SOLUTION BRIEF

Communications Service Providers
CGNAT

NFWare Provides High Performance Virtual Carrier-Grade NAT

With packet throughput of 231 Gbps, NFWare demonstrates new role for vCGNAT in communication service provider (CommSP) networks of all sizes. Network adoption with a Tier 1 CommSP demonstrates scalability to millions of users.

The modern internet was built using internet protocol version 4 (IPv4), but the pool of IPv4 addresses has been exhausted and transitioning to a permanent fix in IPv6 will take many more years. Carrier-grade network address translation (CGNAT) is a proven tool to help communications service providers (CommSPs) make the most of their IPv4 address pools. NFWare is offering a virtualized CGNAT service that provides high-throughput translation functionality with the agility, scalability, and reduced hardware costs that come from virtualization.

CommSPs Must Manage IPv4 Addresses

CommSPs face a significant challenge in overcoming the exhaustion of IPv4 internet addresses. With a 32-bit address space, IPv4 has the capacity for 4 billion unique addresses, and all of these have been assigned to organizations and service providers. After decades of awareness and effort to transition to IPv6, which has an address space of 340 trillion trillion trillion (3.4×10^{38}) addresses, it is estimated that only 25%[1] of all internet networks advertise IPv6 connectivity worldwide. In some countries the IPv6 utilization is less. Because a complete IPv6 chain of communication (client devices, service providers' networks, enterprise applications, web sites, etc.) is required for IPv6 to work, it's taken longer to make the transition than anticipated.

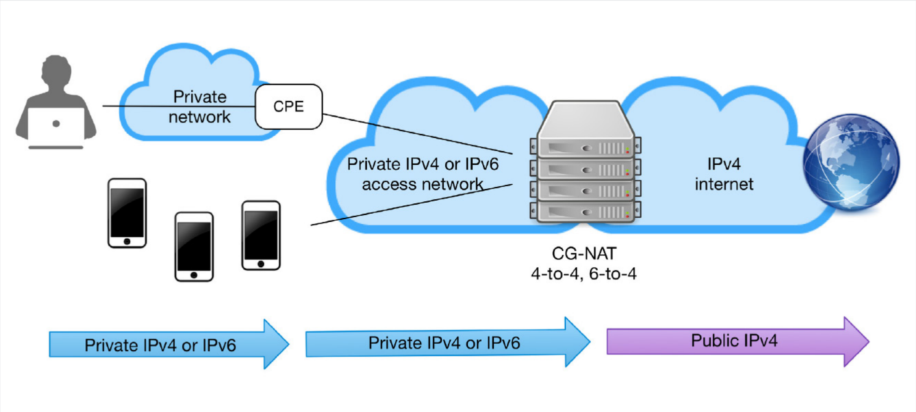

Figure 1. Users on a private network connect with the CGNAT to obtain an IPv4 address for using the public internet.[2]

See backup for configuration details. For more complete information about performance and benchmark results, visit www.intel.com/benchmarks.

Because IPv4 addresses were sold in blocks, many organizations have more addresses than they will use. CommSPs can buy these IP addresses from these organizations, but the cost has increased over time. Carrier grade network address translation (CGNAT) is a tool that is helping CommSPs to manage their IPv4 address pools while still growing the number of IP devices supported by their networks.

CGNAT uses translator software combined with an IP router embedded in the CommSP's network to change private network addresses into public IPv4 addresses. Thus, CommSPs can use the private addresses—which are in wide supply but can't be used on the internet—for all internal network traffic and reserve their IPv4 addresses to be used only when a data stream needs to access an internet resource. This enables the sharing of small pools of public addresses among multiple end sites, thus greatly expanding the capacity of the existing network.

Scaling CGNAT is important, but it is costly. Virtualized CGNAT solutions offer a more cost effective solution because they utilize white box server platforms instead of single function appliances. These solutions have been around for some time, but have not offered the performance needed for core CGNAT applications.

Intel® Network Builders ecosystem partner NFWare has developed its own virtualized CGNAT solution that does offer wire-speed performance for the largest CommSP networks. In this paper, we examine that performance more closely and look at the results of a CommSP who has deployed the vCGNAT service across a population of millions of people.

