

Securing the Digital Campus: Asian Education Ministry Deploys High-Performance Edge Firewalls

NEXCOM edge firewalls, powered by Intel® Xeon® processors, deliver 320 Gbps throughput, 2x VPN performance, and 100,000 VPN tunnels for high-performance academic network security.



Can cybersecurity keep pace with 100 Gbps and above? Discover how NEXCOM and Intel overcame the performance barrier, sustaining deep packet inspection while doubling VPN throughput and dramatically expanding secure connectivity.

The Challenge: Securing 100 Gbps Academic Backbones Without Latency

The rapid expansion of digital classrooms, generative AI tools, and collaborative cloud platforms has reshaped modern education. While these tools create interactive learning environments, they expand the attack surface of academic networks. Universities and schools face frequent distributed denial-of-service (DDoS) events, ransomware attempts, and credential theft targeting intellectual property and personal student data.

To keep pace with rising traffic volumes, educational authorities in Asia executed a nationwide network transformation. Engineers upgraded local access networks to 10 Gbps and deployed 100 Gbps core switching lines between primary regional nodes to guarantee line redundancy.

However, high network bandwidth introduced a compute bottleneck at the security layer:

- **Inspection Overhead:** Legacy security appliances could not execute deep packet inspection (DPI) at 100 Gbps line rates, forcing network administrators to sacrifice inspection depth to maintain traffic flow.
- **Cryptographic Bottlenecks:** Heavy off-campus student traffic (HTTPS and IPsec VPNs) flooded standard CPU cores with compute-intensive encryption and decryption routines.
- **Latency Degradation:** Time-sensitive academic services, such as real-time video lectures and proctored exam portals, suffered unacceptable latency when firewalls performed complex signature matching.

The ministry required an edge security architecture capable of processing massive data pipelines in real time, executing AI-driven threat classification, and preserving line-rate throughput.

"By utilizing platforms with 5th Gen Intel® Xeon® Scalable processors, we ensure peak performance for the school equipment refresh, eliminating product lifecycle issues. This project marks a significant milestone in safeguarding campus networks against emerging threats."

– Allan Chiu
VP of Networking and
Communication Solutions,
NEXCOM

The Solution: High-Throughput Edge Defense Powered by Intel® Xeon® Processors

NEXCOM collaborated with Intel to design and deploy Next-Generation Firewall (NGFW) appliances tailored for high-density academic environments. Built with Intel’s NetSec Software package, Fast Data Project (FD.io) Vector Packet Processing (VPP), and Snort inspection engines, the deployment utilizes two complementary platforms:

- **NEXCOM NSA 7160R (Core Campus Security):** A 2U rackmount platform deployed at central academic nodes for heavy traffic inspection. Powered by 5th Gen Intel® Xeon®

Scalable processors, the platform provides high memory bandwidth and extensive cache capacity for continuous packet evaluation.

- **NEXCOM FTA 5190 (Distributed Edge Security):** A compact 1U server deployed across regional and local school networks where space and power are constrained. Powered by the Intel® Xeon® 6 SoC with 36 Performance-cores and up to 128 GB of DDR5 6400 MHz memory, this appliance enforces local micro-segmentation and security policies.

The Results: Measurable Gains in Throughput and Concurrency

Upgrading the security infrastructure based on 2nd Gen Intel Xeon Scalable processor to 5th Gen Intel Xeon Scalable processor configured in NSA 7160R delivered immediate, quantifiable capacity and performance improvements across the academic network.

Metric	Legacy Appliance based on 2nd Gen Intel® Xeon® Scalable Processor	NEXCOM Appliance based on 5th Gen Intel® Xeon® Scalable Processor	Impact
Firewall Throughput (UDP)	240 Gbps	320 Gbps	+33% throughput, preventing bottlenecks on 100 Gbps lines
VPN Cryptographic Throughput	19 Gbps	38 Gbps	+100% cryptographic speed for off-campus connections
Active VPN Tunnels	60,000	100,000	+67% connection capacity for remote students and faculty
Concurrent Sessions	60,000,000	60,000,000	Maintained session scale under full inspection

