Solution Brief

Telecom
Service Providers

Clavister Tests Throughput of Containerized and Virtualized NetShield

Clavister NetShield* virtual NGFW runs both as a VNF and CNF with great performance[1] on 3rd Gen Intel® Xeon® Scalable processor-based servers. Test results give mobile network operators confidence to deploy in either environment

Mobile network operators (MNOs) are on a journey to become fully cloud native. The promise of a cloud-native network is increased network flexibility, scalability and cost effectiveness due to the use of commercial off the shelf (COTS) servers.

The first step in that journey (see Figure 1) was moving from using fixed-function hardware-based network functions to embracing virtualized network functions to build networks. This was a significant change in mindset and in network architecture. Appliances use proprietary hardware and software with little open connectivity to systems from other vendors. Scaling required system replacement.

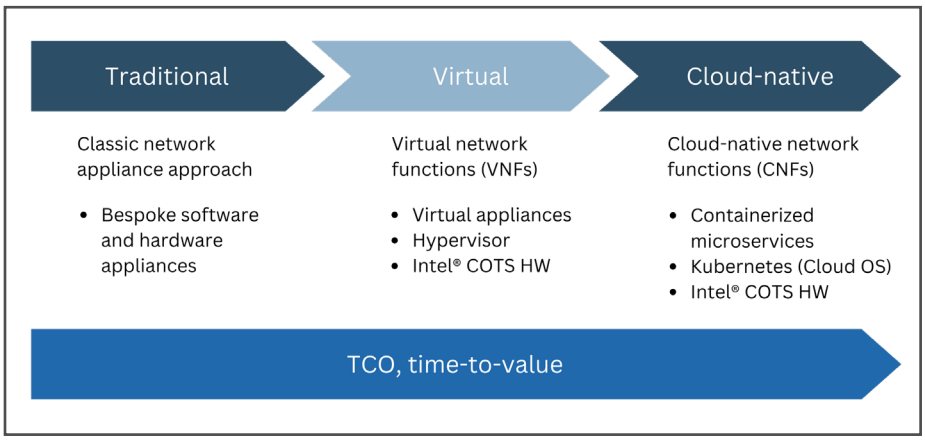

Figure 1. MNO's journey to cloud-native networks.

Virtualization tapped into the growing compute power of Intel® architecture processors and hypervisors to replace the appliance with a software application that can run as a service on a server with other similar virtualized applications.

The next step on the journey is support for cloud native network functions. These are containerized microservices that operate in a cloud operating system (Kubernetes, Docker) that offer similar benefits as virtualization but with some significant changes.

The main difference between containers and virtual machines is that each container shares the host OS running as a separate application or service on that host. VMs are more isolated in that each VM has its own OS instance and are isolated in the sense that the VM contains all the resources and the application for each service.

Feature	Virtualization	Containerization
OS	Has its own kernel	Shares kernel with the host operating system
Portability	Less portable	More portable
Microservices	No	Yes
Speed	Slower to start up and shut down	Faster to start up and shut down
Resource overhead	Uses more compute resources	Uses fewer compute resources
Use cases	Good for isolated applications	Good for portable and scalable applications

Table 1. Differences between virtualization and containerization.

Table 1[2] shows some of the differences between virtualization and containerization and the impact those differences have on the compute platform.

Both virtualization and containerization are viable cloud-native ways to deploy network functions. Which technology is most appropriate depends on the application.

Clavister has developed its next-generation firewalls (NGFWs) to be deployed either as virtual network functions (VNF) or containerization network functions (CNF). The company, an Intel® Network Builders Gold Tier member, is headquartered in Sweden and has provided cyber security solutions for over 25 years.

For this white paper, Clavister collaborated with Intel to test the performance of its Clavister NetShield virtualized NGFW as both a VNF and as a CNF.

NetShield Virtual Next-Generation Firewall

NetShield is a family of carrier-grade, high performance network firewall and 5G security solutions. NetShield is specifically designed for virtual and containerized environments with linear scaling and supports hybrid network models that provide data security for 4G and 5G mobile networks.

NetShield enables a high rate of packet forwarding while keeping data more secure. It runs on Intel architecture processor-based servers. NetShield uses open source Data Plane Development Kit (DPDK), a set of software libraries and drivers to add performance to its data plane.

DPDK facilitates high-performance data throughput in an Intel architecture-based server, processing data packets in user space and avoiding the operating system kernel to reduce latency.

