IT 620 – Wireless Network Security & Administration

Project Title : FIREWALL

Submitted by:
Rutuja Bendre (rb264)

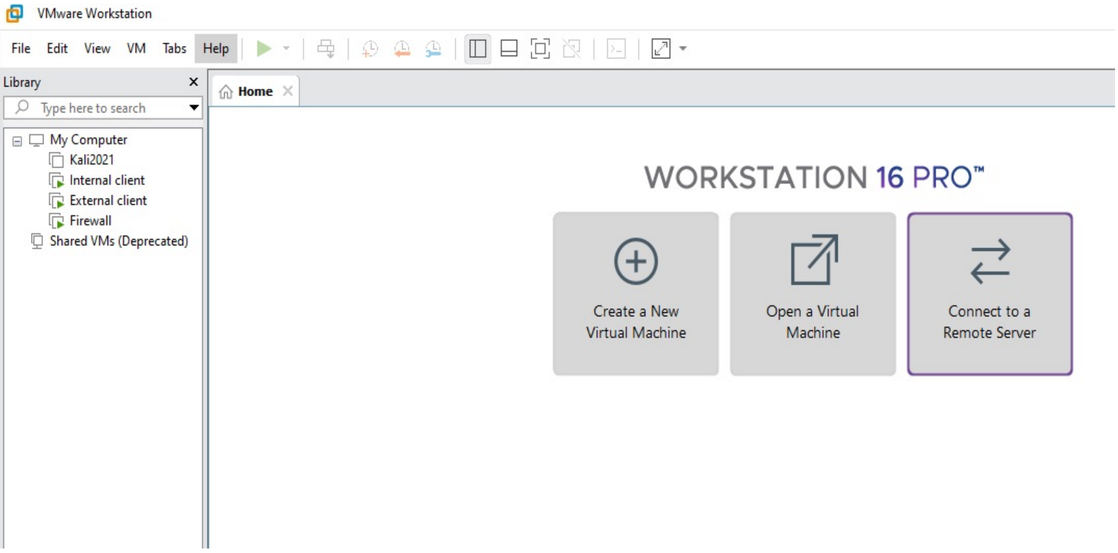
The given project is to build a firewall in Linux using any one of the open source firewall. The project begins by downloading and installing the below mentioned tools on the hardware system.

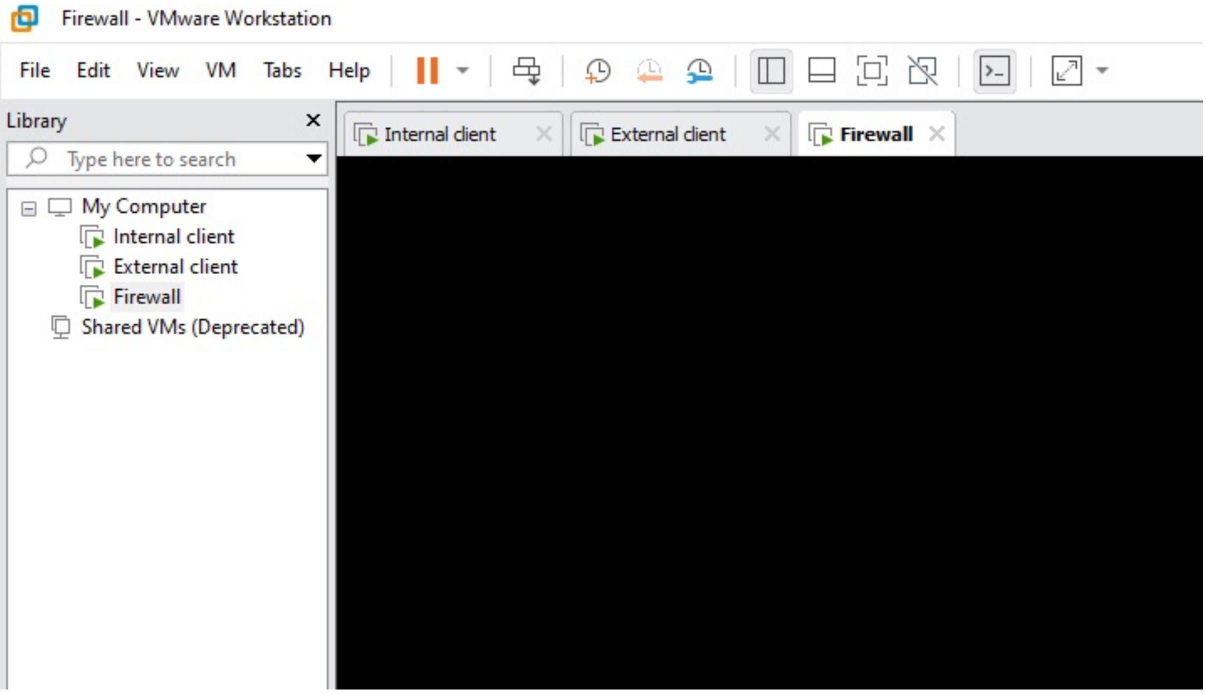
1. VMware Pro 16
2. Firewall - Uncomplicated Firewall (UFW)

Steps involved:

