TASK 2

Understanding Firewalls

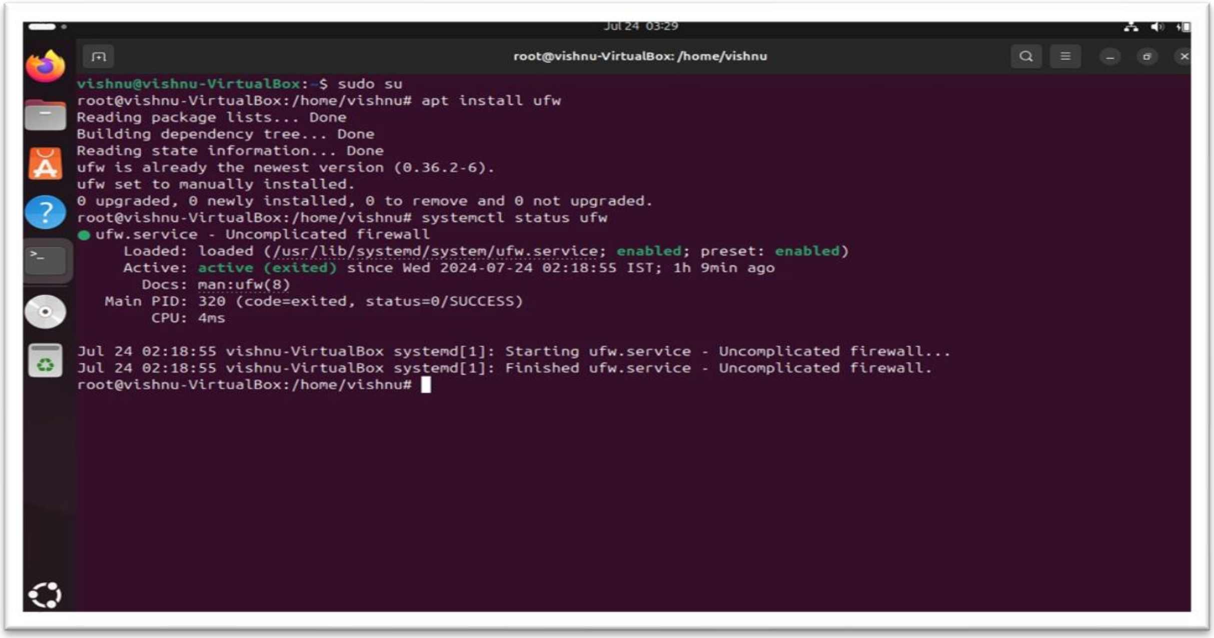
Firewalls are security systems designed to protect your network by controlling incoming and outgoing traffic based on predetermined security rules. They act as a barrier between a trusted internal network and untrusted external networks, such as the internet. There are several types of firewalls, including:

1. **Packet-Filtering Firewalls**: These inspect packets and allow or block them based on source and destination IP addresses, ports, or protocols.
2. **Stateful Inspection Firewalls**: These track the state of active connections and make decisions based on the context of the traffic.
3. **Proxy Firewalls**: These act as intermediaries between end-users and the services they access, providing additional security by masking the internal network.
4. **Next-Generation Firewalls**: These include advanced features like application awareness, intrusion prevention, and cloud-delivered threat intelligence.

Setting Up a Basic Firewall on Ubuntu 20.04

To set up a basic firewall on your Ubuntu 20.04 virtual machine, you can use UFW, which is a user-friendly interface for managing iptables firewall rules.