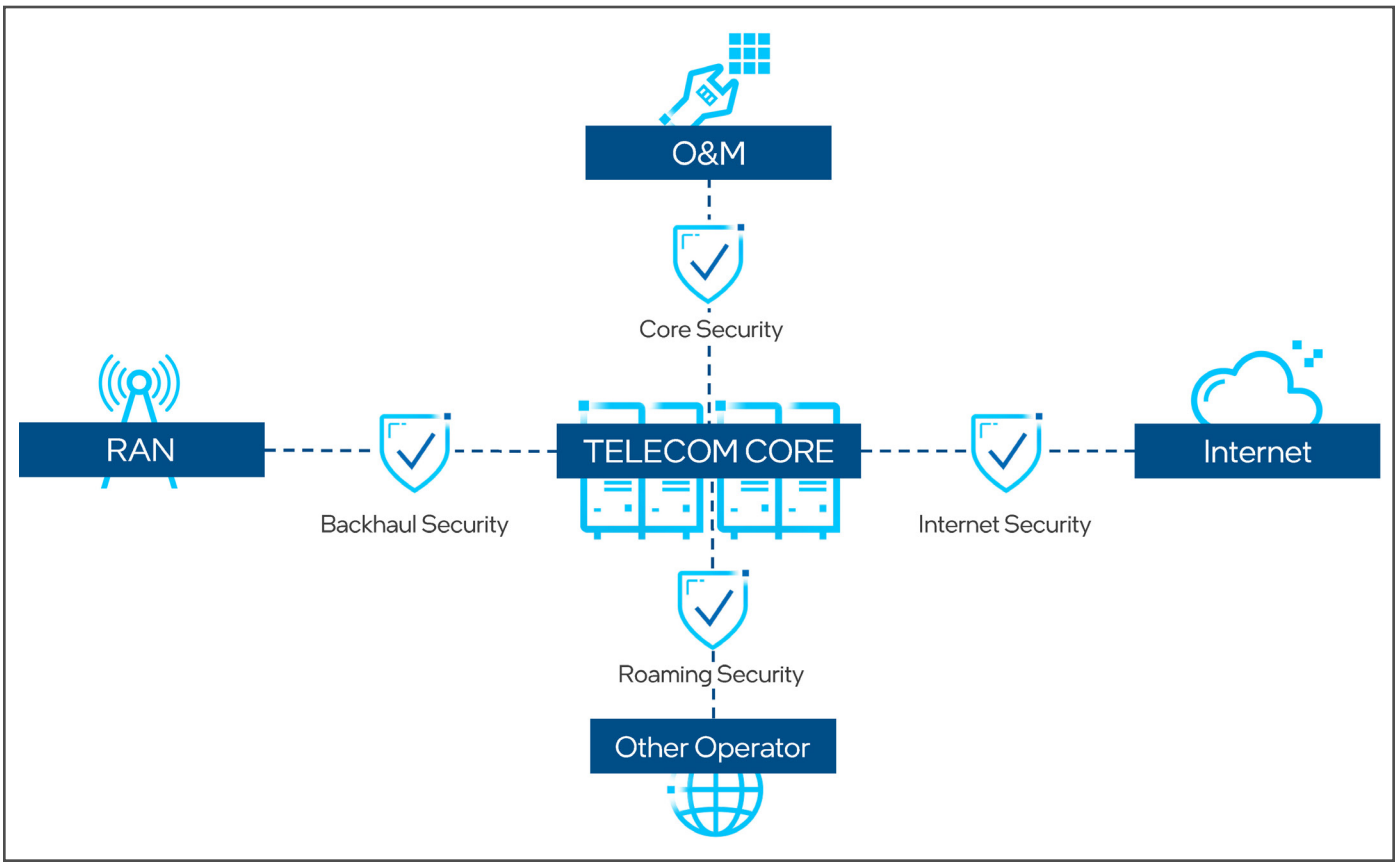

Figure 2. Firewalls provide a barrier against outside cyber security activity by protecting these four data ingress areas.

