

A white paper with black text

AI-generated content may be incorrect.

Name-Hari Om

Operating Systems:

Server: CentOS

Client1:CentOS & Client2:Ubuntu

[Server]

Connecting Adapter 1 to Bridged Network

A screenshot of a computer

AI-generated content may be incorrect.

Connecting Adapter2 to Net2 subnet

A screenshot of a computer

AI-generated content may be incorrect.

Connecting Adapter 3 to Net 3 subnet

A screenshot of a computer

AI-generated content may be incorrect.

[Client1]

Connecting Adapter2 to Net2 subnet

A screenshot of a computer

AI-generated content may be incorrect.

Connecting Adapter4 to Net4 subnet

A screenshot of a computer

AI-generated content may be incorrect.

[Client2]

Connecting Adapter3 to Net3 subnet

A screenshot of a computer

AI-generated content may be incorrect.

Connecting Adapter 4 to Net4 subnet

A computer screen shot of a network

AI-generated content may be incorrect.

Task 1

Configure static addresses on all interfaces on Server.

[Server]

Assign static ips on Server1

Configure enp0s3 

A screenshot of a computer

AI-generated content may be incorrect.

Configure enp0s8



A screenshot of a computer

AI-generated content may be incorrect.

Configure enp0s9

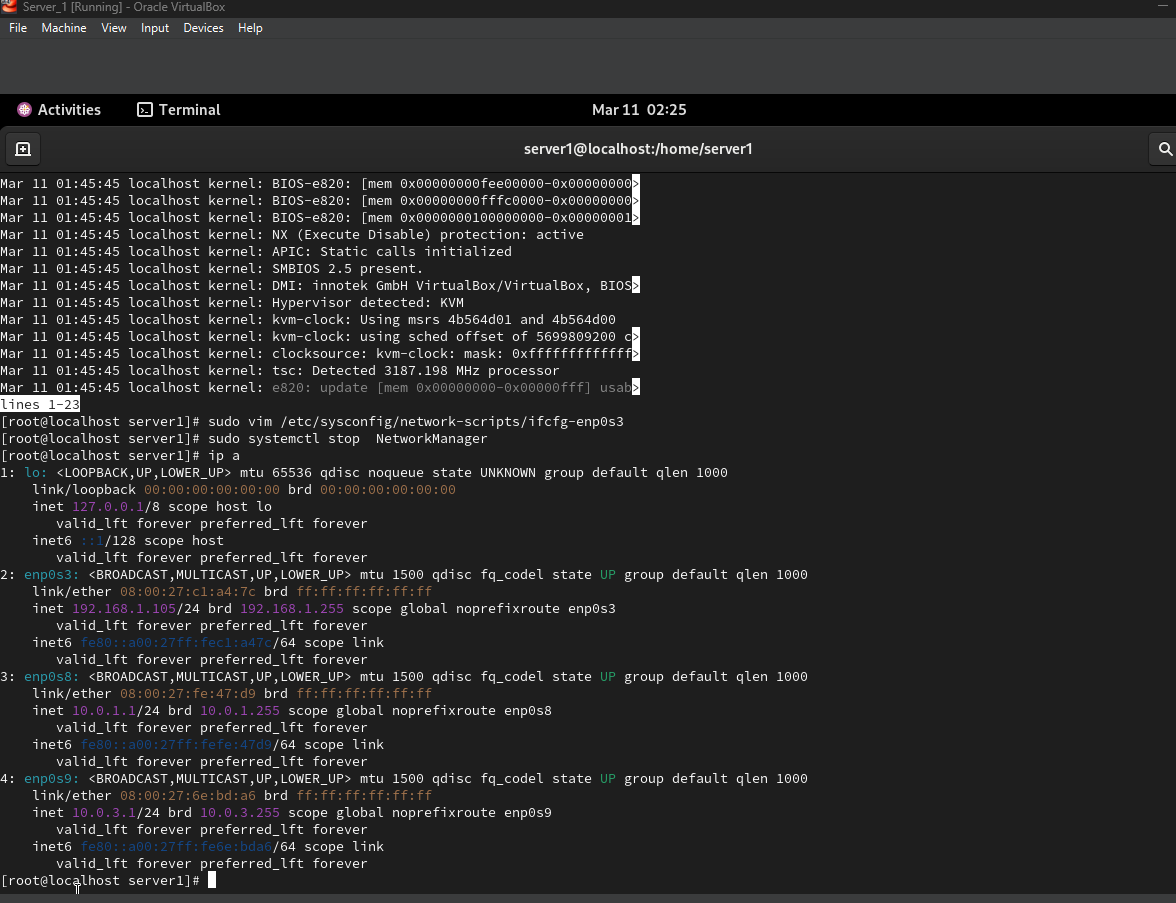


A screenshot of a computer

AI-generated content may be incorrect.

After static ip assignment:

-output of ip a



Task 2

Configure the DHCP service on Server, which will configure the Int1 addresses of Client1 and Client2

[Server]

-install dhcp

-sudo yum install -y dhcp-server



-sudo vim /etc/dhcp/dhcpd.conf

-add necessary configuration



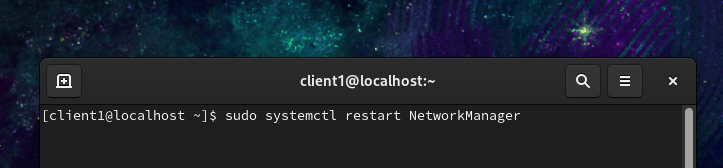
-sudo vim /etc/default/isc-dhcp-server

-add interfaces on which dhcp server will serve requests

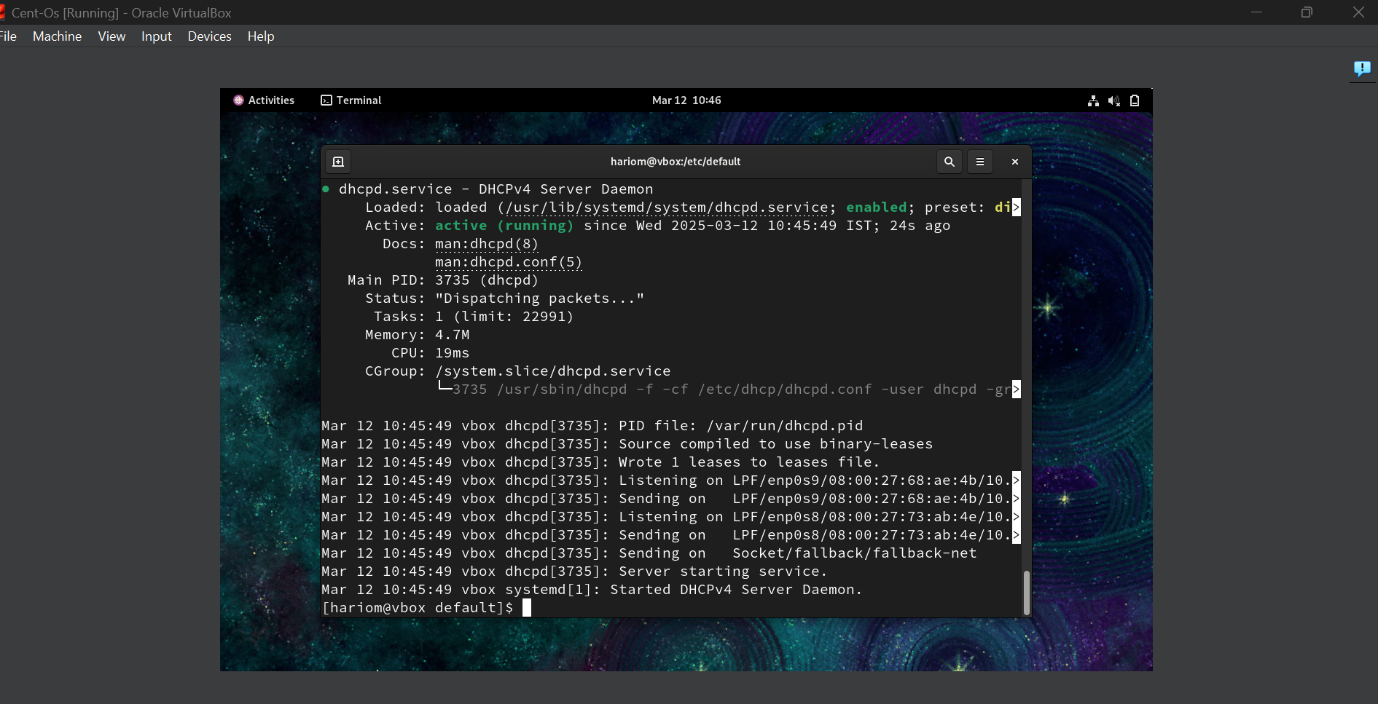
-INTERFACESv4 =”enp0s3 enp0s9”

