Содержание

Questions and answers

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 followin 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 clien-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
```

How many private IP addresses can be hidden behind the public one in CGNAT?

It is recommended to maintain a ratio of 1:10 (better) to 1:100 (worse), although you can hide even a thousand of private IP addresses behind the public one.

Details:

64000 ports are available on one public IP for CGNAT by default, each port corresponds to one tcp and one udp session. The number of sessions created by different groups of subscribers differs: individuals create fewer sessions, legal persons create more (therefore, you need to use a separate pool with different limits on the sessions number in case of legal persons); note that a subscriber with a torrent can create up to 1000 sessions in peak.

On average, an individual creates 50-60 concurrent sessions, i.e. 64000/60 = 1066 individuals can be hidden behind one private IP, but in practice such a significant oversubscription is not recommended, since many popular services (such as mail, video, search) use protection against botnet attacks networks based on IP addresses, so if they receive too many requests from one address, they consider it as an attack and block some requests or enable captcha, which in turn will create inconvenience to subscribers.

It is also necessary to take into account the specialty of the port release mechanism in the NAT Pool:

1. When Service 11 is connected, the subscriber is assigned Public IP based on the distribution algorithm
2. When the subscriber starts to establish sessions, the ports are taken from the general Stingray SG queue and assigned with certain timeouts
3. If there are many subscribers on a specific Public IP who start competing for free ports, subscribers may start experiencing access problems.

Recommendations for NAT Pool creation and operation:

1. The blocked subscribers (Service 5 + policing) should be placed in a separate NAT Pool so that they do not affect the work of active subscribers. This is how the IPhone behaves, for example: it establishes many sessions while searching for a working service
2. Create sparse pools and separate clients into different NAT Pool by type: Individuals and Legal entities

3. Monitor and work with clients who create a heavy load. To receive, process and store NetFlow with DPI, we suggest using a software product for collecting statistics QoE Stor and a DPIUI2 graphical interface. You will be able to analyze the subscriber's traffic and conclude that his PC is infected.