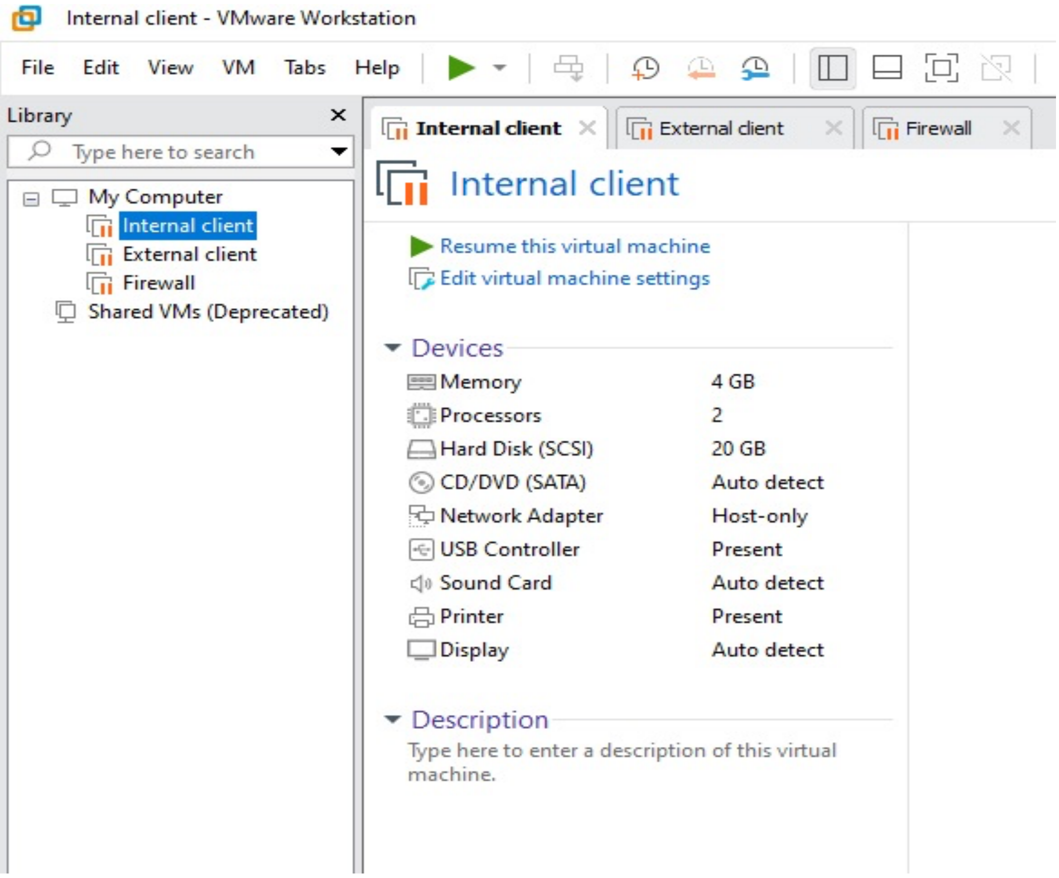
1. Three Linux based virtual machines are installed:
    a. Firewall - a virtual machine that has to be considered while setting up the Uncomplicated firewall.
    b. Internal Client (Ubuntu)
    c. External client (Ubuntu)

The above mentioned Virtual machines are created by using the disc image for





2. Configuring the network settings: After adding two adapters to the hosts network manager of the Virtual machine, two NIC's are added to the firewall. The adapter 1 and adapter 2 blocks are attached to Host-only adapter #2 and #3 respectively.

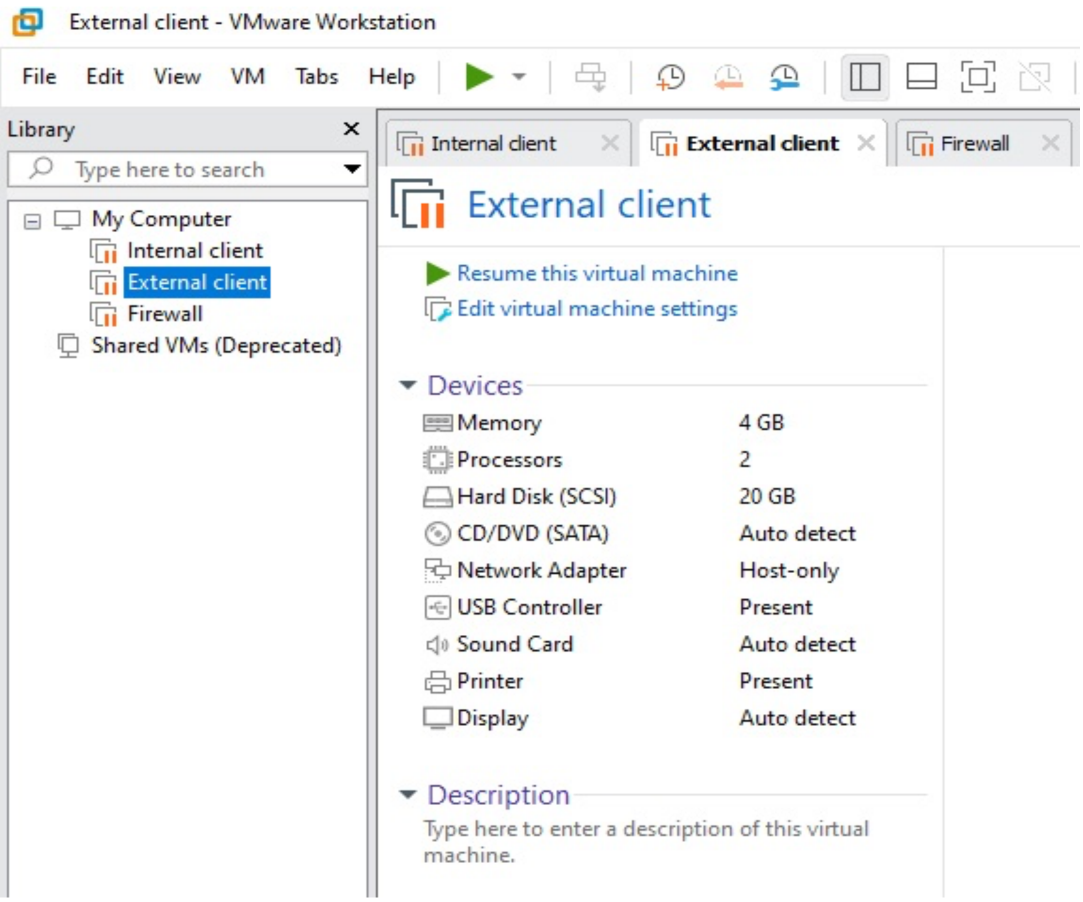


Devices

Memory	4 GB
Processors	2
Hard Disk (SCSI)	20 GB
CD/DVD (SATA)	Auto detect
Network Adapter	Host-only
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Description

Type here to enter a description of this virtual machine.



