EXPERIMENT 6

Ameya Daddikar - 161070015

AIM:

To implement a firewall using GUFW.

THEORY:

Firewalls are programs used to provide security between an internal and an external network (which may be the Internet). They monitor incoming and outgoing traffic and decide to allow or reject traffic depending upon policies, learnt patterns, heuristics etc. In its simplest implementation, a firewall will have a set of rules determining whether particular traffic should be allowed through based on criteria like protocol, port and source/destination IP address.

The various firewalls are:

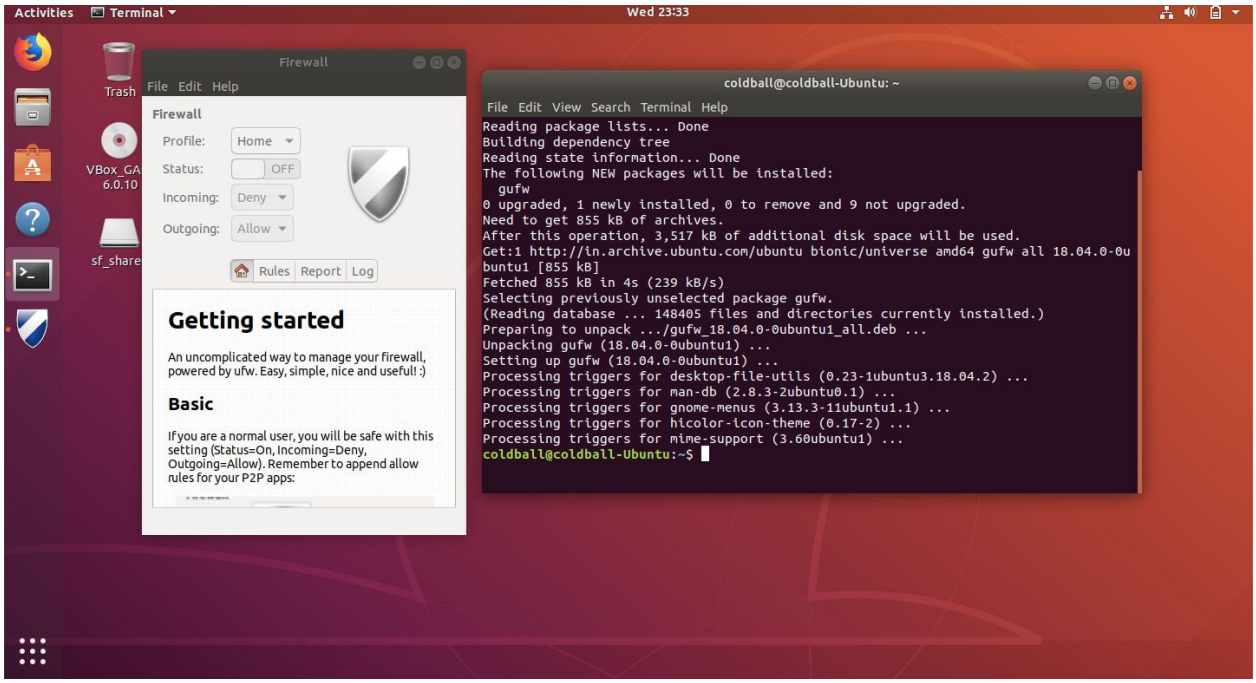
- Packet filters:
  They act by simply inspecting packets. If the packets follow the rules, they are allowed in or out. This is the simplest type, and does not provide protection against unknown vulnerabilities without default deny, in which case availability may be reduced.
- Circuit-level gateways
  It monitors TCP handshaking among packets across trusted clients or servers and untrusted hosts. It thus determines whether a requested session is legitimate. A trusted client requests a service, and the gateway accepts this request. On behalf of the client, the gateway opens a connection to the requested untrusted host and then closely monitors the TCP handshaking that follows. It works at the session layer of the OSI model, transport layer of TCP/IP
- Application gateways:
  These work at the application layer. They can understand the packets coming in and decide if an unwanted service is attempting to break in.

