Solution Brief

Mobile Network Operators
Network Security

Clavister NetShield Firewall Throughput Scales Linearly

Tests by Clavister of virtual services-based firewall using 2nd generation Intel® Xeon® Scalable CPU shows packet throughput rates increase as more cores are incorporated, demonstrating linear scalability for firewalling in a 5G environment[1]

Enterprise demand for more applications and services and the adoption of 5G for networking means more virtualization and containerization of the network as many of the 5G standards call for these technologies. Simultaneously with the proliferation of virtualization has come steadily increasing traffic levels. According to telecommunications research firm TeleGeography, peak internet traffic worldwide increased about 30 percent per year from 2016 to 2020; in 2020, as much of the world was under lockdown, the demand shot up 47 percent.[2]

Moreover, cloud storage—and the related uploading and downloading—as well as online video gaming and video streaming require significant and increasing bandwidth. As of 2019, cloud giants Google, Amazon, Facebook, and Microsoft consumed 64% of the global bandwidth capacity.[3]

As the volume of data flowing through networks increases, so do security risks. More data means more camouflage for malware. As the volume of data rises, mobile network operators (MNOs) find it increasingly difficult to analyze traffic as it enters and exits the network.

Network security that can keep up with this increased data consumption is a key concern for MNOs. The firewall is one critical component of the necessary security. Firewalls prevent unauthorized intrusion, forming a barrier between the internal network and the outside world. A firewall monitors traffic between the two and blocks unauthorized data from crossing the barrier. It repels denial of service (DoS) attacks and prevents attackers from injecting malware into the system. Firewalls can support Internet Protocol Security (IPsec) by enforcing authentication rules when devices attempt to connect, blocking devices that cannot authenticate themselves.

In this environment, the ability to more securely deploy and manage solution elements in a cost-effective way is paramount. Service providers can address this dilemma with a services-based firewall (SBFW). A SBFW is designed for virtualized environments and enables rapid scalability, high data throughput, and easy management. It can also bring functionality such as application management and load balancing.

Clavister NetShield Virtual is a SBFW that provides great flexibility, taking full advantage of modern multi-core Intel architecture processors to provide firewall protection with low impact on the data flow. Clavister, an Intel® Network Builders ecosystem member, tested its product to demonstrate the scalability of the virtual SBFW.

NetShield Virtual Services-Based Firewall from Clavister

For all of its benefits, adopting a services-based architecture demands a new approach to security and enforcement. A distributed cloud network architecture, which characterizes 5G, means that security functions must expand beyond the traditional network perimeter. MNOs must understand that the entire network, on both user and control planes, is now the security battleground. Security measures such as traffic encryption, traffic filtering, and deep packet inspection shift from a static model to a

fluid one, based on just where the applications are running on the cloud. As a result, effective security enforcement now requires a cloud-native, software-driven strategy.

Clavister NetShield Virtual is designed for a services-based environment, enabling a high rate of packet forwarding while keeping data more secure. It runs on Intel® Xeon® Scalable processor- and Intel Atom® processor-based systems. And as packet inspection demand grows, NetShield Virtual scales to match. It's manageable with a single tool, capable of managing tens of thousands of instances.

The Clavister NetShield Virtual SBFW operates using either VMware vSphere or KVM hypervisors. It can run on a minimum of two CPU cores with 2 GB of RAM in its most basic configuration. For larger applications, NetShield Virtual can fully utilize modern multi-core CPUs, efficiently managing firewall functionality at Gigabit data rates. 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 Virtual fully supports the N6 interface in 5G architectures, and efficiently utilizes the SGi interface in 4G.

A 5G services-based architecture is characterized by API exposure, service discovery, and network slicing. These three components create a dynamic network supporting cloud-native microservices, which leads to the development of reusable building blocks that can then be combined to create new services. Security in such an environment is correspondingly complex and demands the kind of fluidity and scalability that Clavister NetShield Virtual provides without slowing data packet throughput.

