Antonio Shields
CYSE 270
April 14, 2023
Lab 12 - Advanced Network configurations

Scenario: You, as a network admin, are going to set up your Ubuntu VM as a gateway to provide Internet access to another client Ubuntu VM. The client VM needs to be in the same internal network as the gateway (**as shown in Figure 1**). Once the connection is ready, you need to configure the firewall to secure the network properly. The following requirements need to be satisfied to receive full credits.

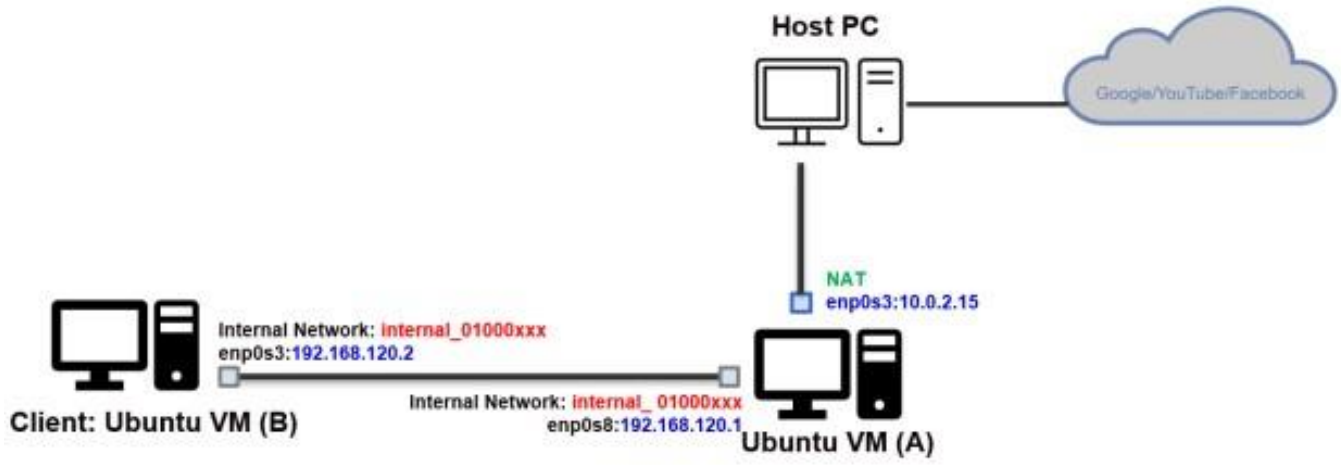


Figure 1 Desired Network Topology

Please note that you need to customize the value in the fields marked in RED above.

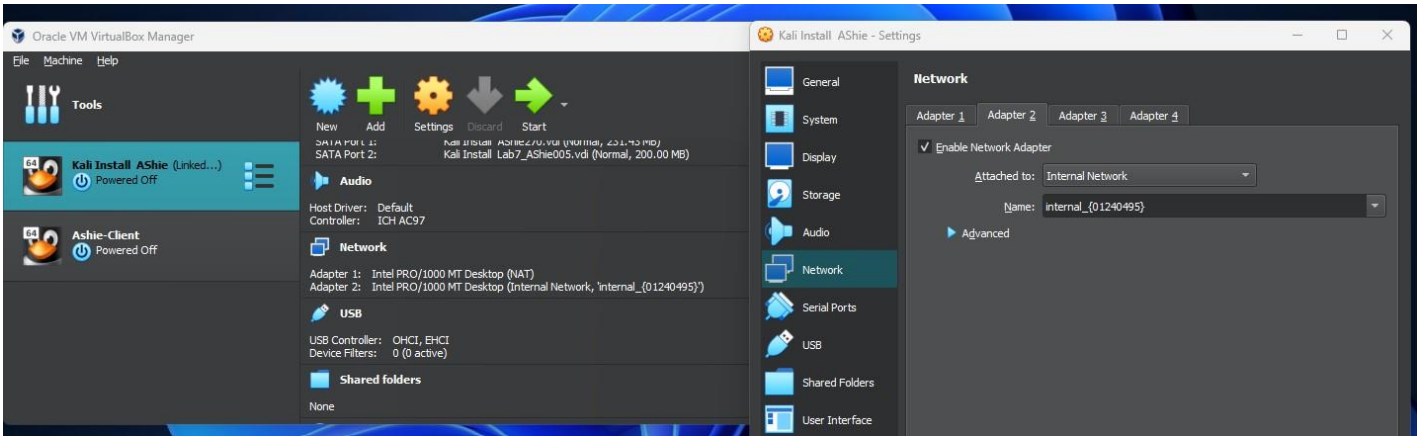
Please configure the network with the following requirement: (You need to clone the existing VM)