-restart services

-sudo systemctl restart NetworkManager

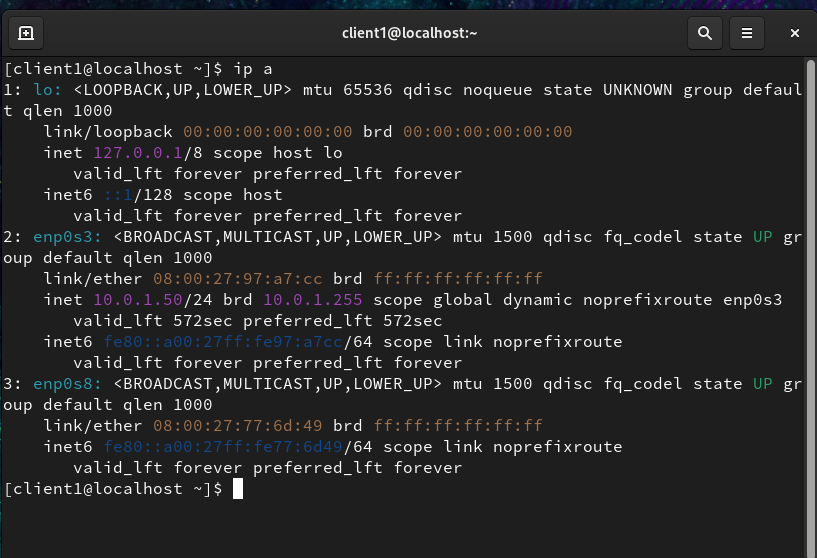


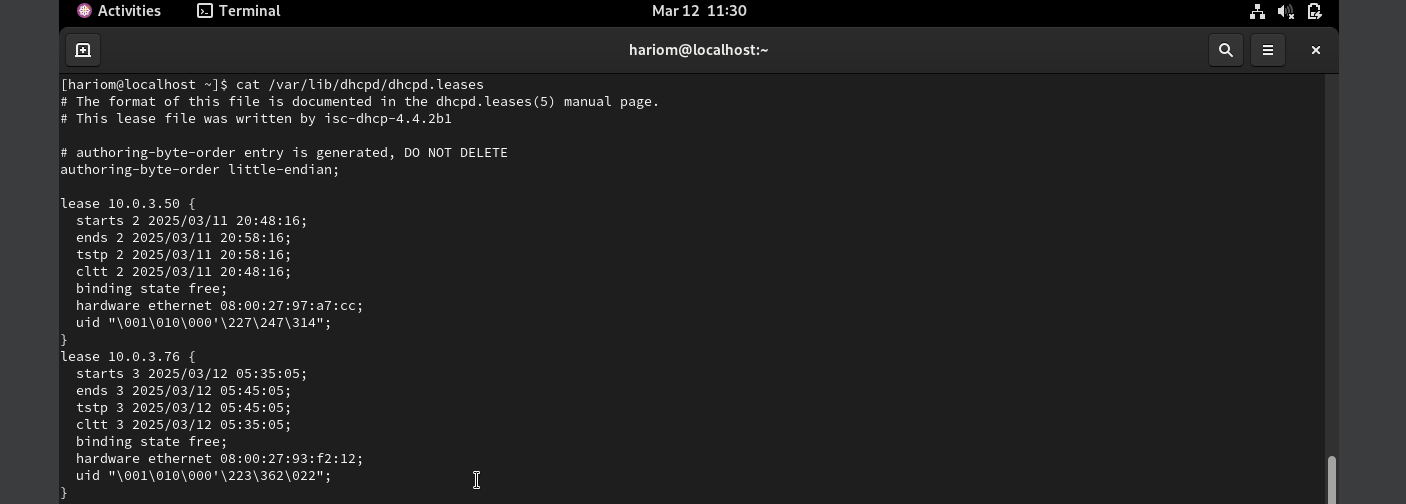
-sudo systemctl status dhcpd.service



Check if client1 and client2 has received dynamic ips from the dhcp server.

[Client1]





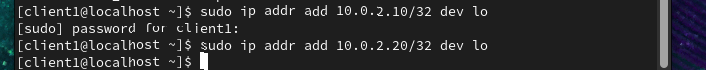
Task 3

On the virtual interface lo Client1, assign two IP addresses IPaddr1 and