Содержание

Description and use cases 3
Types 3
Use cases 3
L3-Connected NAT 3
L2-Connected NAT 4
Implementation options 4
CG-NAT Benefits 7

Description and use cases

Carrier Grade Network Address Translation allows you:

1. to share one public IPv4 address between several subscribers without losing the quality of Internet connection – you can assign up to 100 private IP addresses for one public IP address (the ideal ratio is 1:10);
2. to extend the use of limited IPv4 address space and reduce the cost of buying IPv4 addresses by 90%;
3. to prepare the network for IPv6 addressing with Dual Stack v4-v6 (support both versions of the protocol simultaneously).

When using NAT, keep in mind that in this case NAT is a service provided by DPI, which is not a router and operates in **transparent bridging mode**. Consider this when implementing and configuring your equipment.

Types

CG-NAT (NAT44)

Network address and port translation allows multiple subscribers to share a single IPv4 public address and expands the use of a limited IPv4 address space.

BiNAT (NAT 1:1)

1-to-1 network address translation allows you to provide a static public IP address service without changing the settings on the CPE through the translation of all ports of the private address into one public address.

Use cases

L3-Connected NAT

In the Bridge mode (relevant for L3 BRAS) Stingray SG does not have an IP address on the interfaces for processing subscriber traffic. Based on this, it is necessary to add a static route on the border for the subnets used in NAT, in which the address of the next router will be the address located behind the SSG.

Implementation Example

The network has a router R1, which is a gateway for local subscribers with addresses 10.0.0.0/24, and a border router - BR, which has a connection with R1 on the 10.0.1.0/30 subnet. DPI is set between

them, which enables the NAT service for the subscribers. For the NAT pool, select the subnet 100.0.0.0/24

On R1, our border is the gateway. In order to ensure the passage of traffic from the Internet to subscribers, it is necessary to add a route on the border: ip route add 100.0.0.0/24 via 10.0.1.2 After that, the traffic for the NAT pool will be routed from BR to R1, on the way to which it will be NATed when it gets to DPI. Traffic to addresses without NAT translation will be dropped on DPI.

L2-Connected NAT

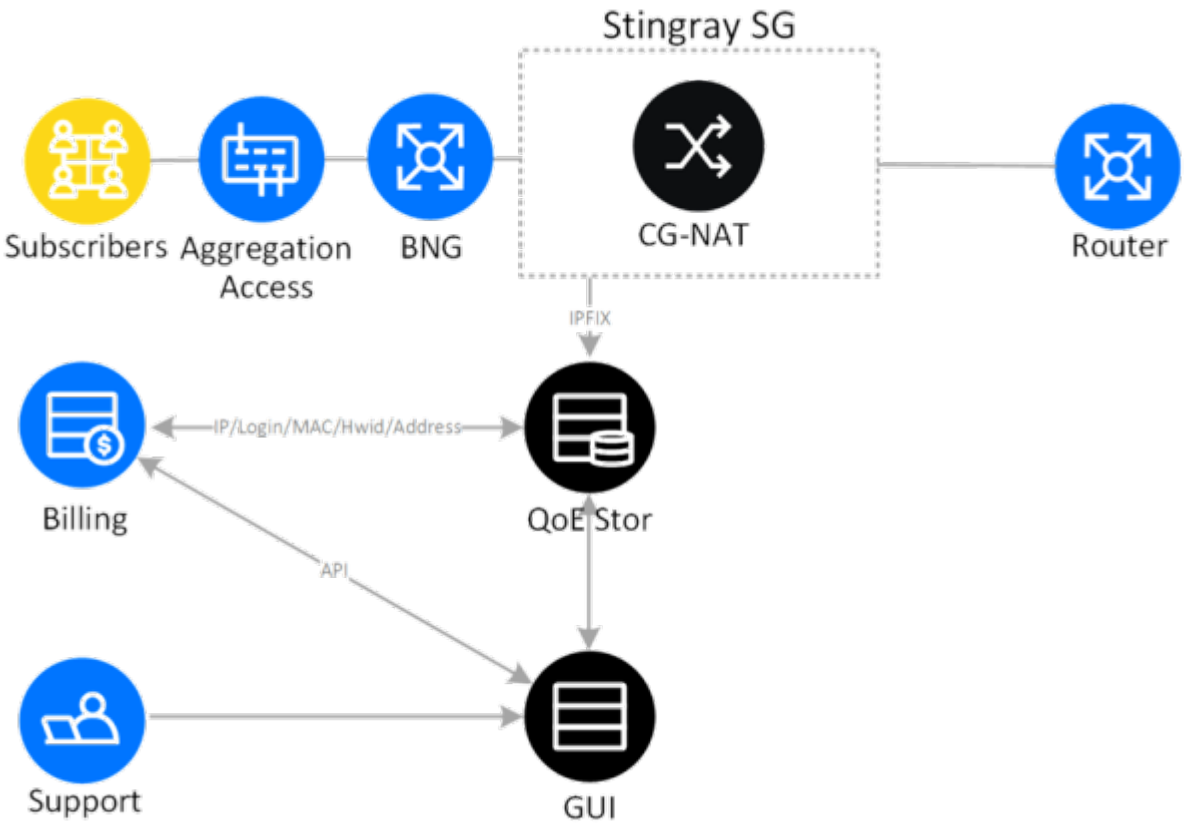
In L2 BRAS mode, the address specified in the bras_arp_ip parameter should be used as the next hop in the route. This route allows you to route traffic for addresses from the NAT pool towards DPI, where the recipient address will be changed in packets from public to private according to the translation table, and the packet will reach the next router in the network with a private recipient. Further routing in the network will be no different.

