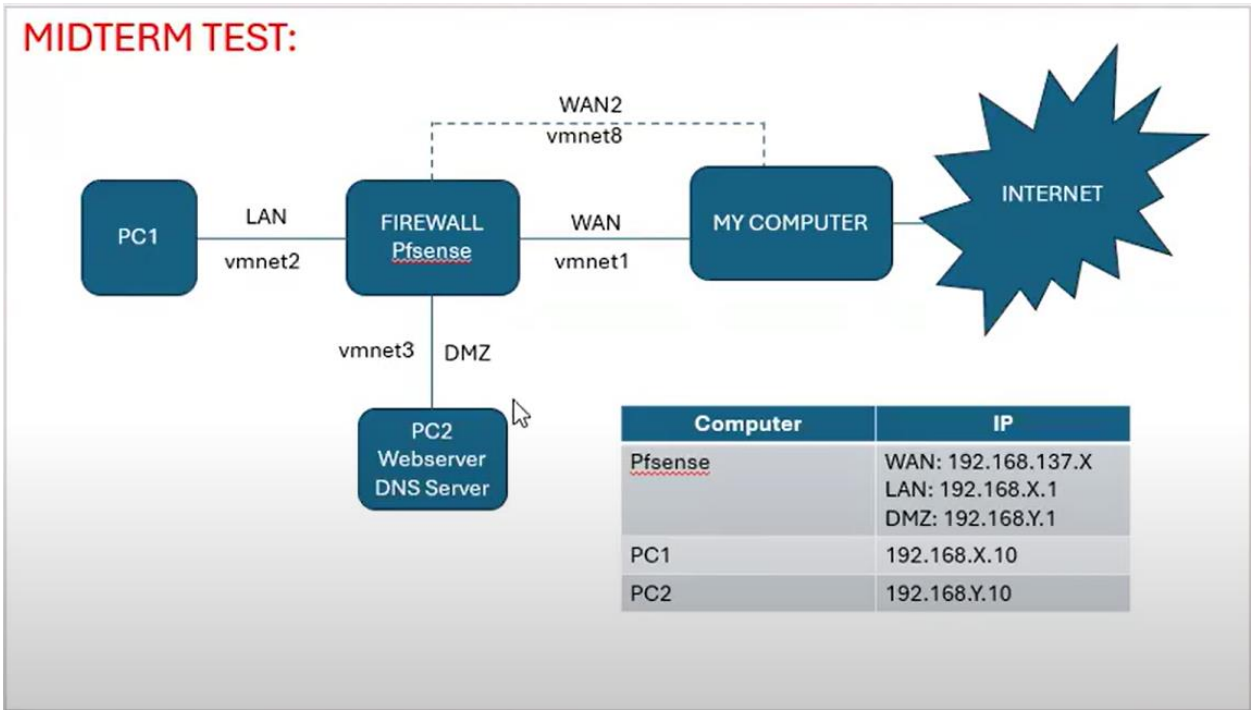
MÔN TRIỂN KHAI AN NINH HỆ THỐNG

Phúc Lâm

GVHD: Đỗ Hà Phương

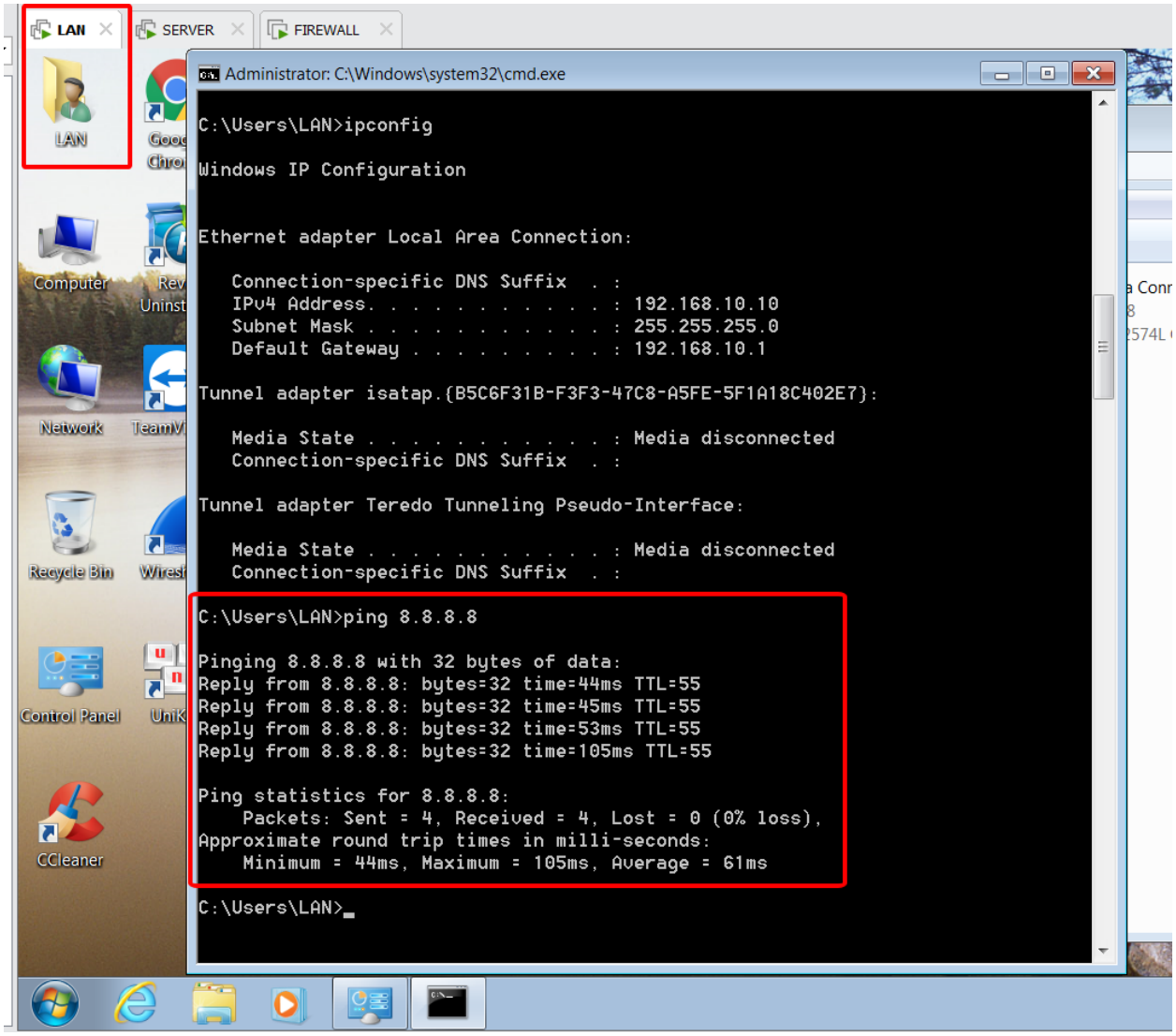


Mission deployments:

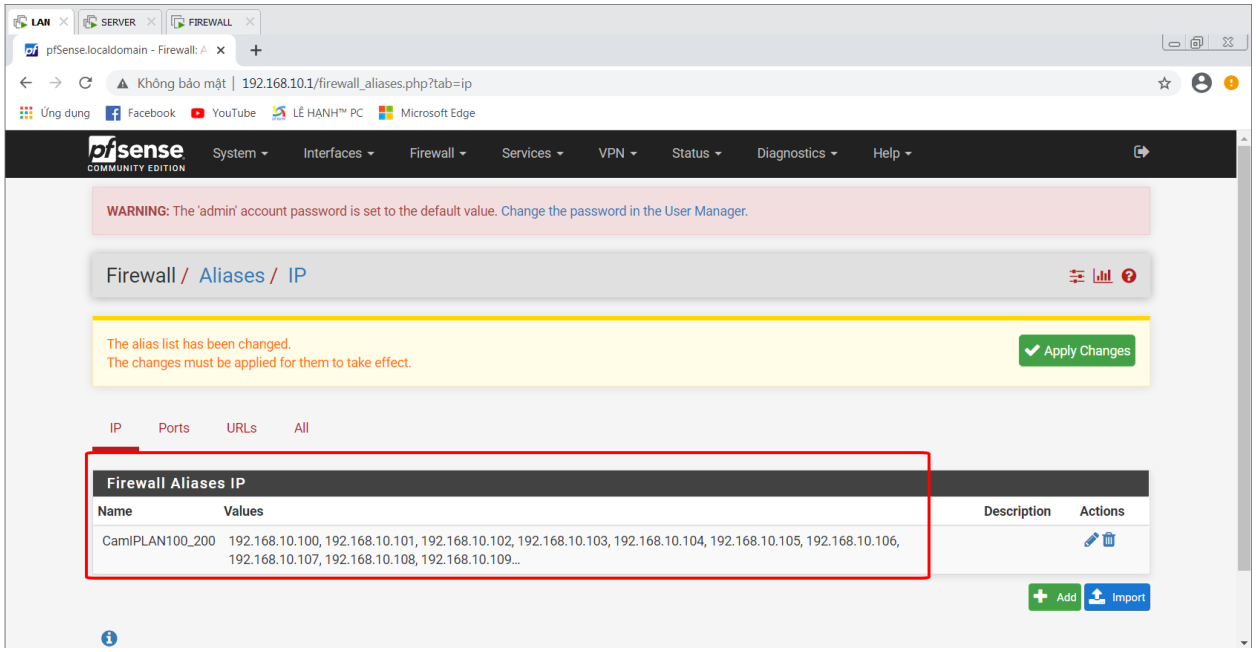
1. **Cấu hình Pfsense, LAN. Kết quả LAN truy cập Internet (1đ)**
2. **Tao Alias cấm IP LAN truy cập Internet: 192.168.X.100-192.168.X.200 (1đ)**
3. **Tao Alias cấm LAN truy cập: www.tp-link.com, www.shopee.vn, shopee.vn**
4. **Thiết lập time: Asia/Ho Chi Minh, lập lịch cấm LAN truy cập Internet giờ hành chính**
5. **Chỉ cho LAN truy cập TCP 80, 443. Kiểm tra LAN chỉ kết nối HTTP bằng IP**
6. **Mở và chặn DNS tại UDP port 53**
7. **Mở và chặn ICMP LAN ping ra Internet**
8. **Thiết lập DNS, WEB Server tại vùng DMZ**
9. **Public WEB Server**
10. **Cấu hình MultiGateway WAN1, WAN2 để dự phòng mất kết nối Internet.**

