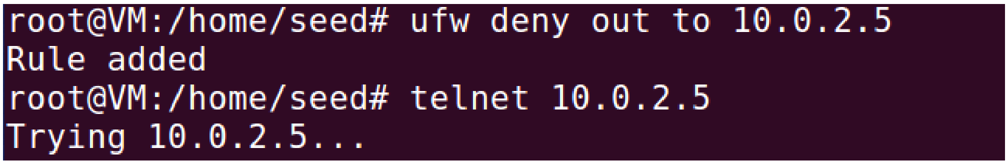
lab6

1. Linux Firewall Exploration Lab

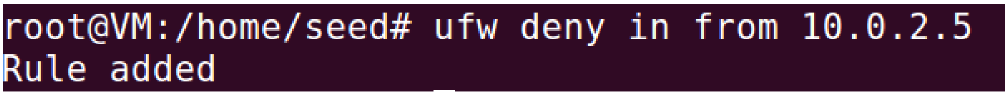
1.1. Task 1: Using Firewall

1. Prevent A from doing telnet to Machine B

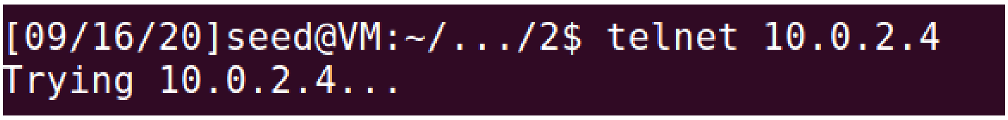


```
root@VM:/home/seed# ufw deny out to 10.0.2.5
Rule added
root@VM:/home/seed# telnet 10.0.2.5
Trying 10.0.2.5...
```

2. Prevent B from doing telnet to Machine A



```
root@VM:/home/seed# ufw deny in from 10.0.2.5
Rule added
```



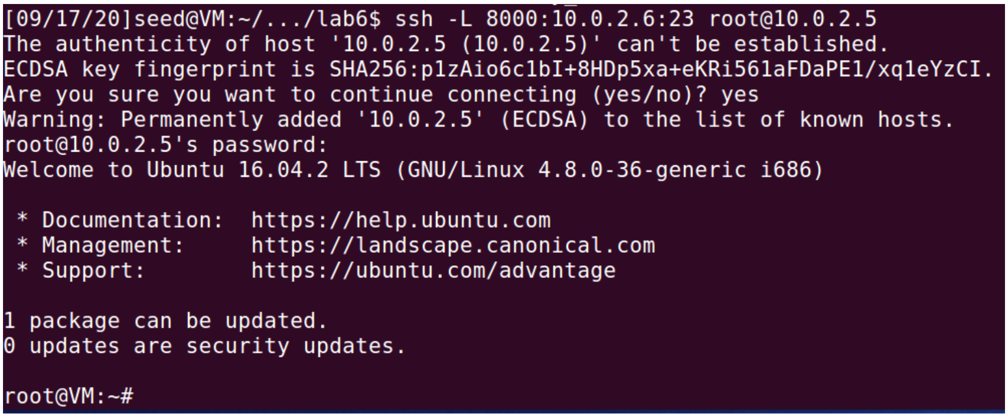
```
[09/16/20]seed@VM:~/.../2$ telnet 10.0.2.4
Trying 10.0.2.4...
```

3. Prevent A from visiting an external web site

1.2. Task 2: Implementing a Simple Firewall

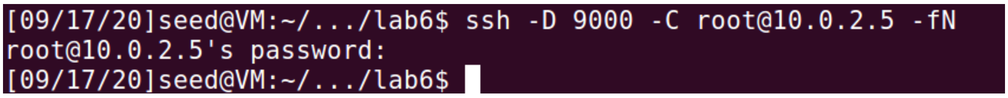
1.3. Task 3: Evading Egress Filtering

1. Task 3.a: Telnet to Machine B through the firewall

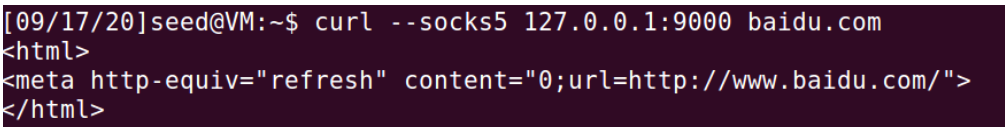


```
[09/17/20]seed@VM:~/.../lab6$ ssh -L 8000:10.0.2.6:23 root@10.0.2.5
The authenticity of host '10.0.2.5 (10.0.2.5)' can't be established.
ECDSA key fingerprint is SHA256:p1zAio6c1bI+8HDp5xa+eKRi561aFDaPE1/xq1eYzCI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.5' (ECDSA) to the list of known hosts.
root@10.0.2.5's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

1 package can be updated.
0 updates are security updates.

root@VM:~#
```

