Công ty TNHH TMDV Giải Pháp Việt
Khóa thực tập : NS014
Mentor : Võ Đại Vương
Thực tập sinh : Hồ Hải Dương

BÁO CÁO KẾT QUẢ BÀI TẬP TUẦN 2

MỤC LỤC

BÀI LÀM

Phần 1

1.1. Yêu cầu

- Nâng cấu hình 2 VM: CPU: 1 core, RAM: 1GB, Disk: 20GB
- VM1: 2 card mạng (vmbr0 - WAN, vmbr1 - LAN)
  WAN: sử dụng IP tuần 1
  LAN: 10.0.x.1/24
- VM2: 1 card mạng (vmbr1)
  LAN: 10.0.x.2/24, GW: 10.0.x.1
- Thiết lập địa chỉ IP tĩnh và thông tin user qua Cloud-Init
- Cấu hình iptables trên VM1 để NAT (MASQUERADE) cho phép VM2 ra Internet
- Reboot VM1, bảo đảm NAT vẫn hoạt động

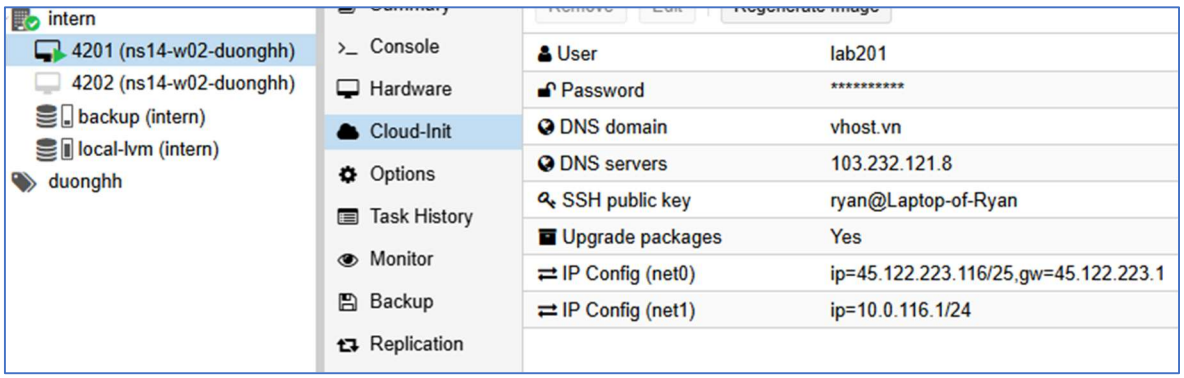
1.2. Các bước thực hiện

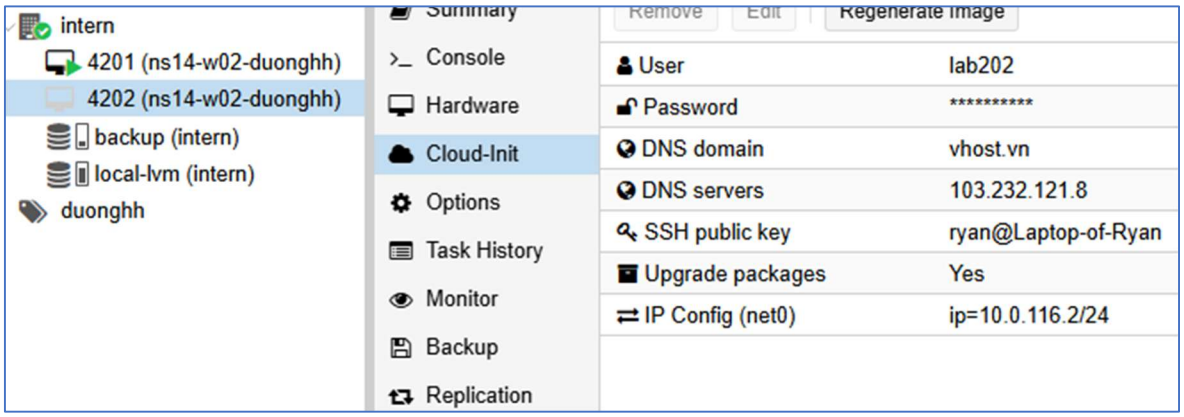
- Thiết lập IP tĩnh cho hai VM trong Cloud-Init
- Bật IP forwarding trên VM1 bằng cách chỉnh sửa /etc/sysctl.conf
- Cấu hình iptables trên VM1:
  sudo iptables -t nat -A POSTROUTING -s 10.0.116.0/24 -o eth0 -j MASQUERADE
  sudo iptables -A FORWARD -s 10.0.116.0/24 -j ACCEPT
  sudo iptables -A FORWARD -d 10.0.116.0/24 -j ACCEPT
- Cấu hình lưu iptables qua file /etc/rc.local để tự động chạy khi reboot

