Project: Configuring a Firewall in Linux

Motivation:

My motivation for choosing the project "Configuring a Firewall in Linux" is to develop practical skills in network security, which are crucial in protecting systems against cyber threats. By working on this project, I aim to enhance my understanding of firewall mechanisms and gain hands-on experience with Linux-based security tools.

What is Firewall:

A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external networks, such as the internet, to block unauthorized access and protect against cyber threats.

What is UFW:

UFW (Uncomplicated Firewall) is a user-friendly interface for managing firewall rules on Linux systems. It simplifies the process of configuring and managing firewall settings, making it accessible even to those with limited experience in network security.

Software Required:

- Linux Operating System
- UFW (Uncomplicated Firewall)
- SSH Client
- Text Editor
- Network Tools
- Log Monitoring Tools

Installing UFW:

- sudo apt-get install ufw

Using UFW to set Default Firewall Rules:

- sudo ufw default allow outgoing
- sudo ufw default deny incoming

Adding Rules:

To allow both incoming and outgoing connections on port 22 for SSH

- **sudo ufw allow 22**

Or we can also run:

- **sudo ufw allow ssh**

Similarly, to deny traffic on a certain port we have to run:

- **sudo ufw deny 22**

To further fine-tune the rules, we can also allow packets based on TCP or UDP. The below command allows TCP packets on port 80:

- **sudo ufw allow 80/tcp**

Or we can also run:

- **sudo ufw allow http/tcp**

This below command will allow UDP packets on 1725:

- **sudo ufw allow 1725/udp**

Advanced Rules:

Along with allowing or denying based solely on port, UFW also allows us to allow/block by IP addresses, subnets, and the IP address/subnet/port combinations.

To allow connections from an IP address:

- **sudo ufw allow from 192.168.58.237**

To allow connections from a specific subnet:

- **sudo ufw allow from 192.168.58/24**

To allow a specific IP address/port combination:

- **sudo ufw allow from 192.168.58.237 to any port 22 proto tcp**

To remove the rules:

To remove a rule, add delete before the rule implementation.

- **sudo ufw delete allow 80/tcp**

Enable the Firewall:

To enable UFW and enforce your firewall rules:

- **sudo ufw enable**

UFW Status:

We can check the status of UFW at any time with the command:

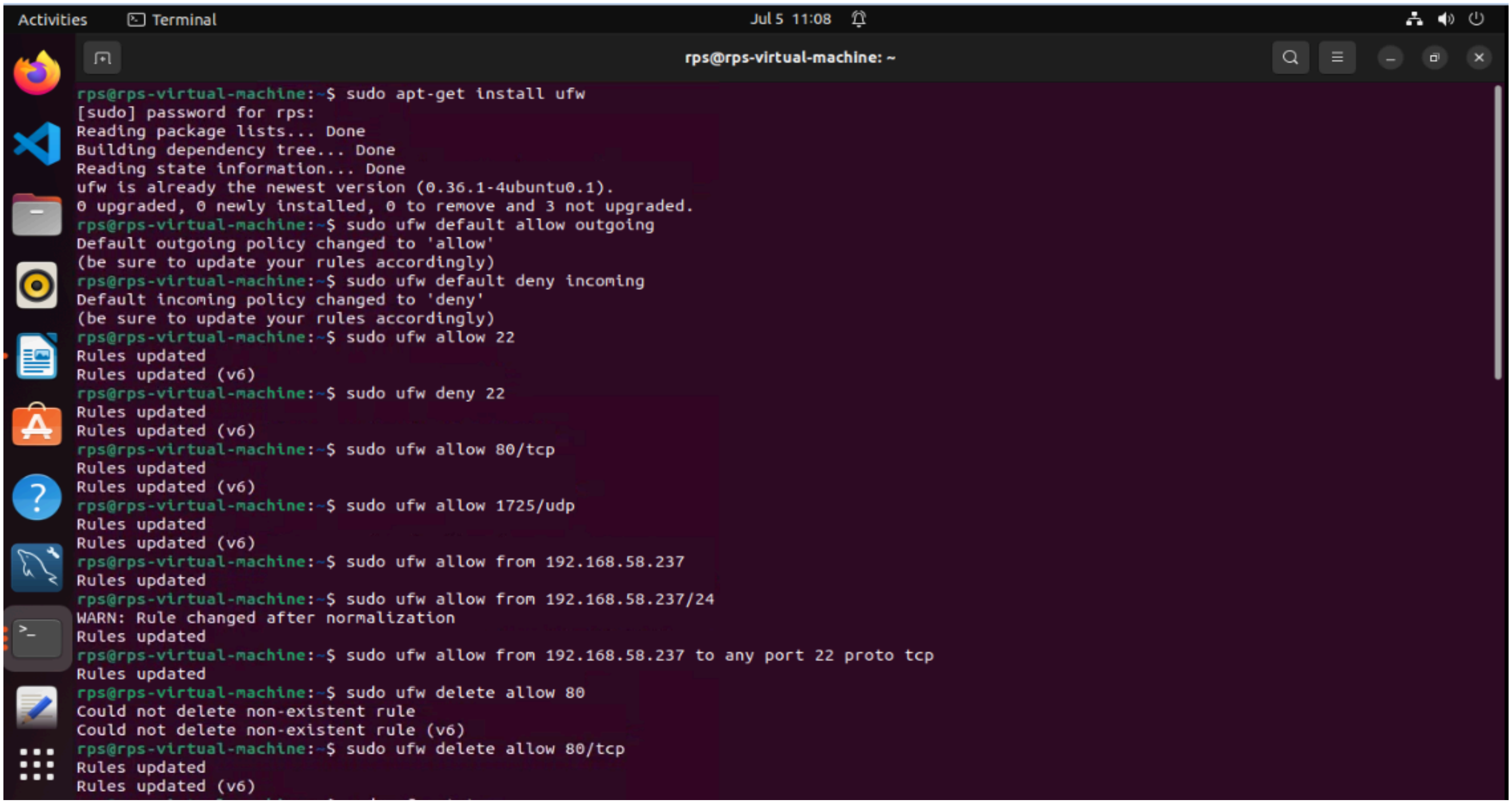
- **sudo ufw status**

This will show a list of all rules, and whether or not UFW is active.