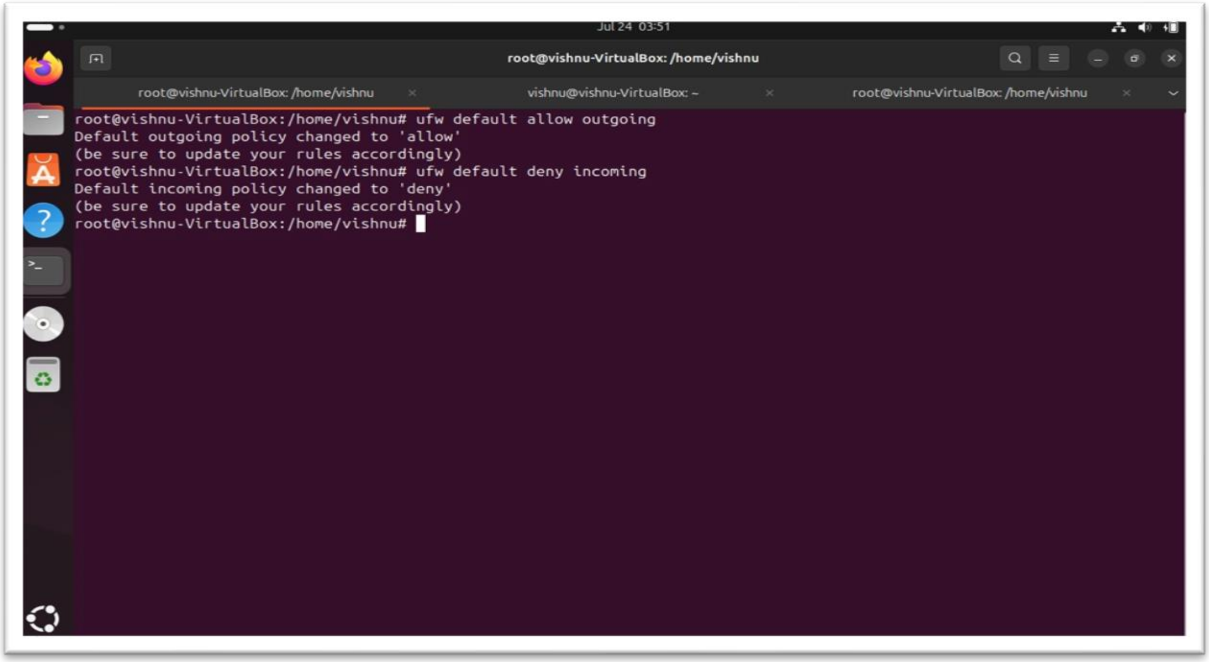
Step-by-Step Guide



```
vishnu@vishnu-VirtualBox:~$ sudo su
root@vishnu-VirtualBox:/home/vishnu# apt install ufw
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ufw is already the newest version (0.36.2-6).
ufw set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@vishnu-VirtualBox:/home/vishnu# systemctl status ufw
● ufw.service - Uncomplicated firewall
     Loaded: loaded (/usr/lib/systemd/system/ufw.service; enabled; preset: enabled)
     Active: active (exited) since Wed 2024-07-24 02:18:55 IST; 1h 9min ago
       Docs: man:ufw(8)
   Main PID: 320 (code=exited, status=0/SUCCESS)
        CPU: 4ms

Jul 24 02:18:55 vishnu-VirtualBox systemd[1]: Starting ufw.service - Uncomplicated firewall...
Jul 24 02:18:55 vishnu-VirtualBox systemd[1]: Finished ufw.service - Uncomplicated firewall.
root@vishnu-VirtualBox:/home/vishnu# 
```

