Table of Contents

CGNAT. Network Address Translation for IPv4

Why NAT is used in practice:

NAT technology helps conserve IPv4 address space and reduces the likelihood of devices in the operator's network being hacked. On the SSG, two modes can be configured:

- CGNAT — Network Address and Port Translation allows multiple subscribers to share a single public IPv4 address, extending the usage of the limited IPv4 address space.
- NAT 1:1 — One-to-one Network Address Translation assigns a public IP address to a subscriber with a private IP without changing the settings on their equipment or the terminating router.

Let’s test this:
Test 1. Configuring CGNAT and NAT 1:1 via CLI
Test 2. Configuring CGNAT and NAT 1:1 via GUI
Test 3. Configuring NAT log export to external collector and locally to file

Test conditions:

1. Installing SSG “in-line”
2. A PC with internet connected via the SSG.
3. The SSG is located between two L2 or L3 devices of the provider

Let’s start testing. The actions can be performed both via the graphical interface of the SSG and through the CLI. The choice of method is up to the client; both methods are presented in the instructions.

Test 1. Configuring CGNAT and NAT 1:1 via CLI

- Creating a NAT service
- Assigning the NAT service to a subscriber
- Creating a reverse route
- Checking traffic flow
- Displaying translation information

1. Creating a NAT service (CLI)

Enter the command in the command line:

CGNAT:

```
fdpi_ctrl load profile --service 11  --profile.name cg_nat --profile.json '{
"nat_ip_pool" : "10.10.10.0/24", "nat_tcp_max_sessions" : 2000,
"nat_udp_max_sessions" : 2000 }'
```

NAT 1:1:

```
fdpi_ctrl load profile --service 11  --profile.name bi_nat --profile.json '{
"nat_ip_pool" : "10.10.10.0/24", "nat_type": 1 }'
```

Command values:

- `load profile` — creating a profile
- `service 11` — service number on the SSG, for the NAT service it is 11
- `profile.name` — name of the created profile, `cg_nat` and `bi_nat`
- `profile.json '{ "nat_ip_pool" : "10.10.10.0/26", "nat_tcp_max_sessions" : 2000, "nat_udp_max_sessions" : 2000 }'` — profile settings in JSON format:
  - `nat_ip_pool` — NAT pool subnets separated by commas. If the extreme addresses need to be excluded, you can add `~ (10.10.10.0/24~)` at the end, so the pool will contain addresses from `10.10.10.1` to `10.10.10.254`.
  - `nat_tcp_max_sessions` — maximum number of TCP sessions per subscriber.
  - `nat_udp_max_sessions` — maximum number of UDP translations per subscriber.
  - `nat_type` — NAT operation mode. 0 — for CGNAT, 1 — for NAT 1:1. The default is 0, so this field is not specified for CGNAT.

2. Assigning the NAT service to a subscriber (CLI)

CGNAT

Assigning the NAT service to a subscriber is possible by IP or CIDR.

Example of assigning the service by IP:

```
fdpi_ctrl load --service 11 --profile.name cg_nat --ip 100.64.0.1
```

Example of assigning the service to the entire CIDR:

```
fdpi_ctrl load --service 11 --profile.name cg_nat --cidr 100.64.0.0/24
```

NAT 1:1

Example of assigning the service by IP:

```
fdpi_ctrl load --service 11 --profile.name bi_nat --ip 100.64.0.1
```

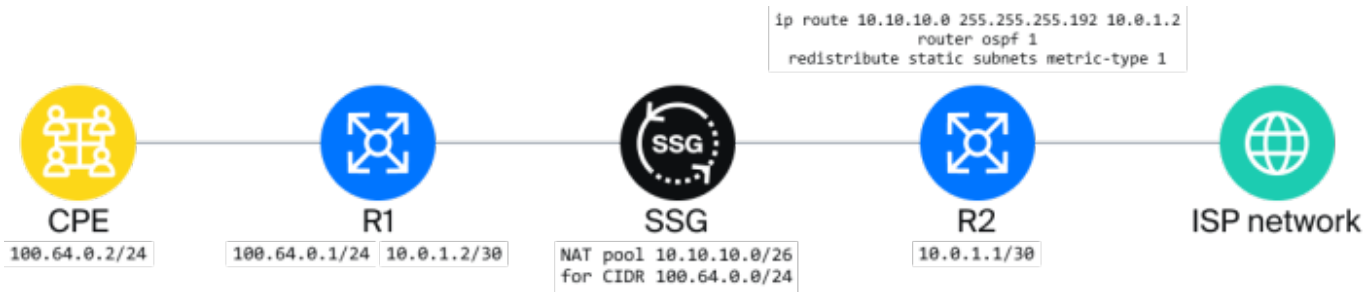
Example of assigning the service to the entire CIDR:

```
fdpi_ctrl load --service 11 --profile.name bi_nat --cidr 100.64.0.0/24
```

These commands are enough to configure NAT on the SSG. The SSG by default operates in bridge mode, meaning it creates NAT translations and forwards traffic in both directions but does not participate in routing.

