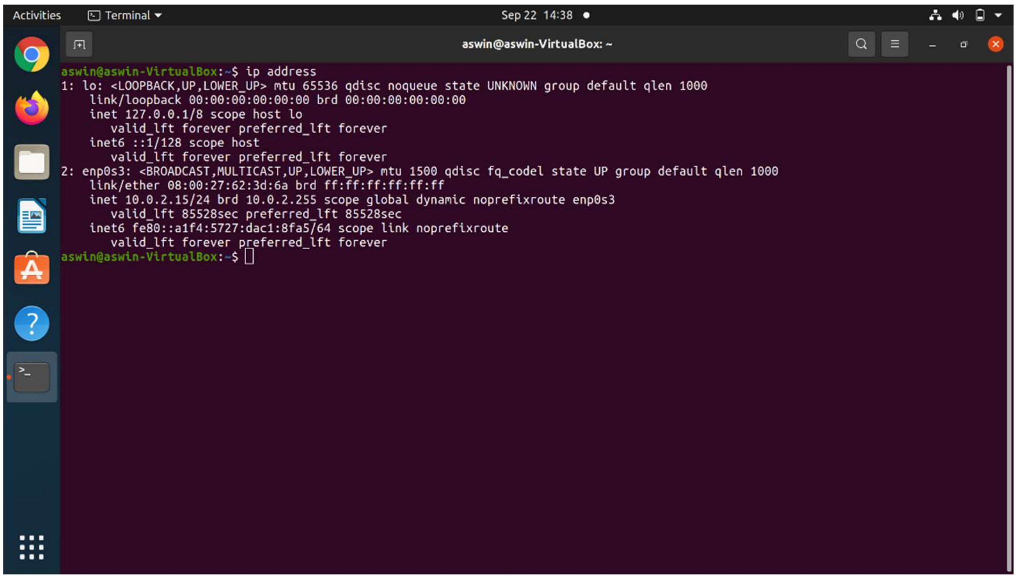
EXPIRIMENT 8:

Aim: Introduction to command line tools for networking IPv4 networking, network commands: ping route traceroute, nslookup, ip. Setting up static and dynamic IP addresses. Concept of Subnets, CIDR address schemes, Subnet masks, iptables, setting up a firewall for LAN, Application layer (L7) proxies.

Solution :-

Setting up static IP addresses

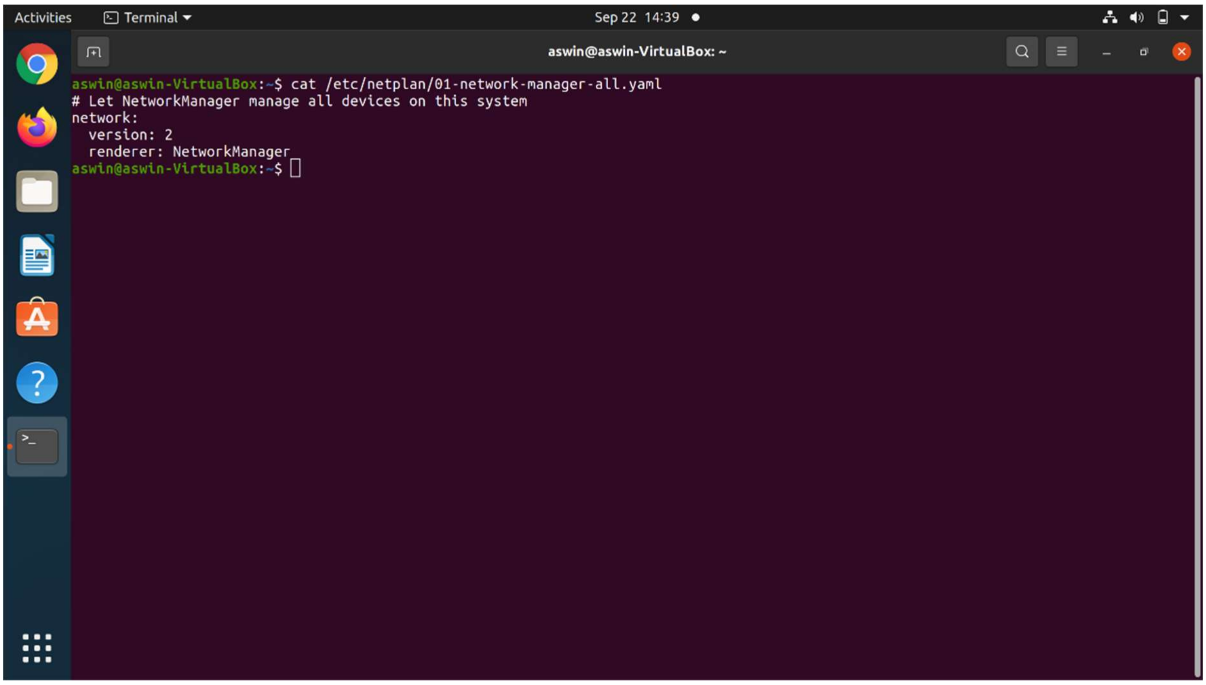
Step 1: List all the interfaces in the system.Use the `ip address` command to define a static IP address on an interface.



```
aswin@aswin-VirtualBox:~$ ip address
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
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:62:3d:6a brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 85528sec preferred_lft 85528sec
    inet6 fe80::a1f4:5727:dac1:8fa5/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
aswin@aswin-VirtualBox:~$ 
```

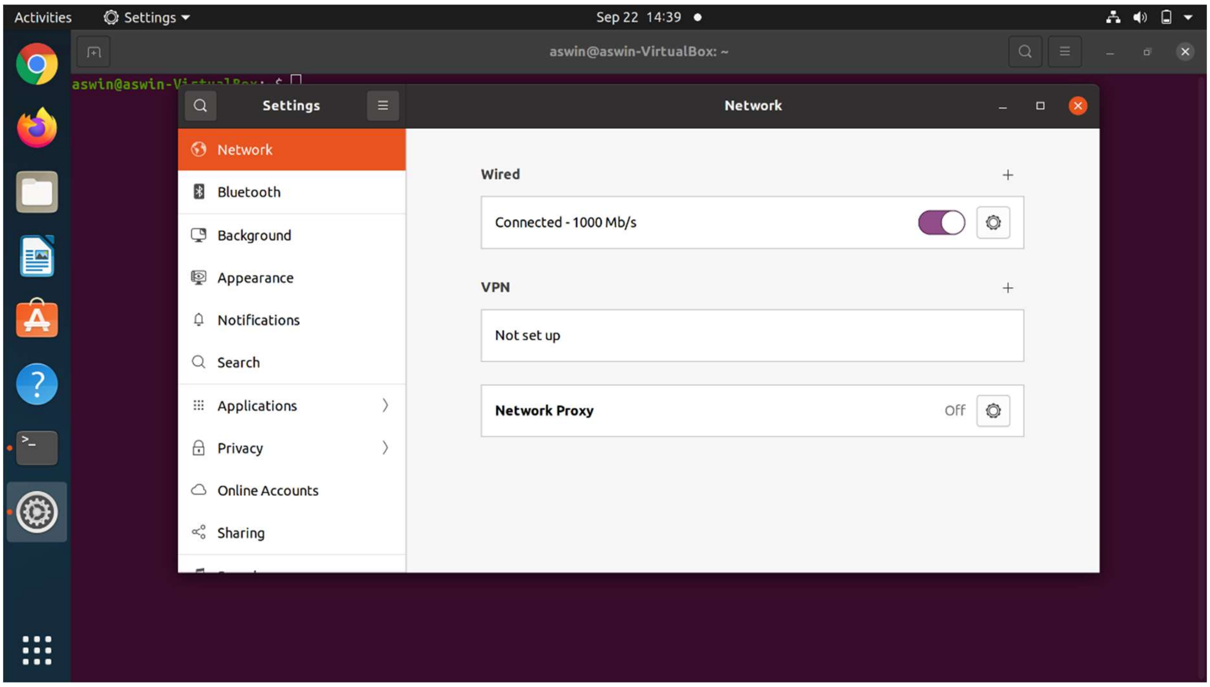
Step 2: To view the content of Netplan network configuration file, run the following command:

```
cat /etc/netplan/01-network-manager-all.yaml
```



```
aswin@aswin-VirtualBox:~$ cat /etc/netplan/01-network-manager-all.yaml
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
aswin@aswin-VirtualBox:~$ 
```

Step 3: Click on the top right network icon and select settings of the network interface you wish to configure to use a static IP address on Ubuntu.

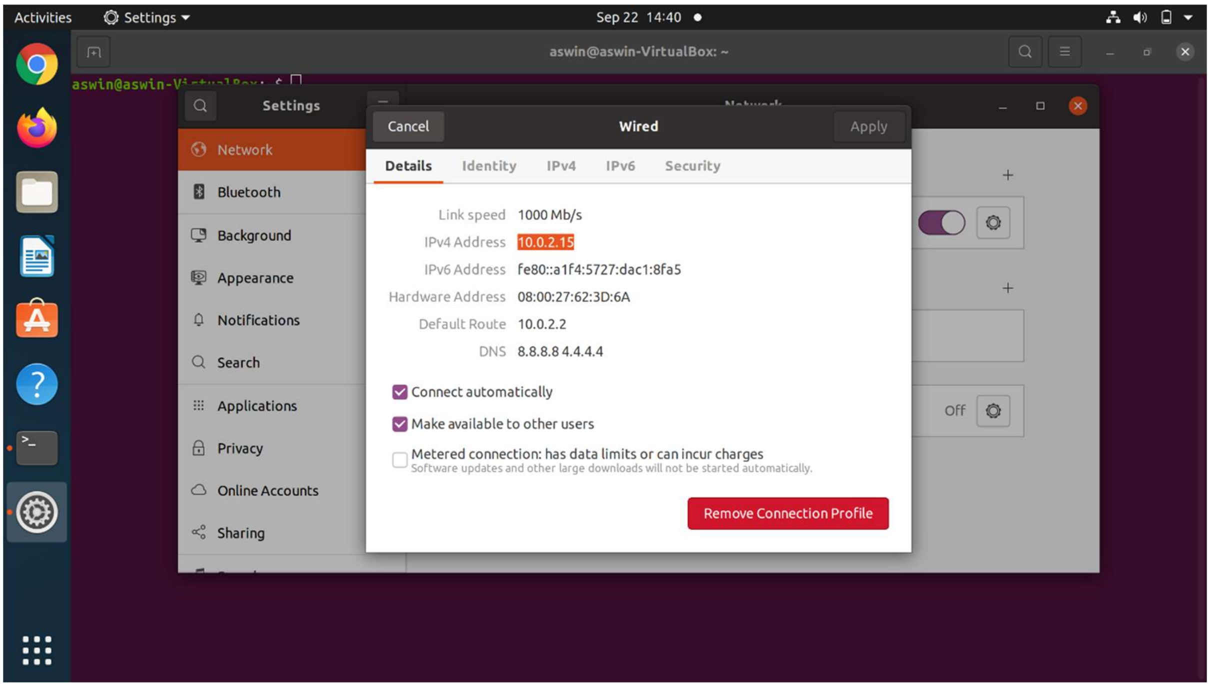


Connected - 1000 Mb/s

Not set up

Network Proxy Off

Click on the settings icon to start IP address configuration.