IPaddr2. Configure routing so that traffic from Client2 to IPaddr1 goes through Server, and to IPaddr2 through Net4. To check, use traceroute.

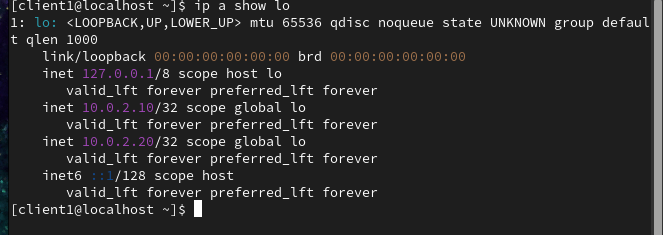
[Client1]

-sudo ip addr add 10.0.2.10/32 dev lo

-sudo ip addr add 10.0.2.20/32 dev lo



Add ip addresses to loopback interface



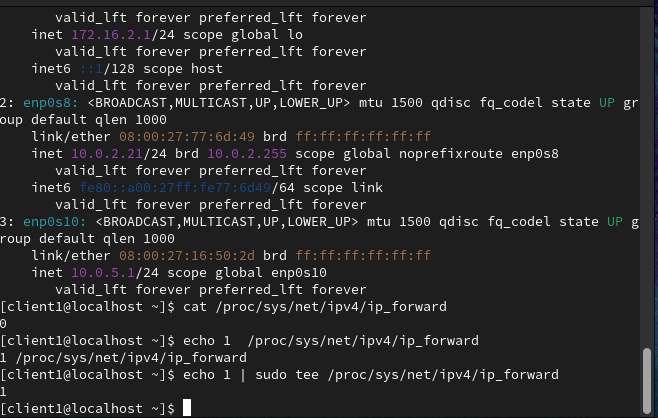
-sudo ip addr add 10.0.2.21/24 dev enp0s8

