Table of Contents

Management of policing and services

Subscribers' management is handled by fdpi_ctrl utility.

We recommend using Named profiles which simplify the services and policies management.

Command syntax

General command format:

```
fdpi_ctrl command { --service service_identifier | --policing
policing_description_file} [IP_list] [LOGIN_list]
```

Here 'command' is:

```
load : load data
del  : remove. You have to specify 'program_identifier' for '--service'. No
need to specify for policing
list : show the information on the specified 'IP_list' or all the
information if the argument is 'all'
```

service_identifier - is one of these values or their comma separated list:

```
1 - bonus program
2 - advertising
3 - block advertisements
4 - block list filtering
5 - allow list and Captive Portal
6 - notification via HTTP redirect
7 - caching
8 - DDos protection passed
9 - RADIUS accounting / collect netflow statistics for billing
10 - DDOS protection
11 - CGNAT and NAT 1:1
12 - traffic recording in PCAP
13 - mini-Firewall
14 - traffic diversion to the TAP interface
15 - specific subscriber (all traffic is placed in cs0, no filtering (4
service) is applied for vChannel and shared channel)
16 - allow list and redirecting to Captive Portal when there is no access to
the Internet
17 - traffic mirroring to a specified VLAN
18 - session policing for certain protocols and traffic class definition at
channel and subscriber levels
```

```
19 - spoofing DNS responses. Plans: redirecting DNS requests to the
provider's DNS server
49 - IPv6 traffic blocking
50 - member of a marketing campaign with notification via HTTP redirect
51 - reserved (internal)
254 - VRF
```

When blocking services are activated (4, 16, 49), only TCP traffic is blocked. To block UDP traffic as well, you must enable the `udp_block` parameter.

IP_list - is a sequence or one of the following options:

```
--file     - a file containing IP list
--ip       - a single IP
--ip_range - inclusive IP range
--cidr     - CIDR (inclusive) CIDR~ (exclusive)
```

You can exclude reserved addresses from the CIDR range (by classless convention, these are gateway and broadcast addresses) by adding the “~” symbol to the range definition at the end of the cidr definition, for example –cidr 5.200.43.0/24~

LOGIN_list - is a sequence or one subscriber's name value in format:

```
--login USER1
--login "FIRST_NAME LAST_NAME" is the option to indicate login with special
symbols screening
```

IP list or LOGIN can be specified as:

```
192.168.0.1             a single IP
192.168.0.1-192.168.0.5 inclusive IP range
192.168.0.0/30          CIDR
"USER1"                 specify LOGIN in quotes
'USER2'                 specify LOGIN in single quotes
```

Lines starting from '#' is as a comment.

One can specify 'all' instead of IP/LOGIN list in commands list, del, clear. It means to apply the command to all subscribers.

Examples

To get the policing application list:

```
fdpi_ctrl list all --policing
```

To get the list of subscribers with active service 1:

```
fdpi_ctrl list all --service 1
```

To get the information for specified IP:

```
fdpi_ctrl list --policing  --ip 192.168.0.1
fdpi_ctrl list --service 1 --ip 192.168.0.1
```

To activate service 1:

```
fdpi_ctrl load --service 1 --ip 192.168.0.1
or
fdpi_ctrl load --service 1 --login USER1
```

To activate policing:

```
fdpi_ctrl load --policing tbf.cfg --ip 192.168.0.1
```

To disable service 1:

```
fdpi_ctrl del --service 1 --ip 192.168.0.1
```

One can specify several options '–file', '–ip', '–ip_range', '–cidr' when specifying IP list:

```
fdpi_ctrl list --service 1 --ip 192.168.0.1 --ip 192.168.0.2 --file
fip_1.txt --ip_range 192.168.0.3-192.168.0.6 --login USER1
```

This action would be applied to all elements that do not cause any errors.


There is no undo for changes that were already implemented is made on errors.

Detailed description on policing and services' management one can find in chapters devoted to the respective options.

Configuring TCP and UDP protocol blocking

The `udp_block` parameter is responsible for blocking the UDP protocol. If the DPI configuration file `/etc/dpi/fastdpi.conf` contains this parameter, then TCP+UDP blocking will take place, if not - only TCP will be blocked.

To start blocking UDP protocols (e.g. QUIC), it is necessary to add the `udp_block` parameter to the configuration file with the value 2 or 3 (to start blocking after two or three packets have passed). Such values are set because there may be a large number of single packets that are not counted in the traffic, but may cause a heavy load on DPI.

```
udp_block=3
```

Adding a parameter does not require a DPI restart, just a reload:

```
service fastdpi reload
```