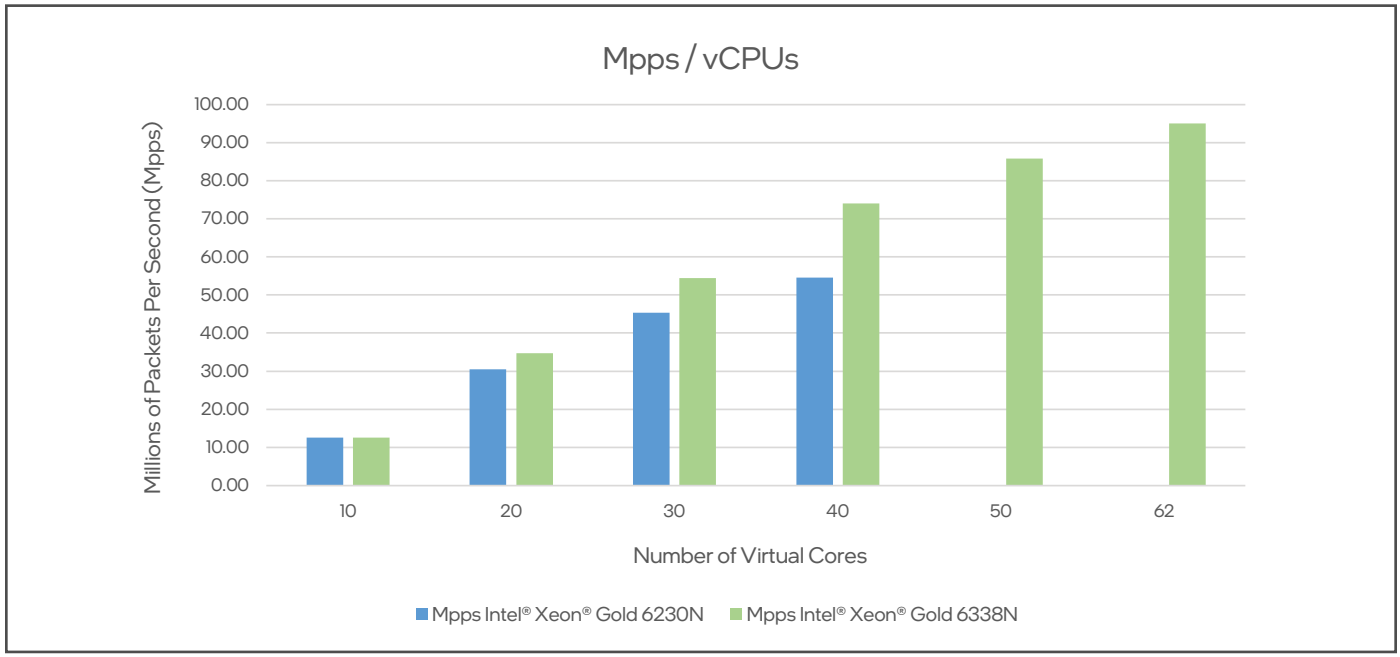

Figure 3. NetShield virtual linear performance showing maximum performance of the Intel® Xeon® Gold 6338N (green lines) at up to 62 virtual cores compared to the results of the performance from tests done in March 2021 using the Intel® Xeon® Gold 6230N (blue lines) which has a maximum of 40 virtual cores (higher is better).

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).

Intel Processors Provide Hardware Performance

For high volume MNO applications, NetShield can run on servers powered by Intel® Xeon® Scalable processor family. These CPUs deliver the performance needed for flexible and highly scalable workload-optimized performance in a network functions virtualization (NFV) environment. 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 consumption configurations.

For customer premises equipment (CPE) or edge network applications, NetShield can also run on servers based on other Intel processors including 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 systems-on-chip (SoC) that have integrated Intel® Ethernet and Intel QAT, ensuring high performance per watt for network edge implementations.

Building on Previous Tests

In 2022, Clavister conducted tests[3] of NetShield VNFs on a 3rd Gen Intel Xeon Scalable processor-based server. The test objectives were to demonstrate the solution's throughput linearity across a 200 GbE server configuration and its performance improvement compared to a server powered by 2nd Gen Intel® Xeon® Scalable processor. Those results can be seen in Figure 3.

CNF and VNF Test Setup

For this paper, the test setup was the same as for the 2022 paper, but the workload is the CNF version of NetShield. In this way the test results can be compared on an "apples-to-apples" basis.

