

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

Phần 1 1

1.1. Yêu cầu 1

1.2. Các bước thực hiện 1

1.3. Kết quả 1

1.4. Hình ảnh demo 1

Phần 2 3

2.1. Yêu cầu 3

2.2. Các bước thực hiện 3

2.3. Kết quả 4

2.4. Hình ảnh demo 4

Phần 3 5

3.1. Yêu cầu 5

3.2. Các bước thực hiện 5

3.3. Kết quả 6

3.4. Hình ảnh demo 6

Cấu hình SSH 6

BÀI LÀM

Phần 1

1.1. Yêu cầu

- Nâng cấp 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

intern	Summary	Remove	Edit	Regenerate image
4201 (ns14-w02-duonghh)	> Console			
4202 (ns14-w02-duonghh)	Hardware			
backup (intern)	Cloud-Init			
local-lvm (intern)	Options			
duonghh	Task History			
	Monitor			
	Backup			
	Replication			
		User	lab201	
		Password	*****	
		DNS domain	vhost.vn	
		DNS servers	103.232.121.8	
		SSH public key	ryan@Laptop-of-Ryan	
		Upgrade packages	Yes	
		IP Config (net0)	ip=45.122.223.116/25,gw=45.122.223.1	
		IP Config (net1)	ip=10.0.116.1/24	

intern

4201 (ns14-w02-duonghh)

4202 (ns14-w02-duonghh)

backup (intern)

local-lvm (intern)

duonghh

Summary

> Console

Hardware

Cloud-Init

Options

Task History

Monitor

Backup

Replication

Remove

Edit

Regenerate image

User	lab202
Password	*****
DNS domain	vhost.vn
DNS servers	103.232.121.8
SSH public key	ryan@Laptop-of-Ryan
Upgrade packages	Yes
IP Config (net0)	ip=10.0.116.2/24

```
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
et.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 Autoconfiguration
# 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.rules
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.service
```

```
[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
lab201@ns14-w02-duonghh:~$
```

```
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

```
root@ns14-w02-duonghh:/home/lab201# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 2223 -j DNAT --to-destination 10.0.116.2:22_
```

```
root@ns14-w02-duonghh:/home/lab201# sudo iptables -A FORWARD -p tcp -d 10.0.116.2 --dport 22 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
```

```
root@ns14-w02-duonghh:/home/lab201# iptables -t nat -L -n -v
Chain PREROUTING (policy ACCEPT 2827 packets, 268K bytes)
 pkts bytes target    prot opt in     out     source    destination
      0      0 DNAT      tcp  --  eth0   *      0.0.0.0/0 0.0.0.0/0
      0      0 tcp dpt:2223 to:10.0.116.2:22

Chain INPUT (policy ACCEPT 1116 packets, 180K bytes)
 pkts bytes target    prot opt in     out     source    destination

Chain OUTPUT (policy ACCEPT 87 packets, 6308 bytes)
 pkts bytes target    prot opt in     out     source    destination

Chain POSTROUTING (policy ACCEPT 87 packets, 6308 bytes)
 pkts bytes target    prot opt in     out     source    destination
      7    508 MASQUERADE all  --  *      eth0    10.0.116.0/24 0.0.0.0/0
```

```
lab202@ns14-w02-duonghh: × + - □
6.2
Swap usage: 0%

=> / is using 93.4% of 1.96GB

290 updates can be applied immediately.
190 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

New release '24.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Thu Apr 24 11:32:00 2025
lab202@ns14-w02-duonghh:~$ |
tcp dpt:2223 to:10.0.116.2:22
root@ns14-w02-duonghh:/home/lab201# telnet 10.0.116.2 22
Trying 10.0.116.2...
Connected to 10.0.116.2.
Escape character is '^]'.
SSH-2.0-OpenSSH_8.9p1 Ubuntu-3
Connection closed by foreign host.
root@ns14-w02-duonghh:/home/lab201#
root@ns14-w02-duonghh:/home/lab201# _
```

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./