

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
KHOA CÔNG NGHỆ THÔNG TIN



BÁO CÁO
BÀI TẬP DMZ NETWORK

Môn học: Quản trị dịch vụ mạng

Lớp: 20_4

Giảng viên hướng dẫn:

Lê Hà Minh

Người thực hiện:

Phan Dương Linh – 20120319

2023 – TP.Hồ Chí Minh

Mục lục

Thông tin bài tập.....	3
Nội dung báo cáo.....	4
1 Thiết lập mô hình mạng như sơ đồ, bao gồm 3 networks:	4
2 Thiết lập Router là 1 server Linux, với các interfaces:	4
3 Thiết lập cho mỗi network một máy Linux với địa chỉ như sau:	6
4 Thiết lập firewalld, zone external cho interface 1, zone dmz cho interface 2, zone internal cho interface 3.....	8
5 Kiểm tra kết nối giữa các máy tính (ping).....	12
6 Cấu hình 1 Web server trên server thuộc DMZ network, chỉ cần phục vụ 1 website đơn giản.....	13
7 Cấu hình NAT, port forwarding trên router để client tại external network và internal network có thể truy cập website tại DMZ network.	14
a. Cấu hình NAT và port forwarding trên Router:	14
b. Tiến hành cho client tại external truy cập website:	17
c. Tiến hành cho client tại internal truy cập website:	17
Tài liệu tham khảo	18
➤ Tài liệu môn học:	18
➤ Tài liệu trực tuyến:	18

Thông tin bài tập

Giảng viên hướng dẫn:

- Lê Hà Minh

Hệ điều hành:

- Linux(lubuntu 18.04 LTS)
- Linux(Ubuntu 22.04 LTS)

Phần mềm hỗ trợ:

- GNS3 2.2.39
- Vmware Workstation Pro 17
- Oracle VM VirtualBox 7.0.8

Ngôn ngữ thực hiện: Bash Shell Script

Người thực hiện:

- Phan Dương Linh – 20120319

Đánh giá mức độ hoàn thành: 100%

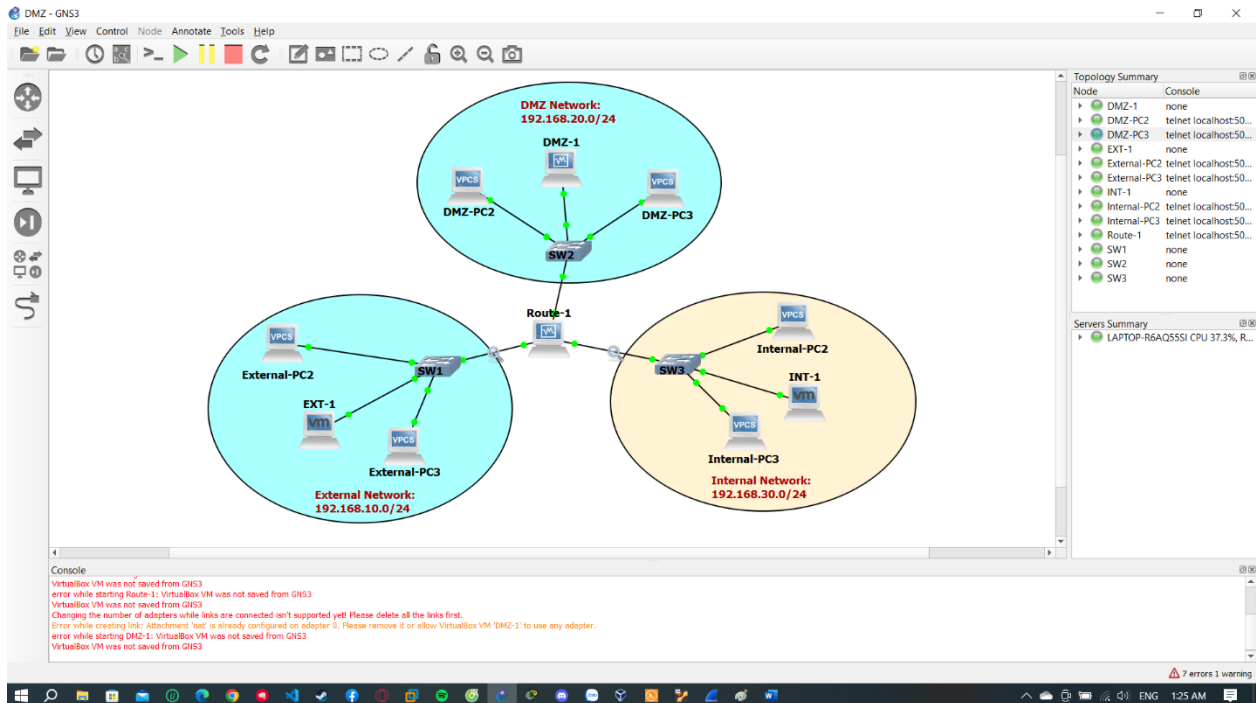
Nội dung hoàn thành:

- Hoàn thành yêu cầu đưa ra.
- Viết báo cáo quá trình thực hiện, nêu giải pháp, thuật giải sử dụng trong script.

Nội dung báo cáo.

1 Thiết lập mô hình mạng như sơ đồ, bao gồm 3 networks:

- External network: 192.168.10.0/24
- DMZ network: 192.168.20.0/24
- Internal network: 192.168.30.0/24



Sử dụng GNS3 để giả lập mô hình mạng như sơ đồ. Sử dụng các máy ảo để giả lập router và host:

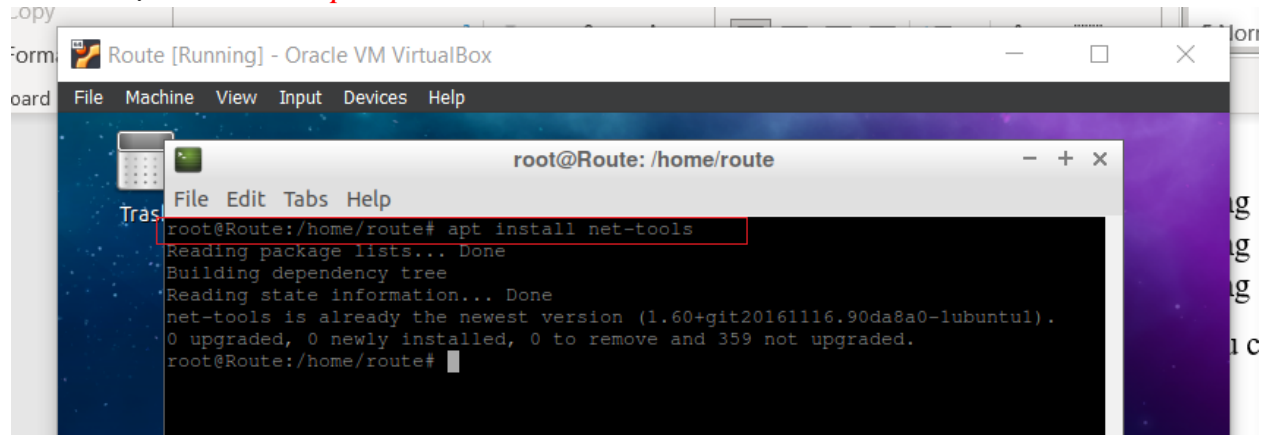
- Router giả lập từ máy ảo Route – Virtual Box Ubuntu 18.04 LTS.
- DMZ-1 giả lập từ máy ảo LTC – Virtual Box Ubuntu 18.04 LTS.
- EXT-1 và INT-1 giả lập từ máy ảo EXT và INT – Vmware Ubuntu 22.04 LTS.

2 Thiết lập Router là 1 server Linux, với các interfaces:

Giả lập router bằng 1 máy ảo Virtual Box có tên là Route chạy Ubuntu 18.04 LTS. Tiến hành thiết lập các Interface:

- Interface 1: 192.168.10.1 (tương ứng interface enp0s3)
- Interface 2: 192.168.20.1 (tương ứng interface enp0s10)
- Interface 3: 192.168.30.1 (tương ứng interface enp0s9)