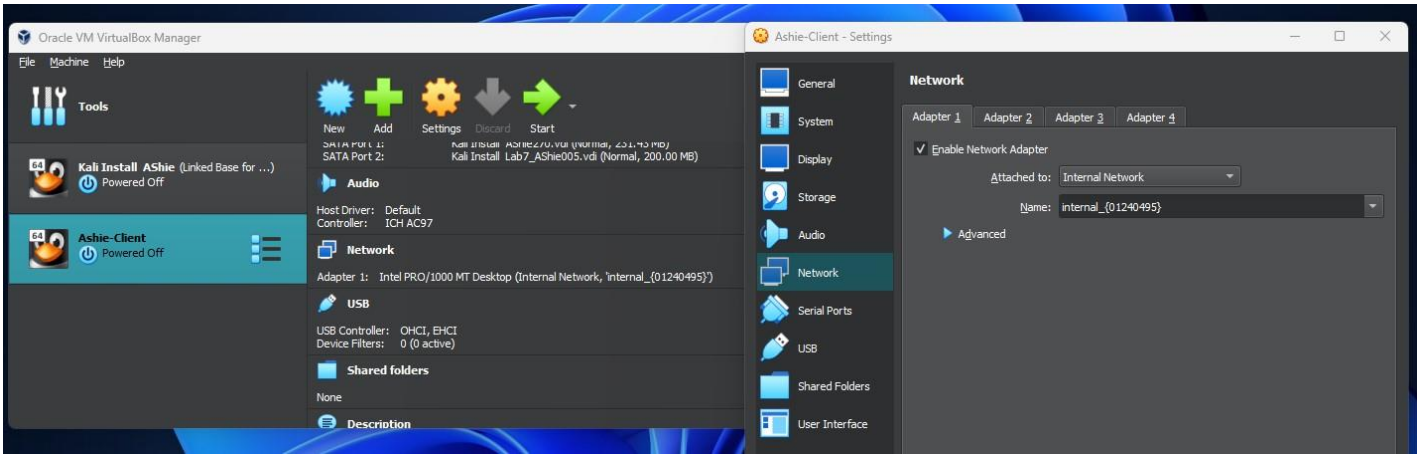
Task A –Network Configuration (**60 points**)

Please submit the screenshot for all the steps.

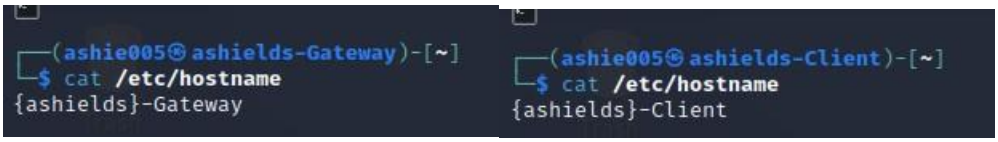
1. In the virtual box setting, connect two VMs in the same internal network, “internal_{UIN}”.

Replace {UIN} with your real UIN.