NFWare vCGNAT Offers Performance

NFWare vCGNAT is a centralized NAT with high-capacity address and port translation capabilities that is installed in telco data centers. The software utilizes NAT44 to map each application data flow on the customer side to a public IPv4 address and a TCP or UDP port. NFWare vCGNAT multiplexes the addresses of many inside devices to a single outside address by mapping application flows, thus minimizing the number of IPv4 addresses needed to serve a particular user base.

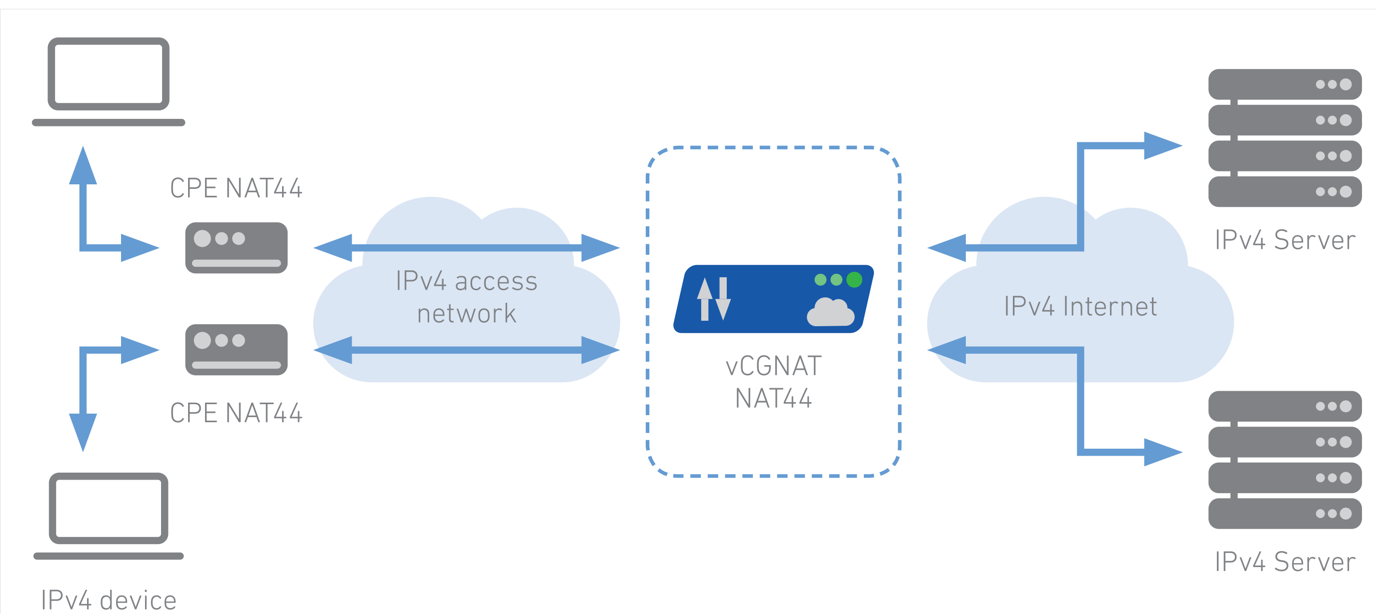

Figure 2. NFWare vCGNAT translates between private network addresses and IPv4 addresses needed for use of the public internet.

The software also supports NAT64, which facilitates mapping a customer IPv6 address to the public IPv4 address using its TCP or UDP port to map a data session to a user. This functionality allows users that have adopted to IPv6 to have access to IPv4 services on the public internet.

NFWare vCGNAT can run on a wide variety of Intel® Xeon® processors and Intel Xeon Scalable processors depending upon the desired throughput. NFWare has demonstrated high performance using Intel Xeon Gold processors, which are part of the Intel Xeon Scalable processor family that is designed for cloud-optimized, virtualized networks. The Intel Xeon Scalable platform features an open architecture that scales and adapts with ease to handle the demands of emerging applications.

Test Results

NFWare vCGNAT is scalable for deployment in a wide range of applications based on the results of tests conducted by the European Advanced Networking Test Center (EANTC). The tests were devised to measure the maximum throughput generated by 99.6 M user sessions. The tests utilized a traffic generator configured to emulate four ports of bi-directional traffic from 20,000 internal client IP addresses to 1,245 server IP addresses. The tests utilized frame sizes ranging from 84 bytes to 1520 bytes in addition to an IMIX frame distribution (see Table 1) comprising a weighted range of packet sizes with nearly 41% of packets at 118 bytes and 26% coming from 1,536 byte frames.