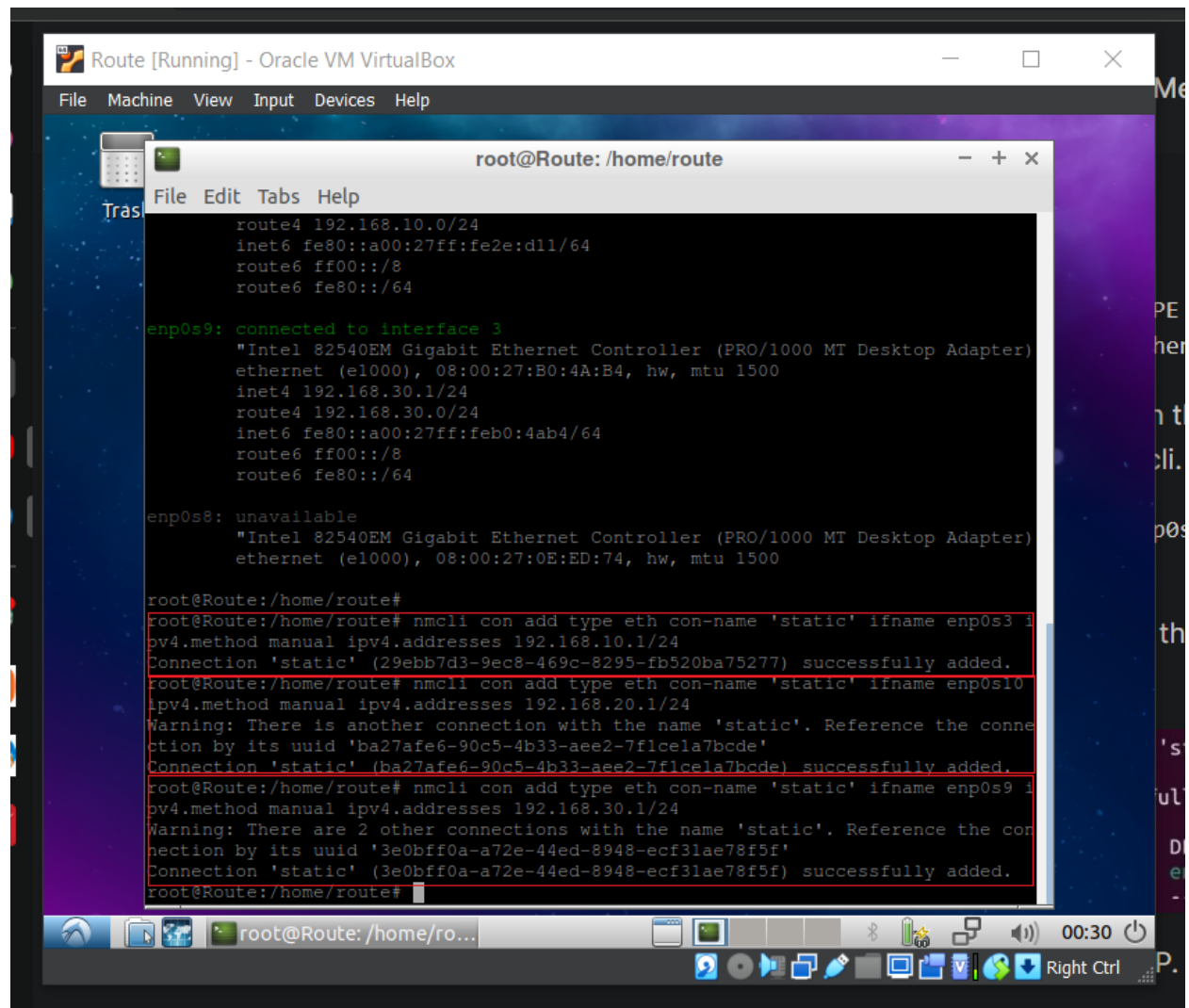
- Cài đặt thiết lập máy ảo với những yêu cầu cơ bản.
- Cài đặt net-tools : *apt install net-tools*



The screenshot shows a terminal window titled 'root@Route: /home/route'. The user has entered the command 'apt install net-tools'. The output shows that the package lists are read, the dependency tree is built, and state information is read. It then states that 'net-tools' is already the newest version (1.60+git20161116.90da8a0-lubuntu1) and that 0 packages were upgraded, 0 newly installed, 0 to be removed, and 359 not upgraded.

```
root@Route:/home/route# apt install net-tools
Reading package lists... Done
Building dependency tree
Reading state information... Done
net-tools is already the newest version (1.60+git20161116.90da8a0-lubuntu1).
0 upgraded, 0 newly installed, 0 to remove and 359 not upgraded.
root@Route:/home/route#
```

- Cài đặt các interface nối với các network theo yêu cầu.



The screenshot shows a terminal window titled 'root@Route: /home/route'. The user has entered several commands to configure network interfaces. The output shows the configuration of 'enp0s9' and 'enp0s8' interfaces, including their IP addresses and network settings. The user has also added static connections for these interfaces using 'nmcli'.

```
route4 192.168.10.0/24
inet6 fe80::a00:27ff:fe2e:d11/64
route6 ff00::/8
route6 fe80::/64

enp0s9: connected to interface 3
"Intel 82540EM Gigabit Ethernet Controller (PRO/1000 MT Desktop Adapter)
ethernet (e1000), 08:00:27:B0:4A:B4, hw, mtu 1500
inet4 192.168.30.1/24
route4 192.168.30.0/24
inet6 fe80::a00:27ff:feb0:4ab4/64
route6 ff00::/8
route6 fe80::/64

enp0s8: unavailable
"Intel 82540EM Gigabit Ethernet Controller (PRO/1000 MT Desktop Adapter)
ethernet (e1000), 08:00:27:0E:ED:74, hw, mtu 1500

root@Route:/home/route#
root@Route:/home/route# nmcli con add type eth con-name 'static' ifname enp0s3 1
pv4.method manual ipv4.addresses 192.168.10.1/24
Connection 'static' (29ebb7d3-9ec8-469c-8295-fb520ba75277) successfully added.
root@Route:/home/route# nmcli con add type eth con-name 'static' ifname enp0s10
pv4.method manual ipv4.addresses 192.168.20.1/24
Warning: There is another connection with the name 'static'. Reference the connection by its uuid 'ba27afe6-90c5-4b33-ae2-7f1c1a7bcde'
Connection 'static' (ba27afe6-90c5-4b33-ae2-7f1c1a7bcde) successfully added.
root@Route:/home/route# nmcli con add type eth con-name 'static' ifname enp0s9 1
pv4.method manual ipv4.addresses 192.168.30.1/24
Warning: There are 2 other connections with the name 'static'. Reference the connection by its uuid '3e0bff0a-a72e-44ed-8948-ecf31ae78f5f'
Connection 'static' (3e0bff0a-a72e-44ed-8948-ecf31ae78f5f) successfully added.
root@Route:/home/route#
```

- Kết quả cấu hình ta có bản route và ip ở các interface như sau:

```

route@Route: ~
File Edit Tabs Help
Tras
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:2e:0d:11 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.1/24 brd 192.168.10.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe2e:d11/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOW
N group default qlen 1000
    link/ether 08:00:27:0e:ed:74 brd ff:ff:ff:ff:ff:ff
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:b0:4a:b4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.30.1/24 brd 192.168.30.255 scope global noprefixroute enp0s9
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feb0:4ab4/64 scope link
        valid_lft forever preferred_lft forever
5: enp0s10: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:18:52:db brd ff:ff:ff:ff:ff:ff
    inet 192.168.20.1/24 brd 192.168.20.255 scope global noprefixroute enp0s10
        valid_lft forever preferred_lft forever
    inet6 fe80::2e07:aaac:d963:13e5/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
route@Route:~$ route
Kernel IP routing table
Destination    Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.10.0    0.0.0.0         255.255.255.0   U        100    0      0 enp0s3
192.168.20.0    0.0.0.0         255.255.255.0   U        102    0      0 enp0s10
192.168.30.0    0.0.0.0         255.255.255.0   U        101    0      0 enp0s9
route@Route:~$
  
```

3 Thiết lập cho mỗi network một máy Linux với địa chỉ như sau:

- Client tại External network: 192.168.10.10/24 – Máy ảo EXT.

```

root@ext-virtual-machine: ~
altname enp2s1
inet 192.168.10.10/24 brd 192.168.10.255 scope global noprefixroute ens33
    valid_lft forever preferred_lft forever
inet6 fe80::ad4e:359d:b36f:9c9a/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
root@ext-virtual-machine:~# ip addr del 127.0.0.1/8 dev lo
root@ext-virtual-machine:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 192.168.10.100/24 scope global lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:bc:54:ab brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.10.10/24 brd 192.168.10.255 scope global noprefixroute ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::ad4e:359d:b36f:9c9a/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
root@ext-virtual-machine:~#
root@ext-virtual-machine:~#

