Solution Brief

Banking/Financial Services, Government, Networking/Telco
Intel® Xeon® 6 Processors

NEXCOM FTA 5190 Server Lets Organizations Act Now for PQC

Powered by Intel® Xeon® 6 SoCs, the FTA 5190, handles larger key size and complex math needed for post-quantum cryptography (PQC). Tests show server offers high performance for traditional cryptography and PQC.

As organizations plan for the reality of quantum computing, standards bodies, such as the US National Institute of Standards and Technology, are preparing new post-quantum cryptography (PQC) standards. These standards are designed to protect organizations from cyberthreats that take advantage of quantum computing's dramatic increase in compute capability.

These PQC standards count on larger key sizes and more complex mathematical operations. For organizations that are protecting their edge networks, this can place significant strain on edge compute resources.

Enterprises need to prepare for PQC because it initiates a fundamental shift in how data must be protected. This emerging challenge underscores the need for enterprise IT teams to anticipate higher infrastructure requirements, plan for more robust compute and memory capabilities, and ensure that critical systems remain responsive while implementing quantum-resistant security measures.

NEXCOM has a long history of developing edge servers that are optimized for cybersecurity. The company is an Intel® Solution Builders ecosystem member and has worked with Intel on the FTA 5190 edge server that delivers PQC protection. In tests described later in this paper, the FTA 5190 was able to deliver PQC processing with the same performance as today's advanced encryption protocols.

NEXCOM FTA 5190 Uses Intel® Xeon® 6 SoC

NEXCOM's FTA 5190 is engineered for advanced edge cybersecurity performance. In a previous paper[1], Intel and NEXCOM show how the FTA 5190 delivers the fast analytics and big data processing essential to edge cybersecurity. This server also supports PQC-ready security architectures that deliver workloads with high-throughput and AI-assisted inspection at the edge.

The NEXCOM FTA 5190 servers are standardized on Intel Xeon 6 SoC with 36 performance-cores (P-cores). This compact 1U server supports up to 128GB of DDR5 memory and three M.2 slots for storage. The system has eight 25GbE SFP+ ports and eight 1GbE ports and a LAN module slot that supports PCIe 4.0 x 16 interface for higher-speed Ethernet connections.

Intel Xeon 6 SoCs feature up to 12 memory channels and doubles the memory bandwidth of the previous generation Intel® Xeon® D processors. These CPUs excel at a wide range of workloads, with a focus on edge applications, where enterprise business workloads and infrastructure workloads such as network and network security are consolidating to a smaller number of servers.

Other Intel technologies that drive the performance of the FTA 5190 include:

Intel® QuickAssist Technology (Intel® QAT) Gen5:
Another key technology supporting high-performance cryptography in modern infrastructure is Intel QAT Gen 5. This accelerator featured in modern Intel Xeon processors offloads and accelerates compute-intensive cryptographic and data compression operations from the CPU to a dedicated hardware engine. This significantly improves throughput for encryption, decryption, hashing, and compression workloads.

The FTA 5190 makes use of Intel QAT to increase the volume of cryptographic operations in parallel, enabling to maintain strong security controls without introducing latency or consuming valuable CPU cycles increasingly needed for general applications and analytics at the edge.

Intel® Crypto Acceleration (QATSW):
Intel Crypto Acceleration is a software-based acceleration of cryptographic workloads using Intel crypto libraries, namely Intel® Cryptography Primitives Library and Intel® Multi-Buffer Crypto for IPsec (Intel IPsec_mb). It utilizes Intel® Advanced Vector Extensions 512 (Intel® AVX-512) that provide vector processing capabilities to accelerate cryptographic workloads. Intel developed PQC optimizations based on Intel AVX-512. These are available today to accelerate PQC algorithms leveraging existing Intel crypto libraries, and are referred to as Intel PQC Software in this document. Refer to Intel's Post-Quantum Cryptography: Accelerating Open Quantum Safe Library with Intel® AVX-512 Keccak 1600 Implementation technology guide for more details.

