

Creating adapter and configuring dhcp server:

Adapter

DHCP Server

☒ Enable Server

Server Address:

192.168.26.2

Server Mask:

255.255.255.0

Lower Address Bound:

192.168.26.3

Upper Address Bound:

192.168.26.254

Apply

Reset

Adapter

DHCP Server

☒ Enable Server

Server Address:

192.168.77.254

Server Mask:

255.255.255.0

Lower Address Bound:

192.168.77.2

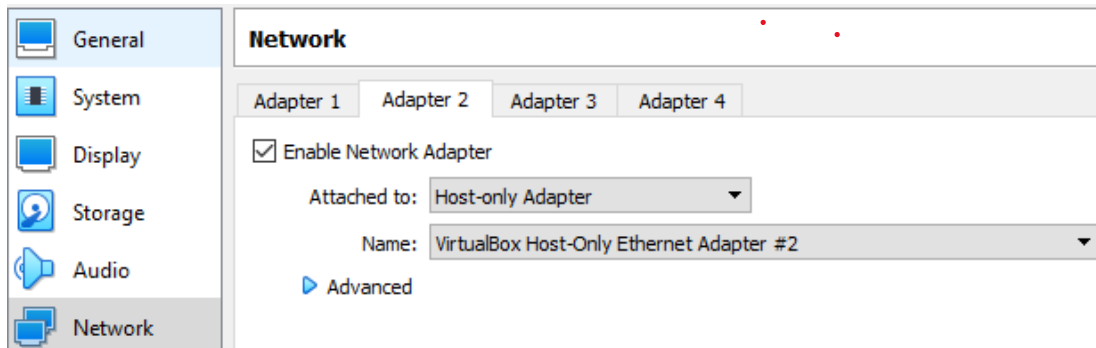
Upper Address Bound:

192.168.77.253

Apply

Reset

Adding adapter to vm's preferences:



Checking if network is available:

```
Debian GNU/Linux 10 vm1 tty1
vm1 login: debian
Password:
Last login: Mon May  9 02:00:52 CEST 2022 on tty2
Linux vm1 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1 (2020-01-26) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
debian@vm1:~$ ip ad
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:b9:2e:d6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.77.2/24 brd 192.168.77.255 scope global dynamic enp0s8
        valid_lft 574sec preferred_lft 574sec
debian@vm1:~$ _
```

Tasks:

1. iptables

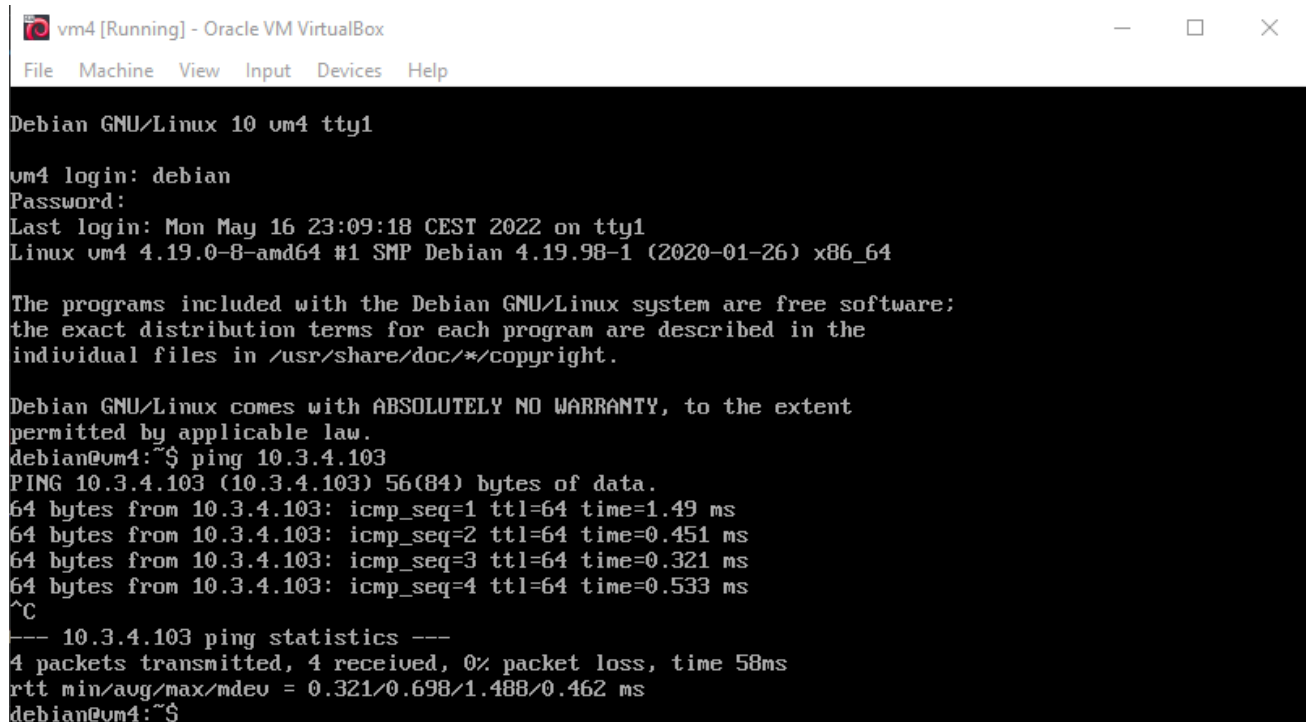
a) Check iptables status: vm3

```
debian@vm3:~$ sudo -i
root@vm3:~# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source destination
root@vm3:~# _
```

