Packet filter firewall project 1

Student Name: Mohammed Ahmed Ragab

Email: maragab@asu.edu

Submission Date: 24 October 2023

Class Name and Term: CSE548 Fall 2023

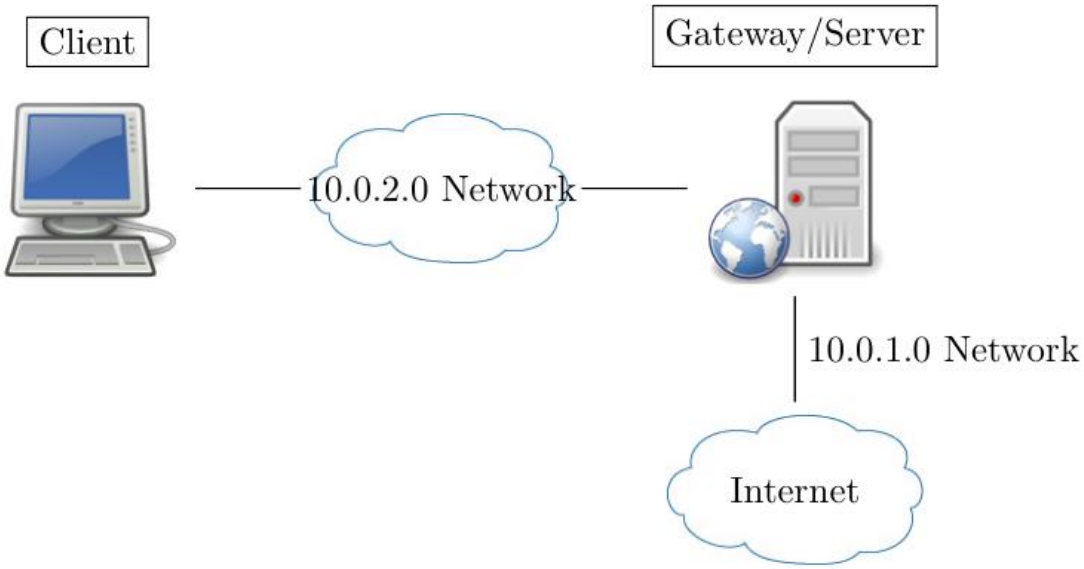
I. Project Overview

This project is about creating a stateless firewall that block/allow the packets on a server_gateway virtual machine which is connected to a client virtual machine on the same NAT network. The firewall can be achieve by using the linux command “iptables” that allow the user to write rules which specifies whether an IP packets is accepted or dropped based on criteria such as source IP and protocol (ICMP, TCP ,… etc).

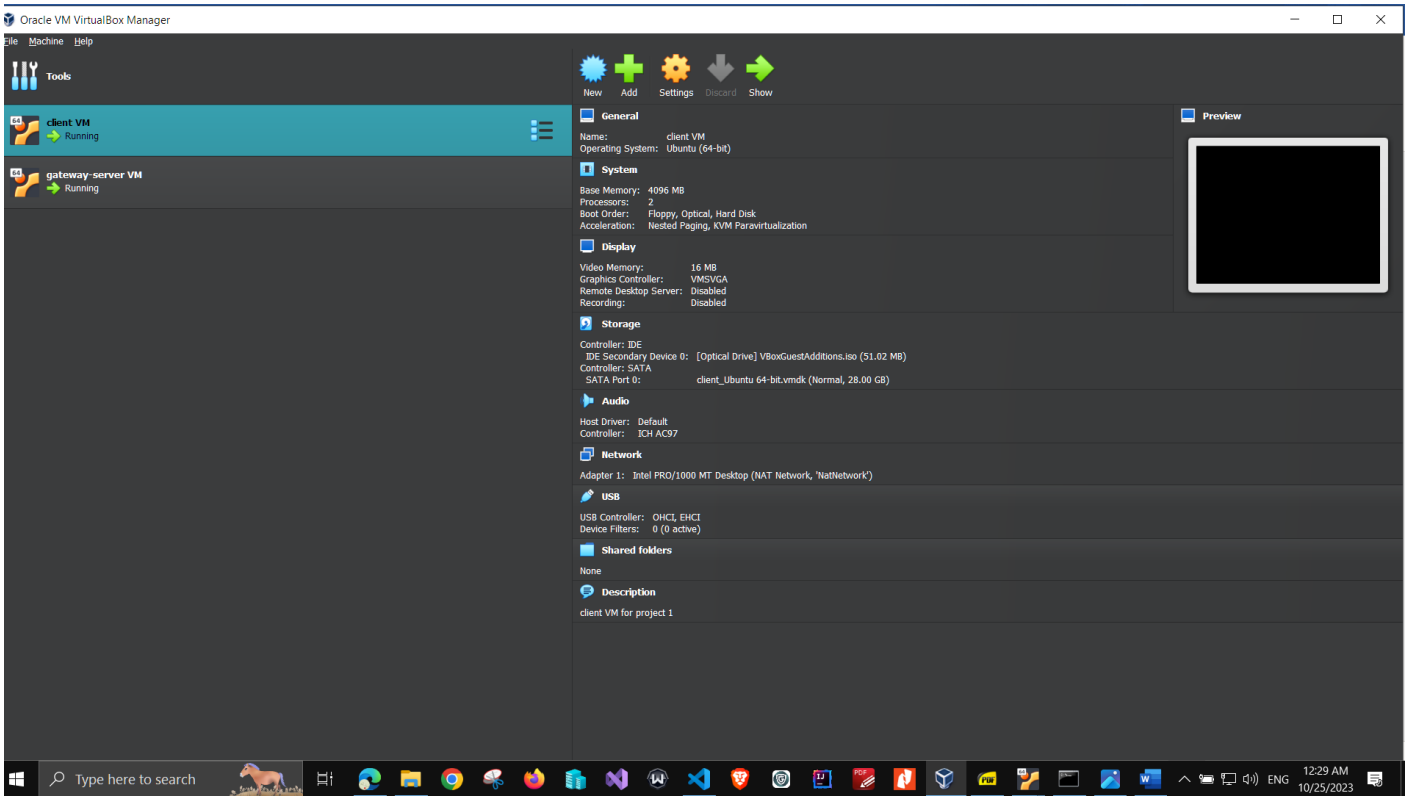
II. Network Setup

The network topology

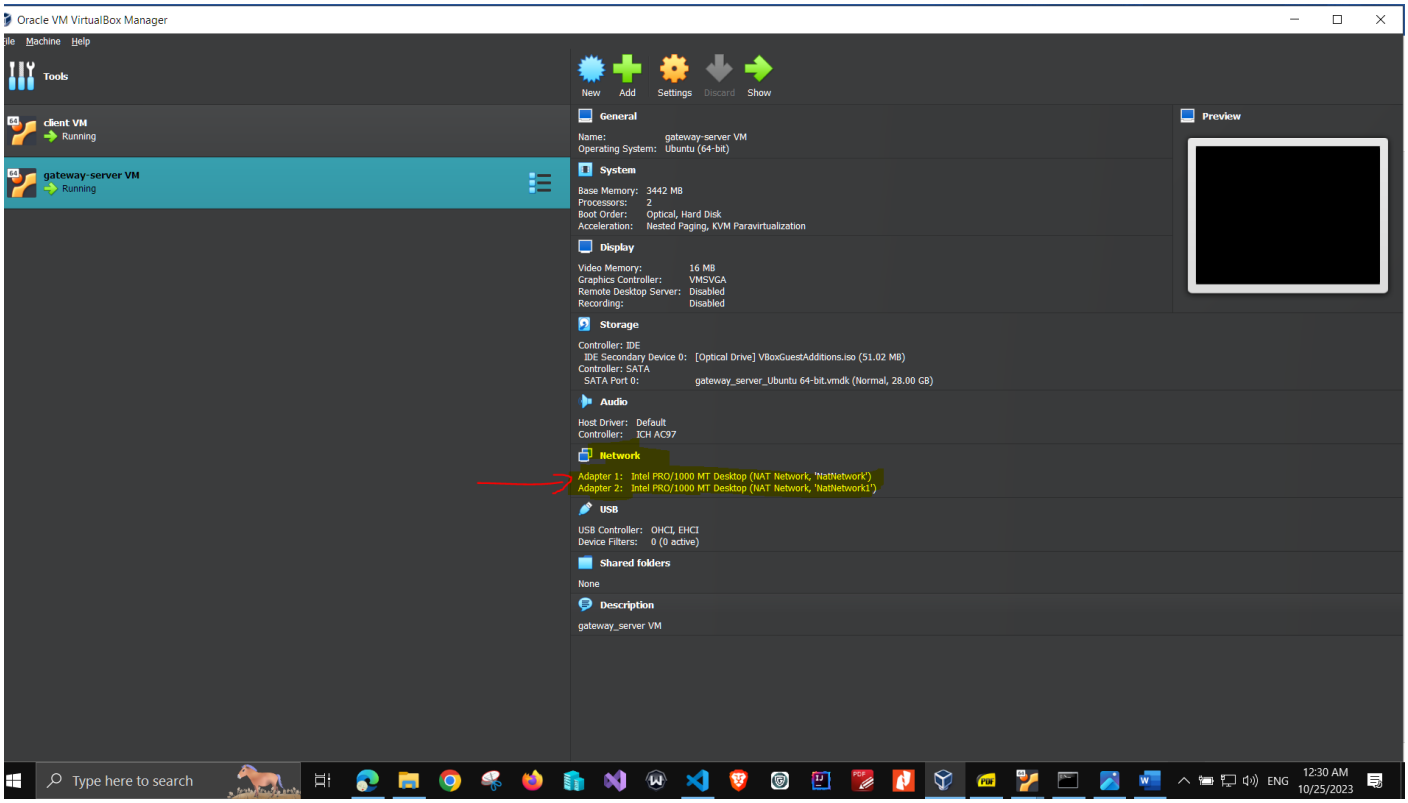
client IP = 10.0.2.6
client interface = enp0s3
gateway/server IP for NATnetwork = 10.0.2.7
gateway/server IP for NATnetwork1 = 10.0.1.4 , interface (to the internet) = enp0s8



The client VM in virtual box



The server/gateway VM in virtual box



III. SOFTWARE

I have used the following tools to test the connection from client VM to the gateway/server VM so that I make sure that the rules which have been written on the gateway/server VM are working fine.

