

Visvesvaraya Technological University
Belagavi, Karnataka-590 018



A MINI PROJECT REPORT
On

‘Configuring and Managing the network traffic using firewall rules to meet the system and user requirements for the incoming and outgoing traffic’

Submitted
In partial fulfilment requirements for the award of the Degree

of
BACHELOR OF ENGINEERING
IN
INFORMATION SCIENCE AND ENGINEERING

by

Pratheeksha K N (4NM21IS111)
Prathvi Hegde(4NM21IS113)

Under the Guidance of

Mr .Santhosh

Assistant Professor Gd-III

Department of Information Science and Engineering



NMAM INSTITUTE
OF TECHNOLOGY

TABLE OF CONTENTS	Page No.
Abstract	3
Introduction	4
Procedure	5
Results	7
Conclusion	9

ABSTRACT

In modern computing environments, managing network traffic is essential to ensure system security and meet user requirements. This project focuses on configuring and managing network traffic using firewall rules to address the needs of both the system and users. By implementing firewall rules, we aim to regulate incoming and outgoing traffic effectively, enhancing system security and ensuring that user requirements for network access are met. This involves creating and enforcing rules that dictate which types of traffic are allowed or denied based on predefined criteria such as source and destination IP addresses, ports, protocols, and application signatures.

INTRODUCTION

In today's interconnected world, network security is paramount. Effective management of incoming and outgoing network traffic is crucial to safeguarding systems against malicious threats and unauthorized access while ensuring that legitimate user needs are fulfilled. This project delves into the configuration and management of network traffic using firewall rules. By implementing firewall policies, we aim to strike a balance between system security and user accessibility, thereby creating a network environment that is both secure and user-friendly. This involves the design and implementation of firewall rules tailored to the specific requirements of the system and its users, including considerations such as the nature of the network infrastructure, the types of services running on the system, and the level of access needed by different users or applications.

PROCEDURE

To implement firewall management in Ubuntu running on Oracle VM the following steps are followed:

1. Launch the Terminal application in Ubuntu. This is done by either searching for 'Terminal' in the applications menu or by using the keyboard shortcut `Ctrl + Alt + T`.

2. The following command is run to update the package lists to ensure that the latest information about available packages and their versions is received.

sudo apt update

3. The following command is run to install the Uncomplicated Firewall (UFW), which is a user-friendly interface for managing iptables firewall rules.