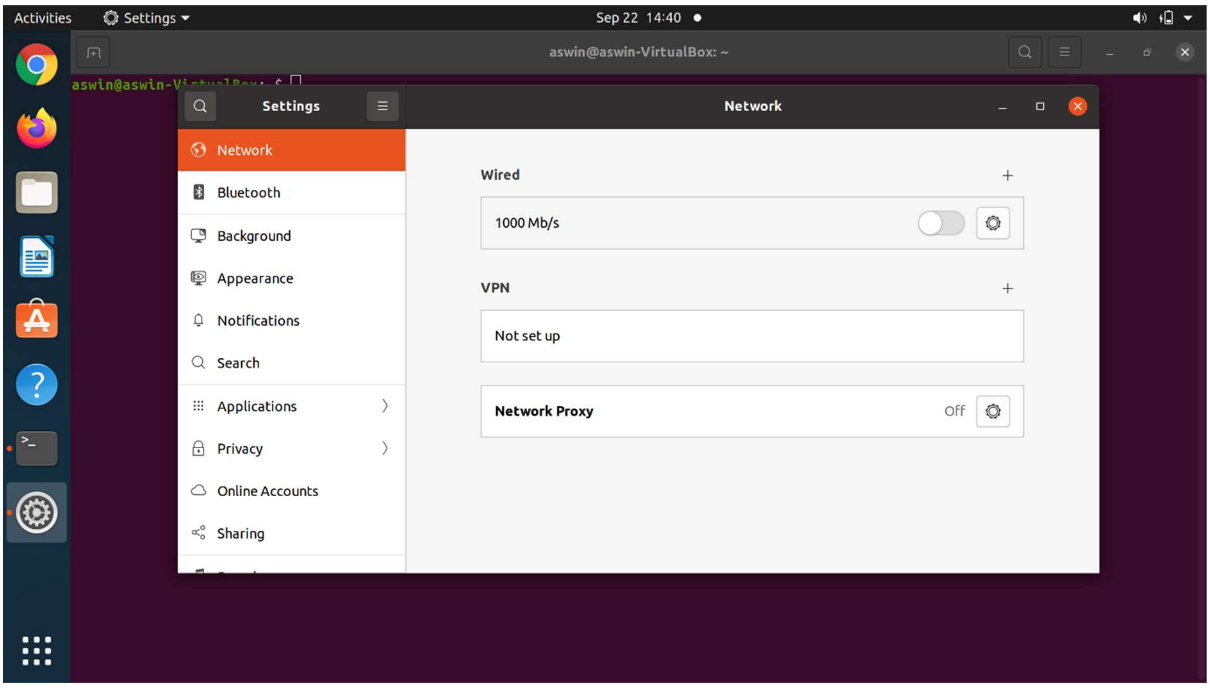


Link speed 1000 Mb/s
IPv4 Address 10.0.2.15
IPv6 Address fe80::a1f4:5727:dac1:8fa5
Hardware Address 08:00:27:62:3D:6A
Default Route 10.0.2.2
DNS 8.8.8.8 4.4.4.4

☑ Connect automatically

☑ Make available to other users

□ Metered connection: has data limits or can incur charges
Software updates and other large downloads will not be started automatically.



Wired

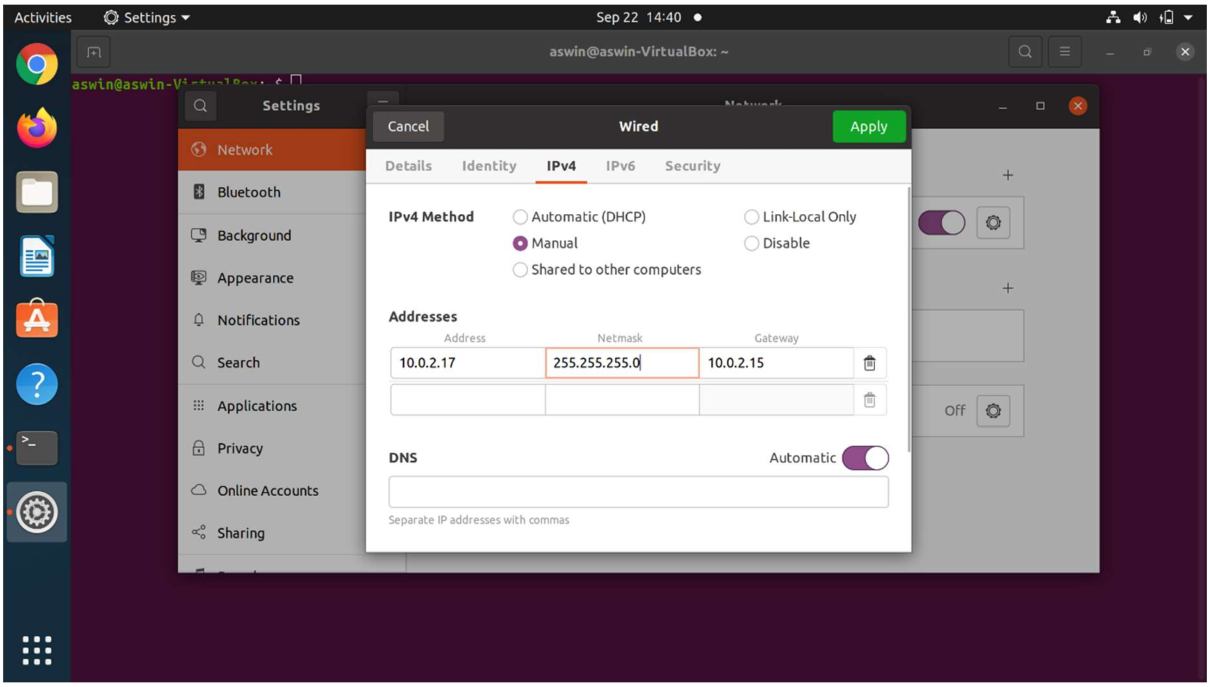
1000 Mb/s

VPN

Not set up

Network Proxy Off

Turn OFF and ON switch to apply your new network static IP configuration settings.



IPv4 Method

○ Automatic (DHCP) ○ Link-Local Only
● Manual ○ Disable
○ Shared to other computers

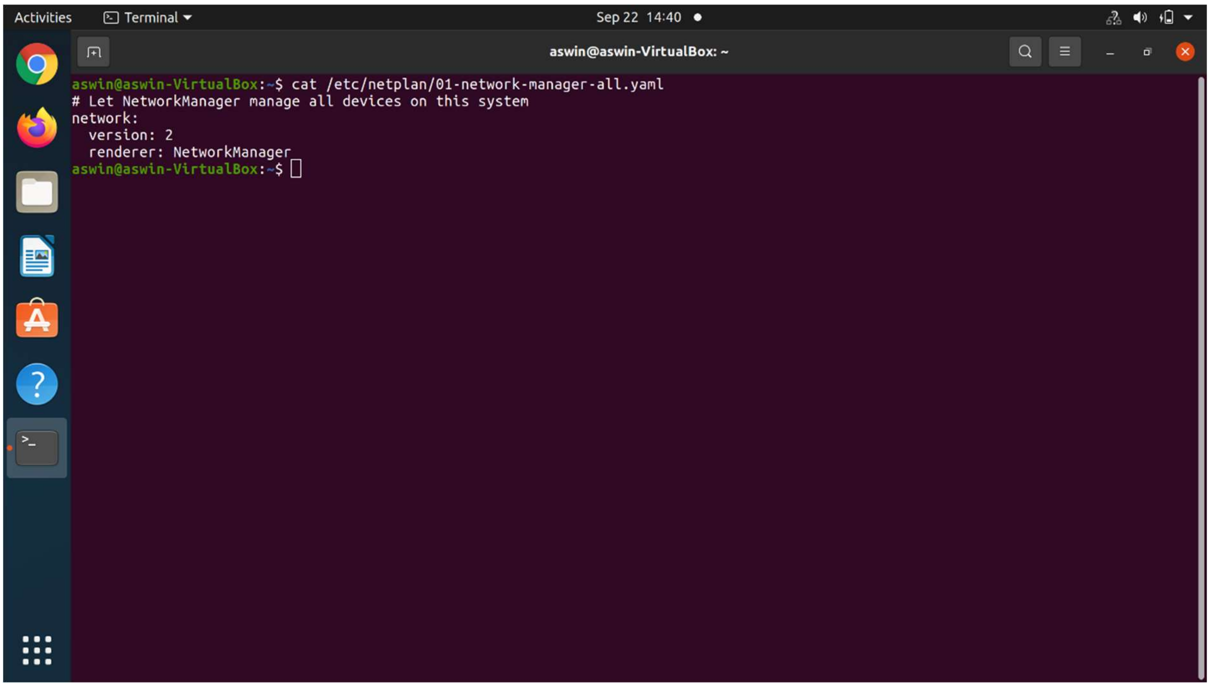
Addresses

Address	Netmask	Gateway
10.0.2.17	255.255.255.0	10.0.2.15

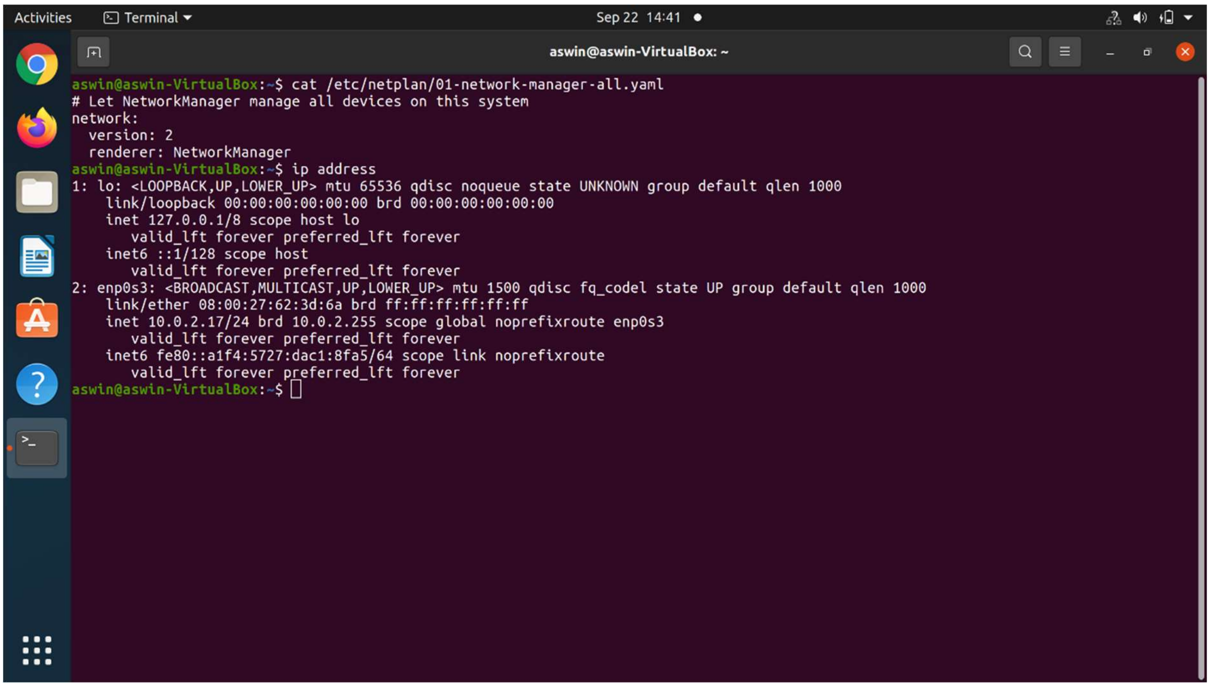
DNS Automatic ●

Separate IP addresses with commas

Step 5: Run the command `ip address` and click on the network settings icon once again to confirm your new static IP address settings.



```
aswin@aswin-VirtualBox:~$ cat /etc/netplan/01-network-manager-all.yaml
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
aswin@aswin-VirtualBox:~$ 
```



```
aswin@aswin-VirtualBox:~$ cat /etc/netplan/01-network-manager-all.yaml
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
aswin@aswin-VirtualBox:~$ ip address
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
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:62:3d:6a brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.17/24 brd 10.0.2.255 scope global noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a1f4:5727:dac1:8fa5/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
aswin@aswin-VirtualBox:~$ 
```

