# Firewall Evasion Lab: Bypassing Firewalls using VPN

2018级 信息安全 管箫 18307130012

## Task 1: VM Setup

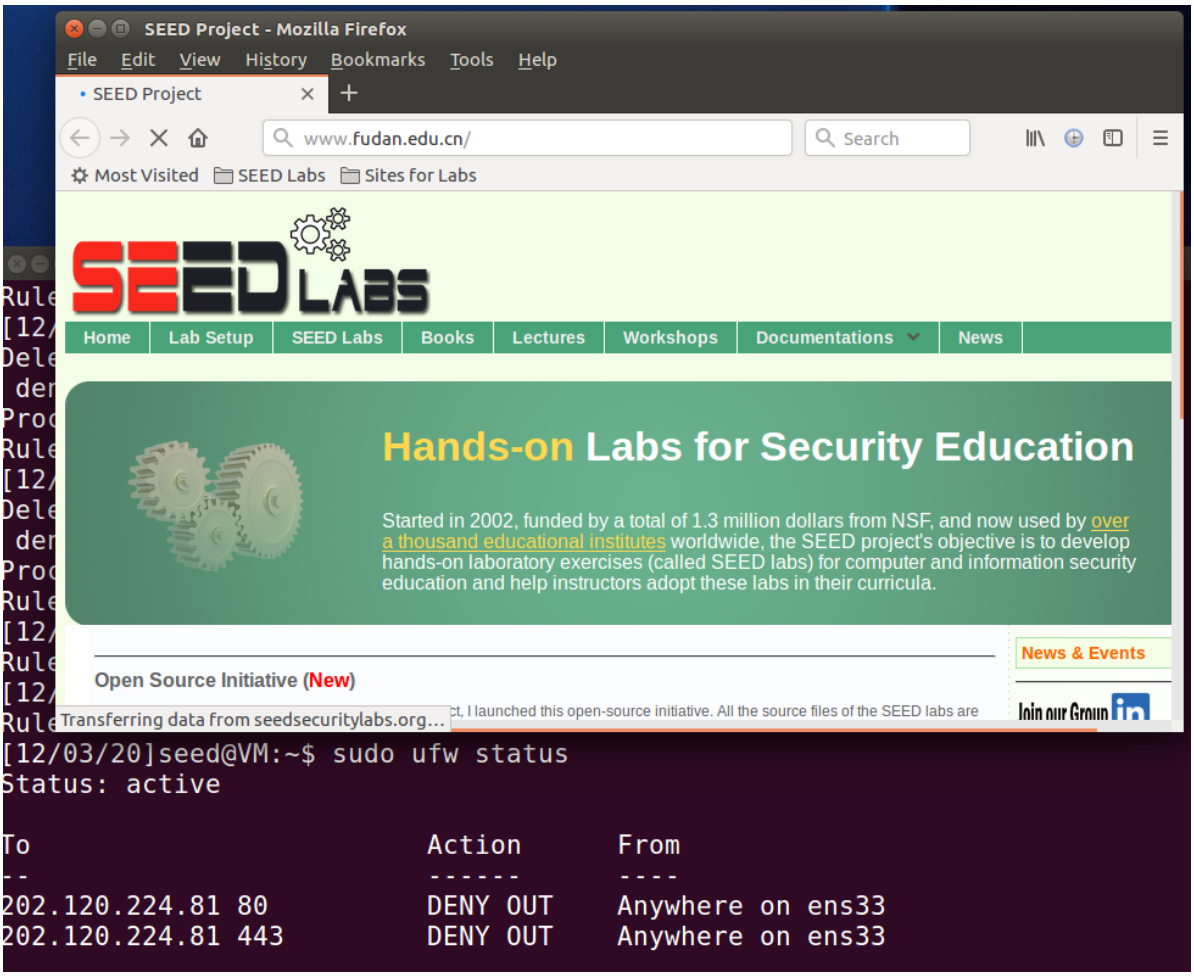
### VM1:

ip：192.168.61.138；mac：00:0c:29:01:41:ae

### VM2:

ip：192.168.61.139；mac：00:0c:29:a3:8a:e6

## Task 2: Set up Firewall




`sudo ufw deny out on ens33 to 202.120.224.81 port 80`

`sudo ufw deny out on ens33 to 202.120.224.81 port 443`

## Task 3: Bypassing Firewall using VPN

## Step 1: Run VPN Server

```
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
-00
          inet addr:192.168.53.1  P-t-P:192.168.53.1  Mask:255.255.255.0
          inet6 addr: fe80::4bd5:1a25:5152:29e1/64 Scope:Link
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

[12/03/20]seed@VM:~$ $ sudo sysctl net.ipv4.ip_forward=1
$: command not found
[12/03/20]seed@VM:~$ sudo sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
```

## Step 2: Run VPN Client.

```
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-0
-00
          inet addr:192.168.53.5  P-t-P:192.168.53.5  Mask:255.255.255
          inet6 addr: fe80::3e8:7098:c38:6bc7/64 Scope:Link
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:48 (48.0 B)
```