b)Pinging vm3 from the vm4;



```
vm4 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

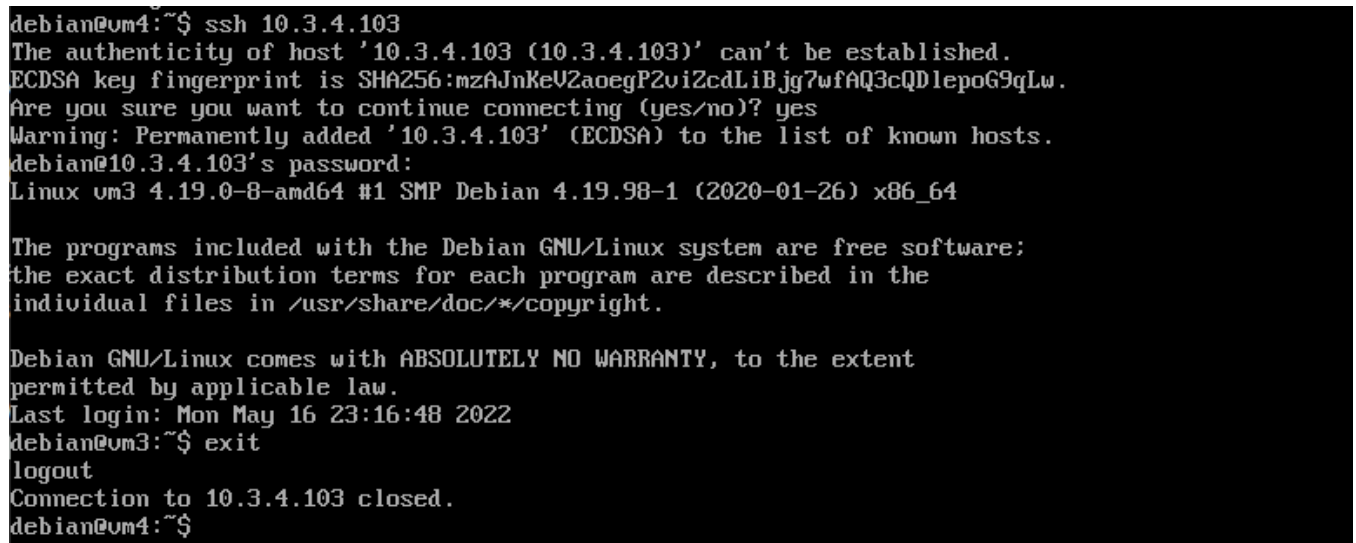
Debian GNU/Linux 10 vm4 tty1

vm4 login: debian
Password:
Last login: Mon May 16 23:09:18 CEST 2022 on tty1
Linux vm4 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1 (2020-01-26) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
debian@vm4:~$ ping 10.3.4.103
PING 10.3.4.103 (10.3.4.103) 56(84) bytes of data.
64 bytes from 10.3.4.103: icmp_seq=1 ttl=64 time=1.49 ms
64 bytes from 10.3.4.103: icmp_seq=2 ttl=64 time=0.451 ms
64 bytes from 10.3.4.103: icmp_seq=3 ttl=64 time=0.321 ms
64 bytes from 10.3.4.103: icmp_seq=4 ttl=64 time=0.533 ms
^C
--- 10.3.4.103 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 58ms
rtt min/avg/max/mdev = 0.321/0.698/1.488/0.462 ms
debian@vm4:~$
```