```

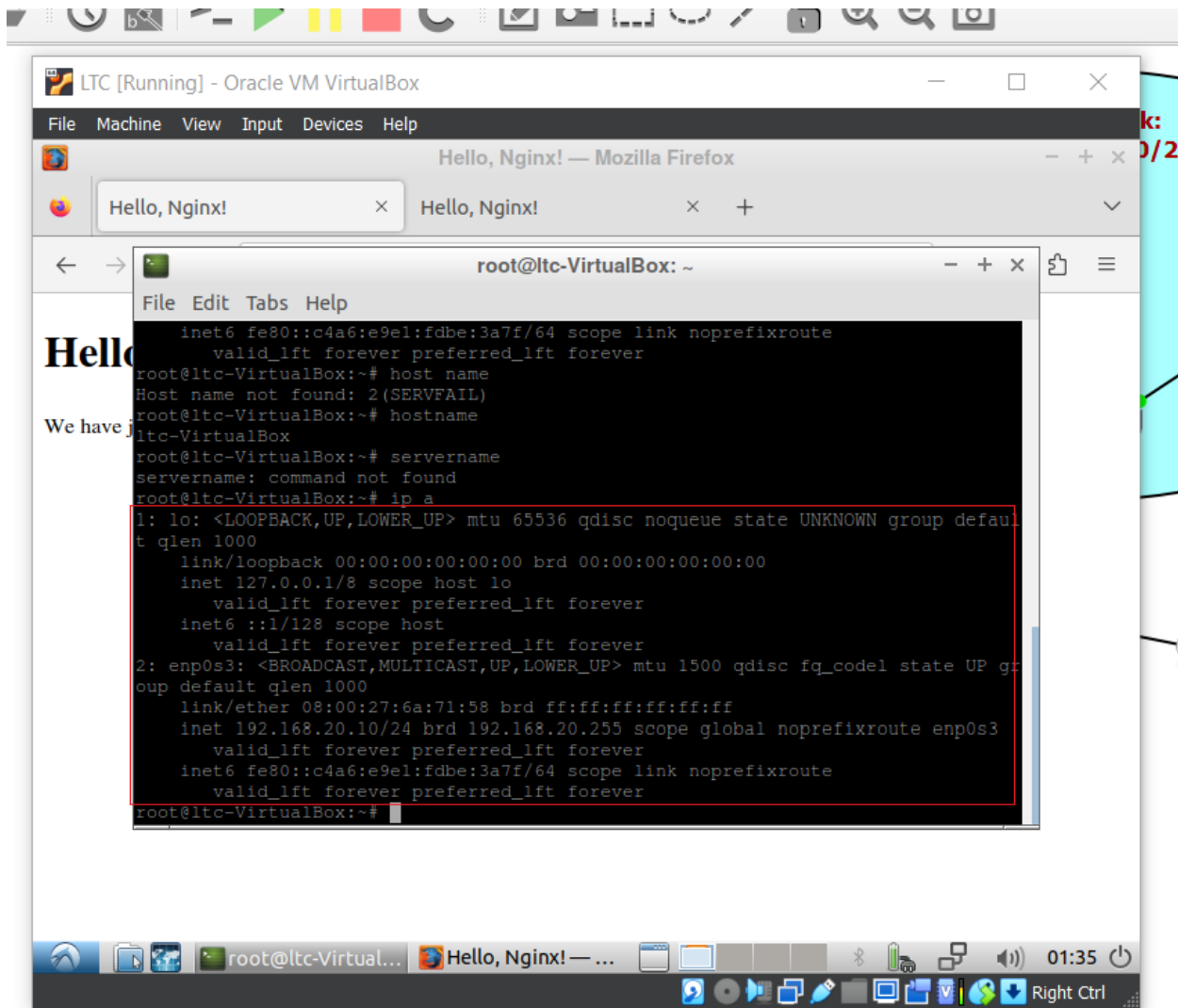
- Client tại Internal network: 192.168.30.10/24 – Máy ảo INT.

```

root@int-virtual-machine: /etc/netplan
altname enp2s1
inet 192.168.30.10/24 brd 192.168.30.255 scope global noprefixroute ens33
    valid_lft forever preferred_lft forever
inet6 fe80::f59c:1f65:b987:440c/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
root@int-virtual-machine:/etc/netplan# ip addr add 192.168.30.100/24 dev lo
root@int-virtual-machine:/etc/netplan# ip addr del 127.0.0.1/8 dev lo
root@int-virtual-machine:/etc/netplan# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 192.168.30.100/24 scope global lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:db:f6:4e brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.30.10/24 brd 192.168.30.255 scope global noprefixroute ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::f59c:1f65:b987:440c/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
root@int-virtual-machine:/etc/netplan#

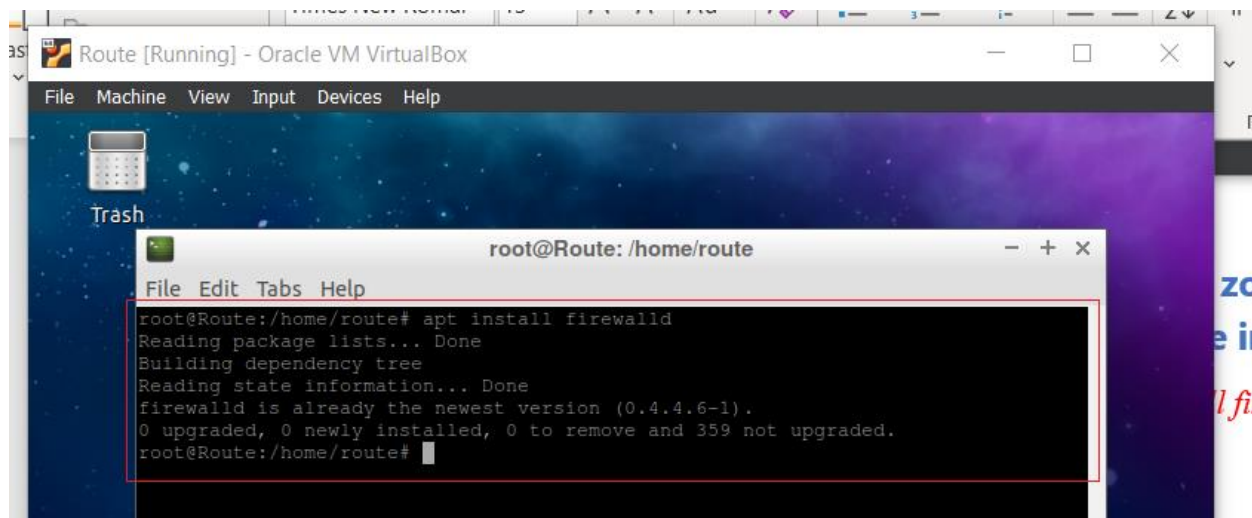
```

- Server tại DMZ network: 192.168.20.10/24 – Máy ảo LTC.



4 Thiết lập firewalld, zone external cho interface 1, zone dmz cho interface 2, zone internal cho interface 3.

- Cài đặt firewalld: *\$ sudo apt install firewalld*



```
Route [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Trash

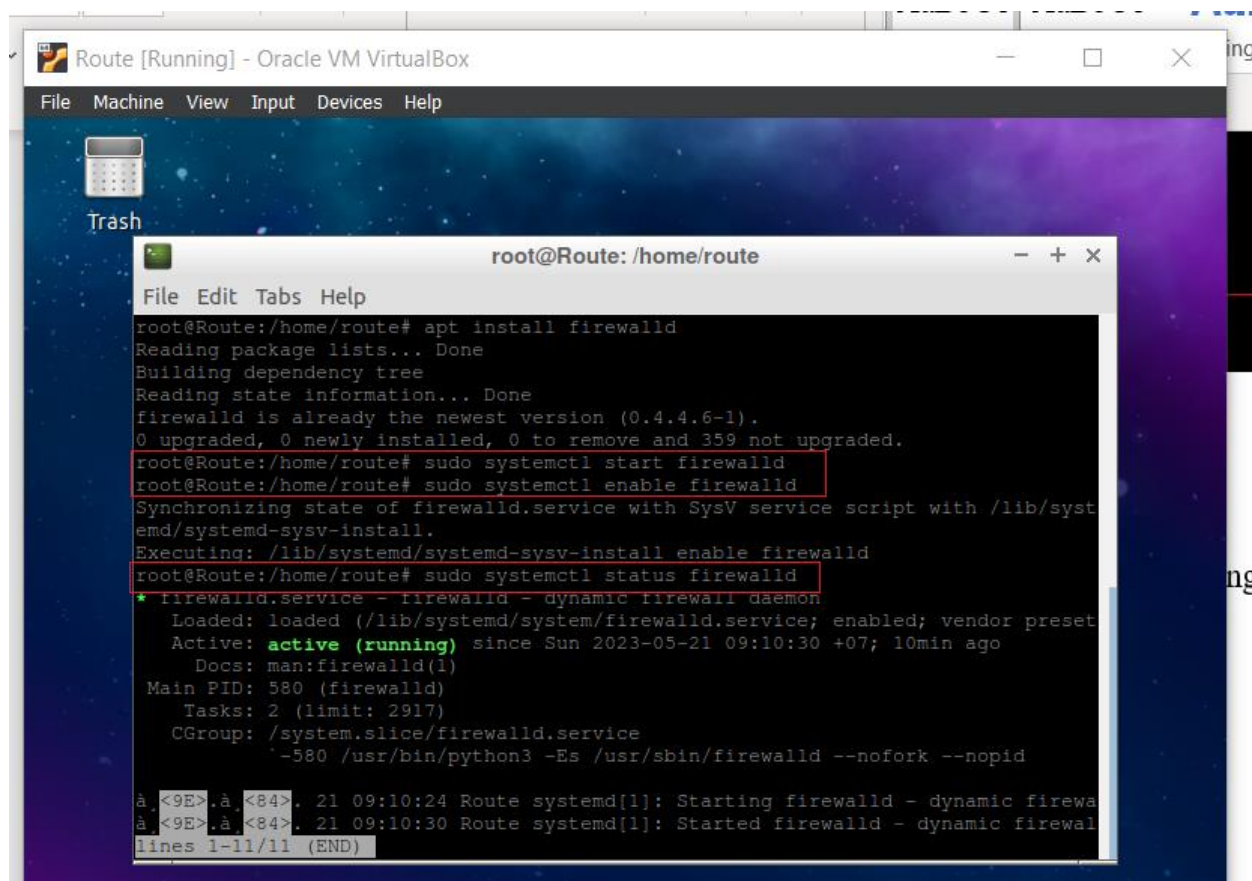
root@Route: /home/route
File Edit Tabs Help
root@Route:/home/route# apt install firewallld
Reading package lists... Done
Building dependency tree
Reading state information... Done
firewalld is already the newest version (0.4.4.6-1).
0 upgraded, 0 newly installed, 0 to remove and 359 not upgraded.
root@Route:/home/route#
```