Configure and Set Up a Firewall on Ubuntu

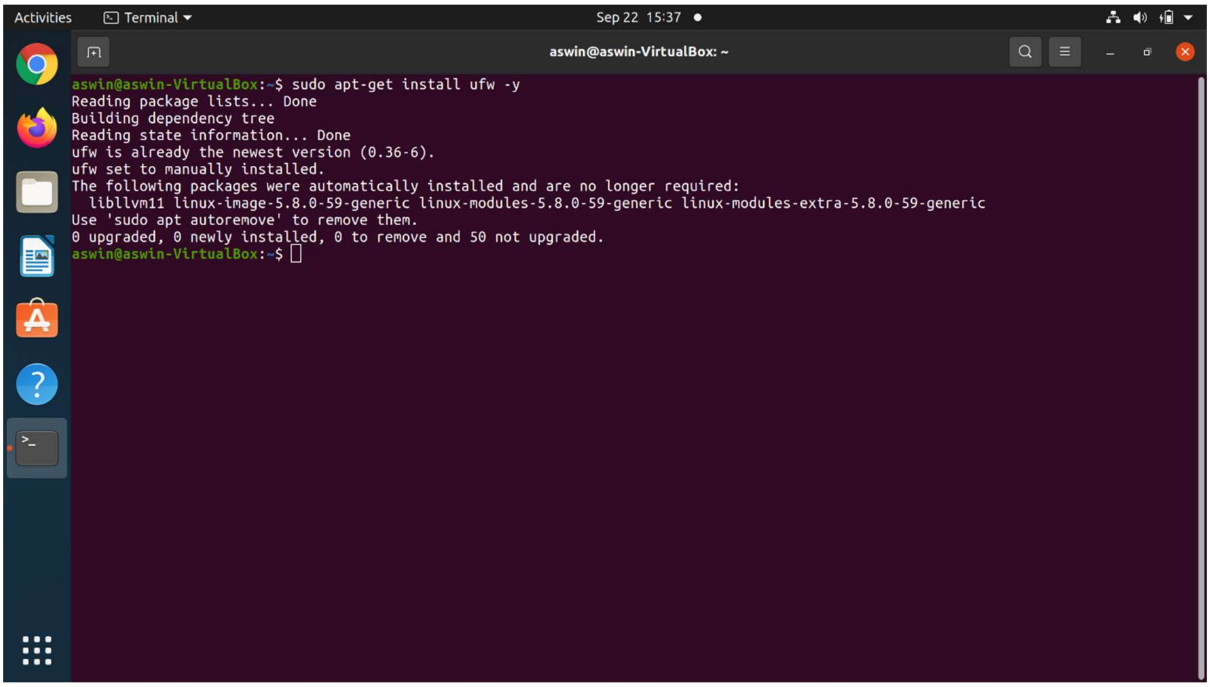
UFW stands for Uncomplicated Firewall which acts as an interface to IPTABLES that simplifies the process of the configuration of firewalls it will be a very hard for a beginner to learns and configure the firewall rules where we will secure the network from unknown users are machines. UFW works on the policies we configure as rules.

- For this, we needed a non-root user with root permission on the machine.

Installing the UFW (Firewall)

UFW is installed by default with Ubuntu, if not installed then we will install them using the below command:

```
sudo apt-get install ufw -y
```

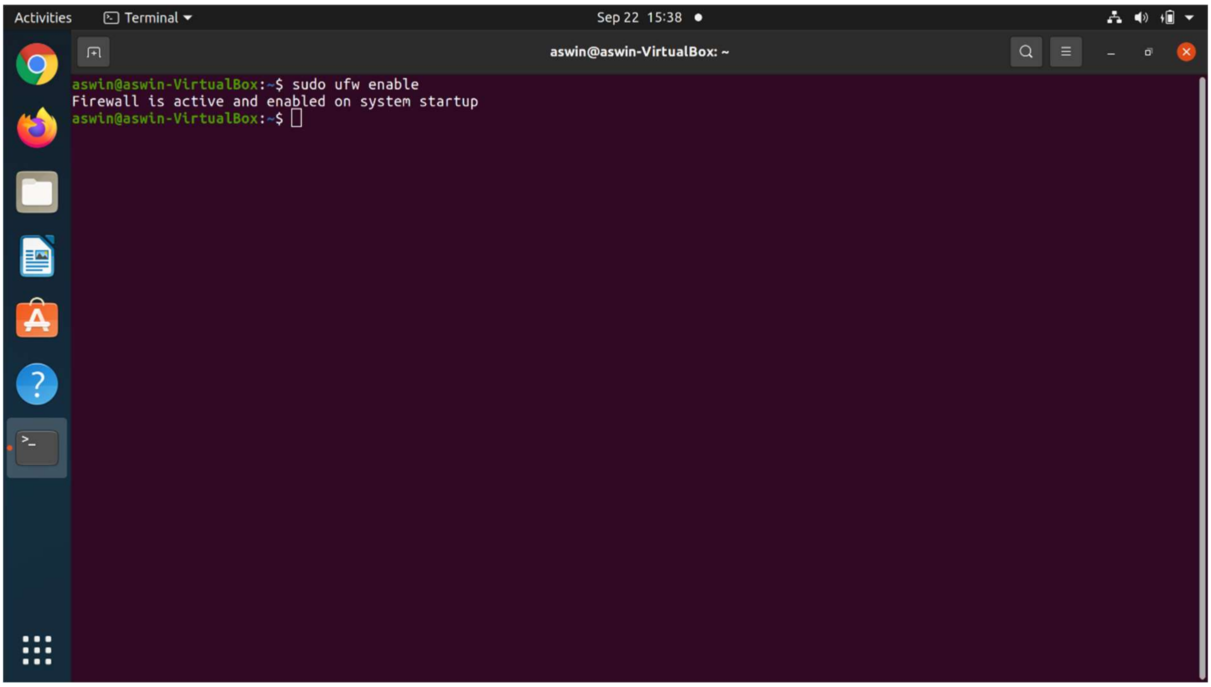


```
aswin@aswin-VirtualBox:~$ sudo apt-get install ufw -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
ufw is already the newest version (0.36-6).
ufw set to manually installed.
The following packages were automatically installed and are no longer required:
  libllvm11 linux-image-5.8.0-59-generic linux-modules-5.8.0-59-generic linux-modules-extra-5.8.0-59-generic
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 50 not upgraded.
aswin@aswin-VirtualBox:~$ 
```

Enabling the UFW (Firewall)

Below is the command to enable the UFW –

```
sudo ufw enable
```



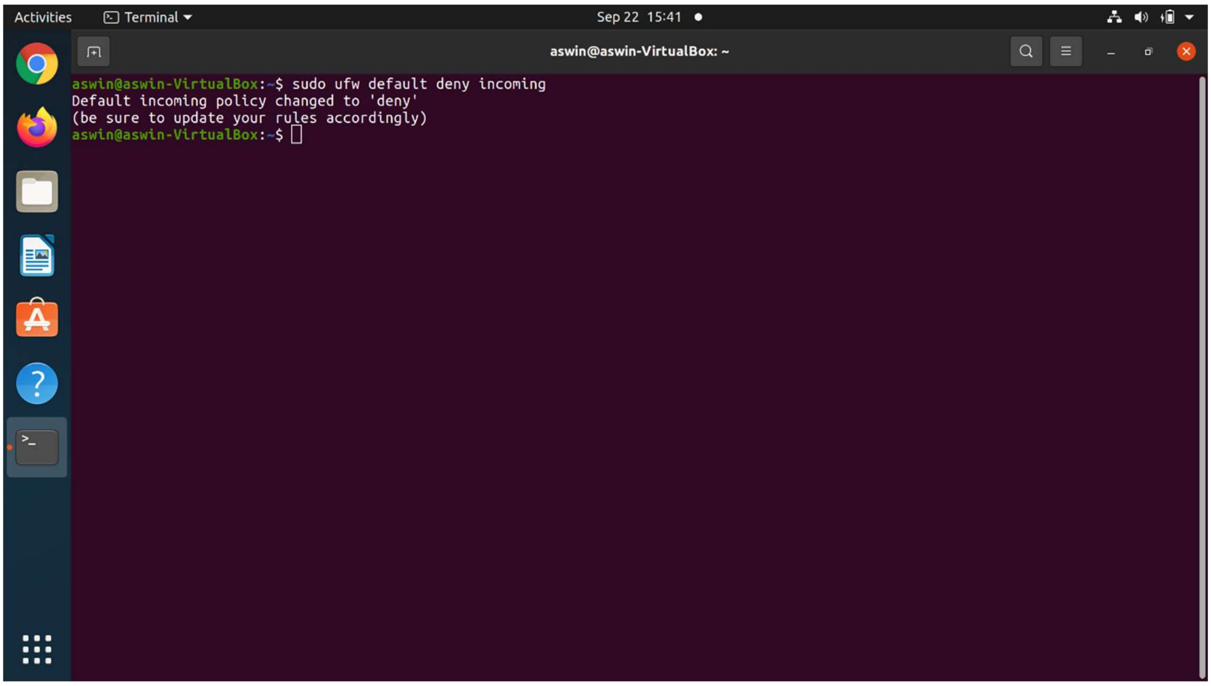
```
aswin@aswin-VirtualBox:~$ sudo ufw enable
Firewall is active and enabled on system startup
aswin@aswin-VirtualBox:~$ 
```