- Firefox browser (to test connecting with the apache server and view the index.html welcome webpage
- virtualbox
- Ping

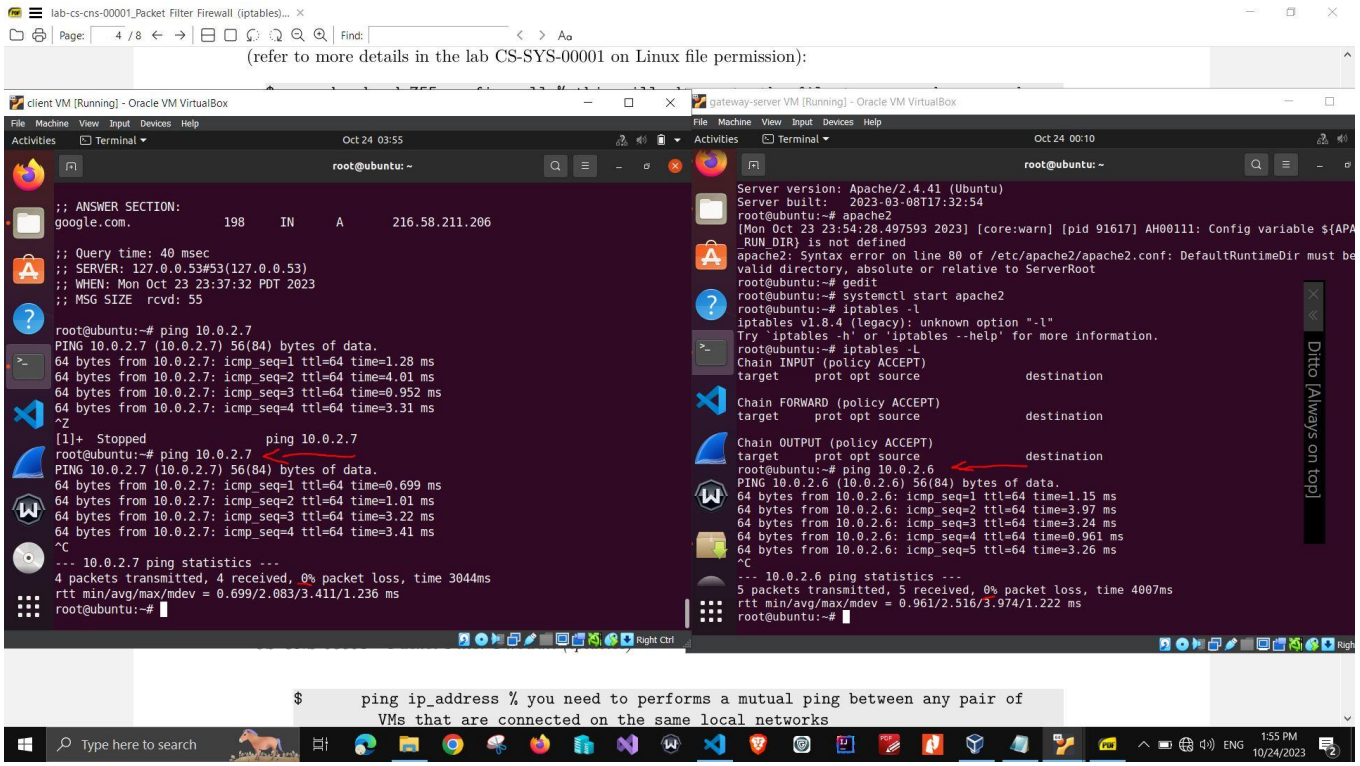
- Traceroute
- Ifconfig
- Gedit (for editing the files)
- Apache2 web server
- Iptables commands
- nmap

IV. PROJECT DESCRIPTION

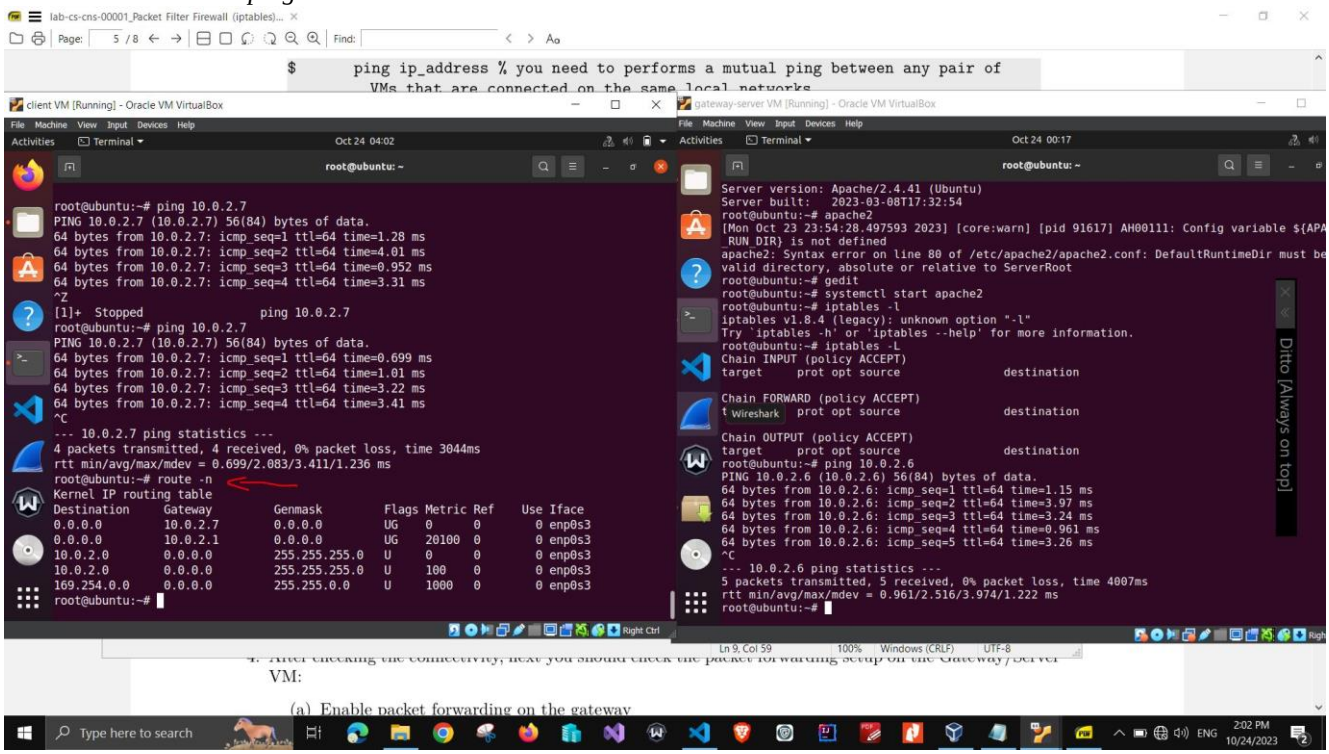
1. First, I have to prepare the test environment by following and apply all the steps in the provided PDF files and run the 2 virtual machines (VMs) at the same time. Then I assigned “natNetwork” to client VM , and “natNetwork”, “natNetwork1” to the gateway_server VM from the settings for VirtualBox software.
2. I followed the instructions in the PDF file “lab-cs-cns-00001” which describes the rules need to be written using iptables command.
3. The following is a step-by-step screenshots of the work I have done to complete the project with some linux commands I used to define the rules for filter and NAT tables:

