Table of Contents

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.