

Содержание

Questions and answers	3
Why an address pool of at least 2 or 4 addresses is recommended to create?	3
How to determine which public address from the pool the subscriber will receive?	3
Idle (inactive) SSH sessions began to get disconnected after enabling NAT	4

Questions and answers

1. [cgnat_faq_1](#)
2. [cgnat_faq_2](#)
3. [cgnat_faq_3](#)
4. [cgnat_faq_4](#)
5. [cgnat_faq_5](#)
6. [cgnat_faq_6](#)
7. [cgnat_faq_7](#)

Why an address pool of at least 2 or 4 addresses is recommended to create?

Lock free scheduling algorithm implemented in the DPI is designed to distribute sessions over the working threads, so it imposes restrictions on the public IP address which can be assigned to subscriber from the pool:

- It is required that the number of addresses within the pool is at least the number of working threads (2 for the Stingray SG-6 and 4 for the Stingray SG-10 and further) in order to ensure that public address is assigned to subscriber.

To find out the number of working threads flows:

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

- If there is the only address in the pool, then the address can be assigned just for those subscribers that are used by balancing algorithm, not all subscribers.

How to determine which public address from the pool the subscriber will receive?

To see which public address was assigned to a private one, you can use the command

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

In NAT 1: 1, the public address is allocated immediately when the service is assigned, in CG-NAT at the time of the session start

Also, the public address allocated to the subscriber is reported to Radius Accounting for the purpose of logging it in billing.

It is impossible to predict in advance which address will be issued to a subscriber from the pool: it depends on various factors and, in particular, on the current load of the pool.

Idle (inactive) SSH sessions began to get disconnected after enabling NAT

Indeed, the NAT session lifetime is limited, since the subscriber sessions number is a limited resource and a large number of idle (inactive) sessions in the pool reduces NAT performance and consequently the total performance.

NAT doesn't have the ability to distinguish whether the session was terminated abnormally or is simply inactive, so NAT closes such sessions because inactivity timeout has been exceeded. Such a behavior is provided by the standard and is supported by most CG-NAT vendors.

Sessions lifetime in Stingray SG can be configured by following settings

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

where `lifetime_flow_long` is a lifetime in seconds of inactive TCP-sessions, `lifetime_flow` regards the remaining TCP-sessions.



The values of reviewed above settings should not be too high, since it can cause CG-NAT performance reduction due to enormous session table, also it can cause the subscriber session limit being exhausted (is set by nat pool settings).

Therefore, it is recommended to use tcp keep-alive mechanism when the long-running inactive connections take place, it means that the empty packet will be sent regularly within the session which indicates the session still active.

You can configure tcp keep-alive either application-wide on the server or client side, or operating system-wide at once.

SSH server setting example

```
in /etc/ssh/ssh_config file add the following line  
ServerAliveInterval 60
```

SSH client-side setting example

```
in ~/.ssh/config file add the following lines  
Host *  
    ServerAliveInterval 60
```

or using terminal

```
ssh -o TCPKeepAlive=yes -o ServerAliveInterval=60 user@example.com
```

System-wide setting example for the CentOS

```
in /etc/sysctl.conf file add the following lines  
net.ipv4.tcp_keepalive_time = 600  
net.ipv4.tcp_keepalive_intvl = 60  
net.ipv4.tcp_keepalive_probes = 20
```