White Paper

Telecommunications, Security Professionals

Clavister NetShield Delivers Scalable Performance up to 95 Mpps[1]

Tests of Clavister NetShield*, virtual NGFW running on 3rd Generation Intel® Xeon® Scalable processor-based server and Intel® Ethernet 800 Series Network Adapters shows performance that scales with increased vCPU resources

Network functions virtualization (NFV) turned 10 years old in 2022 with the anniversary of the presentation of the first NFV white paper[2]. Since that paper was published, NFV has had a major impact on telecom networks and systems. The technology enabled network functions, which had been tightly coupled with specialized hardware, to instead be software running on Intel architecture-based CPUs. This has evolved to containerization and the two virtualization technologies have enabled networks to be more agile and flexible at a lower capital and operational expense.

Before NFV, firewall and other data security appliances had to be placed in the data path to filter packets and detect malware or other security issues. But that approach doesn't work in a virtualized infrastructure because network functions are deployed in containers or virtual machines all over the network and are exposed to customers as service.

The software delivering these services can move to different servers within the data center as they need new compute, memory, or storage resources. Providing firewalling for these services requires the same flexibility, and traditional firewalls needed to evolve to support software-based and virtualized infrastructure.

Firewalls are an important aspect of network security as they are deployed at network data ingress and egress points forming a barrier that protects the internal network from outside forces. To enable telecom core (3G/4G/5G) service availability, it is vital to protect all the interfaces, including (see also Figure 1):

- Internet (core to internet)
- Backhaul (core to RAN)
- Roaming (core to another operator)
- Management (core to O&M)

Each of these use cases benefit from firewall protection even though some are connections between virtual network functions where a hardware firewall cannot be used to intercept traffic.

Clavister is a specialist network security provider, headquartered in Sweden providing cyber security solutions for over 25 years. Clavister NetShield is a series of carrier-grade, high performance network firewall and 5G security solution. NetShield is specifically designed for virtual environments with linear scaling and supports hybrid network models and helps MNOs to transition from 3G and 4G to 5G in a secure way.

