F5 Accelerates Cryptographic Processing with Intel® QAT

Bandwidth increases from 5G and IoT networks along with increased demand for crypto workloads challenge application performance. F5 tested its BIG-IP Virtual Edition application delivery controller software suite with Intel® QuickAssist Technology (Intel® QAT) and saw dramatic performance increases in throughput and transactions along with a decrease in CPU utilization.[1]

Data security is an imperative for enterprises and communications service providers (CommSPs), but higher bandwidth networks and the dramatically increasing number of internet-connected devices make it harder for CPUs in edge networking devices to keep up with the need for wire-speed data encryption/decryption. One solution is to add a hardware cryptography accelerator in the edge server to shoulder the increased traffic and free up the CPU for other compute tasks. To determine the impact of adding an accelerator to an edge server, Intel® Network Builders ecosystem partner F5 tested the throughput its own F5® BIG-IP® Virtual Edition (VE) application delivery controller (ADC) on servers with and without Intel® QuickAssist Technology (Intel® QAT).

The Challenge: Boosting Application Performance and Encryption

The availability of 5G networks will enable new high-speed data services and capabilities for handsets and other mobile devices. At the same time, CommSPs anticipate the addition of billions of connected IoT devices to the network from companies taking advantage of LTE Cat-M and Narrowband IoT (NB-IoT) networks. Even as these trends drive up data traffic and network connections, CommSPs are also seeing much more data traffic that needs encryption/decryption.

Network functions virtualization (NFV) and software defined networking (SDN) applications such as virtual customer premises equipment (vCPE), software-defined wide area networking (SD-WAN), virtual application delivery controllers (vADC), vIPsec, and virtual firewalls need to perform compute-intensive security tasks while maintaining high throughput and low latency. Encryption of web traffic is also growing with the adoption of protocols like HTTP/2 and the increased use of secure sockets layer/transport layer security (SSL/TLS) encryption/decryption. Another emerging use case is DNS over HTTPS.

The performance and CPU utilization of these workloads can be significantly improved by using dedicated hardware accelerators, such as Intel QuickAssist Technology (Intel QAT), which can offload cryptographic workloads from the CPU and accelerate processing. This performance increase allows CommSPs to support increased crypto workloads in a way that also improves virtual network function (VNF) performance.

Many edge servers are optimized for cost, including using lower performance CPUs, which can reduce the amount of computing power available for encryption tasks. When CPU cores must be dedicated to crypto workloads, that means fewer compute cycles are available for other functions. F5 has built its reputation on developing web application and network software that helps user traffic to get to its destination quickly and securely. To demonstrate the increased performance

Table of Contents

of encryption acceleration, the company has tested the performance of its BIG-IP Virtual Edition suite of application delivery controller (ADC) virtual network functions (VNFs) on an Intel® architecture-based edge server utilizing Intel QuickAssist Technology (Intel QAT).

F5 BIG-IP Virtual Edition Improves Security, Application Performance

F5 Networks is a leader in multi-cloud application services and network functions for enterprises and CommSPs. F5's BIG-IP VE products are optimized for virtualized environments and run on servers powered by Intel architecture CPUs. F5 solutions address multiple use cases in CommSPs and enterprises:

- Intelligent traffic management, load balancing, and DNS
- Protocol fluency and tunneling capabilities such as TCP, HTTP/2, Diameter, IPsec
- SGi-LAN/N6 consolidation (policy enforcement, firewall, CGNAT, DDoS)
- IoT security
- Web application firewall
- Identity and access management

Here are some specific BIG-IP VE solutions that address the above use cases and require high performance crypto processing and compression:

- **F5 BIG-IP Local Traffic Manager™ (LTM)** provides advanced load balancing that can control and help secure network traffic by selecting the right destination server based on server performance and availability. The result is fast application performance and increased availability and security.
- **F5 BIG-IP DNS** provides a DNS infrastructure that sends user traffic to the closest or best-performing physical,

virtual, or cloud environment. BIG-IP DNS is designed for hyperscale environments and provides a defense against DDoS attacks.

