Veermata Jijabai Technological Institute, Mumbai 400019

Experiment No.: 04

Aim: Firewall based

Group : Pratiksha Sankhe – 201071049

Kiran Patil - 211070904

Mayuresh Murudkar - 211070903

Branch: Computer Engineering

Batch: D

Aim: Practical Experiment on Firewall

Theory:

Firewall

1. A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
2. Firewalls have been a first line of defense in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.
3. A firewall can be hardware, software, software-as-a service (SaaS), public cloud, or private cloud (virtual).

GUFW

1. The GUFW (graphical uncomplicated firewall) is the graphical user interface for the UFW program. The GUI version of the tool helps control the built-in firewall system on Ubuntu through a simple interface.
2. The simple interface enables creating firewall rules and managing settings with minimal effort. GUFW allows controlling incoming and outgoing network traffic based on specified criteria.

Steps to Set Up Firewall With GUFW

1. Install GUFW Via Terminal

```
$ sudo apt-get install gufw
```

2. Turn on Firewall

To open the Firewall Configuration, enter the following command in the terminal:

```
$ sudo gufw
```

Or open by clicking on Firewall Configuration program in menu

The Status switch controls whether the firewall is running.

Switch the firewall status on or off to enable or disable the firewall. The firewall logo changes color, and the bottom of the window shows the current firewall status.

1. Add GUFW rules

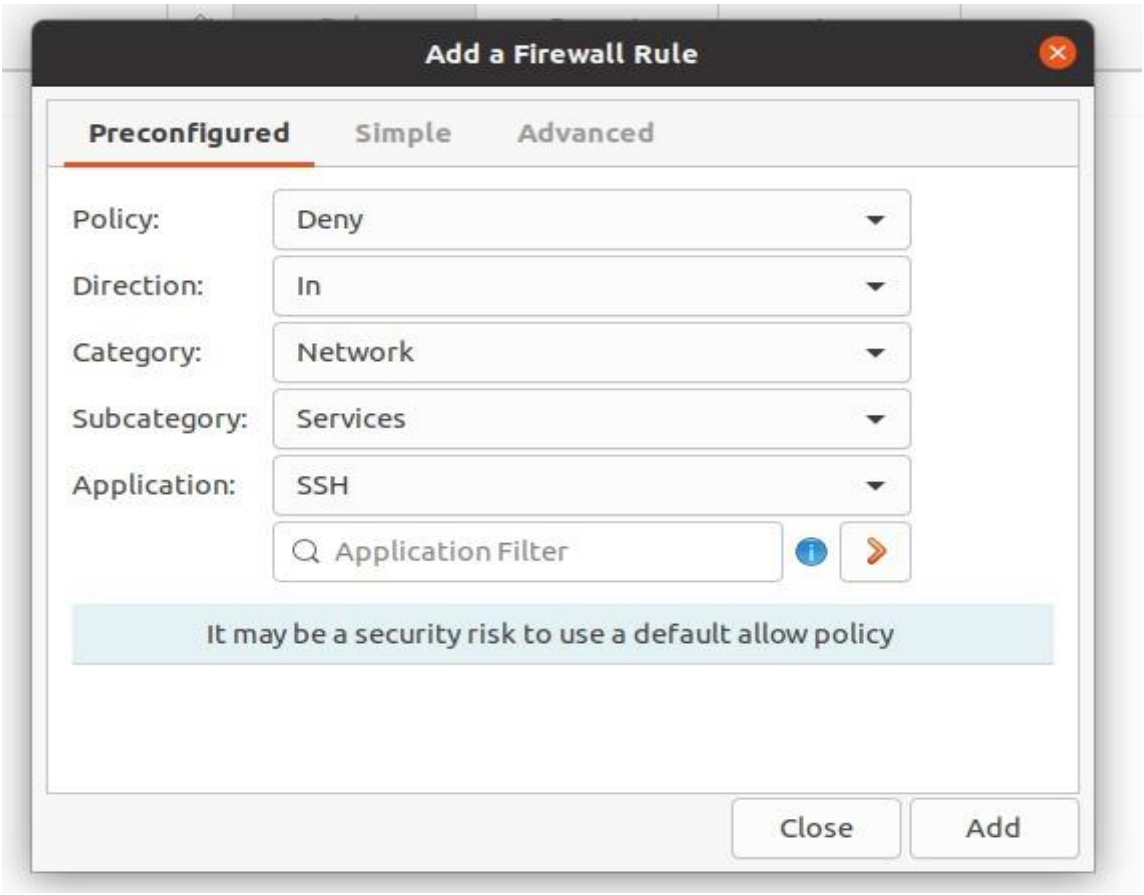
Every GUFW profile allows adding custom rules. The firewall rules require knowledge of the network environment and security requirements. Update and manage rules regularly to control the network traffic.