Table of Contents

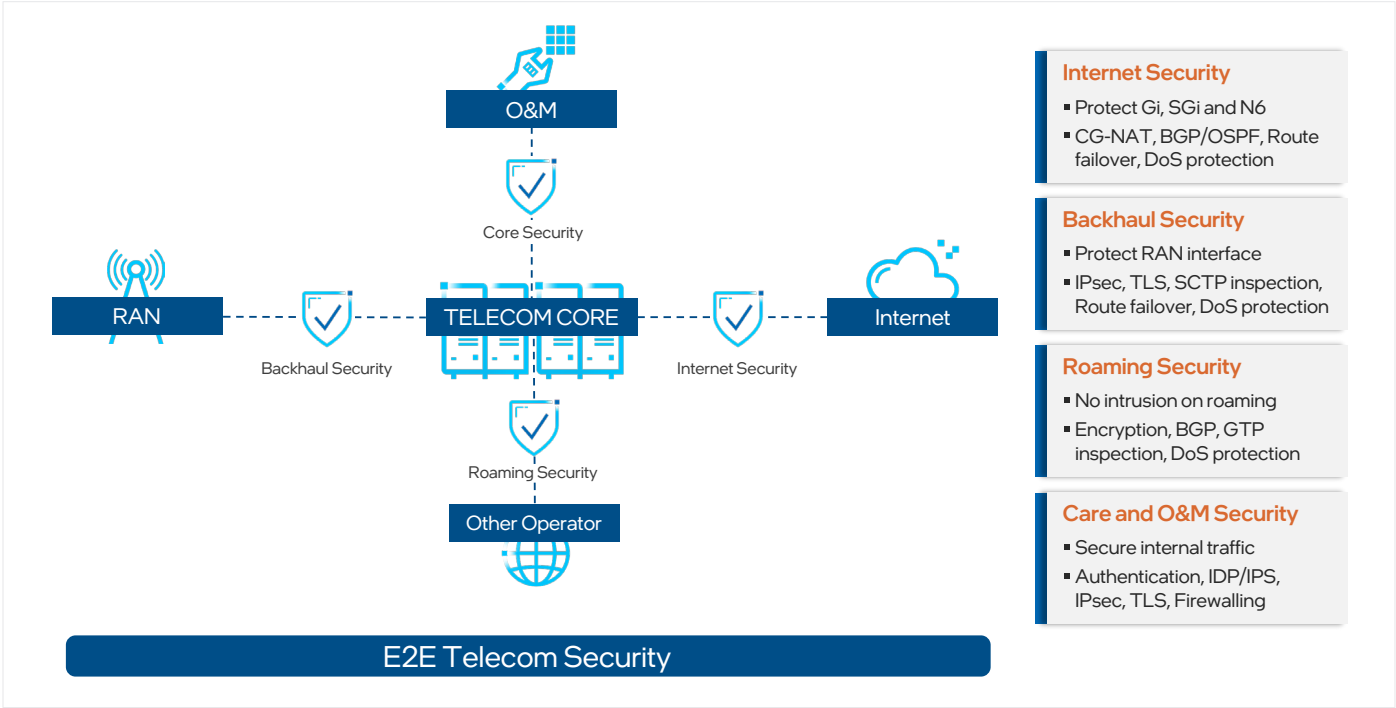

Figure 1. Firewalls provide a barrier against outside cyber security activity by protecting these four data ingress areas.

To demonstrate the performance of NetShield, Clavister, an Intel® Network Builders ecosystem member, tested its virtual edition of NetShield using 3rd Generation Intel® Xeon® Scalable processors and Intel® Ethernet 800 Series Network Adapters to measure the performance of the virtualized system.

Clavister partners with Managed Security Service (MSS) and Network Equipment Vendors (NEPs) like Nokia* to offer NetShield as a managed firewall service.

Clavister NetShield Virtual Firewall

Clavister NetShield enables a high rate of packet forwarding while keeping data more secure. It runs on Intel Xeon Scalable processor- and Intel Atom® processor-based servers. For performance, Clavister NetShield uses open source Data Plane Development Kit (DPDK), a set of software libraries and drivers in to implement its data plane. DPDK facilitates high-performance data throughput in an Intel® architecture-based server, processing the packets in user space and avoiding the operating system kernel to reduce latency. Using DPDK provides virtual network functions (VNFs) with transparent support for Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) and Intel® QuickAssist Technology (Intel® QAT) without significant investment in development and support.

Clavister's tests reveal that adding processing power dramatically increases data throughput, enabling nimble scalability and efficient packet forwarding in a virtualized environment. In passing data from the network behind the firewall on to the Internet or data network, Clavister NetShield fully supports the N6 interface in 5G architectures, and efficiently protects the SGi interface in 4G.

2021 Test Serves as Blueprint for These Results

In March 2021, Intel and Clavister published[3] the results of a performance test of NetShield Virtual on a simulated 5G network using 2nd Generation Intel® Xeon® Scalable processors and Intel® Ethernet Network Adapters XXV710. These two, dual-port adapters supported 25 GbE throughput per port, for a total of 50Gbps capacity per network adapter. The system under test had two XX710-DA2 and which provided for of 100Gbps total capacity.

In those tests, which used 64-byte packets, NetShield demonstrated linear performance increases as more virtual cores were added and reached full line rate throughput at 40 virtual CPUs (see Fig. 2).