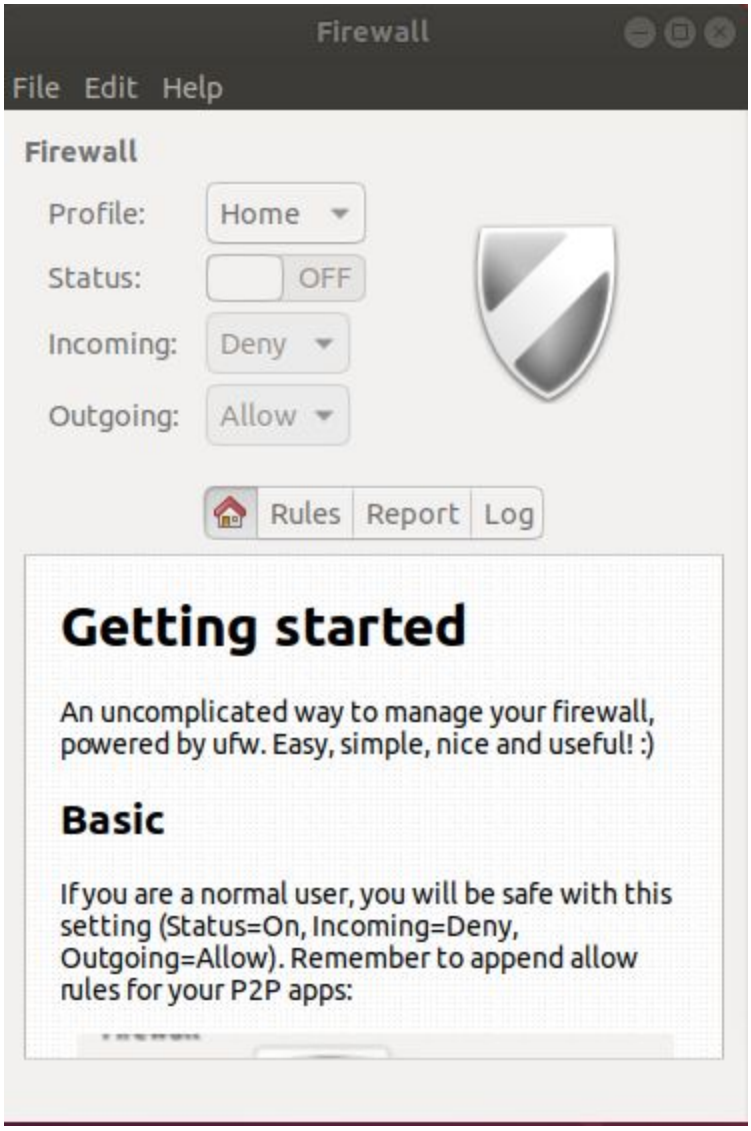
PRACTICAL:

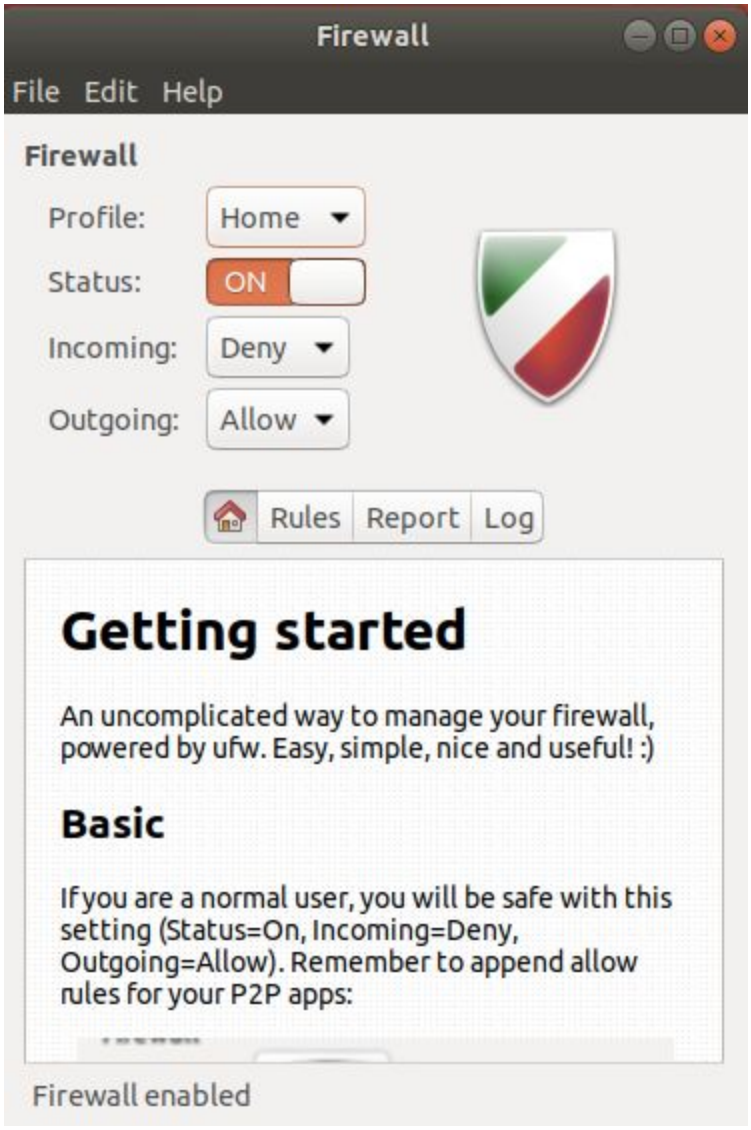
GUFW is a graphical utility for managing Uncomplicated Firewall (**UFW**), which is a frontend to iptables, the basic framework for firewalls.

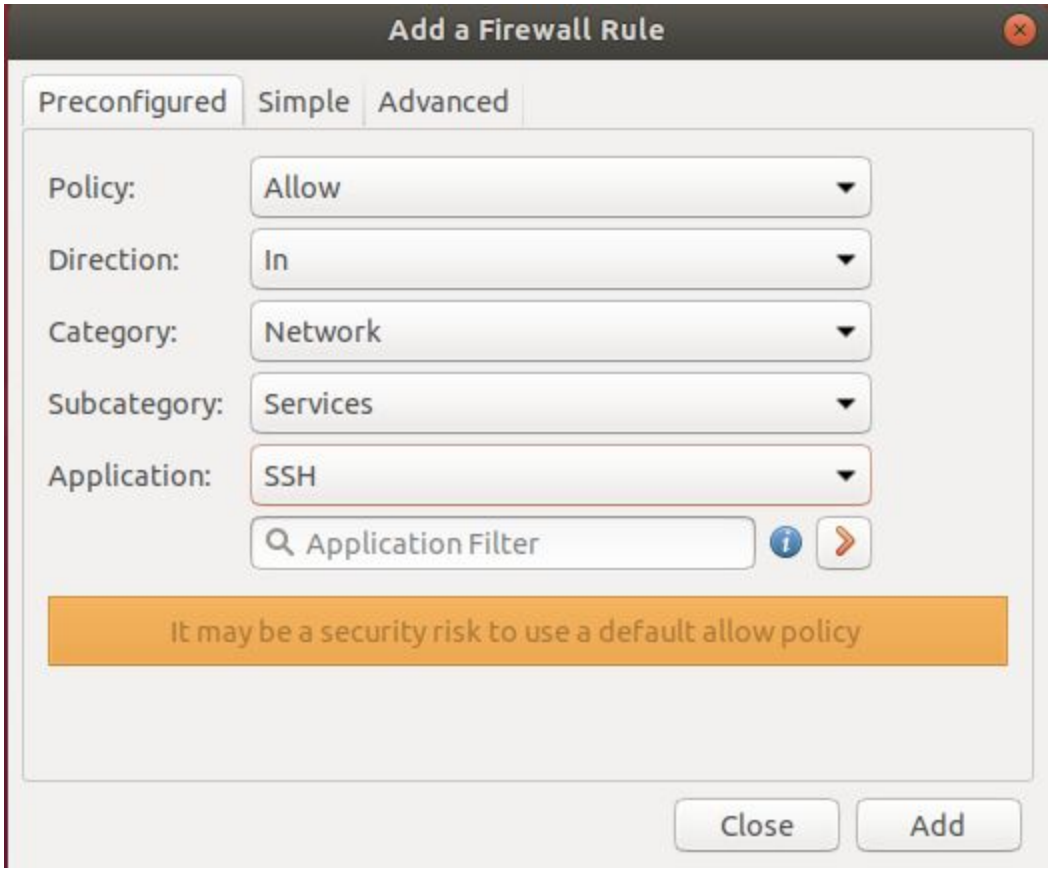
- Install with
  sudo apt install gufw -y
- Turn Status to On
- There are three profiles:
  - Home
  - Public
  - Office