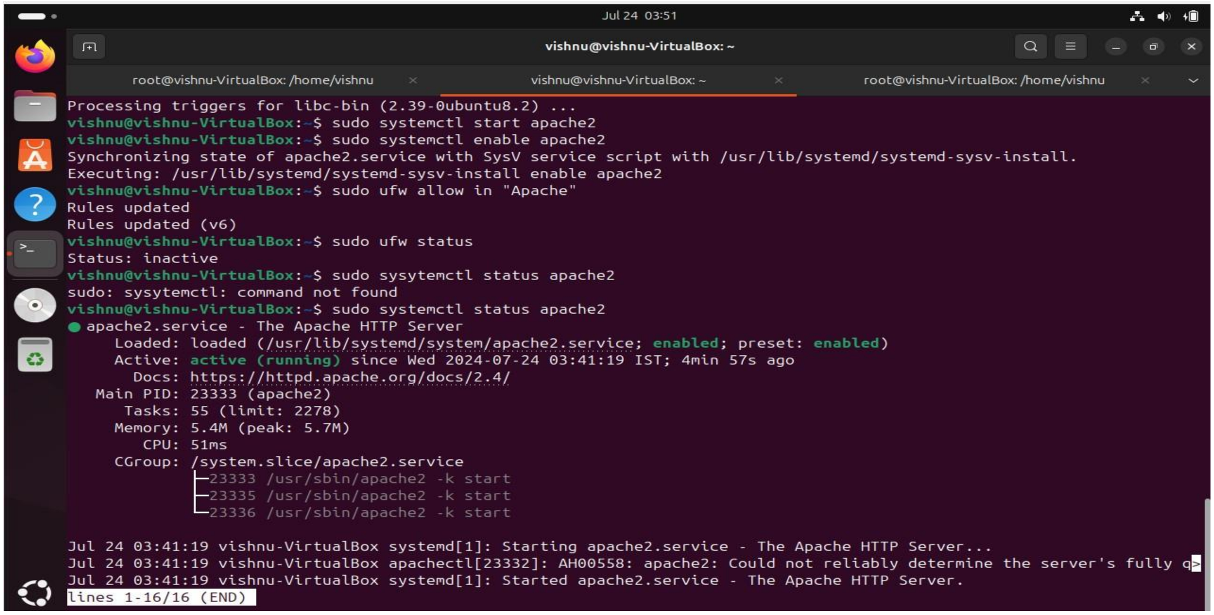
- sudo su : This command allows you to switch to the root user.
- apt install ufw : This command installs UFW on your Ubuntu system. UFW is not enabled by default, so you need to install it first.
- systemctl status ufw : This command checks the current status of UFW to see if it is active or inactive.


Jul 24 03:51
root@vishnu-VirtualBox: /home/vishnu
root@vishnu-VirtualBox: /home/vishnu
vishnu@vishnu-VirtualBox: ~
root@vishnu-VirtualBox: /home/vishnu

```
root@vishnu-VirtualBox:/home/vishnu# ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
root@vishnu-VirtualBox:/home/vishnu# ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
root@vishnu-VirtualBox:/home/vishnu# 
```

- ufw default allow outgoing : This command sets the default policy to allow all outgoing traffic from your system. This means any application on your server can connect to external servers without restrictions.