3. Creating a reverse route (CLI)

To route reverse traffic to the NAT pool towards the subscribers, it will be necessary to create a route to the NAT pool on the router after the SSG and make this route known to the other routers in the network.
Consider a situation where a point-to-point network 10.0.1.0/30 is configured between the routers with the SSG, the router's interface on the subscriber side (R1) has the IP 10.0.1.2, and the router's interface after the SSG (R2) has the IP 10.0.1.1 (see the diagram).



On router R2, it will be necessary to configure the route to the NAT pool. For Cisco-like CLI, the configuration will look like this:

```
conf t
ip route 10.10.10.0 255.255.255.192 10.0.1.2
```

It will also be necessary to configure the redistribution of static routes so that the route is known not only to R2 but also to the rest of the network. If OSPF is used:

```
router ospf 1
redistribute static subnets metric-type 1
```

Where 1 in `router ospf 1` is the OSPF process number on the router.

4. Checking traffic flow and interface orientation (CLI)

From the test PC, check the application of NAT:

- Check the availability of router R2.
- Run the command `ping 10.0.1.2`. If R2 is unavailable, check the orientation of the SSG

interfaces.

The In interface connects the subscribers, the Out interface connects to the internet.
Determine which interface is which by setting the port connected to the SSG to down on R1 and outputting the status of interfaces on the SSG.

```
fdpi_cli dev xstat|grep --no-group-separator -B1 "Link status"|paste - -
|sort
Device 02:00.0: Link status: link down
Device 02:00.1: Link status: link up
```

Check the configuration in fastdpi.conf
If necessary, change the direction and restart the service with the command

```
service fastdpi restart
```

5. Displaying translation information (CLI)

For each IP, it is possible to display the current state of the NAT service.

View the number of active sessions and the assigned public address for a specific private address using `fdpi_ctrl`:

```
fdpi_ctrl list status --service 11 --ip 192.168.4.20
```

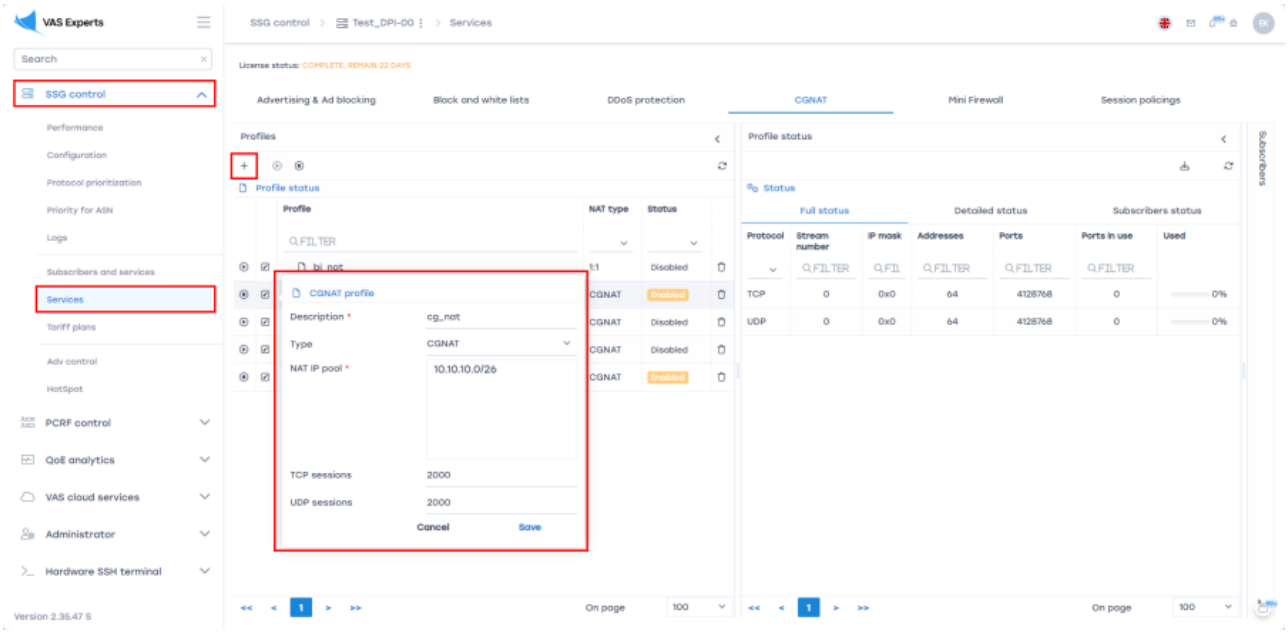
Result:
Private subscriber IP addresses are translated into Public IP addresses.