Enabling the Default Policies

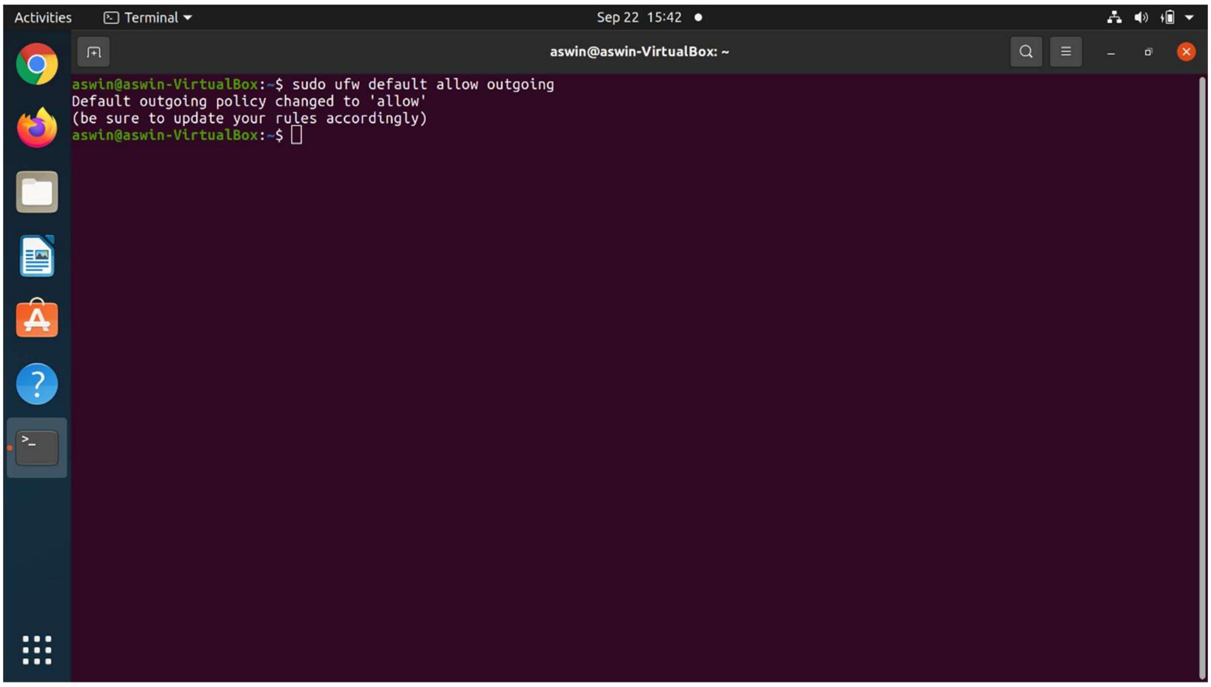
As the beginner, we will first configure default policies, which control and handles the traffic which will not match the other rules. By default, the rules will deny all incoming connections and allow all outgoing connections will be allowed which stops someone trying to reach the machine from the internet world.

```
sudo ufw default deny incoming
```

```
sudo ufw default allow outgoing
```



```
aswin@aswin-VirtualBox:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
aswin@aswin-VirtualBox:~$ 
```

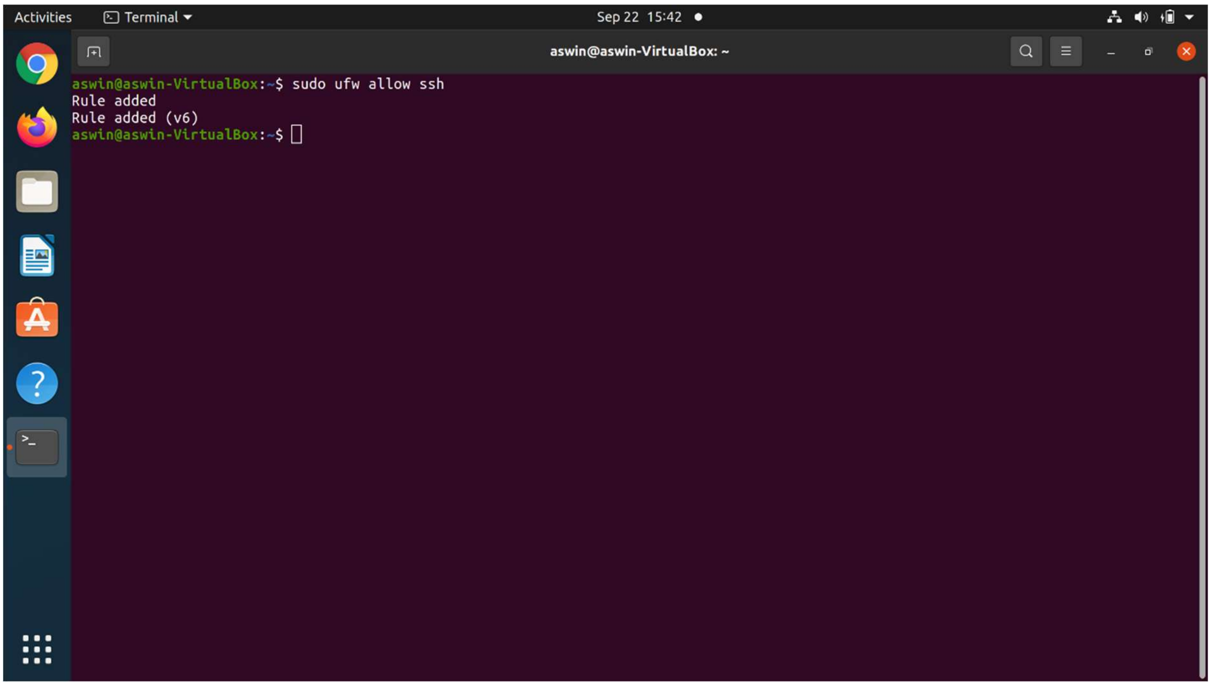


```
aswin@aswin-VirtualBox:~$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
aswin@aswin-VirtualBox:~$ 
```

Enabling SSH Connections

Using the above commands, we have disabled all the incoming connections, it will deny all the incoming connections, we needed to create a rule which will explicitly allow the SSH incoming connection.Below is the command to enable the incoming connection for SSH.

```
sudo ufw allow ssh
```



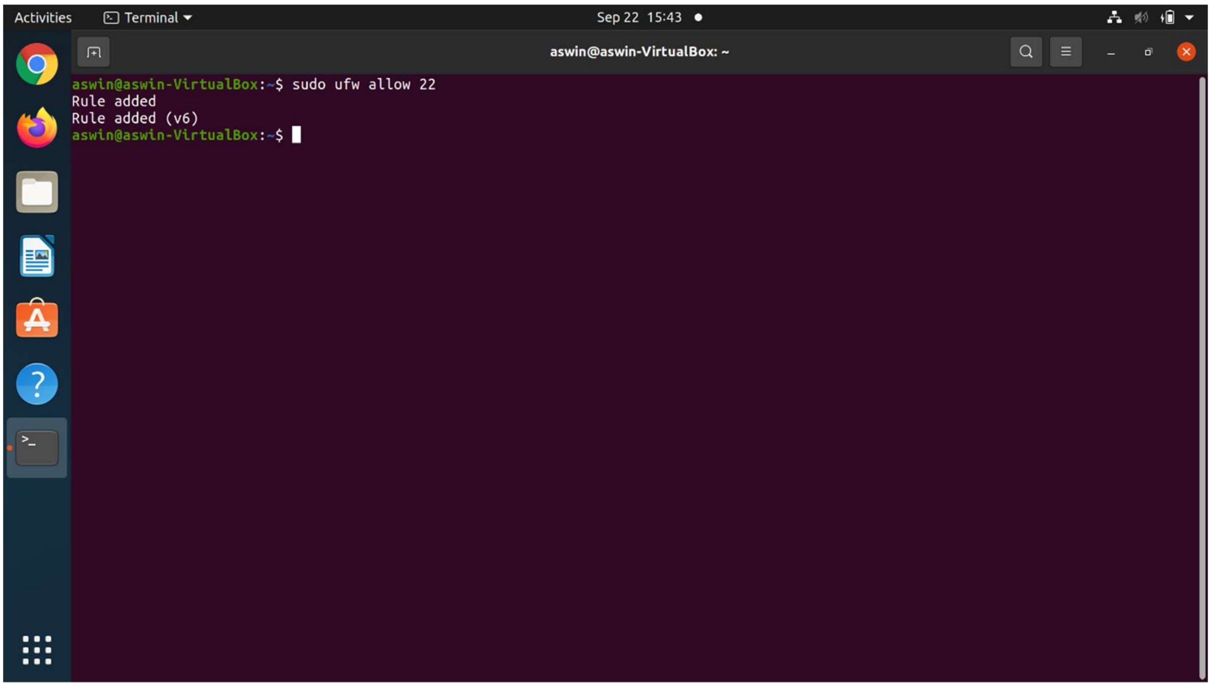
```
aswin@aswin-VirtualBox:~$ sudo ufw allow ssh
Rule added
Rule added (v6)
aswin@aswin-VirtualBox:~$
```

With the above command, the port 22 will be allowed for incoming connections. We can use the below command directly using the port no 22 to allow the SSH connections.

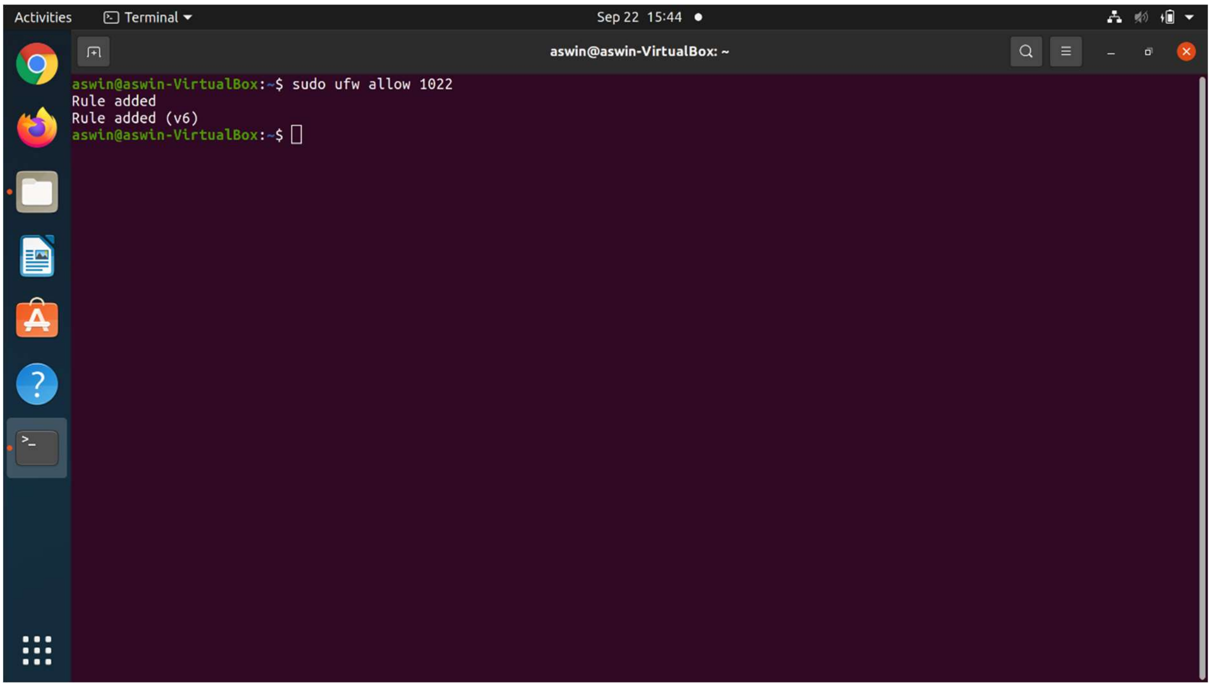
```
sudo ufw allow 22
```

However, if we have configured the SSH daemon to use a different port like 2022 or 1022, then we can use the below command

```
sudo ufw allow 1022
```



```
aswin@aswin-VirtualBox:~$ sudo ufw allow 22
Rule added
Rule added (v6)
aswin@aswin-VirtualBox:~$
```

