Содержание

Подготовка словарей со списком блокируемых ресурсов

Подготовка словаря со списком блокируемых ресурсов 2-х этапная: сначала создается тестовый файл со списком ресурсов, который затем конвертируется во внутренний формат словаря с помощью специальной утилиты.

Для конвертации используются следующие утилиты:

- `url2dic` - для URL, SNI CN
- `ip2bin` - для IP

Утилита для проверки вхождения в черный список - `checklock`.

Формат файла со списком блокируемых URL:

Каждая строка файла содержит один url (без префикса http://), например:

```
1magehut.com/users.php?act=gallery&gal=81&page=4
3dmx.net
```

Конвертирование во внутренний формат:

```
cat my_url_list.txt|url2dic my_url_list.dic
```

Конвертирование во внутренний формат с автоматическим преобразованием доменов и букв в url, написанных в национальном алфавите в кодировке utf-8:

```
cat my_url_list.txt|url2norm|url2dic my_url_list.dic
```

Формат файла со списком блокируемых имен в сертификатах SSL (Common Name):

Каждая строка файла содержит одно имя, например:

```
*.facebook.com
www.vasexperts.ru
```

Конвертирование во внутренний формат:

```
cat my_cn_list.txt|url2dic my_cn_list.dic
```

Формат файла со списком белых SNI (домены https):

Каждая строка файла содержит один SNI (без префикса http://), допускается использование *, например:

```
qiwi.ru
*.qiwi.ru
```

Конвертирование во внутренний формат:

```
cat my_sni_list.txt|url2dic my_sni_list.bin
```

Формат файла со списком блокируемых IP адресов, CIDR:

С версии 12.4 поддерживается создание списка на основе:

- IPv4 <пробел> номер_порта
- IPv4
- IPv6 <пробел> номер_порта
- IPv6
- CIDR IPv4/IPv6

Каждая строка файла содержит только одну запись, пример для IPv4:

```
78.47.115.34 443
95.211.6.93
95.211.4.0/24
```

CKAT разрешает установку TCP соединения клиентом и ожидает передачи данных. По данным CKAT определяет протокол и в случае HTTP/HTTPS ожидает передачи URL/SNI/CN, для других протоколов осуществляет блокировку передачи данных сразу. Данное поведение связано с тем, что на одном IP адресе может находиться множество доменов и приоритетная проверка по URL/SNI/CN.
С версии 13 добавлена поддержка жестких блокировок (несмотря на имя хоста/SNI) — задается путем добавления кодового слова `hard` в IP лист, пример для IPv4:

```
78.47.115.34 443 hard
95.211.6.93 hard
95.211.4.0/24 hard
```

Конвертирование во внутренний формат:

```
cat my_ip_list.txt|ip2bin my_ip_list.bin
```

В случае задания IP адреса или CIDR блокируются **ТОЛЬКО ВСЕ TCP порты**. Для блокировки UDP портов необходимо включить настройку `udp_block=3` в /etc/dpi/fastdpi.conf