

# Содержание

|                                                                |   |
|----------------------------------------------------------------|---|
| <b>CGNAT. Трансляция сетевых адресов для IPv4</b>              | 3 |
| <b>Тест 1. Настройка CGNAT и NAT 1:1 через CLI</b>             | 3 |
| 1. Создание услуги NAT (CLI)                                   | 4 |
| 2. Назначение услуги NAT на абонента (CLI)                     | 4 |
| 3. Создание обратного маршрута (CLI)                           | 5 |
| 4. Проверка прохождения трафика и ориентации интерфейсов (CLI) | 5 |
| 5. Вывод информации о трансляциях (CLI)                        | 6 |
| <b>Тест 2. Настройка CGNAT и NAT 1:1 через GUI</b>             | 6 |
| 1. Создание услуги NAT (GUI)                                   | 6 |
| 2. Назначение услуги NAT на абонента (GUI)                     | 8 |
| 3. Создание обратного маршрута (GUI)                           | 8 |
| 4. Проверка прохождения трафика и ориентации интерфейсов (CLI) | 9 |



# CGNAT. Трансляция сетевых адресов для IPv4

**Зачем NAT применяется на практике:** Технология NAT позволяет экономить адресное пространство IPv4 и снижает вероятность взлома устройств, находящихся в сети оператора связи. На СКАТ доступна настройка двух режимов:

- CGNAT — Трансляция сетевых адресов и портов позволяет совместно использовать публичный IPv4 адрес несколькими абонентами и продлевает использование ограниченного адресного пространства IPv4.
- NAT 1:1 — Трансляция сетевого адреса 1v1 позволяет назначить абоненту с приватным IP публичный IP адрес без изменения настроек на его оборудовании и на маршрутизаторе, где он терминируется.

## Проверим на тестах:

Тест 1. Настройка CGNAT и NAT 1:1 через CLI

Тест 2. Настройка CGNAT и NAT 1:1 через GUI

Тест 3. Настройка выгрузки NAT log на внешний коллектор и локально в файл

### Условия тестов:



1. Установка СКАТ “в разрыв”
2. ПК с интернетом, подключенном через СКАТ.
3. СКАТ расположен между двумя L2- или L3-устройствами провайдера



Приступаем к тестированию. Действия могут выполняться как в графическом интерфейсе СКАТ, так и через CLI. Выбор способа за клиентом, в инструкции представлены оба способа

## Тест 1. Настройка CGNAT и NAT 1:1 через CLI



- Создание услуги NAT
- Назначение услуги NAT на абонента
- Создание обратного маршрута
- Проверка прохождения трафика
- Вывод информации о трансляциях

## 1. Создание услуги NAT (CLI)

Вводим команду в командной строке:  
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 }'
```

Значения в команде:

- `load profile` — создание профиля
- `service 11` — номер услуги на СКАТ, для услуги NAT это 11
- `profile.name` — название создаваемого профиля, `cg_nat` и `bi_nat`
- `profile.json '{ "nat_ip_pool" : "10.10.10.0/26", "nat_tcp_max_sessions" : 2000, "nat_udp_max_sessions" : 2000 }'` — настройки профиля в формате json:
  - `nat_ip_pool` — подсети NAT-пула через запятую. Если требуется исключить крайние адреса, можно добавить в конец `~ (10.10.10.0/24~)`, тогда в пуле будут адреса с 10.10.10.1 по 10.10.10.254.
  - `nat_tcp_max_sessions` — максимальное количество tcp сессий на одного абонента.
  - `nat_udp_max_sessions` — максимальное количество udp трансляций на одного абонента.
  - `nat_type` — режим работы NAT. 0 — для CGNAT, 1 — для NAT 1:1. По умолчанию 0, поэтому данное поле для CGNAT не указано.

## 2. Назначение услуги NAT на абонента (CLI)

### CGNAT

Назначение услуги NAT на абонента возможно по IP или CIDR

Пример команды подключения услуги по IP:

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

Пример подключения услуги на весь CIDR:

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

### NAT 1:1

Пример команды подключения услуги по IP:

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

Пример подключения услуги на весь CIDR:

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

Этих команд достаточно для настройки NAT на СКАТ. При этом СКАТ по умолчанию работает в режиме прозрачного моста, то есть создает NAT трансляции и направляет трафик в обе стороны, но не участвует в маршрутизации.

### 3. Создание обратного маршрута (CLI)

Чтобы обратный трафик в сторону NAT пула был смаршрутизирован к абонентам, потребуется создать маршрут к NAT-пулу на следующем за СКАТ маршрутизаторе и сделать этот маршрут известным остальным маршрутизаторам сети.

Рассмотрим ситуацию, когда на маршрутизаторах, между которыми стоит СКАТ, настроена стыковочная сеть 10.0.1.0/30, IP на интерфейсе маршрутизатора со стороны абонентов (R1) - 10.0.1.2, IP на интерфейсе маршрутизатора после СКАТ (R2) - 10.0.1.1 (см. схему).



На маршрутизаторе R2 потребуется настроить маршрут к NAT-пулу. Для cisco-like CLI настройка будет выглядеть так:

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

Также потребуется настроить редистрибуцию статических маршрутов, чтобы об этом маршруте было известно не только R2, но и в остальной сети оператора. В случае, если используется ospf:

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

Где 1 в `router ospf 1` — номер процесса OSPF на маршрутизаторе.

### 4. Проверка прохождения трафика и ориентации интерфейсов (CLI)

С тестового ПК провести проверку применения NAT:

- Проверить доступность роутера R2.
- Выполнить команду `ping 10.0.1.2`. Если R2 недоступен, то необходимо проверить ориентацию интерфейсов СКАТ.

В In интерфейс подключены абоненты, в Out интерфейс подключен интернет.

Определить где какой интерфейс возможно путем перевода порта, подключенного к СКАТ, в состояние down на R1 и вывести статус интерфейсов на СКАТ.

