Содержание

Settings and management

This service is managed at the separate subscriber level using `fdpi_ctrl`.

Command format:

```
fdpi_ctrl command --service 11 [options list] [IP_list or login]
```

The command syntax and ways of setting IP addresses are described in the Management of policing and services section.

Activation of address translation for subscribers is carried out with service 11.

CG-NAT

Create named profile that defines CGNAT IP pool parameters:

```
fdpi_ctrl load profile --service 11  --profile.name test_nat --profile.json
'{ "nat_ip_pool" : "5.200.43.0/24,5.200.44.128/25", "nat_tcp_max_sessions" :
2000, "nat_udp_max_sessions" : 2000 }'
```

A description of the parameters can be found in the table below.

In case a `login` is bound to several IPs, the session counter is separate for each IP address.

When specifying a range of external IP addresses, you can specify one or more ranges separated by commas; also you can dynamically add additional ranges to a previously created pool.
You can exclude reserved addresses from the range (according to the classless addressing convention, these are gateway and broadcast addresses) by adding the "~" symbol to the range definition at the end of the `cidr` definition, for example `5.200.43.0/24~`.

NAT 1:1

Create profile for service NAT 1:1[1)], where specify the range of IP addresses within the pool:

```
fdpi_ctrl load profile --service 11  --profile.name test_nat --profile.json
'{ "nat_ip_pool" : "5.200.44.0/24", "nat_type" : 1 }'
```

A description of the parameters can be found in the table below.

When specifying a range of external IP addresses, you can specify one or more ranges separated by commas; also you can dynamically add additional ranges to a previously created pool.
You can exclude reserved addresses from the range (according to the classless addressing convention, these are gateway and broadcast addresses) by adding the "~" symbol to the range definition at the end of the cidr definition, for example 5.200.43.0/24~

Temporary restriction: each of the individual pools in the total pool list must contain at least as many public addresses as the number of worker threads.

NAT Service Management

Activate service 11 to subscriber with named profile:

```
fdpi_ctrl load --service 11 --profile.name test_nat --ip 192.168.0.1
or
fdpi_ctrl load --service 11 --profile.name test_nat --login test_subs
or
fdpi_ctrl load --service 11 --profile.name test_nat --cidr 192.168.1.0/24
```

View the list of all NAT profiles:

```
fdpi_ctrl list all profile --service 11
```

Additional Settings

Additional in global parameters **`/etc/dpi/fastdpi.conf`** it is possible to set:

- `nat_ports`
- `nat_max_profiles`
- `nat_exclude_private`
- `nat_private_cidr`
- `lifetime_flow`
- `lifetime_flow_long`

A description of the parameters can be found in the table below.

Starting with version 12.0, it is now possible to select the method of hashing flow by worker threads. When using the new method, address distribution does not depend on the number of worker threads. It is configured by parameter `rx_dispatcher` in fastpdi.conf (**restart** of the service is required to save changes). The values of the parameter are described in the table below.

In order to guarantee NAT (translation) for a private IP address to any public IP address when using

NAT 1:1, you must specify the IP address range that is used in NAT 1:1. This is configured by the `nat_transcode_cidr` parameter in fastdpi.conf (**restart** of the service is required to save changes), which specifies the CIDR of the public operator addresses. It is possible to specify only 2 CIDRs (in case of using more CIDRs, it is allowed to specify a wider CIDR):

```
nat_transcode_cidr=201.201.210.0/24,201.210.210.0/29
```

The description of the parameter can be found in the table below.
The `nat_transcode_cidr` parameter is **only** relevant when using the new distribution method **AND** using NAT 1:1. In other cases this parameter is not taken into account and is not considered an error.

Parameters and possible values

NAT profile parameters	
Parameter	**Value**
`nat_ip_pool` string	A range of external IP addresses in CIDR format. The pool size should **not be smaller** than the number of worker threads.
`nat_tcp_max_sessions` integer	The maximum number of TCP sessions a subscriber can create. Default: 2000.
`nat_udp_max_sessions` integer	The maximum number of UDP sessions a subscriber can create. Default: 2000.
`nat_type` integer	Sets the type of profile. Choices: `0` --- CGNAT; 1 --- NAT 1:1.
`nat_ports` string	The range of ports used for translation on external addresses. Default: 1024-65535.
fastdpi.conf parameters	
Parameter	**Value**
`nat_max_profiles` integer	Maximum number of profiles with pool parameters. Default: 4. Max: 65000 (if sufficient RAM is available).
`nat_exclude_private` integer	Excludes NAT conversion if both addresses are private. Choices: `0` --- off ← (default). 1 --- Not doing NAT for private addresses (ip_src и ip_dst --- private or in nat_private_cidr). 2 --- ip_src — private subject to nat_private_cidr and AS for dst_ip = local. 4 --- ip_src — private subject to nat_private_cidr and AS for dst_ip = peer.
`nat_private_cidr` string	Specifies additional private address ranges in addition to the standard ranges[2)]. Max: 4 ranges.
`lifetime_flow` integer	Specifies the short queue time in seconds for TCP SYN, FIN, UDP. Default: 60.
`lifetime_flow_long` integer	Specifies the long queue time in seconds for a TCP DATA established connection. Default: 300.

`nat_whp_lifetime` integer	Specifies the short queue time in seconds for NAT broadcast for TCP SYN, FIN, UDP. This parameter overrides `lifetime_flow` for NAT broadcasts only. Default: 75.
`nat_whp_lifetime_long` integer	Specifies the long queue time in seconds for NAT broadcast for a TCP DATA established connection. This parameter overrides `lifetime_flow_long` for NAT broadcasts only. Default: 375.
`nat_transcode_cidr` string *Add in 12.0*	Specifies the CIDR of the operator's public addresses. Only 2 CIDRs can be specified (in case of using more CIDRs, it is acceptable to specify a wider CIDR). The values are used when transcoding public → private for NAT 1:1. Any public address can be assigned to a private address for NAT 1:1.

`rx_dispatcher`
integer
Add in 12.0
	The method of hashing flow by workflow.
	Choices:
	`0` --- previous method ← (default). `(IP_SRC+IP_DST)%N ) & IP_MASK`
	`1` --- a method with uniform balancing over an arbitrary number of flows **with** NAT 1:1 support with the requirement to assign specific addresses. `(CRC(IP_SRC)%N+CRC(IP_DST)%N)%N`
	`2` --- a method with uniform balancing over an arbitrary number of flows **without** NAT 1:1 support with the requirement to assign specific addresses.

1)

operators sometimes use broadcast 1:1 as an alternative to routing white IPs to subscriber CPEs, but it is important to understand that although this scheme simplifies administration a bit, it is unequal both from the subscriber's point of view, who usually pays money for the white address service, and from the network point of view, as some client software knows about private addresses and behaves differently than in the case of public addresses, for example, messengers WhatsApp/Viber/Skype/SIP instead of direct P2P connections start using stun-proxy servers, which are often overloaded, which can seriously degrade the quality of voice and video calls, IPSEC VPN without NAT-T support or with certificate authorization does not work, a subscriber cannot use his public IPv4 as an IPv6 address through the mechanism 6to4, autodetection of local tracker stops working in torrents, trackers often give less number of peers to subscribers with gray addresses, which affects download speed, etc. For L2-connected subscribers the best alternative to NAT1:1 is to use unnumbered addresses, which are natively supported by SSG BRAS. Besides, when moving to IPv6/Dual Stack, the operator will still have to learn how to route public IPv6 addresses

2)

Standard ranges: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 100.64.0.0/10