Implementation Example

In this scheme, the gateway for subscribers is the DPI. IP address 10.10.10.1 is configured on DPI, IP address 10.10.10.2 is configured on the Border Router. Let us allocate subnet 100.0.0.0/24 for NAT pool. To pass traffic from the Internet to subscribers you need to add a route on the Border Router: ip route add 100.0.0.0/24 via 10.10.10.1.

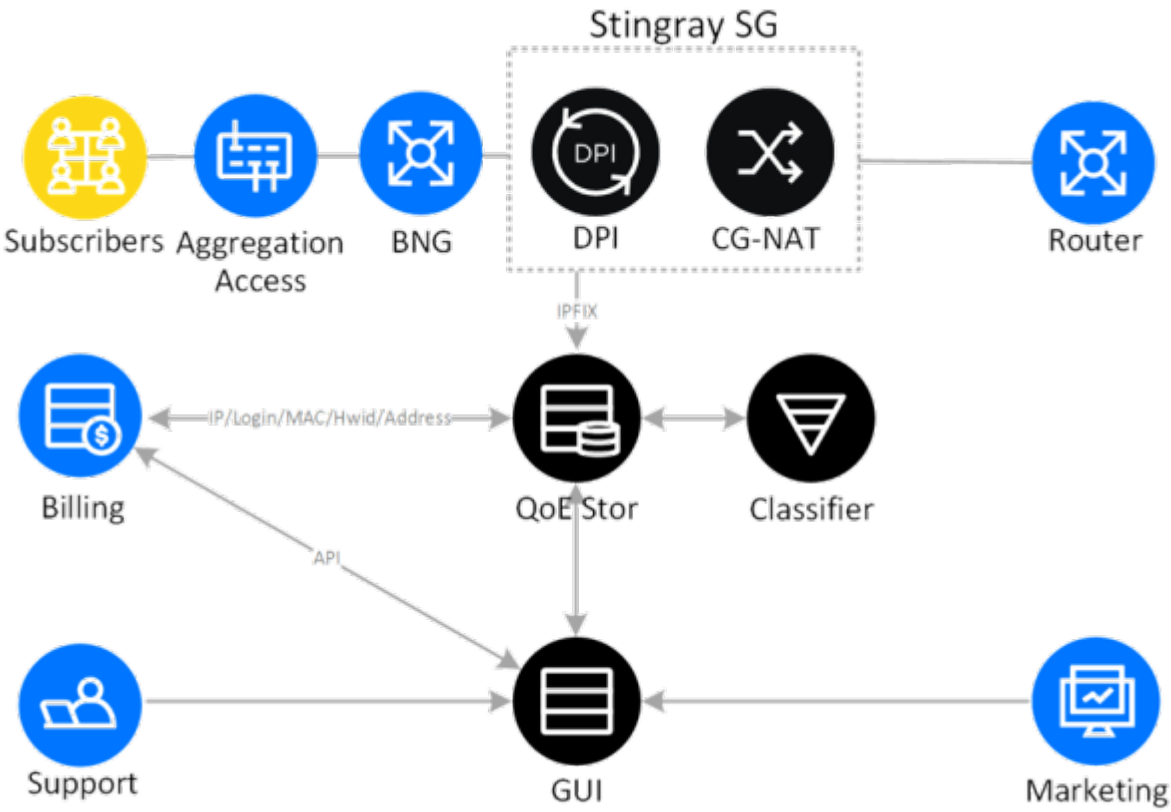
Implementation options

CG-NAT



This is a classic scheme of including a CG-NAT device in the network – between the BNG and the router to provide network address translation. NAT log is transferred via IPFIX protocol (NetFlow v10) to a dedicated server or VM, where the database of this QoE Stor and GUI is installed. This solution allows efficient storage and searching of NAT logs.

