NFWare Virtual CGNAT

Network Address Translation Solution for Service Providers' Networks
to preserve IPv4 and migrate to IPv6

NFWare Carrier-Grade NAT (or Large Scale NAT) is a virtual appliance designed to provide high performance and transparent address and protocol translation.

Highlights

- Virtual appliance
- Runs on COTS HW
- Rich ALG support
- Large scale
- High throughput

Overview

The Internet is running out of unassigned IPv4 addresses, which will limit the number of new devices that can share data on wired and wireless networks. The industry has started down the long road to IPv6, which will solve the problem, but Communications Service Providers need a solution today to provide services to a growing number of customers, and many are adopting carrier-grade network address translation (CG-NAT) to extend IPv4 networks.

NFWare vCGNAT is a virtual NAT placed in the service provider's network to help extend the life of IPv4 network infrastructure and mitigate IPv4 address exhaustion by using address and port translation on a large scale.

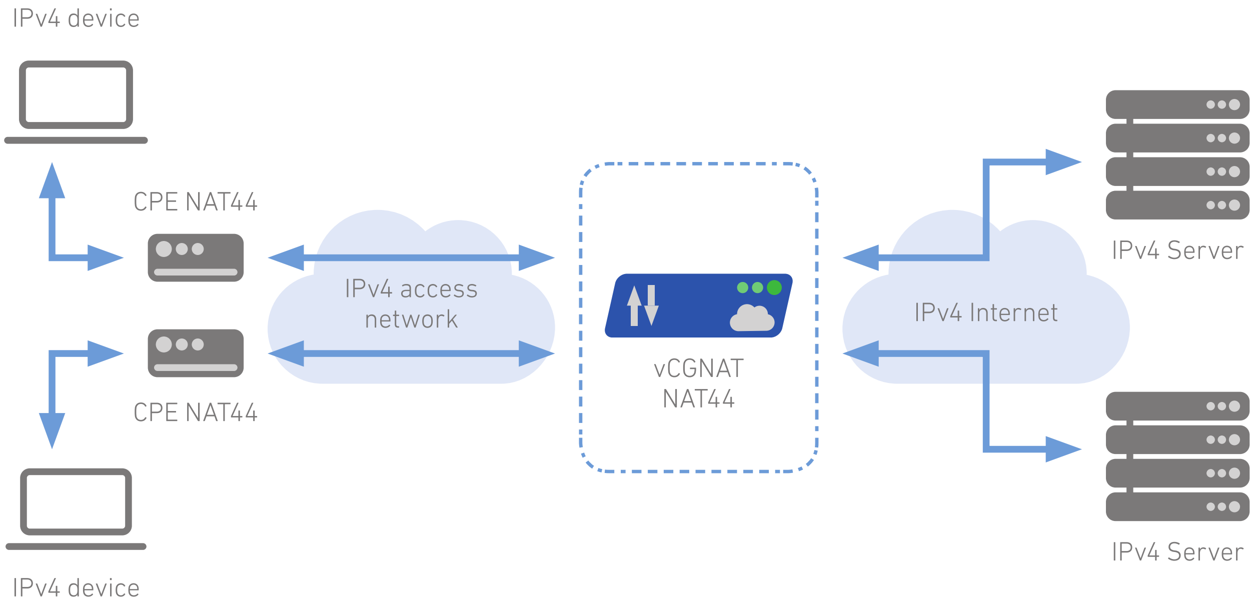
NFWare is one of the first IP routing technology companies to offer a virtualized CG-NAT. NFWare Carrier Grade NAT is software that is optimized to run on standard x86 servers and in a hypervisor.

NAT Modes

NAT44

NAT44 is the vCGNAT operational mode for mapping each application flow on the customer side to the public IPv4 address and one of its TCP or UDP ports as identified by the combination of a private IPv4 address and a TCP or UDP port. vCGNAT multiplexes the addresses of many inside devices to a single outside address by mapping application flows.NFWare Carrier-Grade NAT (or Large Scale NAT) is a virtual appliance designed to provide high performance and transparent address and protocol translation.