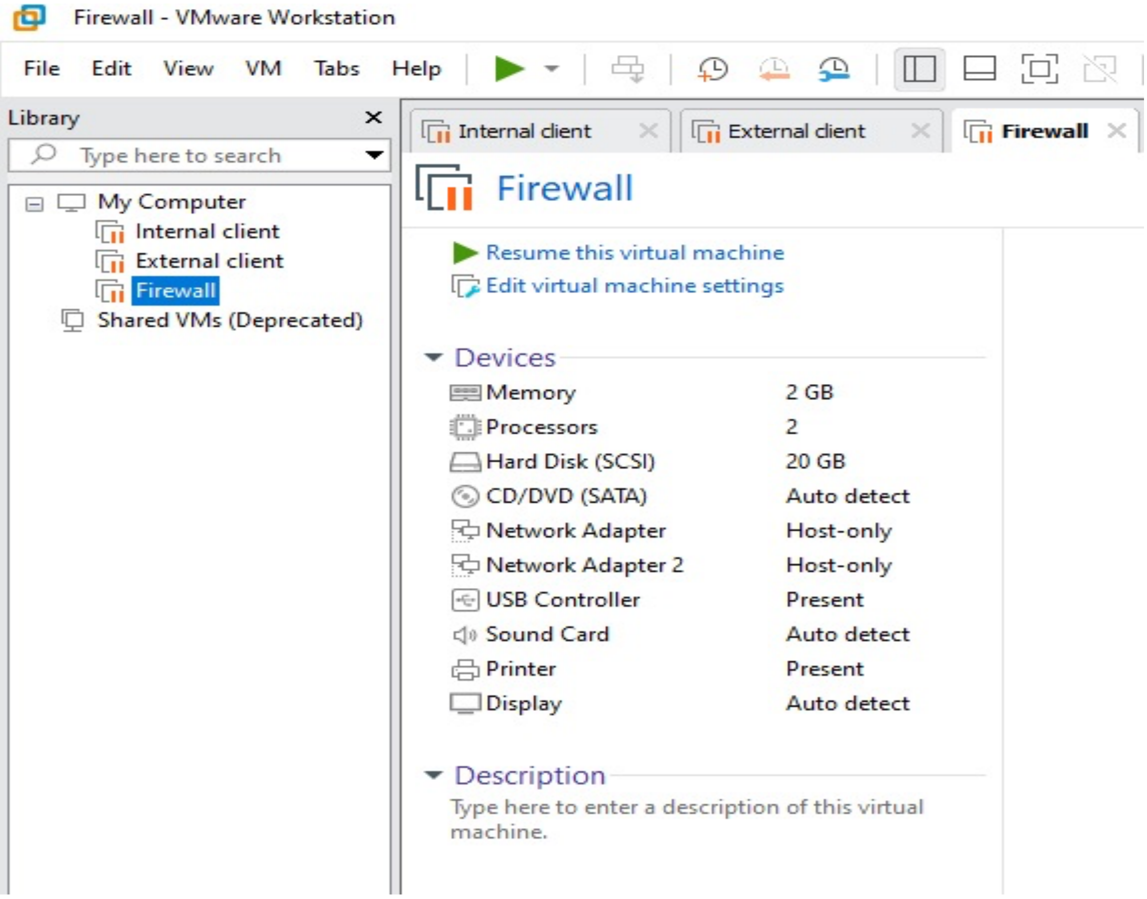
External client

Devices

Memory	4 GB
Processors	2
Hard Disk (SCSI)	20 GB
CD/DVD (SATA)	Auto detect
Network Adapter	Host-only
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Description

Type here to enter a description of this virtual machine.



Firewall

Devices

Memory	2 GB
Processors	2
Hard Disk (SCSI)	20 GB
CD/DVD (SATA)	Auto detect
Network Adapter	Host-only
Network Adapter 2	Host-only
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