sudo apt install ufw

4. Once UFW is installed, it is enabled using the command:

sudo ufw enable

5. The command below is run to verify that UFW is enabled and active by running

sudo ufw status

6. Allow incoming SSH connections (assuming SSH is running on port 22) to ensure remote access to the system

sudo ufw allow 22/tcp

7. Allow outgoing HTTP traffic, which is commonly used for web browsing

sudo ufw allow out 80/tcp

8. To deny incoming traffic from a specific IP address:

sudo ufw deny from <IP_Address>

9. To deny outgoing traffic to a specific IP address:

sudo ufw deny out to <IP_Address>

10. The following command is used to delete a specific rule

sudo ufw delete <rule_number>

11. To reset UFW to its default settings:

sudo ufw reset

RESULTS

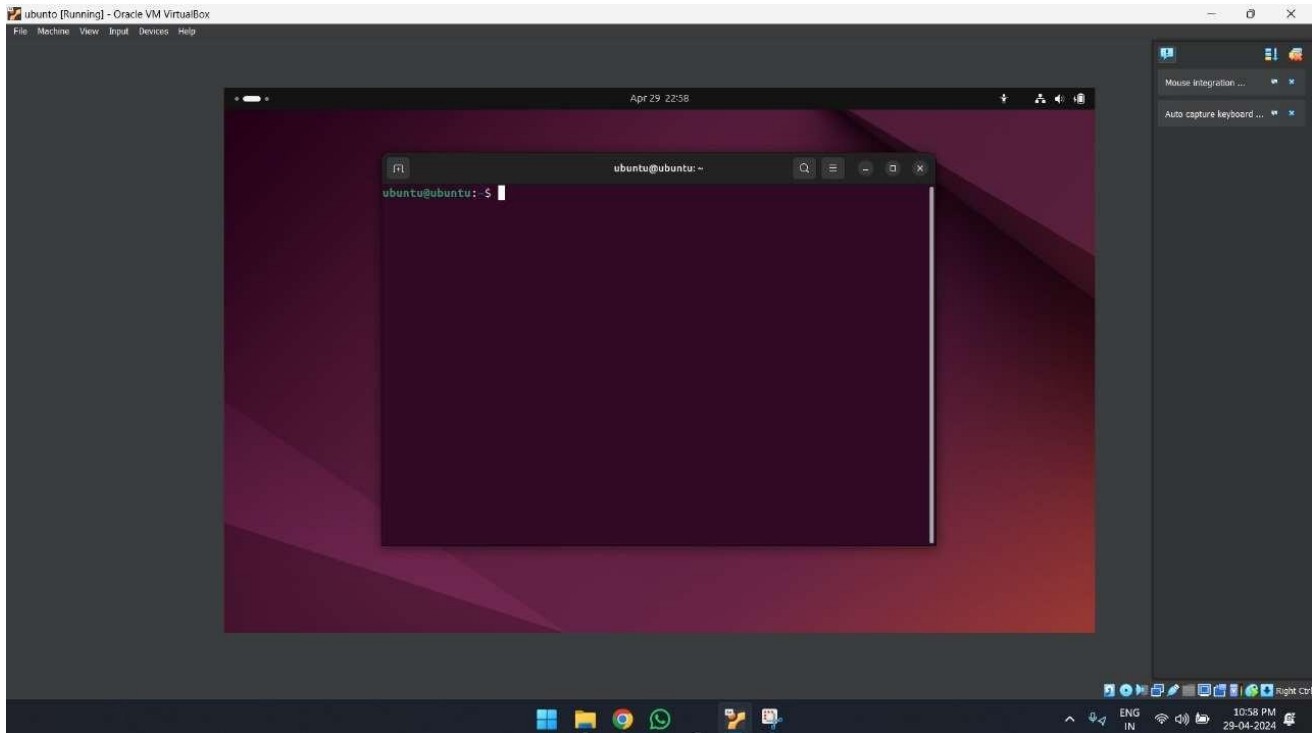


Fig 1. Running Ubuntu on Oracle VM

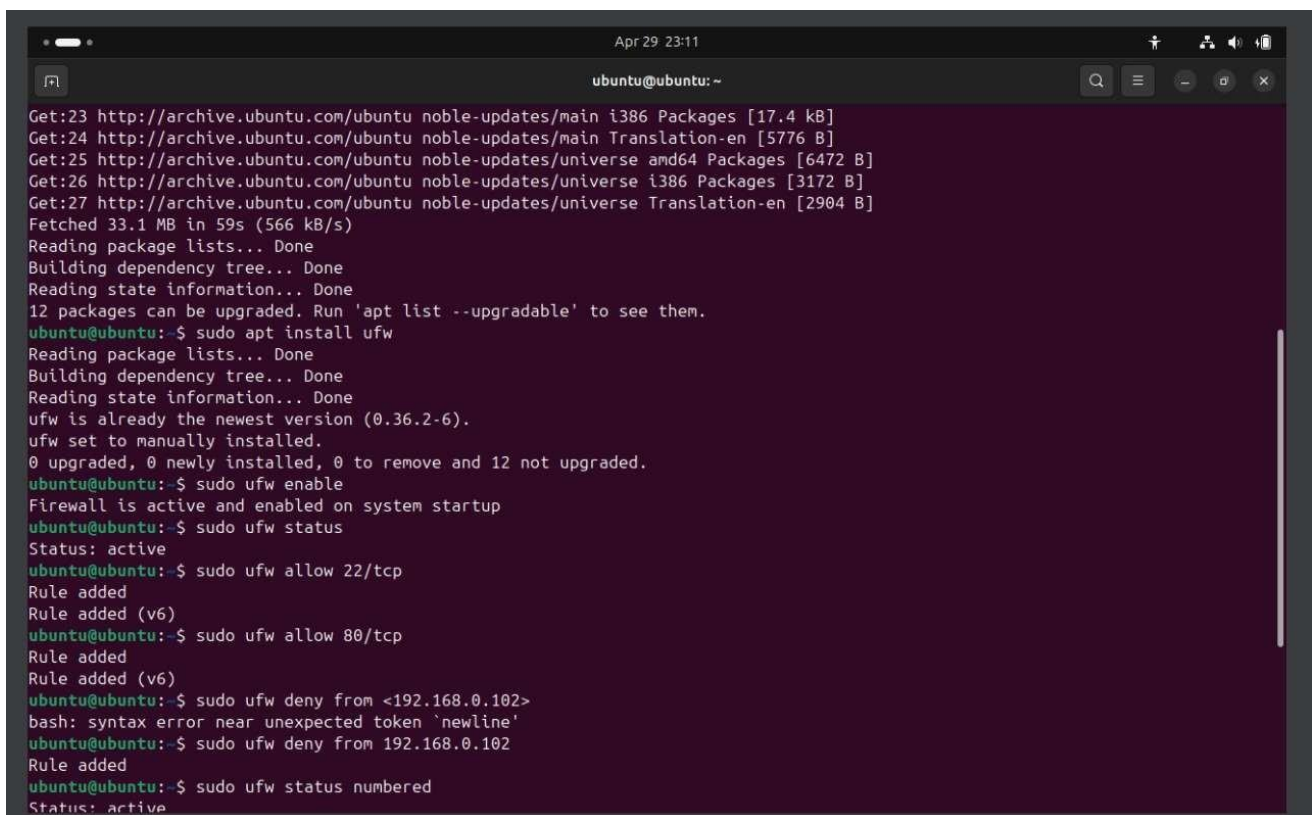
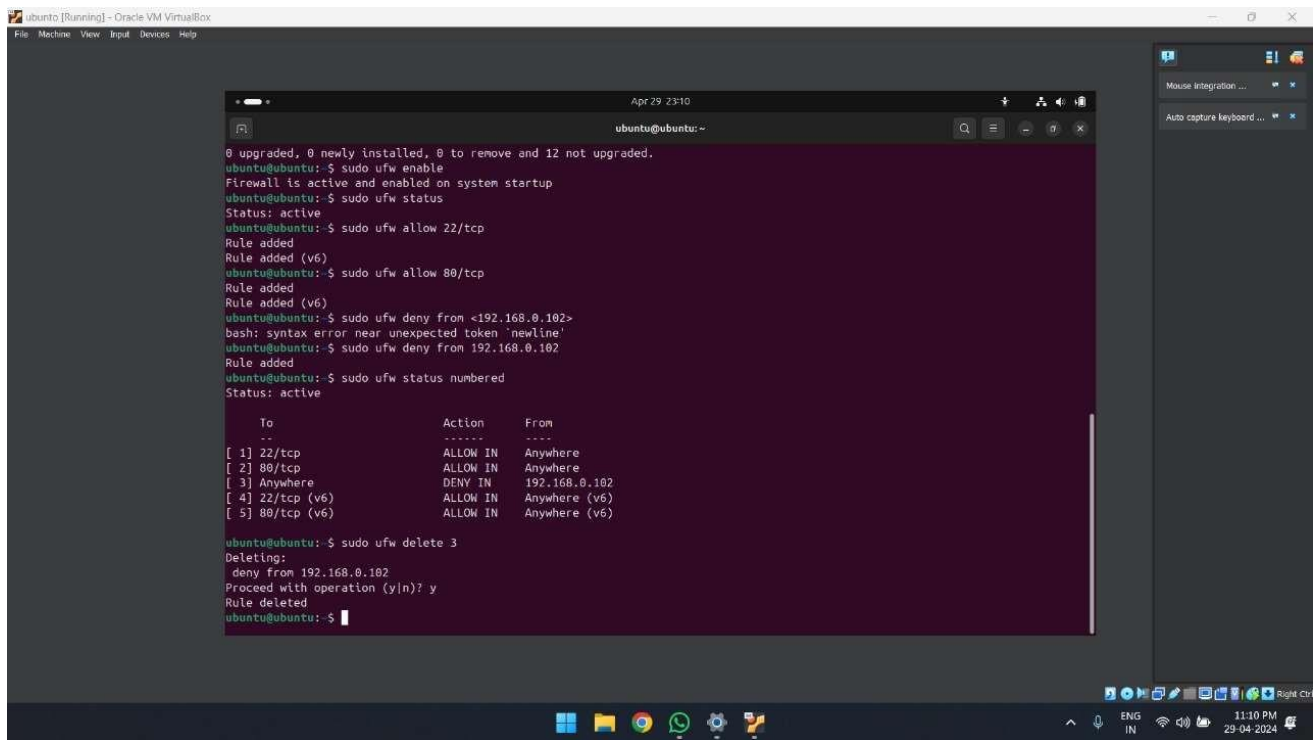