- Khởi động firewalld:

\$ sudo systemctl start firewallld #Khởi động dịch vụ firewallld

\$ sudo systemctl enable firewallld #Bật firewallld khi boot hệ thống

\$ sudo systemctl status firewallld #Kiểm tra trạng thái firewallld



```
Route [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

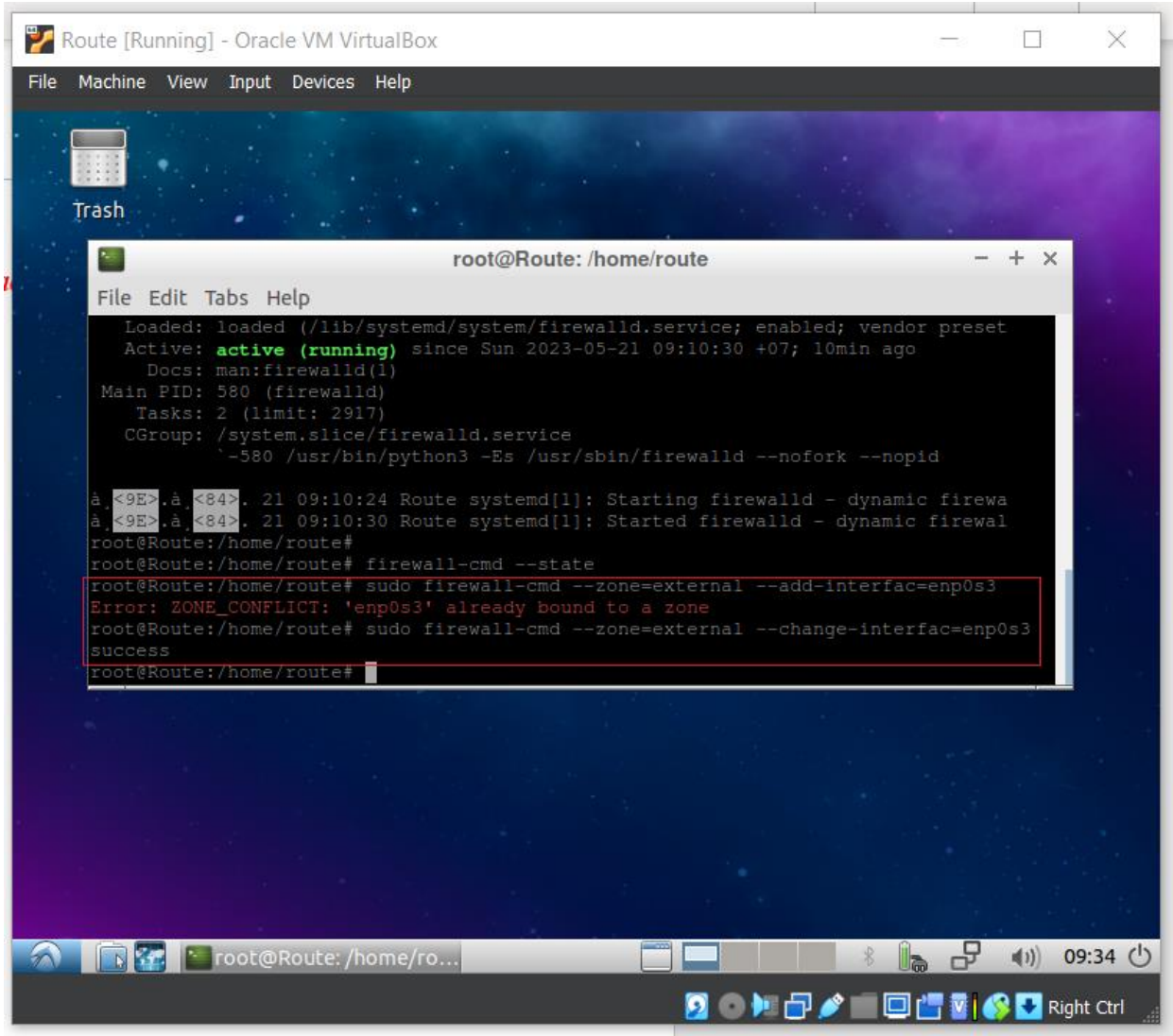
Trash

root@Route: /home/route
File Edit Tabs Help
root@Route:/home/route# apt install firewallld
Reading package lists... Done
Building dependency tree
Reading state information... Done
firewalld is already the newest version (0.4.4.6-1).
0 upgraded, 0 newly installed, 0 to remove and 359 not upgraded.
root@Route:/home/route# sudo systemctl start firewallld
root@Route:/home/route# sudo systemctl enable firewallld
Synchronizing state of firewallld.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable firewallld
root@Route:/home/route# sudo systemctl status firewallld
* firewallld.service - firewallld - dynamic firewall daemon
  Loaded: loaded (/lib/systemd/systemd-firewalld.service; enabled; vendor preset: enabled)
  Active: active (running) since Sun 2023-05-21 09:10:30 +07; 10min ago
    Docs: man:firewalld(1)
  Main PID: 580 (firewalld)
    Tasks: 2 (limit: 2917)
   CGroup: /system.slice/firewalld.service
           └─580 /usr/bin/python3 -Es /usr/sbin/firewalld --nofork --nopid

^[[9E]^[[84] 21 09:10:24 Route systemd[1]: Starting firewallld - dynamic firewallld
^[[9E]^[[84] 21 09:10:30 Route systemd[1]: Started firewallld - dynamic firewallld
lines 1-11/11 (END)
```

- Đặt Zone external cho interface 1(enp0s3):

\$ sudo firewall-cmd --zone=external --add-interface=enp0s3



Vì ở đây khi tạo interface, firewall tự tạo zone default cho interface nên khi ta tiến hành thêm zone khiến xung đột xảy ra.

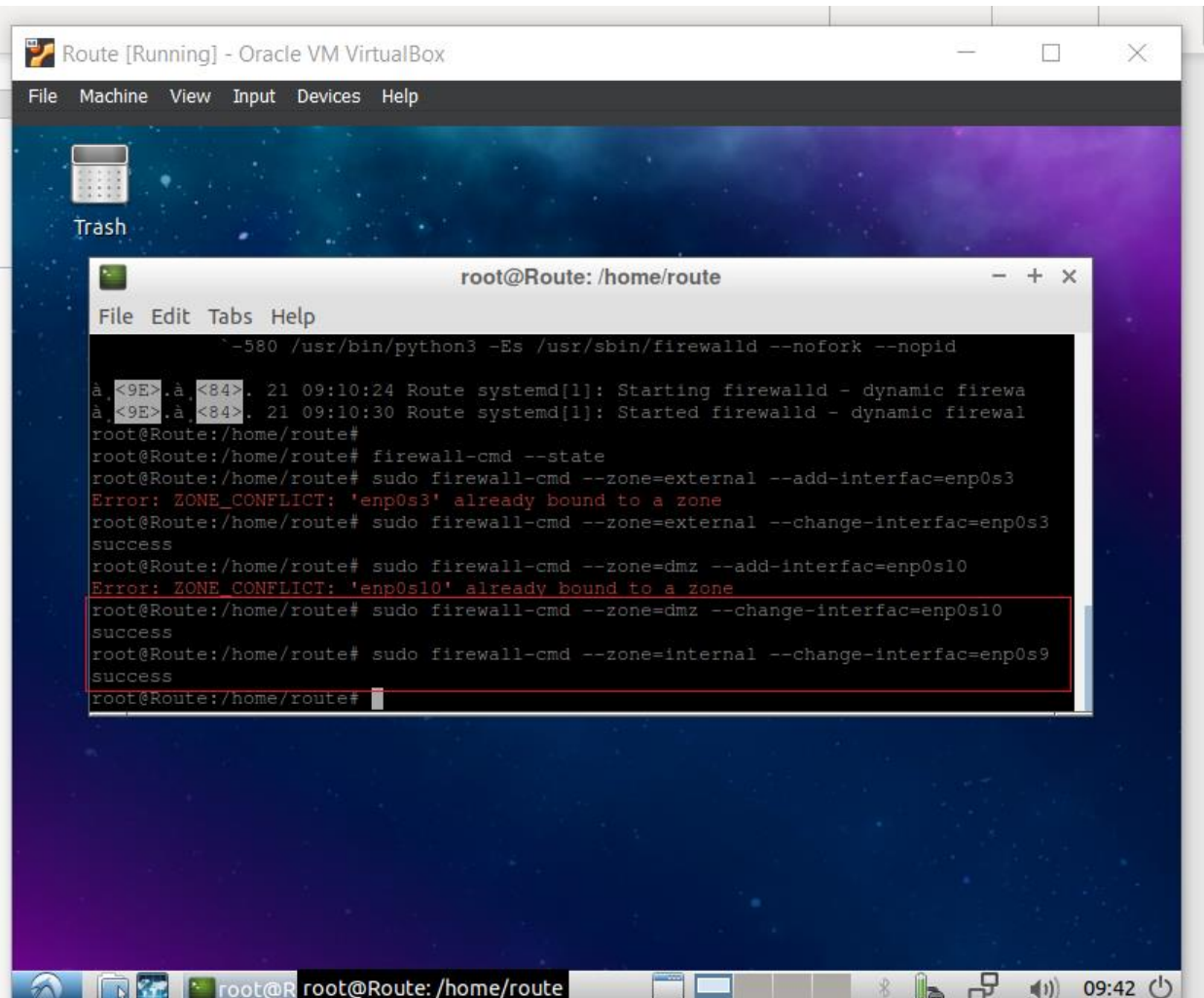
➔ Cách giải quyết là thay vì thêm chúng ta chuyển zone của interface về thành zone của chúng ta mong muốn. Câu lệnh sẽ là:

\$ sudo firewall-cmd --zone=external --change-interface=enp0s3

- Đặt Zone DMZ (interface 2 – enp0s10) và Zone internal (interface 3 – enp0s9) tương tự như trên các câu lệnh lần lượt sẽ là:

\$ sudo firewall-cmd --zone=dmz --change-interface=enp0s10

\$ sudo firewall-cmd --zone=internal --change-interface=enp0s9



```
Route [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Trash

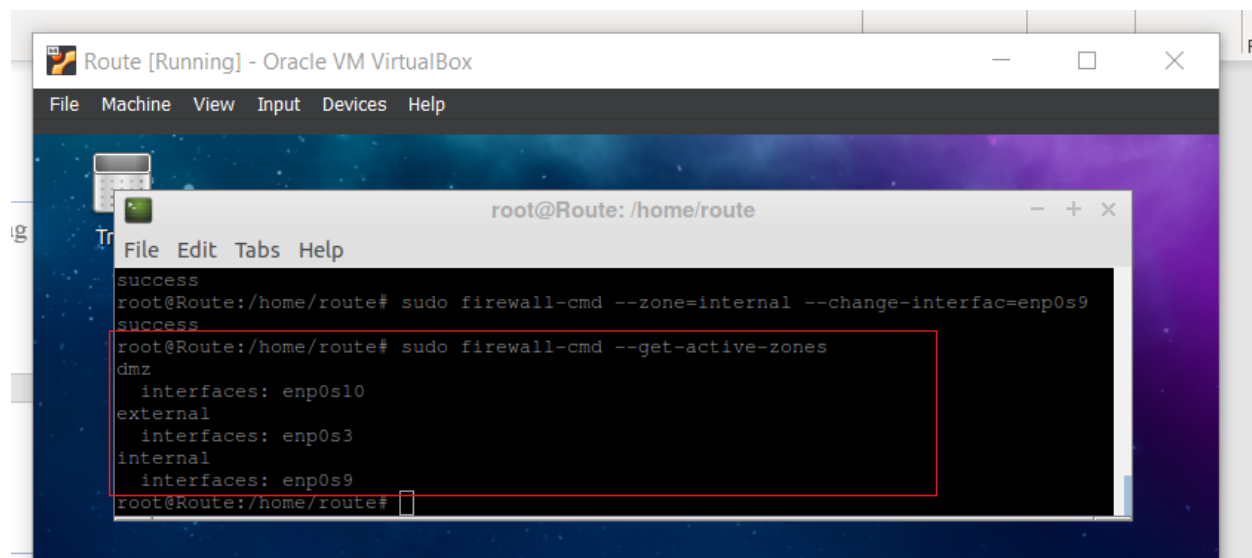
root@Route: /home/route
File Edit Tabs Help

-580 /usr/bin/python3 -Es /usr/sbin/firewalld --nofork --nopid

à <9E>.à.<84>. 21 09:10:24 Route systemd[1]: Starting firewalld - dynamic firewa
à <9E>.à.<84>. 21 09:10:30 Route systemd[1]: Started firewalld - dynamic firewal
root@Route:/home/route#
root@Route:/home/route# firewall-cmd --state
root@Route:/home/route# sudo firewall-cmd --zone=external --add-interfac=enp0s3
Error: ZONE_CONFLICT: 'enp0s3' already bound to a zone
root@Route:/home/route# sudo firewall-cmd --zone=external --change-interfac=enp0s3
success
root@Route:/home/route# sudo firewall-cmd --zone=dmz --add-interfac=enp0s10
Error: ZONE_CONFLICT: 'enp0s10' already bound to a zone
root@Route:/home/route# sudo firewall-cmd --zone=dmz --change-interfac=enp0s10
success
root@Route:/home/route# sudo firewall-cmd --zone=internal --change-interfac=enp0s9
success
root@Route:/home/route#
```

- Kết quả sau khi cấu hình:

\$ sudo firewall-cmd --get-active-zones



```
Route [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

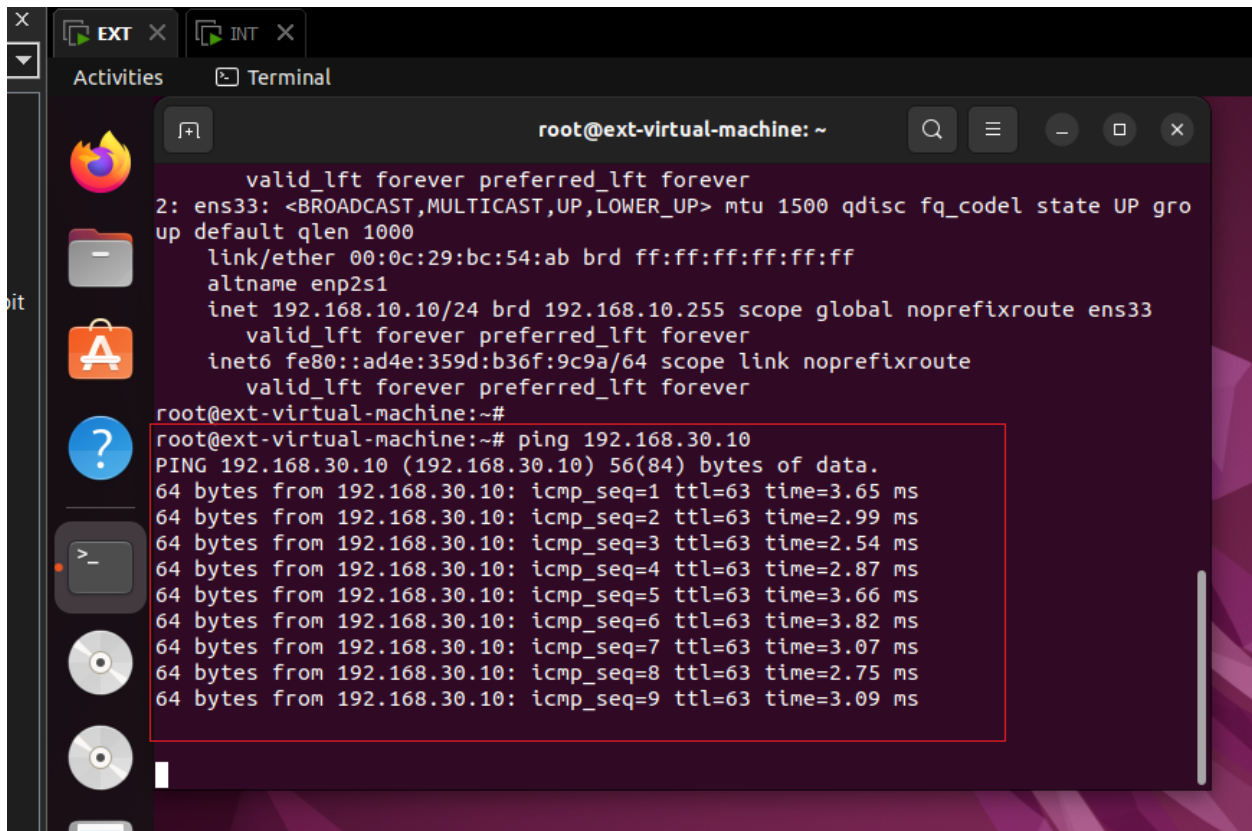
Trash

root@Route: /home/route
File Edit Tabs Help

success
root@Route:/home/route# sudo firewall-cmd --zone=internal --change-interfac=enp0s9
success
root@Route:/home/route# sudo firewall-cmd --get-active-zones
dmz
  interfaces: enp0s10
external
  interfaces: enp0s3
internal
  interfaces: enp0s9
root@Route:/home/route#
```