Add ip address to INT enp0s8 of Client1



-echo 1 | sudo tee /proc/sys/net/ipv4/ip\_forward

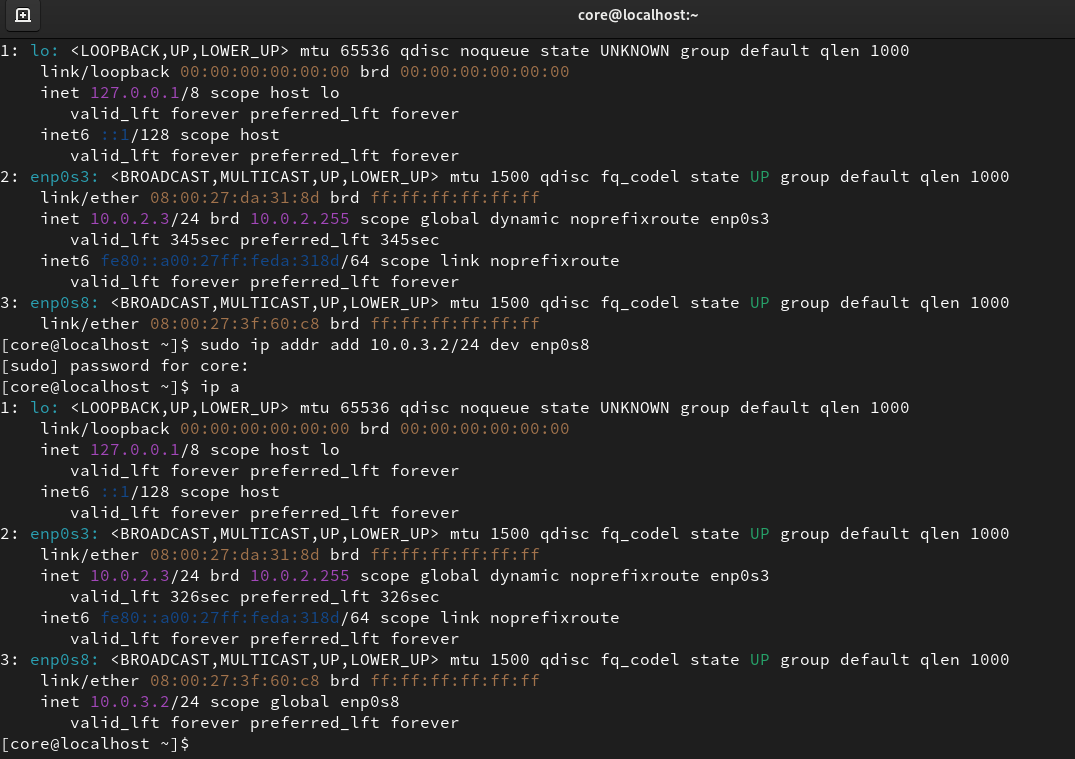
Enable packet forwarding



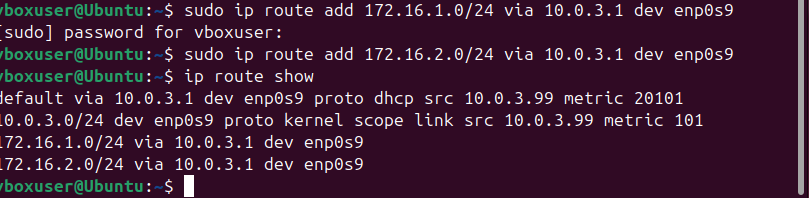
[Client2]

-sudo ip addr add 10.0.3.2/24 dev enp0s8

Add ip address to INT enp0s8



Add route



-sudo ip route add 172.16.1.0/24 via 10.0.3.1

-sudo ip route add 172.16.2.0/24 via 10.0.3.1

-route show

Ping loopback interface on Client1 from Client2

A screenshot of a computer

AI-generated content may be incorrect.

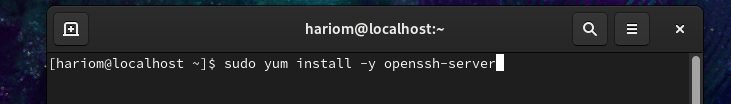
-ping -c 5 172.16.1.1

Task 4

Configure the SSH service so that Client\_1 and Client\_2 can connect to Server\_1 and each other.