The available network rule policies in GUFW are:

- Allow. Accepts all traffic entry on a port.
- Deny. Denies all traffic entry on a port.
- Reject. Denies all traffic entry on a port and informs the requester.
- Limit. Denies traffic if more than six attempts happened in the previous thirtyseconds.

Implementation:

```
pratiksha@pratiksha-ubuntu:~$ sudo apt-get install gufw
[sudo] password for pratiksha:
Sorry, try again.
[sudo] password for pratiksha:
Sorry, try again.
[sudo] password for pratiksha:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  gufw
0 upgraded, 1 newly installed, 0 to remove and 22 not upgraded.
Need to get 860 kB of archives.
After this operation, 3,539 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu focal-updates/universe amd64 gufw all 20.04.1-1ubuntu1 [860 kB]
Fetched 860 kB in 2s (471 kB/s)
Selecting previously unselected package gufw.
(Reading database ... 188940 files and directories currently installed.)
Preparing to unpack .../gufw_20.04.1-1ubuntu1_all.deb ...
Unpacking gufw (20.04.1-1ubuntu1) ...
Setting up gufw (20.04.1-1ubuntu1) ...
Processing triggers for desktop-file-utils (0.24-1ubuntu3) ...
Processing triggers for mime-support (3.64ubuntu1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu1) ...
Processing triggers for man-db (2.9.1-1) ...
pratiksha@pratiksha-ubuntu:~$
```



File Edit Help

Firewall

Profile: Home

Status:

Incoming: Deny

Outgoing: Allow

N°	Rule	Name
1	22/tcp DENY IN Anywhere	SSH
2	22/tcp (v6) DENY IN Anywhere (v6)	SSH

```
pratiksha@pratiksha-ubuntu:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     DENY        Anywhere
22/tcp (v6)                DENY        Anywhere (v6)

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

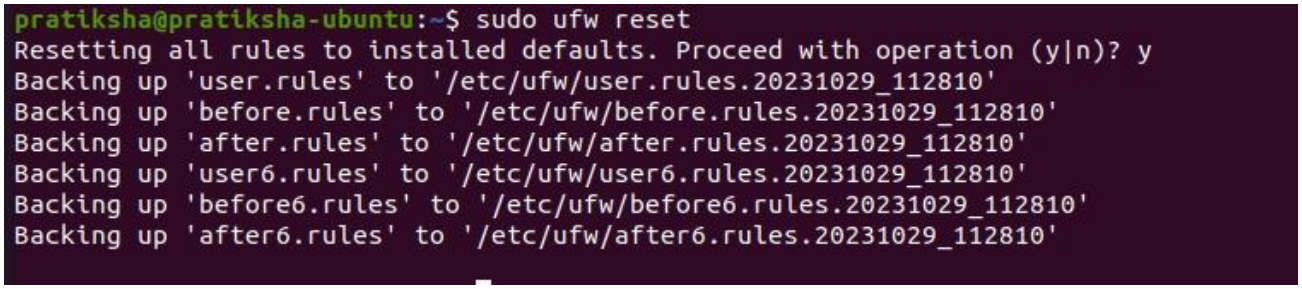
```
pratiksha@pratiksha-ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.198.128  netmask 255.255.255.0  broadcast 192.168.198.255
        inet6 fe80::ddc9:beb9:8efd:9f3  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:a5:d1:de  txqueuelen 1000  (Ethernet)
        RX packets 181613  bytes 272643704 (272.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 33354  bytes 2058473 (2.0 MB)
        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 227  bytes 19931 (19.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 227  bytes 19931 (19.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\PRATIK SANKHE> ssh 192.168.198.128
ssh: connect to host 192.168.198.128 port 22: Connection refused
PS C:\Users\PRATIK SANKHE>
```



Conclusion: Thus, from this experiment, we successfully setup firewall using GUFW in Ubuntu.