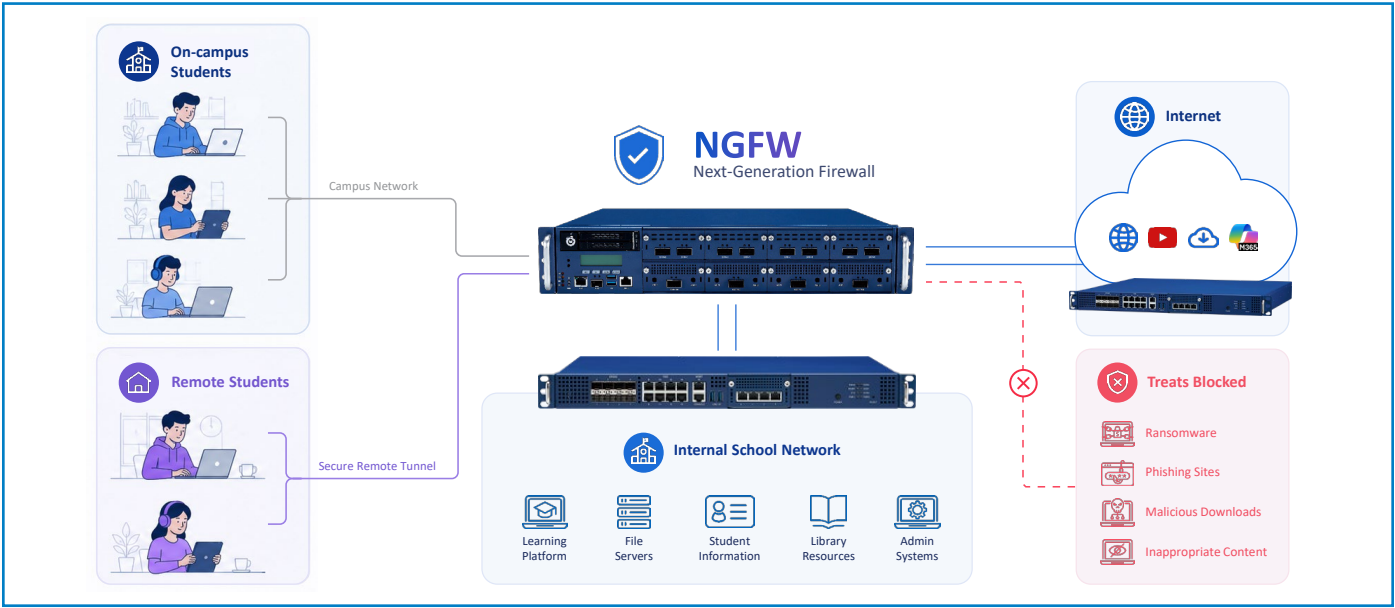


Figure 1. NGFW Deployment Architecture for Secure Campus and Remote Access

Delivering Operational Impact

- **Sustained 100 Gbps Deep Packet Inspection:** The NSA 7160R processes full packet payloads at 100 Gbps line speed, allowing the ministry to utilize the full bandwidth of its redundant network without turning off security features.
- **Doubled Remote Access Capacity:** The system handles peak-hour authentication and encryption loads without connection drops, supporting 100,000 concurrent encrypted tunnels.
- **Consolidated Footprint:** Built-in workload offloading reduces the total number of physical appliances required in regional server rooms, curbing both space and operational energy costs.

Why Intel Xeon Processors Made the Difference

- **Intel® QuickAssist Technology (Intel® QAT):** Offloads symmetric and asymmetric cryptography and data compression from CPU cores. Freeing host cores from encryption cycles directly doubled VPN throughput and improved overall power efficiency.
- **Intel® Advanced Matrix Extensions (Intel® AMX):** Executes built-in matrix math operations to accelerate on-box AI inference. This enables real-time threat telemetry analysis, URL categorization, and anomaly detection in line with data traffic, without requiring discrete PCIe accelerator cards.
- **Intel® Advanced Vector Extensions 512 (Intel® AVX-512):** Accelerates vector-heavy pattern matching, Snort rule evaluation, and payload signature scanning across raw data streams.

Conclusion

By deploying NEXCOM security appliances powered by 5th Gen Intel Xeon Scalable processors and Intel Xeon 6 SoCs, the Asian education ministry solved its core throughput limitation. The deployment proves that high-throughput packet inspection and low latency can coexist on standard x86 architecture when accelerated by integrated silicon engines, ensuring resilient protection for educational data pipelines. Together, NEXCOM and Intel provide a scalable blueprint for modern academic networks, ensuring institutions can proactively mitigate sophisticated cyber threats while delivering a seamless, uninterrupted digital experience for students and educators.

Learn More

- [NEXCOM FTA 5190 Edge Server](#)
- [NEXCOM NSA 7160R Appliance](#)
- [NEXCOM NC 120FIS4-OS LAN Module](#)
- [Intel® Xeon® Processors](#)
- [Intel® QuickAssist Technology](#)

Appendix

Systems Configuration for Performance Evaluation

CPU Generation	2nd Gen Intel® Xeon® Scalable Processor	5th Gen Intel® Xeon® Scalable Processor
CPU Model	Intel® Xeon® Gold 6248R Processor	Intel® Xeon® Gold 6548N Processor
Cores/Threads	24/48	32/64
Memory	8 x DDR4 3200 R-DIMM 32GB	8 x DDR5 5600 R-DIMM 32GB
HDD	2TB	2TB
M.2	N/A	512GB
Interface	8 x LAN Slots	8 x LAN Slots
Power	800~900W	1300W
Firewall Throughput (UDP)	240G	320G
VPN Throughput	19G	38G
VPN Tunnels Capacity	60,000	100,000
Concurrent Sessions	60,000,000	60,000,000



Notices & Disclaimers

Performance varies by use, configuration and other factors. Learn more on the [Performance Index site](#). Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure.

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.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

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.

© Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others. Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.