- **F5 BIG-IP Access Policy Manager® (APM)** is a scalable access gateway that provides management of user connectivity to help secure, simplify, and protect user access to applications.
- **F5 BIG-IP Advanced Firewall Manager™ (AFM)** addresses network threats before they disrupt critical data center resources through security services including firewall, DDoS mitigation, DNS security, and intrusion protection system.
- **F5 Advanced Web Application Firewall™** protects web applications using behavioral analytics, proactive bot defense, and application-layer encryption of sensitive data such as credentials.

High encryption performance is critical for the BIG-IP product family because, as a full proxy that resides between the client and backend server, the BIG-IP products must not be a bottleneck while transferring client and server data that needs to be encrypted/decrypted at scale, whether for security inspection purposes or to make a traffic steering decision.

Before the availability of Intel QAT, F5 software would leverage CPU-based solutions for encryption such as Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI). These software-based encryption solutions deliver very high performance when taking advantage of Intel AES-NI but still consume a percentage of CPU capacity depending on the amount of data and how many requests are directed at that particular application or service. Scaling performance of software-based encryption requires distributing the load across many servers or deploying servers with higher performance CPUs or with multiple CPUs. Utilizing encryption hardware, like Intel QAT, provides increased performance and frees up CPU processor cycles for other compute needs.
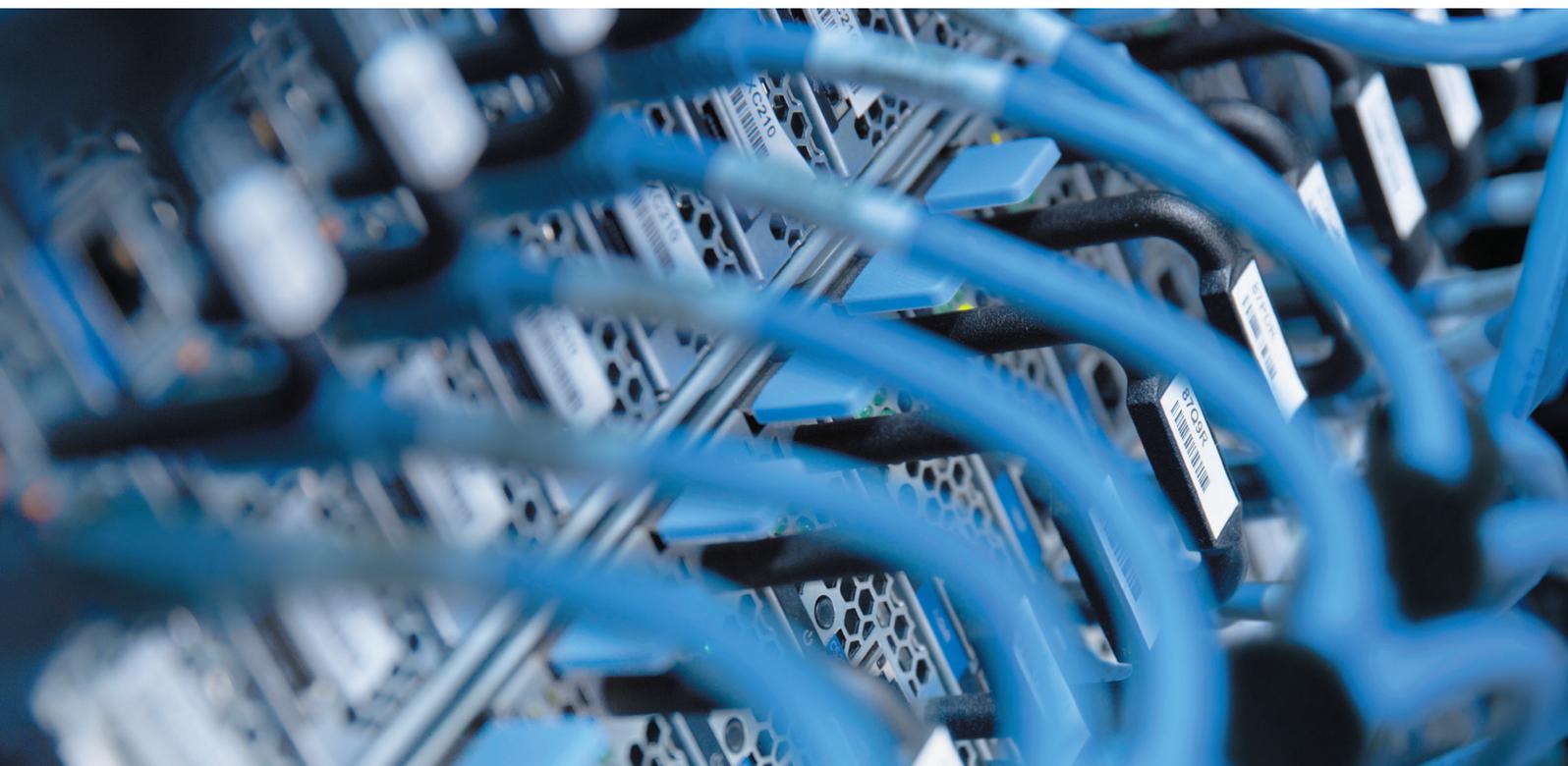
Intel® Xeon® Scalable Processors Support Intel® QAT