SINH VIÊN THỰC HIỆN

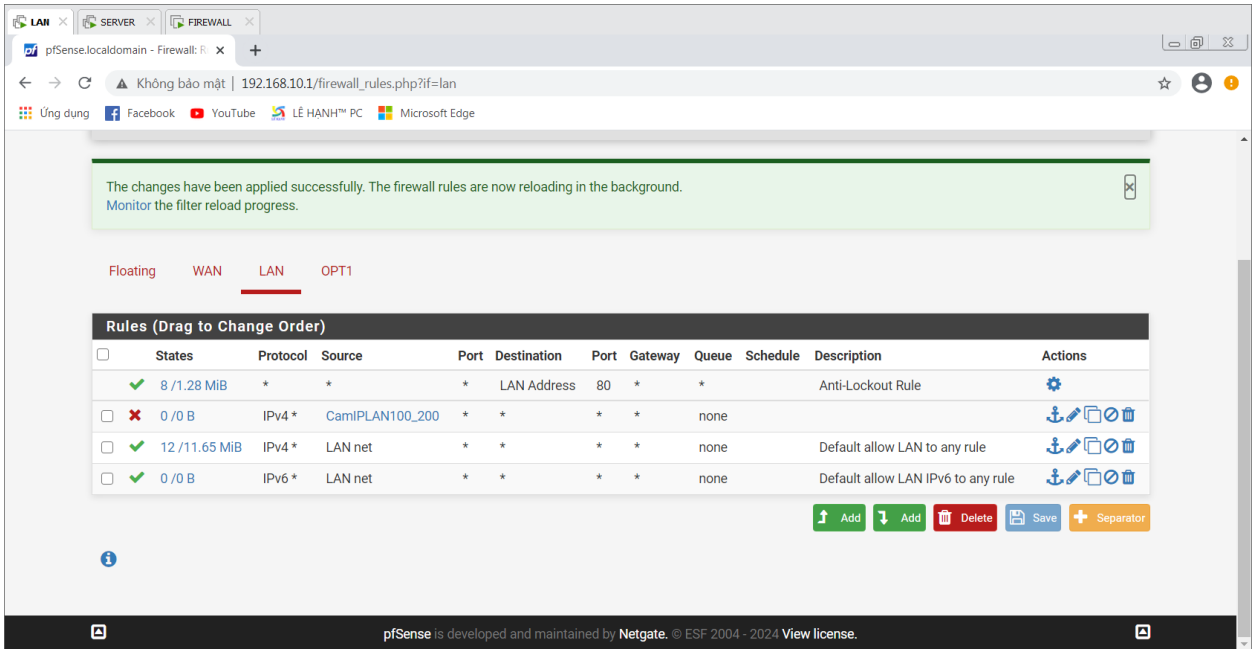
1. Cấu hình Pfsense, LAN. Kết quả LAN truy cập Internet (1đ)



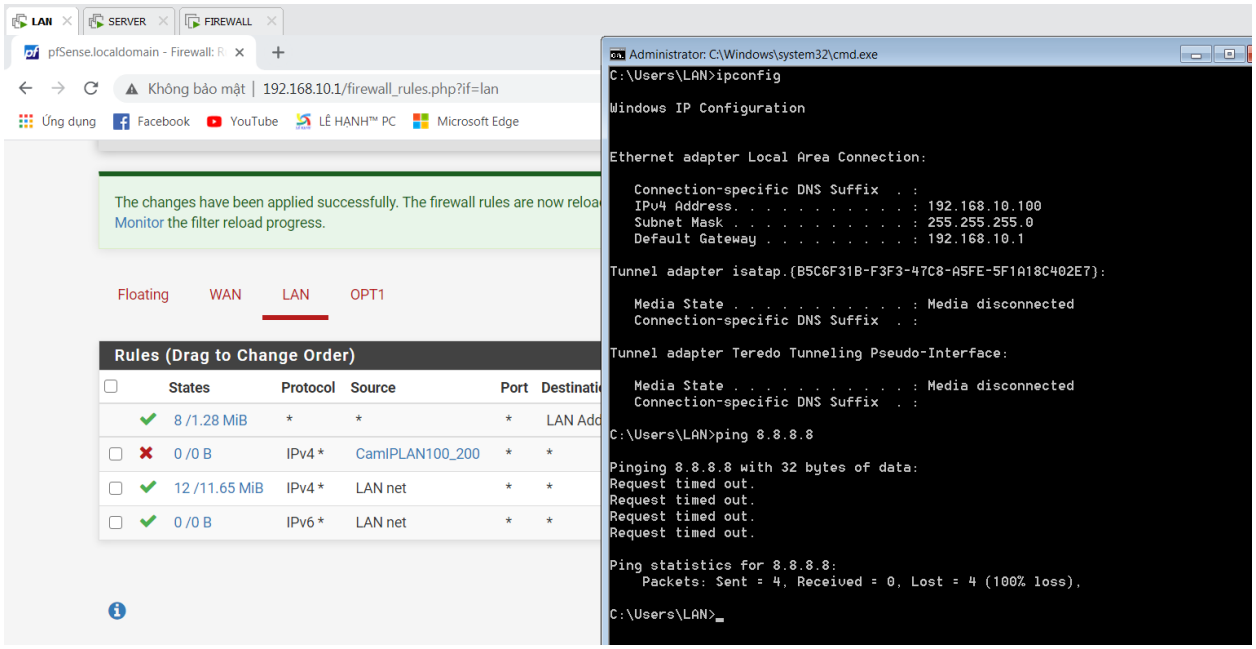
2. Tao Alias cấm IP LAN truy cập Internet: 192.168.X.100-192.168.X.200 (1đ)



