

lab2 : Nắm vững kĩ thuật nat, port forwarding & routing



Lầu 2, 46 Cửu Long, Phường 2, Quận Tân Bình, Thành phố Hồ Chí Minh

Thực tập sinh : Nguyễn Trần Nhân Khoa

Week 2: Nắm vững kỹ thuật NAT, Port Forwarding & Routing.

Phần 1: NAT.

Mỗi bạn tạo 2 VM:

**VM1**: 1/1/20/vmbr0/vmbr1

* IP WAN: liên hệ leader để được cấp IP
* IP LAN: 10.0.22.1/24

**VM2**: 1/1/20/vmbr1

* IP LAN: 10.0.22.2/24 - GW: 10.0.22.1

**Yêu cầu**:

* Sử dụng iptables cấu hình VM1 NAT masquerade để VM2 có thể đi ra internet được thông qua VM1.
* Reboot VM1 và sau khi boot vào OS thì VM2 vẫn có thể đi ra internet được thông qua VM1.

Phần 2: Port Forwarding.

**Yêu cầu**:

* Cấu hình port forwarding trên VM1 để khi SSH vào IP WAN của VM1 port 2222 thì có thể truy cập được SSH được thẳng vào VM2.

Phần 3: Routing.

**Môi trường**: đề tài yêu cầu 2 bạn làm chung 1 bài lab. Mỗi bạn được cấp 2 VM và cấu hình mạng như hình sau:

* Bạn 1: VM2 (có vmbr0 và vmbr1) và VM1 (only vmbr1)
* Bạn 2: VM3 (có vmbr0 và vmbr1) và VM4 (only vmbr1)

Mục lục

[Câu 1 3](#_Toc191069090)

[ Cấu hình máy 3](#_Toc191069091)

[ Ping kết nối máy VM1 và VM2 4](#_Toc191069092)

[ Bật chuyển tiếp gói IPv4 ở VM1: 5](#_Toc191069093)

[ Thiết lập NAT với iptables ở VM1: 5](#_Toc191069094)

[ Lưu cấu hình iptables 6](#_Toc191069095)

[Câu 2: Port Forwarding. 7](#_Toc191069096)

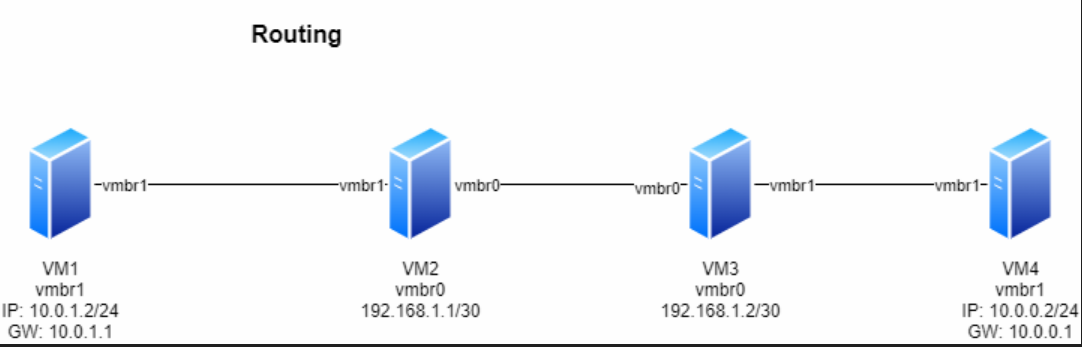
[ cấu hình bảng iptables của máy VM1 7](#_Toc191069097)

[ Tạo key RSA 8](#_Toc191069098)

[Câu 3, ROUTING 9](#_Toc191069099)

[ Bảng cấu hình router từng máy 12](#_Toc191069100)

[ Test ping từ máy VM1 sáng VM4 và ngược lại 13](#_Toc191069101)



**Yêu cầu**:

* Cấu hình VM2 và VM3 để cho network của VM4 và VM1 có thể ping thấy nhau.
* Reboot lại VM2 và VM3 thì hệ thống vẫn hoạt động bình thường (sau khi vào OS).

## Câu 1

* Cấu hình máy
* Đầu tiên ta cấu hình thêm card ens19 của máy vm 1 để làm gateway đến các máy nội bộ trong vlan

Cấu hình máy VM1

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

Cấu hình máy VM2

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

* Ping kết nối máy VM1 và VM2

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, thuật in máy

Nội dung do AI tạo ra có thể không chính xác.