2. Task 3.b: Connect to Facebook using SSH Tunnel.



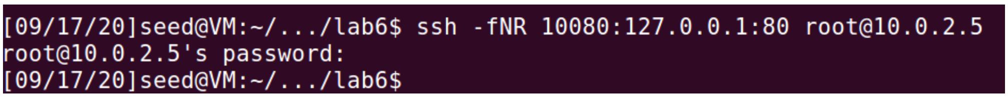
```
[09/17/20]seed@VM:~/.../lab6$ ssh -D 9000 -C root@10.0.2.5 -fN
root@10.0.2.5's password:
[09/17/20]seed@VM:~/.../lab6$
```



```
[09/17/20]seed@VM:~$ curl --socks5 127.0.0.1:9000 baidu.com
<html>
<meta http-equiv="refresh" content="0;url=http://www.baidu.com/">
</html>
```

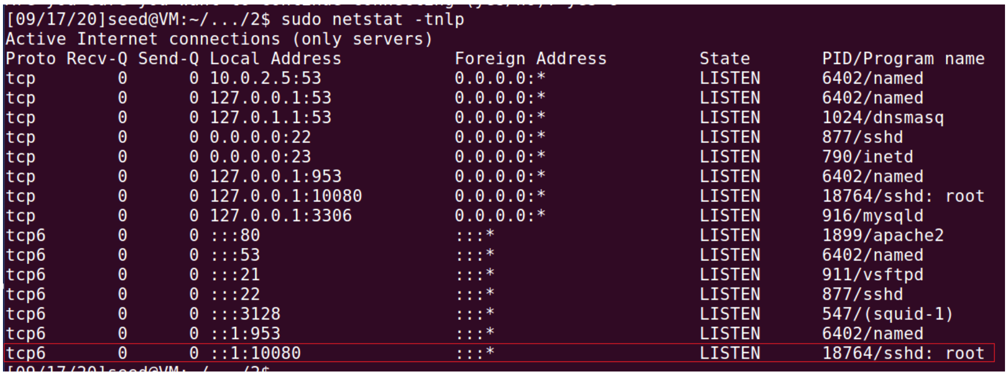
1.4. Task 4: Evading Ingress Filtering

这里实际上是一个正向代理，也就是将本地的端口映射到远程机器上。换而言之，A可以将本地的80端口映射到B的10080端口上，此时B只需访问本地的10080端口，即可访问到运行在A上的web server。



```
[09/17/20]seed@VM:~/.../lab6$ ssh -fNR 10080:127.0.0.1:80 root@10.0.2.5
root@10.0.2.5's password:
[09/17/20]seed@VM:~/.../lab6$
```

A机器



```
[09/17/20]seed@VM:~/.../2$ sudo netstat -tnlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 10.0.2.5:53             0.0.0.0:*               LISTEN      6402/named
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      6402/named
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN      1024/dnsmasq
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      877/sshd
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN      790/inetd
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN      6402/named
tcp        0      0 127.0.0.1:10080         0.0.0.0:*               LISTEN      18764/sshd: root
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      916/mysqld
tcp6       0      0 :::80                   :::*                    LISTEN      1899/apache2
tcp6       0      0 :::53                   :::*                    LISTEN      6402/named
tcp6       0      0 :::21                   :::*                    LISTEN      911/vsftpd
tcp6       0      0 :::22                   :::*                    LISTEN      877/sshd
tcp6       0      0 :::3128                 :::*                    LISTEN      547/(squid-1)
tcp6       0      0 ::1:953                 :::*                    LISTEN      6402/named
tcp6       0      0 ::1:10080               :::*                    LISTEN      18764/sshd: root
```