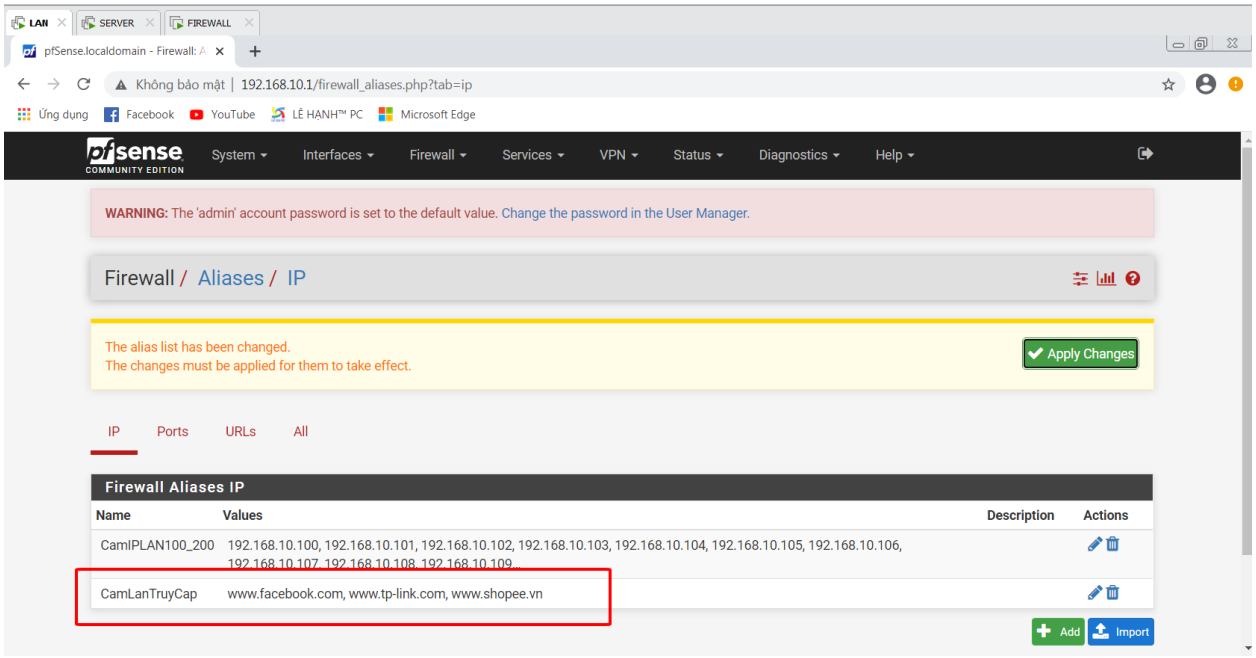
Tạo rules

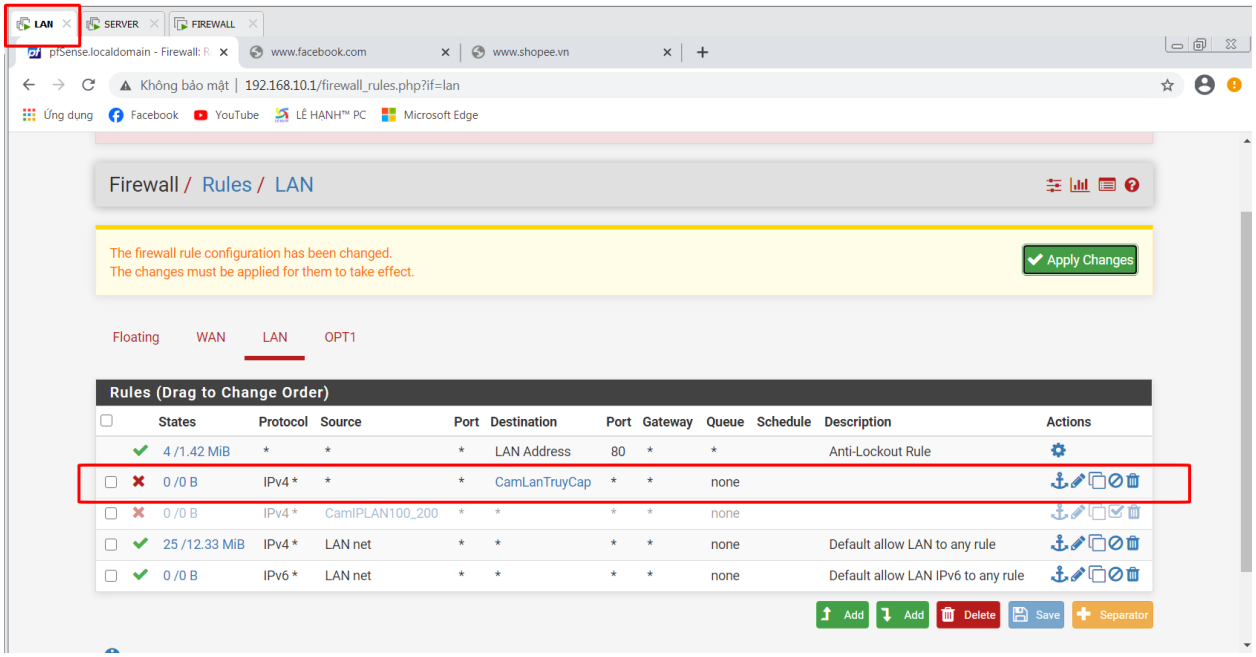


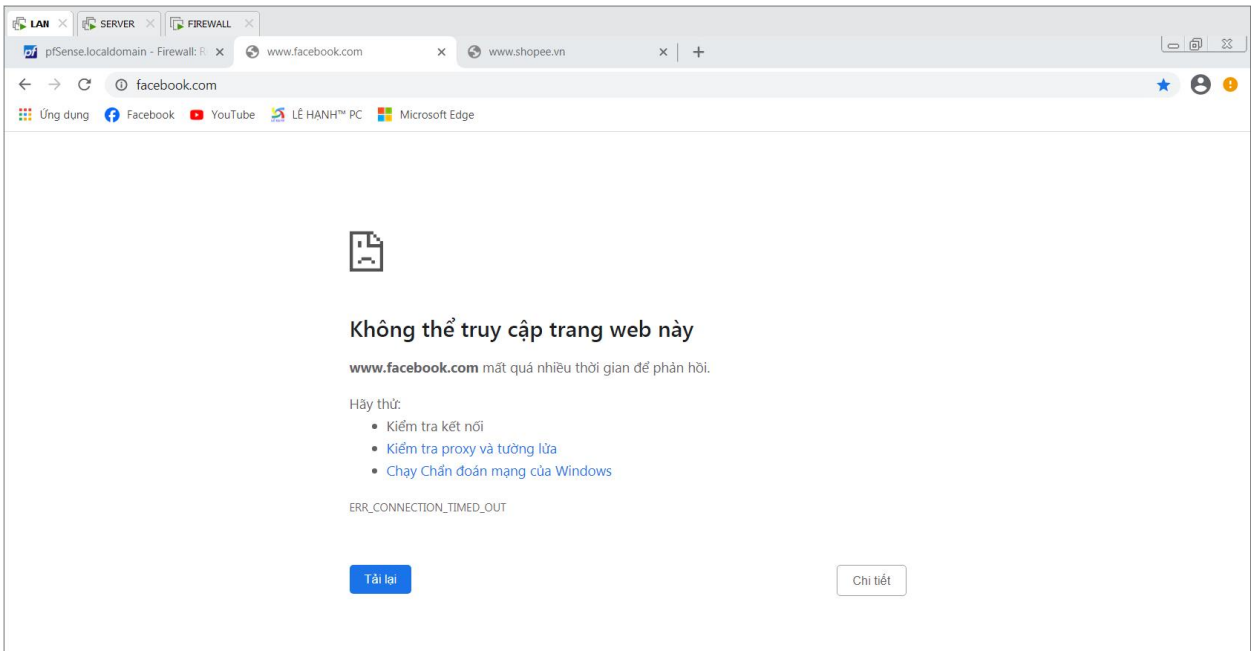
Đổi IP của LAN sang vùng cấm IP để test kết quả = không truy cập được internet



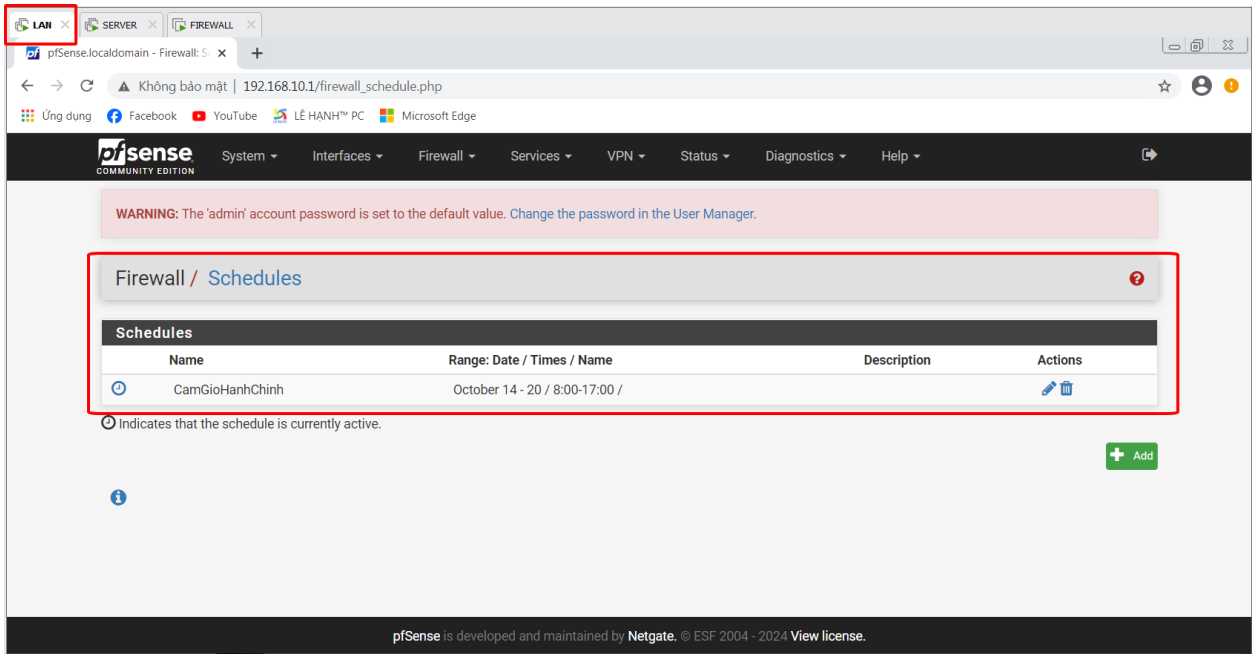
3. Tao Alias cấm LAN truy cập: www.tp-link.com, www.shopee.vn, shopee.vn