Test 2. Configuring CGNAT and NAT 1:1 via GUI

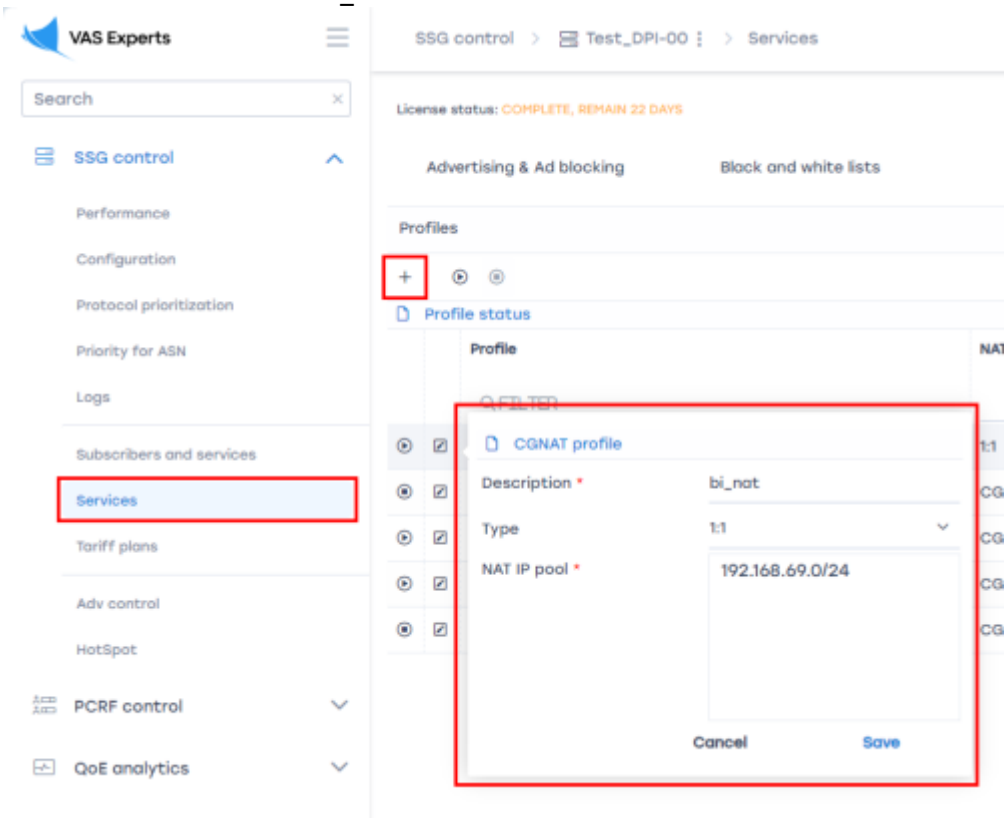
- Creating a NAT service
- Assigning the NAT service to a subscriber
- Creating a reverse route
- Checking traffic flow
- Displaying translation information

1. Creating a NAT service (GUI)

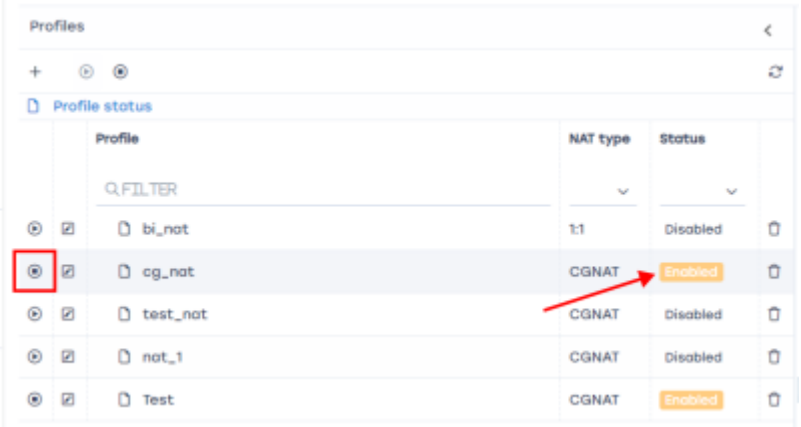
1. Open the DPI/Services section. CGNAT tab. Create a Profile named cg_nat.