B机器

2. Firewall Evasion Lab: Bypassing Firewalls using VPN

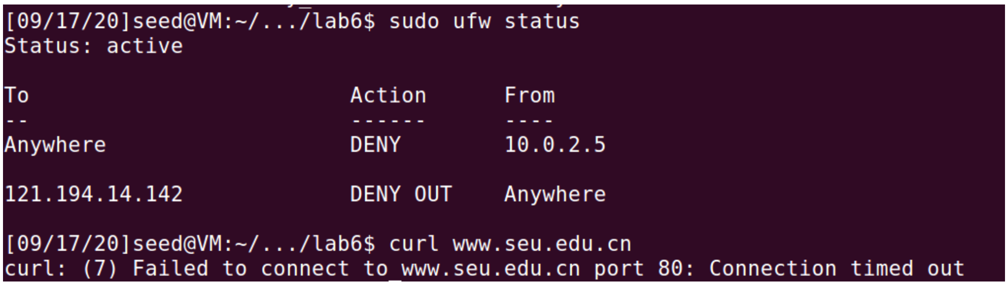
2.1. Task 1: VM Setup

本次实验使用两台VM，分别是：

1. VM1，处于防火墙里，扮演vpn客户端，IP地址为10.0.2.4
2. VM2，处于防护墙外，搬运vpn服务端，IP地址为10.0.2.5

2.2. Task 2: Set up Firewall

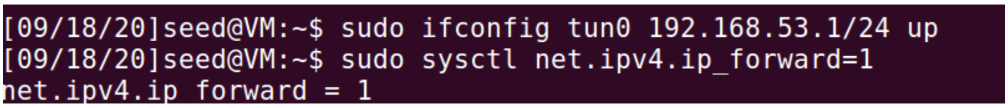
在VM1上，使用防火墙屏蔽`www.seu.edu.cn`的网址，通过curl进行测试可知，在vm1上确实无法连接`www.seu.edu.cn`。



```
[09/17/20]seed@VM:~/.../lab6$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
Anywhere                   DENY        10.0.2.5

121.194.14.142             DENY OUT    Anywhere

[09/17/20]seed@VM:~/.../lab6$ curl www.seu.edu.cn
curl: (7) Failed to connect to www.seu.edu.cn port 80: Connection timed out
```

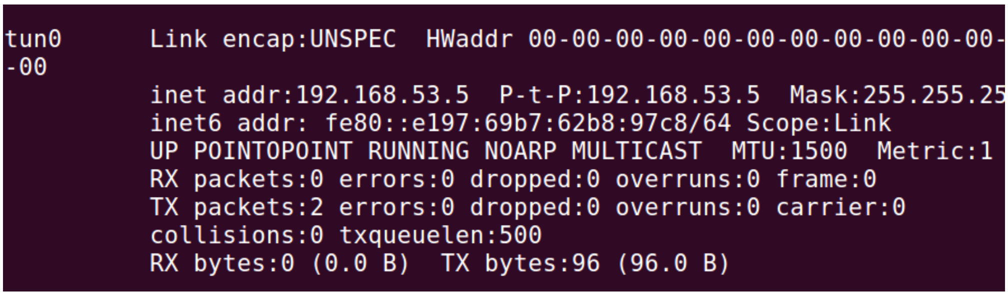
2.3. Task 3: Bypassing Firewall using VPN

1. Step 1: Run VPN Server.



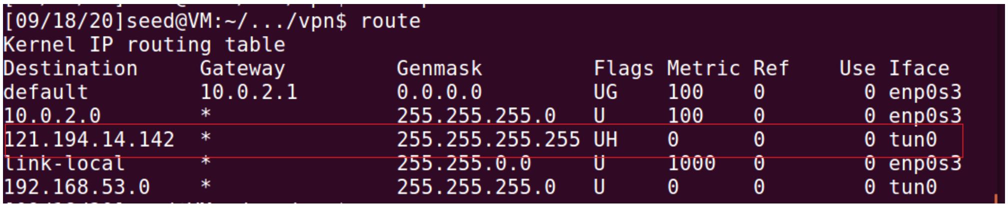
```
[09/18/20]seed@VM:~$ sudo ifconfig tun0 192.168.53.1/24 up
[09/18/20]seed@VM:~$ sudo sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
```