task 1.1

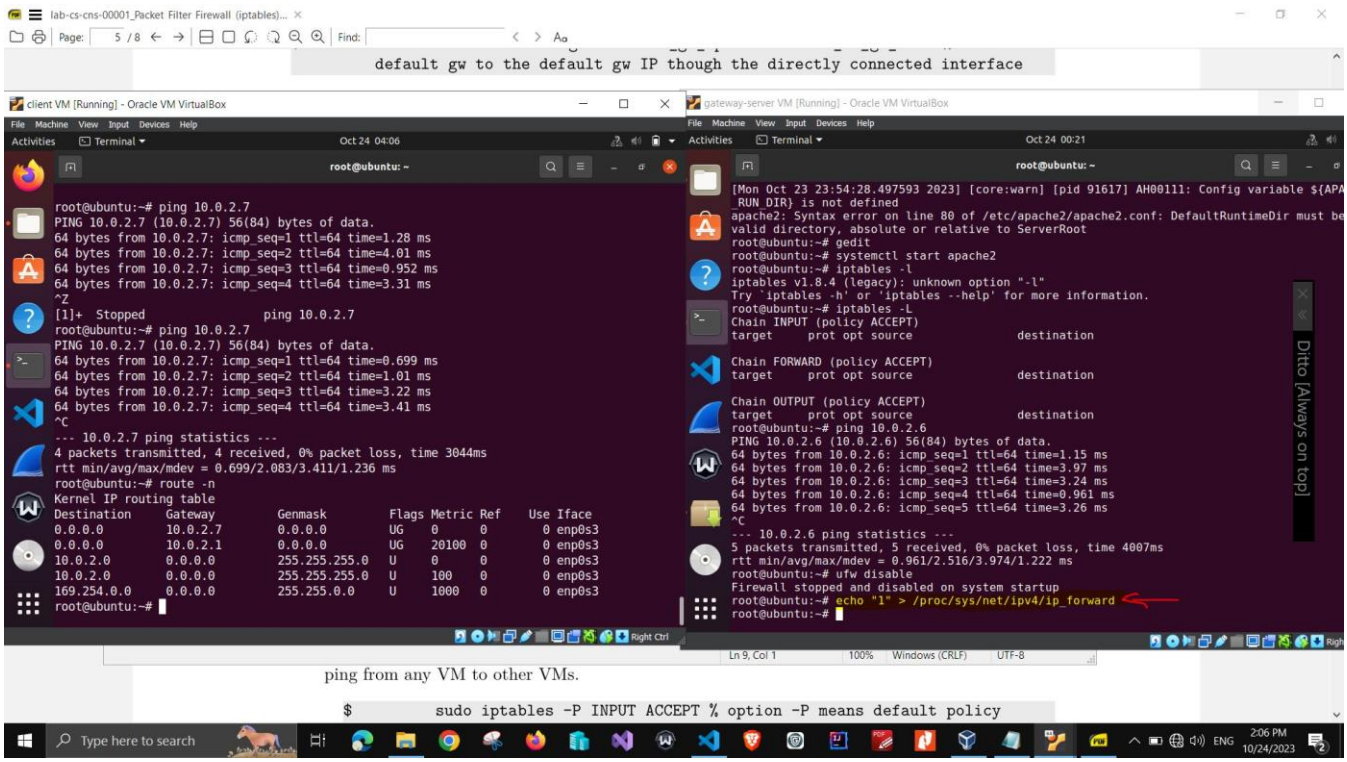
task 1.1 each VM can ping each other



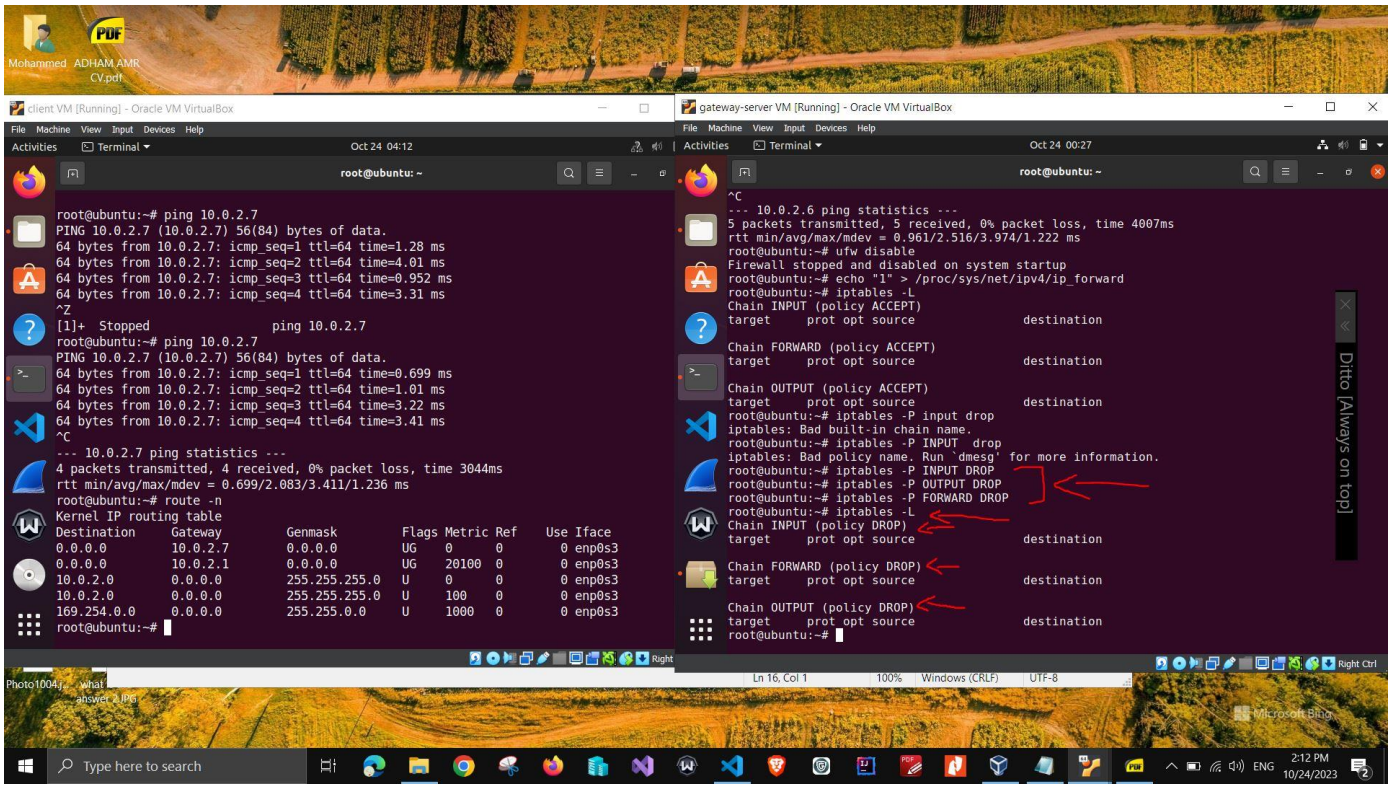
task 1.1 each VM can ping each other



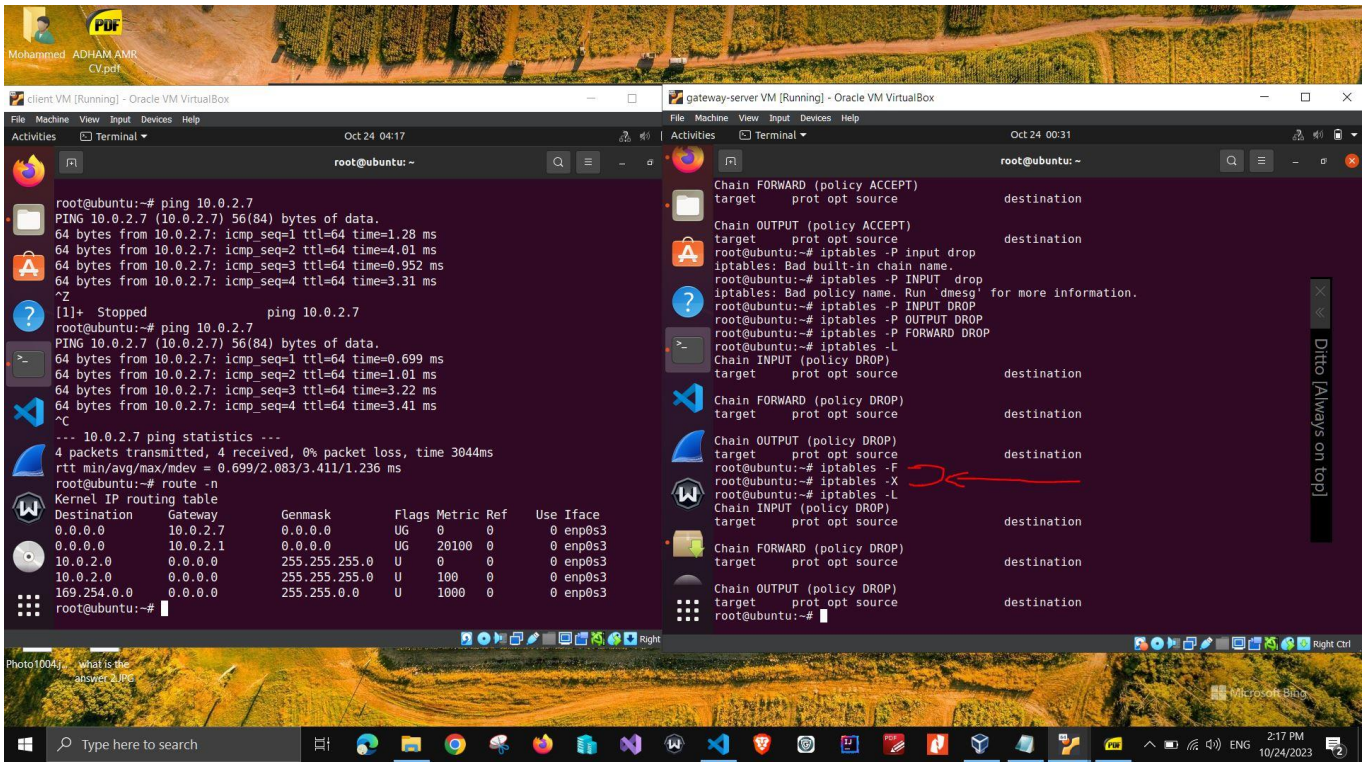
task 1.1 enable packet forwarding on gateway VM



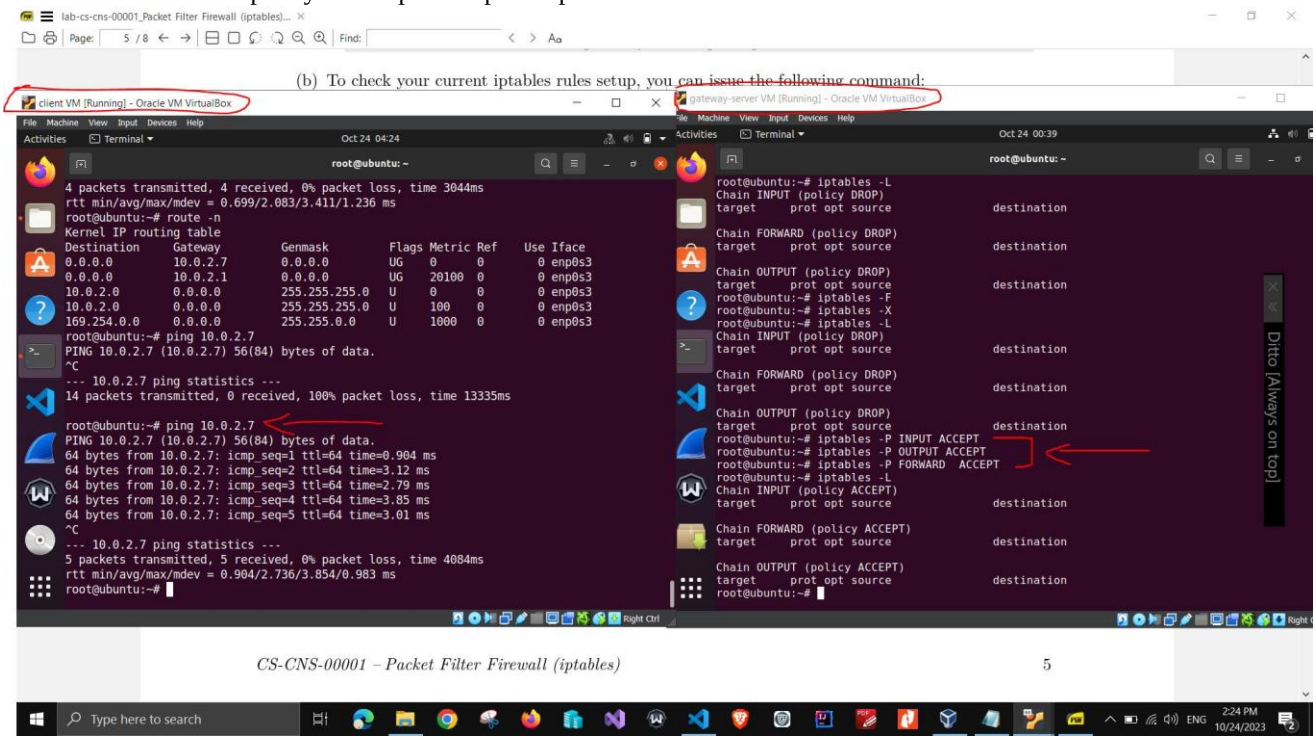
task 1.1.4.b drop policy for input output forward chaines



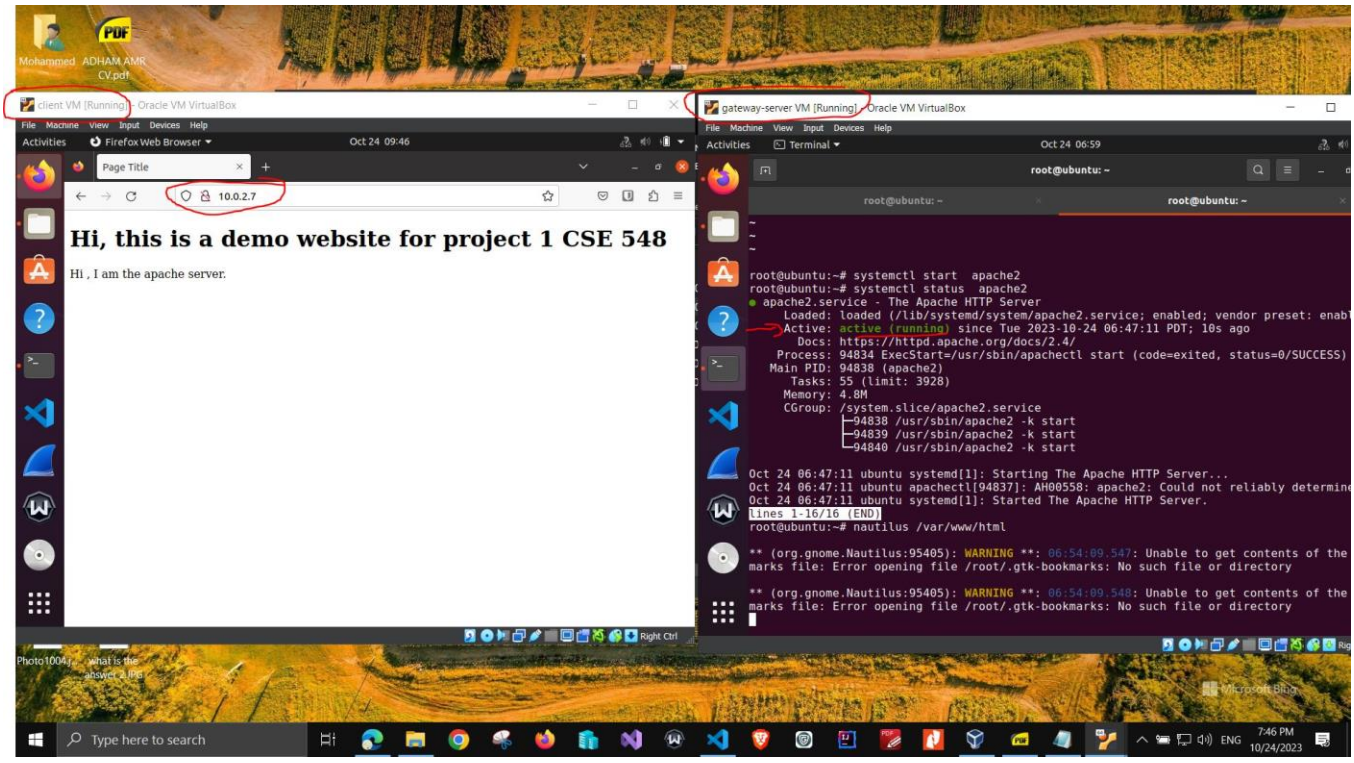
task 1.1.4.c flush all existing chains and delete all user defined chains for iptables



