Table of Contents

Configuration

The system is delivered with black list filtering option turned on.

You can configure the option or turn it off by configuration file **/etc/dpi/fastdpi.conf**. All parameters are optional and have default values.

Filtering service configuration

```
federal_black_list=2 enables automatic loading and application of cloud
service list
(0 - disables)
```

The lists received from clouds are placed to the directory **/var/lib/dpi**. Their names are:

blcache.bin - URL dictionary to block HTTP
blcachecn.bin - names' dictionary to block HTTPS by certificates
blcacheip.bin - IP addresses dictionary to block HTTPS by IP
blcachesni.bin - dictionary to block HTTPS by SNI

The subscriber's browser receives 403 error (Forbidden) as a reply on an attempt to access a restricted page by HTTP protocol. Its look depends on the browser in use.

This behaviour can be modified. The browser can be redirected to a special operator's information page Instead of the error code[1][2]

Page setup for redirect:

```
black_list_redirect=http://operator.com/blockpage.html
```

The black list update period can be configured. It is 60 minutes by default:

```
timeout_check_new_bl=60
```

We recommend making the download period no more than 5 minutes. The lists are updated automatically without interruption of the service and the need to restart /reload.

The service has to load modified parameters after configuration changes. One can do it by the following instructions [3]:

To update modified "hot" parameters:

```
service fastdpi reload
```

To update all parameters by the service's restart:

```
service fastdpi restart
```

The short break (less than 1 second) in service is caused by restart, if the Bypass is not supported.

The "hot" parameters: federal_black_list,only_tcp,timeout_check_new_bl
The "cold" parameters: black_list_redirect,custom_url_black_list,custom_cn_black_list,custom_ip_black_list,custom_sni_black_list
You can find more details here: administering

Custom lists configuration

Preparing dictionaries with URL, SNI, CN and IP addresses is described in the next section of the documentation.

The operator can attach his own black list.

```
#URL dictionary for blocking by HTTP protocol
custom_url_black_list=http://operator.com/url_list.dic

#Names dictionary for blocking HTTPS by certificate
custom_cn_black_list=http://operator.com/cn_list.dic

#IP addresses dictionary for blocking HTTPS by IP
custom_ip_black_list=http://operator.com/ip_list.dic

#Hosts names dictionary for blocking HTTPS by SNI (Server Name Indication)
custom_sni_black_list=http://operator.com/sni_list.dic
```

URL field can be used to specify ftp protocol and authentication parameters.

The lists downloaded from the specified URL are stored in /var/lib/dpi. Their names are:

blcustom.bin - the URL dictionary to block HTTP
blcustomcn.bin - the name's dictionary to block HTTPS by certificate
blcustomip.bin - the IP addresses' dictionary to block HTTPS by IP
blcustomsni.bin - the IP addresses' dictionary to block HTTPS by SNI

Additional Information

'#' character at the beginning of a configuration file line marks the comment.

In case the service is used to filter by black list only, we advise to switch off the analysis of protocols rather than HTTP. It helps increase productivity and reduces CPU load:

```
only_tcp=1
```

If the black lists are created on the same computer that runs DPI: you can just put them to **/var/lib/dpi** directory. Their names must be **blcustom.bin, blcustomsni.bin, blcustomcn.bin and blcustomip.bin,** same as above.

Use only command mv for moving dictionaries - it's atomic, don't use copying!

Switching off the custom lists

To switch off additional (operator's) black lists:

Comment out or remove the parameters from configuration file **/etc/dpi/fastdpi.conf**:

```
custom_url_black_list, custom_ip_black_list, custom_cname_black_list,
custom_sni_black_list
```

To remove local lists:

```
rm /var/lib/dpi/blcustom.bin
rm /var/lib/dpi/blcustomcn.bin
rm /var/lib/dpi/blcustomip.bin
rm /var/lib/dpi/blcustomsni.bin
```

Here's the translation of the blocking settings:

Blocking Settings

Add the parameter `block_options` to the configuration file `/etc/dpi/fastdpi.conf`.

Values:

- 1 — block regardless of the presence of SNI
- 2 — block all ports on the address
- 4 — block all of IPv6 (when the service 4 is enabled)
- 8 — do not generate RST packets for blocking and redirection for `inet->subs` packet direction

[1]

in case this parameter ends by ? or &: the parameter UrlRedir is added to the formed URL. It points to a page selected by the subscriber.

[2] you should add parameters can be added usingr ? or & (by HTTP rules), otherwise the DPI adds /? to the URL

[3] Corrections