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

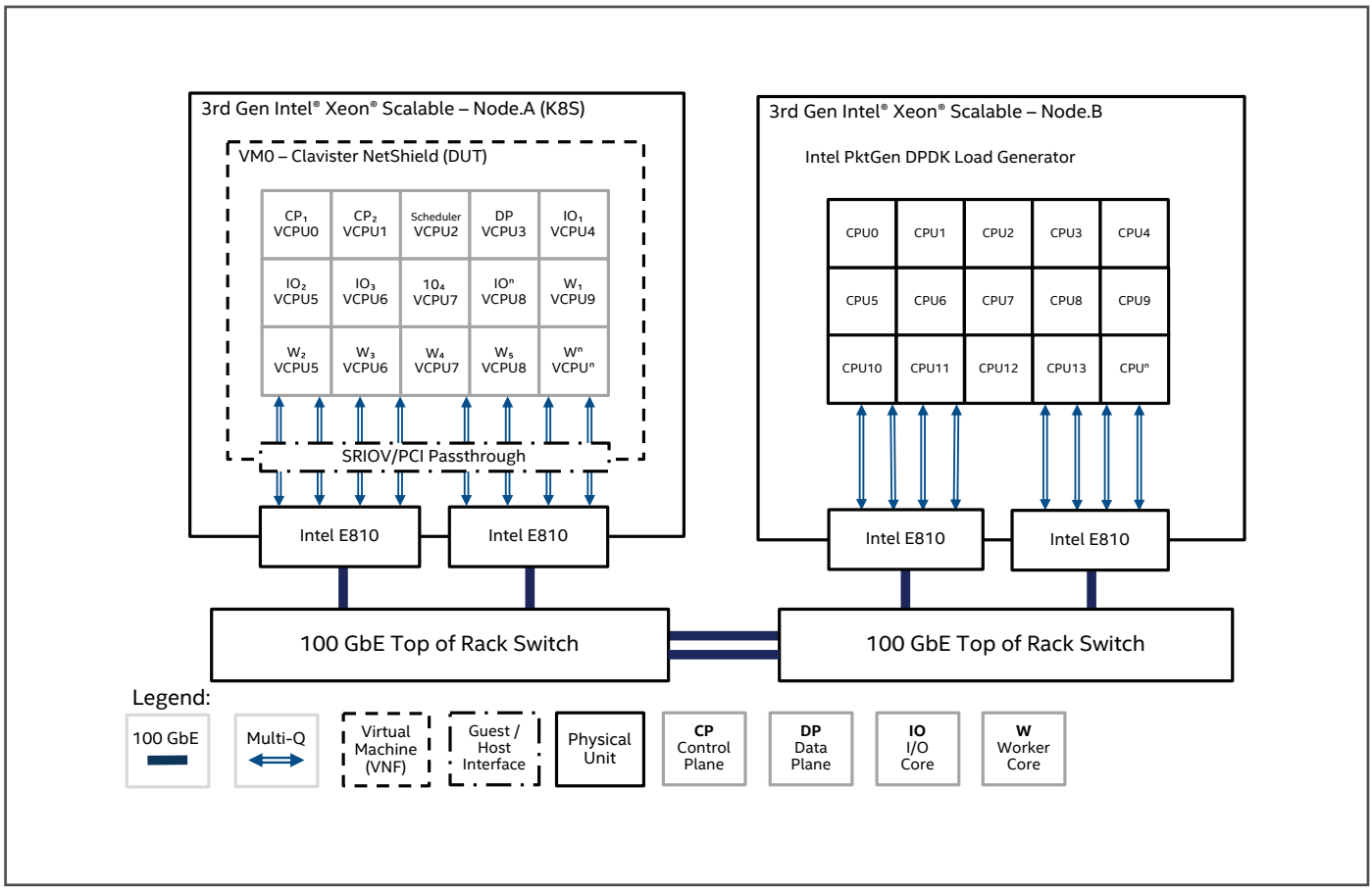

Figure 4. The test setup involves two servers, one supporting containerized NetShield and the other server supporting Pktgen packet generation software.

As shown in Figure 4, two servers were used in the CNF tests, both based on Intel® Xeon® Gold 6338N processors running at 2.20 GHz. The NetShield DUT runs as a container in Kubernetes. DUT throughput is measured in packets-per-second (PPS) using Pktgen as a traffic generator to perform a series of RFC 2544 (64B packets, UDP) tests using increasing numbers (starting at 10 and going to 62) of vCPUs (hyper threads) assigned to the running NetShield.

The result is then compared to test results[4] from a previous white paper where NetShield was running on the same hardware, but as a virtual machine using KVM.

In both tests, each server was connected to a 100GbE top of rack switch. Two Intel® Ethernet Network Adapters E810-2CQDA2 were used to deliver up to 200Gbps of total bandwidth per server. The tests used single root I/O virtualization (SR-IOV)/PCI passthrough to mediate the traffic flow from the virtual CPUs to the Ethernet network adapters.

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.

What's Faster CNF or VNF?

The test shows that NetShield running as a CNF has higher throughput than NetShield running as a VNF but that performance of both is good.

Table 2 and Figure 5 show the PPS performance scaling over different amounts of vCPUs when running NetShield as a container in Kubernetes.

The results show near linear scalability between the number of vCPUs and performance in Mpps. It also shows a slight performance advantage at all levels for the CNFs compared to the VNF, attributable to the infrastructure efficiency when running as a CNF compared to VNF.

vCPUs	Mpps (VNF)	Mpps (CNF)
10	12.57	13.04
20	34.72	36.33
30	54.46	56.55
40	74.00	75.56
50	85.78	87.44
62	95.05	101.43

Table 2. Linear increase in performance when adding vCPUs.