F5 solutions deliver optimized throughput when used on servers that feature Intel® Xeon® Scalable processors or 2nd generation Intel Xeon Scalable processors.

Intel Xeon Scalable processors are designed for cloud-optimized, virtualized networks. The platform features an open architecture that scales and adapts with ease to handle the demands of emerging applications. Intel Xeon Scalable CPUs provide a future-ready foundation for agile networks that provides the right cost-performance balance for cloud networks, are highly automated and responsive, and support rapid and more secure delivery of new and enhanced services. These CPUs are designed to enable enterprises and CommSPs to transition to virtualized, software-defined infrastructure to enable cloud capabilities for agile service delivery throughout the network.

The 2nd generation Intel Xeon Scalable processors provide the foundation for a powerful data center server performance and features for expanded agility and scalability. The innovative processor platform provides platform convergence and capabilities across compute, storage, memory, network, and security.

All 2nd generation Intel Xeon Scalable processors support chipsets with integrated Intel QAT, which offers compression functionality acceleration in addition to public key acceleration and symmetric cryptography acceleration. This technology, which is also available in a PCIe card or on selected Intel CPUs and SoCs, processes these workloads separately from the CPU, providing the ability to scale cryptographic performance beyond Intel AES-NI functionality.

Testing BIG-IP with Intel® QAT

In a set of tests run on a server board powered by a 2nd generation Intel Xeon Gold 6230N processor, the use of an Intel QAT adapter resulted in an up to five times[1] better bulk throughput and transactions per second when compared with a system that utilized the CPU only for cryptography.

The tests used eight vCPUs/physical cores from one socket with no hyperthreading cores. Using this hardware, the performance of the BIG-IP Local Traffic Manager solution was tested with and without Intel QAT providing crypto acceleration functionality. The test results, as can be seen in Figures 1 through 3, include better performance and lower CPU utilization.[1] The CPU utilization, shown in Figure 3, is based on aggregated average across all physical cores.