* Bật chuyển tiếp gói IPv4 ở VM1:
* Chỉnh cấu hình sysctl:  
  **echo "net.ipv4.ip\_forward=1" | sudo tee -a /etc/sysctl.conf**
* Apply thay đổi: **sudo sysctl -p**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

* Giải thích: Đảm bảo VM1 có thể route gói tin giữa các interface

### Thiết lập NAT với iptables ở VM1:

**sudo iptables -t nat -A POSTROUTING -o ens18 -j MASQUERADE**

**sudo iptables -A FORWARD -i ens19 -o ens18 -j ACCEPT**

**sudo iptables -A FORWARD -i ens18 -o ens19 -m state --state RELATED,ESTABLISHED -j ACCEPT**

Sau khi re boot lại cả 2 máy thì máy vm2 vẫn ra mạng bt

Lưu rules:

**sudo netfilter-persistent save**

**sudo netfilter-persistent reload**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

Kiểm tra lại:

**sudo iptables -t nat -L -v -n**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

* Lưu cấu hình iptables

Bây giờ tiến hành cài đặt iptables-persistent để lưu rules và config của mình sau khi reboot:

**sudo apt update**

**sudo apt install iptables-persistent**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

Kiểm tra xem máy 2 đã ra mạng chưa

Ảnh có chứa văn bản, Phông chữ, ảnh chụp màn hình, màu đen

Nội dung do AI tạo ra có thể không chính xác.

## Câu 2: Port Forwarding.

**Yêu cầu**:

* Cấu hình port forwarding trên VM1 để khi SSH vào IP WAN của VM1 port 2223 thì có thể truy cập được SSH được thẳng vào VM2.
* cấu hình bảng iptables của máy VM1

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

* ở đây sudo iptables -t nat -A PREROUTING -p tcp --dport 2223-j DNAT --to-destination 10.0.0.2:22

**-t nat** → Áp dụng quy tắc trên bảng NAT.

**-A PREROUTING** → Thêm quy tắc vào chuỗi PREROUTING, xử lý các gói tin ngay khi chúng đến giao diện mạng.

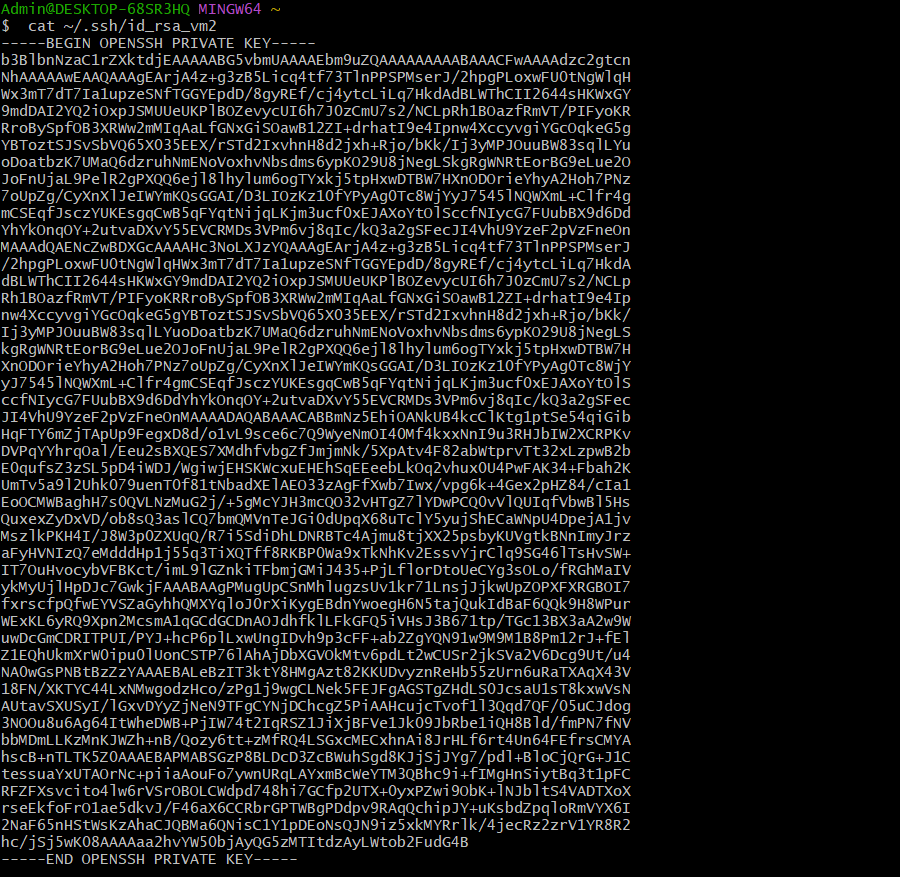
**-p tcp** → Áp dụng quy tắc cho giao thức TCP.