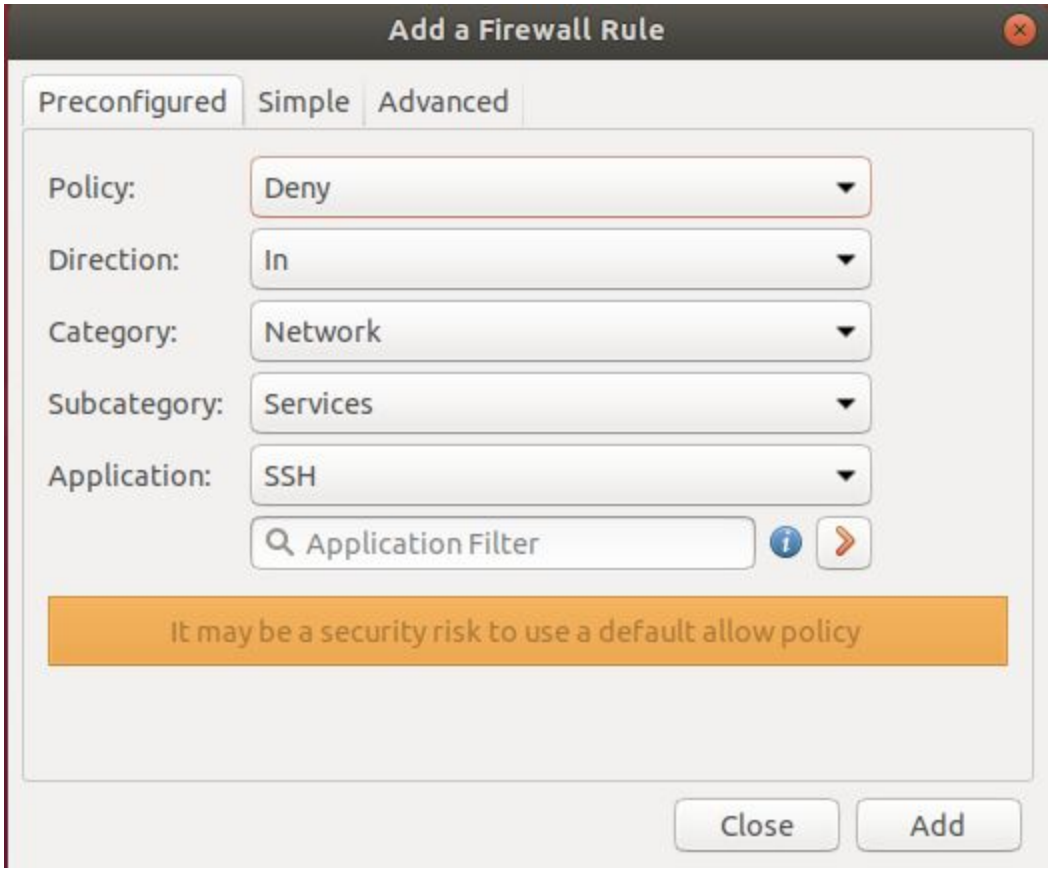
- Select Rules tab
- Select + to add
- Allow, Deny, Reject and Limit are the policies.
    - **Allow:** allows any entry traffic to a port
    - **Deny:** denies any entry traffic to a port
    - **Reject:** denies any entry traffic to a port and informs the requester about the rejection
    - **Limit:** denies entry traffic if an IP address has attempted to initiate 6 or more connections in the last 30 seconds
- Direction may be incoming/outgoing
- Category, Subcategory and application select the scope of the rule
- Finally, press add