Intel® Advanced Matrix Extensions (Intel® AMX):
This built-in accelerator in Intel Xeon 6 SoC uses matrix multiplication that can assist with batching lattice based ML-KEM, ML-DSA operations resulting in improved TLS performance.

PQC Test Bed

To evaluate the performance of the system, NEXCOM and Intel tested an FTA 5190-based solution that is sized for the needs of a large branch office or a colocation point or a small to medium-sized data center[2].

As seen in Figure 1, the FTA 5190 was set up as a NGINX web server and NEXCOM NSA 7160R was set up as a WRK client. The client and server were connected using the NC 120FIS4-OS LAN modules operating at 100Gbps.

The NSA 71690R is a 2U-high rackmount high-performance server that uses dual 5th Gen Intel® Xeon® Scalable processors. The NC 120FIS4-OS is based on the Intel® Ethernet Controller E810-CAM2 and features two 100 GbE ports. PQC encryption was provided by the NetSec v25.12 reference software developed by Intel.

An Ansible host was used for testing management automation. The traffic flow was a simple web request from a WRK client to a NGINX web server over a 100GbE https connection.

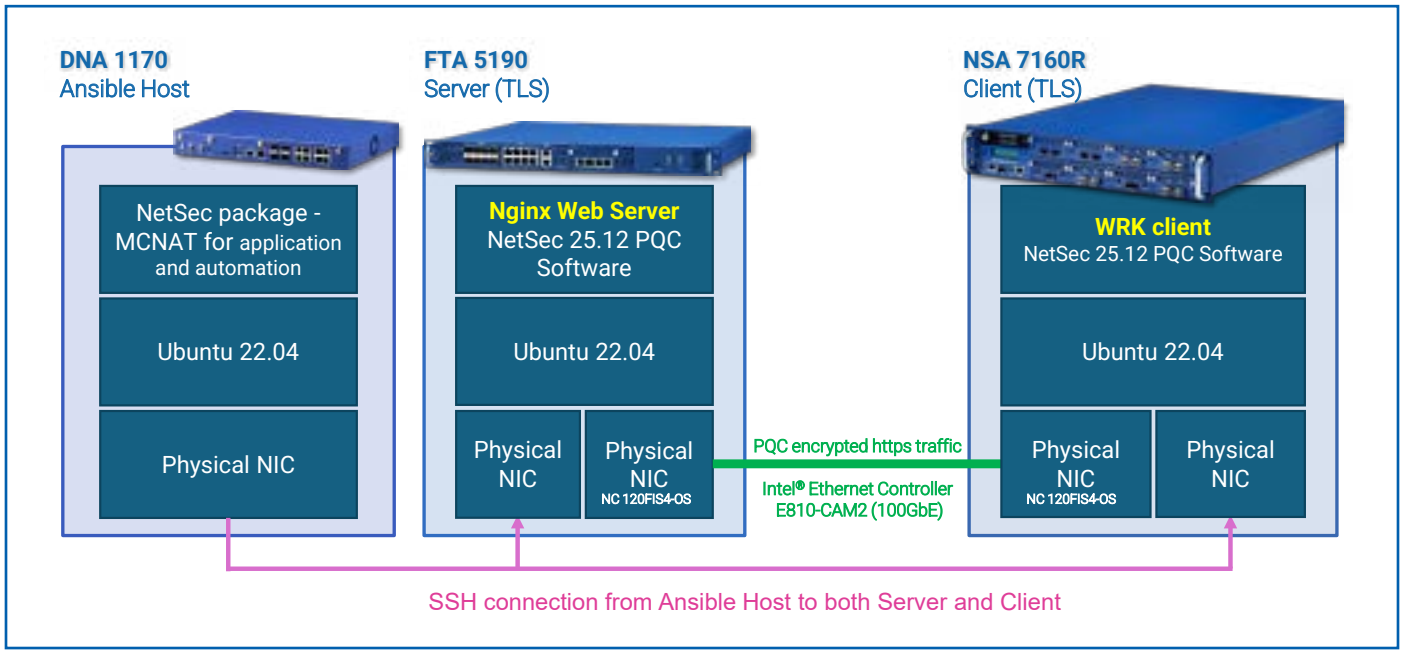

Figure 1. FTA 5190 PQC testbed software configuration using NetSec Reference Software V25.12.