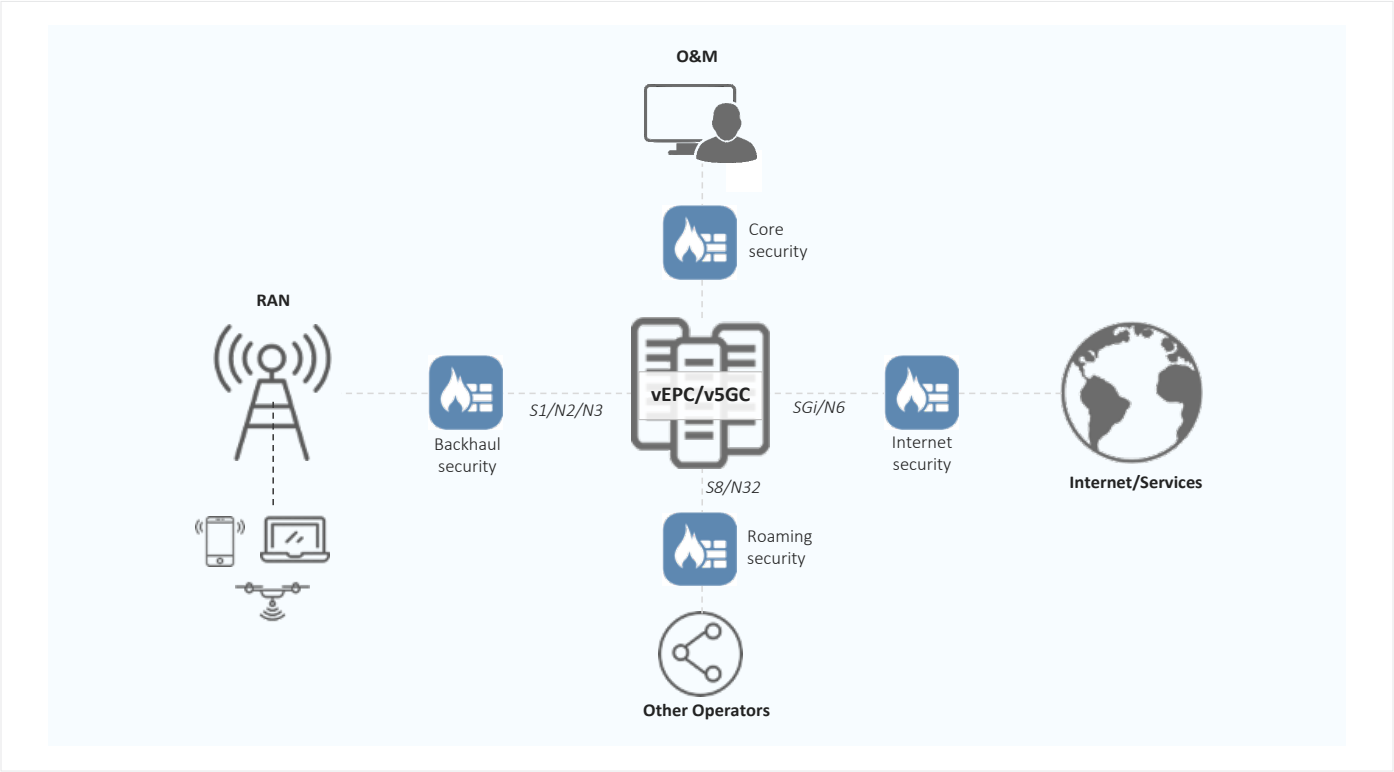

Figure 1. In a 5G network, firewall instances surround key network elements.[4]

Clavister NetShield Virtual: Made for Intel® Processors

Clavister NetShield Virtual is designed for servers based on Intel Xeon Scalable processors and Intel Atom processors. For high-volume applications, processors from the Intel Xeon Scalable processor family—which includes the 2nd generation Intel Xeon Gold 6230N processor used in these tests—are used to deliver the performance needed for flexible and highly scalable workload-optimized performance in an NFV environment.

Intel Xeon Scalable processors are optimal for applications requiring high performance and power efficiency, such as distributed orchestration, high-throughput encryption and firewall processing. The Intel Xeon Gold 6230N processor offers a 27.5 MB cache, 20 cores, and 40 threads per socket. The processor features a 2.3 GHz clock rate, which can go to a maximum of 3.5 GHz in turbo mode.

Intel Atom processors are used for branch office firewall applications. These processors can start faster, work longer, and support high-resolution Ultra HD 4K multimedia within an ultra-thin and lightweight design.[5] Intel Atom processors are systems on chips (SoCs) that are designed for universal customer premises equipment (uCPE) and other low-power, high-density workloads.

Clavister NetShield Virtual Data Plane Readily Adaptable to Customer Needs

Clavister utilized the open source Data Plane Development Kit (DPDK), a set of software libraries and drivers in NetShield Virtual's scalable 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. Through this capability, Clavister implemented a universal data plane for NetShield Virtual, so that the virtual SBFW does not need dedicated cores for specific processes such as IPsec processing or packet filtering.