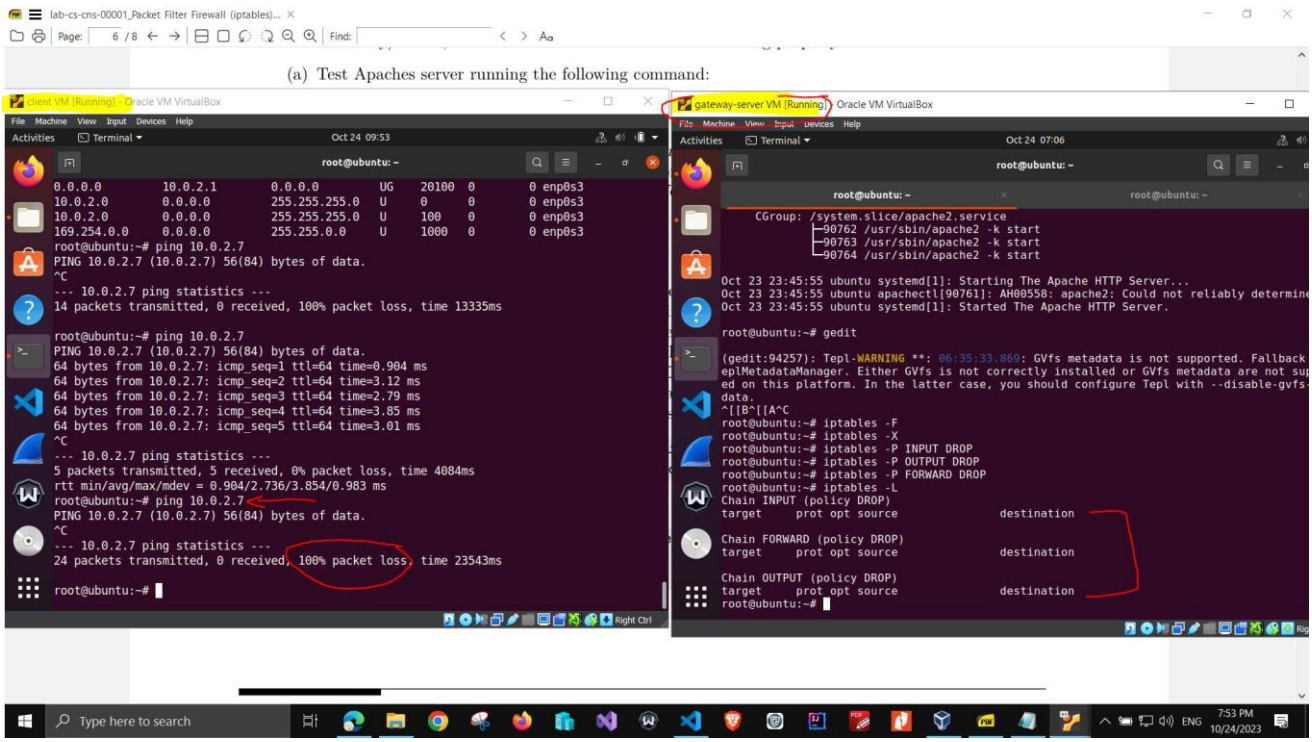
task 1.1.4.d set default policy to accept for input output and forward chains



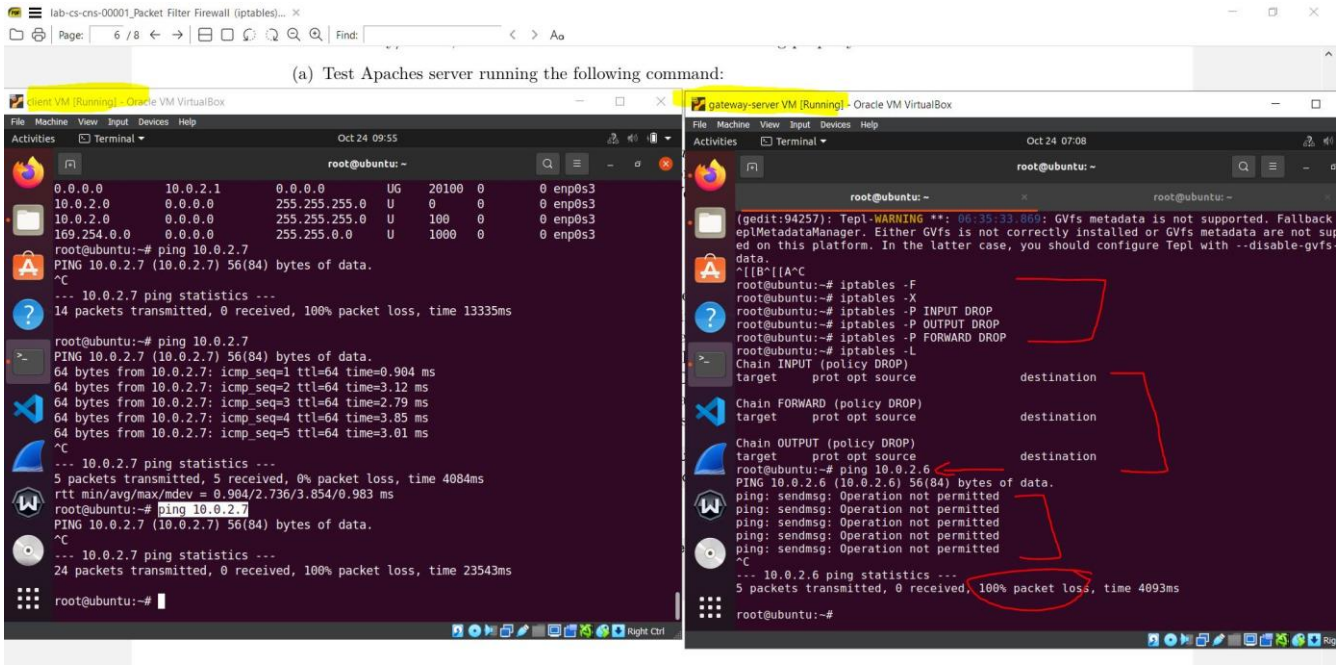
task 1.2 Apache server is running on gateway VM and client can access the server from the web browser



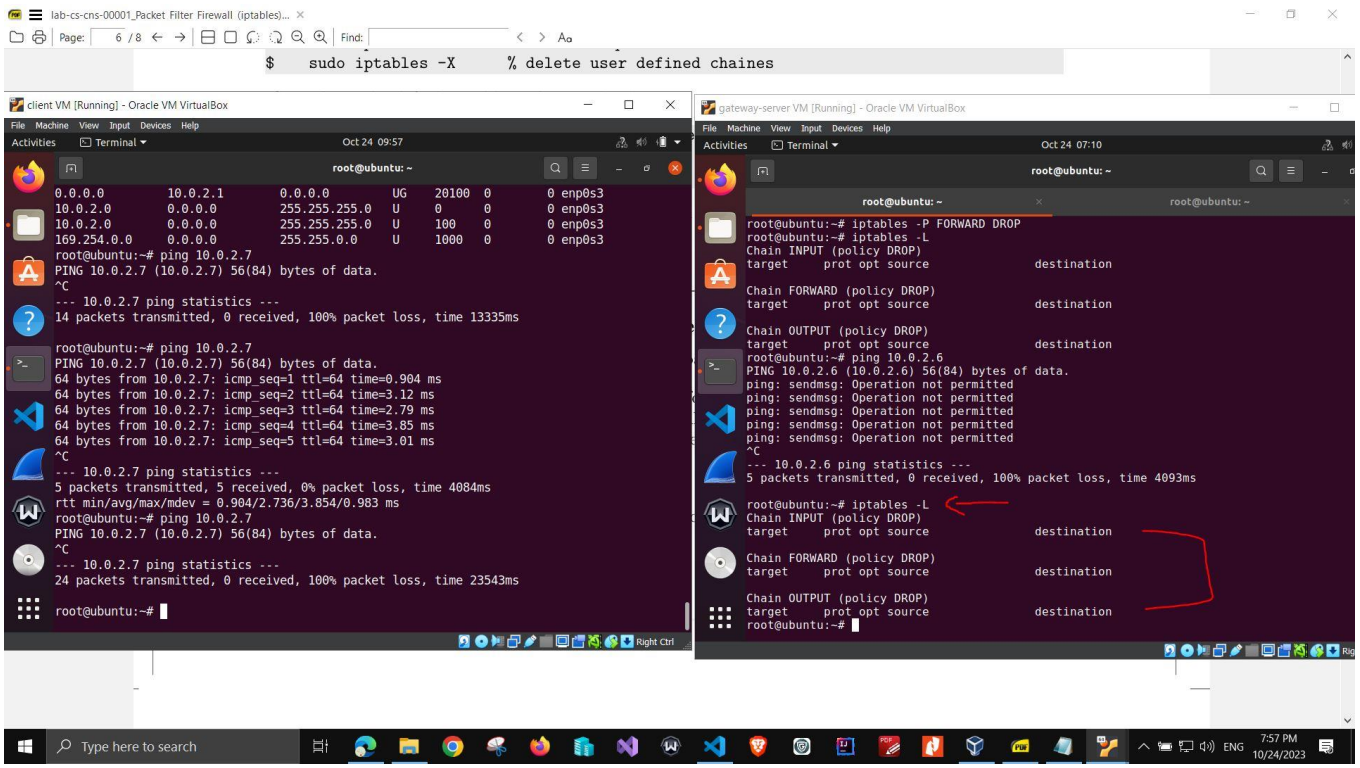
task 1.3 Reset firewall to whitelist and client VM cannot ping server VM



task 1.3 Reset firewall to whitelist and server VM cannot ping client VM

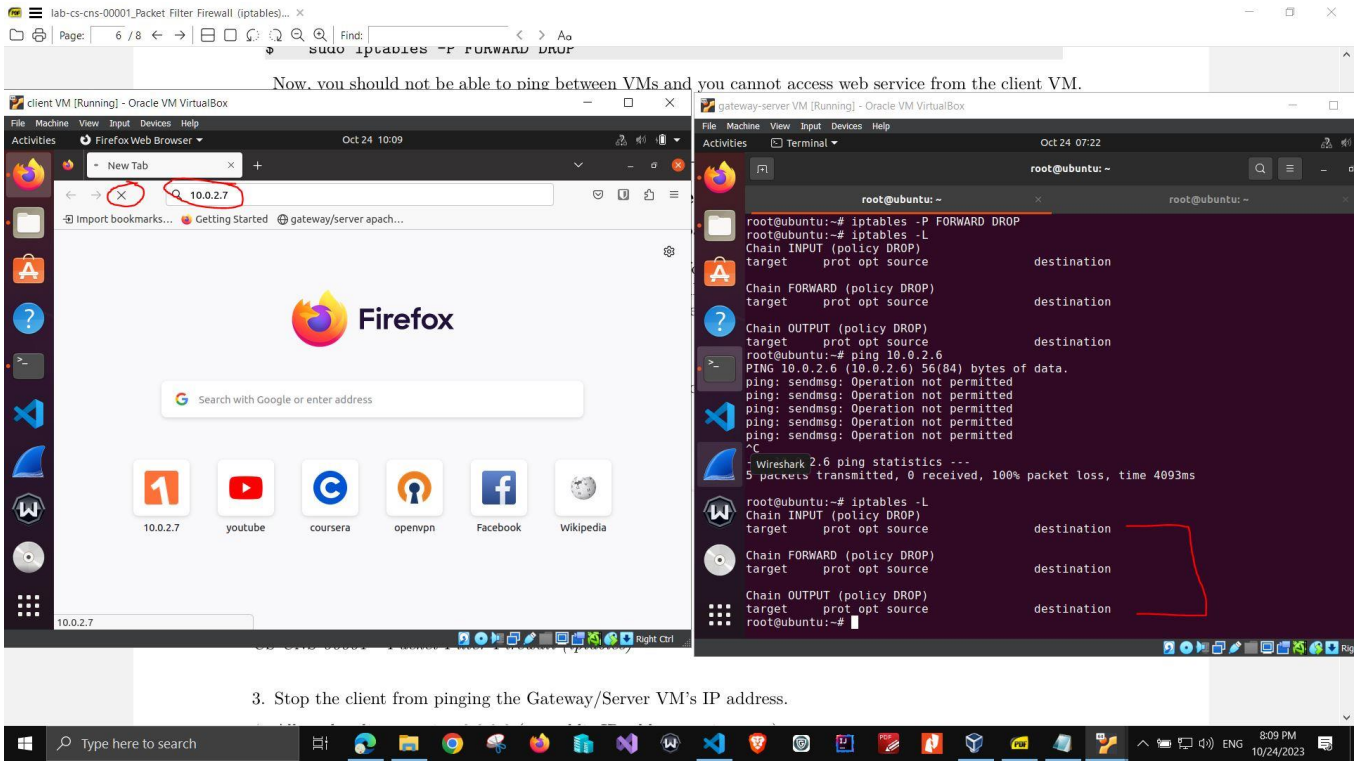


task 2.1 allow whitelist (drop for input output and forward chain) on server_gateway VM

