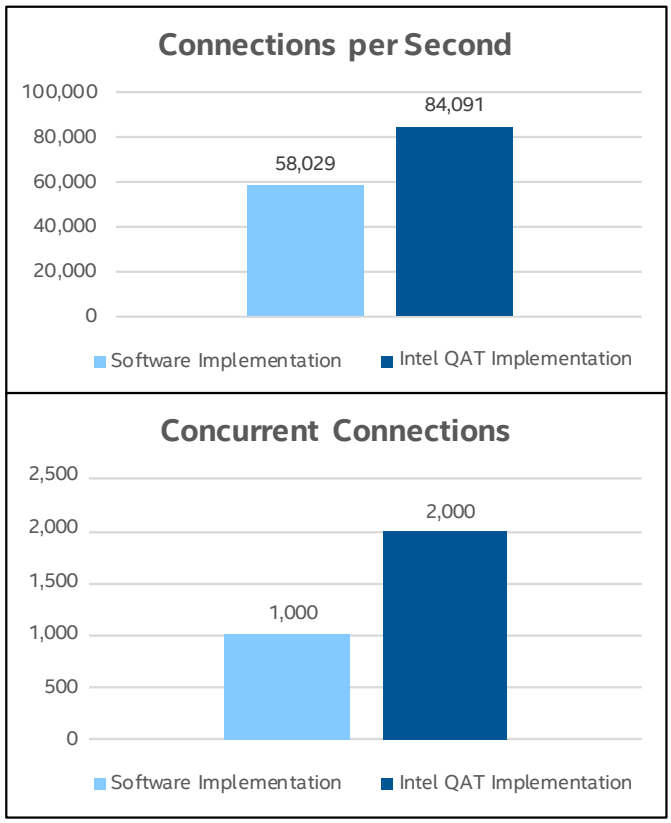

Figure 1. OpenSSL performance improvements utilizing Intel QAT.[1]

When accumulating all of the performance improvements, the result is 3.92 times total speedup, meaning that when using Intel QAT this workload requires only 25 percent of the server's CPU cycles compared with software-only implementation.[1]

Conclusion

Recognizing the importance of encryption to today's computing and communication infrastructure, Intel has built performance enhancements into its latest generation of Intel Xeon processors. And as the tests conducted by Silicom demonstrate, these high-performance CPUs can be further improved by the addition of Intel QAT.

About Silicom Ltd.

Silicom Ltd. is a provider of high-performance networking and data infrastructure solutions. Silicom's solutions are designed primarily to improve performance and efficiency in cloud and data center environments. Its innovative solutions

for high-density networking, high-speed fabric switching, and acceleration, which utilize a range of cutting-edge silicon technologies as well as FPGA-based solutions, are designed for scaling-up and scaling-out cloud infrastructures. Silicom products are used by major cloud players, communication service providers and OEMs as components of their infrastructure offerings, including both add-on adapters in the data center and stand-alone virtualized/universal CPE devices at the edge. Silicom's long-term, trusted relationships with more than 150 customers throughout the world, its more than 400 active design wins and more than 300 product SKUs have made Silicom a "go-to" connectivity/performance partner of choice for technology leaders around the globe.

About Intel® Network Builders

Intel® Network Builders is an ecosystem of infrastructure, software, and technology vendors coming together with communications service providers and end users to accelerate the adoption of solutions based on network functions virtualization (NFV) and software defined networking (SDN) in telecommunications and data center networks. The program offers technical support, matchmaking, and co-marketing opportunities to help facilitate joint collaboration through to the trial and deployment of NFV and SDN solutions. Learn more at **http://networkbuilders.intel.com**.

[1] Testing conducted by Silicom Systems. Baseline: Dual Intel® Xeon® Platinum 8168 processors with 48 cores, turbo and HT on, 192 GB total memory, 12 DIMMs/16 GB/2666 MT/s /DDR4 LRDIMM, 1 x 800 GB, NGINX 1.10.3, OpenSSL 1.1.0e. New: Dual Intel® Xeon® Platinum 8168 processors with 48 cores, turbo and HT on, Intel® C628 chipset, 192GB total memory, 12 DIMMs/16 GB/2666 MT/s DDR4 LRDIMM, 1 x 800 GB , NGINX 1.10.3, OpenSSL 1.1.0e, QAT_Engine 1.0, QAT1.7 Upstream 1.0.1.28.

0418/DO/H09/PDF ♻ Please Recycle 337315-001US