Содержание

Diagnostics 3

Diagnostics

The Stingray Service Gateway logs are placed to */var/log/dpi*

The file fastdpi_alert.log contains the information on errors and informative events. The first field denotes the message class. The diagnostic information and the message text or error text are placed next.

The information on successful renewal of black lists from cloud service:

```
[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.
```

The file fastdpi_stat.log contains statistical information.

The number of verified and blocked URL (for HTTP protocol):

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

The number of verified and blocked sessions by certificate (for HTTPS protocol):

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

The number of verified and blocked packets by IP (for HTTPS protocol):

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

Check that the lists are up to date, the date is usually not far in the past (a few hours):

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

Check if mode bypass is active (if present):

```
bpctl_util all get_bypass

Mistake:
-bash: bpctl_util: command not found
Means you don't have a bypass
```

Check if there is a service on the subscriber, if there is, whether it corresponds to the black_list_sm parameter:

```
looking for a login by IP (if logins are used)
fdpi_ctrl list all --bind_multi | grep 192.168.1.100
user_100:192.168.1.100

check the status of the service:
```

```
fdpi_ctrl list --service 4 --login user_100
Autodetected fastdpi params : dev='eth5', port=29000
connecting 192.168.0.2:29000 ...

================================

user_100 4 (0x8) default
Result processing login=user_100 :
1/1/0
Total: filtering service is active

Checking the state of the parameter:
service fastdpi reload
grep black_list_sm /var/log/dpi/fastdpi_alert.log | tail-1
black_list_sm : 0

ATTENTION! The parameter is set by default, which means that the inversion
works - the active service disables filtering on the subscriber.
For details, see the section on filtering service management.
```

Check that the test subscriber's traffic goes through DPI:

```
check that the log files do not exceed 1GB:
ls -la /var/log/dpi/fastdpi_slave_?.log
if it exceeds then do:
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

Set the IP address of the test computer in the /etc/dpi/fastdpi.conf
configuration:
trace_ip=<IP>
After installation do:
service fastdpi reload

Sample verification for protonmail.com:
1. Request
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. checking log entries
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_

The log shows that the resource is blocked:
... url_blocked=0x22 ...
and redirected to the blocking page:
NEW_URL=http://vasexperts.ru/test/blocked.php_
```