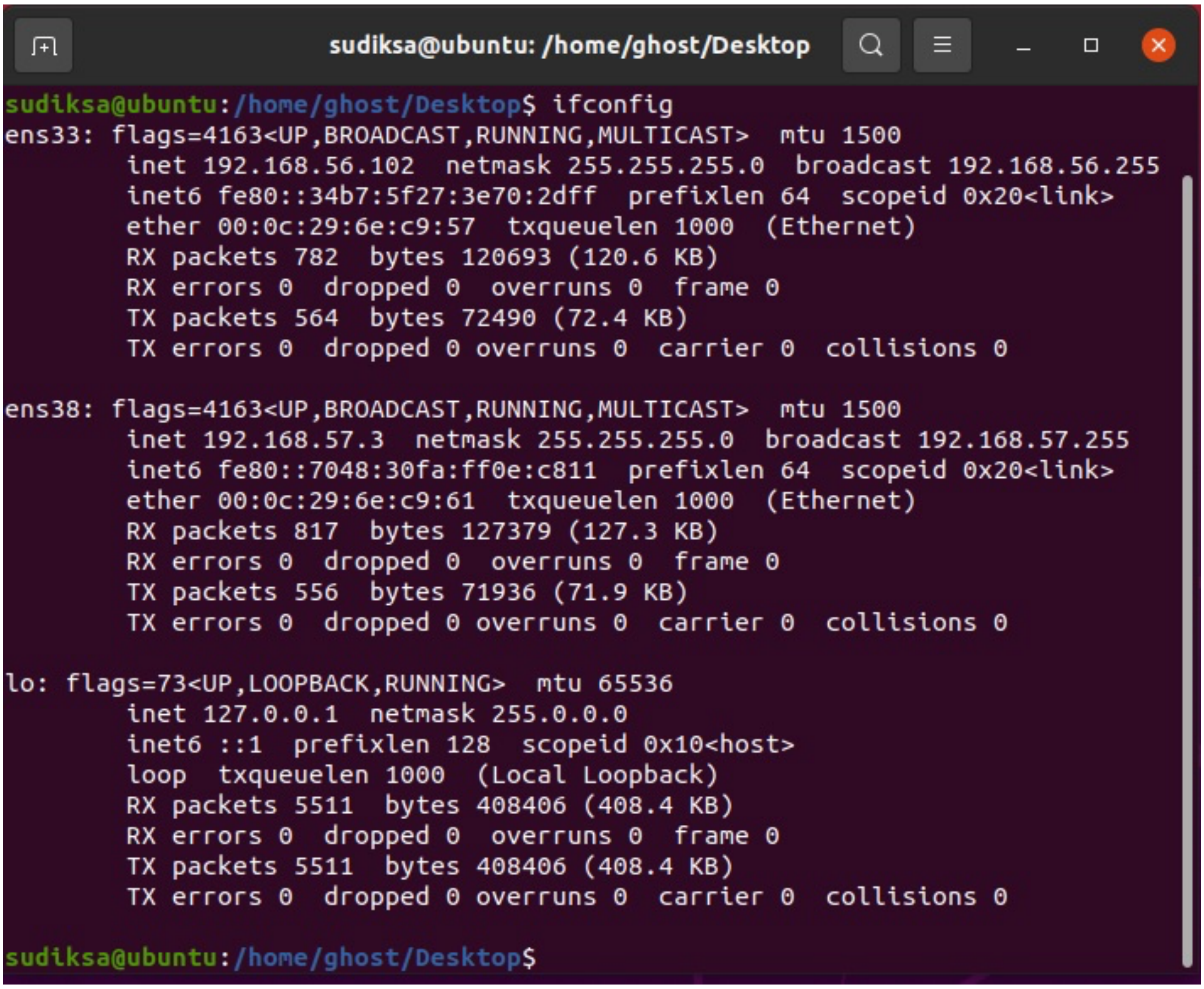
Description

Type here to enter a description of this virtual machine.

3. After initiating the firewall, the IP addresses of the NIC's should be checked. In order to do this, the command "ifconfig" is executed in the terminal window.

The IP's of the two network adapters are:

ens33 -
ens38 -



```
sudiksa@ubuntu:/home/ghost/Desktop$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::34b7:5f27:3e70:2dff  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:6e:c9:57  txqueuelen 1000  (Ethernet)
        RX packets 782  bytes 120693 (120.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 564  bytes 72490 (72.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens38: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.57.3  netmask 255.255.255.0  broadcast 192.168.57.255
        inet6 fe80::7048:30fa:ff0e:c811  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:6e:c9:61  txqueuelen 1000  (Ethernet)
        RX packets 817  bytes 127379 (127.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 556  bytes 71936 (71.9 KB)
        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 5511  bytes 408406 (408.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5511  bytes 408406 (408.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

sudiksa@ubuntu:/home/ghost/Desktop$
```

IP address of internal and external client virtual machines:

External Client :
Internal Client :

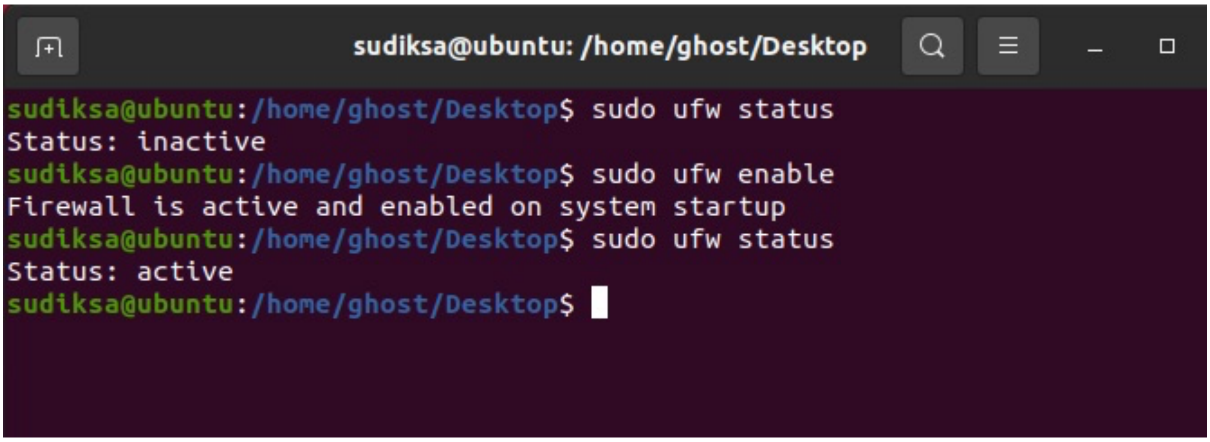
----

4. This step involves enabling of uncomplicated firewall (UFW) in ubuntu 16.04. Sometimes, the firewall is by default not enabled, so there are a few steps to enable it. The ufw will be enabled in the Virtual machine named Firewall . In the terminal window the following commands are executed:

To turn UFW on with the default set of rules:
$ sudo ufw enable

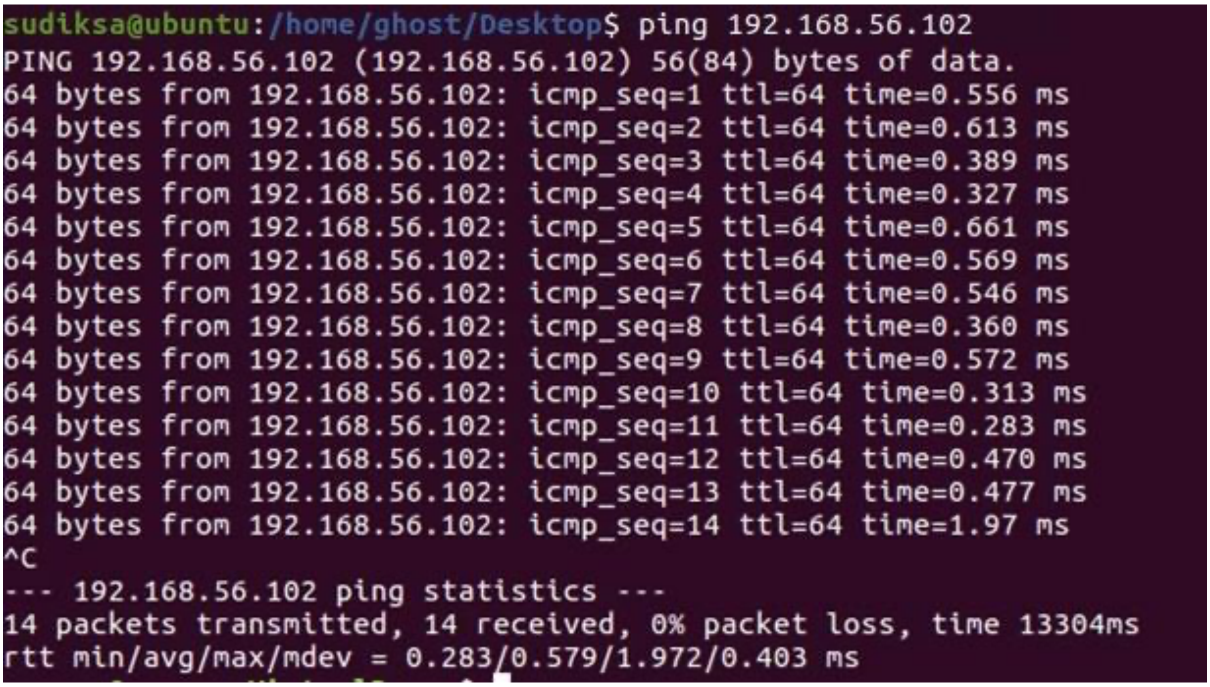
And if UFW is not installed :
$ sudo apt-get install ufw

To check the status of UFW:
$ sudo ufw status

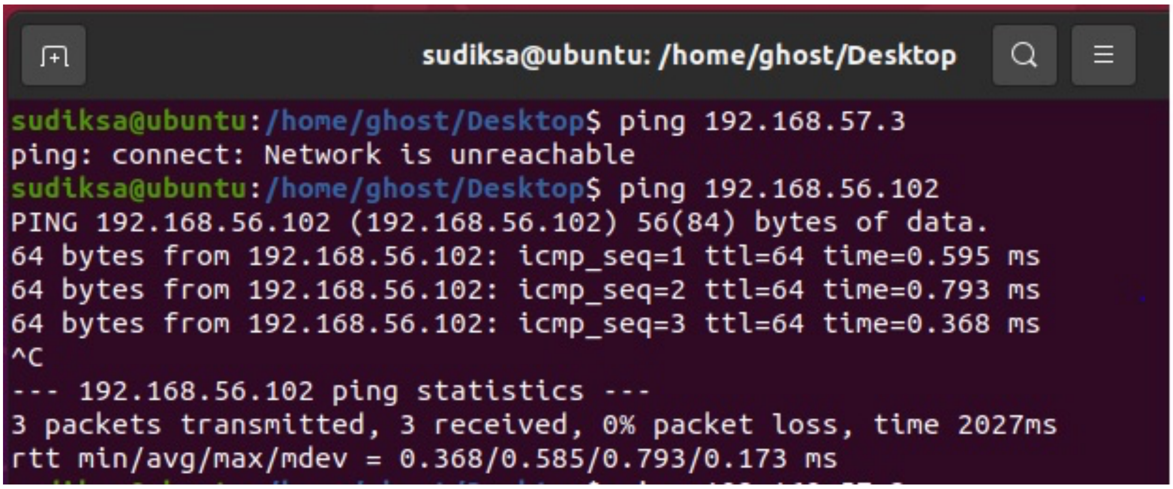


```
sudiksa@ubuntu:/home/ghost/Desktop$ sudo ufw status
Status: inactive
sudiksa@ubuntu:/home/ghost/Desktop$ sudo ufw enable
Firewall is active and enabled on system startup
sudiksa@ubuntu:/home/ghost/Desktop$ sudo ufw status
Status: active
sudiksa@ubuntu:/home/ghost/Desktop$
```

After the firewall is pinged to both the internal and external clients, the icmp messages transmitted along with the packets received and lost is displayed at the bottom of the terminal. The ping commands output denotes that both the internal and external clients are able to send and receive messages from the uncomplicated firewall.



```
sudiksa@ubuntu:/home/ghost/Desktop$ ping 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=0.556 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=0.613 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=0.389 ms
64 bytes from 192.168.56.102: icmp_seq=4 ttl=64 time=0.327 ms
64 bytes from 192.168.56.102: icmp_seq=5 ttl=64 time=0.661 ms
64 bytes from 192.168.56.102: icmp_seq=6 ttl=64 time=0.569 ms
64 bytes from 192.168.56.102: icmp_seq=7 ttl=64 time=0.546 ms
64 bytes from 192.168.56.102: icmp_seq=8 ttl=64 time=0.360 ms
64 bytes from 192.168.56.102: icmp_seq=9 ttl=64 time=0.572 ms
64 bytes from 192.168.56.102: icmp_seq=10 ttl=64 time=0.313 ms
64 bytes from 192.168.56.102: icmp_seq=11 ttl=64 time=0.283 ms
64 bytes from 192.168.56.102: icmp_seq=12 ttl=64 time=0.470 ms
64 bytes from 192.168.56.102: icmp_seq=13 ttl=64 time=0.477 ms
64 bytes from 192.168.56.102: icmp_seq=14 ttl=64 time=1.97 ms
^C
--- 192.168.56.102 ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 13304ms
rtt min/avg/max/mdev = 0.283/0.579/1.972/0.403 ms
```