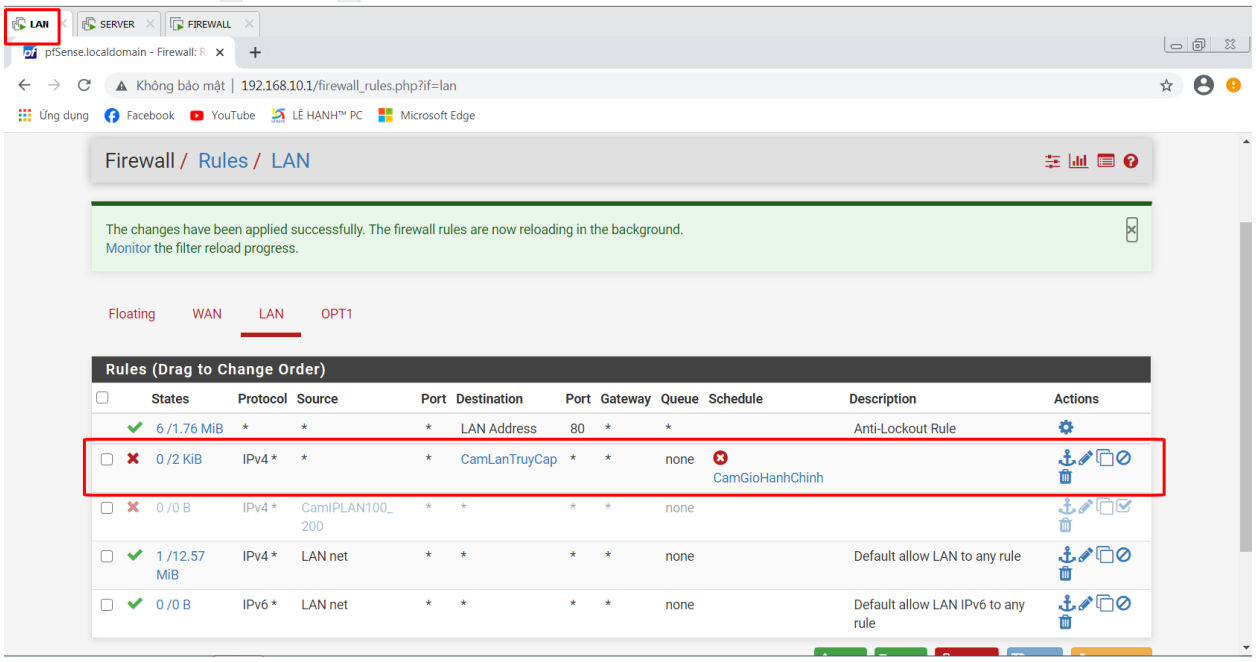




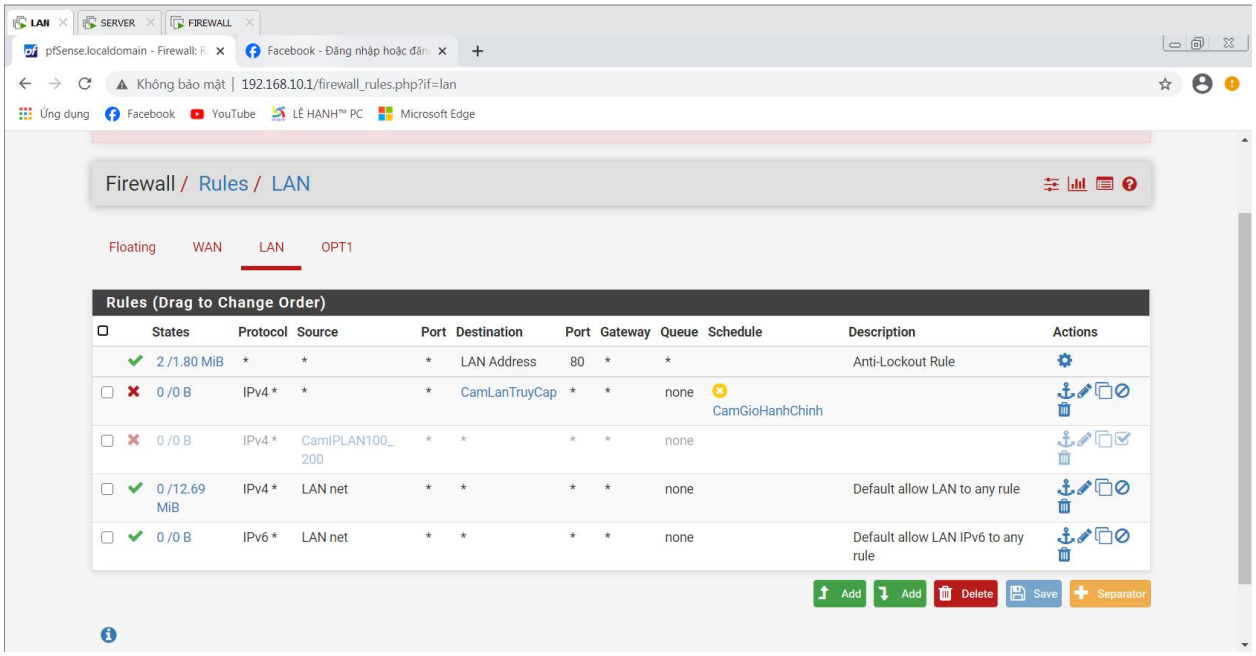

LAN
SERVER
FIREWALL
pfSense.localdomain - Firewall: R
www.facebook.com
www.shopee.vn
facebook.com
Ứng dụng
Facebook
YouTube
LÊ HẠNH™ PC
Microsoft Edge
Không thể truy cập trang web này
www.facebook.com mất quá nhiều thời gian để phản hồi.
Hãy thử:
Kiểm tra kết nối
Kiểm tra proxy và tường lửa
Chạy Chẩn đoán mạng của Windows
ERR_CONNECTION_TIMED_OUT
Tải lại
Chi tiết

