Table of Contents

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
```