```
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
```

Проверить соответствие в `fastdpi.conf`

При необходимости изменить направление и сделать рестарт сервиса через команду

```
service fastdpi restart
```

## 5. Вывод информации о трансляциях (CLI)

По каждому IP возможно сделать вывод текущего состояния услуги NAT.

Просмотр через `fdpi_ctrl` количества активных сессий и назначенного белого адреса для конкретного серого адреса:

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

### Результат:

Абонентские приватные IP-адреса транслируются в Публичные IP-адреса.

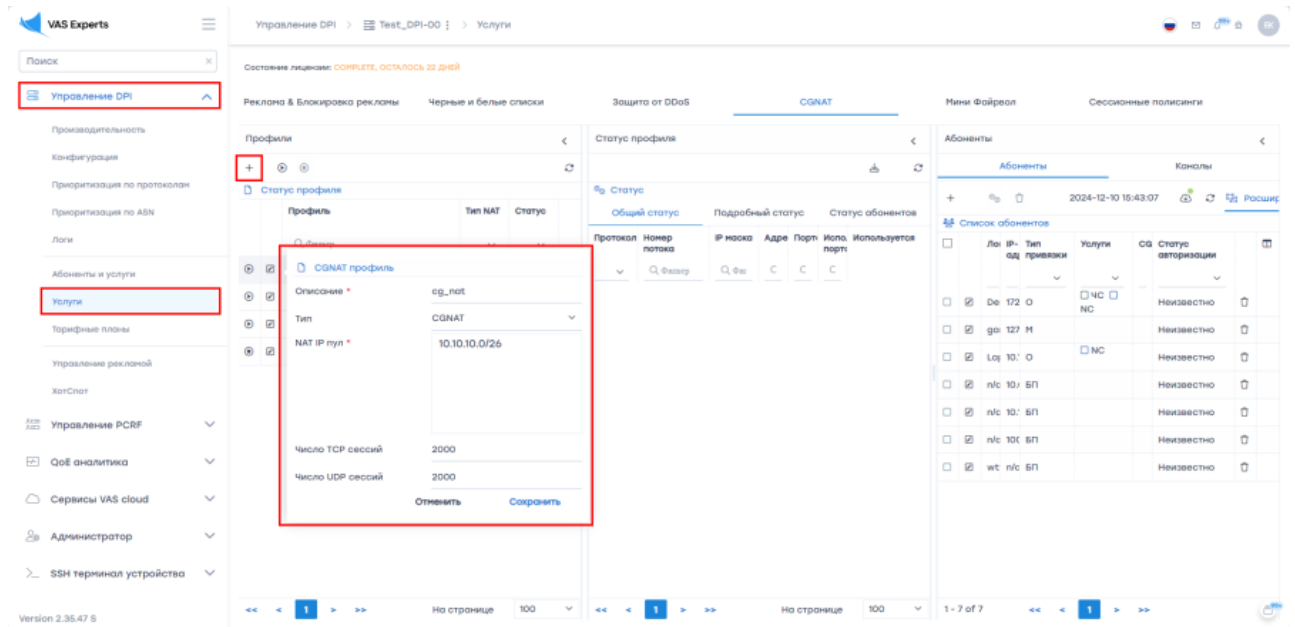
## Тест 2. Настройка CGNAT и NAT 1:1 через GUI



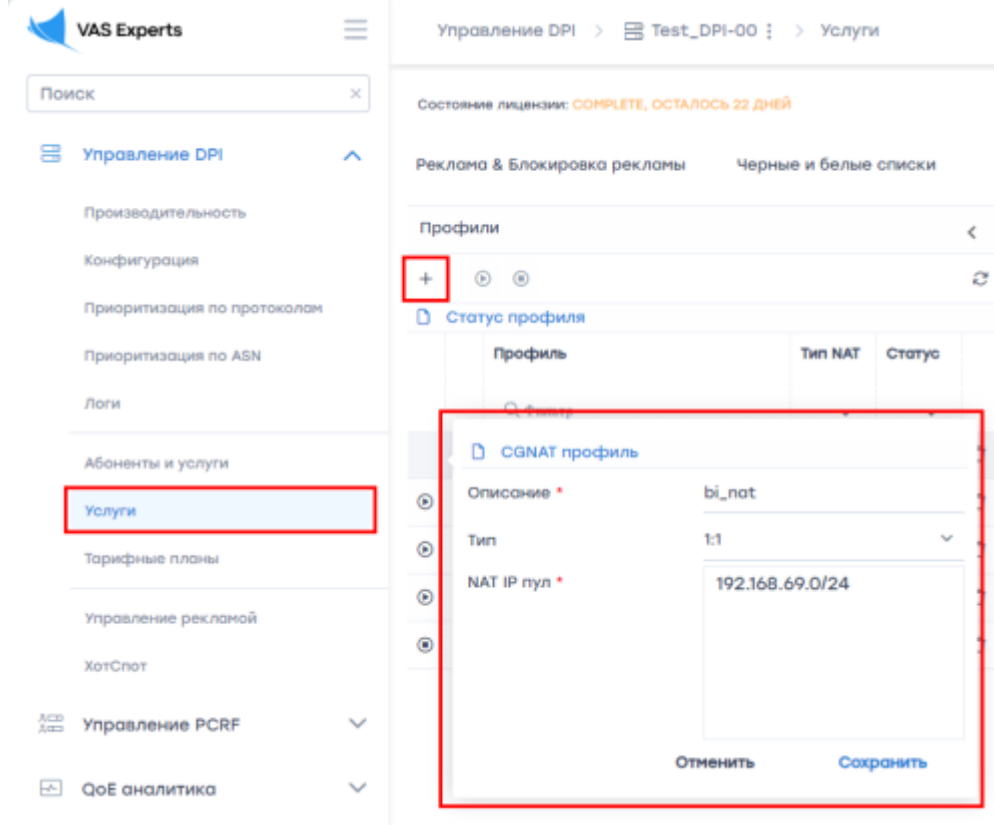
- Создание услуги NAT
- Назначение услуги NAT на абонента
- Создание обратного маршрута
- Проверка прохождения трафика
- Вывод информации о трансляциях

### 1. Создание услуги NAT (GUI)

1. Открываем раздел Управление DPI/Услуги. Вкладка CGNAT. Создаем Профиль с именем `cg_nat`.



2. Создаем Профиль с именем bi\_nat.



3. Затем нужно активировать данную услугу в СКДТ нажатие кнопки Play. Статус поменяется на "включен".

| Профили                          |          |         |          |  |
|----------------------------------|----------|---------|----------|--|
| Статус профиля                   |          |         |          |  |
|                                  | Профиль  | Тип NAT | Статус   |  |
|                                  | Фильтр   |         |          |  |
| <input type="radio"/>            | bi_nat   | 1:1     | Выключен |  |
| <input checked="" type="radio"/> | cg_nat   | CGNAT   | Включен  |  |