c) Connecting to vm3 from vm4 using ssh command to ping:



```
debian@vm4:~$ ssh 10.3.4.103
The authenticity of host '10.3.4.103 (10.3.4.103)' can't be established.
ECDSA key fingerprint is SHA256:mzAJnKeV2aoegP2viZcdLiBjg7wfaQ3cQDlepoG9qLw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.3.4.103' (ECDSA) to the list of known hosts.
debian@10.3.4.103's password:
Linux vm3 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1 (2020-01-26) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon May 16 23:16:48 2022
debian@vm3:~$ exit
logout
Connection to 10.3.4.103 closed.
debian@vm4:~$
```

d) Block pinging vm3 from vm4: on vm3:

```
root@vm3:~# iptables -I INPUT -p icmp -j DROP -i eth1
root@vm3:~#
```

e) Check if it's possible to ping VM3 from VM2 and VM4 (first should work, second - no)

From vm4: cannot

```
debian@vm4:~$ ping 10.3.4.103
PING 10.3.4.103 (10.3.4.103) 56(84) bytes of data.
From 10.3.4.104 icmp_seq=1 Destination Host Unreachable
From 10.3.4.104 icmp_seq=2 Destination Host Unreachable
From 10.3.4.104 icmp_seq=3 Destination Host Unreachable
From 10.3.4.104 icmp_seq=4 Destination Host Unreachable
From 10.3.4.104 icmp_seq=5 Destination Host Unreachable
From 10.3.4.104 icmp_seq=6 Destination Host Unreachable
^C
--- 10.3.4.103 ping statistics ---
8 packets transmitted, 0 received, +6 errors, 100% packet loss, time 160ms
pipe 4
debian@vm4:~$
```

From vm2: pinging sucesfully

```
debian@vm2:~$ ping 10.2.3.103
PING 10.2.3.103 (10.2.3.103) 56(84) bytes of data.
64 bytes from 10.2.3.103: icmp_seq=1 ttl=64 time=1.58 ms
64 bytes from 10.2.3.103: icmp_seq=2 ttl=64 time=0.588 ms
64 bytes from 10.2.3.103: icmp_seq=3 ttl=64 time=0.630 ms
64 bytes from 10.2.3.103: icmp_seq=4 ttl=64 time=0.604 ms
^C
--- 10.2.3.103 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 50ms
rtt min/avg/max/mdev = 0.588/0.850/1.581/0.423 ms
debian@vm2:~$
```

f) Blocking ssh from vm4 on vm3

```
debian@vm3:~$ sudo -i
root@vm3:~# iptables -I INPUT -p tcp -j DROP -i eth1
root@vm3:~#
```

Cannot connect from vm4 to vm3 using ssh command:

```
pipe 4
debian@vm4:~$ ssh 10.3.4.103
ssh: connect to host 10.3.4.103 port 22: No route to host
debian@vm4:~$
```

