Содержание

1 Fastdpi configuration

You need to create services and policies, which will later be transmitted using the Radius attributes from billing. An example of setting up a policy (tariff plan) and Captive Portal, which are the minimum required to start.

1. Create a file aslocal.bin (or correct this file if it already exists). The aslocal file contains those ranges of private IP addresses that are used in the provider's local network. Any of the range 64512 - 65534 is indicated for them as an autonomous system number.

```
vi aslocal.txt
10.0.0.0/8 64512
172.16.0.0/12 64512
192.168.0.0/16 64512
cat aslocal.txt | as2bin /etc/dpi/aslocal.bin
```

FastPCRF authorizes only the local users. The fact whether the user is local or not is determined according to the fact of belonging his IP-address to the list of local autonomous systems.

2. Next, create the asnum.dscp file (or modify it if it already exists). The *local* numbers of autonomous system should be specified in this file, so the authorization will take place for them. Typically these are autonomous systems for the gray IP addresses specified in the aslocal.bin file, plus the white IPs allocated to the provider, if these white IP addresses are used on the local network, that is, they require authorization. Authorization will be done for all the autonomous systems IP addresses marked as local in the asnum.dscp file.

```
vi asnum.txt
64511 local
cat asnum.txt | as2dscp /etc/dpi/asnum.dscp
```

3. To enable authorization in **/etc/dpi/fastdpi.conf**:

```
enable_auth=1
```

4. Set the fastPCRF servers list:

```
auth_servers=127.0.0.1%lo:29002;192.168.10.5%eth1:29002
```

The format for specifying a single server: `ip%dev:port`, here `ip` is the server IP address, dev is the local device by wich the connection can be established. FastDPI connects to the first available fastpcrf server from the list.

Do not forget to activate the user property store:

```
udr=1server
```

IPv6

In order to enable IPv6 addresses authorization you should activate the IPv6 support. Actually, the Stingray SG authorizes a whole subnet with a predefined prefix length (by default it equals to /64) rather than particular individual IPv6 address. For example, if there are incoming packets sent from 2001:1::1 and 2001:1::10 addresses, only one of these addresses will be subject to authorization, so the returned authorization parameters will be applied to all the addresses from 2001:1::/64 subnet.

There is no analog of the `aslocal.bin` file for IPv6, since there are no private addresses. You must mark the AS numbers that require authorization as `local` in the `asnum.dscp` file.

IPv6 authorization is automatically enabled if fastdpi.conf has:

```
ipv6=1
enable_auth=1
```

Starting from SSG version 8.1.4, it is possible to forcibly disable IPv6 address authorization by specifying in fastdpi.conf:

```
enable_auth_ipv6=0
```

Other authorization settings