PQC Test Results

Series of NGINX web server TLS handshake tests were run using NetSec reference software from Intel: one with PQC algorithms, another with hybrid combination of PQC and traditional algorithms, and a third test with traditional algorithms. The algorithms used for the performance testing include:

PQC Algorithms	Hybrid Algorithms	Traditional Algorithms
▪ MLDSA87_MLKEM1024	▪ RSA2K_X25519_MLKEM512	▪ RSA2K_X25519
▪ MLDSA65_MLKEM768	▪ RSA2K_ECDHEP256_MLKEM512	▪ RSA2K_ECDHEP256
▪ MLDSA44_MLKEM512	▪ P256_ECDHEP256_MLKEM512	
	▪ P256_X25519_MLKEM512	

Table 1. Algorithms used for performance testing.

The following three figures show encryption performance of the FTA 5190 server tested with PQC hybrid and traditional algorithms. Each cluster represents a different combination of encryption/key generation technologies. Each bar within a cluster shows the connections per second performance (CPS) with one, two, four or eight CPU cores dedicated to the processing task.

Figure 2 shows test results using PQC algorithms. The FTA 5190 delivers up to 3.5K CPS per one CPU core or two CPU threads (1C2T) with MLDSA65_MLKEM768 using Intel PQC software, NetSec v25.12. Crypto performance scales linearly with more cores with post quantum ciphers.