1.3. Kết quả

- VM2 truy cập Internet thông qua NAT thành công
- Sau reboot, NAT vẫn hoạt động ổn định

1.4. Hình ảnh demo






```
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
#  Enabling this option disables Stateless Address Autoconfigurat
#  based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1
```

```
lab202@ns14-w02-duonghh:~$ ip route
default via 10.0.116.1 dev eth0 proto static
10.0.116.0/24 dev eth0 proto kernel scope link src 10.0.116.2
lab202@ns14-w02-duonghh:~$
lab202@ns14-w02-duonghh:~$
lab202@ns14-w02-duonghh:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=39.5 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=38.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=38.9 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=39.0 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=118 time=39.0 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=118 time=39.0 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=118 time=40.2 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=118 time=39.9 ms
^C
--- 8.8.8.8 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7011ms
rtt min/avg/max/mdev = 38.915/39.312/40.186/0.472 ms
```

```
#!/bin/sh -e
iptables-restore < /etc/iptables.rule
exit 0
```

```
root@ns14-w02-duonghh:/home/lab201# ls -l /etc/rc.local
-rw-r--r-- 1 root root 58 Apr 21 06:26 /etc/rc.local
```

```
root@ns14-w02-duonghh:/home/lab201# sudo nano /etc/systemd/system/rc-local.servi
ce
```

```
[Unit]
Description=/etc/rc.local Compatibility
ConditionPathExists=/etc/rc.local

[Service]
Type=forking
ExecStart=/etc/rc.local start
TimeoutSec=0
RemainAfterExit=yes
GuessMainPID=no

[Install]
WantedBy=multi-user.target
```

```
lab201@ns14-w02-duonghh:~$ ip route
default via 45.122.223.1 dev eth0 proto static
10.0.116.0/24 dev eth1 proto kernel scope link src 10.0.116.1
45.122.223.0/24 dev eth0 proto kernel scope link src 45.122.223.116
```

```
lab202@ns14-w02-duonghh:~$ ip route
default via 10.0.116.1 dev eth0 proto static
10.0.116.0/24 dev eth0 proto kernel scope link src 10.0.116.2
lab202@ns14-w02-duonghh:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=40.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=39.0 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=39.0 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=38.9 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 38.861/39.222/40.086/0.501 ms
```

Phần 2

2.1. Yêu cầu

Cấu hình chức năng Port Forwarding trên máy Gateway (VM1):

- Nguồn: VM1 (qua IP WAN 45.122.223.116, cổng 2223)
- Đích: VM2 (10.0.116.2, cổng 22)
- Mục tiêu: Cho phép kết nối SSH từ bên ngoài vào VM2 thông qua Gateway

2.2. Các bước thực hiện

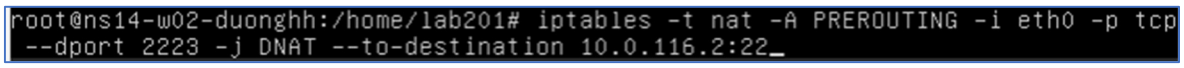
- SSH vào máy VM1 với quyền root
- Thêm rules NAT để chuyển tiếp port:
  sudo iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 2223 -j DNAT --to-destination 10.0.116.2:22

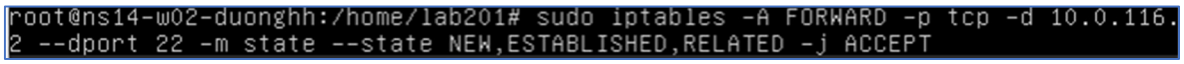
- Thêm rules FORWARD để cho phép lưu lượng đi qua:
  sudo iptables -A FORWARD -p tcp -d 10.0.116.2 --dport 22 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
- Kiểm tra các rules iptables đã được áp dụng:
  sudo iptables -t nat -L -n -v
  sudo iptables -L FORWARD -n -v
- Từ máy tính bên ngoài, thực hiện kết nối:
  ssh -p 2223 lab202@45.122.223.116