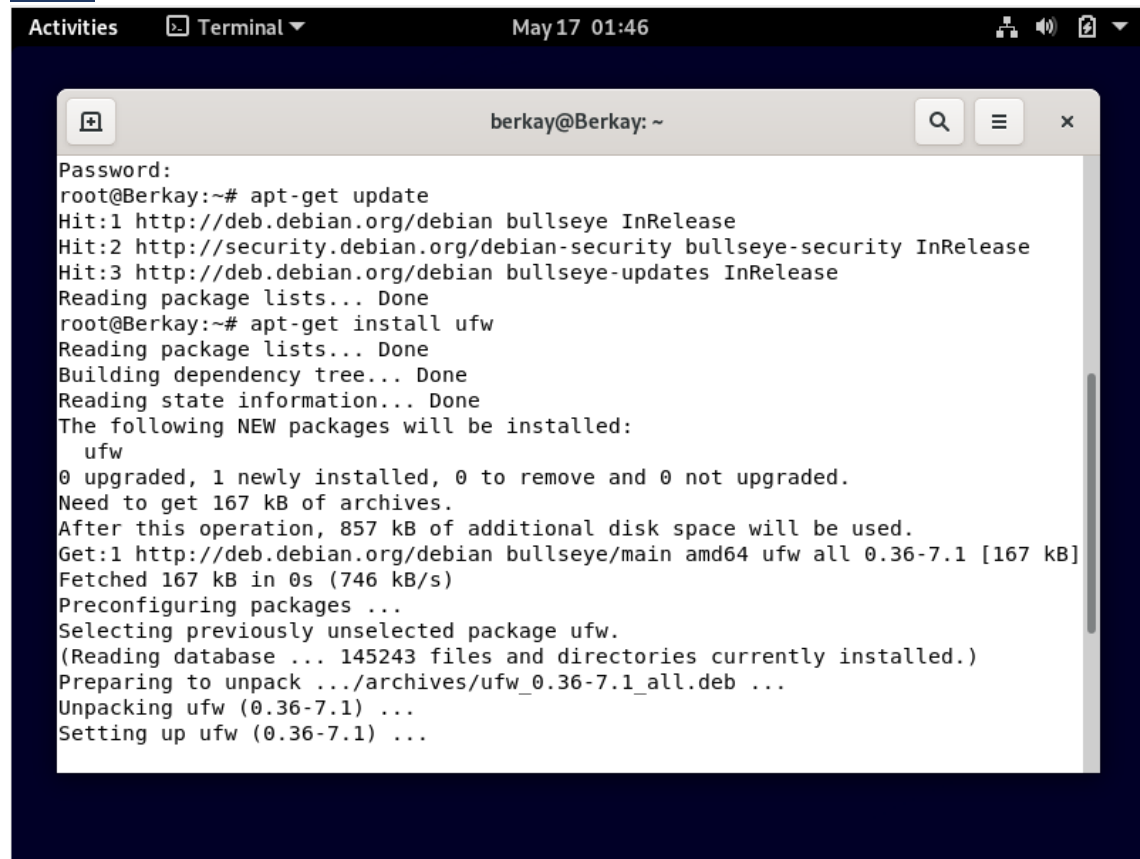
g) Block ping and ssh to vm3 from vm2:

```
root@vm3:~# iptables -I INPUT -p icmp -j DROP -i eth0
root@vm3:~# iptables -I INPUT -p tcp -j DROP -i eth0
root@vm3:~# _
```

h) Pinging vm4 from vm1:

```
debian@vm1:~$ ping 10.3.4.104
PING 10.3.4.104 (10.3.4.104) 56(84) bytes of data:
64 bytes from 10.3.4.104: icmp_seq=1 ttl=62 time=1.57 ms
64 bytes from 10.3.4.104: icmp_seq=2 ttl=62 time=1.27 ms
64 bytes from 10.3.4.104: icmp_seq=3 ttl=62 time=1.62 ms
64 bytes from 10.3.4.104: icmp_seq=4 ttl=62 time=1.32 ms
^C
--- 10.3.4.104 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 1.266/1.443/1.622/0.157 ms
debian@vm1:~$ _
```