4. Thiết lập time: Asia/Ho Chi Minh, lập lịch cấm LAN truy cập Internet giờ hành chính

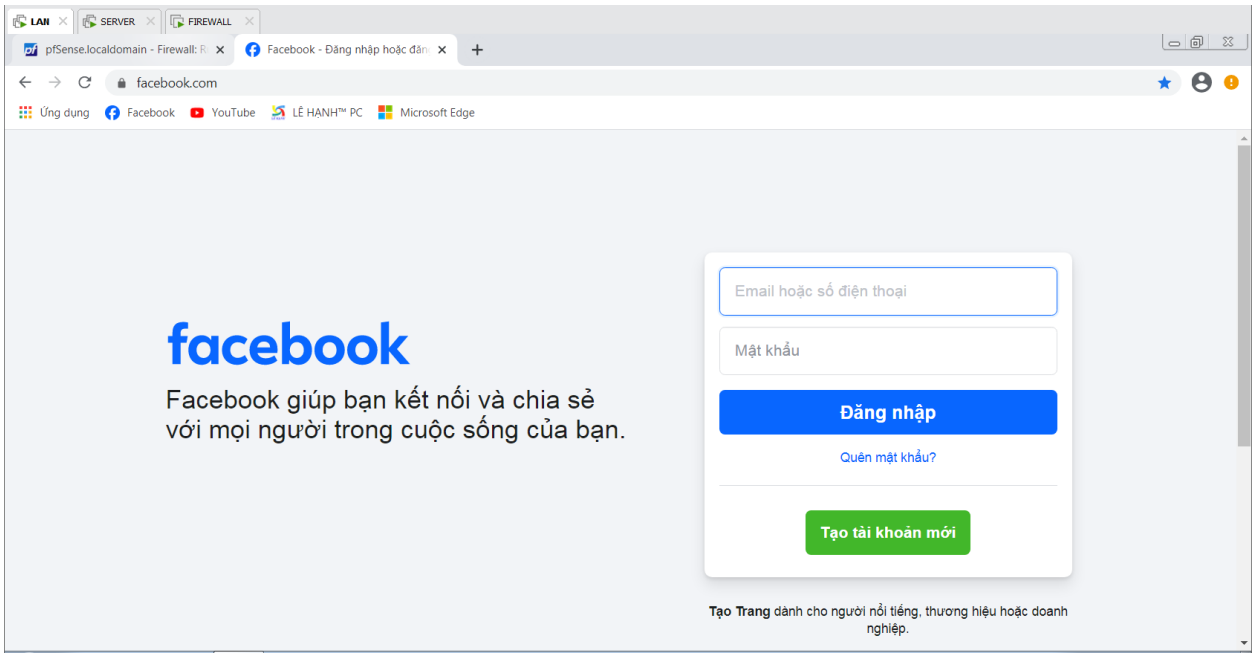




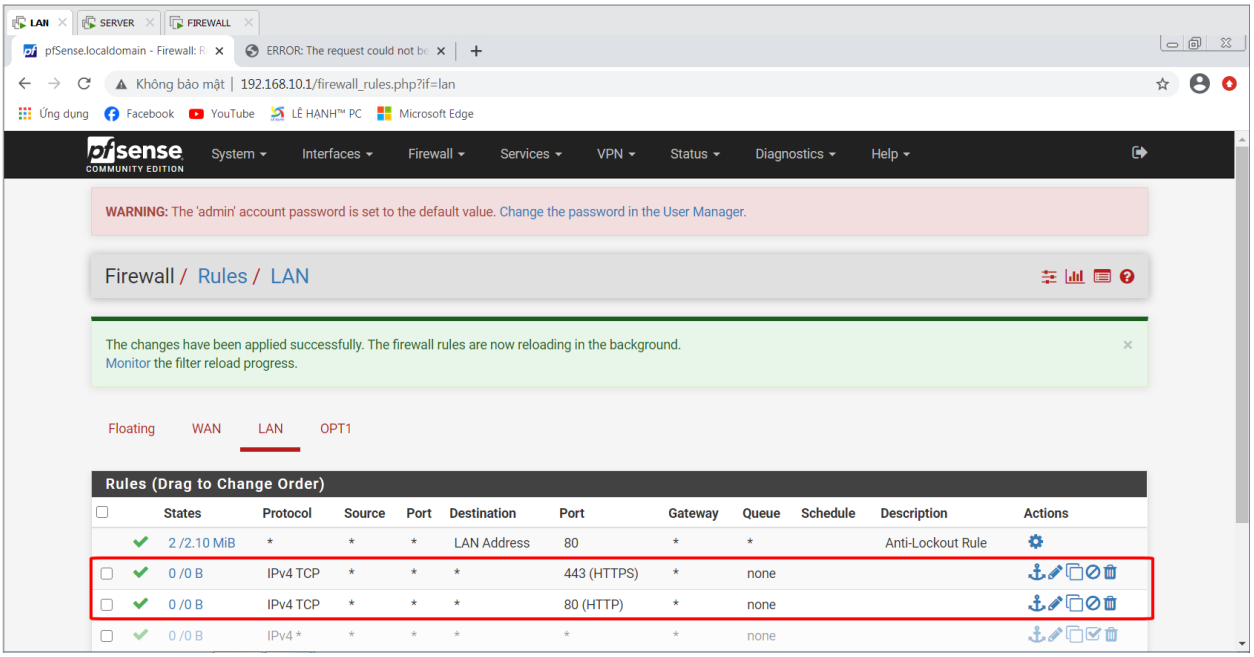
Khi hết giờ



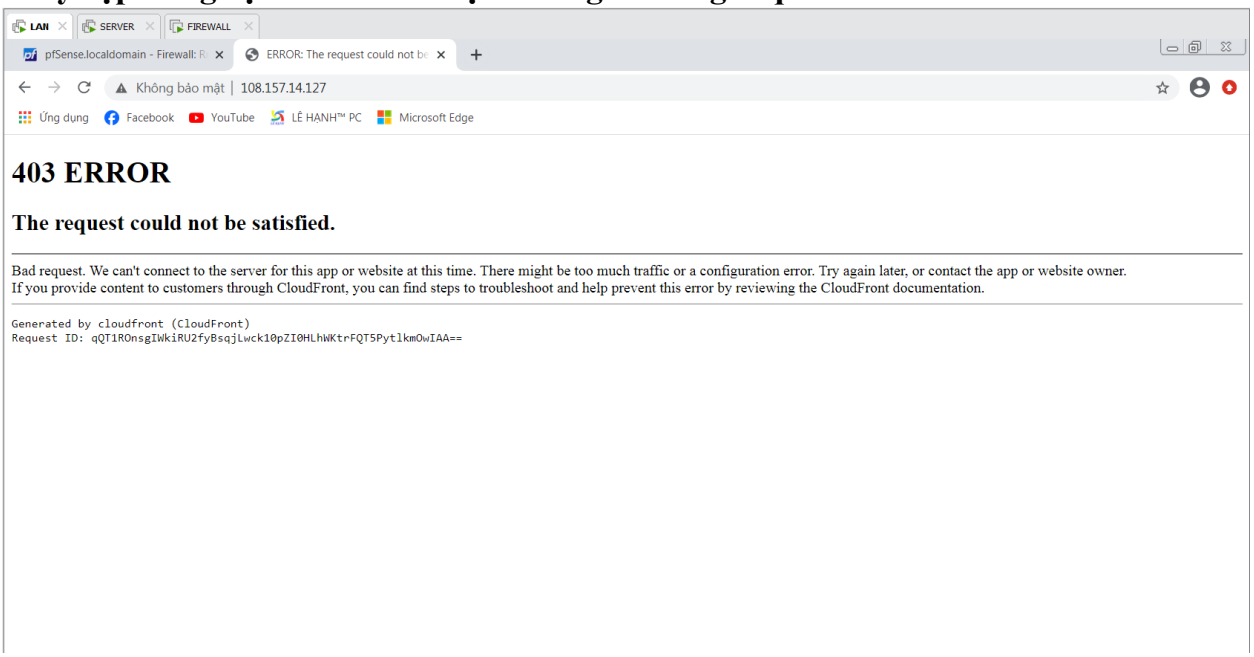
Kiểm tra lại



5. Chỉ cho LAN truy cập TCP 80, 443. Kiểm tra LAN chỉ kết nối HTTP bằng IP

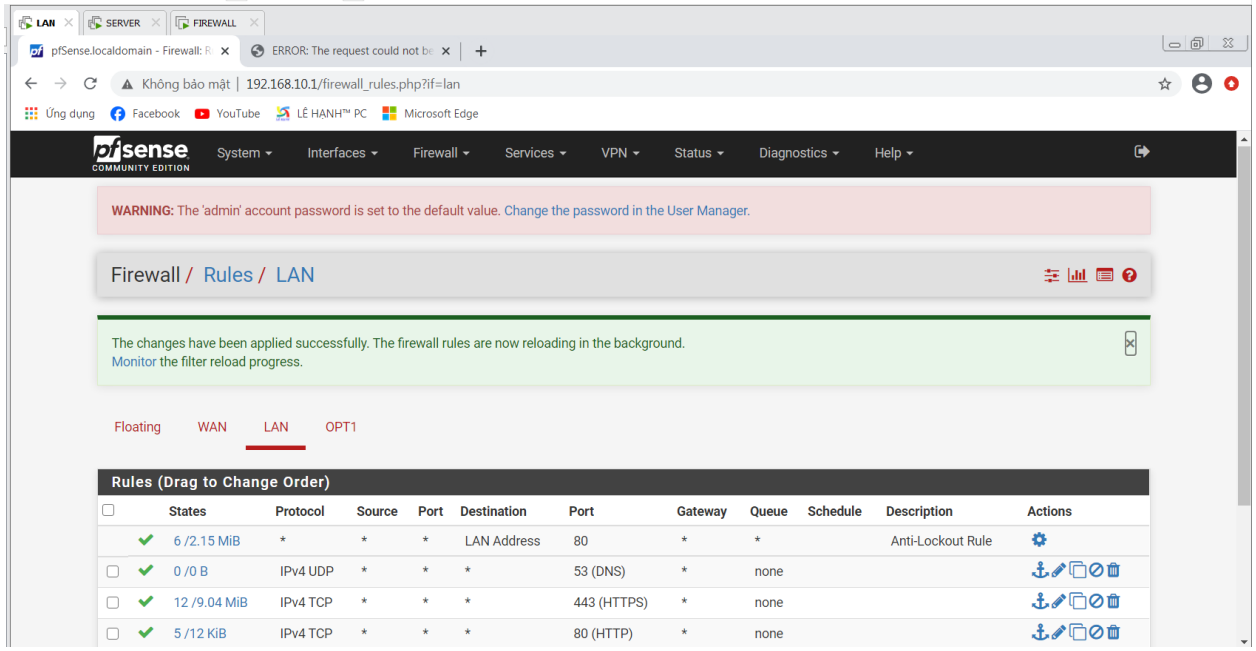


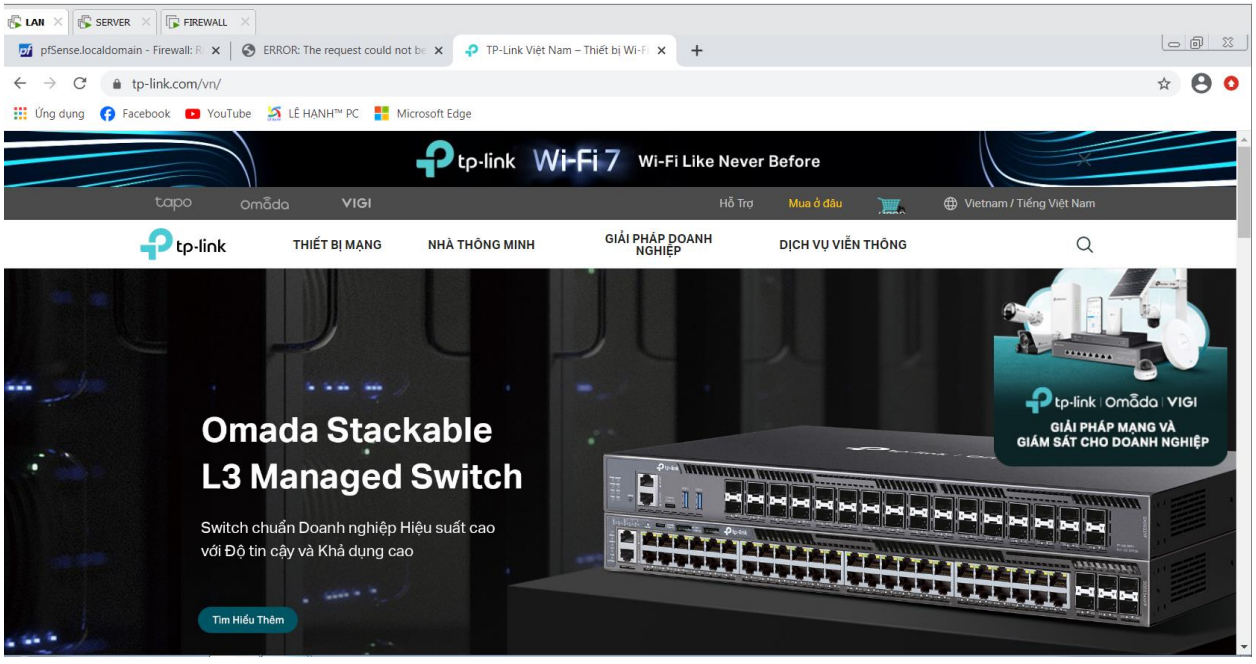
Truy cập bằng địa chỉ IP thì được nhưng lỗi cổng request 403