[Server]

Install ssh on Server



-sudo yum install -y openssh-server

dA screenshot of a computer program

AI-generated content may be incorrect.

-sudo systemctl enable sshd --now

-sudo systemctl status ssh

Make sure port 22 is open

A screenshot of a computer

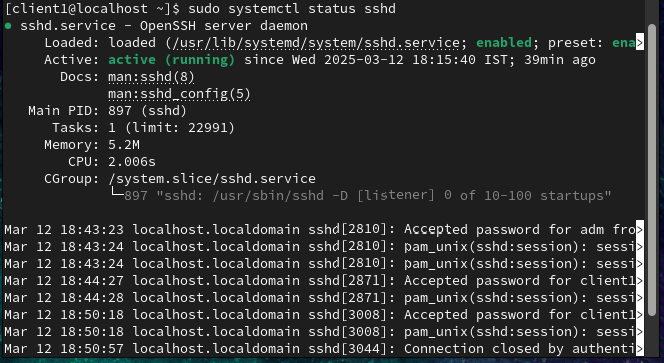
AI-generated content may be incorrect.

-sudo ufw status

[Client1]



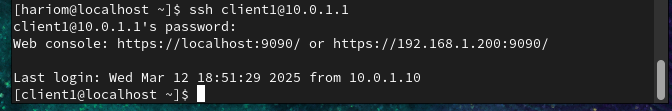
-sudo yum install openssh-server



A screen shot of a computer

AI-generated content may be incorrect.

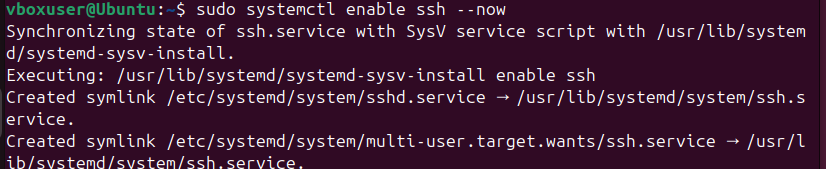
On Server1, to login as client1 from client1, we use “ssh [client1@10.0.1.1](mailto:client1@10.0.1.1)”



[Client2]