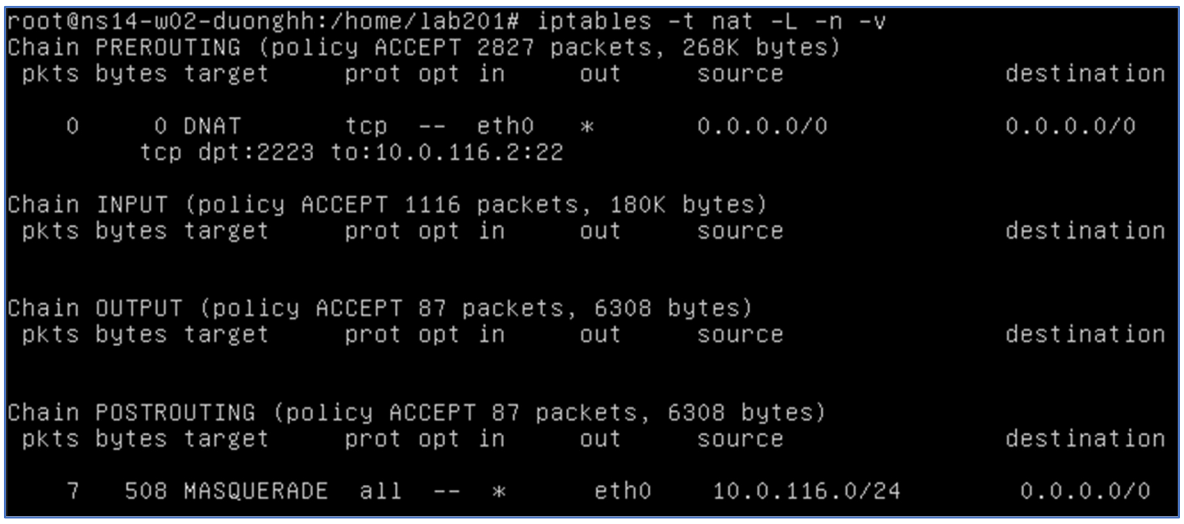
2.3. Kết quả

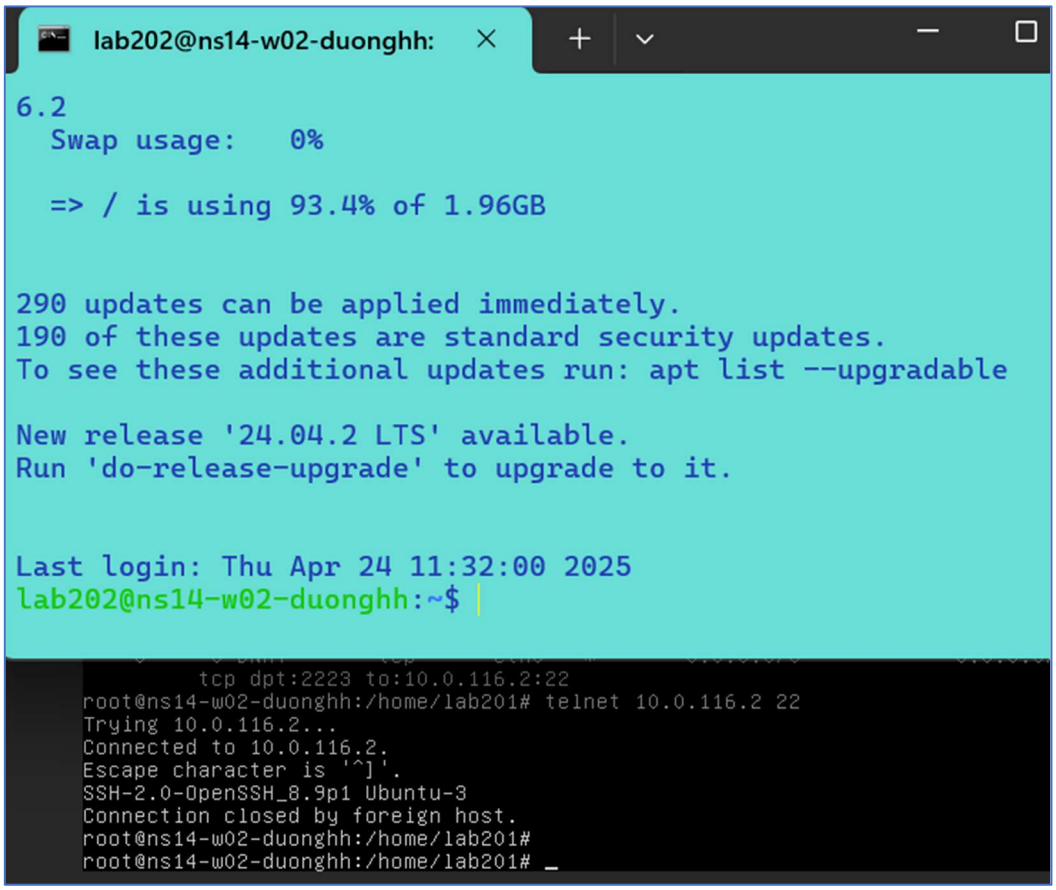
- Các rules NAT và FORWARD hoạt động chính xác.
- Có thể SSH từ ngoài vào máy VM2 qua IP WAN và cổng 2223.
- Cấu hình đúng yêu cầu và bảo đảm bảo mật khi truy cập từ xa.