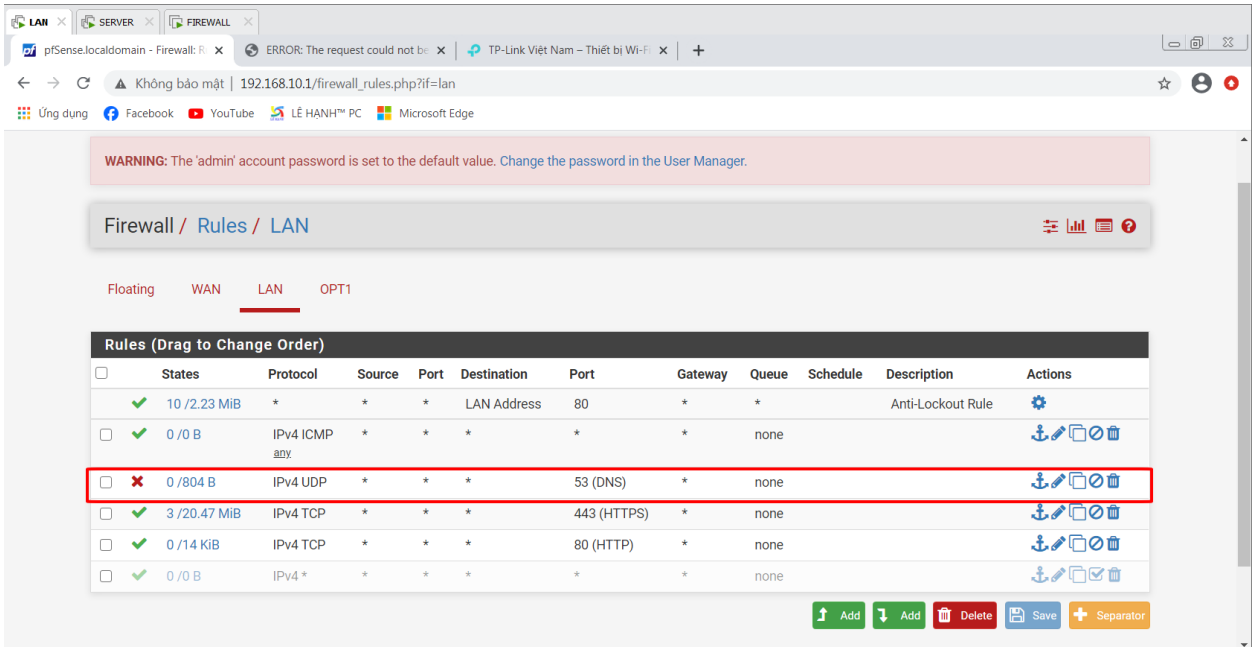
6. Mở và chặn DNS tại UDP port 53

Mở cổng

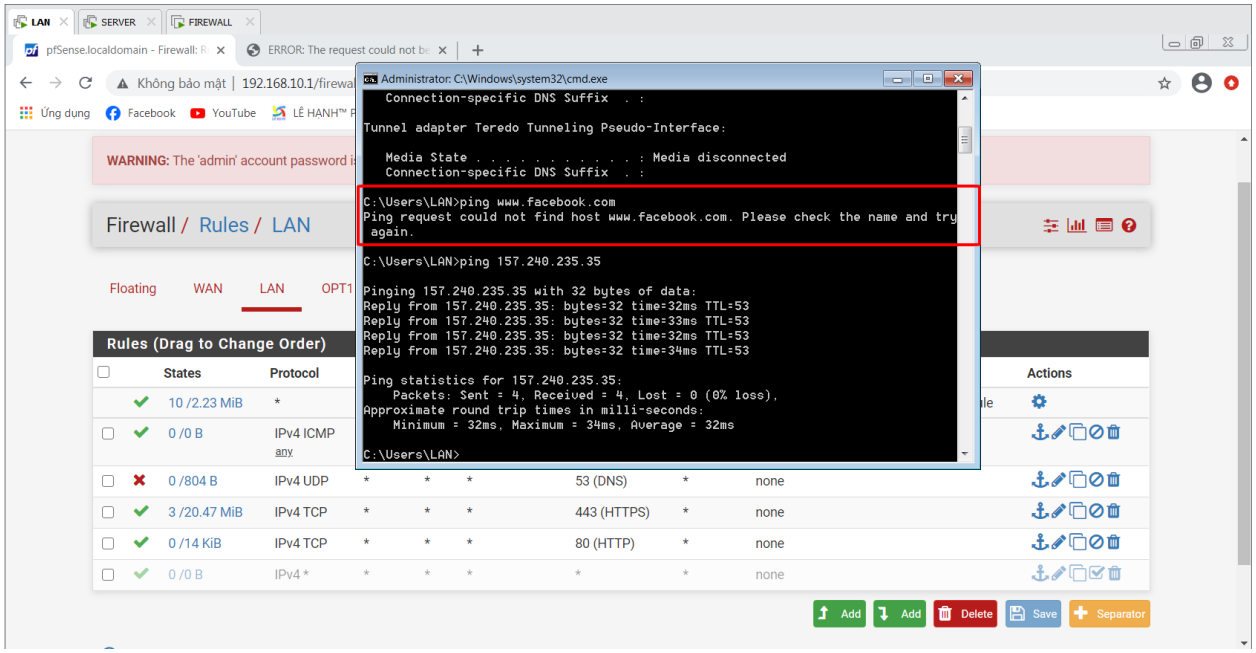




Chặn DNS

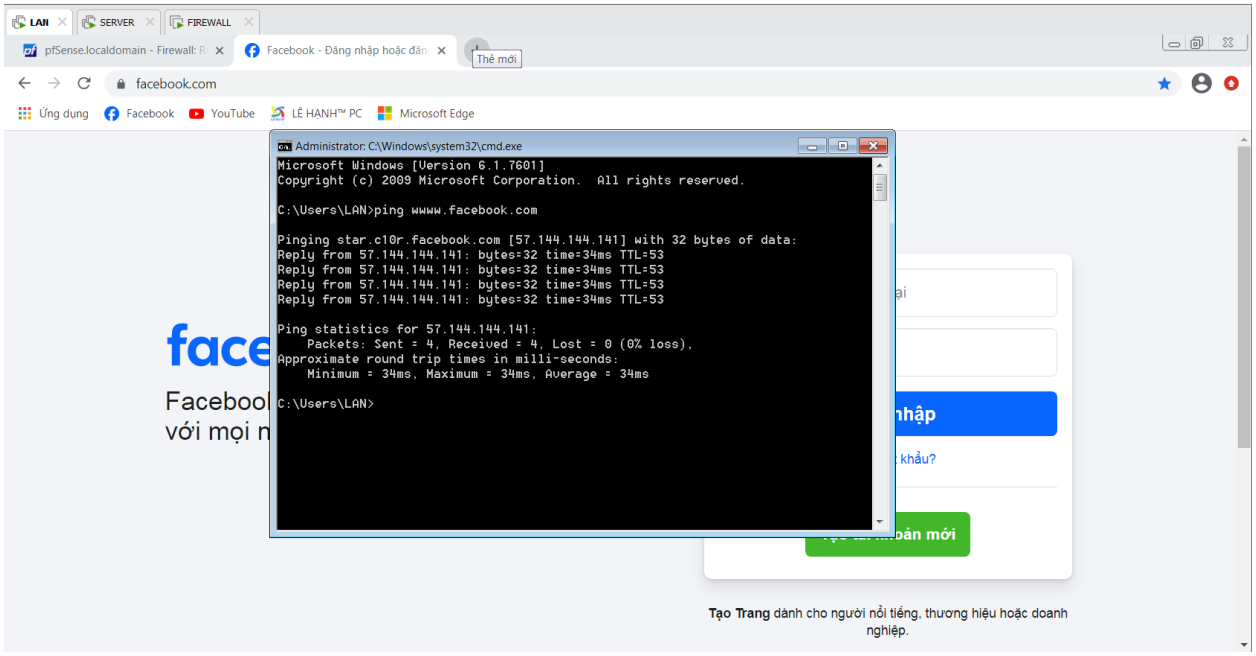


Kết quả là không ping bằng tên miền do không phân giải DNS được và chỉ ping được tới địa chỉ đó

