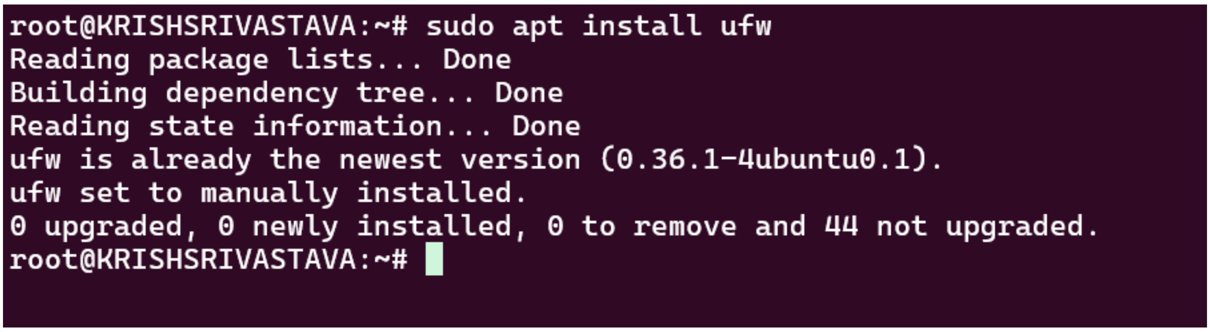
Lab Assignment 11

AP21110010302
Krish Srivastava
CSE – E
Network Security – CSE 315L

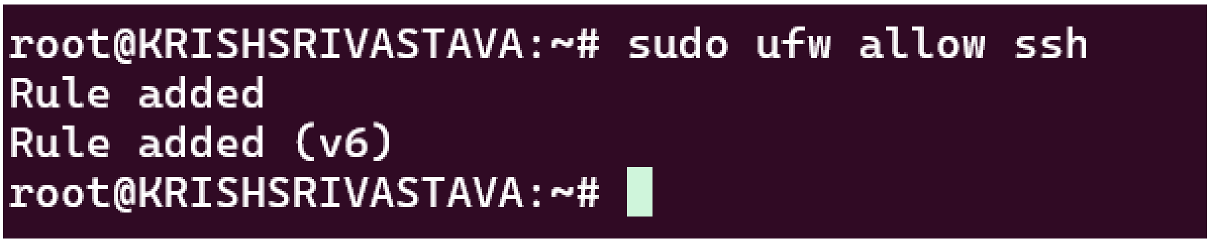


```
root@KRISHSRIVASTAVA:~# sudo apt install ufw
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ufw is already the newest version (0.36.1-4ubuntu0.1).
ufw set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 44 not upgraded.
root@KRISHSRIVASTAVA:~# █
```

Checking for **ufw**. Although it is pre-installed but still.

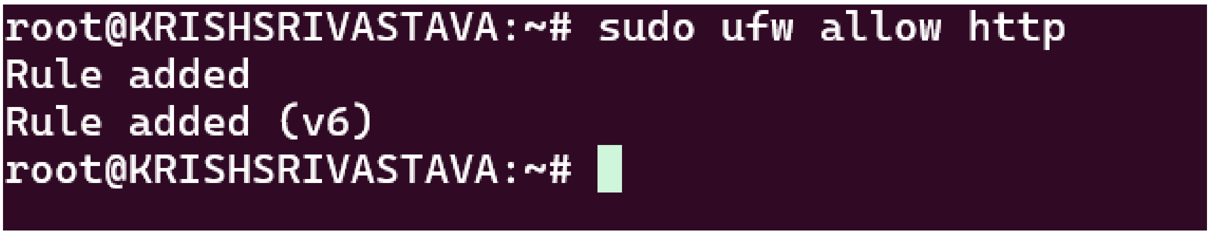
UFW denies all incoming connections and allows all outgoing connections. It means a client trying to reach out server would not be able to connect. But when a application from our server tries to connect to any server outside, it is allowed.

Now by default all incoming connections are denied. So we will allow **SSH** connections, using the following command

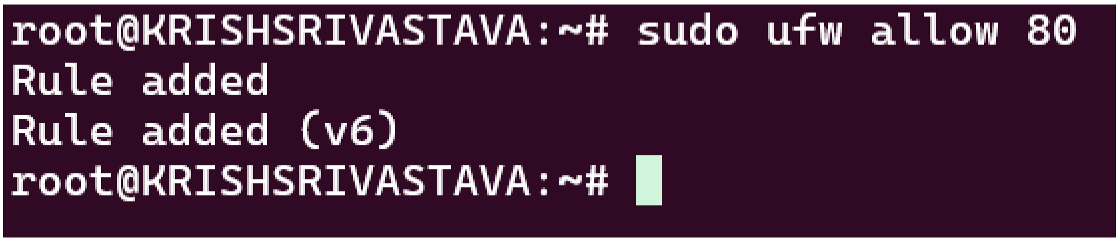


```
root@KRISHSRIVASTAVA:~# sudo ufw allow ssh
Rule added
Rule added (v6)
root@KRISHSRIVASTAVA:~# █
```

This command will allow connections on **port 22** that is the default port for **ssh**.