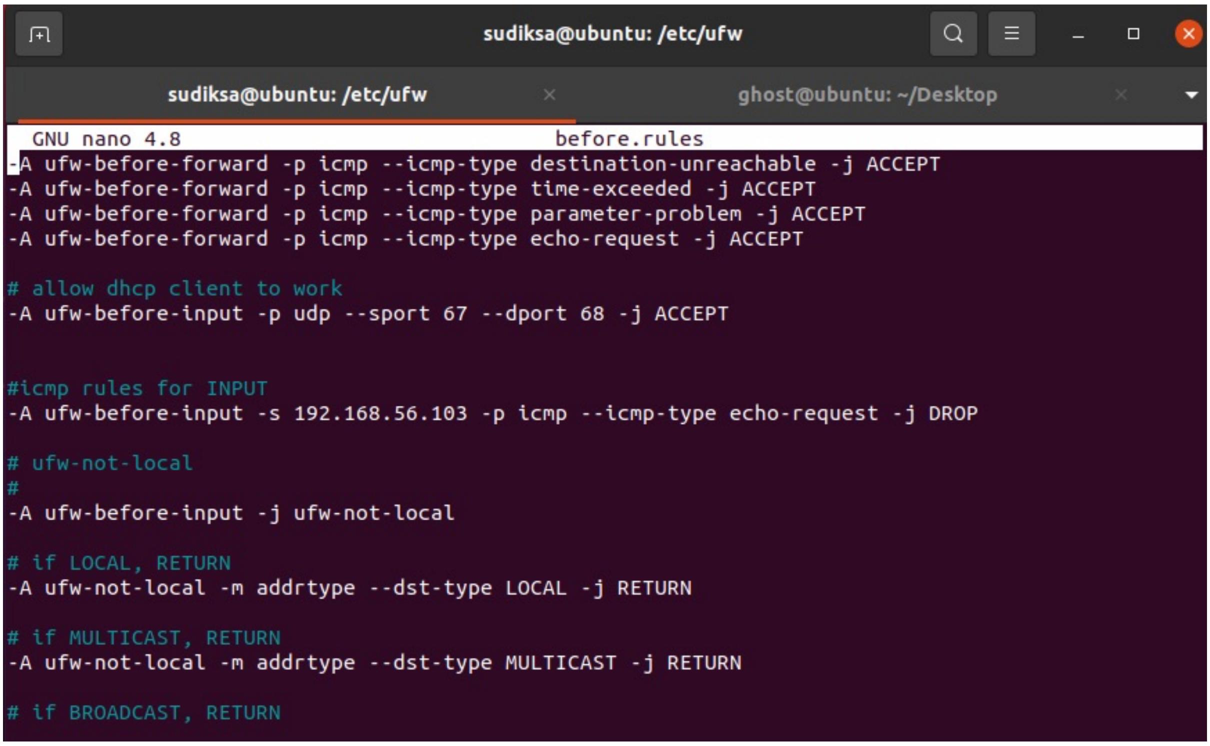
```
sudiksa@ubuntu:/home/ghost/Desktop$ ping 192.168.57.3
ping: connect: Network is unreachable
sudiksa@ubuntu:/home/ghost/Desktop$ ping 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=0.595 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=0.793 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=0.368 ms
^C
--- 192.168.56.102 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2027ms
rtt min/avg/max/mdev = 0.368/0.585/0.793/0.173 ms
```

5. The demonstrated properties implemented in the firewall

Blocking external ICMP messages (ping, traceroute, etc), but allowing them from interior clients.

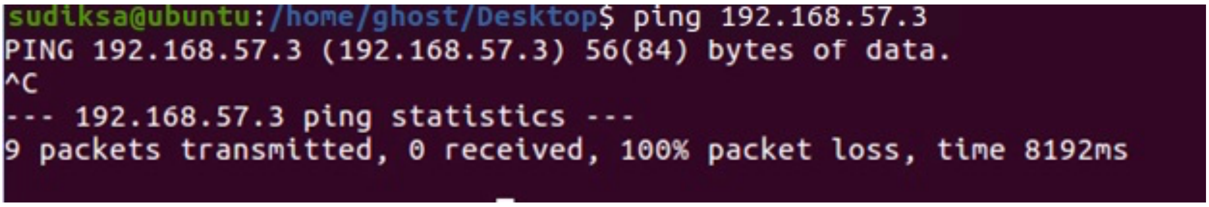
In Debian-based Linux distributions that ship with UFW application firewall, ICMP messages can be blocked by adding the rule that is mentioned below to /etc/ufw/before.rules file.