2. UFW:



```
Activities Terminal May 17 01:46
berkay@Berkay: ~
Password:
root@Berkay:~# apt-get update
Hit:1 http://deb.debian.org/debian bullseye InRelease
Hit:2 http://security.debian.org/debian-security bullseye-security InRelease
Hit:3 http://deb.debian.org/debian bullseye-updates InRelease
Reading package lists... Done
root@Berkay:~# apt-get install ufw
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  ufw
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 167 kB of archives.
After this operation, 857 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bullseye/main amd64 ufw all 0.36-7.1 [167 kB]
Fetched 167 kB in 0s (746 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 145243 files and directories currently installed.)
Preparing to unpack ../archives/ufw_0.36-7.1_all.deb ...
Unpacking ufw (0.36-7.1) ...
Setting up ufw (0.36-7.1) ...
```

```
C:\Users\brkyb>ssh -l debian 192.168.77.7
debian@192.168.77.7's password:
Linux vm1 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1 (2020-01-26) x86_64Linux vm1 4.19.0-8-amd64 #1 S
MP Debian 4.19.98-1 (2020-01-26) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.
Last login: Tue May 17 03:50:30 2022
debian@vm1:~$
```

c) Activating ufw:

```
root@Berkay:~# ufw enable
Firewall is active and enabled on system startup
root@Berkay:~#
```

f)

```
debian@vm1:~$ ssh -l debian 192.168.77.7
The authenticity of host '192.168.77.7 (192.168.77.7)' can't be established.
ECDSA key fingerprint is SHA256:XoYUKl135oR5TTzbuaU1bfTHku2p7kgHuzRt1DNLeLY.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.77.7' (ECDSA) to the list of known hosts.
debian@192.168.77.7's password:
Linux vm1 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1 (2020-01-26) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue May 17 03:51:37 2022 from 192.168.77.1
debian@vm1:~$
```

e) Allowing incoming traffic from 192.168.77.0/24 network:

```
root@Berkay:~# ufw allow from 192.168.77.0/24 to any port 22
Rule added
root@Berkay:~#
```

Firewall rules:

```
Rule added
root@Berkay:~# ufw status numbered
Status: active
```

To	Action	From
--	-----	----
1] 22	ALLOW IN	192.168.77.0/24

```
root@Berkay:~# █
```

g) Blocking connections over http and https (ports 80 and 443 accordingly):

```
root@Berkay:~# ufw deny out 80
Rule added
Rule added (v6)
root@Berkay:~# ufw deny out 443
Rule added
Rule added (v6)
root@Berkay:~#
```

Rules:

```
root@Berkay:~# ufw status numbered
Status: active

    To                Action      From
    --                -
[ 1] 22              ALLOW IN   192.168.77.0/24
[ 2] 80              DENY OUT   Anywhere      (out)
[ 3] 443             DENY OUT   Anywhere      (out)
[ 4] 80 (v6)         DENY OUT   Anywhere (v6) (out)
[ 5] 443 (v6)        DENY OUT   Anywhere (v6) (out)

root@Berkay:~#
```

Two rules for each port (ipv4 and ipv6 traffic)

i) Deactivating and removing ufw firewall

```
root@Berkay:~# ufw disable
Firewall stopped and disabled on system startup
root@Berkay:~# █
```

```

root@Berkay:~# apt-get purge ufw
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be REMOVED:
  ufw*
0 upgraded, 0 newly installed, 1 to remove and 0 not upgraded.
After this operation, 857 kB disk space will be freed.
Do you want to continue? [Y/n] Y
(Reading database ... 145351 files and directories currently installed.)
Removing ufw (0.36-7.1) ...
Skip stopping firewall: ufw (not enabled)
Processing triggers for man-db (2.9.4-2) ...
(Reading database ... 145258 files and directories currently installed.)
Purging configuration files for ufw (0.36-7.1) ...
Processing triggers for rsyslog (8.2102.0-2) ...
root@Berkay:~# █