Figure 1 shows an improvement of between two- to five-times the encrypted HTTP throughput when using Intel QAT, depending on packet size; while Figure 2 shows consistently higher transactions per second with Intel QAT engaged, including five times the performance at 128 B packet sizes. CPU utilization across the different tested packet sizes is shown in Figure 3 with consistently lower percentages when Intel QAT is turned on. At 128 B packet sizes, the utilization is almost half the utilization of the solution that didn't use Intel QAT, meaning that the CPU is at 100% capacity operating by itself, compared to 56% utilization when combined with Intel QAT. CPU utilization is typically the heaviest with small packet sizes.[1]
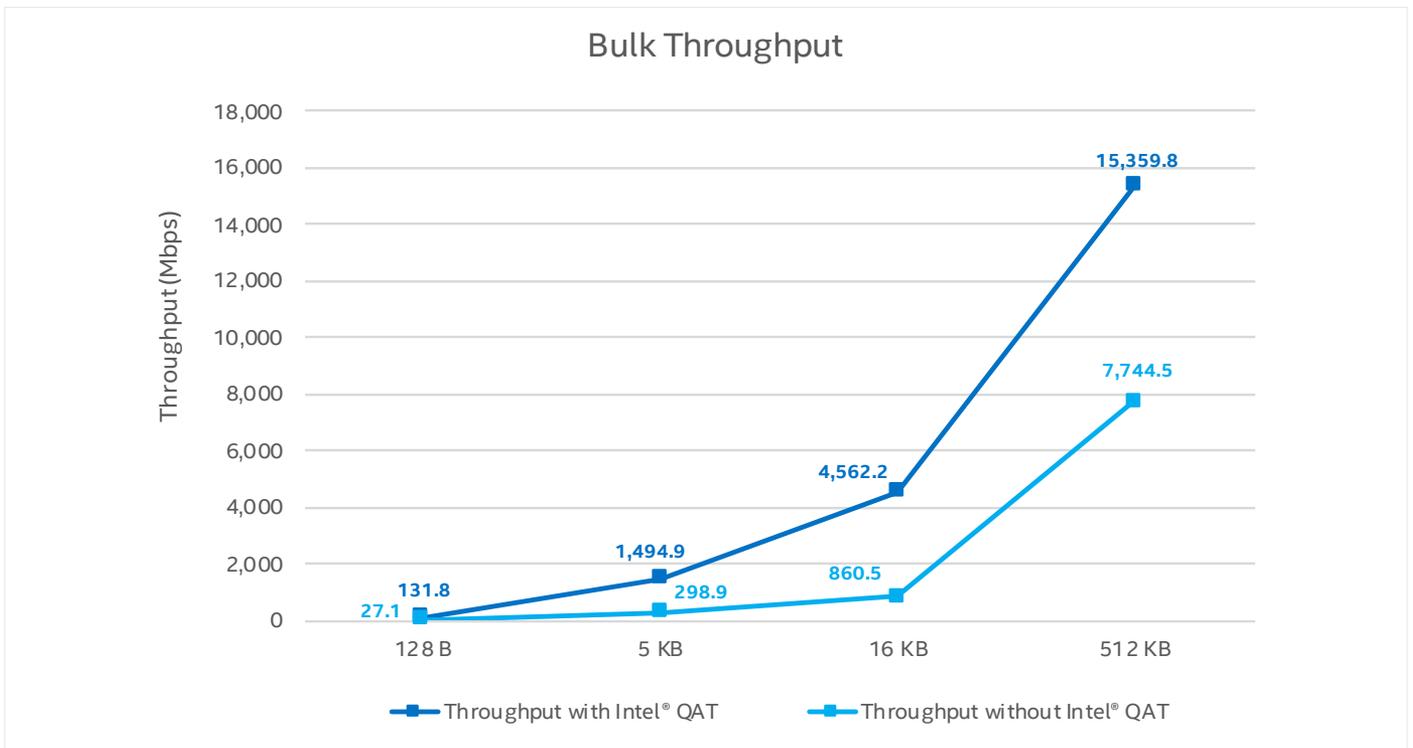

