# Netblock DPI



## Возможности

Реализация Netblock DPI базируется на использовании **libnetfilter_queue + nDPI**

Позволяет блокировку следующими методами :

- блокировка по связке **ip:port**
- блокировка по доменному имени **(DNS)**
- блокировка по **URL**
- блокировка **HTTPS**
- блокировка дополнительных портов **(nDPI)**
- производить перенаправление в случае блокировки

## Установка Linux (на примере Debian 9)

- Подготавливаем систему, устанавливаем необходимые библиотеки

```
apt-get zip install autoconf libtool libpoconet46 g++ libnetfilter-acct-dev libnetfilter-conntrack-
dev libnetfilter-cthelper0-dev libnetfilter-cttimeout-dev libnetfilter-log-dev libnetfilter-queue-dev
```

- Скачиваем и устанавливаем nfq

```
wget https://github.com/max197616/nfqfilter/archive/master.zip
unzip master.zip
cd nfqfilter-master
./autogen.sh
./configure
make && make install
cp src/nfqfilter /usr/local/sbin/
touch /var/log/nfqfilter.log
```

- Настраиваем конфиг ( **/etc/nfq/nfq.ini** ), пример :

```
;
queue = 0
;
domainlist = /etc/nfq/domains
;   url
urllist = /etc/nfq/urls
;   ssl
ssllist = /etc/nfq/ssl_host
;   ip:port
hostlist = /etc/nfq/hosts

;
redirect_url = https://127.0.0.1:9443/
;     (nDPI)
protocols = /etc/nfq/protos
;      ,
statistic_interval = 10
;      iptables      ssl  hosts
mark_value = 10
;    (default: 1024)
 max_pending_packets = 100000

[logging]
loggers.root.level = information
;loggers.root.level = debug
loggers.root.channel = fileChannel
channels.fileChannel.class = FileChannel
channels.fileChannel.path = /var/log/nfqfilter.log
channels.fileChannel.rotation = 1 M
channels.fileChannel.archive = timestamp
channels.fileChannel.formatter.class = PatternFormatter
channels.fileChannel.formatter.pattern = %Y-%m-%d %H:%M:%S.%i [%P] %p %s - %t
channels.fileChannel.formatter.times = local
```

- В iptables создаём :

```
iptables -t mangle -N NETBLOCK_DPI
iptables -t mangle -A NETBLOCK_DPI -m connbytes --connbytes-mode bytes --connbytes-dir both --
connbytes 100000 -j RETURN
iptables -t mangle -A NETBLOCK_DPI -p tcp --dport 80 -j NFQUEUE --queue-num 0
iptables -t mangle -A NETBLOCK_DPI -p tcp --dport 443 -j NFQUEUE --queue-num 0

ipset -N NETBLOCK_DPI_SSL
iptables -A FORWARD -m mark --mark 10 =p tcp -j REJECT --reject-with tcp-rst
iptables -A FORWARD -m set --match-set NETBLOCK_DPI_SSL dst -p tcp -j REJECT --reject-with tcp-rst

iptables -t mangle -A PREROUTING -j NETBLOCK_DPI
```

- Запускаем следующим образом (daemonize, PID location, config location) :

```
/usr/local/sbin/nfqfilter --daemon --pidfile=/var/run/nfqfilter.pid -c /etc/nfq/nfq.ini
```

## Использование в связке с Abills

- Скачиваем и инициализируем блок-лист UABlock (например), или настраиваем нужные нам блокировки с помощью админки ( Интер фейс управления ресурсами блокировки )

```
/usr/abills/libexec/billd netblock TYPE=uablock FETCH=1 INIT=1
```

- В конфигурационном файле **/usr/abills/libexec/config.pl** указываем параметры для установленного nfq :

```
#
$conf{NETBLOCK_NFQ_ETC} = "/etc/nfq/"
# restart command line
$conf{NETBLOCK_NFQ_RESTART} = "/usr/local/sbin/nfqfilter --daemon --pidfile=/var/run/nfqfilter.pid -c
/etc/nfq/nfq.ini";
```

- Запускаем блокировку :

```
/usr/abills/libexec/billd netblock TYPE=uablock ACTIVE_BLOCK=1  DPI_BLOCK=1
```