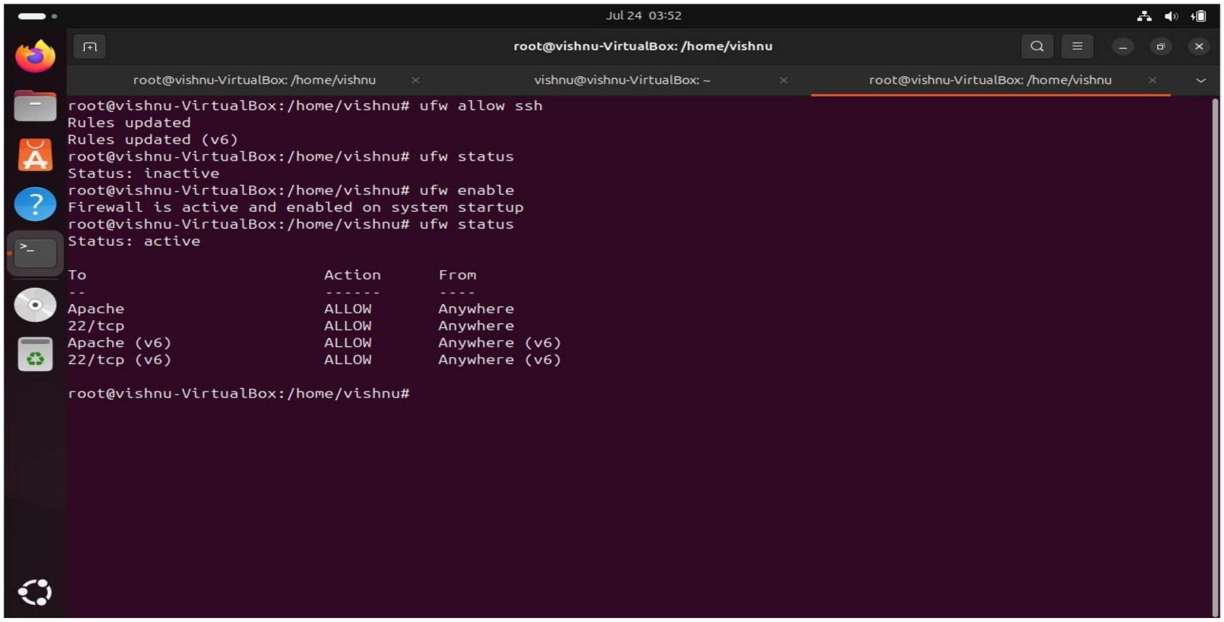
- ufw default deny incoming : This command sets the default policy to deny all incoming traffic to your system. This ensures that no external connections can be made to your server unless explicitly allowed


Jul 24 03:51
vishnu@vishnu-VirtualBox: ~
root@vishnu-VirtualBox: /home/vishnu
vishnu@vishnu-VirtualBox: ~
root@vishnu-VirtualBox: /home/vishnu

```
Processing triggers for libc-bin (2.39-0ubuntu8.2) ...
vishnu@vishnu-VirtualBox:~$ sudo systemctl start apache2
vishnu@vishnu-VirtualBox:~$ sudo systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
vishnu@vishnu-VirtualBox:~$ sudo ufw allow in "Apache"
Rules updated
Rules updated (v6)
vishnu@vishnu-VirtualBox:~$ sudo ufw status
Status: inactive
vishnu@vishnu-VirtualBox:~$ sudo sysytemctl status apache2
sudo: sysytemctl: command not found
vishnu@vishnu-VirtualBox:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Wed 2024-07-24 03:41:19 IST; 4min 57s ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 23333 (apache2)
      Tasks: 55 (limit: 2278)
     Memory: 5.4M (peak: 5.7M)
        CPU: 51ms
     CGroup: /system.slice/apache2.service
             ├─23333 /usr/sbin/apache2 -k start
             ├─23335 /usr/sbin/apache2 -k start
             └─23336 /usr/sbin/apache2 -k start

Jul 24 03:41:19 vishnu-VirtualBox systemd[1]: Starting apache2.service - The Apache HTTP Server...
Jul 24 03:41:19 vishnu-VirtualBox apachectl[23332]: AH00558: apache2: Could not reliably determine the server's fully q>
Jul 24 03:41:19 vishnu-VirtualBox systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-16/16 (END)
```

- sudo systemctl start apache2 : This command starts the Apache web server service on your system.
- sudo systemctl enable apache2 : This command enables the Apache service to start automatically at boot time.
- sudo ufw allow in “Apache” : This command allows incoming traffic for the Apache web server through the firewall. ufw uses predefined profiles for common applications like Apache.
- sudo ufw status : This command displays the current status of UFW, including active rules and policies.
- sudo systemctl status apache2 : This command shows the current status of the Apache service, including whether it is active and running.