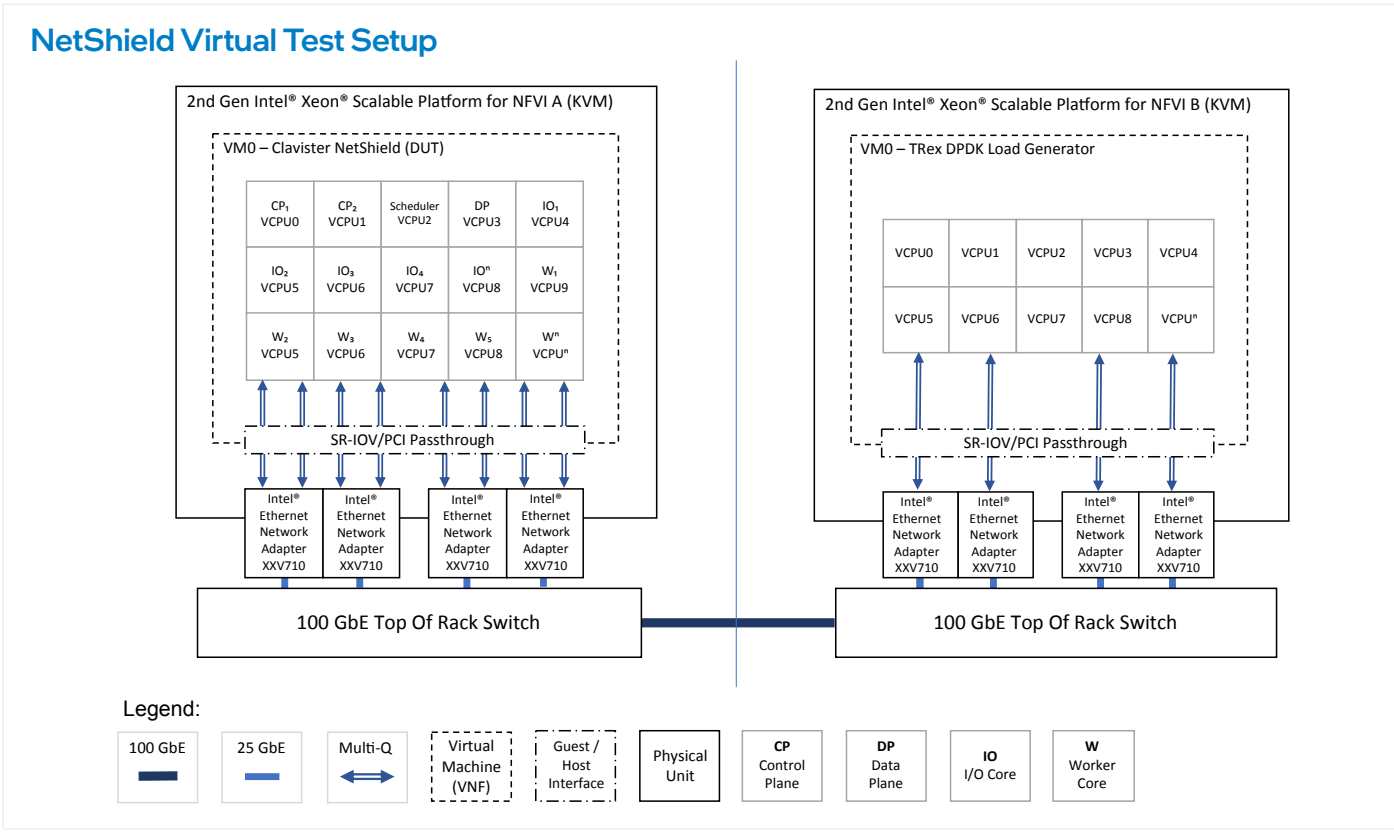

Figure 2. Block diagram of test configuration for Clavister NetShield Virtual firewall.

Clavister set out to test data rates, measured as millions of packets per second (Mpps) on a simulated 5G network deploying a fully virtualized N6 firewall. For testing purposes, the NetShield Virtual software ran on a 2nd generation Intel Xeon Gold 6230N processor-based server. Traffic flowed through four Intel Ethernet Network Adapters XXV710-DA2 25 GbE NICs, equaling 100 Gbps total throughput. The test utilized 64-byte UDP packets with packet losses measured in accordance with RFC 2544. Traffic was generated by a TRex traffic generator.

The TRex DPDK load generator ran on one KVM, passing data through four NICs to a 100 GbE top-of-rack switch, which sent it to another 100 GbE switch in the Clavister NetShield Virtual KVM. Packets then flowed through another quartet of 25 GbE NICs and through the NetShield Virtual device under test (DUT).

Clavister used single root I/O virtualization (SR-IOV)/PCI Passthrough to mediate the traffic flow from the virtual CPUs to the NICs.

To determine how increased processor capacity affected the rate of packet flow, the test compared four configurations as seen in Table 1.

CORES	VCPUS (THREADS)	MPPS
5	10	12.6
10	20	30.5
15	30	45.4
20	40	54.6

Table 1. Clavister NetShield Virtual throughput test results showing increasing performance as additional cores are utilized.