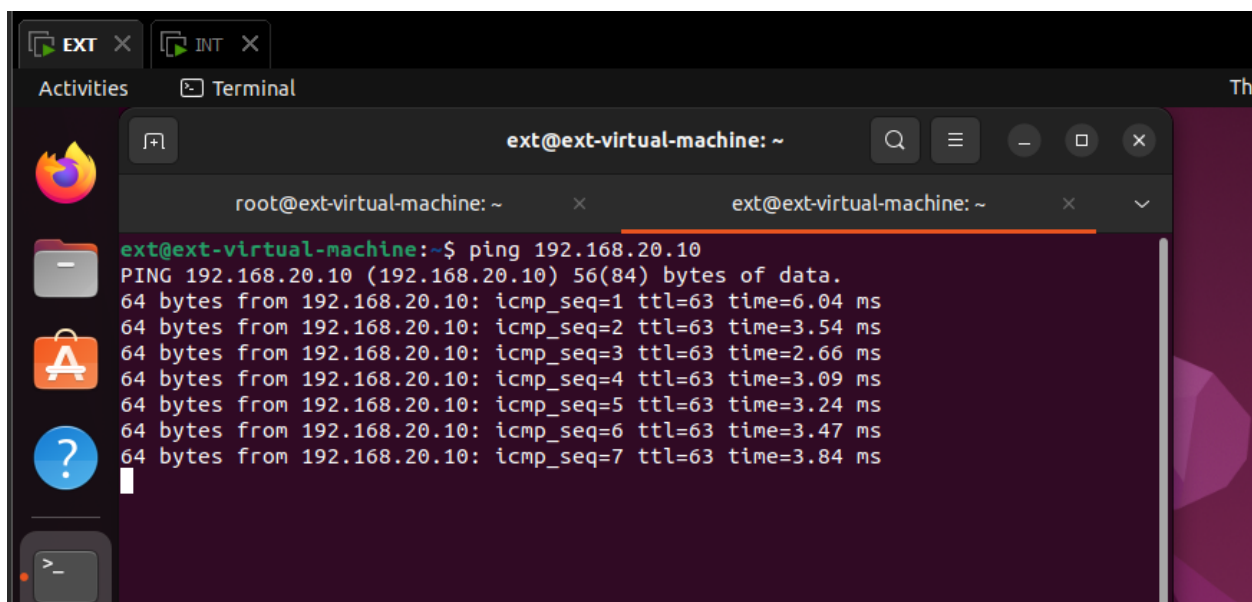
5 Kiểm tra kết nối giữa các máy tính (ping)

External network ping Internal network:



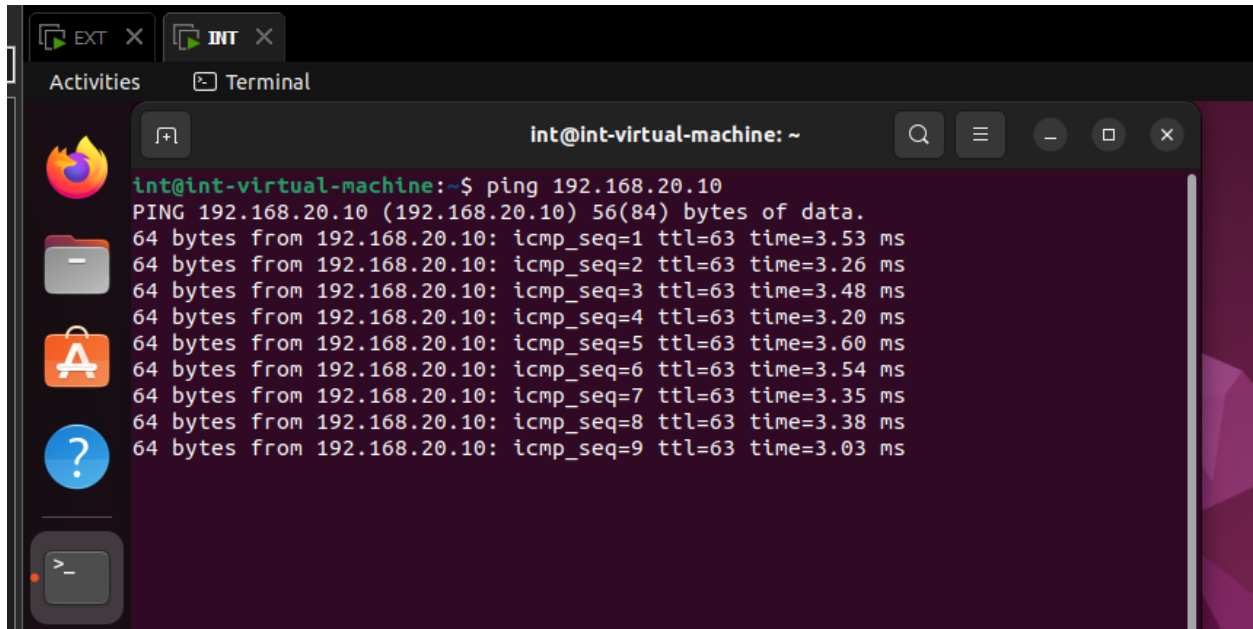
```
valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:bc:54:ab brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.10.10/24 brd 192.168.10.255 scope global noprefixroute ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::ad4e:359d:b36f:9c9a/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
root@ext-virtual-machine:~#
root@ext-virtual-machine:~# ping 192.168.30.10
PING 192.168.30.10 (192.168.30.10) 56(84) bytes of data.
64 bytes from 192.168.30.10: icmp_seq=1 ttl=63 time=3.65 ms
64 bytes from 192.168.30.10: icmp_seq=2 ttl=63 time=2.99 ms
64 bytes from 192.168.30.10: icmp_seq=3 ttl=63 time=2.54 ms
64 bytes from 192.168.30.10: icmp_seq=4 ttl=63 time=2.87 ms
64 bytes from 192.168.30.10: icmp_seq=5 ttl=63 time=3.66 ms
64 bytes from 192.168.30.10: icmp_seq=6 ttl=63 time=3.82 ms
64 bytes from 192.168.30.10: icmp_seq=7 ttl=63 time=3.07 ms
64 bytes from 192.168.30.10: icmp_seq=8 ttl=63 time=2.75 ms
64 bytes from 192.168.30.10: icmp_seq=9 ttl=63 time=3.09 ms
```

External network ping DMZ network:



```
ext@ext-virtual-machine:~$ ping 192.168.20.10
PING 192.168.20.10 (192.168.20.10) 56(84) bytes of data.
64 bytes from 192.168.20.10: icmp_seq=1 ttl=63 time=6.04 ms
64 bytes from 192.168.20.10: icmp_seq=2 ttl=63 time=3.54 ms
64 bytes from 192.168.20.10: icmp_seq=3 ttl=63 time=2.66 ms
64 bytes from 192.168.20.10: icmp_seq=4 ttl=63 time=3.09 ms
64 bytes from 192.168.20.10: icmp_seq=5 ttl=63 time=3.24 ms
64 bytes from 192.168.20.10: icmp_seq=6 ttl=63 time=3.47 ms
64 bytes from 192.168.20.10: icmp_seq=7 ttl=63 time=3.84 ms
```