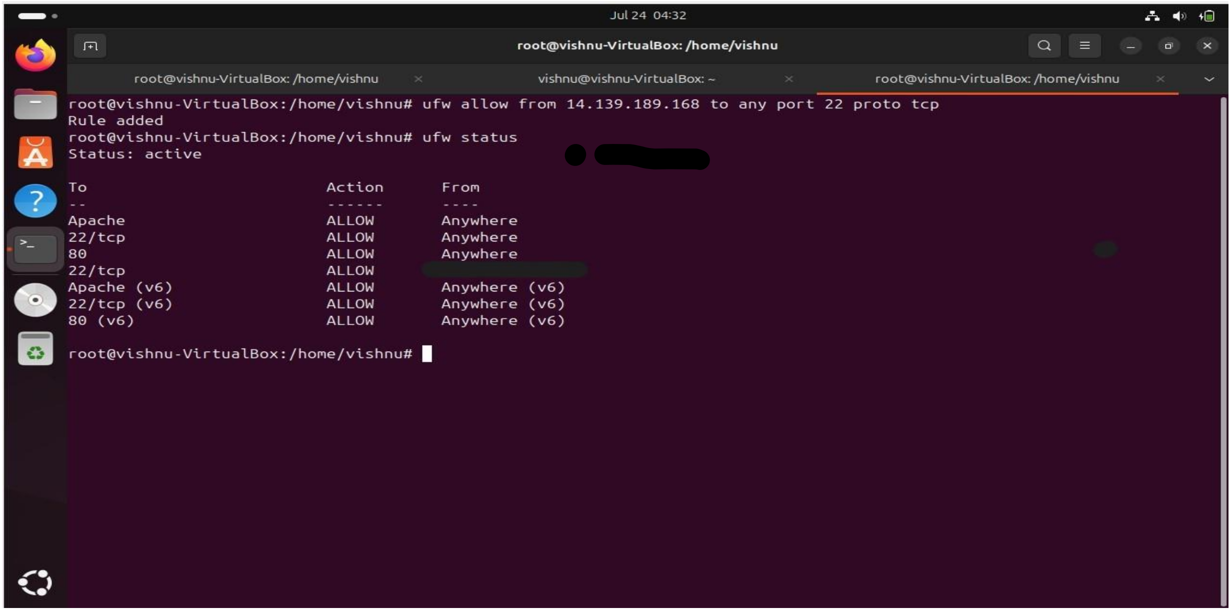

Jul 24 03:52
root@vishnu-VirtualBox: /home/vishnu
root@vishnu-VirtualBox: /home/vishnu
vishnu@vishnu-VirtualBox: ~
root@vishnu-VirtualBox: /home/vishnu

```
root@vishnu-VirtualBox:/home/vishnu# ufw allow ssh
Rules updated
Rules updated (v6)
root@vishnu-VirtualBox:/home/vishnu# ufw status
Status: inactive
root@vishnu-VirtualBox:/home/vishnu# ufw enable
Firewall is active and enabled on system startup
root@vishnu-VirtualBox:/home/vishnu# ufw status
Status: active

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

root@vishnu-VirtualBox:/home/vishnu#
```

- ufw allow ssh : This command allows incoming SSH traffic on port 22, which is essential for remote management of your server.
- ufw enable : This command enables ufw, starting the firewall with the configured rules.
- ufw status : This command displays the current status of ufw, including active rules and policies.