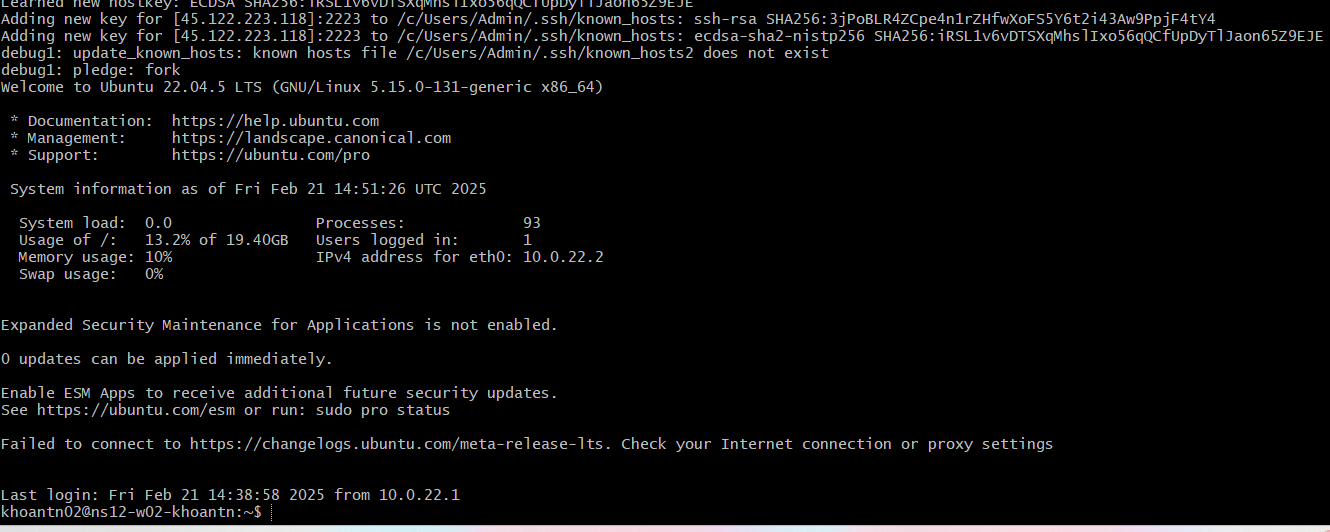
**--dport 2223** → Chỉ áp dụng cho các gói tin đến cổng **2223**.

**-j DNAT** → Chuyển hướng địa chỉ đích (Destination NAT).

**--to-destination 10.0.22.2:22** → Chuyển hướng đến địa chỉ IP nội bộ **10.0.22.2** trên cổng **22**.

* + Lệnh này chuyển hướng tất cả các kết nối đến **cổng 2223** trên máy chủ của bạn đến máy nội bộ có địa chỉ IP **10.0.22.2** trên **cổng 22** (mặc định của SSH).
  + Điều này cho phép người dùng từ bên ngoài kết nối vào địa chỉ IP công cộng của máy chủ qua cổng 2222 nhưng thực chất sẽ truy cập vào dịch vụ SSH của máy 10.0.22.2
  + Tiếp theo ta tiến hành tạo key rsa như ở lab 1 và trao đổi key. Publish key thì để bên máy VM2 và private key thì để trong máy thật
* Tạo key RSA
* Giống như lab 1 ta tạo key rồi cất key Private ở máy thật và cất Pubkey ở máy VM2





## Câu 3, ROUTING

Môi trường: đề tài yêu cầu 2 bạn làm chung 1 bài lab. Mỗi bạn được cấp 2 VM và cấu hình mạng như hình sau:

• Bạn 1: VM2 (có vmbr0 và vmbr1) và VM1 (only vmbr1)

• Bạn 2: VM3 (có vmbr0 và vmbr1) và VM4 (only vmbr1)

Ảnh có chứa văn bản, ảnh chụp màn hình, hàng, biểu đồ

Nội dung do AI tạo ra có thể không chính xác.

Cấu hình máy câu 3

Cấu hình mạng VM1

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

Cấu hình máy VM2

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, màn hình

Nội dung do AI tạo ra có thể không chính xác.

Cấu hình máy VM3

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, màn hình

Nội dung do AI tạo ra có thể không chính xác.

Cấu hình máy vm4

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, màn hình

Nội dung do AI tạo ra có thể không chính xác.

* Bảng cấu hình router từng máy

VM1:

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

VM2:

Ảnh có chứa văn bản, Phông chữ, ảnh chụp màn hình, màu đen

Nội dung do AI tạo ra có thể không chính xác.

VM3:

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, màu đen

Nội dung do AI tạo ra có thể không chính xác.

VM4:

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

* Test ping từ máy VM1 sáng VM4 và ngược lại

Máy VM1 sáng VM4

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

Máy VM4 sang VM1

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

* Vấn đề lưu lại các cấu hình route thì ta lưu ở file mạng luôn : sudo nano /etc/netplan/(file mạng) lúc mở lên nó sẽ tự động cấu hình luôn

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, phần mềm

Nội dung do AI tạo ra có thể không chính xác.

* Các máy khác tương tự.

END