

Содержание

5 Диагностика 3

5 Диагностика

Протоколы работы SKAT DPI расположены в каталоге /var/log/dpi

В файле fastdpi_alert.log находится информация об ошибках и информационных событиях. Первое поле = класс сообщения. Далее следует диагностическая информация и текст информационного сообщения или сообщения об ошибке.

Информация об успешном обновлении черных списков из облачного сервиса:

```
[INFO    ] bl_updater_thread : URL black list download with result, rc=1001 : Success.  
[INFO    ] bl_updater_thread : IP black list download with result, rc=1001 : Success.
```

В файле fastdpi_stat.log находится статистическая информация.

Количество проверенных и заблокированных URL (для протокола HTTP):

```
url/lock=881557942/644
```

Количество проверенных и заблокированных сессий по сертификату (для протокола HTTPS):

```
ssl/lock=1656734322/58
```

Количество проверенных и заблокированных пакетов по IP (для протокола HTTPS):

```
https/lock=3021320891/3
```

Проверить, что списки актуальны, дата обычно не сильно в прошлом до нескольких часов:

```
ls -la /var/lib/dpi/blcache*
```

Проверьте активность [байпасс режима](#) (при наличии):

```
bpctl_util all get_bypass
```

Ошибка:

```
-bash: bpctl_util: command not found
```

Означает что у вас нет байпасс

Проверить что трафик тестового абонента проходит через DPI:

```
проверьте что файлы логов не превышают 1Гб:  
ls -la /var/log/dpi/fastdpi_slave_?.log  
если превышают то сделайте:  
echo "" > /var/log/dpi/fastdpi_slave_0.log  
echo "" > /var/log/dpi/fastdpi_slave_1.log  
echo "" > /var/log/dpi/fastdpi_slave_2.log
```

```
echo "" > /var/log/dpi/fastdpi_slave_3.log
```

Установить в конфигурации /etc/dpi/fastdpi.conf IP адрес тестового компьютера:

```
trace_ip=<IP>
```

После установки сделать:

```
service fastdpi reload
```

Сделать на тестовом компьютере:

```
wget metfen.com
```

Проверьте что есть записи в логе DPI:

```
grep -E "metfen.com" -A5 /var/log/dpi/fastdpi_slave_?.log
```

Пример для protonmail.com:

1. Запрос

```
wget protonmail.com
```

```
--2020-02-09 19:50:15-- http://protonmail.com/
```

```
Resolving protonmail.com... 5.3.3.17, 2a02:2698:a002:1::3:17
```

```
Connecting to protonmail.com|5.3.3.17|:80... connected.
```

```
HTTP request sent, awaiting response... 302 Moved Temporarily
```

```
Location: http://vasexperts.ru/test/blocked.php [following]
```

```
--2020-02-09 19:50:16-- http://vasexperts.ru/test/blocked.php
```

```
Resolving vasexperts.ru... 45.151.108.17
```

```
Connecting to vasexperts.ru|45.151.108.17|:80... connected.
```

```
HTTP request sent, awaiting response... 200 OK
```

2. проверка записей в логе

```
grep -E "proton" -A5 /var/log/dpi/fastdpi_slave_?.log
```

```
/var/log/dpi/fastdpi_slave_1.log:HTTP_HOST=_protonmail.com_
```

```
/var/log/dpi/fastdpi_slave_1.log-HTTP_REFERER(0)=_null_
```

```
/var/log/dpi/fastdpi_slave_1.log-HTTP_USER-AGENT=_Wget/1.12 (linux-gnu)_
```

```
/var/log/dpi/fastdpi_slave_1.log-HTTP_COOKIE=_null_
```

```
/var/log/dpi/fastdpi_slave_1.log-[TRACE
```

```
][000000045177957936][0167666FC85BFC15] CHECK_HTTP 192.168.1.8:24359 -->
```

```
5.3.3.17:80 url_blocked=0x22, method=1 : URL=_/_
```

```
/var/log/dpi/fastdpi_slave_1.log: HTTP_HOST=_protonmail.com_
```

```
/var/log/dpi/fastdpi_slave_1.log- HTTP_REFERER=_null_
```

```
/var/log/dpi/fastdpi_slave_1.log- new_prg_id=0x0(0x0)
```

```
/var/log/dpi/fastdpi_slave_1.log- other_prg_id=0x0(0x0)
```

```
/var/log/dpi/fastdpi_slave_1.log- prof_idx={0,0,0,0,0,0}
```

```
/var/log/dpi/fastdpi_slave_1.log- ddos=0
```

```
--
```

```
/var/log/dpi/fastdpi_slave_1.log: HTTP_HOST=_protonmail.com_
```

```
/var/log/dpi/fastdpi_slave_1.log- HTTP_REFERER=_null_
```

```
/var/log/dpi/fastdpi_slave_1.log-
```

```
NEW_URL=http://vasexperts.ru/test/blocked.php_
```

```
/var/log/dpi/fastdpi_slave_1.log- NEW_REFERER=_null_
```

По логу видно что ресурс заблокирован:

```
... url_blocked=0x22 ...
```

и произведена переадресация на страницу блокировки:

NEW_URL=http://vasexperts.ru/test/blocked.php_