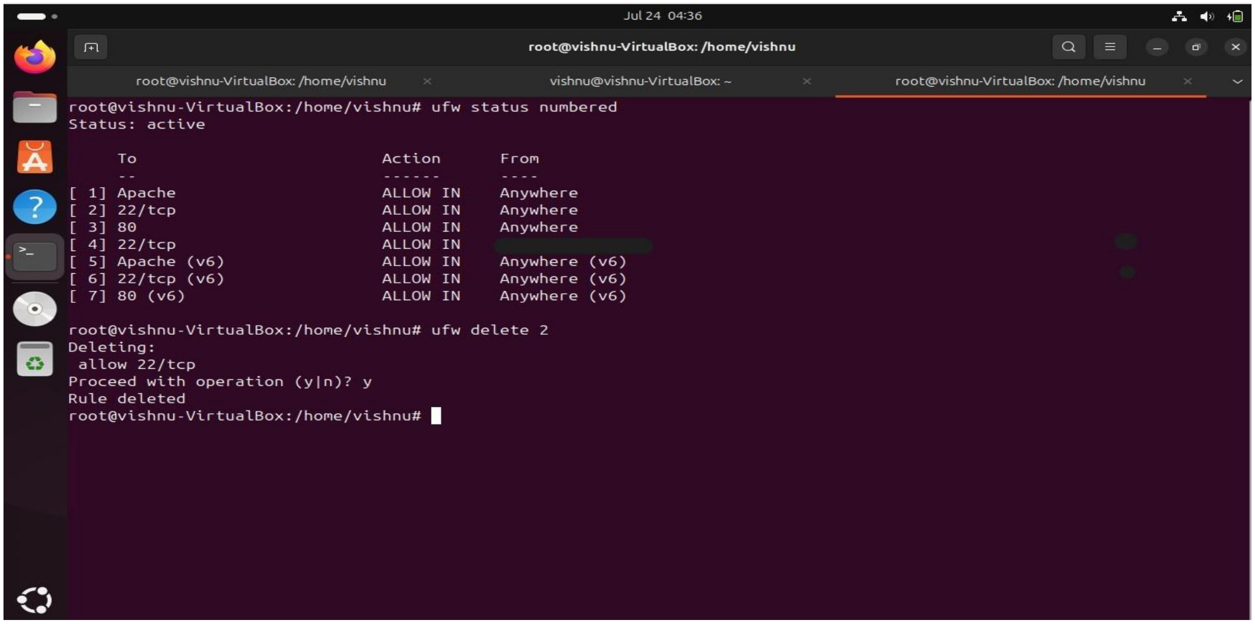

Jul 24 04:32
root@vishnu-VirtualBox: /home/vishnu
root@vishnu-VirtualBox: /home/vishnu
vishnu@vishnu-VirtualBox: ~
root@vishnu-VirtualBox: /home/vishnu

```
root@vishnu-VirtualBox:/home/vishnu# ufw allow from 14.139.189.168 to any port 22 proto tcp
Rule added
root@vishnu-VirtualBox:/home/vishnu# ufw status
Status: active                                         [redacted]

To                         Action      From
--                         ------      ----
Apache                     ALLOW       Anywhere
22/tcp                     ALLOW       Anywhere
80                         ALLOW       Anywhere
22/tcp                     ALLOW       [redacted]
Apache (v6)                ALLOW       Anywhere (v6)
22/tcp (v6)                ALLOW       Anywhere (v6)
80 (v6)                    ALLOW       Anywhere (v6)

root@vishnu-VirtualBox:/home/vishnu#
```

- ufw allow from <your public ip> to any port 22 proto tcp : This command allows SSH traffic only from a specific IP address to port 22, adding an extra layer of security by restricting access to trusted sources

