Solution Brief

Retail, Banking/Financial Services, Manufacturing, Networking/Telco

Lanner Delivers Mid-Range Network Appliance for Branch Cybersecurity

Lanner NCA-2530 with Intel Atom® P6900 SoC delivers advanced AI/ML and network security performance for next-generation firewalls (NGFW)

IT teams work in an environment where branch office network applications are evolving rapidly as technology is in a state of consistent ongoing change. The impact on edge compute of new AI models, new cybersecurity technology, virtualization, data encryption, WAN optimization, edge servers and appliances demand an edge server with performance and flexibility.

Keeping up with advanced cybersecurity threats to ensure data is safe and private is a foundational challenge for branch office computing. One important tool in this battle is the next-generation firewall (NGFW). The NGFW is the front line of defense against ransomware, zero-day attacks, phishing attacks and other threats such as distributed denial of service (DDoS) attacks.

But NGFWs require significant processing power in order to perform deep packet inspection, application control, and to maintain intrusion prevention defenses on every packet. The NGFW also decrypts and encrypts traffic (SSL/TLS), and runs AI/ML threat detection, all while handling high traffic volumes.

Many network appliances can't keep up with the processing demands of NGFW, leaving branch offices and small businesses exposed. Recognizing this market need, Lanner Electronics, an Intel® Industry Solutions Builders Partner, has developed the NCA-2530 high-performance network appliance based on Intel Atom® P6900 SoC.

Optimized for Small Businesses and Branch Networks

The NCA-2530 is a rack mount, 1U-high network appliance / universal customer premises equipment (uCPE). The system is optimized for medium-sized branch offices or small businesses. The NCA-2530 delivers optimized thermal design, ample I/O options, and long-life industrial support.

Powered by an Intel Atom P6900 SoC with either 16 or 24 cores, the appliance has capacity for up to 64 GB of DDR5 5600 MHz RAM. The appliance has flexible networking options. The front panel has four 10GbE RJ45 ports and eight SFP28 ports for 10GbE / 25GbE connectivity.

The appliance can accept expansion boards, including Lanner F.A.S.T solutions that make the NCA-2530 flexible, adaptable and scalable. The available F.A.S.T modules include a 100 GbE module, a PoE+ module and a video module.

Intel SoC and Cyber Security Protection Software from Intel

The NCA-2530 gets its processing power from the Intel Atom P6900 SoC, which is designed to deliver mid-range performance and capabilities within Intel processor portfolio for network security solutions. With 16 to 24 Efficient-cores (E-cores), the low-power server processor can be designed into network appliances and micro

servers. The SoC features up to 2.6 GHz of single-thread performance and are designed for high throughput, low latency processing. The processor offers up to 20 ports of up to 50 GbE networking with the ability to create five port groups to maximize the throughput of a QSFP28 fiber port.

To aid development of network security solutions for the SoC, Intel offers cybersecurity protection software tailored to develop secure networking applications, including NGFW, SD-WAN appliances, secure routers, and edge security gateways. The system makes use of the NGFW reference solutions that are available in NetSec software release (v25.12) from Intel.

Intel® Secure Boot, a security feature incorporated in Intel Atom P6900 SoC, provides a hardware-based root of trust that verifies the integrity of firmware and operating system images before execution. In secure networking appliances, this prevents unauthorized or malicious software from being introduced at boot time, protecting critical network infrastructure from persistent threats.

Intel® Virtualization Technology (Intel® VT), another feature of the Intel Atom P6900 SoC, enables strong hardware-enforced isolation between virtualized networking and security functions running on the same platform. This isolation supports secure multi-function appliances—such as combining firewall, IDS/IPS, and routing services—while reducing the risk of lateral movement between workloads within one server system.

Intel® QuickAssist Technology (Intel® QAT) is an accelerator integrated in the Intel Atom P6900 SoC that accelerates cryptographic operations commonly used in secure networking, including IPsec, SSL/TLS, and other cryptography processing. By offloading encryption and decryption to dedicated Intel QAT hardware, the NCA-2530 maintains its high throughput and low latency and delivers more predictable performance for security-intensive network traffic.

Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) provides hardware-accelerated AES encryption for protecting data in motion across secure network connections. This acceleration allows networking devices to maintain strong encryption for VPNs and encrypted tunnels without sacrificing packet processing performance or increasing CPU utilization.

NGFW Security Use Cases

The NGFW serves as a primary security control in branch and small office environments, providing deep packet inspection, application awareness, and integrated threat prevention to protect users, devices, and data at the network edge.

For distributed locations, the NGFW must deliver consistent security policy enforcement while maintaining predictable performance for business-critical applications.

Beyond core firewall functionality, small businesses and branch offices often need the flexibility to enable additional security capabilities as threats evolve or network architectures change.

Unified threat management (UTM) features can be activated to consolidate functions such as web filtering, anti-malware, and application control into a single platform, simplifying deployment and management. Similarly, integrated intrusion detection and prevention capabilities allow organizations to identify and block known exploits and anomalous traffic patterns in real time, reducing the risk of breaches without requiring separate, single function security appliances.

As connectivity becomes more distributed and cloud-centric, secure SD-WAN is an important network capability in branch environments. When integrated with an NGFW, secure SD-WAN enables encrypted connectivity, intelligent traffic steering, and centralized policy control across multiple sites and transport links.

This approach allows small businesses to improve application performance and resilience while extending consistent security controls from headquarters to every branch location, all without significantly increasing operational complexity.

Testing NGFW Performance

To test the NGFW performance on the system, Lanner set up the following test environment. The DUT system running Snort IPS was provisioned using a Lanner NCA 2530 with 24-core Intel Atom® P6962 processor with a pair of 25GbE ports and a pair of 10GbE LAN connections.