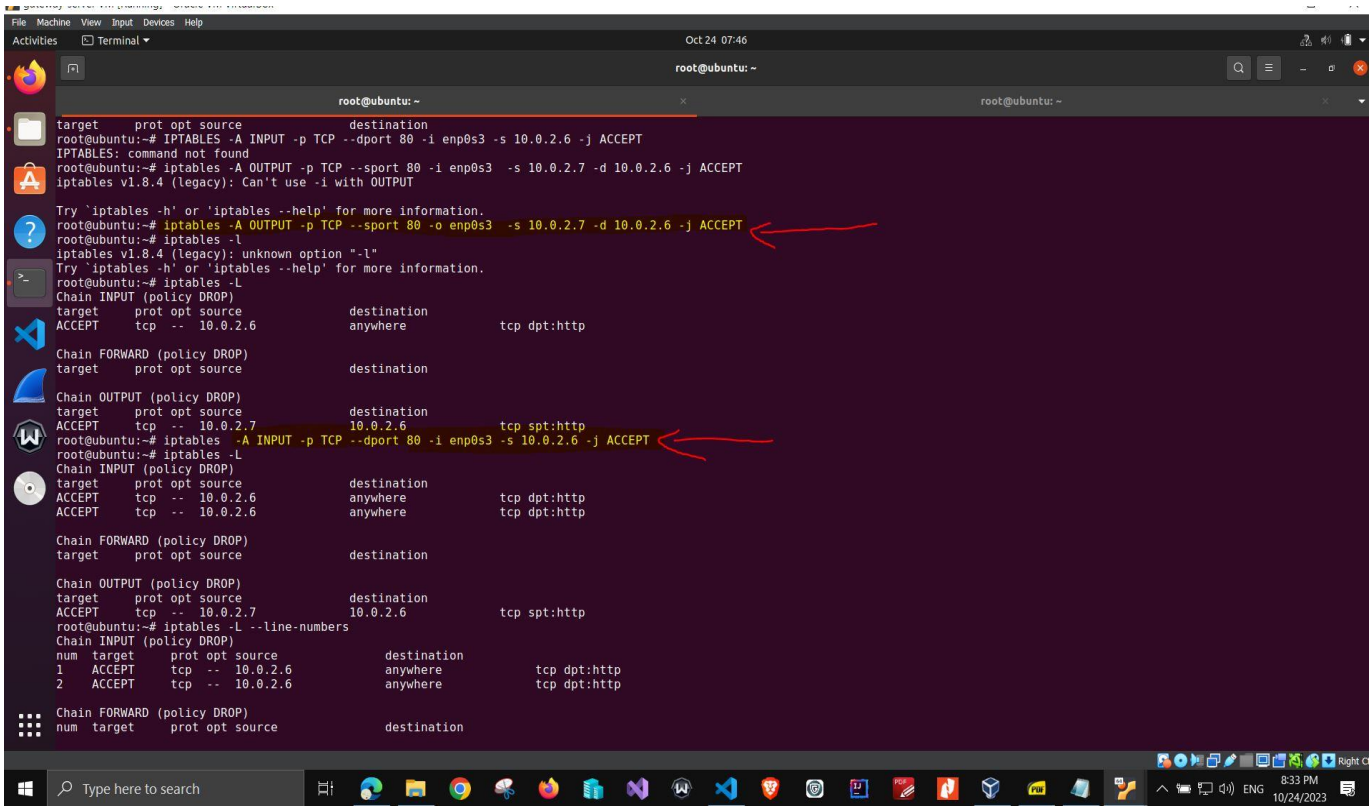


task 2.1 after allow whitelist on server_gateway VM , client VM cannot access apache web server web page fom the browser

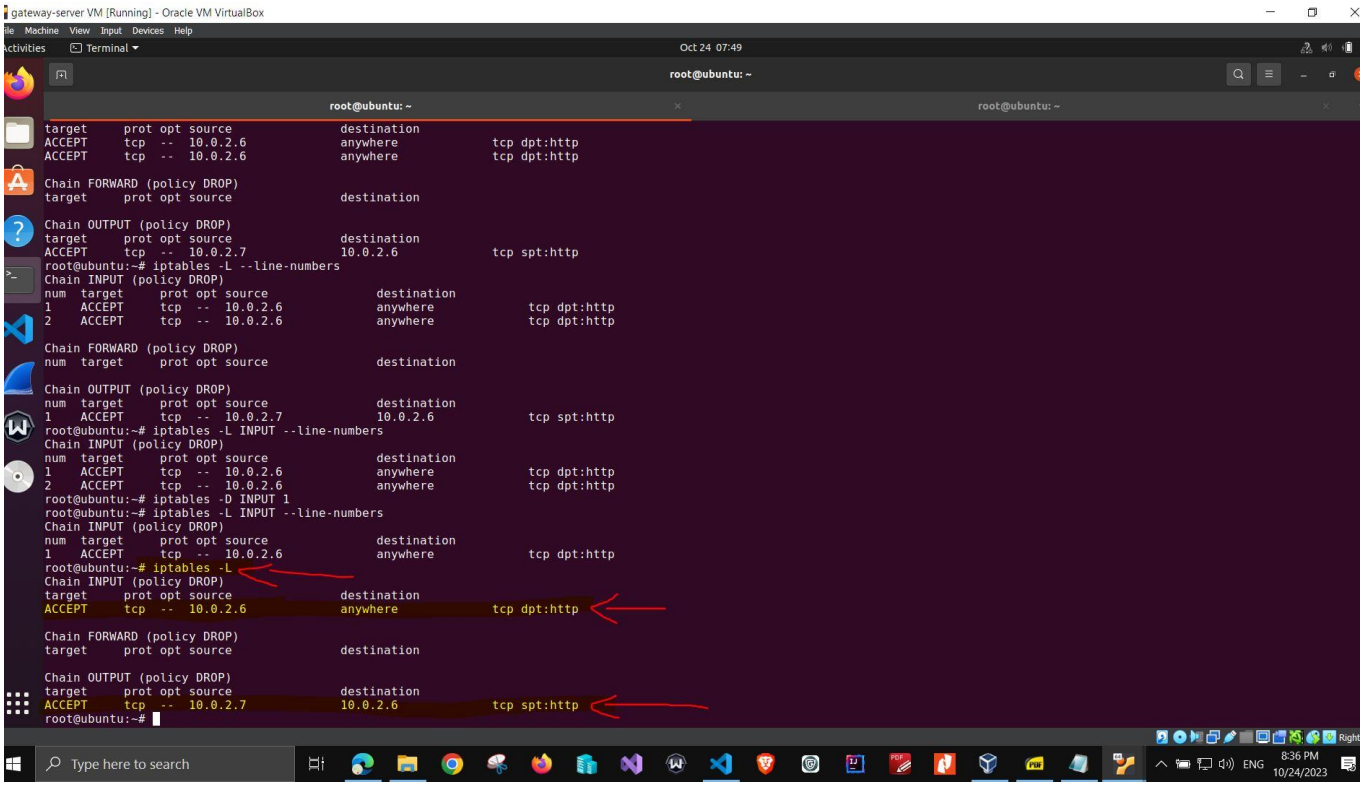
in the following screenshot, the page was loading and the Apache welcome webpage has not loaded as the client VM is blocked from accessing the server_gateway VM



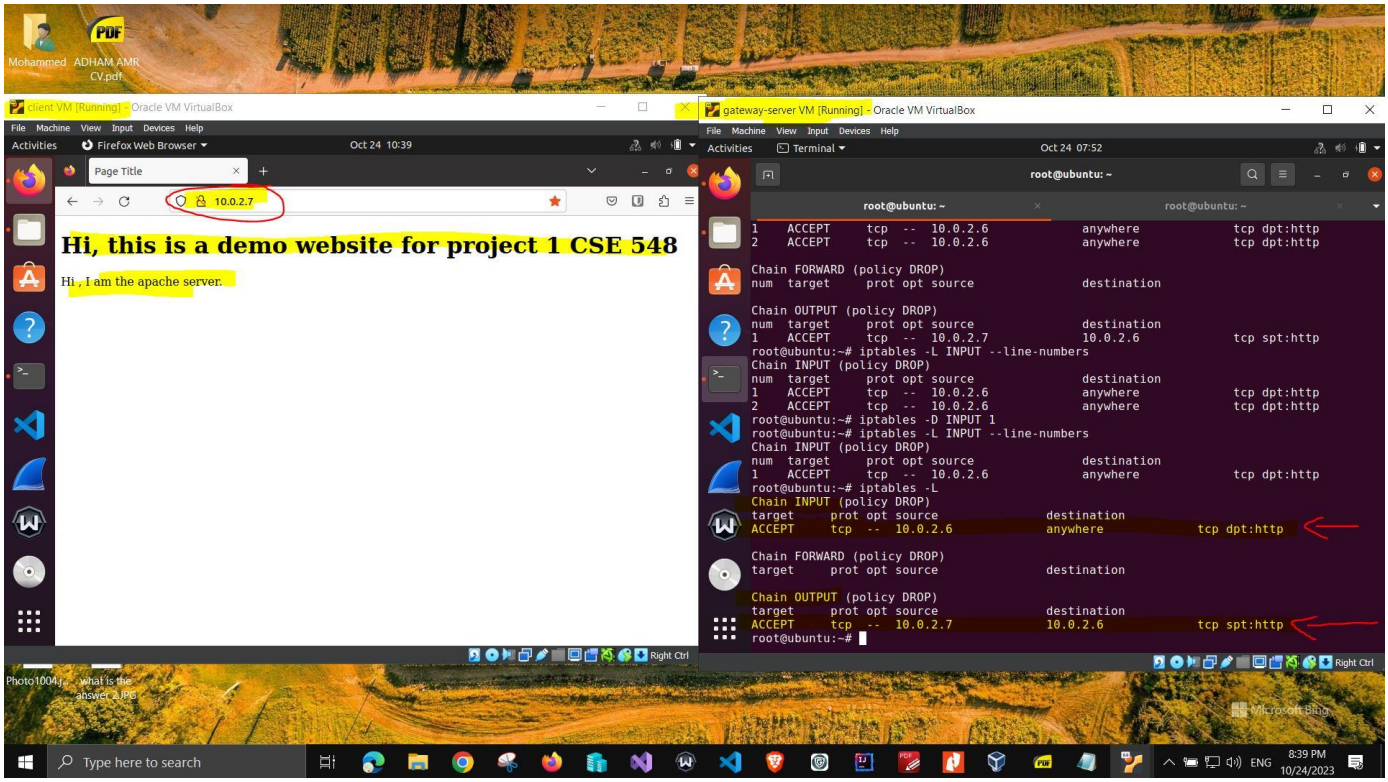
task 2.2 define the rule to allow client access the server apache on server VM



