CIS 410

Assignment 6

Qianyi Feng

Setting Up Your VM:

For the set up part, I modified the .yaml file at first, then on Thursday's class, Luke and Erric told us how to modified the file correctly, which was to use `ip link` command to find the name of the new ethernet interface enp0s8, and assign the IP address below:

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT
 group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mo
de DEFAULT group default qlen 1000
    link/ether 08:00:27:ae:3d:41 brd ff:ff:ff:ff:ff:ff
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mo
de DEFAULT group default qlen 1000
    link/ether 08:00:27:58:95:17 brd ff:ff:ff:ff:ff:ff
```

```
# This file is generated from information provided by
# the datasource.  Changes to it will not persist across an instance.
# To disable cloud-init's network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
    ethernets:
        enp0s3:
            addresses: []
            dhcp4: true
        enp0s8:
            dhcp4: no
            dhcp6: no
            addresses: [192.168.73.10/24]
            nameservers:
                addresses: [127.0.0.53, 8.8.8.8]
                search: [cs.uoregon.edu]
    version: 2
```

After that, I used ping command to ping to other classmates' ip address, which got success.

Managing Routing Table on your VM:

For this exercise, I used `route -n` command:

```
btmp begins Fri Feb  1 09:00:17 2019
[osboxes@osboxes:~$ ip route
default via 10.0.2.2 dev enp0s3 proto dhcp src 10.0.2.15 metric 100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15
10.0.2.2 dev enp0s3 proto dhcp scope link src 10.0.2.15 metric 100
192.168.73.0/24 dev enp0s8 proto kernel scope link src 192.168.73.10
osboxes@osboxes:~$
```

```
[osboxes@osboxes:~$ sudo route -n
[sudo] password for osboxes:
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.2.2        0.0.0.0         UG    100    0        0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     0      0        0 enp0s3
10.0.2.2        0.0.0.0         255.255.255.255 UH    100    0        0 enp0s3
192.168.73.0    0.0.0.0         255.255.255.0   U     0      0        0 enp0s8
osboxes@osboxes:~$
```

From the routing table, the interface enp0s3 routes to two gateways and has three destination, while the interface enp0s8 has only one destination, which is the assigned ip address, and one gateway 0.0.0.0.

Firewall configuration NAT/IPTables:

Blacklisting all Traffic: For this exercise, I used the command `iptables -P INPUT DROP.` Then I cannot ssh to my VM from my local machine, and the VM runs really slow. After I `ACCEPT` the traffic, the ssh works.

```
Chain INPUT (policy DROP)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
osboxes@osboxes:~$
```

Whitelisting benign traffic: For this exercise, I tried to block Zahra's ip address and only allowed her to ssh to my VM. I have tried the command on this website:

https://unix.stackexchange.com/questions/11851/iptables-allow-certain-ips-and-block-all-other-connection

After setting the iptables with these commands, I asked Zahra to ssh to my VM, and she succeed. Also, when I tried to ping my VM from my local machine, I was refused.

```
[tengqianyideMacBook-Pro:~ tengqianyi$ ping 192.168.73.10
PING 192.168.73.10 (192.168.73.10): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
Request timeout for icmp_seq 5
Request timeout for icmp_seq 6
Request timeout for icmp_seq 7
Request timeout for icmp_seq 8
```

Logging firewall events:

For this exercise, I have tried the commands from this website:

https://unix.stackexchange.com/questions/405550/how-to-log-only-iptables-messages-into-my-var-log-iptables-log

Firstly, I modified the /etc/rsyslog.conf file, then add the "kern.* /var/log/iptables.log" at the end. Then I reload the configuration with the restart command, and used the command "iptables -A INPUT -j LOG —log-prefix 'iptables'", and then cat the /var/log/iptables.log file:

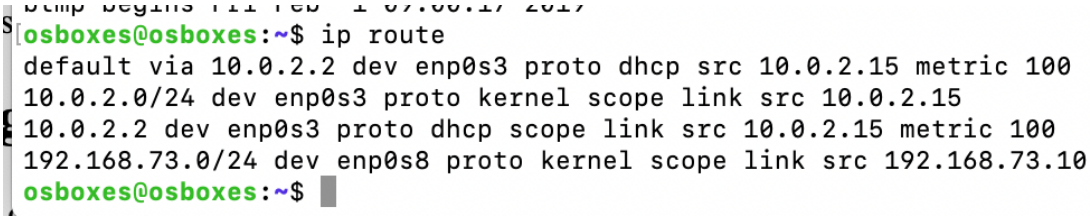
```
Feb 16 06:15:37 osboxes kernel: [ 2017.882749] iptablesIN=enp0s3 OUT= MAC=08:00:
27:ae:3d:41:52:54:00:12:35:02:08:00 SRC=10.0.2.2 DST=10.0.2.15 LEN=40 TOS=0x00 P
REC=0x00 TTL=64 ID=1997 PROTO=TCP SPT=62634 DPT=22 WINDOW=42112 RES=0x00 ACK URG
P=0
Feb 16 06:15:37 osboxes kernel: [ 2017.882755] iptablesIN=enp0s3 OUT= MAC=08:00:
27:ae:3d:41:52:54:00:12:35:02:08:00 SRC=10.0.2.2 DST=10.0.2.15 LEN=40 TOS=0x00 P
REC=0x00 TTL=64 ID=1998 PROTO=TCP SPT=62634 DPT=22 WINDOW=40900 RES=0x00 ACK URG
P=0
Feb 16 06:15:37 osboxes kernel: [ 2017.882992] iptablesIN=enp0s3 OUT= MAC=08:00:
27:ae:3d:41:52:54:00:12:35:02:08:00 SRC=10.0.2.2 DST=10.0.2.15 LEN=40 TOS=0x00 P
REC=0x00 TTL=64 ID=1999 PROTO=TCP SPT=62634 DPT=22 WINDOW=39440 RES=0x00 ACK URG
P=0
Feb 16 06:15:37 osboxes kernel: [ 2017.883000] iptablesIN=enp0s3 OUT= MAC=08:00:
27:ae:3d:41:52:54:00:12:35:02:08:00 SRC=10.0.2.2 DST=10.0.2.15 LEN=40 TOS=0x00 P
REC=0x00 TTL=64 ID=2000 PROTO=TCP SPT=62634 DPT=22 WINDOW=37980 RES=0x00 ACK URG
P=0
Feb 16 06:15:37 osboxes kernel: [ 2017.883006] iptablesIN=enp0s3 OUT= MAC=08:00:
27:ae:3d:41:52:54:00:12:35:02:08:00 SRC=10.0.2.2 DST=10.0.2.15 LEN=40 TOS=0x00 P
REC=0x00 TTL=64 ID=2001 PROTO=TCP SPT=62634 DPT=22 WINDOW=36768 RES=0x00 ACK URG
P=0
```

Configuring Your VM as an Internet Gateway For Another VM:

I have tried command from the website and created the NAT.sh files for making the FORWARD status into ACCEPT, and start NAT on enp0s3 interface:

http://blog.sina.com.cn/s/blog_7285600f0100ru05.html

However, I and my partner had not enough time to test if the set up is correct due to the time limit.



Also, if I am the client, I would modify my gateway as my partner's ip address in *.yaml file.