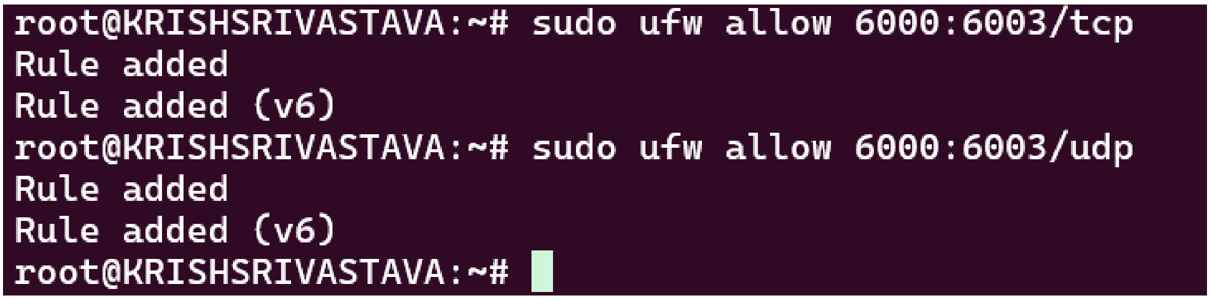
```
root@KRISHSRIVASTAVA:~# sudo ufw allow http
Rule added
Rule added (v6)
root@KRISHSRIVASTAVA:~# █
```



```
root@KRISHSRIVASTAVA:~# sudo ufw allow 80
Rule added
Rule added (v6)
root@KRISHSRIVASTAVA:~# █
```

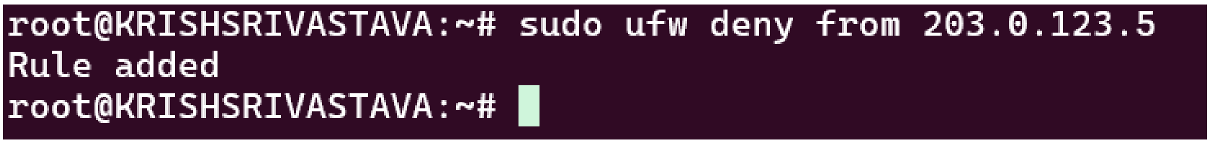
Allowing **http connection on port 80.** Therefore, above both commands are same.

To specify a range of ports with a protocol, that can also be done.



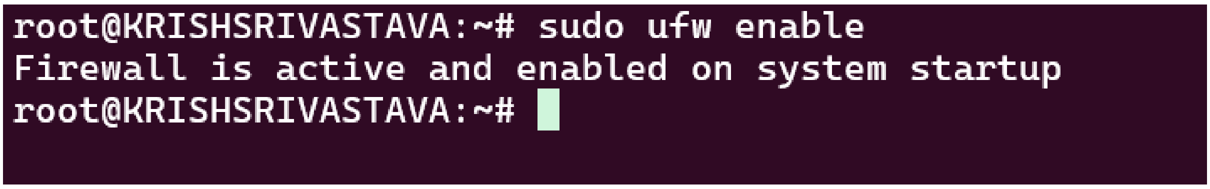
```
root@KRISHSRIVASTAVA:~# sudo ufw allow 6000:6003/tcp
Rule added
Rule added (v6)
root@KRISHSRIVASTAVA:~# sudo ufw allow 6000:6003/udp
Rule added
Rule added (v6)
root@KRISHSRIVASTAVA:~#
```

Some malicious IP addresses can also be denied using this:



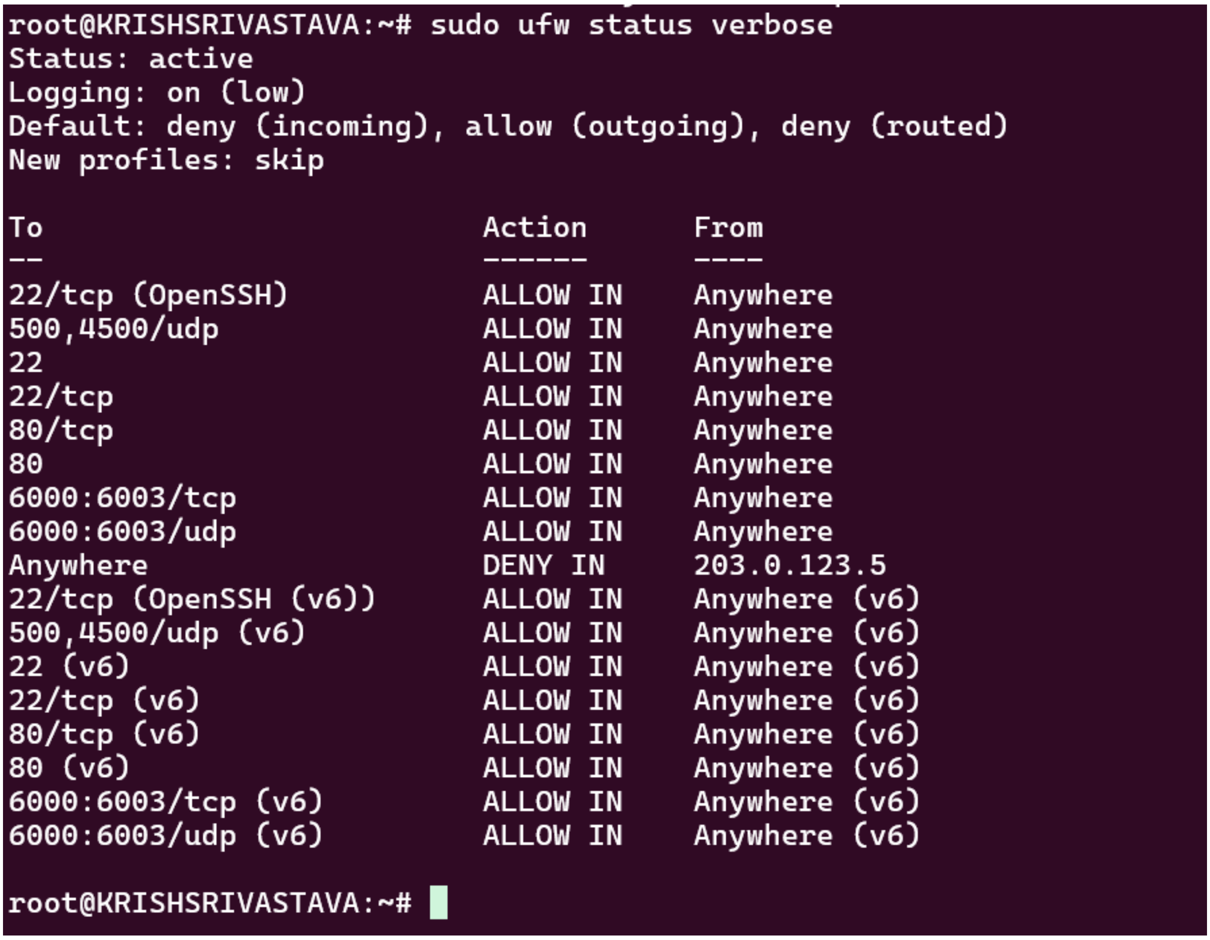
```
root@KRISHSRIVASTAVA:~# sudo ufw deny from 203.0.123.5
Rule added
root@KRISHSRIVASTAVA:~#
```

At the end we will enable the firewall



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

Now to check the status of **ufw**,



```
root@KRISHSRIVASTAVA:~# sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), deny (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp (OpenSSH)           ALLOW IN    Anywhere
500,4500/udp               ALLOW IN    Anywhere
22                         ALLOW IN    Anywhere
22/tcp                     ALLOW IN    Anywhere
80/tcp                     ALLOW IN    Anywhere
80                         ALLOW IN    Anywhere
6000:6003/tcp              ALLOW IN    Anywhere
6000:6003/udp              ALLOW IN    Anywhere
Anywhere                   DENY IN     203.0.123.5
22/tcp (OpenSSH (v6))      ALLOW IN    Anywhere (v6)
500,4500/udp (v6)          ALLOW IN    Anywhere (v6)
22 (v6)                    ALLOW IN    Anywhere (v6)
22/tcp (v6)                ALLOW IN    Anywhere (v6)
80/tcp (v6)                ALLOW IN    Anywhere (v6)
80 (v6)                    ALLOW IN    Anywhere (v6)
6000:6003/tcp (v6)         ALLOW IN    Anywhere (v6)
6000:6003/udp (v6)         ALLOW IN    Anywhere (v6)

root@KRISHSRIVASTAVA:~#
```