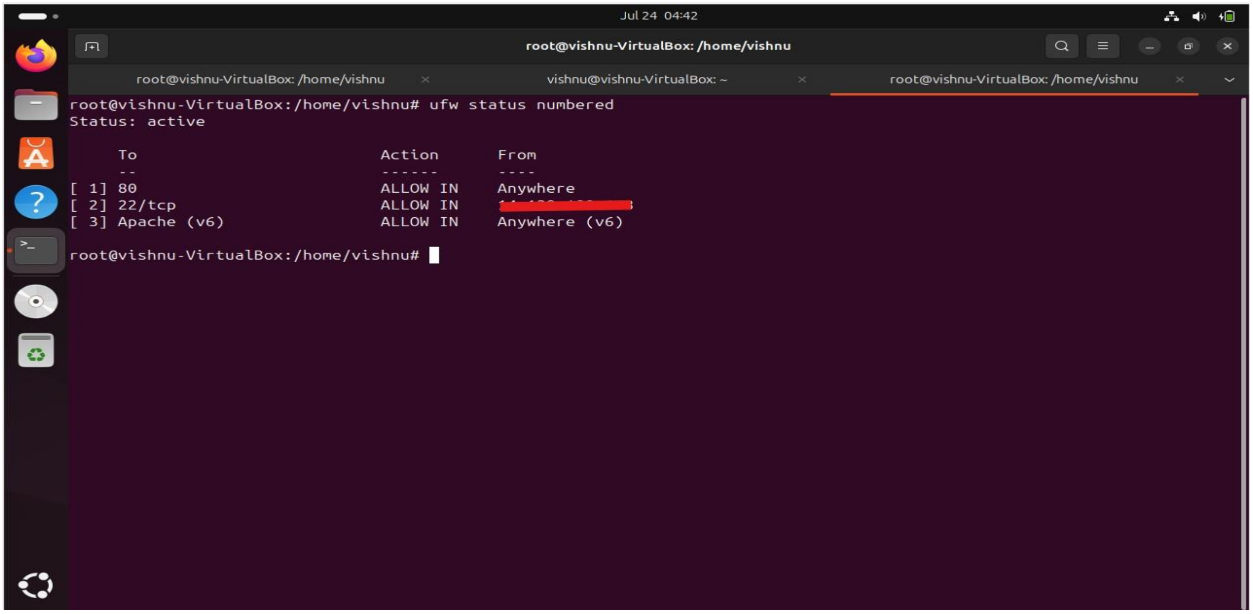

Jul 24 04:36
root@vishnu-VirtualBox: /home/vishnu
root@vishnu-VirtualBox: /home/vishnu
vishnu@vishnu-VirtualBox: ~
root@vishnu-VirtualBox: /home/vishnu

```
root@vishnu-VirtualBox:/home/vishnu# ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] Apache                     ALLOW IN    Anywhere
[ 2] 22/tcp                     ALLOW IN    Anywhere
[ 3] 80                         ALLOW IN    Anywhere
[ 4] 22/tcp                     ALLOW IN    [redacted]
[ 5] Apache (v6)                ALLOW IN    Anywhere (v6)
[ 6] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
[ 7] 80 (v6)                    ALLOW IN    Anywhere (v6)

root@vishnu-VirtualBox:/home/vishnu# ufw delete 2
Deleting:
 allow 22/tcp
Proceed with operation (y|n)? y
Rule deleted
root@vishnu-VirtualBox:/home/vishnu#
```

- ufw status numbered : This command lists all the current firewall rules with numbers, making it easier to manage and delete specific rules if needed
- ufw delete 2 : This command deletes the rule numbered 2 from the firewall configuration.


Jul 24 04:42
root@vishnu-VirtualBox: /home/vishnu
root@vishnu-VirtualBox: /home/vishnu
vishnu@vishnu-VirtualBox: ~
root@vishnu-VirtualBox: /home/vishnu

```
root@vishnu-VirtualBox:/home/vishnu# ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 80                         ALLOW IN    Anywhere
[ 2] 22/tcp                     ALLOW IN    [redacted]
[ 3] Apache (v6)                ALLOW IN    Anywhere (v6)

root@vishnu-VirtualBox:/home/vishnu#
```

- ufw status numbered : This command lists all the current firewall rules with numbers, providing a final overview of the active rules.

Conclusion

In conclusion, I have successfully set up and configured a basic firewall on your Ubuntu 20.04 virtual machine using ufw. Throughout this process, I have learned to set default policies for outgoing and incoming traffic, start and enable the Apache web server, allow specific traffic for SSH and Apache, restrict SSH access to a specific IP address, and manage and delete firewall rules. These steps ensure enhanced security and controlled access to your system.