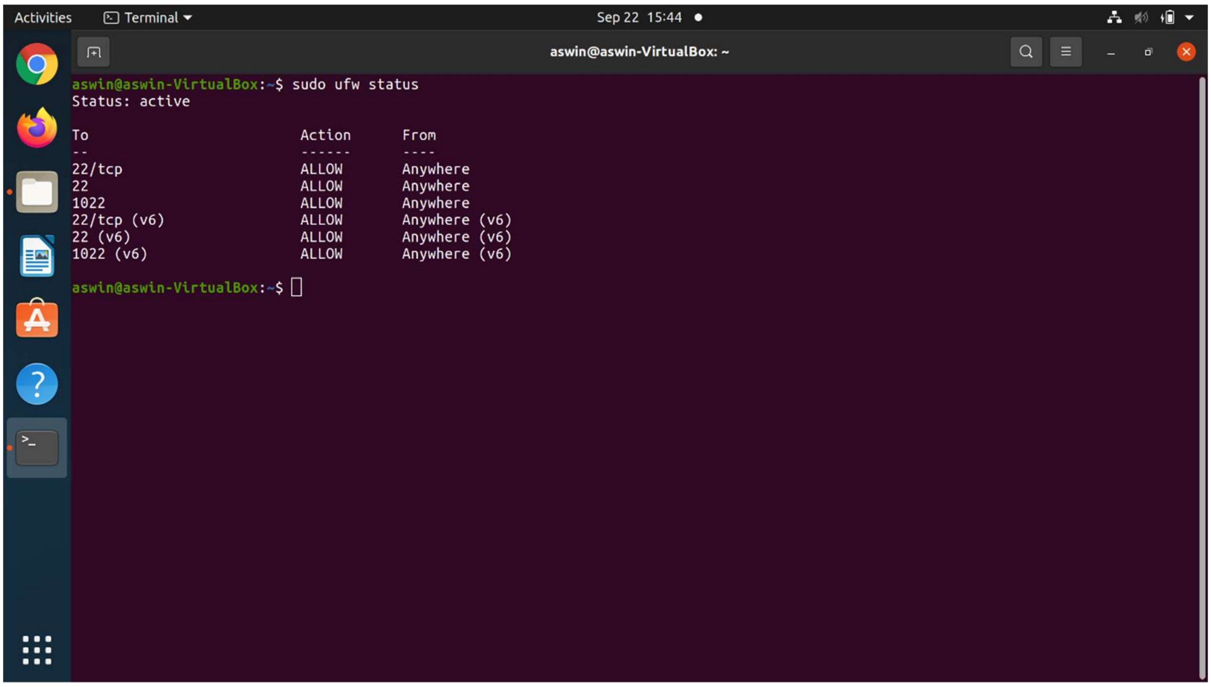


```
aswin@aswin-VirtualBox:~$ sudo ufw allow 1022
Rule added
Rule added (v6)
aswin@aswin-VirtualBox:~$
```

Checking the UFW (Firewall) Status

Below is the command to check the current status of the firewall rules.

```
sudo ufw status
```



```
aswin@aswin-VirtualBox:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
22                         ALLOW       Anywhere
1022                       ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
22 (v6)                    ALLOW       Anywhere (v6)
1022 (v6)                  ALLOW       Anywhere (v6)

aswin@aswin-VirtualBox:~$
```

Enabling the UFW for regular port like (HTTP, HTTPS & FTP)

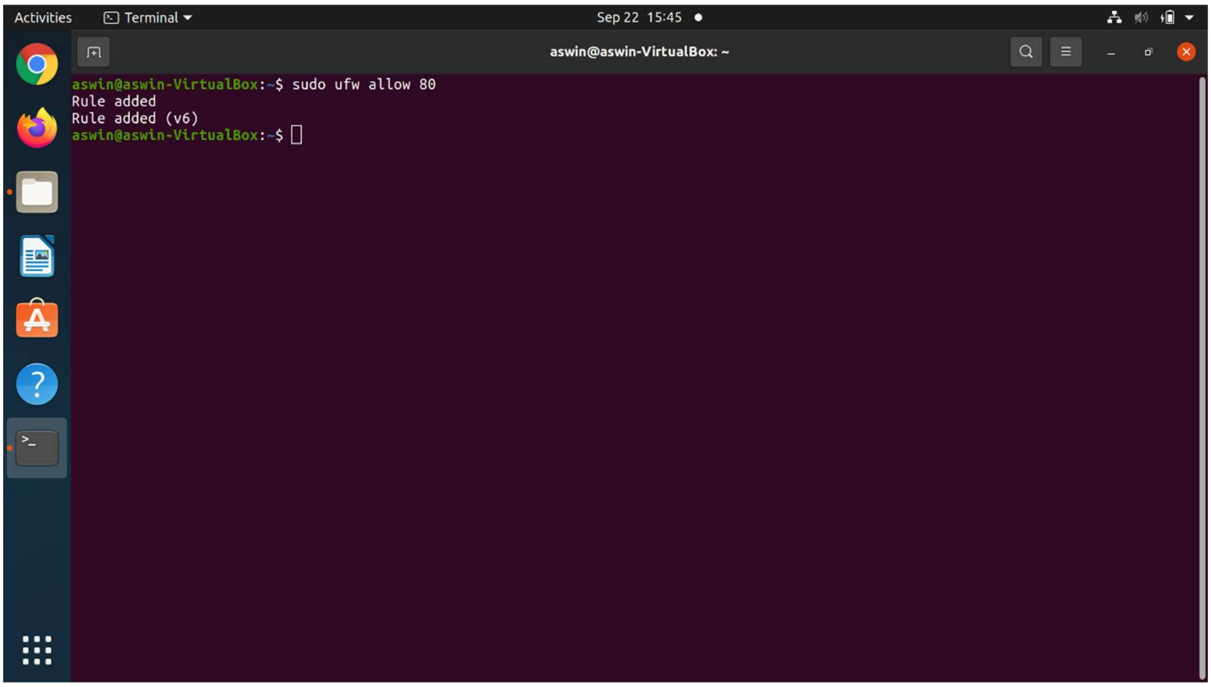
At this point, we will allow others to connect to the server for the regular ports like HTPP, HTTPS, and FTP ports respectively.

HTTP port 80

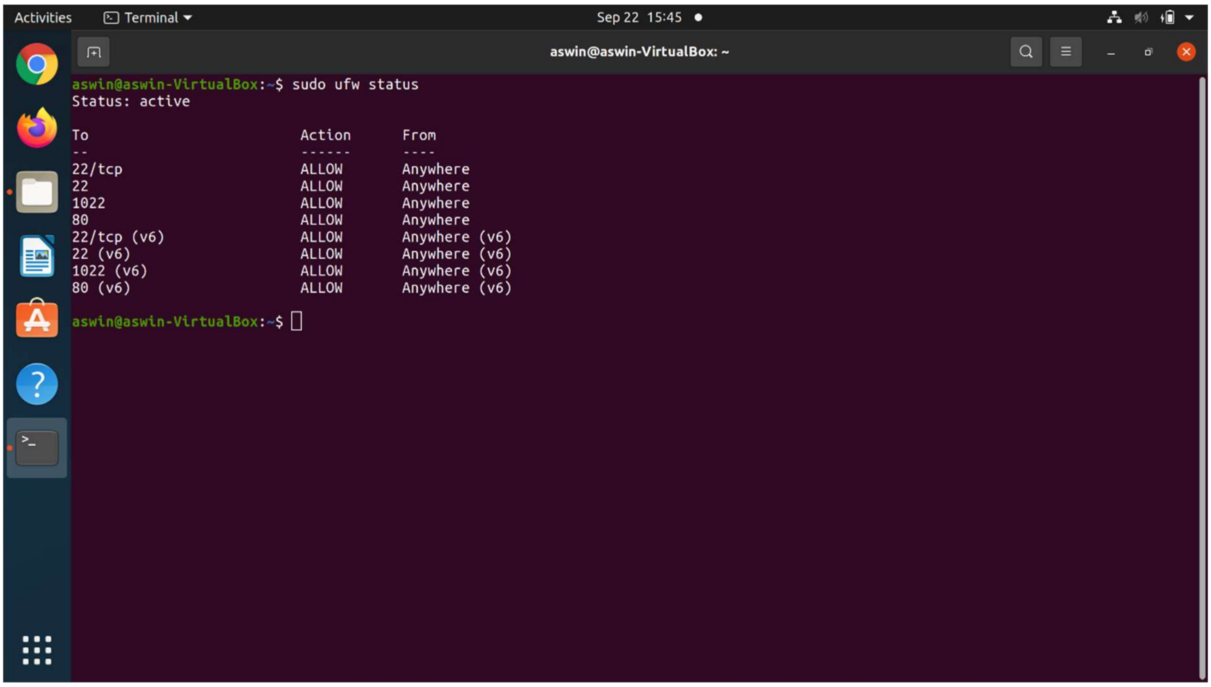
```
sudo ufw allow 80
```

We can check the UFW (Firewall) status using the below command

```
sudo ufw status
```



```
aswin@aswin-VirtualBox:~$ sudo ufw allow 80
Rule added
Rule added (v6)
aswin@aswin-VirtualBox:~$
```