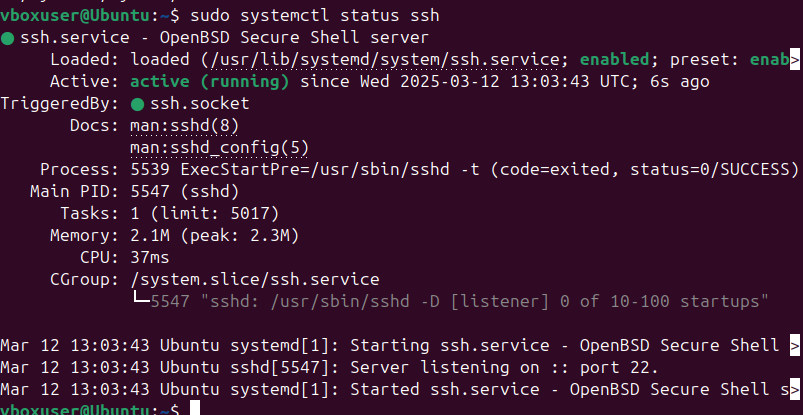


-sudo apt install -y openssh-server

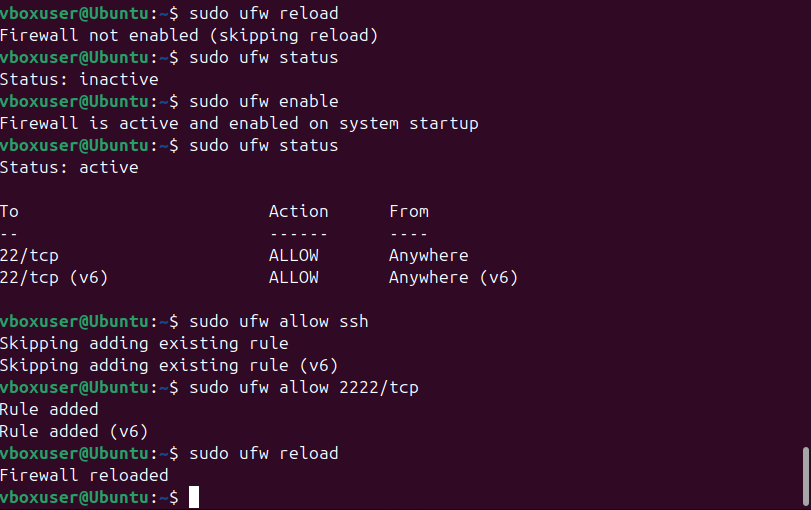


-sudo systemctl enable sshd

-sudo systemctl status sshd



Setting up Firewall to allow SSH

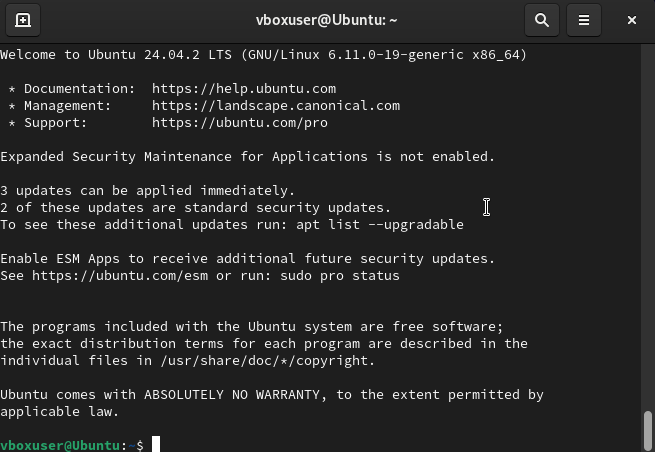


-sudo ufw allow ssh

- sudo ufw allow 2222/tcp

-sudo ufw reload

On Server1, to login as vboxuser from client2, we use “ssh [vboxuser@10.0.3.99](mailto:vboxuser@10.0.3.99)”



Task 5

Configure the firewall on Server\_1 as follows:

• Allowed to connect via SSH from Client1 and forbidden from Client2

• Client2 may ping IPaddr1, but may not ping IPaddr2

[Server]

Allow Client1 via SSH



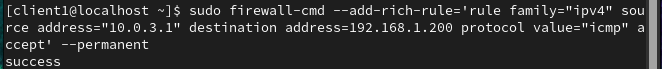
-sudo firewall-cmd –add-rich-rule=’rule family=”ipv4” source address=”10.0.1.1” service name=”ssh” accept’ --permanent

Deny Client2 via SSH



-sudo firewall-cmd –add-rich-rule=’rule family=”ipv4” source address=”10.0.1.1” service name=”ssh” accept’ --permanent

Client2 allowed to ping IPaddr1



-sudo firewall-cmd –add-rich-rule=’rule family=”ipv4” source address=”10.0.3.1” destination address=192.168.1.200 protocol value=”icmp” accept’ --permanent

Client2 not allowed to ping IPaddr2



-sudo ufw deny from 10.0.2.3 to 172.16.2.1



Apply the new rules

A screenshot of a computer program

AI-generated content may be incorrect.