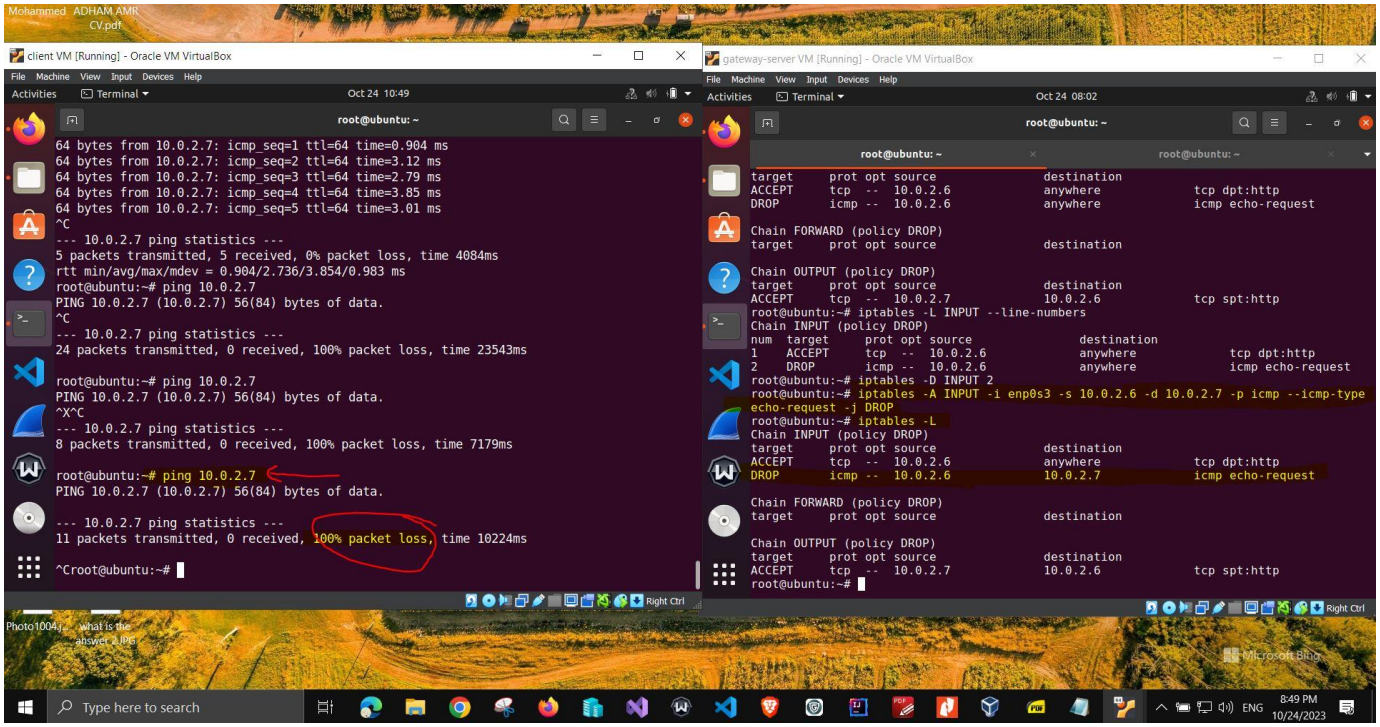
task 2.2 view the rule to allow client access the server apache on server VM



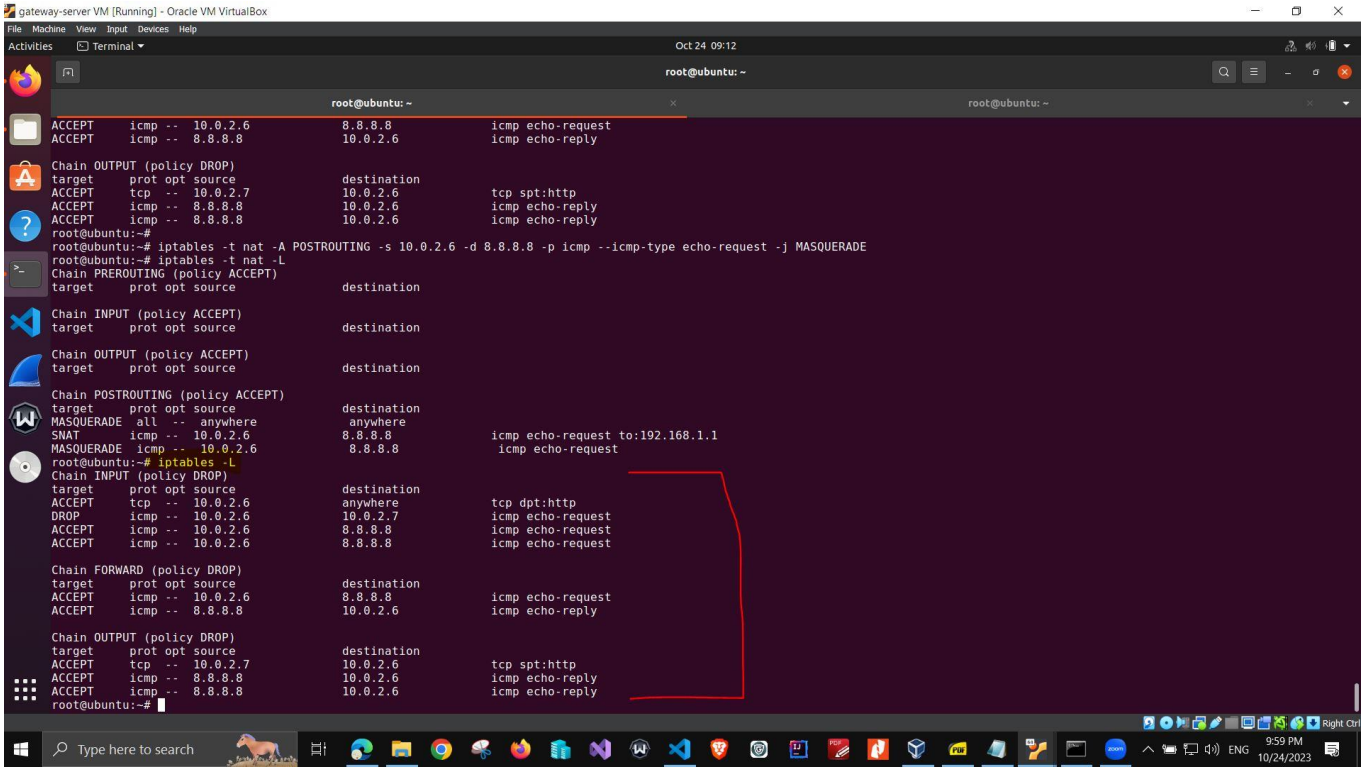
task 2.2 client can access the server apache on server VM and welcome webpage is viewed



task 2.3 Stop the client from pinging the Gateway_Server VM IP address



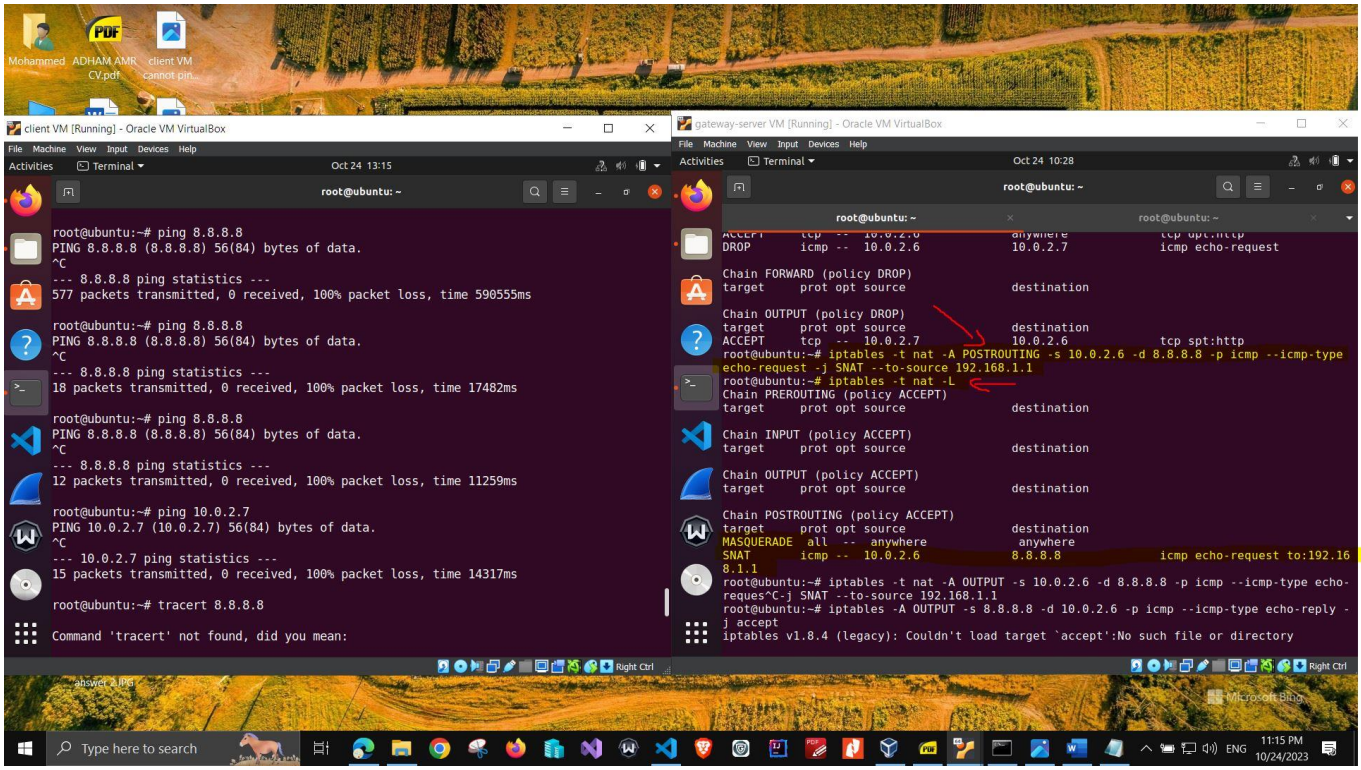
task 2.3 Stop the client from pinging the Gateway_Server VM IP address_iptables rules for filter table



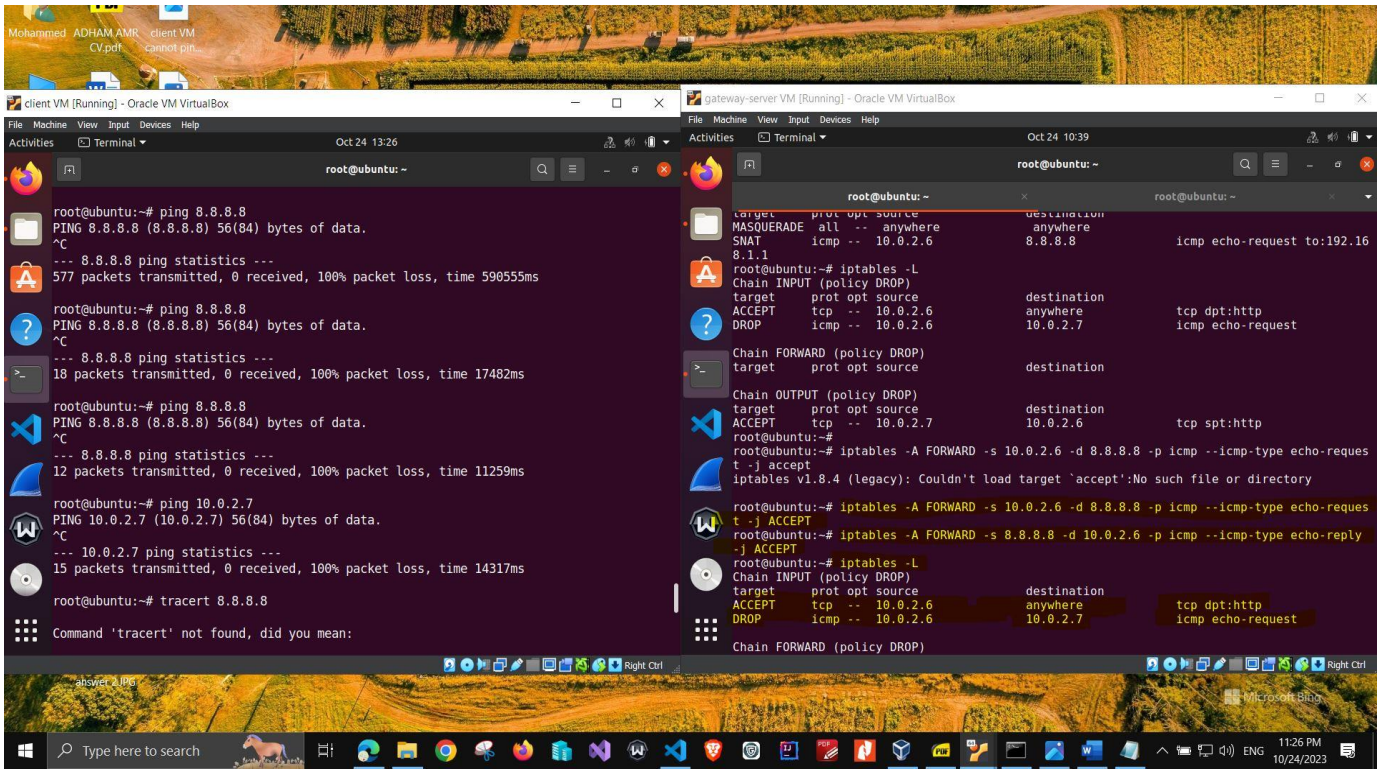
task 2.4 Allow the client to ping 8.8.8.8 (an public IP address on internet)_iptables rule for NAT table for POSTROUTING chain

note: the client VM cannot ping 8.8.8.8 , the TA reviewed my rules for the NAT table and it seems everything is correct, but the issue still appear. I posted this on the discussion website (Ed) website and also I added another rules for the filter table for INPUT and OUTPUT chain to allow ICMP request and ICMP response from client IP = 10.0.2.6 to 8.8.8.8 , unfortunately client VM still cannot ping 8.8.8.8