Fig 2. Installing and enabling UFW

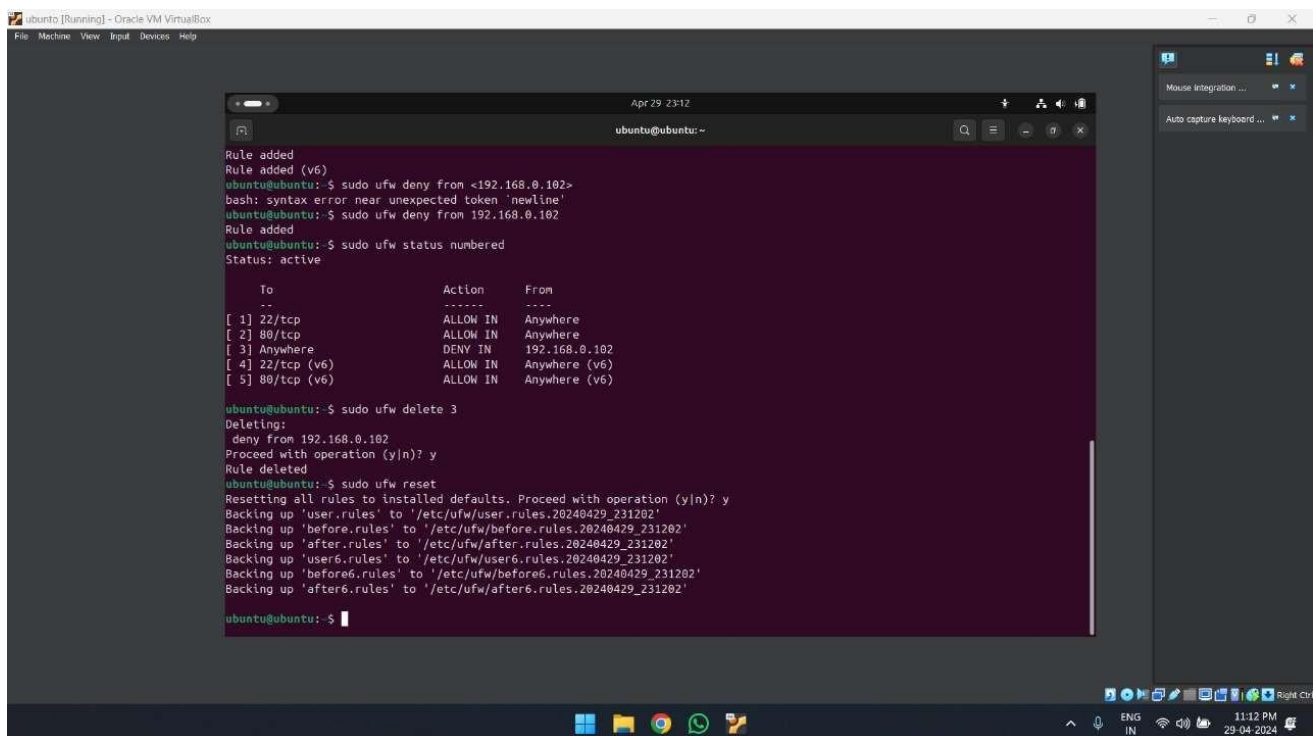


```
0 upgraded, 0 newly installed, 0 to remove and 12 not upgraded.
ubuntu@ubuntu:~$ sudo ufw enable
Firewall is active and enabled on system startup
ubuntu@ubuntu:~$ sudo ufw status
Status: active
ubuntu@ubuntu:~$ sudo ufw allow 22/tcp
Rule added
Rule added (v6)
ubuntu@ubuntu:~$ sudo ufw allow 80/tcp
Rule added
Rule added (v6)
ubuntu@ubuntu:~$ sudo ufw deny from <192.168.0.102>
bash: syntax error near unexpected token 'newline'
ubuntu@ubuntu:~$ sudo ufw deny from 192.168.0.102
Rule added
ubuntu@ubuntu:~$ sudo ufw status numbered
Status: active

    To      Action     From
    --      -
[ 1] 22/tcp    ALLOW IN   Anywhere
[ 2] 80/tcp    ALLOW IN   Anywhere
[ 3] Anywhere  DENY IN    192.168.0.102
[ 4] 22/tcp (v6) ALLOW IN   Anywhere (v6)
[ 5] 80/tcp (v6) ALLOW IN   Anywhere (v6)

ubuntu@ubuntu:~$ sudo ufw delete 3
Deleting:
deny from 192.168.0.102
Proceed with operation (y/n)? y
Rule deleted
ubuntu@ubuntu:~$
```