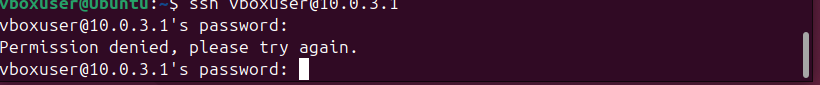
-sudo firewall-cmd –list-all

On client1, test SSH to Server1:

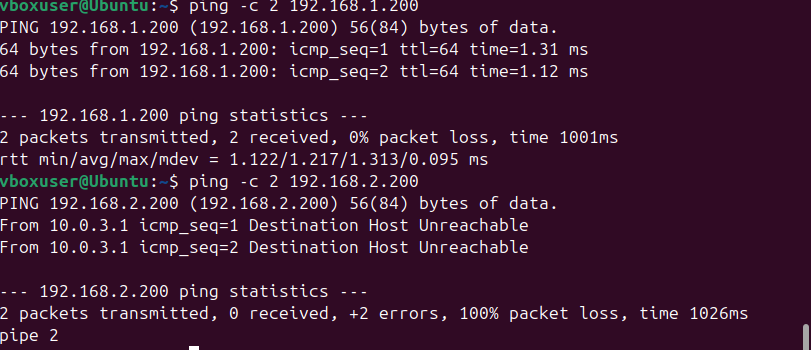
A screen shot of a computer

AI-generated content may be incorrect.

On client2, test SSH to Server1:



On client2, test ping to Ipaddr1 and Ipaddr2:



Task 6

On Server\_1, configure the NAT service so that Client\_1 and Client\_2 may ping the Internet resources, for example 8.8.8.8

[Server]

Allow packet forwarding

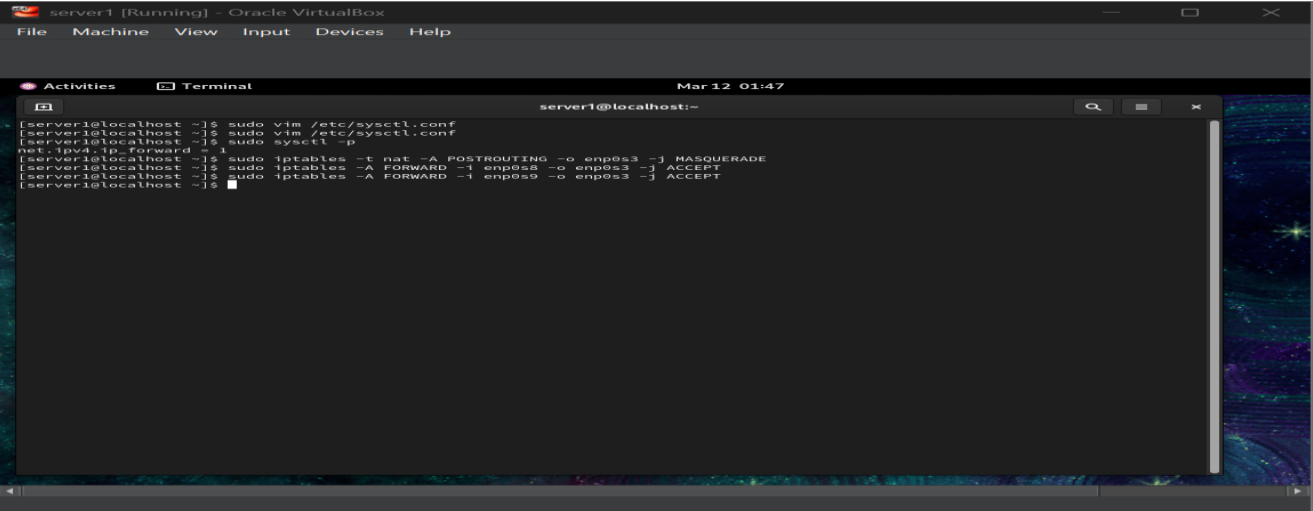
-sudo sysctl -w net.ipv4.ip\_forward=1

Configure NAT Using iptables

-sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE

-sudo iptables -A FORWARD -i enp0s8 -o enp0s3 -j ACCEPT

-sudo iptables -A FRWARD -i enp0s9 -o enp0s3 -j ACCEPT



Save iptables Rules

-sudo yum install iptables-services

-sudo systemctl enable iptables

-sudo service iptables save

A screenshot of a computer

AI-generated content may be incorrect.

Test Net4 connectivity