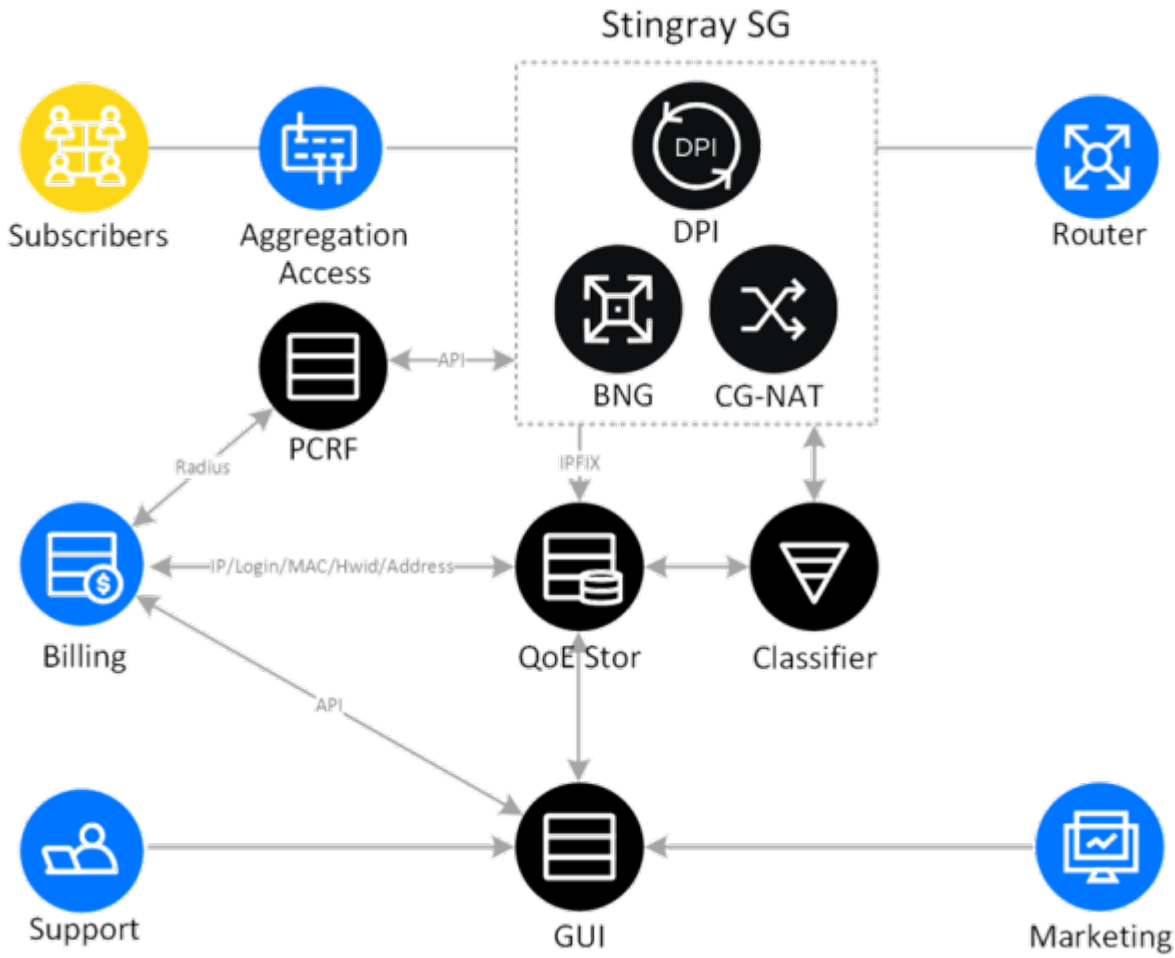
CG-NAT + DPI



We offer to combine CG-NAT functionality with DPI on one device, not only to broadcast addresses, but also to detect and classify traffic by protocols and directions, to use common channel policing, to mark traffic, to work with statistics (Full NetFlow and Clickstream).

Additional subscriber information might be used in sales, marketing and technical support departments.

CG-NAT + DPI + BNG



The best option is to combine CG-NAT, DPI and BNG functionality on a single device. In this way to build a flexible and easily manageable core network – this significantly reduces the TCO (Total Cost of Ownership) through compactness, high performance, uniform management and operation.

In this scheme, in addition to network address translation and deep traffic analysis, IPoE/PPPoE subscriber authorization, BGP/OSPF are also implemented; integration with billing (AAA) is done via PCRF.

CG-NAT Benefits

Full Cone NAT

The CG-NAT function uses Full Cone NAT technology, which allows sending packets coming from any external system via an external displayed TCP/UDP port, which is a source of traffic from the subscriber.

Hairpinning

Subscribers inside the NAT access each other’s public addresses without translating and forwarding packets outside the device.

Limits on TCP and UDP connections for a subscriber

A limit of the number of TCP and UDP connections per subscriber is set individually for each IP address pool, which allows the operator to sparingly allocate address space resources between corporate and private clients. In the absence of activity, unused connections are closed, freeing up ports.

Paired IP address pooling function