2. Create a Profile named bi_nat.

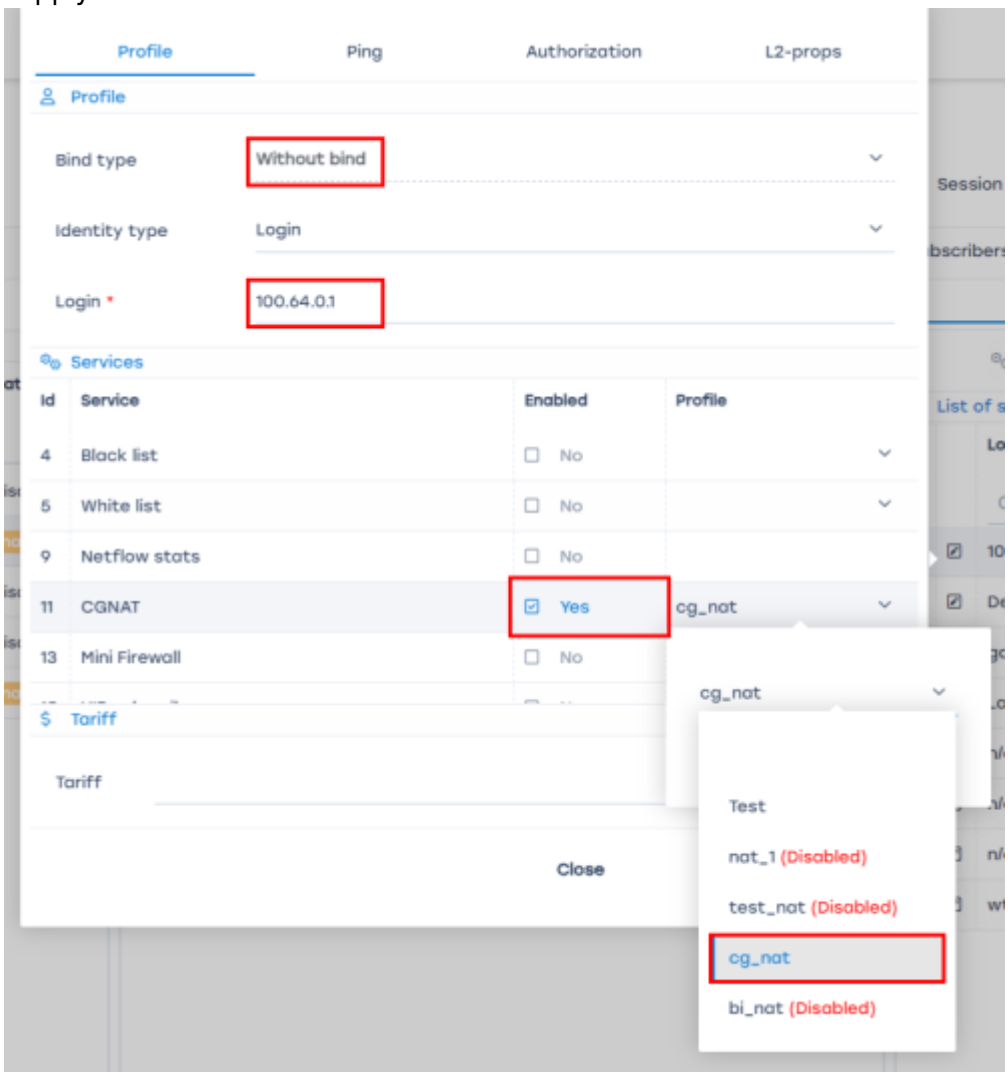


3. Then activate the service on the SSG by clicking the Play button. The status will change to "enabled".



2. Assigning the NAT service to a subscriber (GUI)

In the same section “DPI/Services”, CGNAT tab.
In the right column "Subscribers", add a subscriber, select the "Unbound" type, enter the subscriber’s IP, select service 11 “CGNAT” or “NAT 1:1”, check the box "Yes" to enable, select the profile, click "Apply" and "Save".



3. Creating a reverse route (GUI)

To route reverse traffic to the NAT pool towards the subscribers, it will be necessary to create a route to the NAT pool on the router after the SSG and make this route known to the other routers in the network. The process is the same as in Test 1. The steps and commands do not change.

4. Checking traffic flow and interface orientation (GUI)

In the GUI, navigate to DPI > Statistics > NAT Statistics

Check the orientation of the SSG interfaces as shown in Test 1.

5. Displaying translation information (GUI)

In the GUI, navigate to DPI > Statistics > NAT Statistics
Check the number of active sessions and the assigned public address for each private address.

Test 3. Configuring NAT log export to external collector and locally to file

1. Exporting NAT log to external collector

```
fdpi_ctrl log set nat --export-collector-ip 10.10.10.2 --export-collector-port 514
```

To export logs, specify the IP address and port of the external collector.

2. Exporting NAT log locally

```
fdpi_ctrl log set nat --export-local-file /var/log/nat.log
```

To export logs locally, specify the desired file path.

Additional information on NAT log management: You can use the SSG's built-in options to filter, search, and manage the NAT logs. You can also configure automatic log rotation and archiving.