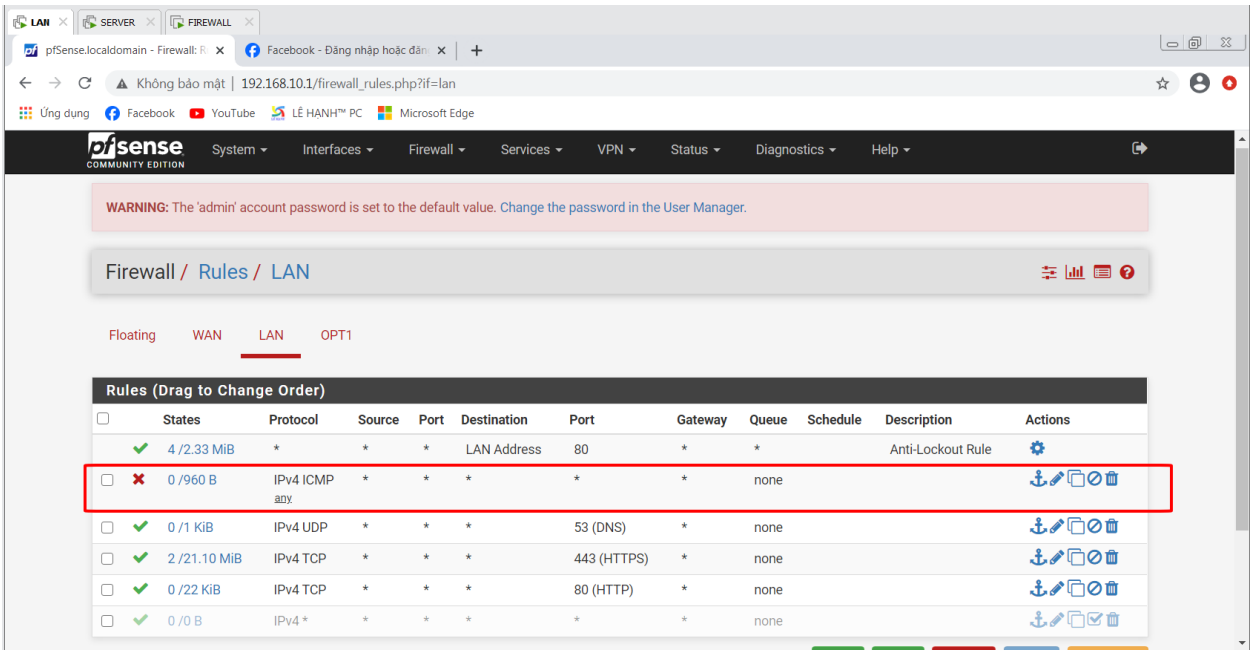


7. Mở và chặn ICMP LAN ping ra Internet

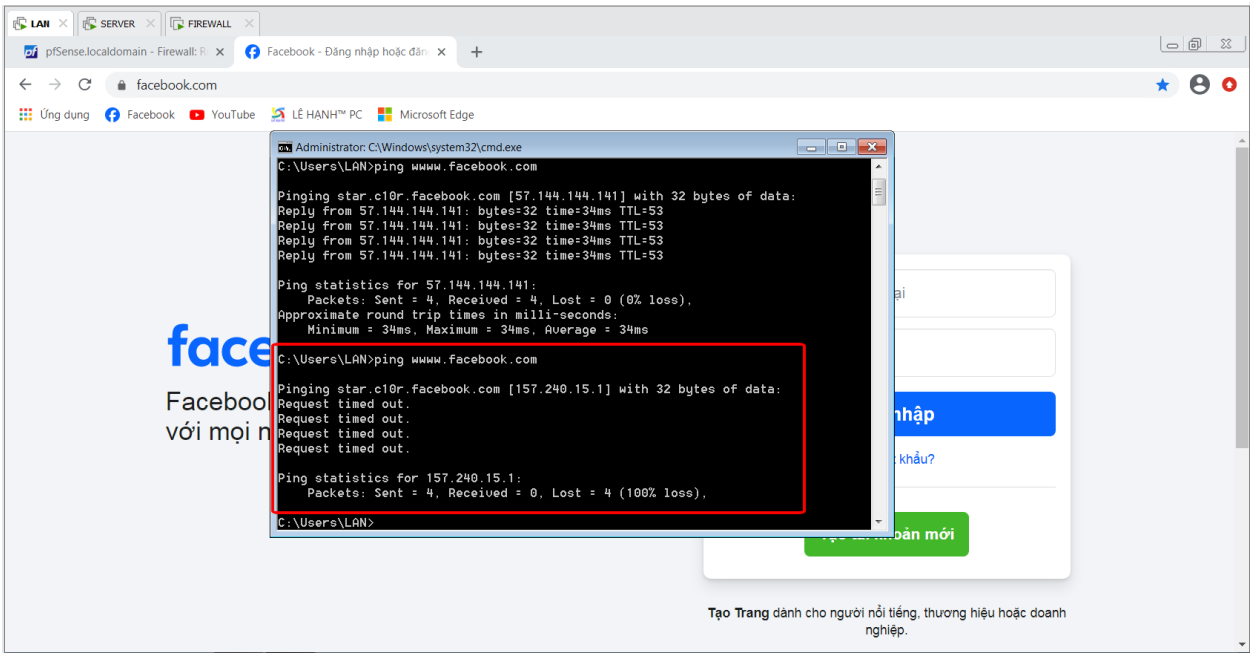
Mở ICMP để ping



Chặn ICMP để không ping được

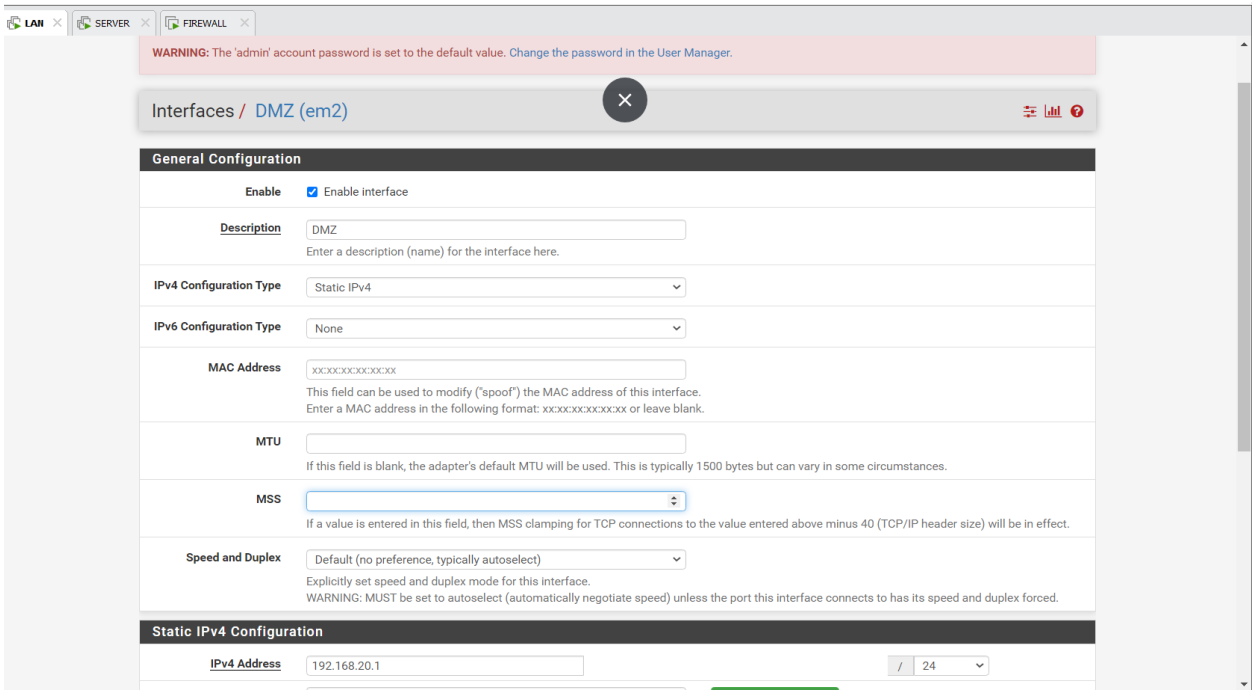


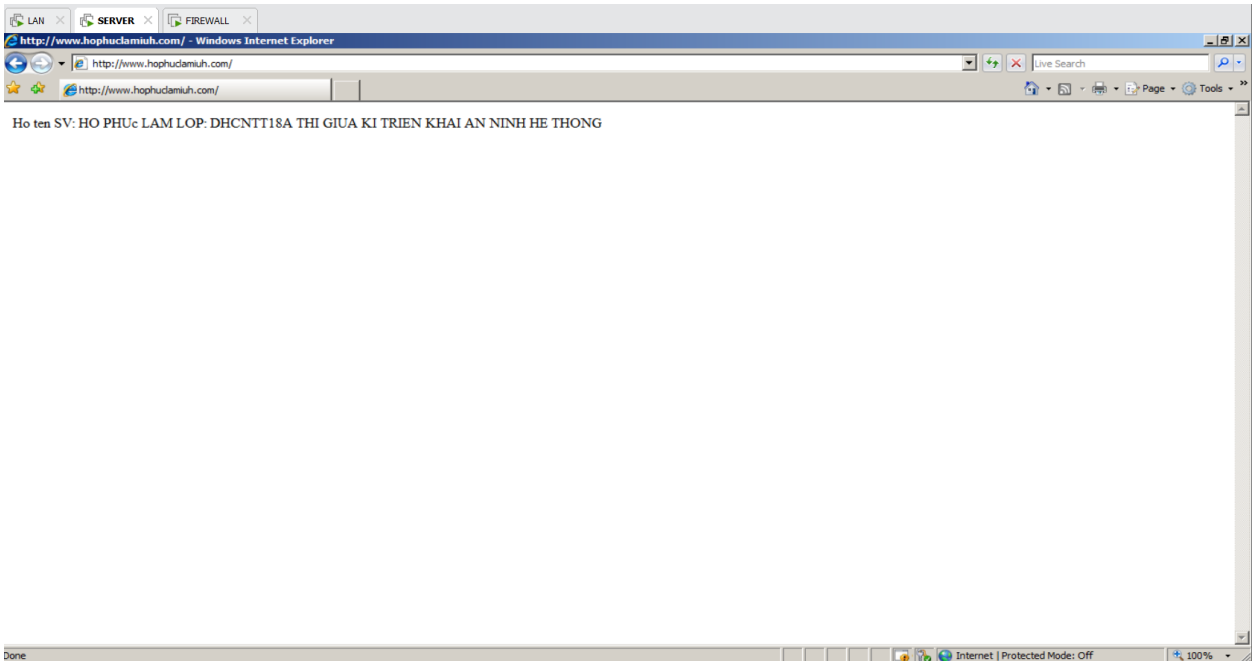
Kết quả của chặn ICMP là không ping được tới địa chỉ IP mà vẫn truy cập web được



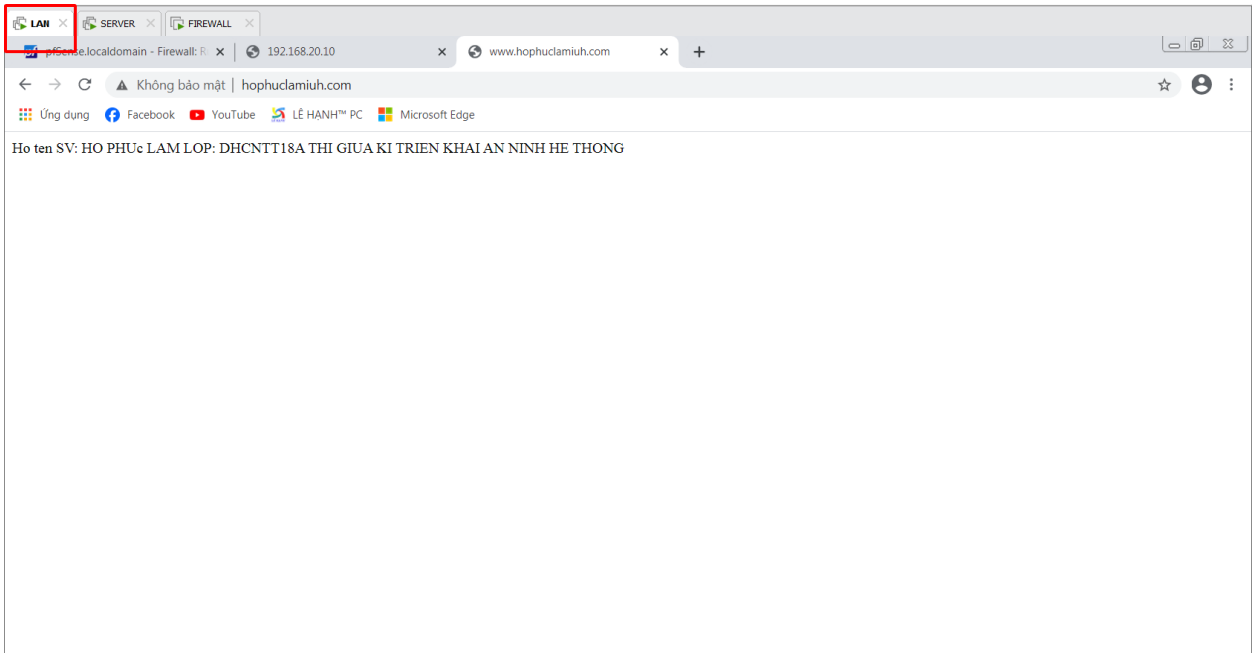
8. Thiết lập DNS, WEB Server tại vùng DMZ