Firewall
File Edit Help
Firewall
Profile:
Home
Status:
OFF
Incoming:
Deny
Outgoing:
Allow
Rules
Report
Log
Getting started
An uncomplicated way to manage your firewall, powered by ufw. Easy, simple, nice and useful! :)
Basic
If you are a normal user, you will be safe with this setting (Status=On, Incoming=Deny, Outgoing=Allow). Remember to append allow rules for your P2P apps:


Firewall
File Edit Help
Firewall
Profile:
Home
Status:
ON
Incoming:
Deny
Outgoing:
Allow
Rules
Report
Log
Getting started
An uncomplicated way to manage your firewall, powered by ufw. Easy, simple, nice and useful! :)
Basic
If you are a normal user, you will be safe with this setting (Status=On, Incoming=Deny, Outgoing=Allow). Remember to append allow rules for your P2P apps:
Firewall enabled

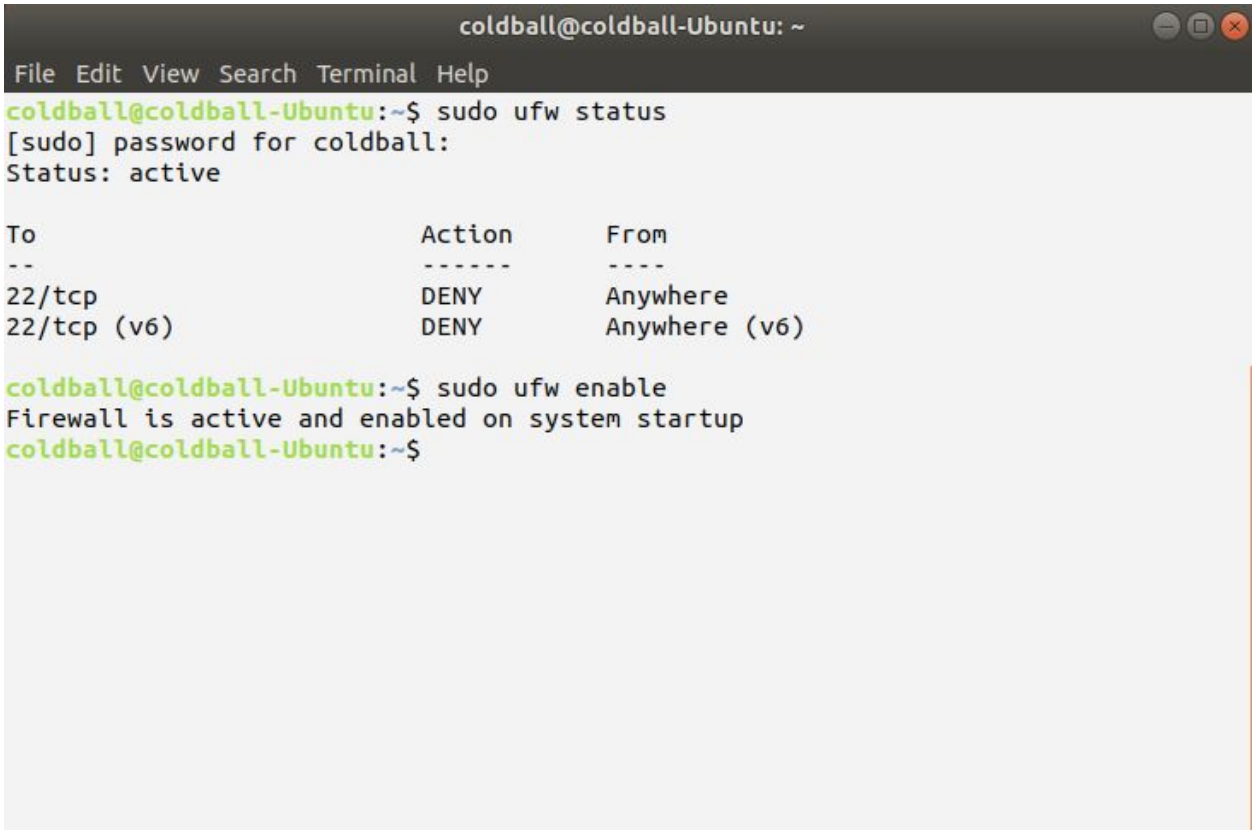

Add a Firewall Rule
Preconfigured
Simple
Advanced
Policy:
Allow
Direction:
In
Category:
Network
Subcategory:
Services
Application:
SSH
Application Filter
It may be a security risk to use a default allow policy
Close
Add