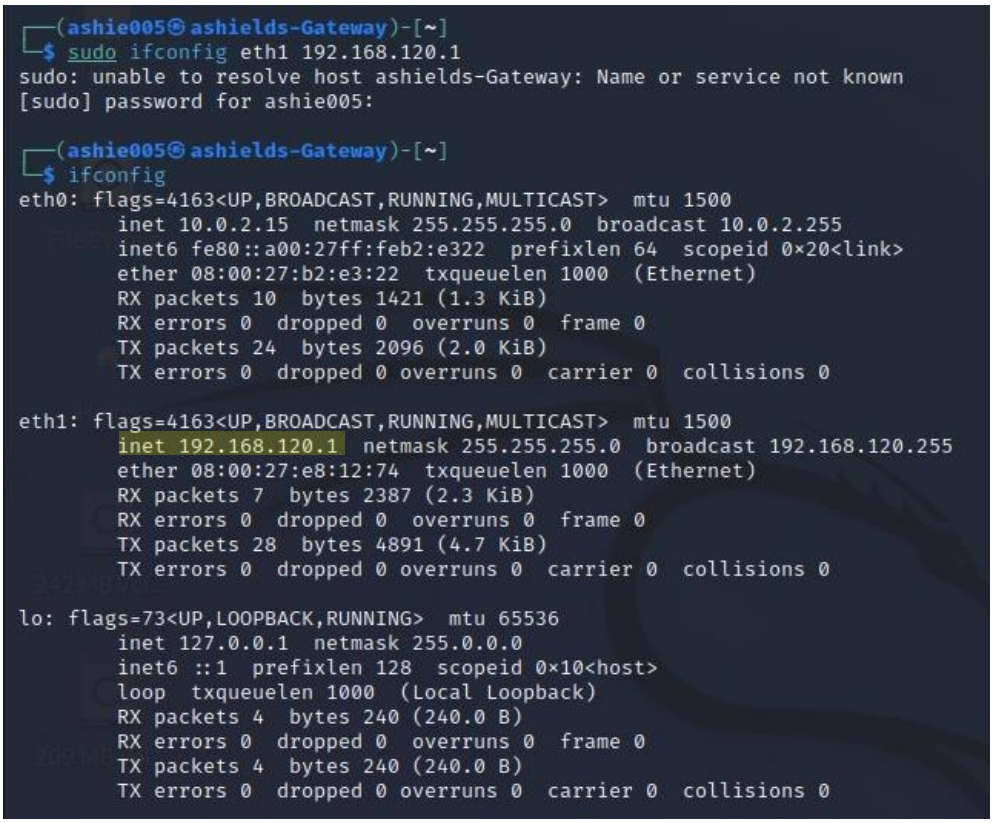




2. Change the hostname of the Client VM to “{MIDASname}-Client.” **Replace {MIDAS name} with your real MIDAS name.**

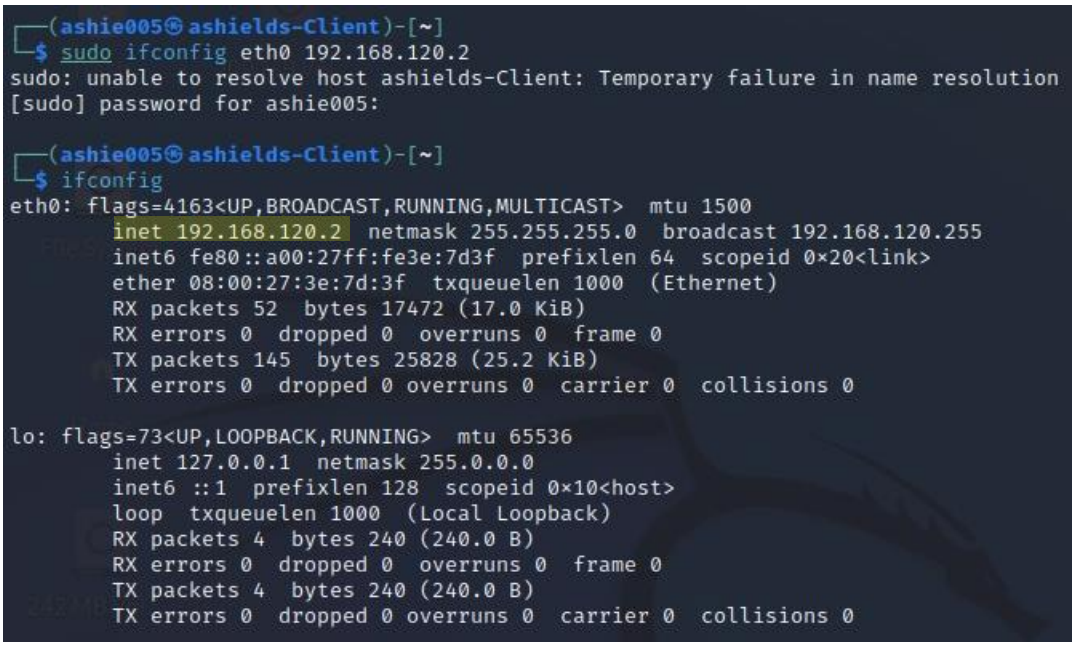


3. Configure the temporary IP address on the Gateway Ubuntu, as shown in Figure 1.



4. Configure the temporary IP address, routing table, and DNS server on Client VM as shown in Figure 1.

Temporary IP address:



Routing Table:

```
┌──(ashie005㉿ashields-Client)-[~]
└─$ sudo ip route add 192.168.120.0/24 dev eth0
sudo: unable to resolve host ashields-Client: Temporary failure in name resolution

┌──(ashie005㉿ashields-Client)-[~]
└─$ sudo ip route add default via 192.168.120.1
sudo: unable to resolve host ashields-Client: Temporary failure in name resolution

┌──(ashie005㉿ashields-Client)-[~]
└─$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.120.1   0.0.0.0         UG    0      0        0 eth0
192.168.120.0   0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

DNS Server:

```
┌──(ashie005㉿ashields-Client)-[~]
└─$ cat /etc/resolv.conf
# Generated by NetworkManager
search mynetworksettings.com
nameserver 8.8.8.8
```

5. Configure gateway Ubuntu to enable IP forwarding (to forward the traffic) (also NAT configuration)

```
┌──(ashie005㉿ashields-Gateway)-[~]
└─$ sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
sudo: unable to resolve host ashields-Gateway: Name or service not known
[sudo] password for ashie005:

┌──(ashie005㉿ashields-Gateway)-[~]
└─$ sudo iptables -A FORWARD -i eth0 -o eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT
sudo: unable to resolve host ashields-Gateway: Name or service not known

┌──(ashie005㉿ashields-Gateway)-[~]
└─$ sudo iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
sudo: unable to resolve host ashields-Gateway: Name or service not known

┌──(ashie005㉿ashields-Gateway)-[~]
└─$ su root
Password:
┌──(root㉿ashields-Gateway)-[/home/ashie005]
└─# echo 1 > /proc/sys/net/ipv4/ip_forward

┌──(root㉿ashields-Gateway)-[/home/ashie005]
└─# cat /proc/sys/net/ipv4/ip_forward
1
```

6. Test your ping connection to 8.8.8.8 and www.google.com in the client VM, respectively.

```
┌──(ashie005㉿ashields-Client)-[~]
└─$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=58 time=21.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=58 time=130 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=58 time=19.2 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=58 time=22.6 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=58 time=17.8 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=58 time=22.2 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=58 time=22.5 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=58 time=17.2 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=58 time=19.4 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=58 time=121 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=58 time=20.5 ms
^C
── 8.8.8.8 ping statistics ──
11 packets transmitted, 11 received, 0% packet loss, time 10226ms
rtt min/avg/max/mdev = 17.171/39.409/129.672/40.639 ms

┌──(ashie005㉿ashields-Client)-[~]
└─$ ping www.google.com
PING www.google.com (142.250.31.147) 56(84) bytes of data.
64 bytes from bj-in-f147.1e100.net (142.250.31.147): icmp_seq=1 ttl=106 time=14.7 ms
64 bytes from bj-in-f147.1e100.net (142.250.31.147): icmp_seq=2 ttl=106 time=20.5 ms
64 bytes from bj-in-f147.1e100.net (142.250.31.147): icmp_seq=3 ttl=106 time=17.1 ms
64 bytes from bj-in-f147.1e100.net (142.250.31.147): icmp_seq=4 ttl=106 time=19.2 ms
64 bytes from bj-in-f147.1e100.net (142.250.31.147): icmp_seq=5 ttl=106 time=17.9 ms
64 bytes from bj-in-f147.1e100.net (142.250.31.147): icmp_seq=6 ttl=106 time=22.9 ms
64 bytes from bj-in-f147.1e100.net (142.250.31.147): icmp_seq=7 ttl=106 time=48.7 ms
64 bytes from bj-in-f147.1e100.net (142.250.31.147): icmp_seq=8 ttl=106 time=19.7 ms
64 bytes from bj-in-f147.1e100.net (142.250.31.147): icmp_seq=9 ttl=106 time=18.3 ms
64 bytes from bj-in-f147.1e100.net (142.250.31.147): icmp_seq=10 ttl=106 time=16.2 ms
64 bytes from bj-in-f147.1e100.net (142.250.31.147): icmp_seq=11 ttl=106 time=18.8 ms
^C
── www.google.com ping statistics ──
11 packets transmitted, 11 received, 0% packet loss, time 10028ms
rtt min/avg/max/mdev = 14.689/21.278/48.744/8.933 ms
```

Task B –Firewall Configuration (**40 points**)

1. Configure the iptables on the gateway Ubuntu to block all the inbound ICMP packets from the Client VM.