2.4. Hình ảnh demo









Phần 3

3.1. Yêu cầu

- Cấu hình máy VM Gateway có thể NAT giữa 2 dải mạng LAN:
  LAN1: 10.0.116.0/24
  LAN2: 10.0.118.0/24
- Các máy trong LAN1 có thể ping và kết nối được tới các máy trong LAN2.
- Áp dụng quy tắc NAT để định tuyến đúng luồng dữ liệu giữa 2 mạng nội bộ thông qua máy Gateway trung gian.

3.2. Các bước thực hiện

- Cấu hình chính sách Forward giữa 2 mạng LAN:
  sudo iptables -A FORWARD -s 10.0.116.0/24 -d 10.0.118.0/24 -j ACCEPT
  sudo iptables -A FORWARD -s 10.0.118.0/24 -d 10.0.116.0/24 -j ACCEPT
- Cấu hình NAT để chuyển đổi gói tin giữa hai dải mạng:
  sudo iptables -t nat -A POSTROUTING -s 10.0.116.0/24 -d 10.0.118.0/24 -j MASQUERADE
- Kiểm tra khả năng giao tiếp giữa 2 mạng LAN bằng lệnh ping từ các máy trong mỗi mạng.

- Kiểm tra lại bằng iptables -t nat -L -n -v và ip route để bảo đảm các rules được áp dụng đúng và bảng định tuyến hợp lý.

3.3. Kết quả

- Các máy trong mạng LAN 10.0.116.0/24 đã có thể ping và truy cập thành công đến các máy trong mạng 10.0.118.0/24 thông qua máy Gateway.
- Các rules NAT và FORWARD hoạt động ổn định giúp bảo đảm kết nối thông suốt giữa 2 dải mạng LAN.

3.4. Hình ảnh demo

```
lab202@ns14-w02-duonghh:~$ ping 45.122.223.118
PING 45.122.223.118 (45.122.223.118) 56(84) bytes of data.
64 bytes from 45.122.223.118: icmp_seq=1 ttl=63 time=2.25 ms
64 bytes from 45.122.223.118: icmp_seq=2 ttl=63 time=1.31 ms
64 bytes from 45.122.223.118: icmp_seq=3 ttl=63 time=1.33 ms
64 bytes from 45.122.223.118: icmp_seq=4 ttl=63 time=1.11 ms
^C
--- 45.122.223.118 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.112/1.498/2.246/0.439 ms
lab202@ns14-w02-duonghh:~$ ping 10.0.118.2
PING 10.0.118.2 (10.0.118.2) 56(84) bytes of data.
64 bytes from 10.0.118.2: icmp_seq=1 ttl=64 time=0.776 ms
64 bytes from 10.0.118.2: icmp_seq=2 ttl=64 time=0.716 ms
64 bytes from 10.0.118.2: icmp_seq=3 ttl=64 time=0.650 ms
^C
--- 10.0.118.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.650/0.714/0.776/0.051 ms
```

```
10.0.118.0/24 dev eth0 proto kernel scope link src 10.0.118.2
10.0.121.0/24 via 10.0.118.1 dev eth0
root@ns14-w02-khangvm:/home/khangvm# ping 10.0.116.2
PING 10.0.116.2 (10.0.116.2) 56(84) bytes of data.
64 bytes from 10.0.116.2: icmp_seq=1 ttl=64 time=0.653 ms
64 bytes from 10.0.116.2: icmp_seq=2 ttl=64 time=0.736 ms
64 bytes from 10.0.116.2: icmp_seq=3 ttl=64 time=0.650 ms
64 bytes from 10.0.116.2: icmp_seq=4 ttl=64 time=0.805 ms
64 bytes from 10.0.116.2: icmp_seq=5 ttl=64 time=0.757 ms
64 bytes from 10.0.116.2: icmp_seq=6 ttl=64 time=0.631 ms
64 bytes from 10.0.116.2: icmp_seq=7 ttl=64 time=0.689 ms
64 bytes from 10.0.116.2: icmp_seq=8 ttl=64 time=0.676 ms
```

Cấu hình SSH

VM1:

```
root@ns14-w02-duonghh:/home/lab201# grep -Ei 'port|passwordauthentication|pubkey
authentication|permitrootlogin' /etc/ssh/sshd_config | grep -v '^#'
Port 5000
PermitRootLogin prohibit-password
PubkeyAuthentication yes
PasswordAuthentication no
```

VM2:

```
lab202@ns14-w02-duonghh:~$ sudo grep -Ei 'port|passwordauthentication|pubkeyauth
entication|permitrootlogin' /etc/ssh/sshd_config | grep -v '^#'
Port 2222
PermitRootLogin prohibit-password
PubkeyAuthentication yes
PasswordAuthentication no
```

HẾT./.