## Step 3: Set Up Routing on Client and Server VMs.

### 在Client端

```
sudo route add -net 202.120.224.0/24 tun0
```

## Step 4: Set Up NAT on Server VM.

| | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 6454 | 2020-12-03 23:09:51.6982706… | 202.120.224.81 | 192.168.53.5 | TCP | 1516 | [TCP segment of a reassembled PD… |
| 6455 | 2020-12-03 23:09:51.6982755… | 192.168.53.5 | 202.120.224.81 | TCP | 56 | 35776 → 443 [ACK] Seq=408356182 … |
| 6456 | 2020-12-03 23:09:51.6982833… | 192.168.61.138 | 192.168.61.139 | UDP | 84 | 39266 → 55555 Len=40 |
| 6457 | 2020-12-03 23:09:51.6983015… | 202.120.224.81 | 192.168.53.5 | TCP | 1456 | [TCP segment of a reassembled PD… |
| 6458 | 2020-12-03 23:09:51.6983086… | 202.120.224.81 | 192.168.53.5 | TLSv1.2 | 1516 | Application Data[TCP segment of … |
| 6459 | 2020-12-03 23:09:51.6983122… | 192.168.53.5 | 202.120.224.81 | TCP | 56 | 35776 → 443 [ACK] Seq=408356182 … |
| 6460 | 2020-12-03 23:09:51.6983175… | 192.168.61.138 | 192.168.61.139 | UDP | 84 | 39266 → 55555 Len=40 |
| 6461 | 2020-12-03 23:09:51.6984760… | 192.168.61.139 | 192.168.61.138 | UDP | 1516 | 55555 → 39266 Len=1500 |
| 6462 | 2020-12-03 23:09:51.6984791… | 192.168.61.139 | 192.168.61.138 | IPv4 | 64 | Fragmented IP protocol (proto=UD… |
| 6463 | 2020-12-03 23:09:51.6984988… | 192.168.61.139 | 192.168.61.138 | UDP | 1417 | 55555 → 39266 Len=1373 |
| 6464 | 2020-12-03 23:09:51.6985029… | 192.168.61.139 | 192.168.61.138 | UDP | 1516 | 55555 → 39266 Len=1500 |
| 6465 | 2020-12-03 23:09:51.6985053… | 192.168.61.139 | 192.168.61.138 | IPv4 | 64 | Fragmented IP protocol (proto=UD… |
| 6466 | 2020-12-03 23:09:51.6985078… | 192.168.61.139 | 192.168.61.138 | UDP | 1516 | 55555 → 39266 Len=1500 |
| 6467 | 2020-12-03 23:09:51.6985092… | 192.168.61.139 | 192.168.61.138 | IPv4 | 64 | Fragmented IP protocol (proto=UD… |
| 6468 | 2020-12-03 23:09:51.6985121… | 192.168.61.139 | 192.168.61.138 | UDP | 1516 | 55555 → 39266 Len=1500 |
| 6469 | 2020-12-03 23:09:51.6985135… | 192.168.61.139 | 192.168.61.138 | IPv4 | 64 | Fragmented IP protocol (proto=UD… |
| 6470 | 2020-12-03 23:09:51.6985178… | 192.168.61.139 | 192.168.61.138 | UDP | 1516 | 55555 → 39266 Len=1500 |
| 6471 | 2020-12-03 23:09:51.6985192… | 192.168.61.139 | 192.168.61.138 | IPv4 | 64 | Fragmented IP protocol (proto=UD… |
| 6472 | 2020-12-03 23:09:51.6985218… | 192.168.61.139 | 192.168.61.138 | UDP | 1516 | 55555 → 39266 Len=1500 |
| 6473 | 2020-12-03 23:09:51.6985233… | 192.168.61.139 | 192.168.61.138 | IPv4 | 64 | Fragmented IP protocol (proto=UD… |
| 6474 | 2020-12-03 23:09:51.6985258… | 192.168.61.139 | 192.168.61.138 | UDP | 1357 | 55555 → 39266 Len=1313 |
| 6475 | 2020-12-03 23:09:51.6989360… | 202.120.224.81 | 192.168.53.5 | TCP | 1516 | [TCP segment of a reassembled PD… |
| 6476 | 2020-12-03 23:09:51.6989589… | 202.120.224.81 | 192.168.53.5 | TCP | 1389 | [TCP segment of a reassembled PD… |
| 6477 | 2020-12-03 23:09:51.6989672… | 192.168.53.5 | 202.120.224.81 | TCP | 56 | 35776 → 443 [ACK] Seq=408356182 … |
| 6478 | 2020-12-03 23:09:51.6989789… | 192.168.61.138 | 192.168.61.139 | UDP | 84 | 39266 → 55555 Len=40 |
| 6479 | 2020-12-03 23:09:51.6990874… | 202.120.224.81 | 192.168.53.5 | TCP | 1516 | [TCP segment of a reassembled PD… |
| 6480 | 2020-12-03 23:09:51.6990986… | 202.120.224.81 | 192.168.53.5 | TCP | 1516 | [TCP segment of a reassembled PD… |
| 6481 | 2020-12-03 23:09:51.6991038… | 192.168.53.5 | 202.120.224.81 | TCP | 56 | 35776 → 443 [ACK] Seq=408356182 … |

### 包路径：

对于202.120.224.81，包的通信目的ip是192.168.53.5。

而这实际上是由202.120.224.81先发到Server，Server再由192.168.53.1转发到192.168.53.5，也即Client上。