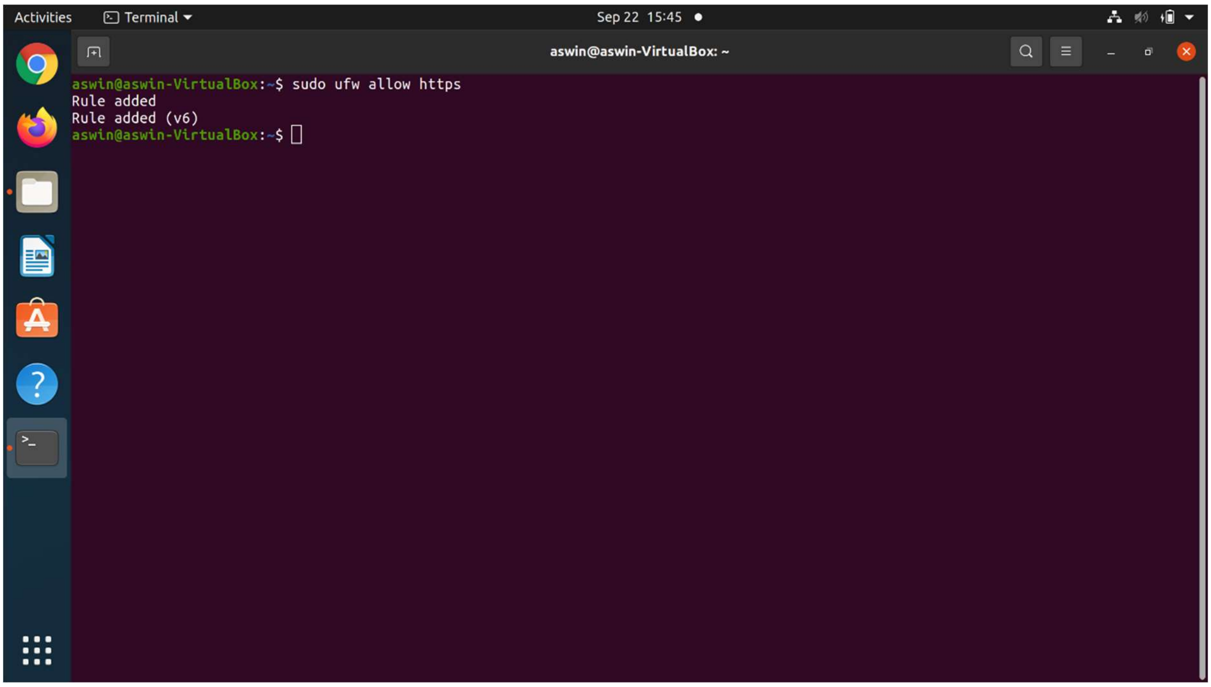


```
aswin@aswin-VirtualBox:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
22                         ALLOW       Anywhere
1022                       ALLOW       Anywhere
80                         ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
22 (v6)                    ALLOW       Anywhere (v6)
1022 (v6)                  ALLOW       Anywhere (v6)
80 (v6)                    ALLOW       Anywhere (v6)

aswin@aswin-VirtualBox:~$
```

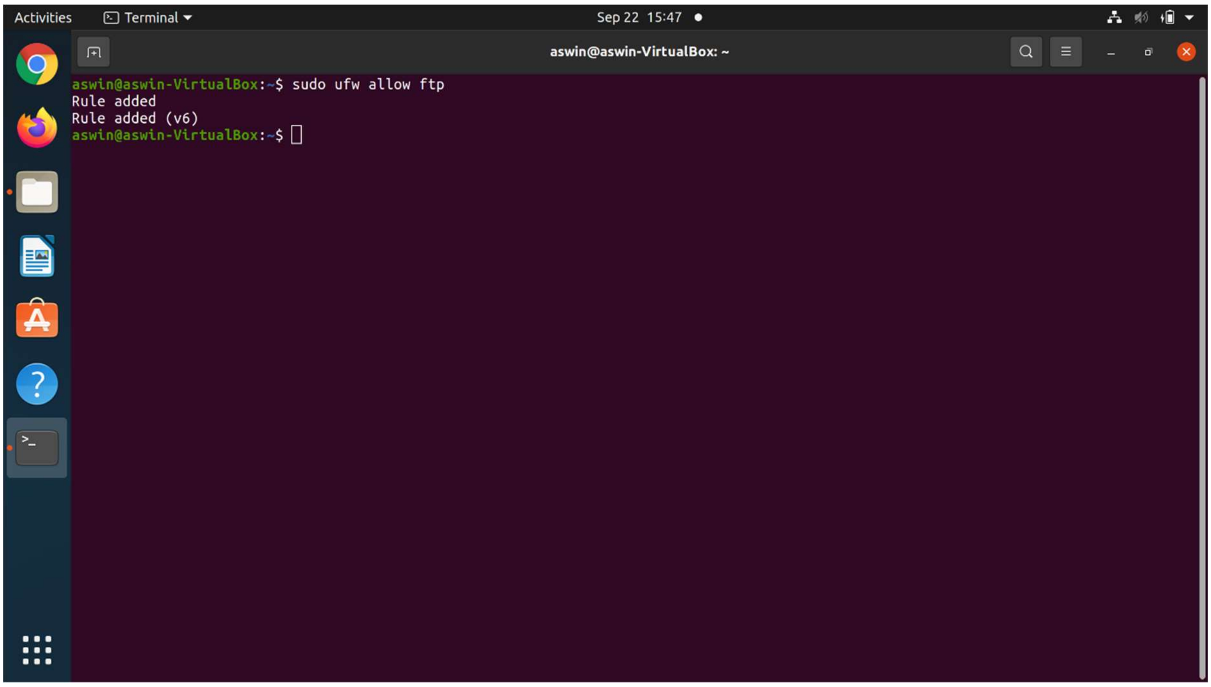
Like that will use the below command to enable HTTPs and FTP ports (443 and 21) respectively.

```
sudo ufw allow https
```

```
sudo ufw allow ftp
```



```
aswin@aswin-VirtualBox:~$ sudo ufw allow https
Rule added
Rule added (v6)
aswin@aswin-VirtualBox:~$
```

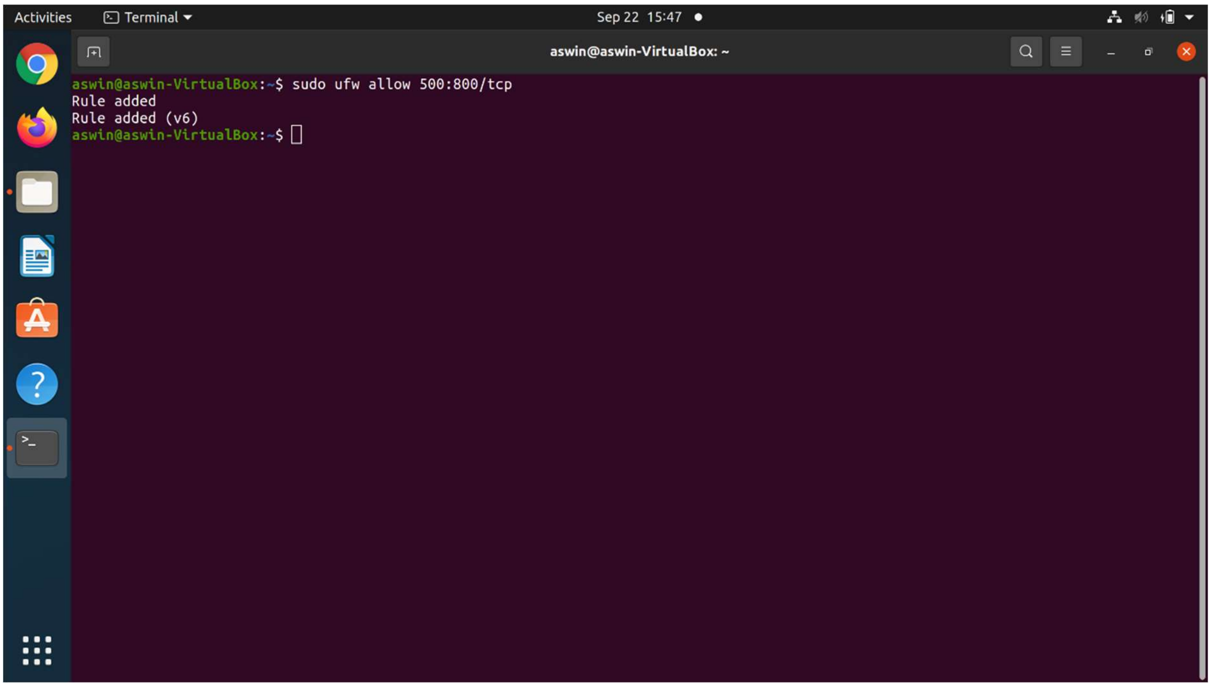


```
aswin@aswin-VirtualBox:~$ sudo ufw allow ftp
Rule added
Rule added (v6)
aswin@aswin-VirtualBox:~$ 
```

Enabling to Allow Specific Range of Ports

We can also allow or deny particular ranges of ports with UFW to allow the multiple ports instead of allowing single ports. Below is the command to enable a specific range of ports.

```
sudo ufw allow 500:800/tcp
```

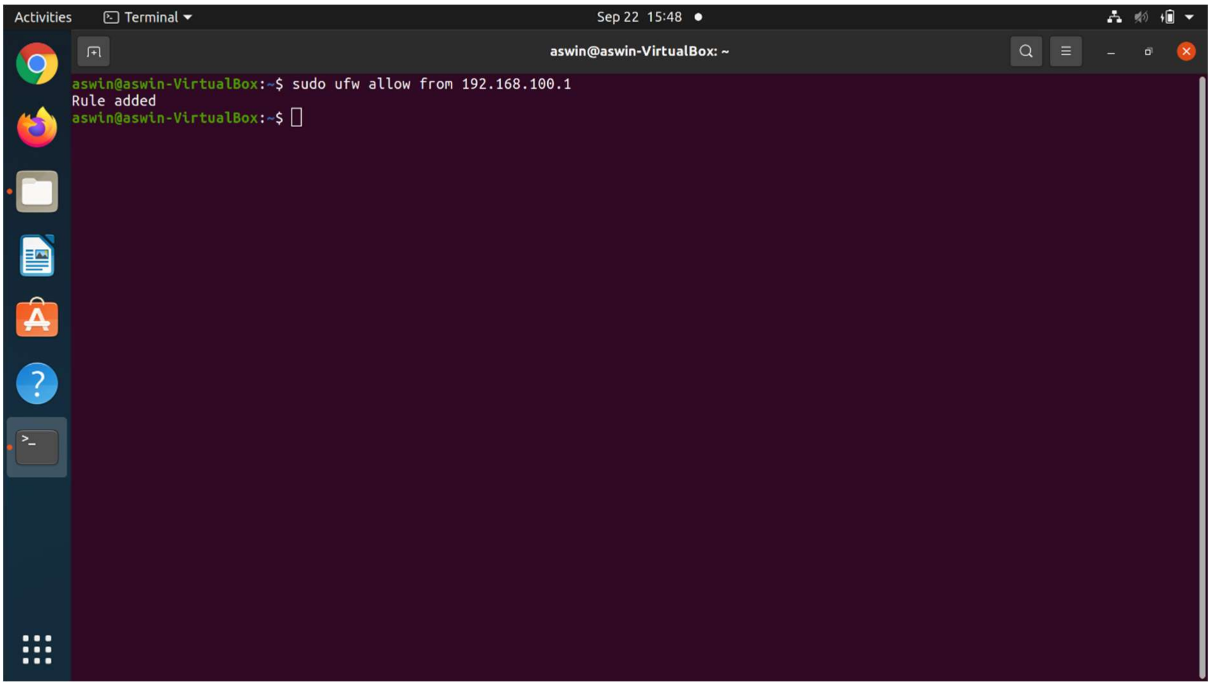


```
aswin@aswin-VirtualBox:~$ sudo ufw allow 500:800/tcp
Rule added
Rule added (v6)
aswin@aswin-VirtualBox:~$ 
```

Enable to Allow specific IP Addresses

If we want to allow a particular machine to allow for all the ports. We can use the below command.