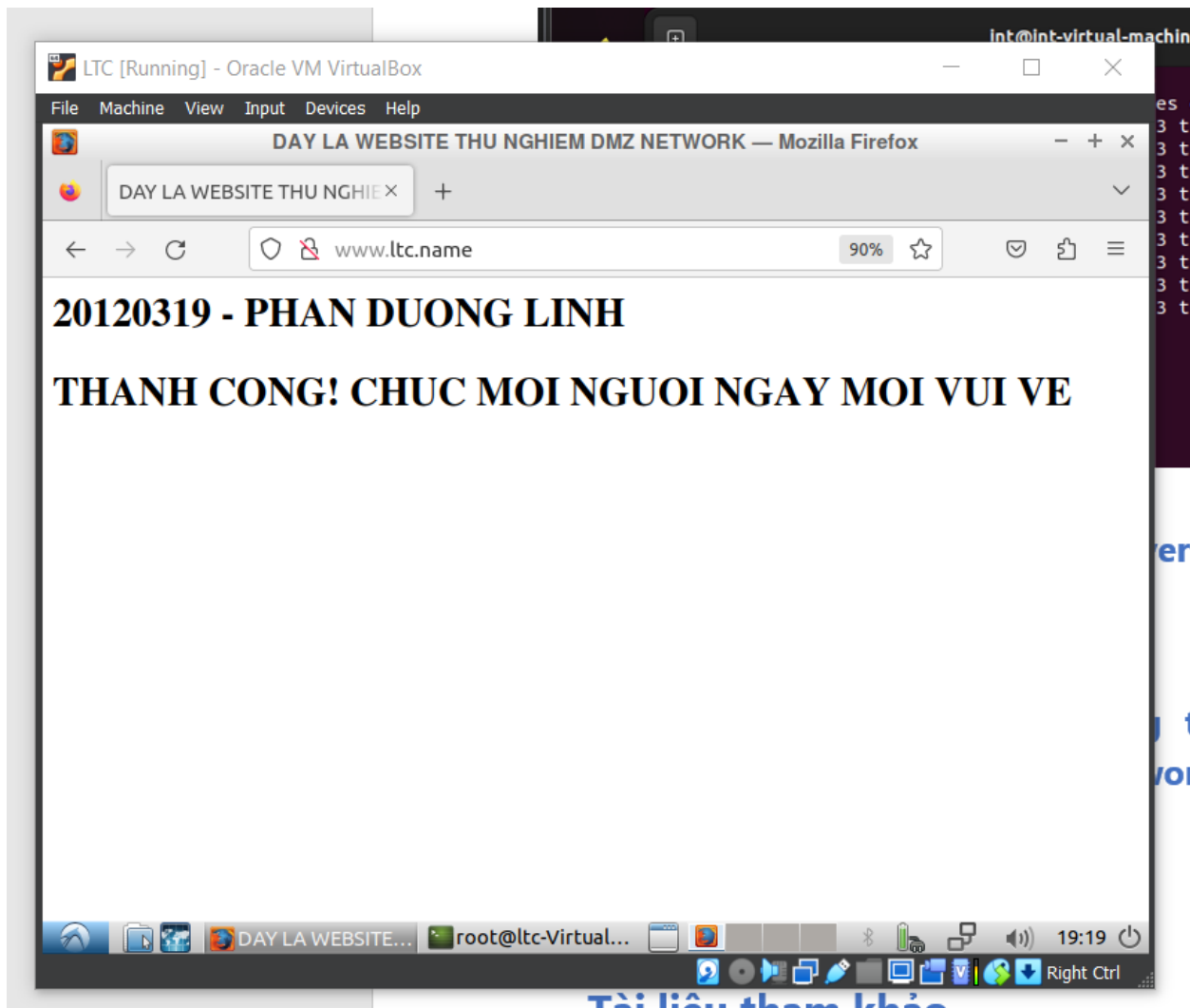

Internal network ping DMZ network:

A screenshot of a Linux terminal window. The window title is 'int@int-virtual-machine: ~'. The terminal shows the command 'ping 192.168.20.10' and its output. The output indicates that the ping is successful, showing 9 successful pings with varying times. The terminal window is part of a desktop environment with a sidebar on the left showing icons for Firefox, Files, and the App Store. The top of the window has tabs for 'EXT' and 'INT', and a search bar. The terminal output is as follows:

```
int@int-virtual-machine:~$ ping 192.168.20.10
PING 192.168.20.10 (192.168.20.10) 56(84) bytes of data.
64 bytes from 192.168.20.10: icmp_seq=1 ttl=63 time=3.53 ms
64 bytes from 192.168.20.10: icmp_seq=2 ttl=63 time=3.26 ms
64 bytes from 192.168.20.10: icmp_seq=3 ttl=63 time=3.48 ms
64 bytes from 192.168.20.10: icmp_seq=4 ttl=63 time=3.20 ms
64 bytes from 192.168.20.10: icmp_seq=5 ttl=63 time=3.60 ms
64 bytes from 192.168.20.10: icmp_seq=6 ttl=63 time=3.54 ms
64 bytes from 192.168.20.10: icmp_seq=7 ttl=63 time=3.35 ms
64 bytes from 192.168.20.10: icmp_seq=8 ttl=63 time=3.38 ms
64 bytes from 192.168.20.10: icmp_seq=9 ttl=63 time=3.03 ms
```

6 Cấu hình 1 Web server trên server thuộc DMZ network, chỉ cần phục vụ 1 website đơn giản.

Cấu hình Webserver thuộc DMZ network phục vụ website www.ltc.name đơn giản.



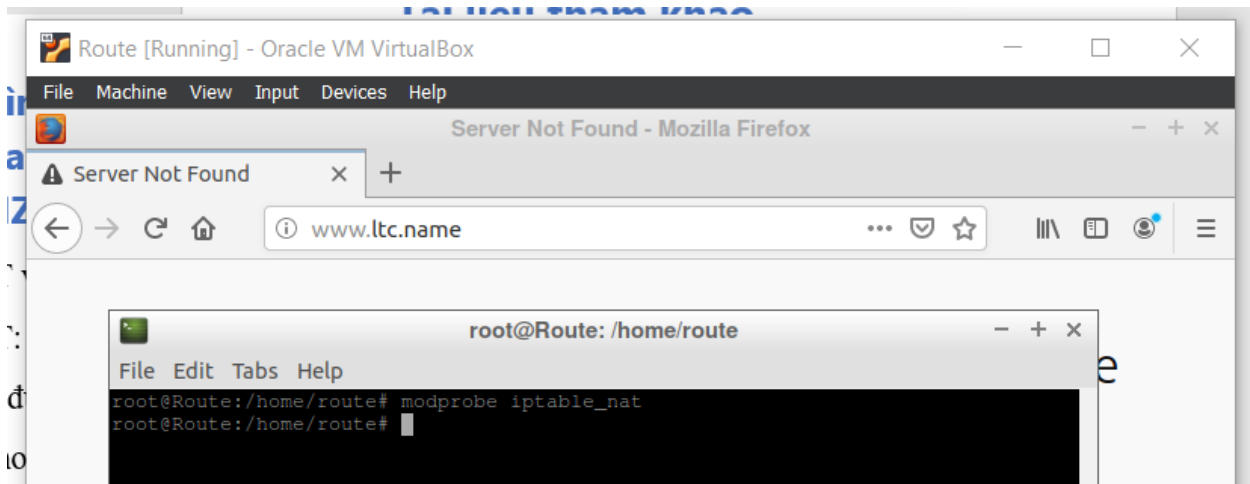
7 Cấu hình NAT, port forwarding trên router để client tại external network và internal network có thể truy cập website tại DMZ network.

a. Cấu hình NAT và port forwarding trên Router:

- Kích hoạt mô-đun

Tải mô-đun cho NAT bằng lệnh modprobe.

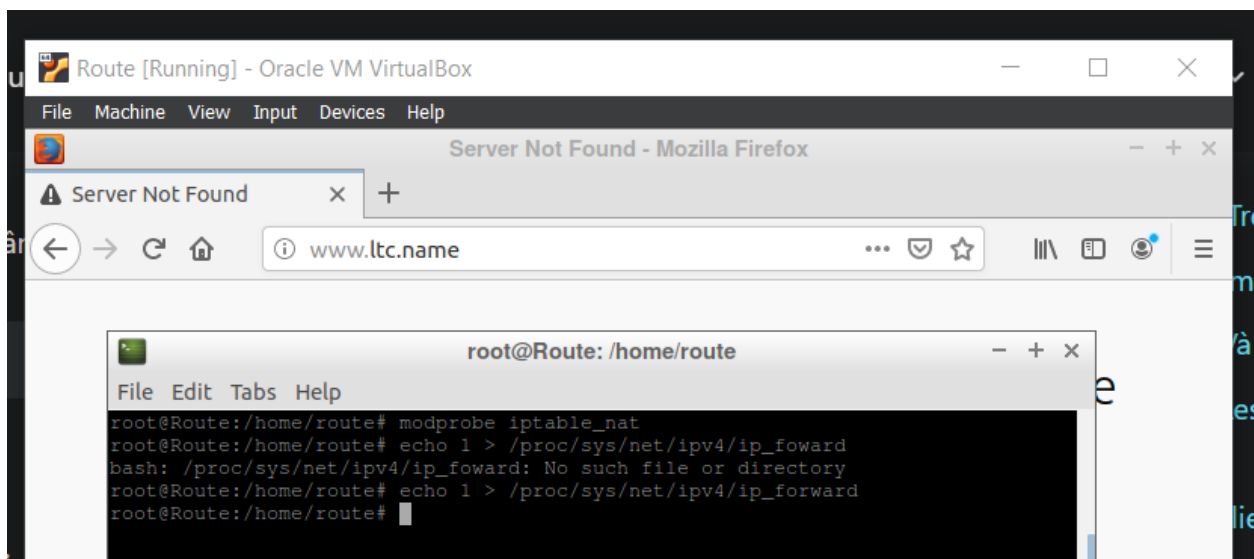
\$ sudo modprobe iptable_nat



- Chuyển tiếp lưu lượng tạm thời

Định cấu hình các tham số kernel trong thời gian chạy để chuyển tiếp lưu lượng truy cập Kích hoạt chuyển tiếp bằng cách thêm 1 vào hệ thống tệp tạm thời /proc Sau khi chúng tôi khởi động lại máy chủ, thay đổi này sẽ không khả dụng. Vì vậy, để các thay đổi được duy trì trong suốt quá trình khởi động lại, hãy đảm bảo sử dụng bước tiếp theo.

echo 1 > /proc/sys/net/ipv4/ip_forward



- Post routing và forwarding:

Thêm các quy tắc IPtables để thực hiện định tuyến post routing và forwarding lưu lượng truy cập.