The testing systems were deployed on a Lanner NCA-6530A server running both wrk HTTP benchmarking software and NGINX web server software. Vector packet processing (VPP) software was also run on these test systems to provide packet routing.

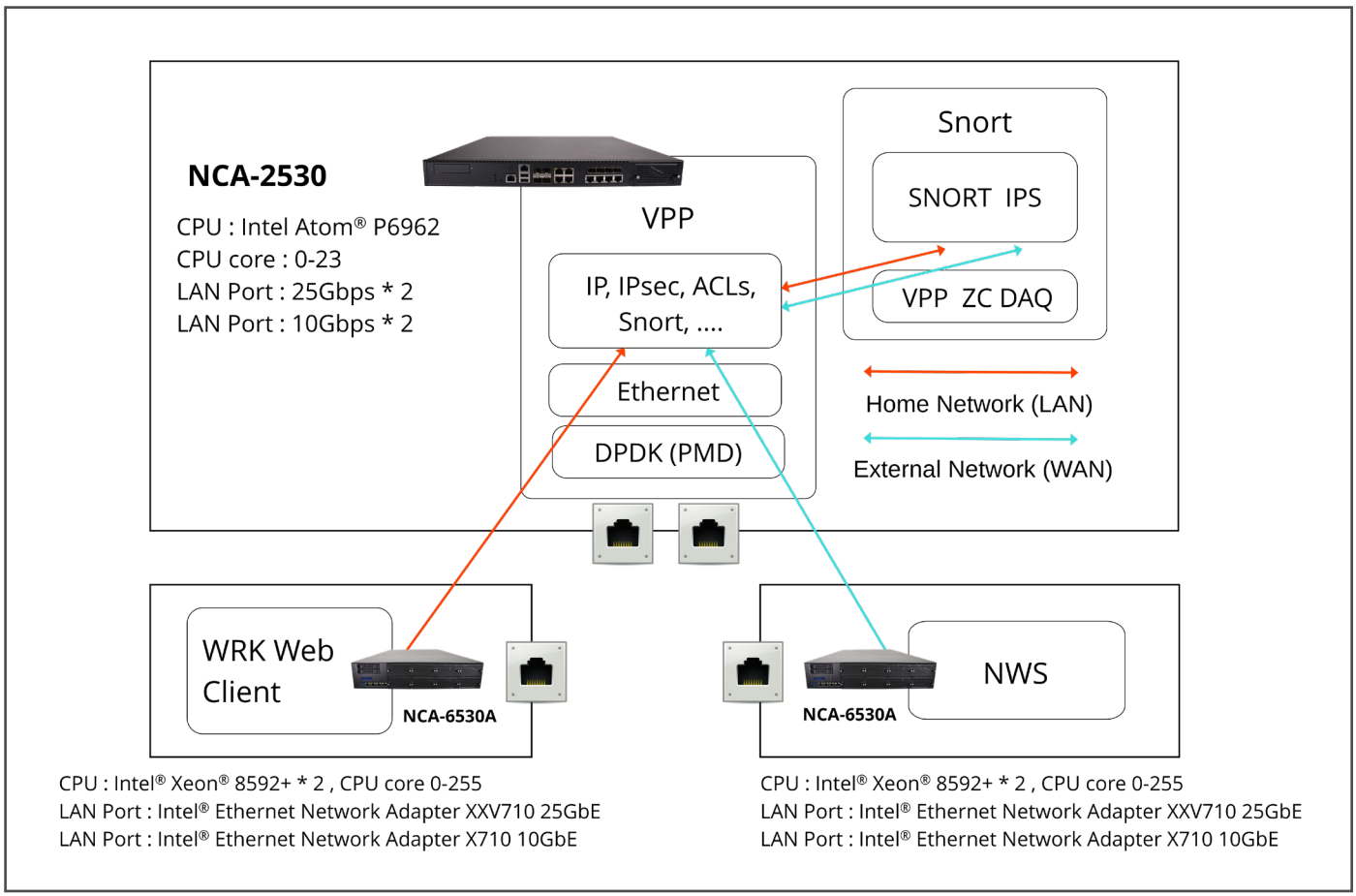

Figure 1. Test system logical view.

The Lanner NCA-6530A is powered by dual 64-core Intel® Xeon® 8592+ processors. The Lanner 6530A also was equipped with a pair of 25GbE ports and a pair of 10GbE LAN connections.

The logical view of the test system is seen in Figure 1.

To achieve the maximum throughput performance of the platform, dedicated VPP cores were allocated for data plane processing and Snort was installed for security inspection. Since the major performance bottleneck is the Snort processing, most of the CPU cores were dedicated to Snort. Table 1 shows the core allocation configurations that achieve best performance. This configuration yielded 30Gbps of total throughput and 1.5Gbps of Snort performance per core. This will meet the requirements of most mid-range NGFW appliance designs.

Core Configurations	
No. of VPP Cores	2C2T
No. of Snort Cores	20C20T
Performance	
Total Throughput (Gbps)	30
Throughput per Snort Core (Gbps)	1.5
Throughput per Core (Gbps)	1.4

Table 1. This table shows how the DUT cores were divided for the tests and the resulting performance.

Conclusion

Small branch offices and businesses face sophisticated cybersecurity attacks just like larger businesses and need cost-effective and powerful appliances to ensure their defenses are effective. The Lanner NCA-2530 is designed for these applications getting processing power from the Intel Atom P6900 SoC. The solution is a scalable, flexible and high-performance system that help IT departments with the rapid evolution of branch office networks.

Learn More

Lanner NCA 2530

F.A.S.T. Modules

Lanner N2S-IPU01

Intel® Industry Solutions Builders

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.

0226/KF/DJA/PDF Please Recycle 367891-001US