

DPI(Deep Packet Inspection) 3

..... 3

MTU 3

notsodeep 3

..... 3

..... 4

iptables 4

firewalld rule 4

..... 4

zapret 5

zapret clone 5

..... 5

..... 5

..... 6

..... 6

DPI(Deep Packet Inspection)

- <https://secretsni.kilho.net/> - SecretSNI()
- <https://github.com/ValdikSS/GoodbyeDPI> - GoodbyeDPI
- <https://github.com/Include-sys/GUI-for-GoodbyeDPI> - GoodbyeDPI-GUI
- <https://safevisit.org/ko> - SafeVisit


: <https://terzeron.com/confluence/pages/viewpage.action?pageId=34734083>

- Windows GoodbyeDPI GUI for GoodbyeDPI DPI
- Linux DPI , MTU , zapret
notsodeep 가 가
- notsodeep zapret 가 iptables 가
- zapret 가 가

MTU

-
- MTU 220 400 가
◦ https://www.clien.net/service/board/cm_mac/13158762
MTU , 가 220
DPI 가
- ◦ MTU

notsodeep



notsodeep 가 가 .

: <https://github.com/farukuzun/notsodeep>

```
# Debian
sudo apt-get install libnetfilter-queue-dev libc6-dev

# RedHat
yum install libnetfilter_queue-devel compat-glibc
```

```
git clone https://github.com/farukuzun/notsodeep.git
cd notsodeep
make
sudo nohup ./notsodeep &
```

iptables

```
iptables TCP connection handshake NFQUEUE notsodeep
```

```
sudo iptables -A INPUT -p tcp --tcp-flags SYN,ACK SYN,ACK --sport 443 -j
NFQUEUE --queue-num 200 --queue-bypass
sudo iptables -t raw -I PREROUTING -p tcp --sport 80 --tcp-flags SYN,ACK
SYN,ACK -j NFQUEUE --queue-num 200 --queue-bypass
```

```
, -s IP
notsodeep
```

```
sudo iptables -I INPUT -s < IP> -p tcp --tcp-flags SYN,ACK SYN,ACK --
sport 443 -j ACCEPT
```

```
-A -I
```

firewalld rule

```
firewall-cmd --permanent --direct --passthrough ipv4 -I INPUT 1 -p tcp --
tcp-flags SYN,ACK SYN,ACK --sport 443 -j NFQUEUE --queue-num 200 --queue-
bypass
firewall-cmd --permanent --direct --passthrough ipv4 -t raw -I PREROUTING 1
-p tcp --sport 80 --tcp-flags SYN,ACK SYN,ACK -j NFQUEUE --queue-num 200 --
queue-bypass

firewall-cmd --reload
```

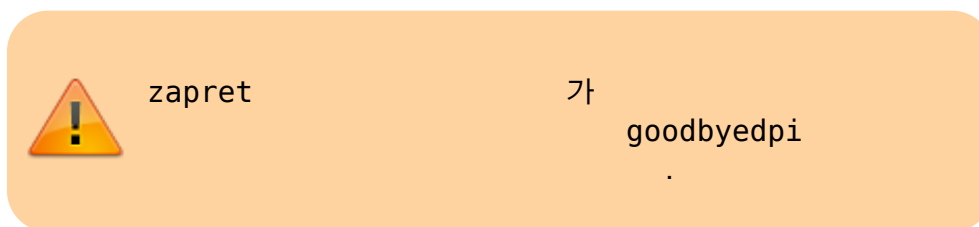
```
cd /tmp
```

```
git clone https://github.com/farukuzun/notsodeep.git
cd notsodeep
make
cd ..
sudo su
cp -R notsodeep /opt
cp /opt/notsodeep/notsodeep.service /etc/systemd/system/
systemctl enable notsodeep.service
iptables -A INPUT -p tcp --tcp-flags SYN,ACK SYN,ACK --sport 443 -j NFQUEUE
--queue-num 200 --queue-bypass
iptables -t raw -I PREROUTING -p tcp --sport 80 --tcp-flags SYN,ACK SYN,ACK
-j NFQUEUE --queue-num 200 --queue-bypass

apt install iptables-persistent

netfilter-persistent save
```

zapret



: <https://github.com/bol-van/zapret>

zapret

clone

```
git clone https://github.com/bol-van/zapret
```

```
apt install lsb-core libnetfilter-queue-dev ipset
```

```
cd zapret
cd nfq
make
cd tpws
make
```

```
sudo cp -r zapret /opt
cd /opt/zapret
sudo cp /opt/zapret/init.d/debian7/zapret /etc/init.d/
sudo /etc/init.d/zapret start
sudo /opt/zapret/nfq/nfqws --daemon --qnum=200 --wsize=4 --hostspell=HoSt --
hostdot --host-tab --hostnospace ...
```

- iptables.txt
 - <https://raw.githubusercontent.com/bol-van/zapret/master/iptables.txt>
- iptables
 - [iptables](#)

window size

- TCP window size (DPI HTTP 가 TCP)

```
sudo nfqws
iptables -t raw -I PREROUTING -p tcp --sport 80 --tcp-flags SYN,ACK SYN,ACK
-j NFQUEUE --queue-num 200 --queue-bypass
iptables -t raw -I PREROUTING -p tcp --sport 80 --tcp-flags SYN,ACK SYN,ACK
-m set --match-set zapret src -j NFQUEUE --queue-num 200 --queue-bypass
```

Host:

- Host: host: DPI (DPI 가)

```
sudo nfqws
iptables -t mangle -I POSTROUTING -p tcp --dport 80 -j NFQUEUE --queue-num
200 --queue-bypass
iptables -t mangle -I POSTROUTING -p tcp --dport 80 -m set --match-set
zapret dst -j NFQUEUE --queue-num 200 --queue-bypass
iptables -t mangle -I POSTROUTING -p tcp --dport 80 -m set --match-set
zapret dst -m connbytes --connbytes-dir=original --connbytes-mode=packets --
connbytes 1:5 -j NFQUEUE --queue-num 200 --queue-bypass
```

TPROXY

```
sysctl -w net.ipv4.ip_forward=1
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

ip -f inet rule add fwmark 1 lookup 100
ip -f inet route add local default dev lo table 100

# prevent loop
iptables -t filter -I INPUT -p tcp --dport 1188 -j REJECT
iptables -t mangle -A PREROUTING -i eth1 -p tcp --dport 80 -j MARK --set-mark 1
iptables -t mangle -A PREROUTING -i eth1 -p tcp --dport 80 -j TPROXY --tproxy-mark 0x1/0x1 --on-port 1188

iptables -t mangle -A PREROUTING -i eth1 -p tcp --dport 80 -m set --match-set zapret dst -j MARK --set-mark 1
iptables -t mangle -A PREROUTING -i eth1 -p tcp --dport 80 -m mark --mark 0x1/0x1 -j TPROXY --tproxy-mark 0x1/0x1 --on-port 1188
```

DNAT

```
# run tpws as user "tpws". its required to avoid loops.
sudo -u tpws
sysctl -w net.ipv4.conf.eth1.route_localnet=1
iptables -t nat -I PREROUTING -p tcp --dport 80 -j DNAT --to 127.0.0.1:1188
iptables -t nat -I OUTPUT -p tcp --dport 80 -m owner ! --uid-owner tpws -j DNAT --to 127.0.0.1:1188
```

From:

<https://atl.kr/dokuwiki/> - AllThatLinux!

Permanent link:

https://atl.kr/dokuwiki/doku.php/dpi_deep_packet_inspection_%EC%9A%B0%ED%9A%8C?rev=1667707631

Last update: 2022/11/06 04:07

