Содержание

15 Mini Firewall

The service is designed to to improve security against unauthorized access in case of subscribers having public [1)] IPv4 and IPv6 addresses. All incoming requests for ports below the specified threshold are closed to the subscriber's address (usually the threshold equals to 1024 - i.e. all system ports will be closed), but some ports could be left opened, for example, to access a home NAS. In addition, some malicious activity coming from the subscriber can be blocked via mini firewall, for example, if as a result of netflow analysis or receiving abuse it turned out that the subscriber is engaged in spam activity, then outgoing ports associated with the mailing list can be closed by means of mini firewall service.


It should be borne in mind that often in such cases the subscriber is not guilty, just his laptop is infected with a virus or is a part of someone else's botnet network. In this case, it is recommended to show the subscriber a notification page using service 6 with a problem description and an antivirus subscription offer, and thereby increase sales of additional services. This process will be further even more automated in the very near future within the QoE Store/Marketing Campaigns in terms of infection detection, blocking malicious activity and automatically issuing an alert.

The service management at the individual subscribers level is carried out using the fdpi_ctrl

Command format:

```
fdpi_ctrl command --service 13 [options_list] [IP_list or Login]
```

More details on command syntax and ways to specify IP addresses are described in Management commands

Examples:

to enable mini Firewall for specific subscriber having named (preconfigured) profile

```
fdpi_ctrl load profile --service 13 --profile.name strict_firewall --
profile.json '{  "max_port" : 1024, "port_holes" : [ 80, 8080 ], "out_port"
: [ 25, 465 ] }'
fdpi_ctrl load --service 13 --profile.name strict_firewall --login
mike.williams
```

here the json format is used to specify the following profile settings
max_port - the port number, below which access is blocked
port_holes - list of ports that are allowed to access bypassing the max_port limit
out_port - list of ports to which outbound traffic is closed

Enabling mini Firewall service to subscriber having anonymous profile (i.e. profile without name which exists until the corresponding service is enabled)

```
fdpi_ctrl load --service 13 --profile.json '{  "max_port" : 1024,
"port_holes" : [ 80, 8080 ], "out_port" : [ 25, 465 ] }' --login
mike.williams
```

Search for subscribers having enabled mini Firewall service with the specified profile name

```
fdpi_ctrl list all --service 13 --profile.name strict_firewall
```

Delete the named profile (the subscribers using it shouldn't exit)

```
fdpi_ctrl del profile --service 13  --profile.name strict_firewall
```

To change profile settings (it should be borne in mind that new settings will be applied to all the subscribers with specified service profile)

```
fdpi_ctrl load profile --service 13 --profile.name strict_firewall --
profile.json '{  "max_port" : 1024, "port_holes" : [ 80 ] }'
```

The maximum number of profiles for the mini Firewall is specified by the configuration parameter in /etc/dpi/fastdpi.conf

```

max_profiles_frwl=24
```

here the value 24 is the default value (maximum possible value is (2^16 - 1) == 65535) It is not "on-the-fly" parameters, so when changing it the restart is needed.

1)
NAT is a kind of information security measure in case of private IP addresses