Содержание

Configuring protection 3

Configuring protection

The service can be configured through the GUI. Instruction

This protection trigs when a load goes beyond one of the thresholds configured by the file /etc/dpi/fastdpi.conf

```
ddos_reqsec_threshold=300
ddos_reqsec_variation=5
```

here ddos_reqsec_threshold - is the number of requests per second addressed to the protected site. It is configured usually to be equal to maximal number of requests observed in normal operation. ddos_reqsec_variation - is the deviation from requests' number specified by ddos_reqsec_threshold that causes the protection to be switched on and off. It is used to prevent random switches between states. It is expressed in percent and equals to 5% by default.

```
ddos_pktsec_threshold=5000
ddos_pktsec_variation=5
```

Here ddos_pktsec_threshold - is the number of packets per second that comes to the protected site. It is configured usually to be equal to maximal number of packets observed in normal operation. ddos_pktsec_variation - is the deviation from packets' number specified by ddos_pktsec_threshold that causes the protection to be switched on and off. It is used to prevent random switches between states. It is expressed in percent and equals to 5% by default.

The parameter ddos_reqsec_threshold has the priority over ddos_pktsec_threshold in case both are specified. The latest value is ignored in this case.

The following parameter specifies the page containing CAPTCHA. One is redirected to this page for verification:

```
ddos_check_server=www.server_name.ru/path/page.html?
ddos_security_key=123567890
```

here the `ddos_security_key` is the encription key used when forming the tokens indicating to the DPI that the test is successful

Alert logging can be enabled by the following option

```
ddos_trace=1
```

The list of legit IP addresses can be obtained by the analysis of the protected site's WEB server's logs. (The script to process these logs can be implemented independently or using the VAS Experts DPI technical support.) Alternatively, the list can be formed based on the DPI logs.

This list is loaded to the DPI by the instruction:

```
fdpi_ctrl load --service 8 --file ip_list.txt
```

Here ip_list.txt is the generated trusted list. You can learn more about fdpi_ctrl instruction and how to ensure data persistence here: Configuring subscribers. Users of the site under protection are considered to be subscribers in this case.

DPI can generate the access log by itslef, as described here: Lawful Interception. After configuring the log parameters, IP addresses collection is started by the instruction:

```
fdppi_ctrl setenv --ddos_ip_gathering 1
```

It is switched off by sending 0 by this command.