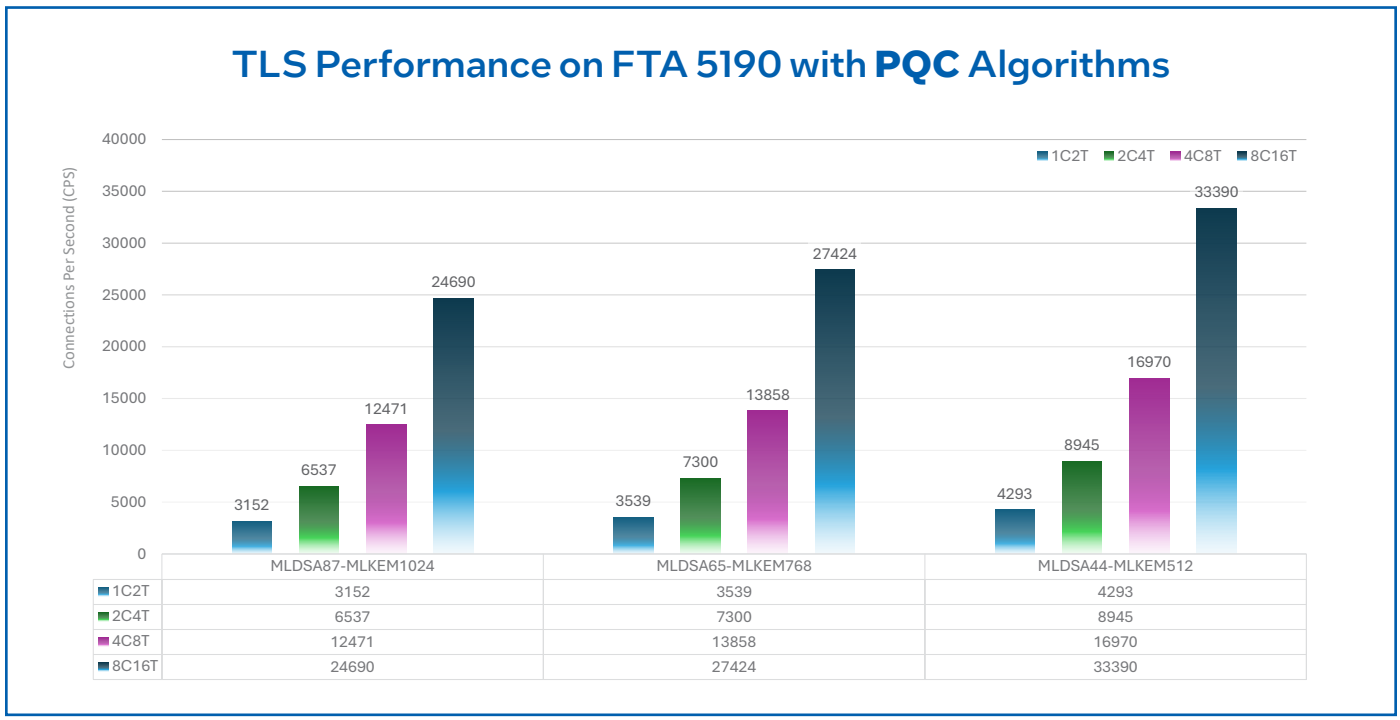

Figure 2. FTA 5190 TLS performance with PQC ciphers.

Figure 3 shows Nginx web server TLS handshake performance using hybrid PQC - X25519 and ML-KEM for key encapsulation. FTA 5190 delivers up to 2.1x TLS connections per second at 1C2T with X25519_MLKEM512, using Intel optimized PQC software.