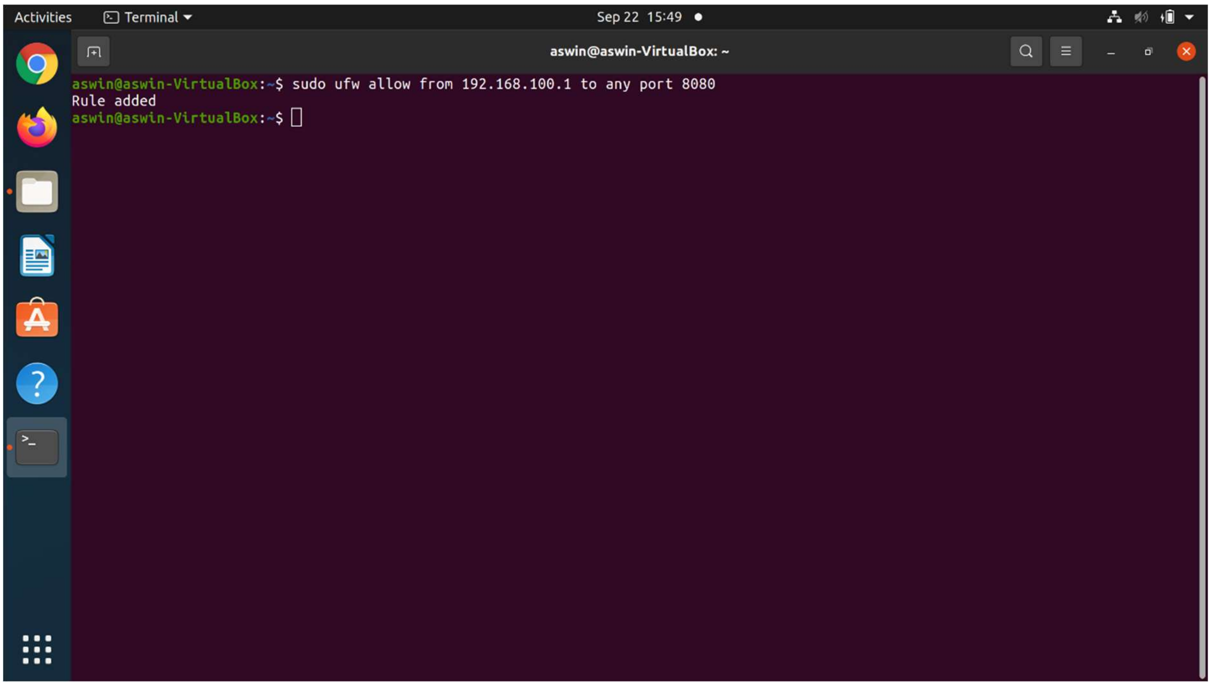
```
sudo ufw allow from 192.168.100.1
```



```
aswin@aswin-VirtualBox:~$ sudo ufw allow from 192.168.100.1
Rule added
aswin@aswin-VirtualBox:~$ 
```

If we want to allow for only specific port we can use the below command.

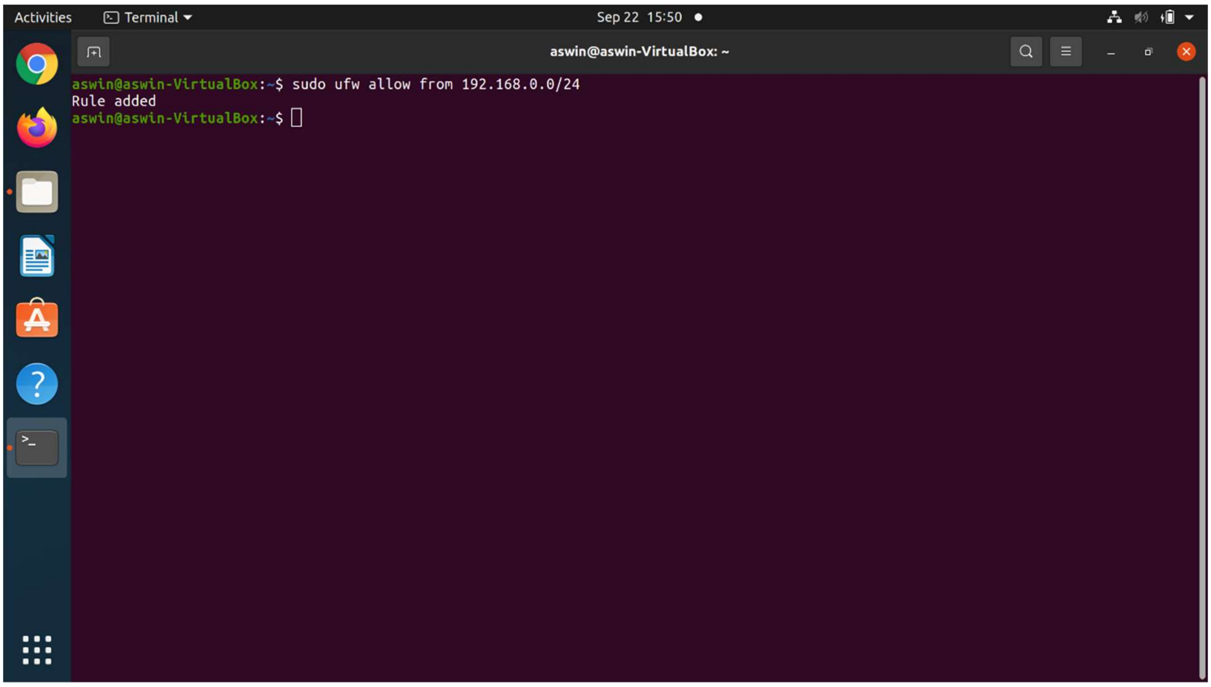
```
sudo ufw allow from 192.168.100.1 to any port 8080
```



```
aswin@aswin-VirtualBox:~$ sudo ufw allow from 192.168.100.1 to any port 8080
Rule added
aswin@aswin-VirtualBox:~$ 
```

If we want to enable the specific subnets like we want to enable for office networks we can use the below command.

```
sudo ufw allow from 192.168.0.0/24
```

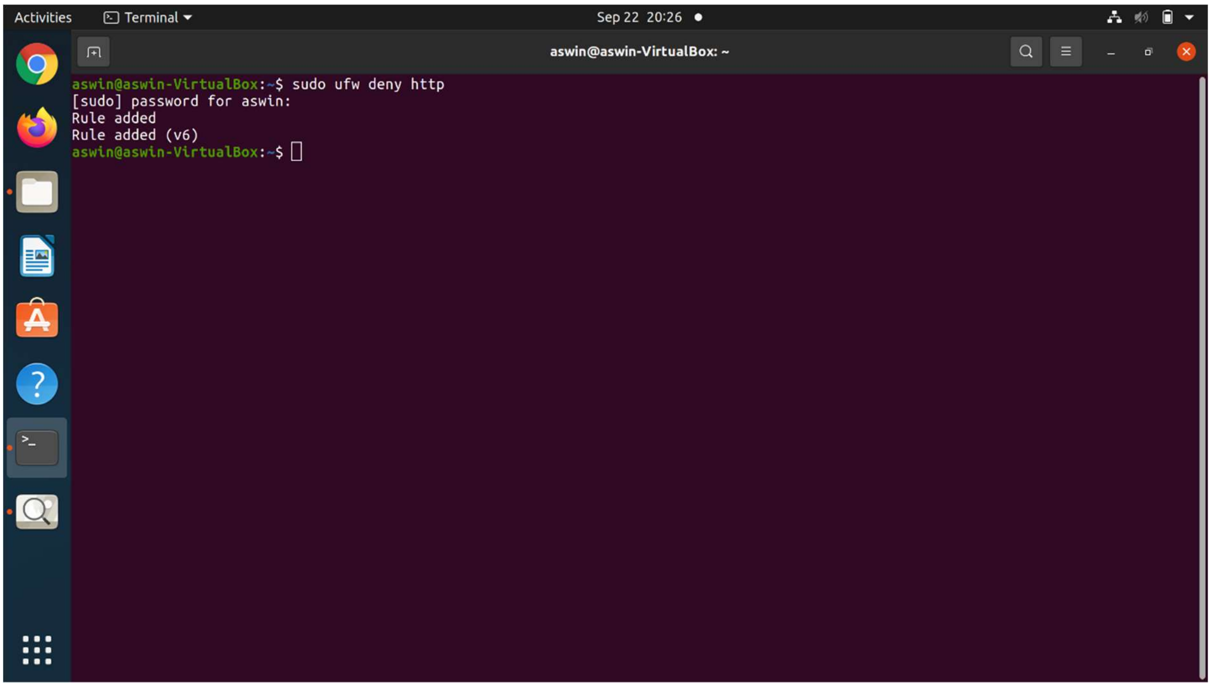


```
aswin@aswin-VirtualBox:~$ sudo ufw allow from 192.168.0.0/24
Rule added
aswin@aswin-VirtualBox:~$
```

Deny the Connections or Rules

If we want to deny any ports or network we can use the below commands to deny the connections.

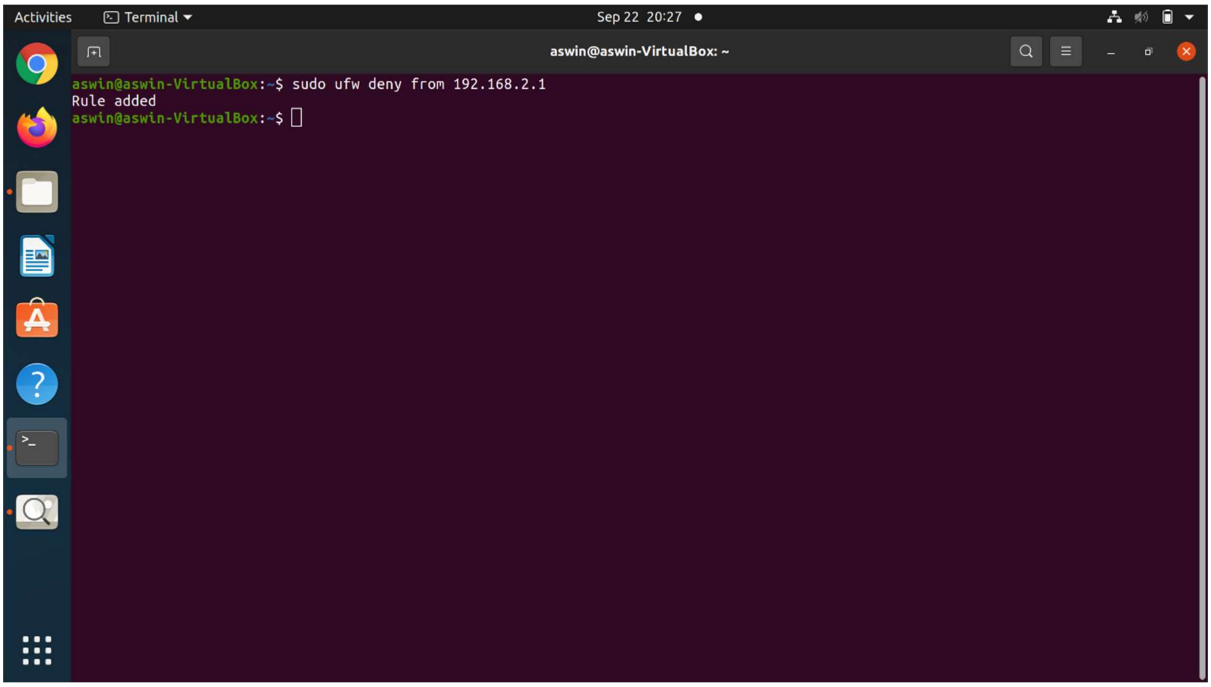
```
sudo ufw deny http
```



```
aswin@aswin-VirtualBox:~$ sudo ufw deny http
[sudo] password for aswin:
Rule added
Rule added (v6)
aswin@aswin-VirtualBox:~$
```

