Содержание

Settings and management 3
CG-NAT 3
NAT 1:1 4
NAT Service Management 4
Additional Settings 4

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" : "5.200.43.0/24,5.200.44/25", "nat_tcp_max_sessions" :
2000, "nat_udp_max_sessions" : 2000 }'
```

Here:

- `nat_ip_pool` - exernal (public) IP addresses in CIDR, the pool size should not be smaller than the number of worker threads
- `nat_tcp_max_sessions` - maximum number of TCP session that subscriber can create
- `nat_udp_max_sessions` - maximum number of UDP session that subscriber can create

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 }'
```

where `nat_ip_pool` is the range of external IP addresses in CIDR format, the pool size must be at least the number of worker threads

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 Service Management

Activate service 11 to subscriber with named profile (assign the pool with pareameters above)

```
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=1024-65535` - port range using for NAT translation on public IP addreses (default value is in example)
- `nat_max_profiles=24` - maximum number of named profiles with CGNAT pool parameters (allowed maximum parameter value 65000, server memory also limit this parameter)
- `nat_exclude_private=1` - prevent NAT translation when both addresses are private (bitmask)
    - 0 — always convert private → public
    - 1 — do not do NAT for private addresses (ip_src and ip_dst are grayed out or are in

psz_prms_user_private)
    - 2 — ip_src — private with psz_prms_user_private and AS for dst_ip = local
    - 4 — ip_src — private with prms_user_private and AS for dst_ip = peer
- `nat_private_cidr=201.201.201.201/24,8.8.8.8/32` - specifies the extended private address ranges (at most 4 addresses) in addition to the standard ones:

```
10.0.0.0/8
172.16.0.0/12
192.168.0.0/16
100.64.0.0/10
```

- `lifetime_flow=60` - short queue lifetime in seconds for TCP SYN, FIN, UDP (60 is the default value)
- `lifetime_flow_long=300` - long queue lifetime for TCP DATA connection (300 is the default value)

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):

- `rx_dispatcher=0` - **default** method `(IP_SRC+IP_DST)%N ) & IP_MASK`
- `rx_dispatcher=1` - 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`
- `rx_dispatcher=2` - method with uniform balancing over an arbitrary number of flows **without** NAT 1:1 support with the requirement to assign specific addresses

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 `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.

1)

many operators use 1:1 address translation as an alternative solution for routing public IPs to subscriber's Customer Premise Equipment (CPE), but it's important to know that although this scheme simplifies administration until the introduction of IPv6, it is unequal both from the subscriber's point of view because the service is usually chargeable, and from the networking point of view, because some client software knows about private addresses and behaves differently than in case of public addresses, for example, in torrents, the local retracker autodetection ceases to work, trackers sometimes give out lower number of peers to subscribers with private addresses, which affects the download speed, furthermore the subscriber can not use his public IPv4 address as IPv6 through the mechanism 6to4, supported by many routers used to deploy home networks, so the SIP clients try to use the STUN server, though it is not necessary and so on, in addition with the IPv6/Dual Stack using

the operator still have to learn how to route public addresses