| <input type="radio"/>            | test_nat | CGNAT   | Выключен |  |
| <input type="radio"/>            | nat_1    | CGNAT   | Выключен |  |
| <input type="radio"/>            | Test     | CGNAT   | Включен  |  |

## 2. Назначение услуги NAT на абонента (GUI)

В том же разделе “Управление DPI/Услуги”, вкладка CGNAT.

В правой колонке “Абоненты” добавляем абонента, выбираем тип “без привязки”, вводим IP абонента, выбираем 11 услугу “CGNAT” или “NAT 1:1”, указываем галочка “Да” включить, выбираем профиль, нажимаем “Применить” и “Сохранить”.

| Код | Услуга             | Подключена                             | Профиль |
|-----|--------------------|----------------------------------------|---------|
| 4   | Чёрный список      | <input type="checkbox"/> Нет           |         |
| 5   | Белый список       | <input type="checkbox"/> Нет           |         |
| 9   | Netflow статистика | <input type="checkbox"/> Нет           |         |
| 11  | CGNAT              | <input checked="" type="checkbox"/> Да |         |
| 13  | Мени Файрвол       | <input type="checkbox"/> Нет           |         |

Этих команд достаточно для настройки NAT на SKAT. При этом SKAT по умолчанию работает в режиме прозрачного моста, то есть создает NAT трансляции и направляет трафик в обе стороны, но не участвует в маршрутизации.

## 3. Создание обратного маршрута (GUI)

Действия те же, что и в п. 3 настройки через CLI

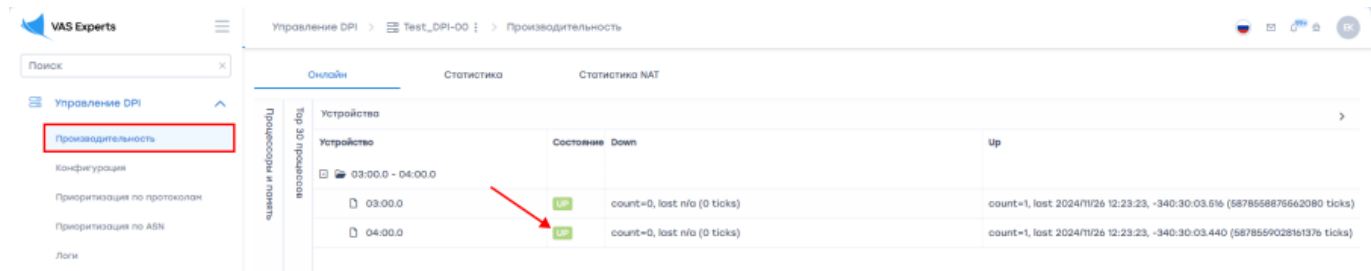
## 4. Проверка прохождения трафика и ориентации интерфейсов (CLI)

С тестового ПК провести проверку применения NAT:

- Проверить доступность роутера R2.
