Содержание

Настройка параметров защиты

Услугу можно настроить через GUI. Инструкция

Активация данного вида защиты срабатывает при превышении одного из порогов, установленных в конфигурационном файле */etc/dpi/fastdpi.conf*

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

где ddos_reqsec_threshold - количество запросов в секунду, приходящее на защищаемый сайт, обычно выбирается максимальное значение, которой наблюдалось при нормальной работе сайта
ddos_reqsec_variation - это заданное в процентах возможное отклонение от заданного в ddos_reqsec_threshold порога, при котором происходит соответственно включение или отключение защиты, задается для избежания эффекта "дребезга" и по умолчание составляет 5%

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

где ddos_pktsec_threshold - количество пакетов в секунду, приходящее на защищаемый сайт, обычно выбирается максимальное значение, которой наблюдалось при нормальной работе сайта
ddos_pktsec_variation - это заданное в процентах возможное отклонение от заданного в ddos_pktsec_threshold порога, при котором происходит соответственно включение или отключение защиты, задается для избежания эффекта "дребезга" и по умолчание составляет 5%

Если заданы оба параметры, то более приоритетным считается ddos_reqsec_threshold и значение параметра ddos_pktsec_threshold не учитывается.

Страничка с CAPTCHA, на которую производится перенаправление для проверки, указывается в параметре

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

где ddos_security_key ключ шифрования, используемый при формировании токенов, индицирующих для dpi успешное прохождение проверки

Логирование срабатывания защиты можно включить настройкой

```
ddos_trace=1
```

Можно заранее собрать список доверенных IP адресов на основе анализа логов WEB-сервера защищаемого сайта (скрипт для их анализа пишется самостоятельно или службой техподдержки) или на основе лога, созданного самим DPI.

Созданный таким образом список загружается в DPI командой

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

где ip_list.txt список Подробнее про команды fdpi_ctrl и обеспечение персистентности данных можно прочитать в разделе Управление абонентами. Абонентами в этом случае считаются пользователи защищаемого сайта.

DPI может генерировать лог доступа самостоятельно, как описано в разделе про COPM.