If we want to deny all the connects from a specific network we can use the below command.

```
sudo ufw deny from 192.168.2.1
```



```
aswin@aswin-VirtualBox:~$ sudo ufw deny from 192.168.2.1
Rule added
aswin@aswin-VirtualBox:~$ 
```

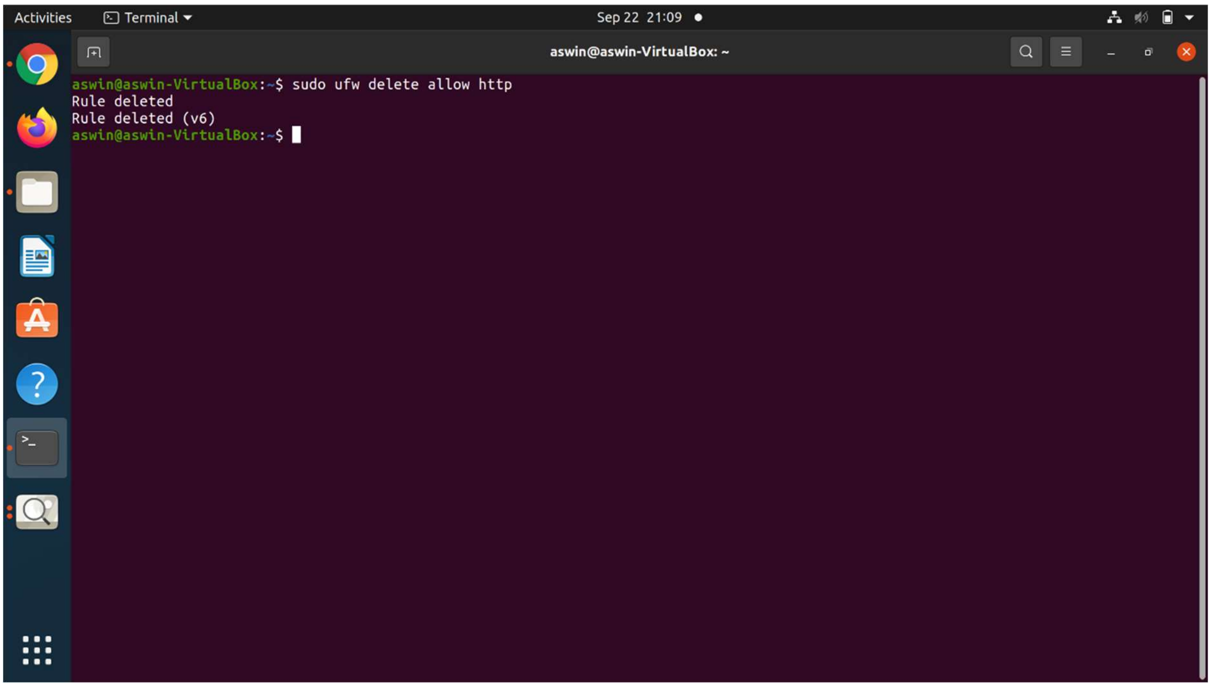
Deleting the Rules

We can delete the rules in two ways one with the actual rules and other with the rules numbers.

Actual Rules

The rules can be deleted using the actual rule which we allowed using the allow command. Below is the command to delete the HTTP rules from UFW.

```
sudo ufw allow http
```



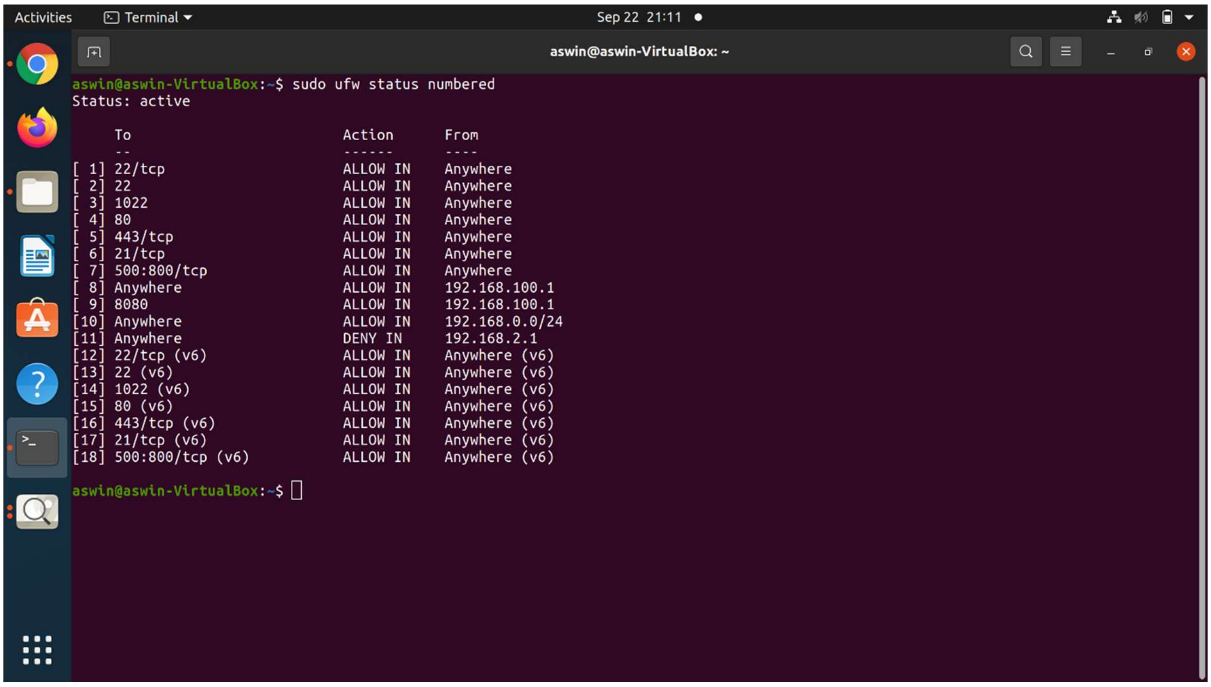
```
aswin@aswin-VirtualBox:~$ sudo ufw delete allow http
Rule deleted
Rule deleted (v6)
aswin@aswin-VirtualBox:~$ 
```

```
sudo ufw delete allow http
```

Rules Number

We can use the Rules numbers to delete the firewall rules, we can get the list of firewall rules with the below command.

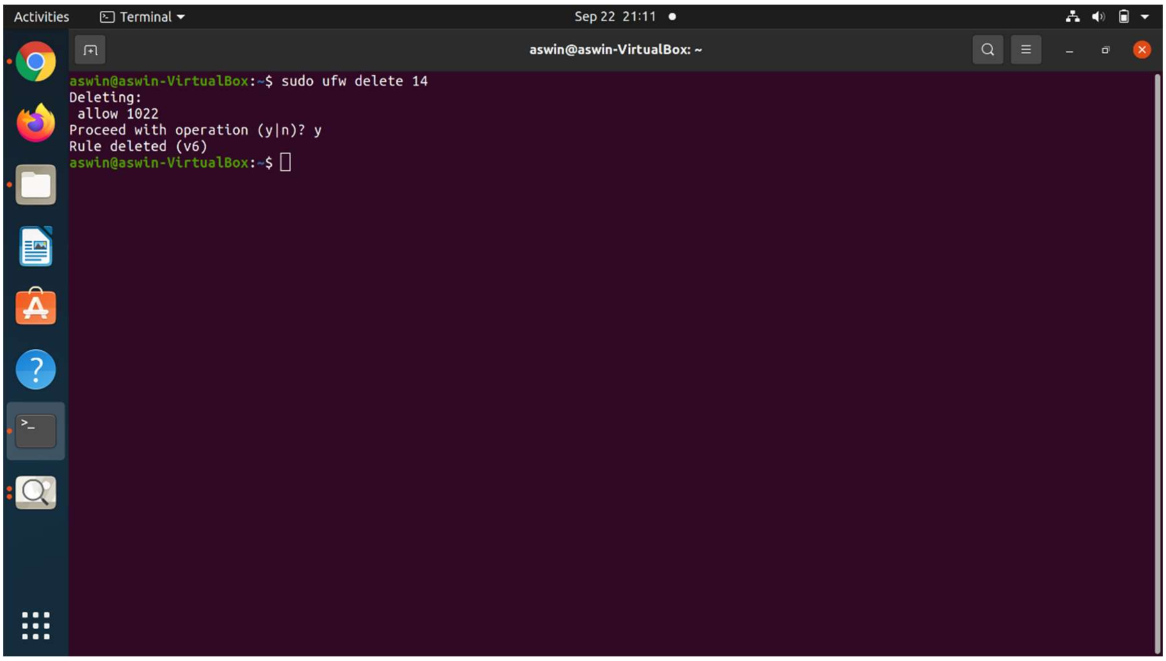
```
sudo ufw status numbered
```



```
aswin@aswin-VirtualBox:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22/tcp                     ALLOW IN    Anywhere
[ 2] 22                         ALLOW IN    Anywhere
[ 3] 1022                       ALLOW IN    Anywhere
[ 4] 80                         ALLOW IN    Anywhere
[ 5] 443/tcp                    ALLOW IN    Anywhere
[ 6] 21/tcp                     ALLOW IN    Anywhere
[ 7] 500:800/tcp                ALLOW IN    Anywhere
[ 8] Anywhere                   ALLOW IN    192.168.100.1
[ 9] 8080                       ALLOW IN    192.168.100.1
[10] Anywhere                   ALLOW IN    192.168.0.0/24
[11] Anywhere                   DENY IN     192.168.2.1
[12] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
[13] 22 (v6)                    ALLOW IN    Anywhere (v6)
[14] 1022 (v6)                  ALLOW IN    Anywhere (v6)
[15] 80 (v6)                    ALLOW IN    Anywhere (v6)
[16] 443/tcp (v6)               ALLOW IN    Anywhere (v6)
[17] 21/tcp (v6)                ALLOW IN    Anywhere (v6)
[18] 500:800/tcp (v6)           ALLOW IN    Anywhere (v6)

aswin@aswin-VirtualBox:~$
```

If we want to delete the rule 14, then we can use the below command to delete the rules with the below command.

```
sudo ufw delete 14
```



```
aswin@aswin-VirtualBox:~$ sudo ufw delete 14
Deleting:
 allow 1022
Proceed with operation (y|n)? y
Rule deleted (v6)
aswin@aswin-VirtualBox:~$
```