[4] Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.
Read the paper at https://networkbuilders.intel.com/solutionslibrary/clavister-netshield-delivers-scalable-performance-up-to-95-mpps1

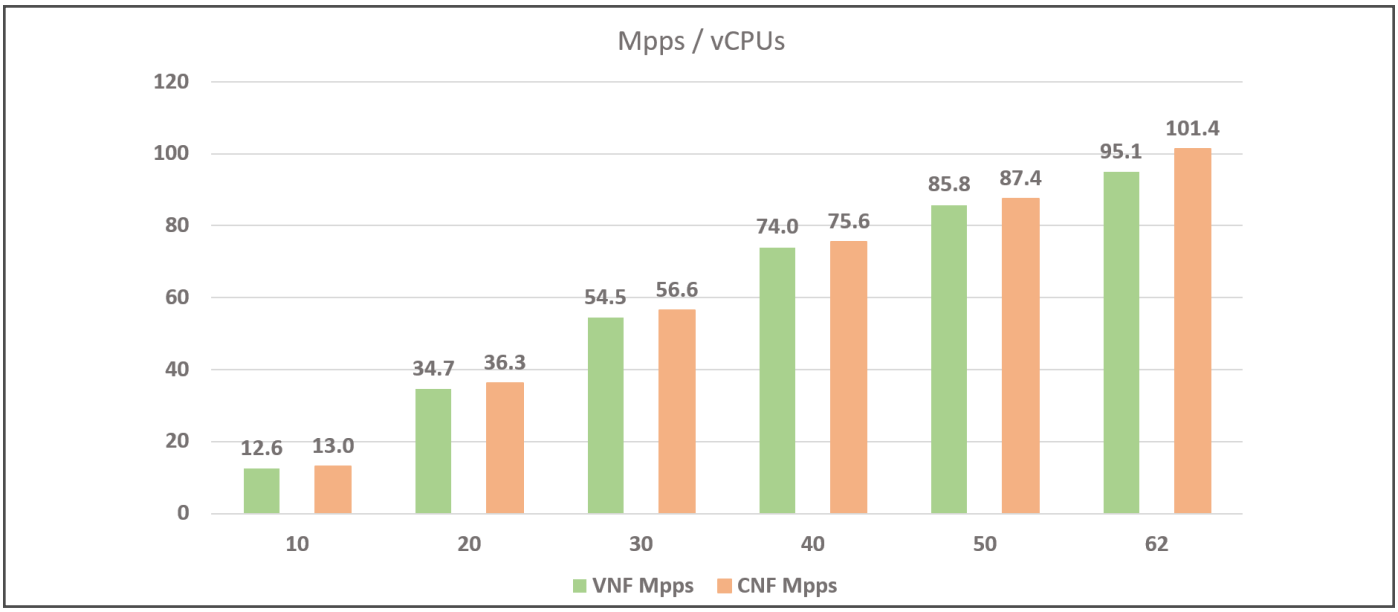

Figure 5. This chart is a graphical view of the performance of NetShield running as a VNF (green) and a CNF (orange) as more vCPUs are dedicated to the application. CNFs always have a bit better performance, but both instances offer very good throughput.

Conclusion

MNOs are on a journey to fully support cloud native technology throughout their networks. The first step in that journey – moving from fixed-function appliances to virtualized network functions – was a straightforward decision. The next step – choosing between VNFs and CNFs – is not as evident. Applications will have different needs for app isolation, portability, scalability and MNOs will choose VNFs or CNFs accordingly. It's possible that the cloud ready network of the future will have a combination of both technologies and Clavister is ready to support both options.

Clavister tested[5] its NetShield NGFW in each virtualization mode to determine if there was a performance advantage that should also be factored into customer decisions. The tests showed that both deployment modes are fast, but that CNFs are slightly faster.

These results should give MNOs peace of mind that they can secure their network using either VNFs or CNFs.

Learn More

Clavister

Clavister NetShield

Clavister NetShield Delivers Scalable Performance up to 95 Mpps

Intel Network Builders

Intel Xeon Scalable processor family

Intel Ethernet Network Adapter E810-2CQDA2

[1] DUT (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, two Intel Ethernet Network Adapter E810-2CQDA2. Test by Clavister on 10/23/23.

[2] Source: https://cloud.google.com/discover/containers-vs-vms

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

Notices & Disclaimers

0624/TM/DJA/PDF Please Recycle 360290-001US