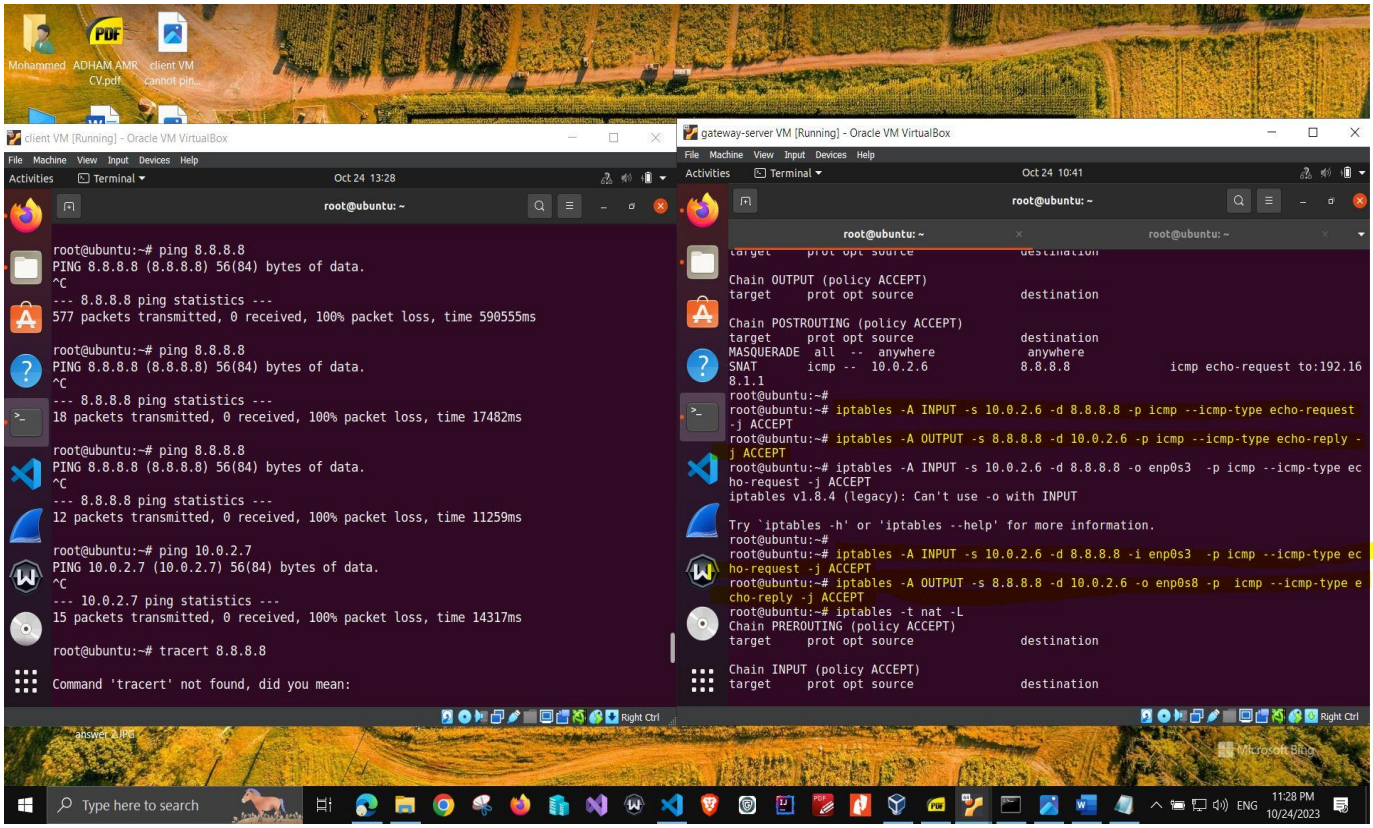
also I added a rule for FORWARD chain for filter table , and added a rule for INPUT and OUTPUT chains for filter table, but still client VM still cannot ping 8.8.8.8



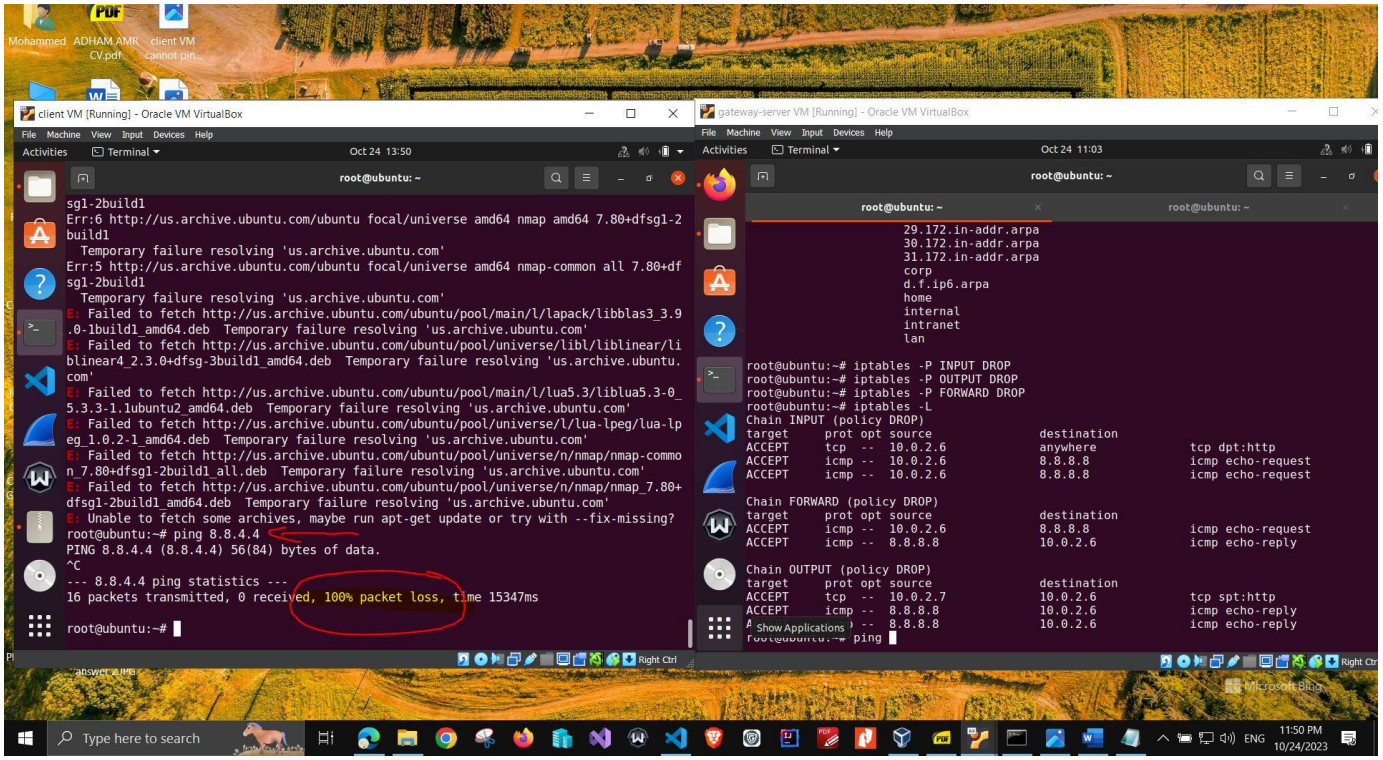
task 2.4 Allow the client to ping 8.8.8.8 (an public IP address on internet)_iptables rule for FORWARD chain for filter table



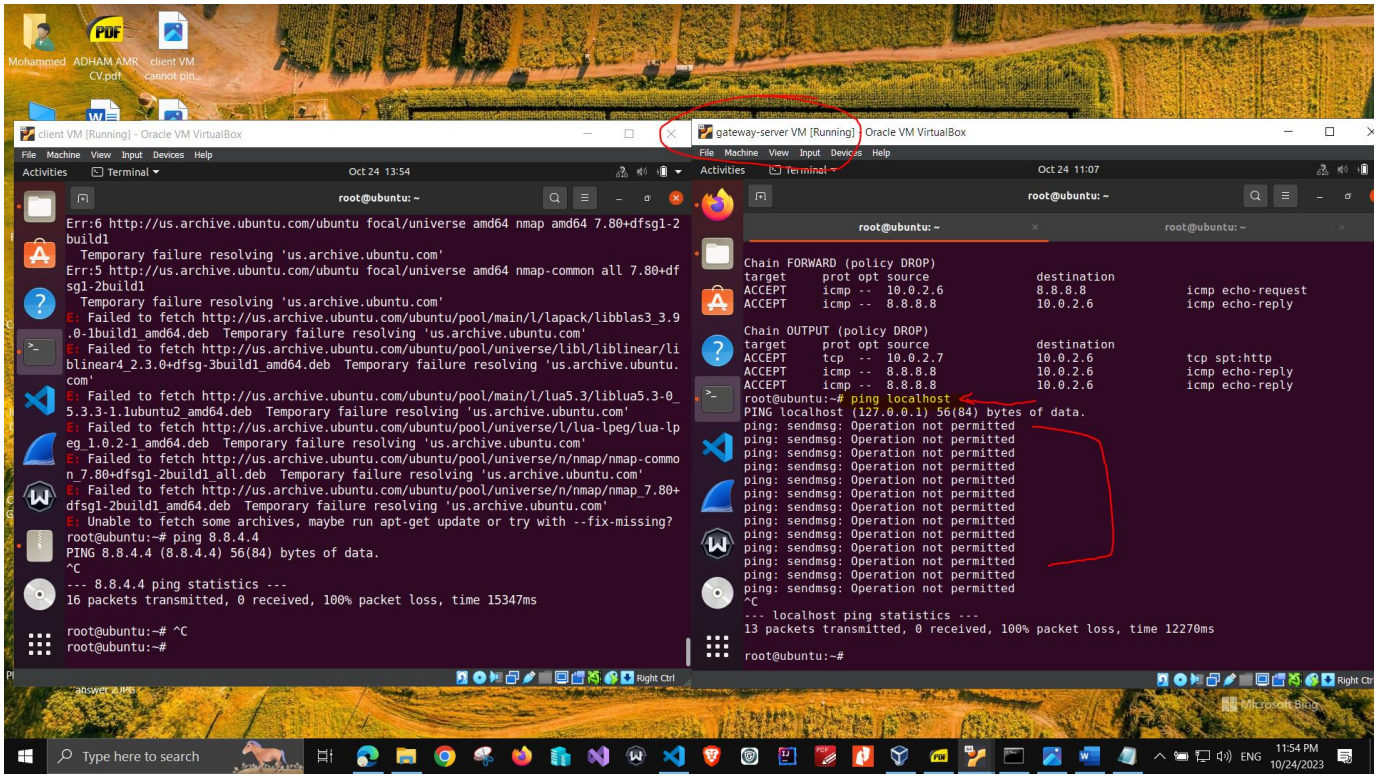
task 2.4 Allow the client to ping 8.8.8.8 (an public IP address on internet)_iptables rule for INPUT and OUTPUT chains for filter table.JPG



