Table of Contents

Filtering by the Register of Banned Websites (service 4)

Product Description

1. The filtering management through service 4 does not deactivate the service. What is the reason?

1. Check the `black_list_sm` parameter in the configuration file `/etc/dpi/fastdpi.conf`. If it is set to 1, the service is enabled and blocking is not global for all.
2. On a test subscriber (IP/login), ensure that the service is deactivated:

   ```
   fdpi_ctrl list --service 4 --ip 192.168.1.60
   ```

   Output options:
   `1/0/1` - service removed
   `1/1/0` - service available

   ```
   Result processing ip=192.168.1.60 : 1/0/1
   ```

   — service is deactivated

3. Set the IP address of the deactivated subscriber in the configuration `/etc/dpi/fastdpi.conf`:

   ```
   trace_ip=<IP>
   ```

   After setting, reload:

   ```
   service fastdpi reload
   ```

   Make a request from a test PC to the resource metfen.com
   Check the log for the test site:

   ```
   grep -A5 metfen fastdpi_slave_?.log
   ```

   or

   ```
   cat fastdpi_slave_?.log | grep metfen.com -A 5
   ```

   Output:

   ```
   HTTP_HOST=_metfen.com_
     HTTP_REFERER(0)=_null_
     HTTP_USER-AGENT=_Mozilla/5.0 (Windows NT 6.1; WOW64)
   AppleWebKit/537.36 (KHTML, like Gecko)
   ```

```
  Chrome/43.0.2357.65 Safari/537.36_
  HTTP_COOKIE=_null_
  [TRACE   ][001693490086826396][2888570700] CHECK_HTTP : URL=_/_
        HTTP_HOST=_metfen.com_
        HTTP_REFERER=_null_
        blocked=0
        new_prg_id=0
```

As seen in the output, `blocked = 0` (no redirection), `new_prg_id=0` (no service connected). SSG — does not conduct redirection/blocking.

4. Capture the requests dump to the banned resource on the deactivated subscriber, e.g., using `fiddler`. If redirection remains, the issue lies on the blocking page — there is no information on its caching on the browser side, and the browser independently redirects the request without SSG involvement.
   To prevent this, use:

   ```
   Cache-Control: max-age=0, no-cache, no-store, must-revalidate
   Pragma: no-cache
   ```

2. On fragmentation and setting MTU

Request: The auditor found the page https://vip-club-vulkan.net/ accessible, the auditor's report code — 409. The page does not load, but access is present.
Actions: check MTU on the router to the SSG DPI, the problem is related to packet fragmentation and is solved as follows — setting only `hardware mtu` (`jumbo frame`) is not sufficient, in addition, `ip mtu` should be set to 1500. After this, the site will stop opening and appear in the Auditor's report.

3. Checking the availability of cloud lists

To check the availability of cloud lists, use the `curl` utility with the following parameters:

```
curl -A "user-agent: FastDPI_blcheck" -o /dev/nul
https://www.vasexperts.ru/data/lastdump.zip
```

```
curl -v -o blacklist.dict https://vasexperts.ru/data/belarus/blacklist.dict
```

4. Uploading your own list

There is a possibility to force DPI to work only with your list of banned resources. Work with the cloud/custom list is managed by the `federal_black_list` parameter.

5. Redirecting https requests

Redirect to a "stub" page is performed for http requests; for https, this action is impossible. To do this, you need to decrypt the traffic using a private key or root certificate, so only traffic blocking is performed.

6. Joint use of custom and cloud lists

Custom lists are used separately, in addition to the cloud lists (if the service is enabled). More about parameters - `federal_black_list`.

7. Filtering and VLAN. Is it possible to apply a filtering policy to specific VLANs?

Yes. On setting up external channels and connecting services of allow/block lists — see the description of the 4 service.

All tagged traffic passing through the DPI will be filtered, and there is no need to create any VLANs on the DPI server itself. There is no need to create additional VLANs.

8. Get a list of addresses for filtering according to the BGP scheme

This filtering scheme is not supported "out of the box," but you can organize it yourself: since DPI does not filter by IP, you will need to convert hosts to IP addresses yourself, for example:

```
#1
bin2ip /var/lib/dpi/blcacheip.bin > tmp.txt
#2
dic2host /var/lib/dpi/blcache.bin|dig +short -f -|grep -E
'[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}' » tmp.txt\\
#3
sort -u tmp.txt > ip.lst
```

To track the loading of new lists on DPI and run the conversion scripts, you can set up `incron`, and you can announce routes via exabgp.