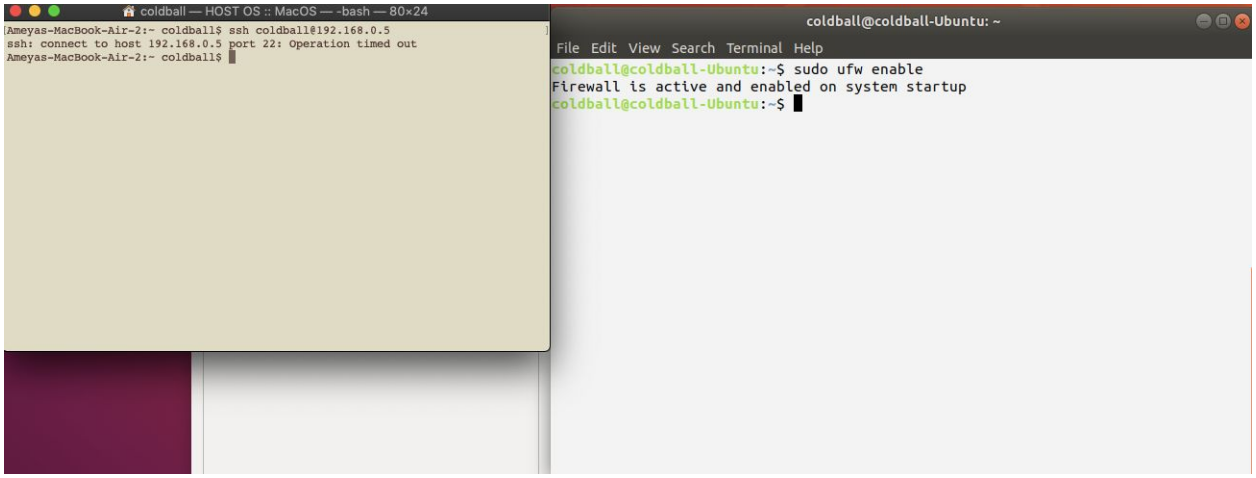


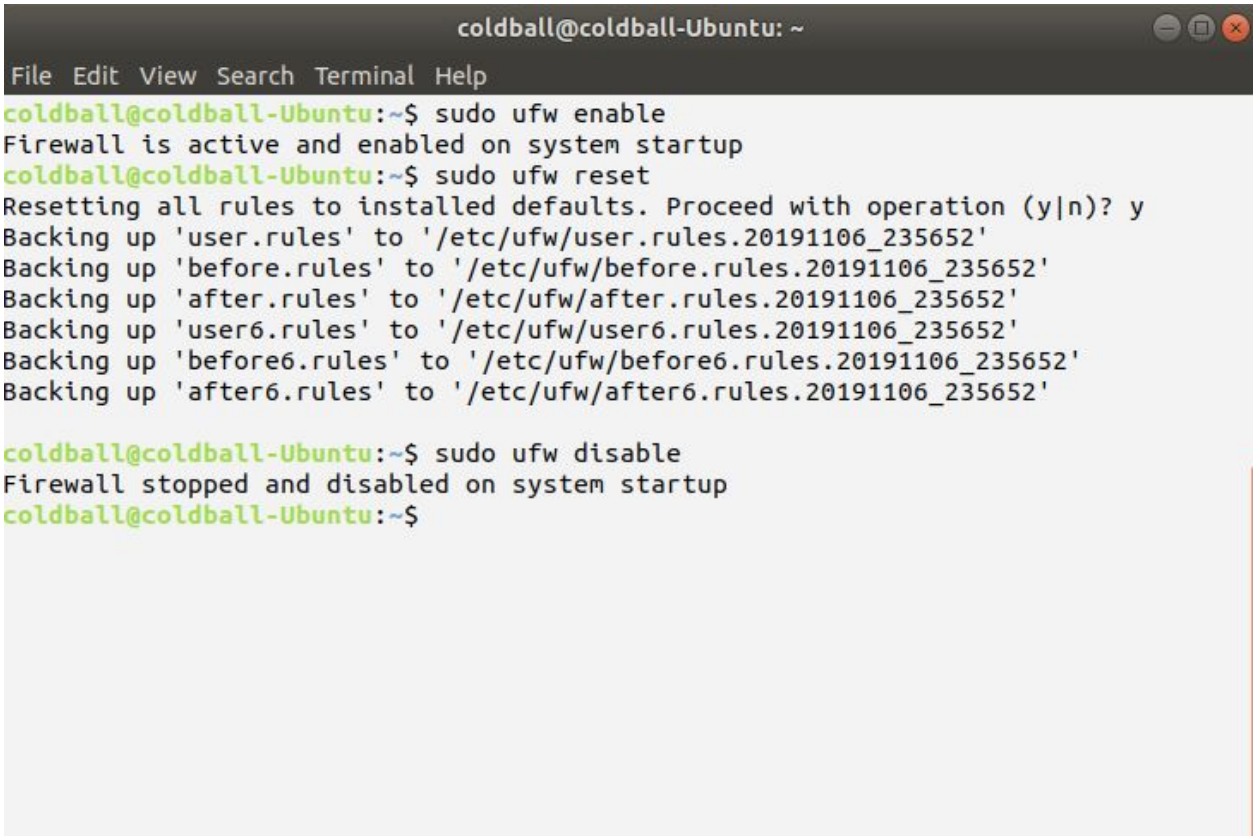

```
coldball@coldball-Ubuntu: ~
File  Edit  View  Search  Terminal  Help
coldball@coldball-Ubuntu:~$ sudo ufw status
[sudo] password for coldball:
Status: active

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

coldball@coldball-Ubuntu:~$
```


coldball@coldball-Ubuntu: ~
File Edit View Search Terminal Help
coldball@coldball-Ubuntu:~$ sudo ufw status
[sudo] password for coldball:
Status: active
To Action From
-- ------ ----
22/tcp DENY Anywhere
22/tcp (v6) DENY Anywhere (v6)
coldball@coldball-Ubuntu:~$ sudo ufw enable
Firewall is active and enabled on system startup
coldball@coldball-Ubuntu:~$


coldball — HOST OS :: MacOS — -bash — 80×24
Ameyas-MacBook-Air-2:~ coldball$ ssh coldball@192.168.0.5
ssh: connect to host 192.168.0.5 port 22: Operation timed out
Ameyas-MacBook-Air-2:~ coldball$
coldball@coldball-Ubuntu: ~
File Edit View Search Terminal Help
coldball@coldball-Ubuntu:~$ sudo ufw enable
Firewall is active and enabled on system startup
coldball@coldball-Ubuntu:~$



CONCLUSION:

Hence, a firewall is implemented in GUFW