- Выполнить команду `ping 10.0.1.2`. Если R2 недоступен, то необходимо проверить ориентацию интерфейсов SKAT.

В In интерфейс подключены абоненты, в Out интерфейс подключен интернет.

Определить где какой интерфейс возможно путем перевода порта, подключенного к SKAT, в состояние down на R1 и вывести статус интерфейсов на SKAT.

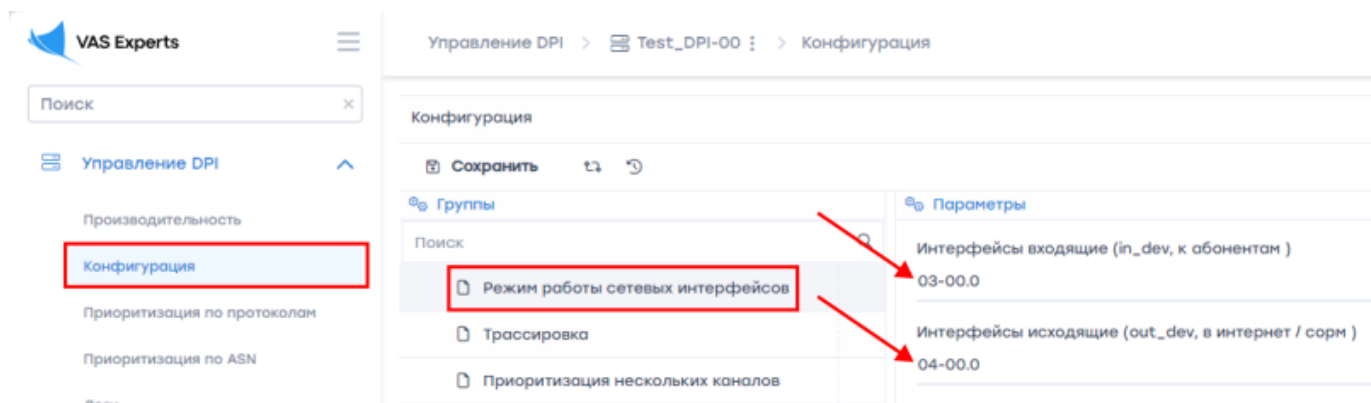


| Устройство | Состояние | Down                        | Up                                                                         |
|------------|-----------|-----------------------------|----------------------------------------------------------------------------|
| 03-00.0    | Up        | count=0, last n/a (0 ticks) | count=1, last 2024/11/26 12:23:23, -340:30:03.516 (587856887662080 ticks)  |
| 04-00.0    | Up        | count=0, last n/a (0 ticks) | count=1, last 2024/11/26 12:23:23, -340:30:03.440 (5878559028161376 ticks) |

Проверить соответствие в `fastdpi.conf`

При необходимости изменить направление и сделать рестарт сервиса через команду

```
service fastdpi restart
```



| Группы                           | Параметры                                          |
|----------------------------------|----------------------------------------------------|
| Режим работы сетевых интерфейсов | Интерфейсы входящие (in_dev, к абонентам )         |
| Трассировка                      | 03-00.0                                            |
| Приоритизация нескольких каналов | Интерфейсы исходящие (out_dev, в интернет / сорм ) |
|                                  | 04-00.0                                            |