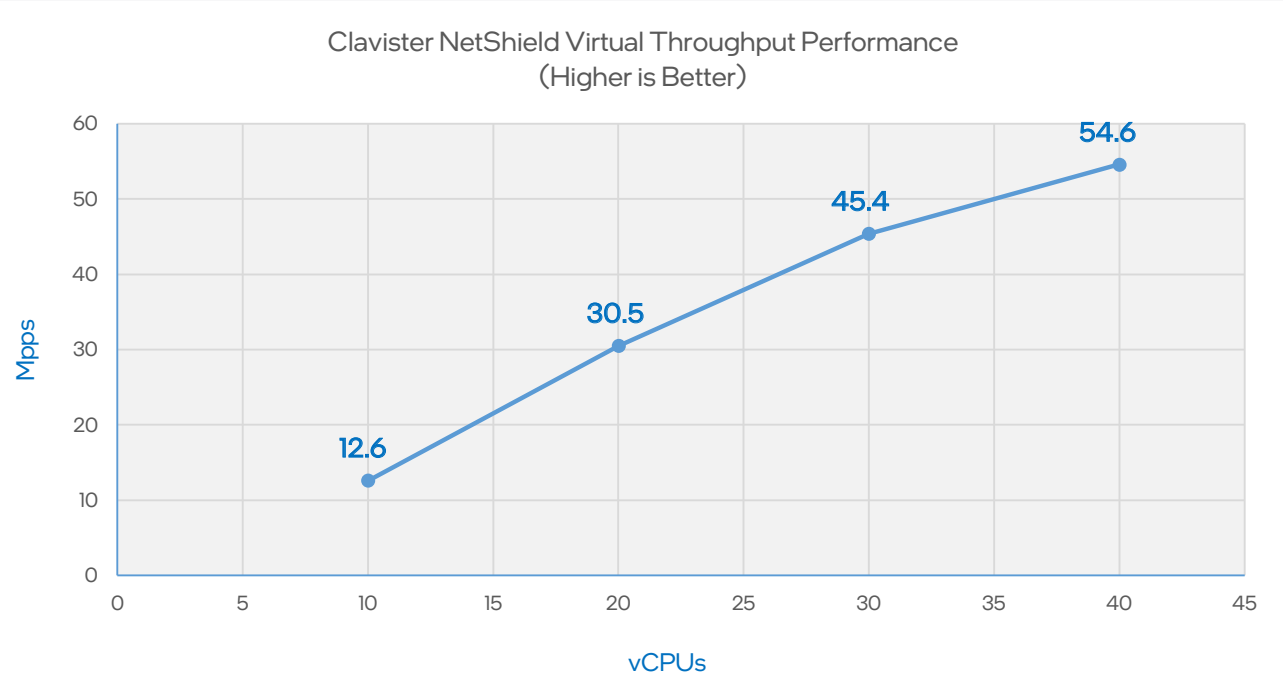

Figure 2. Linear performance demonstrated from tests done using servers equipped with 2nd Generation Intel® Xeon® Scalable processors and Intel® Ethernet Network Adapters XXV710 (higher is better). System under test details can be found in link to solution brief in Learn More section of this paper.

The performance matches the firewalling needs of 4G and 5G networks and set the stage for the test results in this paper.

The goal of the 2022 tests and this paper was to see if the linearity would be demonstrated across a 200 GbE server configuration using a very similar test set up. The results in this paper show the processing efficiency improvements made in the latest version of NetShield Virtual, as well as the improvements made in the CPU and network adapters[1]. Combined, these deliver the performance needed for today's 5G networks.

Clavister NetShield: Made for Intel® Processors

For high volume MNO applications, NetShield can run on servers powered by 3rd Generation Intel® Xeon® Scalable processor family—which includes the Intel® Xeon® Gold 6338N processor used in these tests. These CPUs deliver the performance needed for flexible and highly scalable workload-optimized performance in an NFV environment.

3rd Gen Intel® Xeon® Scalable processors offer a balanced architecture and are designed to support diverse network environments. Optimized for many workloads and performance levels, they are available in a wide range of cores, frequencies, features, and power.

NetShield can also be deployed in customer premises equipment (CPE) or edge network locations using servers based on Intel Atom® processors. Intel Atom® processors are available with a broad range of core counts and hardware features to support different edge use cases.

The platforms are based on energy efficient system-on-chip (SoC) form factors with integrated Intel® Ethernet and Intel® QuickAssist Technology (Intel® QAT), ensuring high performance per watt for network edge implementations.

Test Setup

The tests in this paper are based on tests done in 2021 using the Intel® Xeon® Gold 6230N, a processor that is part of the 2nd Generation Intel® Xeon® Scalable processor family. [Refer to Sidebar.]