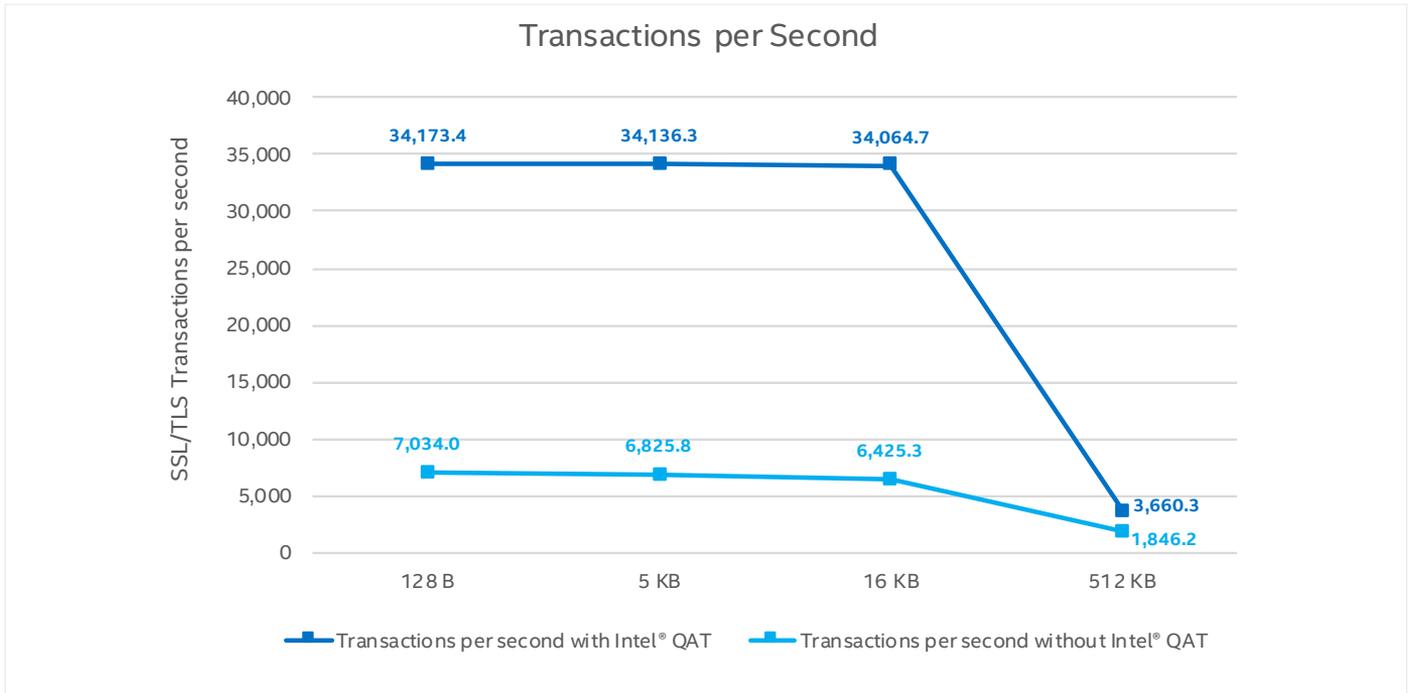**Figure 1.** Bulk throughput with Intel® QAT and without.[1]

Transactions per Second

SSL/TLS Transactions per second

	128 B	5 KB	16 KB	512 KB
With Intel QAT	34,173.4	34,136.3	34,064.7	3,660.3
Without Intel QAT	7,034.0	6,825.8	6,425.3	1,846.2

■— Transactions per second with Intel® QAT   ■— Transactions per second without Intel® QAT

Figure 2. SSL/TLS transactions per second with Intel® QAT and without.[1]