Figure 3 shows the performance results with max throughput of 231 Gbps at 1,520 byte packets and 212 Gbps using the IMIX packet distribution. The maximum packets per second of 88 Mpps was recorded at 260 byte packet sizes.[3]

EANTC's standards ensure that its customers can reproduce the test that was performed and get the same results, provided that the same system under test (SUT) configurations and conditions are fulfilled.

Due to that, EANTC selected the frame sizes in the latest NFWare vCGNAT performance test based on different technical reasons. Specifically, the 84 byte frame size was determined because of:

- The 84 byte Ethernet frame size = 18 Byte Ethernet header + 20 Byte IPv4 header + 8 Byte UDP header + 38 Byte data payload
- That size of payload (38 bytes) enables us to measure the network latency consistently and adequately.

FRAME SIZE (BYTES)	WEIGHT	PERCENTAGE (%)
82	1	3.7
118	11	40.74
391	3	11.11
588	2	7.4
1,318	3	11.11
1,536	7	25.92

Table 1. IMIX Packet Distribution

EANTC increased the MTU size on the SUT's interfaces to jumbo-frame size (9,000 byte). This allowed EANTC to generate frame sizes larger than the standard MTU size (1,518 byte).

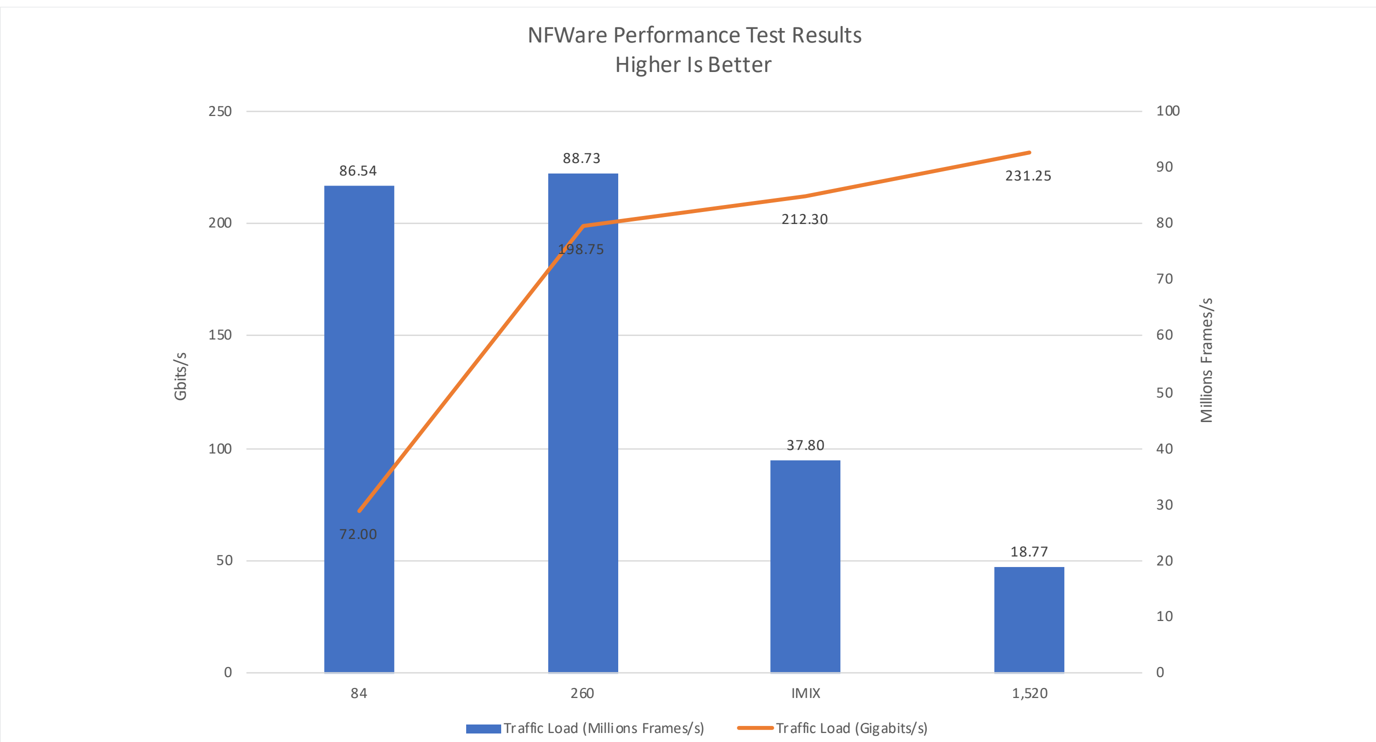

Figure 3. NFWare performance test results. See backup for configuration details. For more complete information about performance and benchmark results, visit www.intel.com/benchmarks.