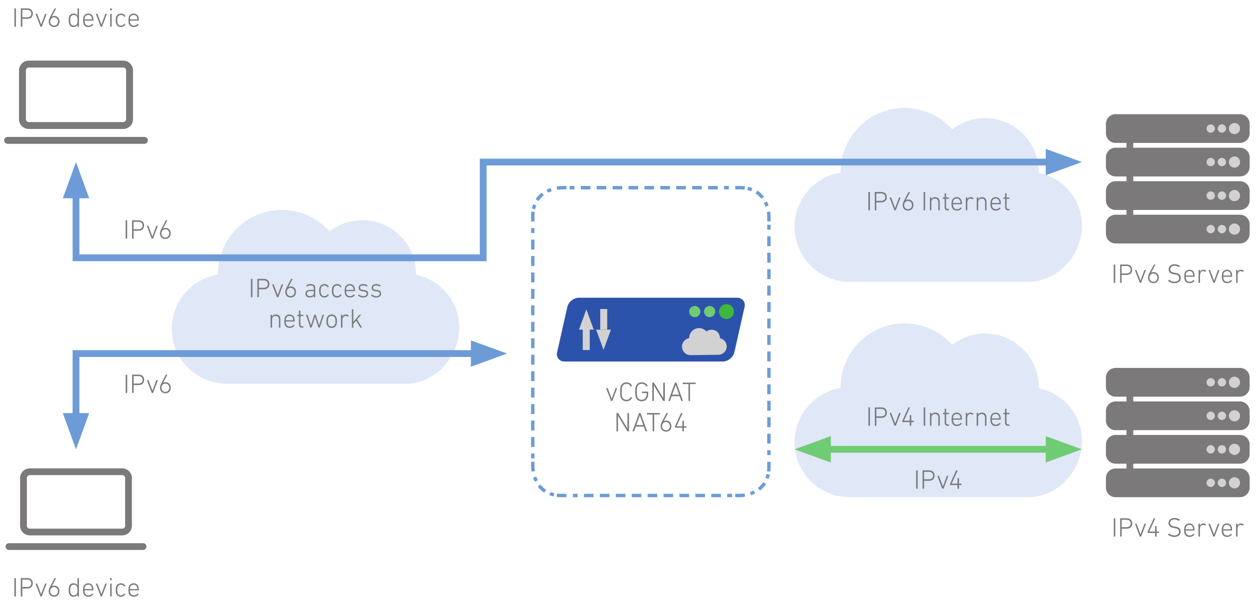
Typical use-case. A Service Provider, who must somehow continue to assign addresses to large numbers of new customers when there are no new IPv4 addresses to use. Assigning IPv6 addresses is ofen not possible because many customers are still running operating systems or end-points that have some shortcomings in their IPv6 support.



NAT64

NAT64 is the vCGNAT operational mode for mapping a customer IPv6 address to the public IPv4 address with one of its TCP or UDP ports. Because many services accessible on the public Internet are still IPv4 only, NAT64 is needed to allow customers who use IPv6-only devices to transparently access IPv4 services.

Typical use-case. A Service Provider or Enterprise, who supports customers with IPv6-only devices, needs to provide access to both IPv6- and IPv4- only services.



Key Benefits of NFWare vCGNAT

Ultimate performance and scalability to optimize network performance

NFWare vCGNAT is able to scale to hundreds of gigabits to ensure optimal performance during IPv6 migration. vCGNAT can process up to 370 Gbps on a single server.
This capacity helps to reduce costs as it is possible to handle the high volume of traffic with fewer servers in the network.

On-demand Pay-as-you-go licensing

NFWare ofers throughput-based and subscriber-based pay-as-you-go license model, where license cost depends only on actual needs and can be gradually scaled. This allows operators to keep the cost of the network under control and facilitates exponential trafc growth.

Works on top of COTS hardwarev

CGNAT is purpose-built to be deployed on standard x86 servers and designed for virtualized and cloud environments. The sofware can run on servers with a variety of standard processors and network controllers, so it can be deployed in diferent parts of a network.

Flexible integration into Virtualized Environment

Due to NFWare's design principles of openness and fexibility, the integration with any VNF Manager and NFV Orchestration is always smooth and completed within a short time frame.

Product's Features

Application Layer Gateways functionality allows vCGNAT to transparently translate IP addresses and ports in messages for protocols like FTP, TFTP, PPTP, SIP, RTSP, and DNS.

Mapping features. When an internal endpoint opens an outgoing session through a vCGNAT, vCGNAT creates a mapping between an internal IP address and port and external IP:port tuple. Mapping type defnes for which subsequent outgoing sessions from the same internal IP:port vCGNAT shall use the same mapping for translation. vCGNAT supports Endpoint-Independent mapping.

Filtering features. When a mapping is created, fltering type defnes which external endpoints can reach internal endpoints using this mapping. vCGNAT supports several types of fltering: Endpoint-Independent Filtering (EIF), Address-Dependent Filtering, and Address and Port-Dependent Filtering.

NAT Bindings Logging vCGNAT supports logging to external servers to store session details such as private to public IP address translation, port numbers, and several others. It supports various protocols such as Syslog, RADIUS, IPFIX and Netfow. In addition, vCGNAT is able to send logs to multiple syslog servers, even if it requires two types of protocols to be used simultaneously.

Deterministic NAT mode allows to eliminate the need for logging, as in this mode the subscriber's IP address is always mapped to the same external IP and port range.

Port Block Allocation (PBA) mode decreases the amount of necessary logging. For private IP addresses, vCGNAT pre-allocates a set of ports so that logging of only two records will be required - when the port set is created and when it is released.

Paired Pooling Mode allows a private IP address to be mapped to the same public IP address from a vCGNAT pool for all its sessions. The frst packet seen from a private host triggers the binding between private IP and public IP.

Hairpinning allows two endpoints on the internal side of the vCGNAT to communicate even if they only use each other's external IP addresses and ports.

Port Control Protocol (PCP) allows clients to request the creation of mappings ("open ports" reachable from the outside), create or control the lifetime of sessions through NAT to reduce the number of keep-alives, or restore lost state afer NAT restart.