```

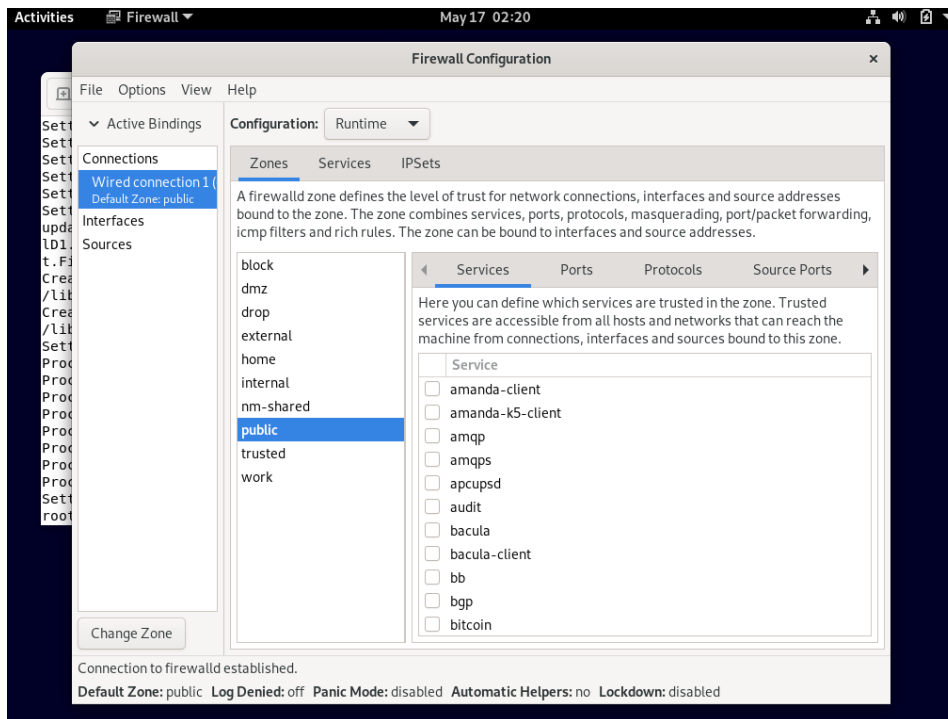
3. configuration of firewall using GUI

a) Running firewall applet:

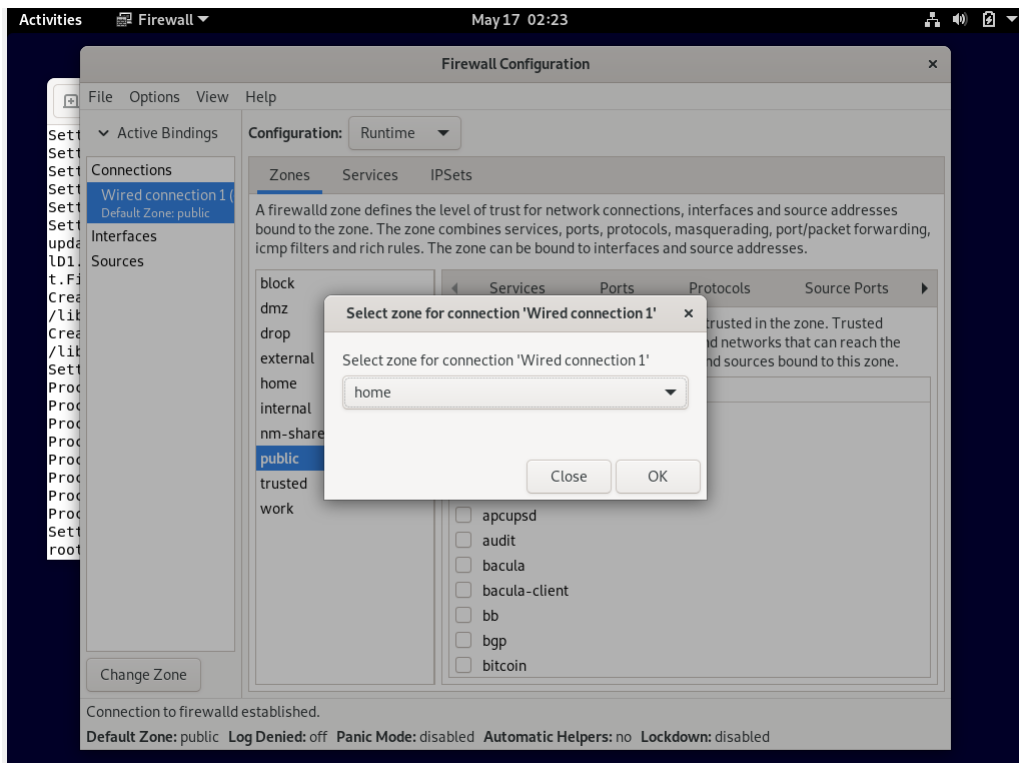
```

berkay@Berkay: ~
Reading package lists... Done
root@Berkay:~# apt-get install firewall-applet firewallld
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  firewall-config ipset libdouble-conversion3 libipset13 libmd4c0
  libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5designer5 libqt5gui5
  libqt5help5 libqt5network5 libqt5printsupport5 libqt5sql5 libqt5sqlite5
  libqt5svg5 libqt5test5 libqt5widgets5 libqt5xml5 libxcb-xinerama0
  libxcb-xinput0 python3-dbus.mainloop.pyqt5 python3-decorator
  python3-firewall python3-nftables python3-pyqt5 python3-pyqt5.sip
  python3-selinux python3-slip python3-slip-dbus qt5-gtk-platformtheme
  qttranslations5-l10n
Suggested packages:
  qt5-image-formats-plugins qtwayland5 python3-pyqt5-dbg
The following NEW packages will be installed:
  firewall-applet firewall-config firewallld ipset libdouble-conversion3
  libipset13 libmd4c0 libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5designer5
  libqt5gui5 libqt5help5 libqt5network5 libqt5printsupport5 libqt5sql5
  libqt5sqlite5 libqt5svg5 libqt5test5 libqt5widgets5 libqt5xml5
  libxcb-xinerama0 libxcb-xinput0 python3-dbus.mainloop.pyqt5
  python3-decorator python3-firewall python3-nftables python3-pyqt5
  python3-pyqt5.sip python3-selinux python3-slip python3-slip-dbus

```

b) Changing zone to home:



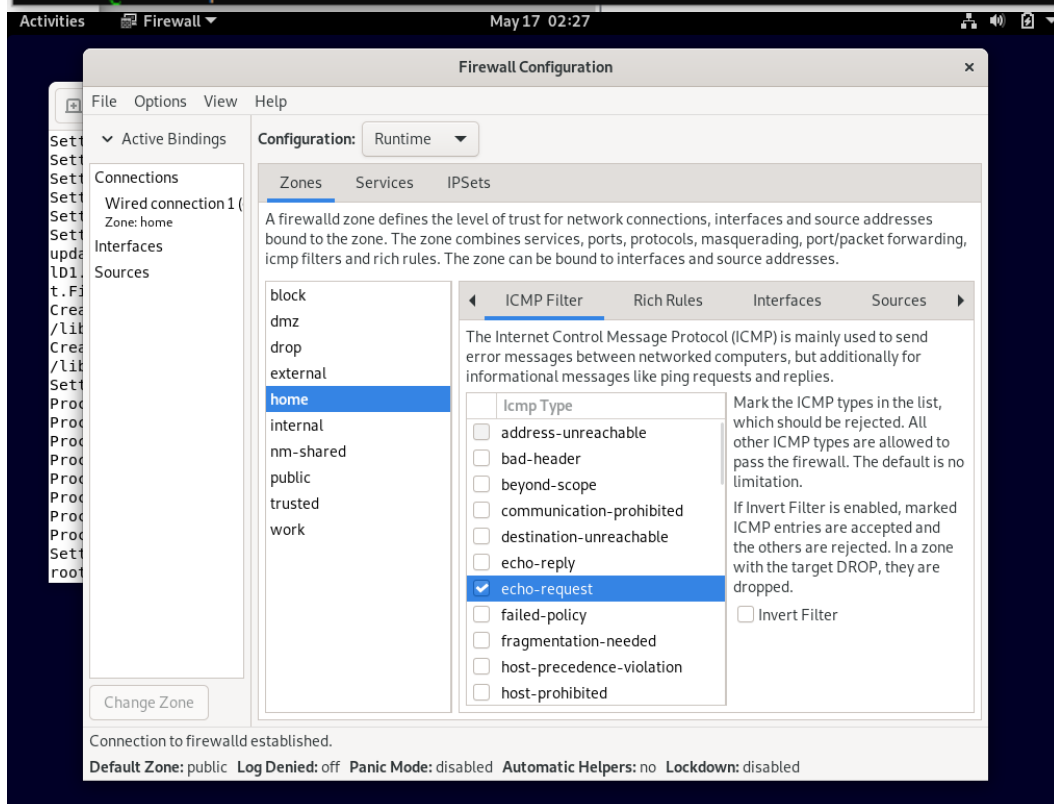
Login:

```
debian@vm1:~$ ssh -l debian 192.168.77.7
debian@192.168.77.7's password:
Linux vm1 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1 (2020-01-26) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue May 17 04:24:21 2022 from 192.168.77.7
debian@vm1:~$
```

```
debian@vm1:~$ ping 192.168.77.7
PING 192.168.77.7 (192.168.77.7) 56(84) bytes of data.
64 bytes from 192.168.77.7: icmp_seq=1 ttl=64 time=0.030 ms
64 bytes from 192.168.77.7: icmp_seq=2 ttl=64 time=0.026 ms
64 bytes from 192.168.77.7: icmp_seq=3 ttl=64 time=0.025 ms
^C
--- 192.168.77.7 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 4ms
rtt min/avg/max/mdev = 0.025/0.027/0.030/0.002 ms
debian@vm1:~$
```



```
debian@vm1:~$ ping 192.168.77.7
PING 192.168.77.7 (192.168.77.7) 56(84) bytes of data.
64 bytes from 192.168.77.7: icmp_seq=1 ttl=64 time=0.034 ms
64 bytes from 192.168.77.7: icmp_seq=2 ttl=64 time=0.027 ms
^C
--- 192.168.77.7 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2ms
rtt min/avg/max/mdev = 0.027/0.030/0.034/0.006 ms
debian@vm1:~$
```

```
root@Berkay:~# sudo apt-get purge firewall-applet firewallld
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  ipset libdouble-conversion3 libipset13 libmd4c0 libpcre2-16-0 libqt5core5a
  libqt5dbus5 libqt5designer5 libqt5gui5 libqt5help5 libqt5network5
  libqt5printsupport5 libqt5sql5 libqt5sql5-sqlite libqt5svg5 libqt5test5
  libqt5widgets5 libqt5xml5 libxcb-xinerama0 libxcb-xinput0
  python3-dbus.mainloop.pyqt5 python3-decorator python3-firewall
  python3-nftables python3-pyqt5 python3-pyqt5.sip python3-selinux
  python3-slip python3-slip-dbus qt5-gtk-platformtheme qttranslations5-l10n
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
  firewall-applet* firewall-config* firewallld*
0 upgraded, 0 newly installed, 3 to remove and 0 not upgraded.
After this operation, 3,892 kB disk space will be freed.
Do you want to continue? [Y/n] Y
(Reading database ... 146320 files and directories currently installed.)
Removing firewall-applet (0.9.3-2) ...
Removing firewall-config (0.9.3-2) ...
Removing firewallld (0.9.3-2) ...
update-alternatives: using /usr/share/polkit-1/actions/org.fedoraproject.FirewallD1.desktop.policy
choice to provide /usr/share/polkit-1/actions/org.fedoraproject.FirewallD1.policy (org.fedora
project.FirewallD1.policy) in auto mode
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for gnome-menus (3.36.0-1) ...
Processing triggers for libgl2.0-0:amd64 (2.66.8-1) ...
```