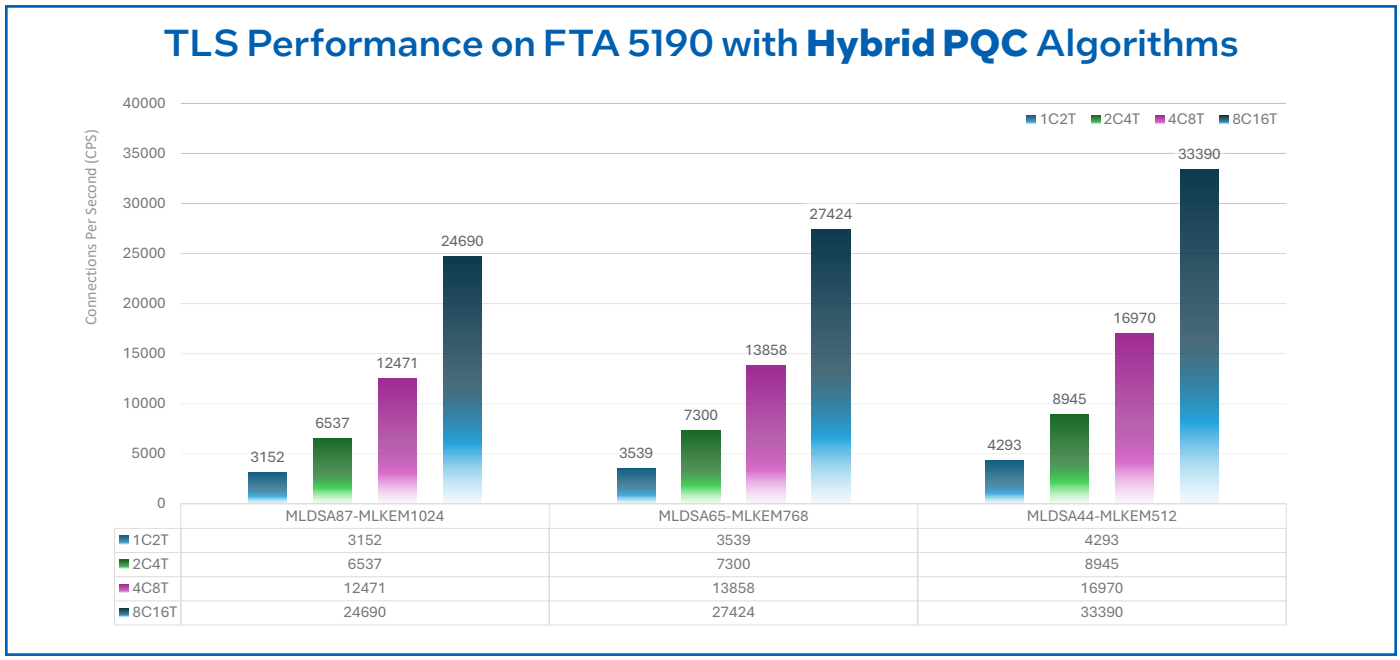

Figure 3. FTA 5190 TLS performance with hybrid PQC ciphers.

Figure 4 shows the performance of the solution that uses traditional cryptographic algorithms. FTA 5190 delivers 2x TLS connections per second at 1C2T with traditional cryptography using Intel crypto software.

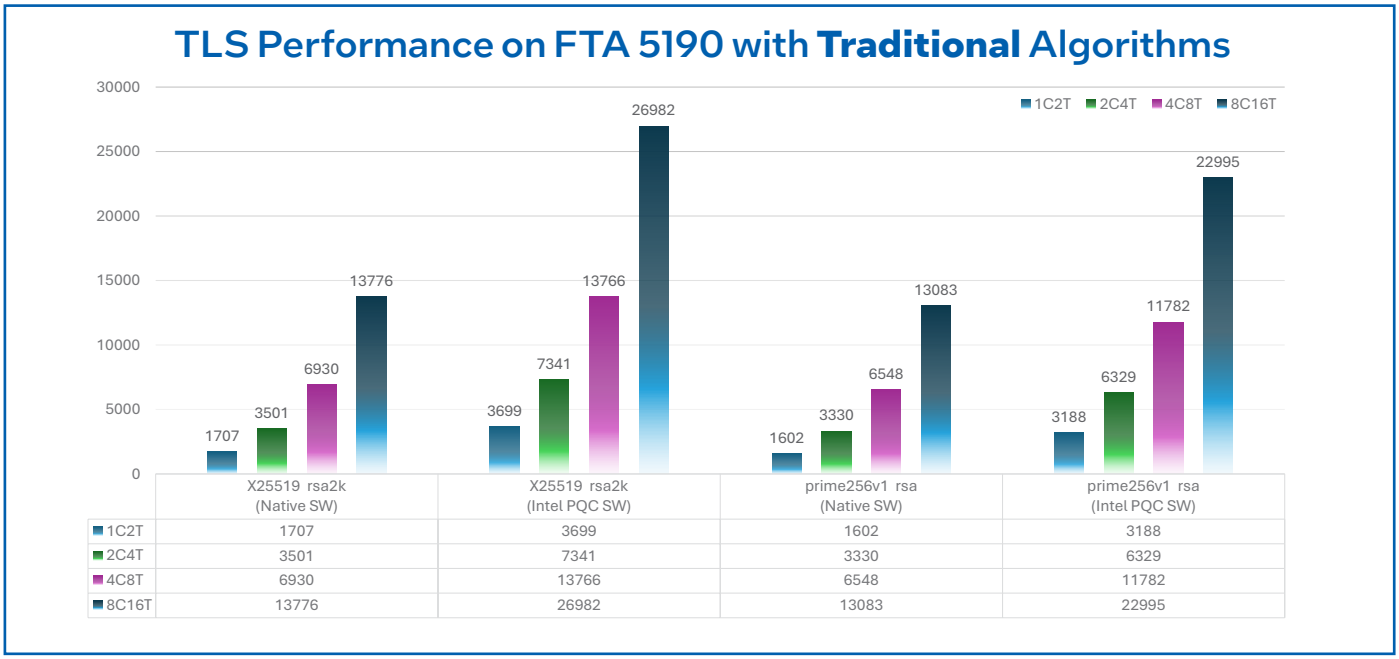

Figure 4. FTA 5190 TLS performance with traditional ciphers.