Fig 3. Adding a rule of denying incoming traffic



```
Rule added
Rule added (v6)
ubuntu@ubuntu:~$ sudo ufw deny from <192.168.0.102>
bash: syntax error near unexpected token 'newline'
ubuntu@ubuntu:~$ sudo ufw deny from 192.168.0.102
Rule added
ubuntu@ubuntu:~$ sudo ufw status numbered
Status: active

    To      Action     From
    --      -
[ 1] 22/tcp    ALLOW IN   Anywhere
[ 2] 80/tcp    ALLOW IN   Anywhere
[ 3] Anywhere  DENY IN    192.168.0.102
[ 4] 22/tcp (v6) ALLOW IN   Anywhere (v6)
[ 5] 80/tcp (v6) ALLOW IN   Anywhere (v6)

ubuntu@ubuntu:~$ sudo ufw delete 3
Deleting:
deny from 192.168.0.102
Proceed with operation (y/n)? y
Rule deleted
ubuntu@ubuntu:~$ sudo ufw reset
Resetting all rules to installed defaults. Proceed with operation (y/n)? y
Backing up 'user.rules' to '/etc/ufw/user.rules.20240429_231202'
Backing up 'before.rules' to '/etc/ufw/before.rules.20240429_231202'
Backing up 'after.rules' to '/etc/ufw/after.rules.20240429_231202'
Backing up 'user6.rules' to '/etc/ufw/user6.rules.20240429_231202'
Backing up 'before6.rules' to '/etc/ufw/before6.rules.20240429_231202'
Backing up 'after6.rules' to '/etc/ufw/after6.rules.20240429_231202'
ubuntu@ubuntu:~$
```

Fig 4. Resetting all the rules to installed defaults

Conclusion

In conclusion, the implementation of firewall rules using the Uncomplicated Firewall (UFW) in Ubuntu on Oracle VM has proven to be an effective method for managing network traffic. By configuring specific rules, we were able to control incoming and outgoing traffic, enhance system security, and meet user requirements for network access. Through the utilization of commands, we could tailor the firewall configuration to the needs of the system, allowing or blocking traffic based on predefined criteria. Furthermore, the ability to delete and reset rules provided flexibility in adapting the firewall setup as needed. Overall, this project demonstrates the importance of proactive network security measures and highlights the utility of firewall management tools in maintaining a secure and reliable computing environment.