

# Table of Contents

<b>Вопросы и ответы</b> .....	3
<b>1 Почему рекомендуется создавать пул не менее чем из 2х или 4х адресов?</b> .....	3
<b>2 Как определить, какой белый адрес из пула получит абонент?</b> .....	3
<b>3 После подключения NAT стали отваливаться неактивные SSH сессии</b> .....	4
<b>4 Сколько "серых" IP можно спрятать за одним "белым" в CG-NAT?</b> .....	5



# Вопросы и ответы

1. Почему рекомендуется создавать пул не менее чем из 2х или 4х адресов?
2. Как определить, какой белый адрес из пула получит абонент?
3. После подключения NAT стали отваливаться неактивные SSH сессии
4. Сколько "серых" IP можно спрятать за одним "белым" в CGNAT?
5. Как поменять параметры уже существующего и используемого пула?
6. Как выдать конкретный адрес абоненту с NAT 1:1?
7. Диагностика NAT
8. Как найти абонента за NAT? Работа с abuse letters

## 1 Почему рекомендуется создавать пул не менее чем из 2х или 4х адресов?

Неблокирующий алгоритм диспетчеризации в DPI, распределяющий сессии по рабочим потокам, накладывает ограничение на то, какой белый IP адрес может быть назначен абоненту из пула:

- Чтобы гарантированно абонент получил свой белый адрес, необходимо чтобы в пуле было не меньше адресов, чем рабочих потоков (в типовой конфигурации это 2 для SKAT-6 и 4 для SKAT-10 и выше).

Узнать число рабочих потоков можно командой

```
expr $(ps -p `pidof fastdpi` H -o comm|grep wrk|wc -l) / $(ps -p `pidof fastdpi` H -o comm|grep rx|wc -l)
```

- Если в пуле всего один адрес, то не всем абонентам он может быть назначен, а только тем, которые попадут под алгоритм балансировки

## 2 Как определить, какой белый адрес из пула получит абонент?

Посмотреть, какой белый адрес был назначен серому, можно командой

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

В NAT 1:1 белый адрес выделяется сразу при назначении услуги, в CG-NAT в момент начала сессии

Также выделенный абоненту белый адрес рапортуется в Radius Accounting в целях его логгирования в биллинге.

Заранее предсказать какой-именно адрес будет выдан абоненту из пула невозможно: это зависит от разных факторов и в частности от текущей загрузки пула.

## 3 После подключения NAT стали отваливаться неактивные SSH сессии

Действительно, время жизни сессии в NAT ограничено, т.к. количество сессий у абонента - ограниченный ресурс и большое количество мертвых сессий в пуле уменьшает производительность NAT и общую.

У NAT нет возможности отличить, умерла сессия аварийно или просто в ней нет никакой активности, и закрывает такие долго висящие сессии по таймауту неактивности. Такое поведение предусмотрено стандартом и поддержано большинством производителей CG-NAT.

В SKAT время жизни сессий можно корректировать следующими параметрами

```
lifetime_flow=60  
lifetime_flow_long=600
```

где `lifetime_flow_long` время жизни в секундах неактивных TCP-сессий, `lifetime_flow` остальных.



Но не следует делать эти настройки слишком большими, т.к. тогда может слишком разрастись таблица сессий и это повлияет на производительность CG-NAT, а также у абонента может закончиться лимит сессий (который задается в параметрах `nat` пула).

Поэтому при необходимости поддержания долгоиграющих неактивных соединений рекомендуется использовать механизм `tcp keep-alive`, когда периодически в сессии передается пустой пакет, который сигнализирует, что сессия все еще активна.

Настроить `tcp keep-alive` можно как индивидуально для приложения на стороне сервера или клиента, так и на уровне операционной системы для всех приложений сразу.

**Пример** настройки на ssh сервере

```
в файл /etc/ssh/ssh_config добавляем строку  
ServerAliveInterval 60
```

**Пример** настройки на ssh клиенте

```
в файл ~/.ssh/config добавляем строки  
Host *  
    ServerAliveInterval 60  
или в командной строке  
ssh -o TCPKeepAlive=yes -o ServerAliveInterval=60 user@example.com
```

**Пример** настройки для всех приложений в centos

```
в файл /etc/sysctl.conf добавляем строки
net.ipv4.tcp_keepalive_time = 600
net.ipv4.tcp_keepalive_intvl = 60
net.ipv4.tcp_keepalive_probes = 20
```

## 4 Сколько "серых" IP можно спрятать за одним "белым" в CG-NAT?



Рекомендуется поддерживать соотношение от 1:10 (лучше) до 1:100 (хуже), хотя можно спрятать и тысячу.

Подробнее:

По умолчанию на 1 белом IP для CG-NAT доступны 64512 портов (65535-1023, первые 1024 порта не используются, т.к. являются системными), каждый порт это одна TCP сессия и одна UDP. Количество сессий, которое создают абоненты отличается: физ. лица создают меньше сессий, юр. лица больше (поэтому для юр. лиц нужно использовать отдельный пул с другим лимитами на количество сессий), абонент с торрентом может создать в пике до 1000 сессий.

В среднем физическое лицо создает 50-60 одновременно работающих сессий, т.е.  $64512/60=1075$  физ. лиц можно спрятать за одним серым IP, но на практике такую значительную переподписку использовать не рекомендуется, т.к. многие популярные сервисы (почта, видео, поиск) используют защиту от атак ботнет сетей, основанную на IP адресах. Поэтому если с одного адреса им придет слишком много запросов, они могут принять это за атаку и заблокировать часть запросов или включить капчу, что создаст неудобства для абонентов.

Так же необходимо учесть особенность механизма освобождения портов в NAT Pool:

1. При подключении 11 услуги абоненту [назначается Public IP исходя из алгоритма распределения](#)
2. Когда абонент начинает устанавливать сессии, порты берутся из общей очереди СКАТ DPI и [закрепляются с определенными тайм-аутами](#)
3. В случае если на конкретном Public IP находится много абонентов, которые начинают конкурировать за свободные порты, абоненты могут начать чувствовать проблемы с доступом.

Рекомендации при создании NAT Pool и эксплуатации:

1. Абонентов, которые находятся в блокировке (5 услуга + полисинг), помещать в отдельный NAT Pool, чтобы они не влияли на работу активных абонентов. Так ведет себя iPhone, к примеру, устанавливает множество сессий в поиске рабочего сервиса.
2. Создавайте разряженные пулы и разделяйте клиентов в разные NAT Pool по типу: Физические лица и Юридические лица.

3. Осуществляйте мониторинг клиентов, которые создают большую нагрузку и проводите с ними работу. Для приема, обработки и хранения NetFlow с DPI предлагаем использовать [программный продукт для сбора статистики QoE Store](#) и [графический интерфейс DPIUI2](#). Вы сможете провести анализ трафика абонента и сделать вывод, что его ПК заражен.