As seen in all the test results, performance of the FTA 5190 scaled linearly as the core/thread count increased, allowing solutions that are scalable depending on the use case. In addition, the platform delivers the same level of performance across all of the cryptographic combinations. This ensures that the FTA 5190 has the performance to meet today's cryptographic needs, which can quickly evolve to support PQC transitions.

Conclusion

Quantum computing is becoming a reality and that will unleash a new wave of cybercrime that takes advantage of quantum performance to break today's most secure encryption protocols. But new PQC algorithms are being standardized that will protect an enterprise's core and edge computing. NEXCOM provides the hardware platform to enable PQC at the edge with FTA 5190. Using the Intel Xeon 6 SoC, the server delivered high performance for both traditional and advanced PQC algorithms. The results show that the server can be deployed to serve today's network security applications and be upgraded to full PQC with no loss of performance.

Learn More

NEXCOM FTA 5190

NEXCOM NSA 7160R

NEXCOM NC 120FIS4-OS

Intel® Xeon® 6556P-B processor

Intel® Ethernet

Solution Brief: NEXCOM FTA 5190 Offers Advanced Edge Cybersecurity Performance

Solution Brief: Accelerate Artificial Intelligence (AI) Workloads with Intel Advanced Matrix Extensions (Intel AMX)

Intel® Industry Solution Builders

[1] https://builders.intel.com/solutionslibrary/nexcom-fta-5190-offers-advanced-edge-cybersecurity-performance.

[2] FTA 5190 SUT: Single node, single socket server powered by 36-core Intel® Xeon® 6556P-B processors. Total DDR5 memory was 128 GB (4 slots/ 32GB/ 6400 MHz); microcode 0x1000214;Intel® Hyper-Threading Technology enabled; Intel® Turbo Boost Technology 2.0 enabled. BIOS version: American Megatrends 5.35 ; network interface is Intel® Ethernet Controller E810-CAM2 for QSFP 100Gbit/s, 1TB of application storage.

Software: OS was Ubuntu 24.04.5 LTS; kernel was 5.15.0-164-generic.

Workload software: NetSec v25.12; Compiler was 11.04.0; Libraries were OQS provider/Liboqs, QAT engine/QATlib/QAT driver. Other software: python3 python3-venv python3-pip; ansible paramiko pyyaml jinja2 xmltodict. Test conducted by NEXCOM in January 2026.

NSA 7160R SUT: Single node, dual socket server powered by 32-core Intel® Xeon® Gold 6530 processors. Total DDR5 memory was 32 GB (16 / DDR5 32G / 4800); microcode 0x1000214. Intel® Hyper-Threading Technology enabled; Intel® Turbo Boost Technology 2.0 enabled. BIOS version: American Megatrends 5.35. 64GB of application storage; Intel® Ethernet Controller E810-CAM2 for QSFP 100Gbit/s.

Software: OS was Ubuntu 24.04.5 LTS; kernel was 5.15.0-164-generic. Workload software: NetSec v25.12; Compiler was 11.04.0; Libraries were OQS provider/Liboqs, QAT engine/QATlib/QAT driver. Other software: python3 python3-venv python3-pip; ansible paramiko pyyaml jinja2 xmltodict.

Test conducted by NEXCOM in January 2026.

Notices & Disclaimers

Performance varies by use, configuration and other factors.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See configuration disclosure for details. No product or component can be absolutely secure.

Intel optimizations, for Intel compilers or other products, may not optimize to the same degree for non-Intel products.

Your costs and results may vary.

Intel technologies may require enabled hardware, software or service activation.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

See our complete legal Notices and Disclaimers.

Intel is committed to respecting human rights and avoiding causing or contributing to adverse impacts on human rights. See Intel's Global Human Rights Principles. Intel's products and software are intended only to be used in applications that do not cause or contribute to adverse impacts on human rights.

0426/KF/DJA/PDF ♻Please Recycle 368830-001US