-A ufw-before-input -s 192.168.56.103 -p icmp --icmp-type echo-request -j DROP

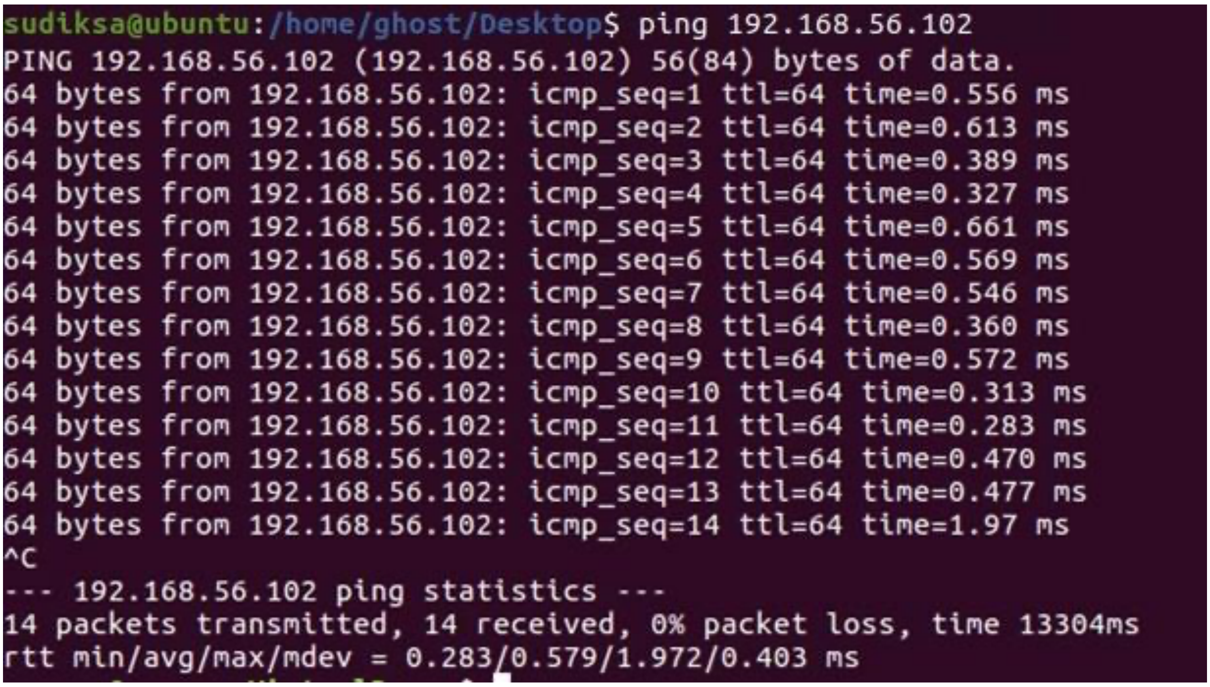


```
  GNU nano 4.8                          before.rules
-A ufw-before-forward -p icmp --icmp-type destination-unreachable -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type time-exceeded -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type parameter-problem -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type echo-request -j ACCEPT

# allow dhcp client to work
-A ufw-before-input -p udp --sport 67 --dport 68 -j ACCEPT


#icmp rules for INPUT
-A ufw-before-input -s 192.168.56.103 -p icmp --icmp-type echo-request -j DROP

# ufw-not-local
#
-A ufw-before-input -j ufw-not-local

# if LOCAL, RETURN
-A ufw-not-local -m addrtype --dst-type LOCAL -j RETURN

# if MULTICAST, RETURN
-A ufw-not-local -m addrtype --dst-type MULTICAST -j RETURN

# if BROADCAST, RETURN
```

The changes that occurred in the previous screenshots will not allow the ICMP messages that are received from the external clients but keeps sending the ICMP messages from the internal clients.



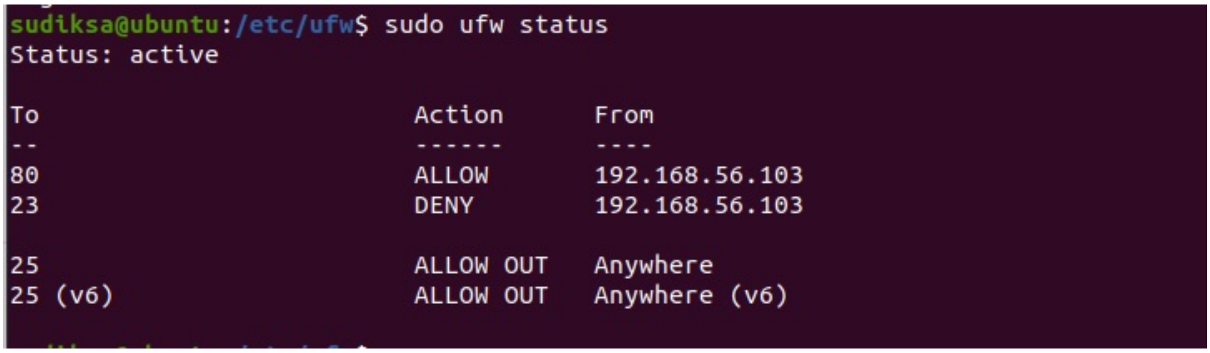
```
sudiksa@ubuntu:/home/ghost/Desktop$ ping 192.168.57.3
PING 192.168.57.3 (192.168.57.3) 56(84) bytes of data.
^C
--- 192.168.57.3 ping statistics ---
9 packets transmitted, 0 received, 100% packet loss, time 8192ms
```



```
sudiksa@ubuntu:/home/ghost/Desktop$ ping 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=0.556 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=0.613 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=0.389 ms
64 bytes from 192.168.56.102: icmp_seq=4 ttl=64 time=0.327 ms
64 bytes from 192.168.56.102: icmp_seq=5 ttl=64 time=0.661 ms
64 bytes from 192.168.56.102: icmp_seq=6 ttl=64 time=0.569 ms
64 bytes from 192.168.56.102: icmp_seq=7 ttl=64 time=0.546 ms
64 bytes from 192.168.56.102: icmp_seq=8 ttl=64 time=0.360 ms
64 bytes from 192.168.56.102: icmp_seq=9 ttl=64 time=0.572 ms
64 bytes from 192.168.56.102: icmp_seq=10 ttl=64 time=0.313 ms
64 bytes from 192.168.56.102: icmp_seq=11 ttl=64 time=0.283 ms
64 bytes from 192.168.56.102: icmp_seq=12 ttl=64 time=0.470 ms
64 bytes from 192.168.56.102: icmp_seq=13 ttl=64 time=0.477 ms
64 bytes from 192.168.56.102: icmp_seq=14 ttl=64 time=1.97 ms
^C
--- 192.168.56.102 ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 13304ms
rtt min/avg/max/mdev = 0.283/0.579/1.972/0.403 ms
```