All subscriber connections from one IP-private internal address are bound to one external address.

Translation logging

Network translations are recorded in a text file or transmitted to an external collector via the IPFIX protocol (also known as NetFlow v10).

Transparency for P2P and online gaming

Predictable NAT behavior is provided by the Full Cone and HairPinning functions. User quotas ensure an even distribution of public IP ports between subscribers, and viruses and malware cannot deplete their resources.

ALG support

It is important for operators to maintain connectivity for all application services and users while ensuring application integrity. ALG ensures that protocols — such as FTP, TFTP, RTSP, PPTP, SIP, ICMP, H.323, ESP, MGCP and DNS — remain operational. Many legacy NAT implementations do not provide this level of transparency.

VLAN and On-Stick support

In CG-NAT, VLAN support saves ports in the operator’s equipment and increases the efficiency of using NIC. This makes it possible to determine downstream and upstream traffic not by NIC, but by VLAN ID, which in turn makes it possible to use the same network interface card for both downstream and upstream traffic. This option is especially effective when used together with LACP.

LACP

Link Aggregation Control Protocol allows you to combine several physical ports to form a single logical channel and increase fault tolerance.

Availability

The reliability of the solution is guaranteed by using the standby modes Active-Standby and Active-Active. In both variants, two devices are involved: if the first one (active) fails, then traffic is switched to the second one without loss using routing protocols.