The 2022 test results reflect performance improvements with 3rd Generation Intel® Xeon® Scalable processors along with the support for PCIe 4.0 and 100 GbE network adapters from the Intel® Ethernet 800 Series Network Adapters product line.

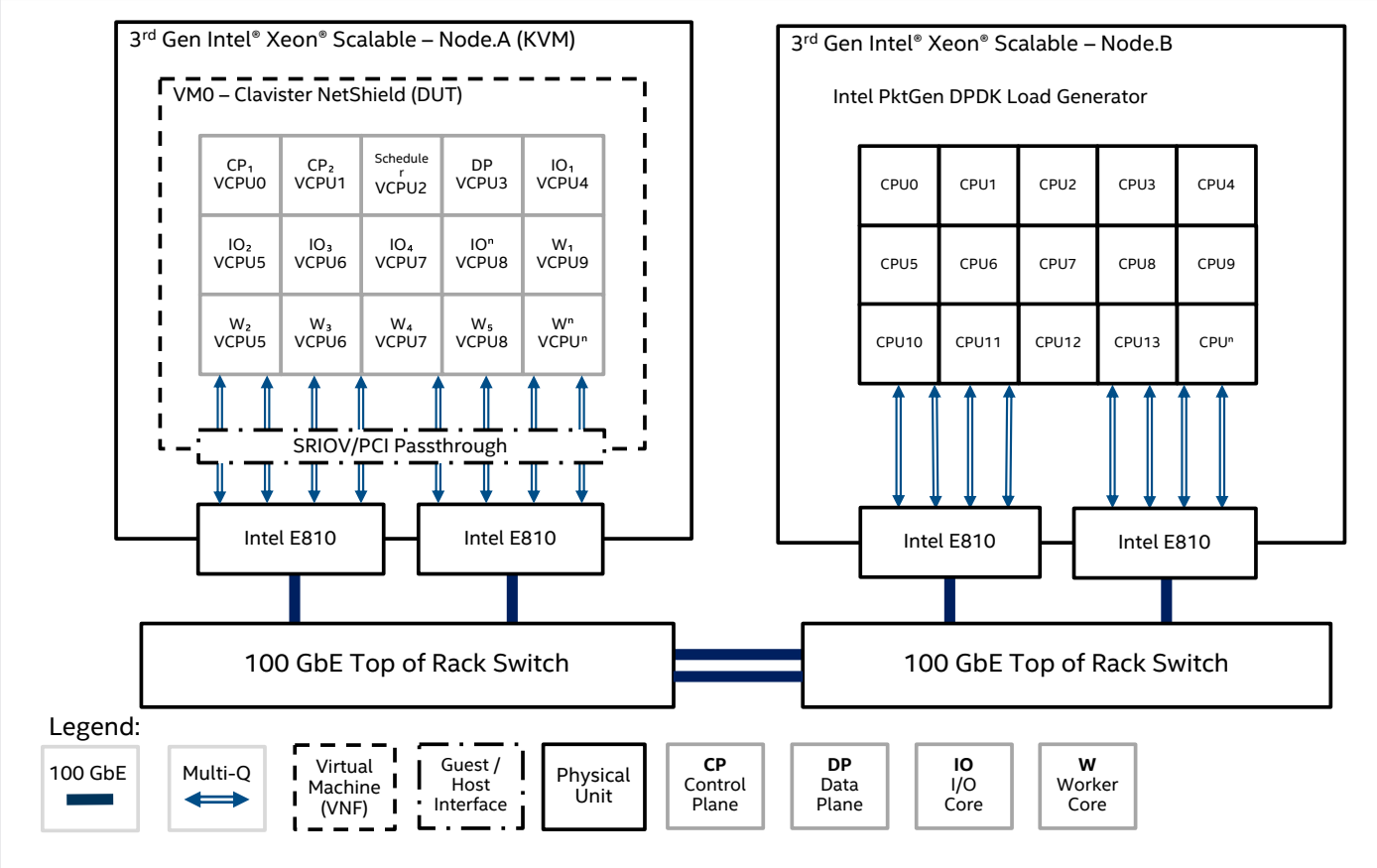

Figure 3. The test setup involves two servers, one supporting virtual Clavister NetShield and the other server supporting Pktgen packet generation software.