CPU Utilization Percentage

CPU utilization percentage

	128 B	5 KB	16 KB	512 KB
Without Intel QAT	99.9	100.0	99.9	97.0
With Intel QAT	56.1	62.8	74.0	67.4

■—CPU utilization with Intel® QAT   ■—CPU utilization without Intel® QAT
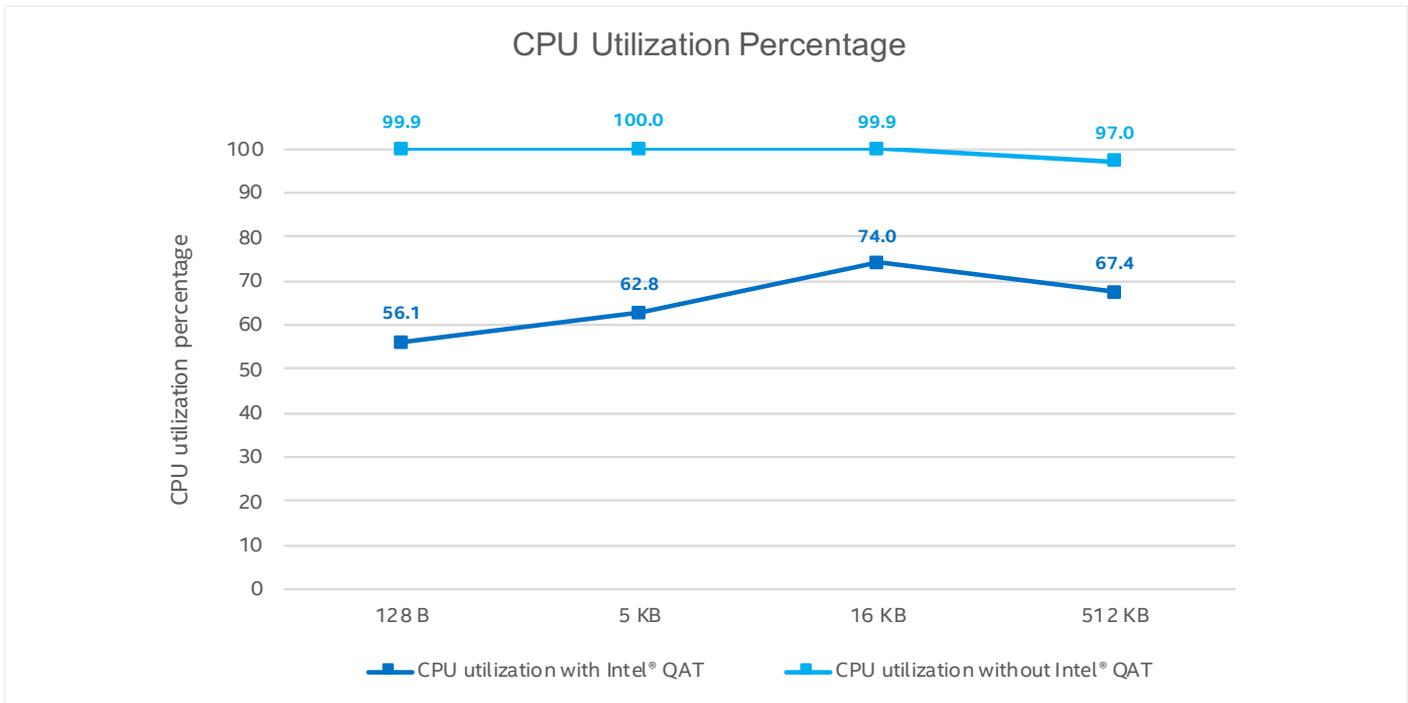
Figure 3. CPU utilization for encryption functionality with Intel® QAT and without.[1]

Conclusion

More encrypted data traffic is a mainstream reality and network core, edge, and data center infrastructure will need to handle this traffic while designing for cost efficiency. The impact will come from an increase in data traffic from smartphones and mobile devices and increased device connectivity from IoT. CommSPs and enterprises are looking for solutions to build a network and data center infrastructure that is responsive to these increases while offering high-performance crypto processing for data security. Intel QAT accelerates crypto performance and according to tests from F5 offers dramatic performance improvements with a decrease in CPU utilization.[1] This combination helps CommSPs and enterprises to maintain VNF and application performance in a 5G world.

About F5

F5 provide application services that give the world's largest businesses, service providers, governments, and consumer brands the freedom to securely deliver every app, anywhere with confidence. F5 delivers cloud and security application services that enable organizations to embrace the infrastructure they choose without sacrificing speed and control. For more information, go to f5.com. You can also follow @f5networks on Twitter or visit us on LinkedIn and Facebook for more information about F5, its partners, and technologies.

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.