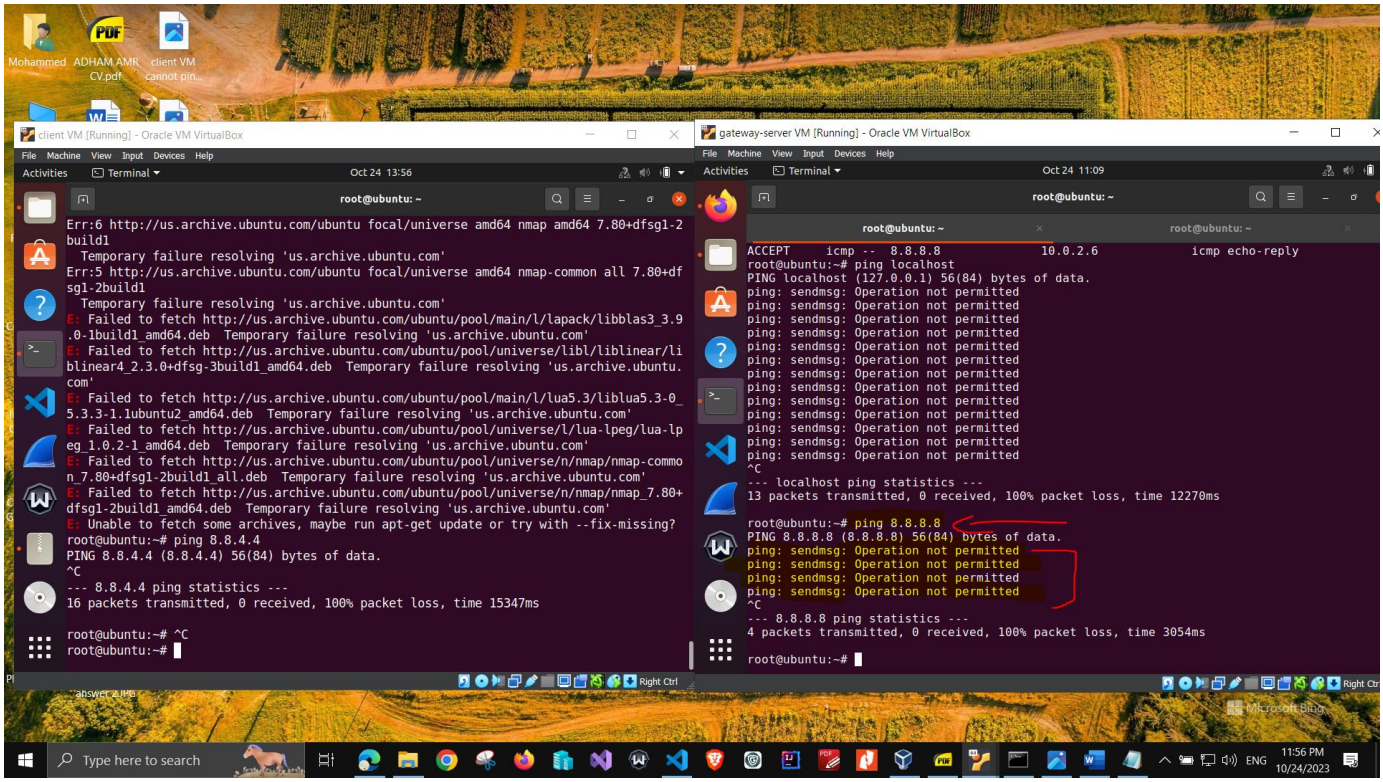
task 2.4 the client cannot ping 8.8.4.4 (an public IP address on internet)



task 2.4 cannot ping localhost on gateway_server VM

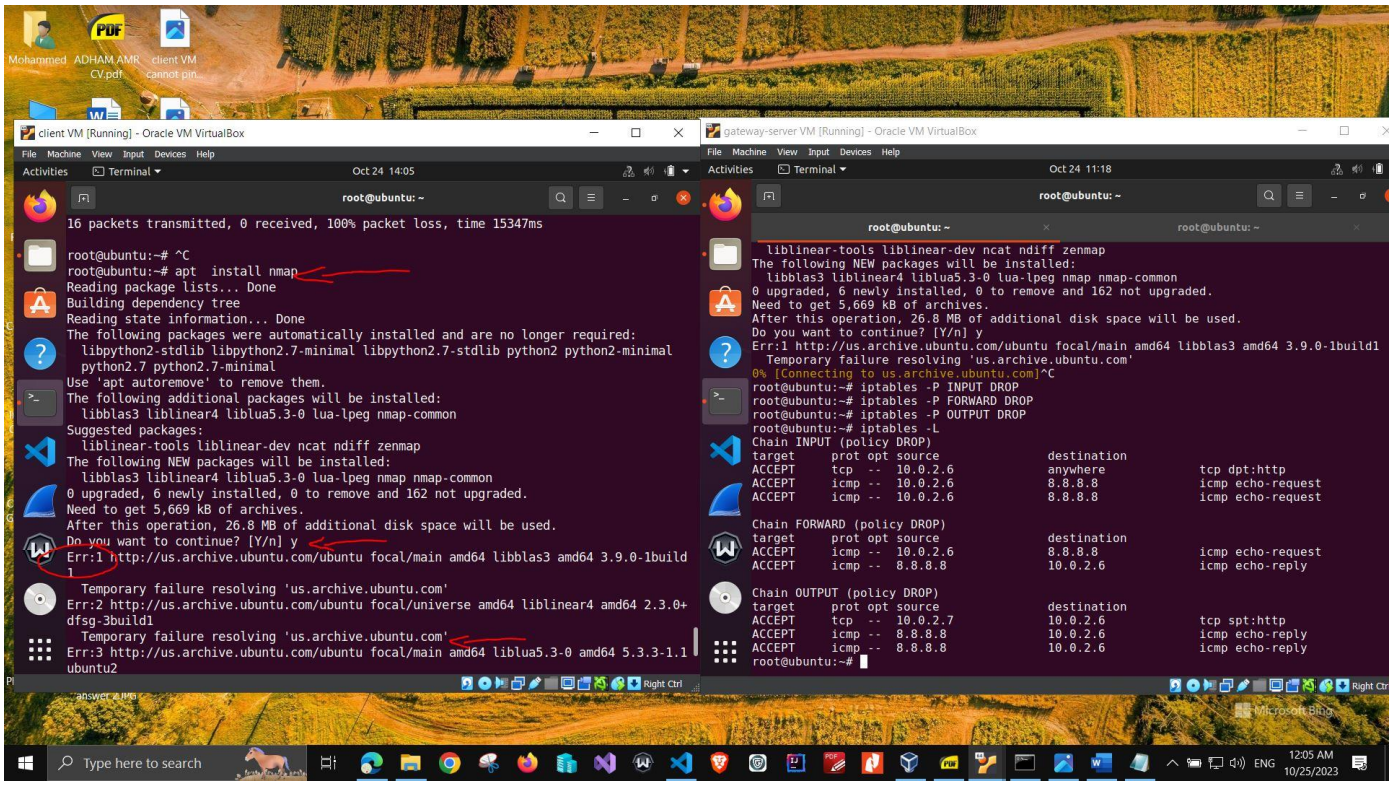


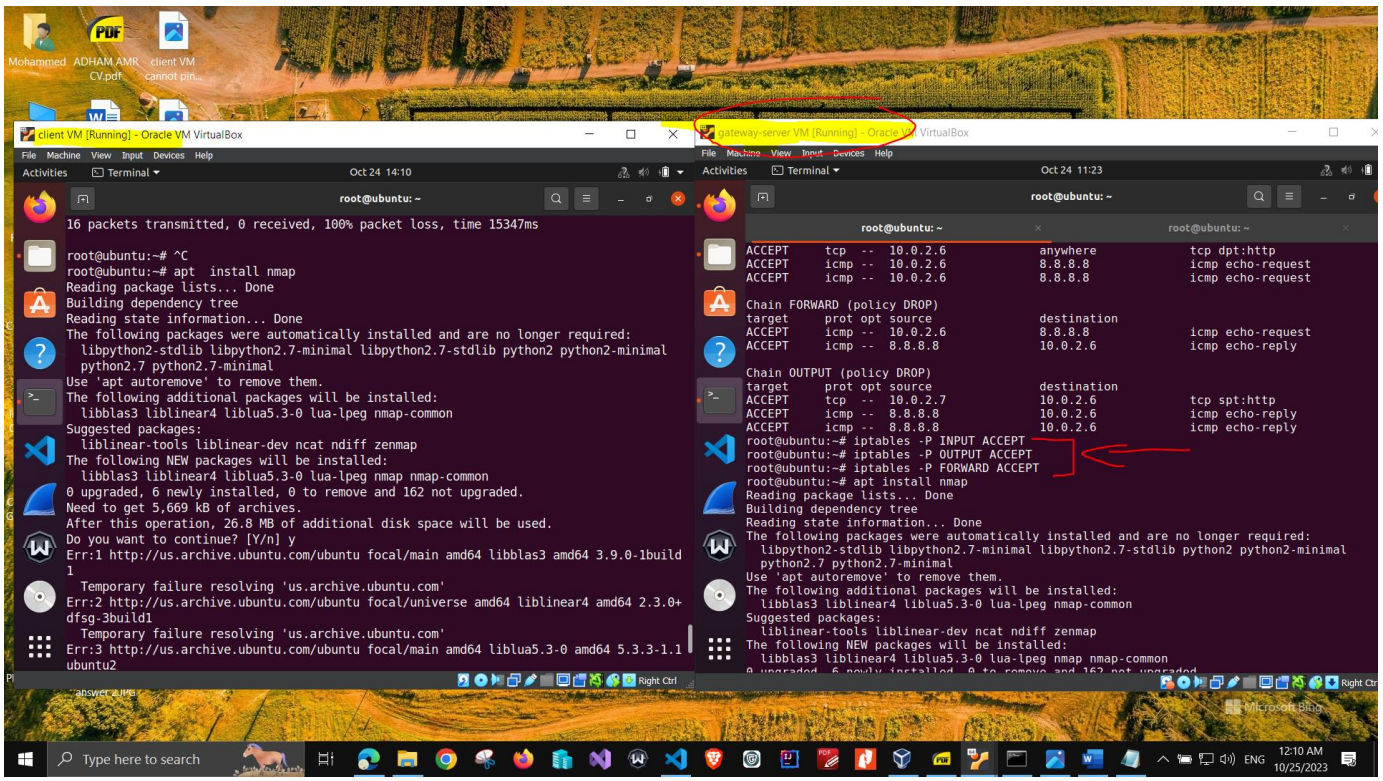
task 2.4 cannot ping localhost on gateway_server VM



Note: I failed to install NMAP tool on client VM after I SET the rules for filter table although I set to ACCEPT for INPUT , OUTPUT, and FORWARD chain for filter table , I tried to install NMAP tool offline and it failed, so I could not run the following commands on client VM:

sudo nmap -sT -p- 10.0.2.x % x is the value of your Gateway/Server VM's IP address
sudo nmap -sU -p- 10.0.2.x % x is the value of your Gateway/Server VM's IP address





V. Conclusion

I have learned many useful and practical linux commands to filter the network packets , this helped me to discover the iptables command and run 2 virtual machines simultaneously so that I have a home lab to simulate 2 machines on the same NAT network. I really liked the instructions provided because it is easy to follow with and apply hands-on experience.

VI. Appendix B: Attached files

I have not used configuration file to run the iptables commands, I used the terminal on the virtual machine directly and I asked the professor on the zoom live session on 22-10-2023 and she said it is fine to do this .

I uploaded a text file on GitHub that contains a draft for the commands I used and my process of thinking of meeting the required tasks.

https://github.com/Mohammed-Ragab/CSE-548-advanced-network-security/blob/main/project%201%20draft%20and%20notes.txt

References

Reference is optional, but nice to have to allow others to read your report with additional linked source for validation and learning.

- (n.d.). Retrieved from https://linux-training.be/networking/ch14.html#:~:text=The%20filter%20table%20in%20iptables,(routed)%20through%20the%20system
- (n.d.). Retrieved from YOUTUBE: https://www.youtube.com/watch?v=H1WPwAjMXRo