This rise in packet throughput means the virtualized firewall supports growing 4G and 5G traffic volumes efficiently with minimal cost. In the virtualized environment that characterizes 5G providers and those moving from 4G to 5G, this performance increase is just one benefit of the virtual NetShield, joining nimble scaling and lower total cost of ownership to make the technology compelling for service providers.

The objective of the tests was to explore the data rates, measured as millions of packets per second (Mpps) on a simulated 5G network terminating at a virtualized N6-connected firewall.

As shown in Figure 3, two servers were used in the tests, both based on Intel® Xeon® Gold 6338N processors running at 2.20 GHz. In the tests, the virtual Clavister NetShield NGFW used a Kernel-based Virtual Machine (KVM) hypervisor.

Each server was connected via a 100GbE top of rack switch using Intel Ethernet Network Adapter E810-C 100Gbps NICs, each of which featured dual 100 GbE ports. Support for PCIe gen4 enabled the full 100Gbps throughput to the CPU. Hyperthreading of the CPU cores was turned on, allowing for each physical core to become two virtual cores. As shown in Fig. 3 NetShield was deployed on a server with 62 vCPUs to help enable the maximum performance. (The software can run on a minimum of two CPU cores with 2 GB of RAM in its most basic configuration.)

The tests used single root I/O virtualization (SR-IOV)/PCI passthrough to mediate the traffic flow from the virtual CPUs to the NICs. Traffic was generated by Pktgen, a traffic generation tool built using DPDK.

Delivering 95 Mpps Throughput

The 3rd Generation Intel Xeon Scalable processor based SUT was tested for maximum performance using 62 virtual cores. The results emphasize scaling in terms of millions of packets per second (Mpps) since the throughput in Gbps was capped by the number of, and speed of, the network adapters at 200 Gbps. As seen in the green bar in Figure 4 this server reached 95 Mpps. This performance and scalability enables MNOs to deploy a single firewall solution across their network with the ability to match the throughput of different network segments.

