목차

DPI(Deep Packet Inspection) 우회 3
관련프로그램 3
MTU 조정 방법 3
notsodeep을 이용한 방법 3
라이브러리 의존성 설치 3
바이너리 빌드 4
iptables 규칙 적용 4
firewalld rule 4
서비스등록 형식 4
zapret을 이용한 방법(추천) 5
필요 패키지 설치 5
zapret 프로젝트를 clone받음 5
ISP체크 5
설치 6

DPI(Deep Packet Inspection) 우회

관련프로그램

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

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

- Windows에서는 `GoodbyeDPI`나 `GUI for GoodbyeDPI` 패키지를 이용하면 손쉽게 DPI를 우회할 수 있음
- Linux에서는 쉽게 DPI를 우회할 수 있는 방법이 없으나, MTU를 조정하는 방법, `zapret`을 이용한 방법과 `notsodeep`을 이용한 방법 등이 존재하므로 세 가지 중 한 가지를 선택해서 사용하면 됨
- `notsodeep`과 `zapret` 두 가지 방법 모두 `iptables`의 라우팅 규칙을 이용하고 있음
- `zapret`의 경우 기술문서가 러시아어로 작성되어 있어서 적용에 주의가 필요함

MTU 조정 방법

- 이 방법은 시스템에 충격을 줄 수 있기 때문에 권장하는 방법이 아님
- 우선 MTU 크기를 `220` 또는 `400` 정도의 값으로 조정하는 방법으로 우회 가능한지 확인해볼 것
  - https://www.clien.net/service/board/cm_mac/13158762에 언급된 내용에 따르면 브라우저마다 MTU 값이 다르게 요구된다고 하는데, 가장 성능이 낮게 나오긴 하지만 220으로 설정하면 어지간한 DPI는 우회 가능함
- 다음 문서를 참조할 것
  - 강제로 네트웍 인터페이스의 MTU 조정하기

notsodeep을 이용한 방법

> `notsodeep`은 업데이트가 중지된지 오래되어 현재는 정상적으로 우회되지 않는경우가 많다.

참고: https://github.com/farukuzun/notsodeep

라이브러리 의존성 설치

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

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

바이너리 빌드

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

iptables 규칙 적용

iptables로 TCP connection handshake의 패킷들을 NFQUEUE 응용프로그램인 notsodeep에서 처리할 수 있도록 넘기는 규칙을 적용함

```
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
```

특정 서버와의 통신인 경우에는, -s 옵션을 이용하여 서버 IP를 적어주면 그 서버와의 통신에 대해서만 적용됨 특정 서버를 notsodeep으로 필터링하지 않는 예외 규칙을 적용하려면 다음 명령을 사용할 수 있음

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

-A 옵션 대신 -I 옵션을 사용하여 규칙 테이블 맨 위에 등록해두는 것이 중요함

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
```

서비스등록 형식

```
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
```

zapret을 이용한 방법(추천)

zapret은 현재까지도 업데이트가 꾸준히 이루어지고 있으며 다양한 방법으로 우회시도를 하므로 goodbyedpi와 더불어 아주 잘 동작하는 솔루션 중에 하나이다.

링크 : https://github.com/bol-van/zapret

아래 내용은 debian 11버전에서 테스트 되었습니다.

필요 패키지 설치

```
root@dpi:~# apt install vim unzip git curl wget
```

zapret 프로젝트를 clone받음

```
root@dpi:~# git clone https://github.com/bol-van/zapret
Cloning into 'zapret'...
remote: Enumerating objects: 4171, done.
remote: Counting objects: 100% (782/782), done.
remote: Compressing objects: 100% (416/416), done.
remote: Total 4171 (delta 370), reused 769 (delta 365), pack-reused 3389
Receiving objects: 100% (4171/4171), 41.13 MiB | 8.24 MiB/s, done.
Resolving deltas: 100% (2208/2208), done.
```

ISP체크

일단 현재 본인의 ISP에서 차단을 우회하는 방식을 찾아야 한다. 먼저 `zapret` 바이너리 실행파일을 설치한 이후 `blockcheck.sh` 로 차단방식을 찾아서 우회하는 방법을 알아낸다.

```
root@dpi:~# cd zapret/
root@dpi:~/zapret# ./install_bin.sh
x86_64 is OK
installing binaries ...
linking : ../binaries/x86_64/ip2net => /root/zapret/ip2net
linking : ../binaries/x86_64/mdig => /root/zapret/mdig
linking : ../binaries/x86_64/nfqws => /root/zapret/nfq
linking : ../binaries/x86_64/tpws => /root/zapret/tpws


### 본인의 ISP에서 차단/우회 되는 방식을 체크한다.
root@dpi:~/zapret# ./blockcheck.sh
...
* SUMMARY
ipv4 xvideos.com curl_test_http : tpws --hostcase
ipv4 xvideos.com curl_test_http : nfqws --hostcase
ipv4 xvideos.com curl_test_https_tls12 : working without bypass

press enter to continue
```

체크가 될때 사이트 주소는 본인 ISP에서 warning으로 차단되는 사이트 아무거나 넣어주면 된다. 위 테스트는 `xvideos.com`으로 테스트 한 결과이다. SUMMARY에 나온대로 `tpws --hostcase`나 `nfqws --hostcase`방식을 이용하면 우회가 가능하다.

설치

이후 이전 과정에서 확인한 우회 방식으로 설치를 진행한다.

```
root@dpi:~/zapret# ./install_easy.sh
```

이후 해당 사이트로 우회 접근 되는지 확인해보도록 한다.

From:
https://atl.kr/dokuwiki/ - **AllThatLinux!**

Permanent link:
https://atl.kr/dokuwiki/doku.php/dpi_deep_packet_inspection_%EC%9A%B0%ED%9A%8C

Last update: **2023/02/02 02:19**