2. Step 2: Run VPN Client.



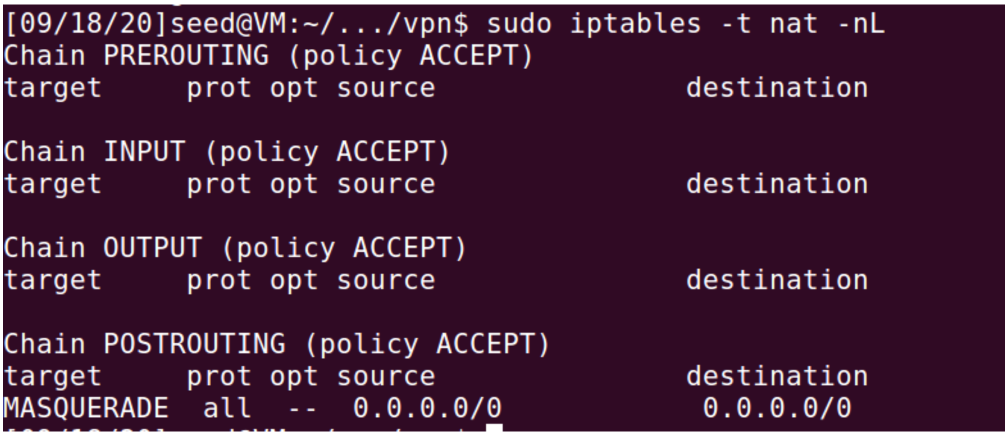
```
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-
-00
          inet addr:192.168.53.5  P-t-P:192.168.53.5  Mask:255.255.25
          inet6 addr: fe80::e197:69b7:62b8:97c8/64 Scope:Link
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:96 (96.0 B)
```

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



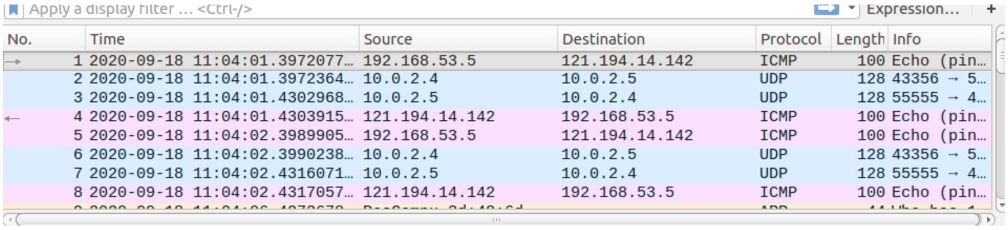
```
[09/18/20]seed@VM:~/.../vpn$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.0.2.1        0.0.0.0         UG    100    0        0 enp0s3
10.0.2.0        *               255.255.255.0   U     100    0        0 enp0s3
121.194.14.142  *               255.255.255.255 UH    0      0        0 tun0
link-local      *               255.255.0.0     U     1000   0        0 enp0s3
192.168.53.0    *               255.255.255.0   U     0      0        0 tun0
```

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



```
[09/18/20]seed@VM:~/.../vpn$ sudo iptables -t nat -nL
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  0.0.0.0/0            0.0.0.0/0
```

5. Demonstration



No.	Time	Source	Destination	Protocol	Length	Info
1	2020-09-18 11:04:01.3972077…	192.168.53.5	121.194.14.142	ICMP	100	Echo (pin…
2	2020-09-18 11:04:01.3972364…	10.0.2.4	10.0.2.5	UDP	128	43356 → 5…
3	2020-09-18 11:04:01.4302968…	10.0.2.5	10.0.2.4	UDP	128	55555 → 4…
4	2020-09-18 11:04:01.4303915…	121.194.14.142	192.168.53.5	ICMP	100	Echo (pin…
5	2020-09-18 11:04:02.3989905…	192.168.53.5	121.194.14.142	ICMP	100	Echo (pin…
6	2020-09-18 11:04:02.3990238…	10.0.2.4	10.0.2.5	UDP	128	43356 → 5…
7	2020-09-18 11:04:02.4316071…	10.0.2.5	10.0.2.4	UDP	128	55555 → 4…
8	2020-09-18 11:04:02.4317057…	121.194.14.142	192.168.53.5	ICMP	100	Echo (pin…

去程：192.168.53.5 -> 121.194.14.142

回程：121.194.14.142 -> 192.168.53.5

这证明vpn的确发挥了效果。