Link Aggregation Control Protocol (LACP) allows the bundling of several physical ports to form a single logical channel. When the number of active bundled ports on a port channel is changing, trafc patterns refect the rebalanced state of the port channel.

VLAN support in vCGNAT increases the efciency of network interface controllers usage. It enables diferentiation of inbound and outbound trafc, not by NIC but by VLAN ID, creating the ability to use the same NIC for both inbound and outbound trafc. This feature is most efective when used alongside the LACP feature.

Scalability vCGNAT is designed with an NFV-approach and provides granular elastic, scalability on commodity hardware.

Packet tracing allows detailed debugging and analysis of processes occurring on vCGNAT and user traffic packets arriving at interfaces.

AAA vCGNAT uses the AAA subsystem, which stands for Authentication, Authorization, and Accounting. This subsystem is used when it is necessary to provide user identification, determine what commands the user is authorized to execute, and track all user actions. It includes the ability to create local users with different roles (guest, operator, administrator), as well as the ability to use the TACACS+ and RADIUS protocols

High Availability (HA) improves the reliability of the service. vCGNAT works in an Active/ Standby and Active/Active N+1 modes. In both options, there are at least two CGNAT instances: if an active one becomes inoperable, another instance of vCGNAT takes control and traffic goes through it.

Detailed Feature List

Modes

- NAT44
- NAT64

Routing

- VRF
- Static routing
- BGP
- BFD
- OSPF
- IS-IS
- RIP

Application Layer Gateways

- FTP
- DNS
- PPTP
- IPSec
- SIP
- RTSP
- TFTP

Mapping and Filtering

- EIM/EIF
- Address Dependent Filtering
- Address and Port Dependent Filtering

Logging

- Syslog
- RADIUS
- Netflow
- IPFIX
- Subscriber information collected from received RADIUS messages
- Customizable syslog format

Advanced Logging Features

- Deterministic NAT
- Ability to send logs to multiple syslog servers
- Port Block Allocation (PBA)

Other NAT Features

- Hairpinning
- Paired Pooling
- Port Control Protocol (PCP)
- Access Control Lists (ACL)

Interface management

- Link Aggregation Control Protocol (LACP)
- VLAN support

OAM

- CLI
- SNMP
- Performance monitoring and statistics
- Syslog
- Packet tracer

AAA

- TACACS+
- Radius

High Availability (HA)

- Active-Standby
- Active-Active N+1
- VRRP version 3 IPv4/IPv6
- Real Time Management (RTM) subsystem
- Sessions' synchronization

Cloud

- OpenStack integration
- MANO compliant
- ETSI compliant

Hypervisor Compatibility

- KVM

Hardware Requirements

Required CPU: any Intel Xeon processors starting from the Haswell (v3) family

Supported NICs: Intel X520, Intel X710, Intel E810, Mellanox ConnectX-5, Mellanox ConnectX-6

Examples of Hardware Configuration

Max throughput	CPU model	NICs	# of v-cores per CPU (hyper-threading enabled)
3 Gbps	1 x Intel Xeon Bronze 3106	1 x 10 GbE Intel X520/X710	4
10 Gbps	1 x Intel Xeon Silver 4110	1 x 10 GbE Intel X520/X710	4
20 Gbps	1 x Intel Xeon Silver 4110	2 x 10 GbE Intel X520/X710	8
40 Gbps	1 x Intel Xeon Silver 4110	1 x 40 GbE Intel XL710	14
80 Gbps	1 x Intel Xeon Gold 6230	1 x 100 GbE ConnectX-6	20
100 Gbps	1 x Intel Xeon Gold 6230	1 x 100 GbE ConnectX-6	26
150 Gbps	1 x Intel Xeon Gold 6230	2 x 100 GbE ConnectX-6	38
180 Gbps	1 x Intel Xeon Platinum 8360Y	2 x 100 GbE ConnectX-6	30
280 Gbps	2 x Intel Xeon Platinum 8360Y	4 x 100 GbE ConnectX-6	22 + 22
330 Gbps	2 x Intel Xeon Platinum 8360Y	4 x 100 GbE ConnectX-6	26 + 26
440 Gbps	2 x Intel Xeon Platinum 8360Y	4 x 100 GbE ConnectX-6	66 + 66

Memory Requirements

Concurrent Sessions	Memory (1xCPU)	Memory (2xCPU)
10M	23 GB	37 GB
50M	77 GB	91 GB
100M	144 GB	158 GB
200M	270 GB	284 GB
300M	358 GB	371 GB

About NFWare

NFWare, Inc. is an innovative network software vendor which supplies Service Providers, Operators and Data Centers with super-fast virtualized IP routing solutions for their networks. NFWare software-based NFV technology provides a level of performance and reliability which was historically associated only with dedicated proprietary hardware. NFWare was established in 2014 by experienced professionals in telecommunications, computer networking and virtualization technologies. For more information, visit www.nfware.com

Contact Information

1990 North California Boulevard, Suite 800
Walnut Creek, CA 94596
Unites States

sales@nfware.com

www.nfware.com