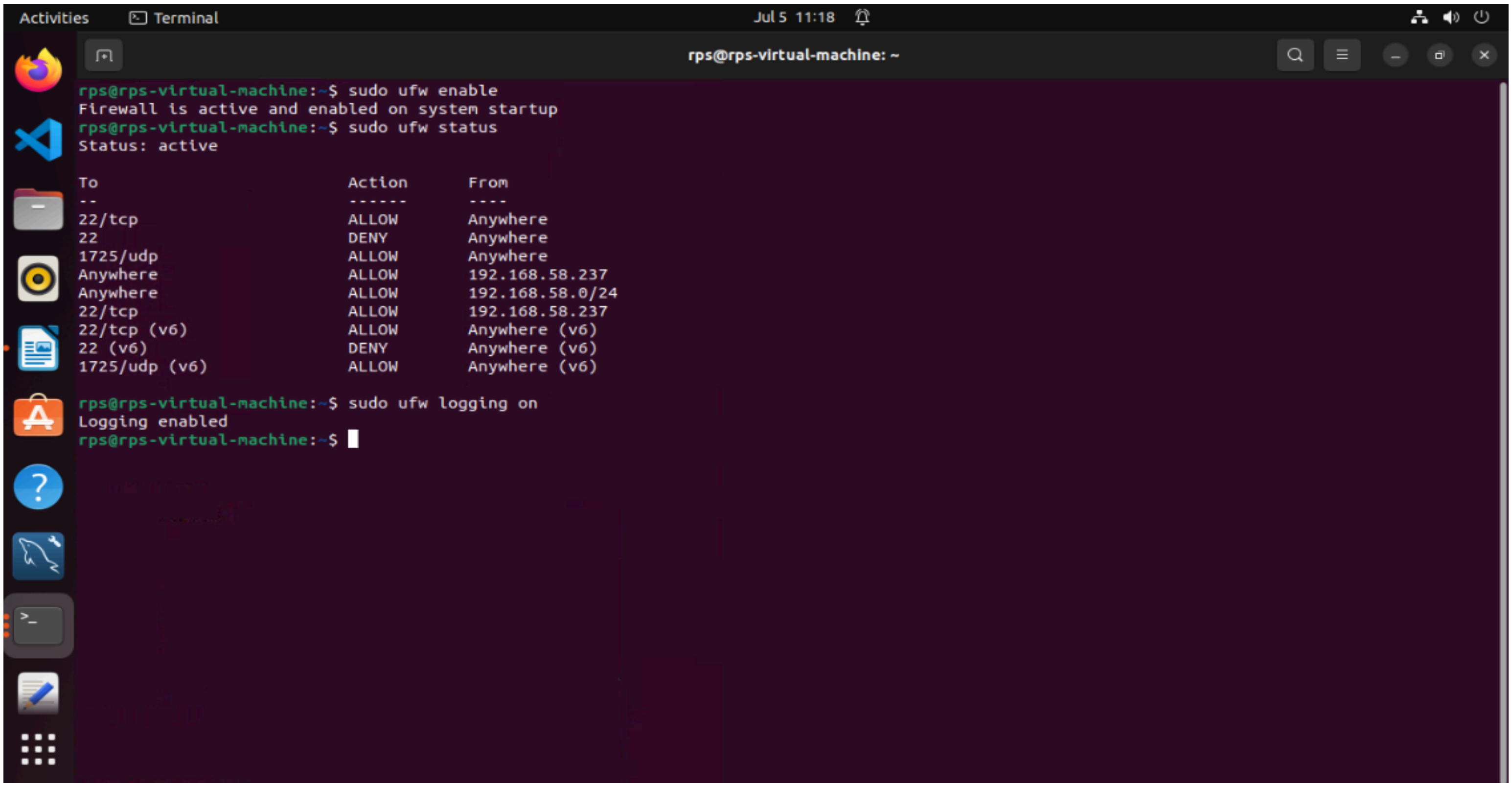
Logging:

We can enable logging with the command:

- **sudo ufw logging on**



```
rps@rps-virtual-machine:~$ sudo apt-get install ufw
[sudo] password for rps:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ufw is already the newest version (0.36.1-4ubuntu0.1).
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
rps@rps-virtual-machine:~$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
rps@rps-virtual-machine:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
rps@rps-virtual-machine:~$ sudo ufw allow 22
Rules updated
Rules updated (v6)
rps@rps-virtual-machine:~$ sudo ufw deny 22
Rules updated
Rules updated (v6)
rps@rps-virtual-machine:~$ sudo ufw allow 80/tcp
Rules updated
Rules updated (v6)
rps@rps-virtual-machine:~$ sudo ufw allow 1725/udp
Rules updated
Rules updated (v6)
rps@rps-virtual-machine:~$ sudo ufw allow from 192.168.58.237
Rules updated
rps@rps-virtual-machine:~$ sudo ufw allow from 192.168.58.237/24
WARN: Rule changed after normalization
Rules updated
rps@rps-virtual-machine:~$ sudo ufw allow from 192.168.58.237 to any port 22 proto tcp
Rules updated
rps@rps-virtual-machine:~$ sudo ufw delete allow 80
Could not delete non-existent rule
Could not delete non-existent rule (v6)
rps@rps-virtual-machine:~$ sudo ufw delete allow 80/tcp
Rules updated
Rules updated (v6)
```



```
rps@rps-virtual-machine:~$ sudo ufw enable
Firewall is active and enabled on system startup
rps@rps-virtual-machine:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
22                         DENY        Anywhere
1725/udp                   ALLOW       Anywhere
Anywhere                   ALLOW       192.168.58.237
Anywhere                   ALLOW       192.168.58.0/24
22/tcp                     ALLOW       192.168.58.237
22/tcp (v6)                ALLOW       Anywhere (v6)
22 (v6)                    DENY        Anywhere (v6)
1725/udp (v6)              ALLOW       Anywhere (v6)

rps@rps-virtual-machine:~$ sudo ufw logging on
Logging enabled
rps@rps-virtual-machine:~$ 
```