```
┌──(ashie005㉿ashields-Gateway)-[~]
└─$ sudo iptables -A INPUT -s 192.168.120.2 -p icmp -j DROP
sudo: unable to resolve host ashields-Gateway: Name or service not known
[sudo] password for ashie005:
```

Additional Ping Test on Client

```
┌──(ashie005㉿ashields-Client)-[~]
└─$ ping 192.168.120.1
PING 192.168.120.1 (192.168.120.1) 56(84) bytes of data.
^C
── 192.168.120.1 ping statistics ──
104 packets transmitted, 0 received, 100% packet loss, time 106256ms
```

Additional Deleted IP TABLES to unblock ICMP traffic

```
┌──(ashie005㉿ashields-Gateway)-[~]
└─$ sudo iptables -D INPUT 1
sudo: unable to resolve host ashields-Gateway: Name or service not known
```

Additional Ping Test to ensure unblock of ICMP

```
┌──(ashie005㉿ashields-Client)-[~]
└─$ ping 192.168.120.1
PING 192.168.120.1 (192.168.120.1) 56(84) bytes of data.
64 bytes from 192.168.120.1: icmp_seq=1 ttl=64 time=0.876 ms
64 bytes from 192.168.120.1: icmp_seq=2 ttl=64 time=2.02 ms
64 bytes from 192.168.120.1: icmp_seq=3 ttl=64 time=1.21 ms
^C
── 192.168.120.1 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2014ms
rtt min/avg/max/mdev = 0.876/1.367/2.021/0.481 ms
```

2. Configure the iptables on the gateway Ubuntu to block all the outbound ICMP packets that originated from the gateway Ubuntu itself.

```
┌──(ashie005㉿ashields-Gateway)-[~]
└─$ sudo iptables -A OUTPUT -s 10.0.2.15 -p icmp -j DROP
sudo: unable to resolve host ashields-Gateway: Name or service not known
```

Additional Ping test to 8.8.8.8 and www.google.com

```
┌──(ashie005㉿ashields-Gateway)-[~]
└─$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
── 8.8.8.8 ping statistics ──
13 packets transmitted, 0 received, 100% packet loss, time 12567ms


┌──(ashie005㉿ashields-Gateway)-[~]
└─$ ping www.google.com
PING www.google.com (142.251.163.104) 56(84) bytes of data.
^C
── www.google.com ping statistics ──
10 packets transmitted, 0 received, 100% packet loss, time 9596ms
```

Additional configured iptables for 192.168.120.1 outbound and Ping Test to 192.168.120.2

```
┌──(ashie005㉿ashields-Gateway)-[~]
└─$ sudo iptables -A OUTPUT -s 192.168.120.1 -p icmp -j DROP
sudo: unable to resolve host ashields-Gateway: Name or service not known
[sudo] password for ashie005:

┌──(ashie005㉿ashields-Gateway)-[~]
└─$ ping 192.168.120.2
PING 192.168.120.2 (192.168.120.2) 56(84) bytes of data.
^C
── 192.168.120.2 ping statistics ──
10 packets transmitted, 0 received, 100% packet loss, time 9218ms
```

Extra credit:

Set the permanent IP address on the Client Ubuntu based on the above network topology.

```
┌──(ashie005㉿ashields-Client)-[~]
└─$ cat /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
        address 192.168.120.2
        netmask 255.255.255.0
        gateway 192.168.120.1
```

```
┌──(ashie005㉿ashields-Client)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.120.2  netmask 255.255.255.0  broadcast 192.168.120.255
        inet6 fe80::a00:27ff:fe3e:7d3f  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:3e:7d:3f  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 17  bytes 2494 (2.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```