iptables -t nat -A POSTROUTING -o enp0s10 -j MASQUERADE

```
# iptables -A FORWARD -i enp0s3 -j ACCEPT
```

```
# iptables -A FORWARD -i enp0s9 -j ACCEPT
```

```

Route [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

root@Route: /home/route
File Edit Tabs Help

root@Route:/home/route# iptables -t nat -A POSTROUTING -o enp0s10 -j MASQUERADE
root@Route:/home/route# iptables -A FORWARD -i enp0s3 -j ACCEPT
root@Route:/home/route# iptables -A FORWARD -i enp0s9 -j ACCEPT
root@Route:/home/route#
  
```

– Trên giao thức TCP/UDP:

```

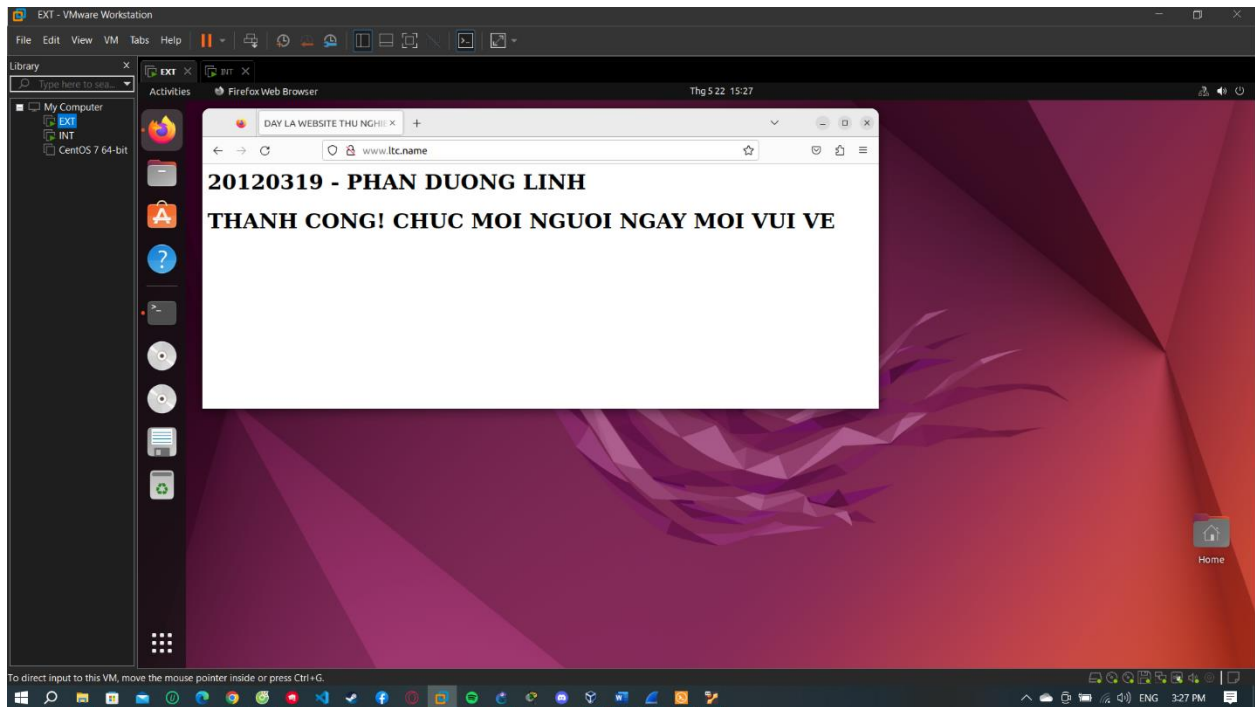
Route [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

root@Route: /home/route
File Edit Tabs Help

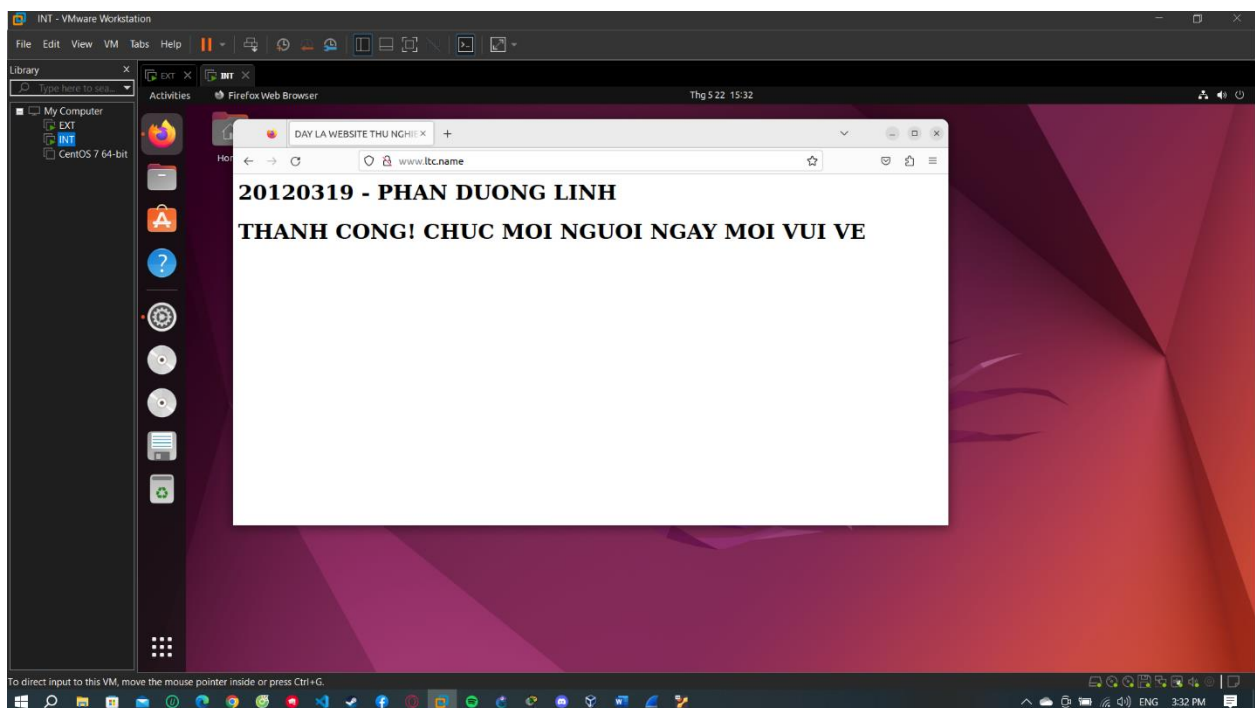
Error: INVALID_PROTOCOL: 'http' not in ('tcp','udp','sctp','dccp')
root@Route:/home/route# firewall-cmd --permanent --add-port=80/tcp
success
root@Route:/home/route# firewall-cmd --reload
success
root@Route:/home/route# firewall-cmd --permanent --add-port=443/tcp
success
root@Route:/home/route# firewall-cmd --reload
success
root@Route:/home/route# iptables -A FORWARD -s 0/0 -i enp0s3 -d 192.168.20.1 -o
enp0s10 -p TCP --sport 1024:65535 -m multiport --dports 80,443 -j ACCEPT
Bad argument `--sport'
Try `iptables -h' or 'iptables --help' for more information.
root@Route:/home/route# iptables -A FORWARD -s 0/0 -i enp0s3 -d 192.168.20.1 -o
enp0s10 -p TCP --sport 1024:65535 -m multiport --dports 80,443 -j ACCEPT
root@Route:/home/route# iptables -A FORWARD -s 0/0 -i enp0s3 -d 192.168.20.1 -o
enp0s10 -p TCP --sport 1024:65535 -m multiport --dports 80,443 -j ACCEPT
root@Route:/home/route# iptables -A FORWARD -d 0/0 -i enp0s3 -s 192.168.20.1 -o
enp0s10 -p TCP -m state --state ESTABLISHED -j ACCEPT
iptables v1.6.1: Bad state "ESTABLISHED"
Try `iptables -h' or 'iptables --help' for more information.
root@Route:/home/route# iptables -A FORWARD -d 0/0 -i enp0s3 -s 192.168.20.1 -o
enp0s10 -p TCP -m state --state ESTABLISHED -j ACCEPT
root@Route:/home/route#
  
```

Cấu hình tương tự với interface enp0s9 của internal network.

b. Tiến hành cho client tại external truy cập website:



c. Tiến hành cho client tại internal truy cập website:



Tài liệu tham khảo

➤ Tài liệu môn học:

- [1] 09_iptables.pdf – Lê Hà Minh
- [2] 09_firewalld.pdf – Lê Hà Minh

➤ Tài liệu trực tuyến:

- [1] [Setup a Linux server as a NAT router to share the Internet | 1 Easy guide – by Babin Lonston – linuxsysadmins.com](#)
- [2] [Linux NAT\(Network Address Translation\) Router Explained – by Sarath Pillai - slashroot.in](#)
- [3] [How To Set Up a Firewall Using Iptables on Ubuntu 14.04 – by Justin Ellingwood - digitalocean.com](#)