Allowing port 80 requests to the interior client

Command: $ sudo ufw allow from 192.168.56.103 to any port 80



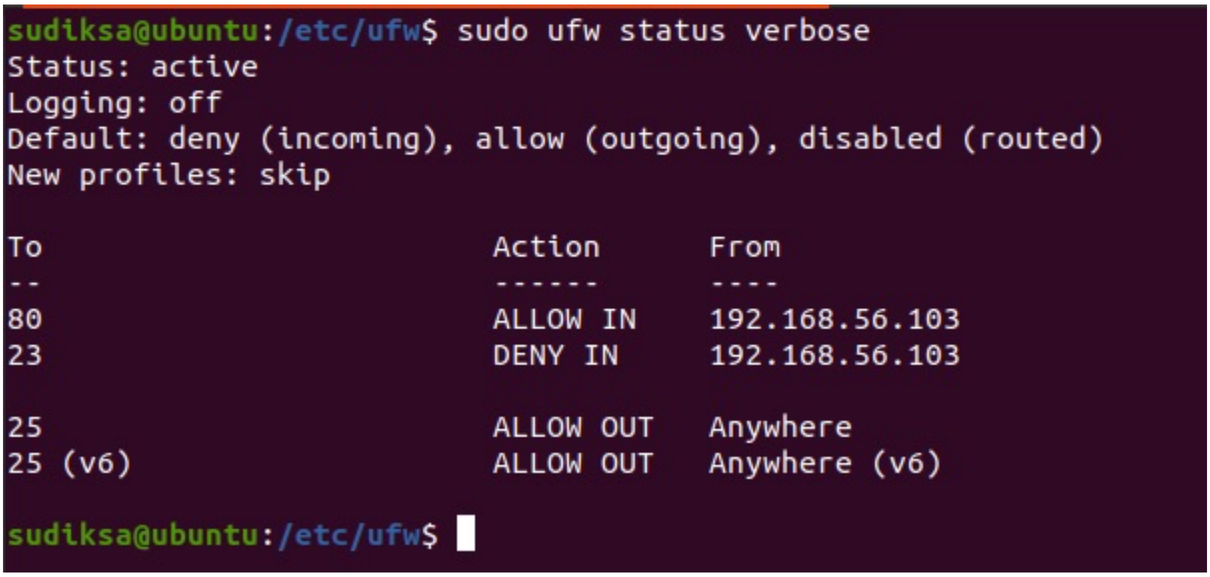
```
sudiksa@ubuntu:/etc/ufw$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
80                         ALLOW       192.168.56.103
23                         DENY        192.168.56.103

25                         ALLOW OUT   Anywhere
25 (v6)                    ALLOW OUT   Anywhere (v6)
```

Blocking external telnet, login, and other similar requests
Command: $ sudo ufw deny from 192.168.56.103 to any port 23

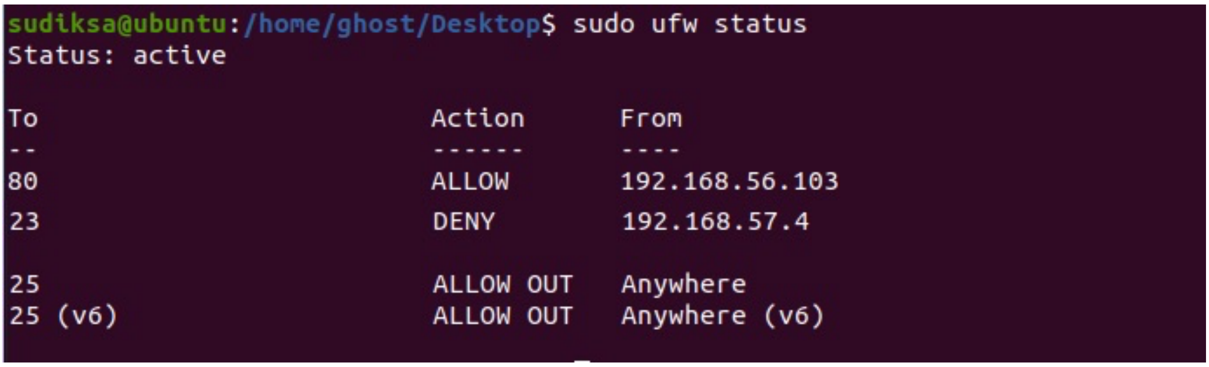
$ sudo ufw logging off

Allowing internal messages using SMTP to be sent through the firewall

```
$ sudo ufw allow out 25
```



```
sudiksa@ubuntu:/etc/ufw$ sudo ufw status verbose
Status: active
Logging: off
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
80                         ALLOW IN    192.168.56.103
23                         DENY IN     192.168.56.103

25                         ALLOW OUT   Anywhere
25 (v6)                    ALLOW OUT   Anywhere (v6)

sudiksa@ubuntu:/etc/ufw$ 
```



```
sudiksa@ubuntu:/home/ghost/Desktop$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
80                         ALLOW       192.168.56.103
23                         DENY        192.168.57.4

25                         ALLOW OUT   Anywhere
25 (v6)                    ALLOW OUT   Anywhere (v6)
```