Case Study

NFWare vCGNAT has been deployed in CommSP networks in the USA, Europe, and the Asia-Pacific region.

The largest NFWare vCGNAT implementation is in a large Tier 1 CommSP. The CGNAT deployed in the CommSPs' servers in data centers in the country's largest cities. Each server was configured to provide throughput of up to 160 Gbps, with all network traffic processed through these high-throughput servers. The implementation went extremely smoothly with a full functioning commercial service two weeks after the hardware was delivered.

Conclusion

The diminishing availability and high cost of IPv4 addresses will have a significant impact on how CommSPs can grow their user base and launch new services. CGNAT offers a solution, but until recently CommSPs have had to choose between costly and complicated fixed-function appliances or virtualized versions that offered better cost effectiveness, but lower performance. However, NFWare's vCGNAT solution offers very high performance—up to 231 Gbps.[3] With design wins across the world, the NFWare solution is giving CommSPs a new option for better managing IPv4 addresses in a way that doesn't limit service deployments or growth and allows for a managed transition to IPv6.

NFWare vCGNAT Product Features

- Application Layer Gateways to connect to other IP protocols such as FTP, DNS, SIP, IPsec, and others
- Expanded network throughput using Link Aggregation Control Protocol
- Filtering features to manage external endpoint access to devices on the internal network
- More control over port mapping using Port Control Protocol
- Paired pooling mode to reserve an IPv4 address for a device
- VLAN support
- OpenStack integration
- Redundant instance for high availability
- Deterministic NAT mode to map an IP address to the same IP and port range
- Port block allocation to reduce logging
- NAT bindings logging providing a record of bindings per connected client

About NFWare

NFWare develops disruptive virtualized network software for operators and data-centers to help them build more efficient and flexible network infrastructure. By leveraging NFV technologies the company helps its customers to reduce TCO and achieve operational efficiencies while accelerating new service deployment. NFWare's Multicore Network Stack is designed for fast processing of network traffic on standard Intel architectures servers. More information is at https://www.nfware.com.

About Intel® Network Builders

Intel Network Builders is an ecosystem of infrastructure, software, and technology vendors coming together with communications service providers and end users to accelerate the adoption of solutions based on network functions virtualization (NFV) and software defined networking (SDN) in telecommunications and data center networks. The program offers technical support, matchmaking, and co-marketing opportunities to help facilitate joint collaboration through to the trial and deployment of NFV and SDN solutions. Learn more at http://networkbuilders.intel.com.

Notices & Disclaimers

[1] https://www.internetsociety.org/resources/2018/state-of-ipv6-deployment-2018/

[2] Figures 1 and 2 provided courtesy of NFWare.

[3] Tests conducted by EANTC in October 2019. Configurations: Server was a Lenovo ThinkSystem SR650 featuring dual 2.1 GHz Intel Xeon Gold 6252 CPUs each with 24 cores (microcode: 0x4000021). Server memory featured 768 GB of RAM comprised of 24 32GB TruDDR4 2667 MHz RDIMMs and Intel P4500 2TB Entry NVMe PCIe 2.0 SSD. Five Intel XXV710-DA2 PCIe 25Gb two port 25GbE adapters were installed for network connectivity. Firmware: BIOS v2.13, BMC V2.12. Host OS: RHEL 7.7 (Kernel: Linux 3.10.0-1062.el7.x86_64). Hypervisor: KVM/QEMU 2.12.0. VIM: Red Hat Open Stack 13, Lenovo Open Cloud Automation v0.9. Intel Hyper-Threading Technology and Intel Turbo Boost Technology were enabled. EPA features: Non-Uniform, Memory Access (NUMA) and CPU Pinning enabled.

0520/DO/H09/PDF ♻ Please Recycle 343186-001US