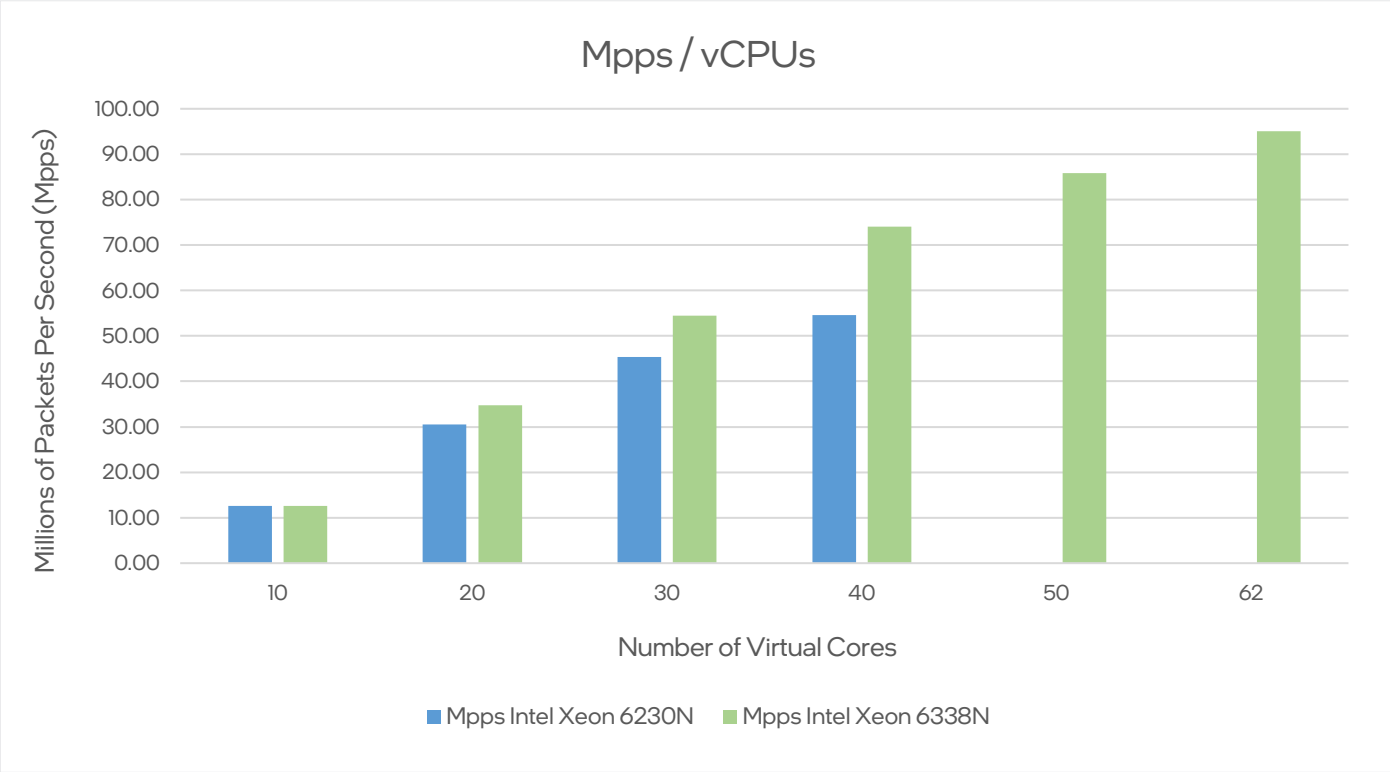

Figure 4. NetShield Virtual linear performance showing maximum performance of the Intel Xeon 6338N (green lines) at up to 62 virtual cores compared to the results of the performance from tests done in March 2021 using the Intel Xeon 6230N (blue lines) which has a maximum of 40 virtual cores. (Higher is better).

Conclusion

NFV has changed the fundamental telecom infrastructure replacing fixed-function, bespoke hardware appliances with more flexible network functions running on commercial off the shelf (COTS) Intel architecture servers. This change required a new approach to deliver firewall protection for these networks. Clavister's NetShield offers the scalability and flexibility needed for virtualized networks. The software has already demonstrated a linear scalability with 25Gbps links to meet the needs of 5G networks. But other areas of the network are moving to 100Gbps links and with the test results described in this paper, Clavister has demonstrated that NetShield, running on a server configured with 3rd Generation Intel® Xeon® Scalable processors and Intel® 800 Series Ethernet Adapters, can deliver at least 95 Mpps at line rate of 200Gbps. This allows MNOs to deploy one firewall to protect a wide range of network assets.

Learn More

Clavister

Clavister NetShield

Clavister NetShield Firewall Throughput Scales Linearly

Intel® Network Builders

Intel® Xeon® Scalable processors

Notices & Disclaimers

[1] New SUT (2022): 1-node, 2x Intel® Xeon® Gold 6338N with 32 cores and 512 GB (16 slots/ 32GB/ 3200) total DDR4 memory, microcode 0xd000375, HT Yes, Turbo Yes, Ubuntu 20.04.5 LTS, Kernel 5.4, Pktgen 3.2.4, DPDK 20.02, NetShield (cOS Stream) 3.90.00, test by Clavister on 11/22/2022.

Baseline SUT (2020): 1-node, 1 socket 2.30 GHz Intel® Xeon® Gold 6230N with 20 cores and 384 GB (24 slots/ 16GB/ 2666) total DDR4 memory, microcode 0x500001c, HT Yes, Turbo Yes, Ubuntu 18.04.2, Kernel 4.15, TRex v2.64, DPDK 20.02, NetShield (cOS Stream) 3.80.00, test by Clavister on 11/2020.

[2] https://portal.etsi.org/nfv/nfv_white_paper.pdf

[3] https://networkbuilders.intel.com/solutionslibrary/clavister-netshield-firewall-throughput-scales-linearly

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.

0223/LV/H09/PDF ♻Please Recycle 354409-001US