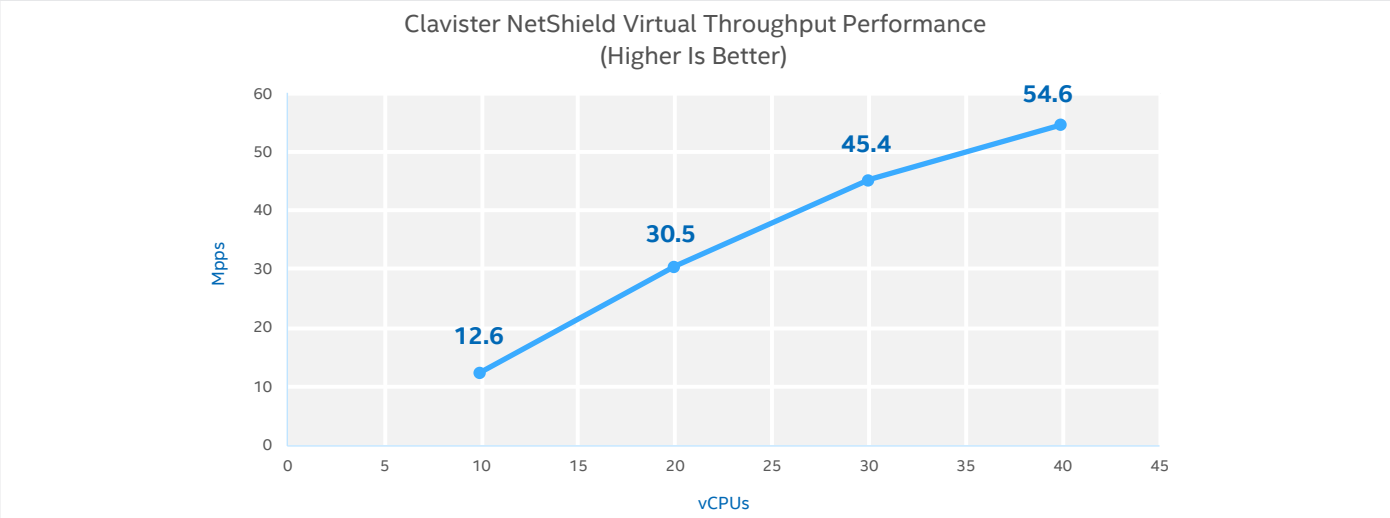

Figure 3. Chart showing the linear performance of the NetShield Virtual as new cores are added.

As shown in the test results in Figure 3, running NetShield Virtual on Intel architecture processors leads to linear data rate increases as more cores and threads are utilized. Service providers need to keep packets flowing at a high rate. Clavister's tests demonstrate significant packet throughput increases—up to 54.6 Mpps by adding more physical cores and vCPUs within a single Intel processor-based server. The amount of packets per second corresponds to a traffic volume of between 36 Gbps (small packets) and 600 Gbps (large packets).

This demonstrates the scalability of the NetShield Virtual as multiple processors, dynamically managed, can ensure data security at any level of traffic at a low cost and with negligible overhead.

Conclusion

The tests by Clavister show a dramatic and consistent increase in packet forwarding rate when using Clavister NetShield Virtual on an Intel Xeon Scalable Gold processor as more cores and threads are recruited. This rise in packet throughput means the virtualized firewall can support growing 4G and 5G traffic volumes efficiently with minimal cost. In the virtualized environment that characterizes 5G providers and those moving to 5G from 4G, this performance increase is just one benefit of the NetShield Virtual SBFW, joining nimble scaling and lower total cost of ownership to make the technology compelling for service providers.

Learn More

Clavister

Clavister NetShield Virtual

Intel® Network Builders

Intel® Xeon® Scalable Processors

Notices & Disclaimers

[1] Testing done by Clavister in Q4 2020. DUT server configuration featured a 2.30 GHz Intel Xeon Gold 6230N processor (microcode: 0x500001c). Intel® Hyper-Threading Technology was turned on and Intel® Turbo Boost Technology 2.0 was turned on. BIOS version was Intel Corporation SE5C620.86B.0D.01.0395.02272019140. The server featured 384 GB of RAM (24 slots of 16 GB 2666 MHz RAM). The test utilized one node and one socket. Networking was provided by 4 Intel® Ethernet Network Adapter XXV710 SFP28 (Rev 02) NICs at 25 GbE each. Operating system was Ubuntu Linux release 18.04.2 LTS with kernel 4.15.0-47-generic. Workload was Clavister NetShield 3.80.00.

[2] https://blog.telegeography.com/2021-global-internet-map-tracks-global-capacity-traffic-and-cloud-infrastructure

[3] https://blog.telegeography.com/lets-just-say-demand-is-thriving-in-the-global-bandwidth-market

[4] Figures provided courtesy of Clavister.

[5] https://www.intel.com/content/www/us/en/products/details/processors/atom.html

Performance varies by use, configuration and other factors. Learn more at https://www.intel.com/PerformanceIndex.

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

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

0421/DO/H09/PDF ♻ Please Recycle 346831-001US