- thiết lập vùng DMZ VMnet3

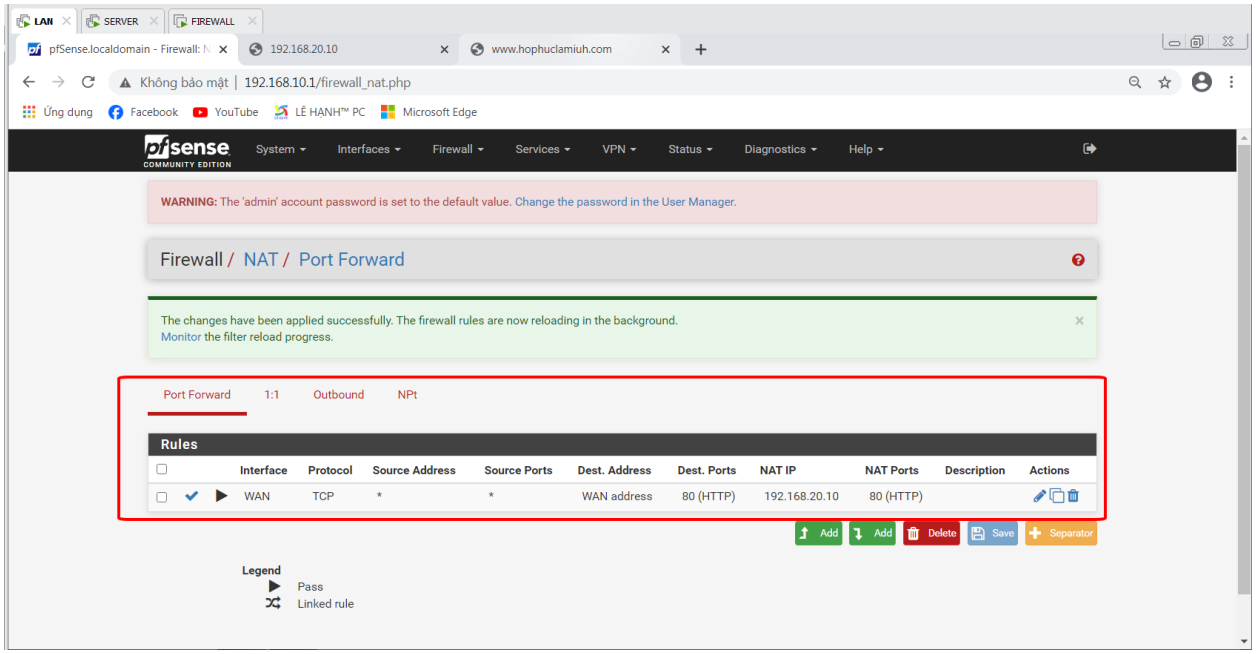


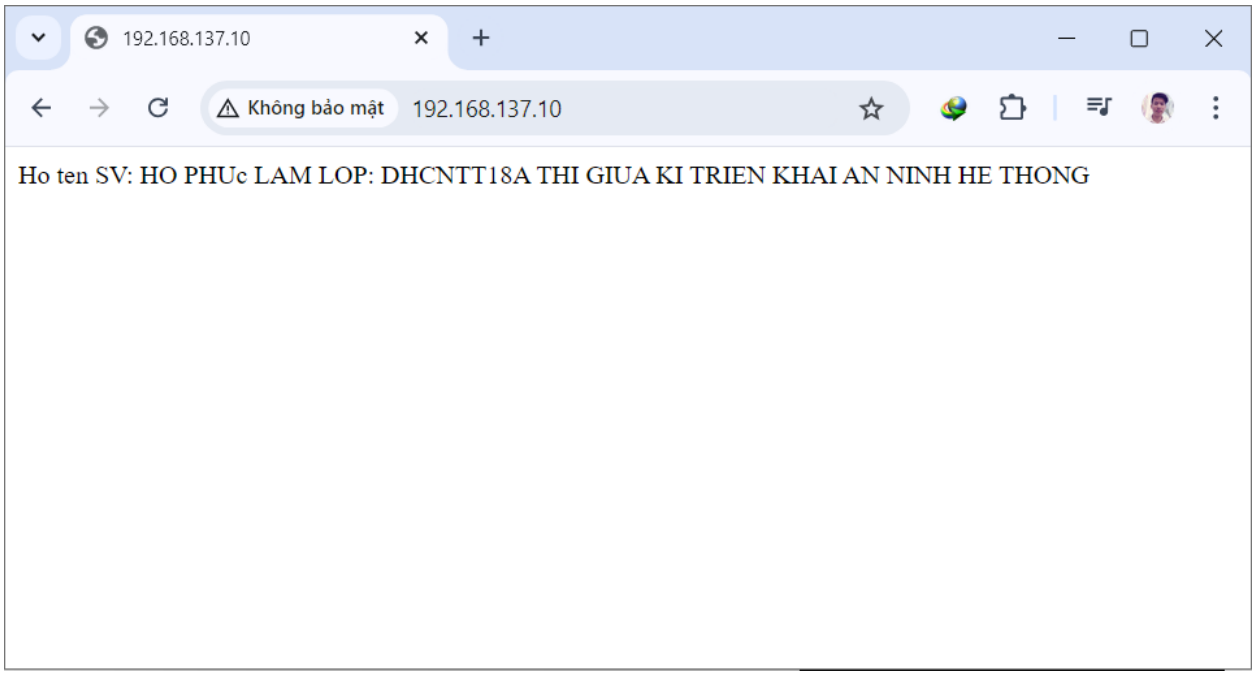


LAN đã truy cập được DMZ

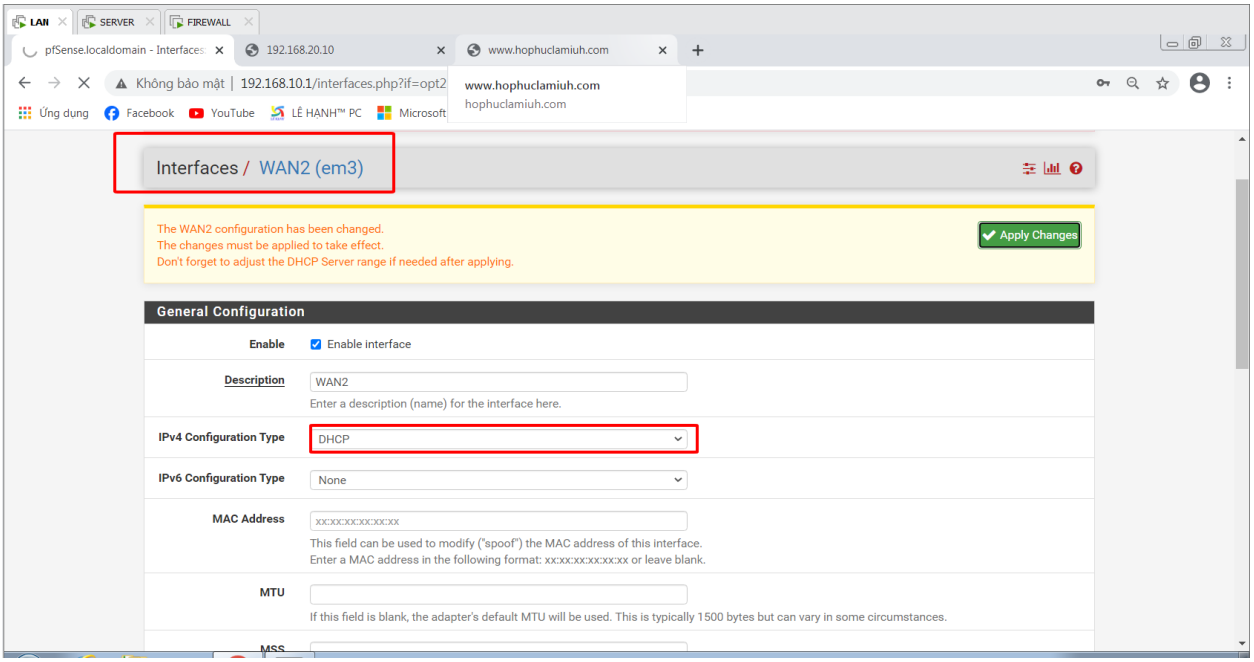


9. Public WEB Server

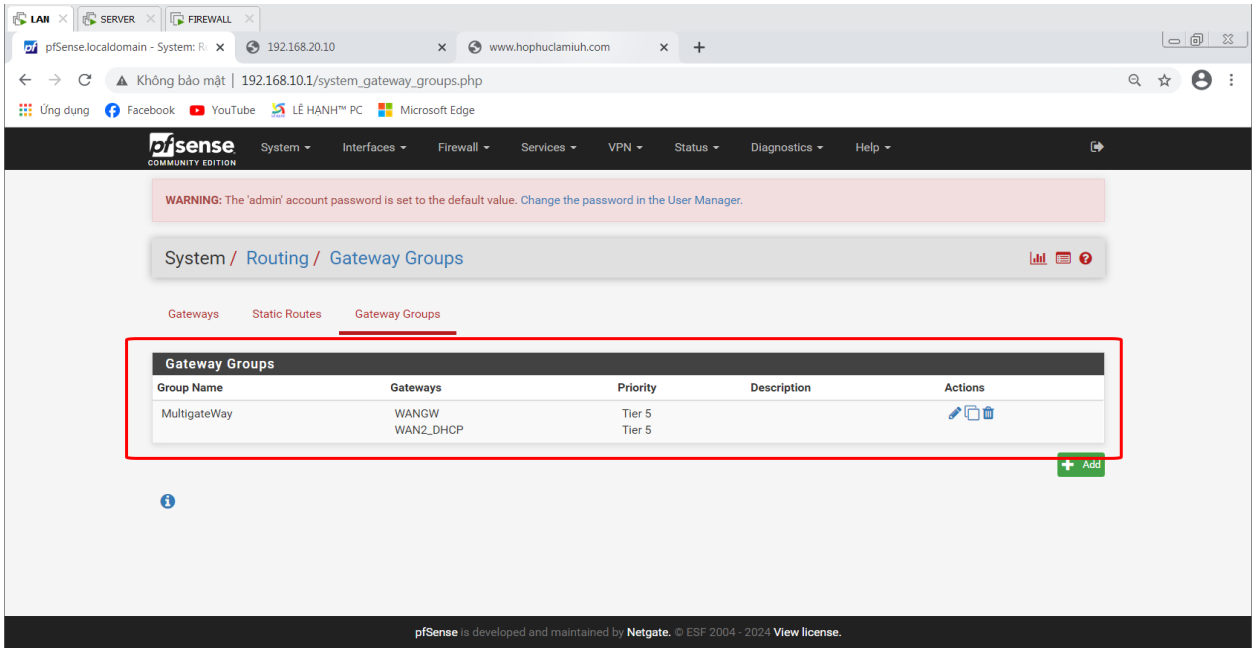


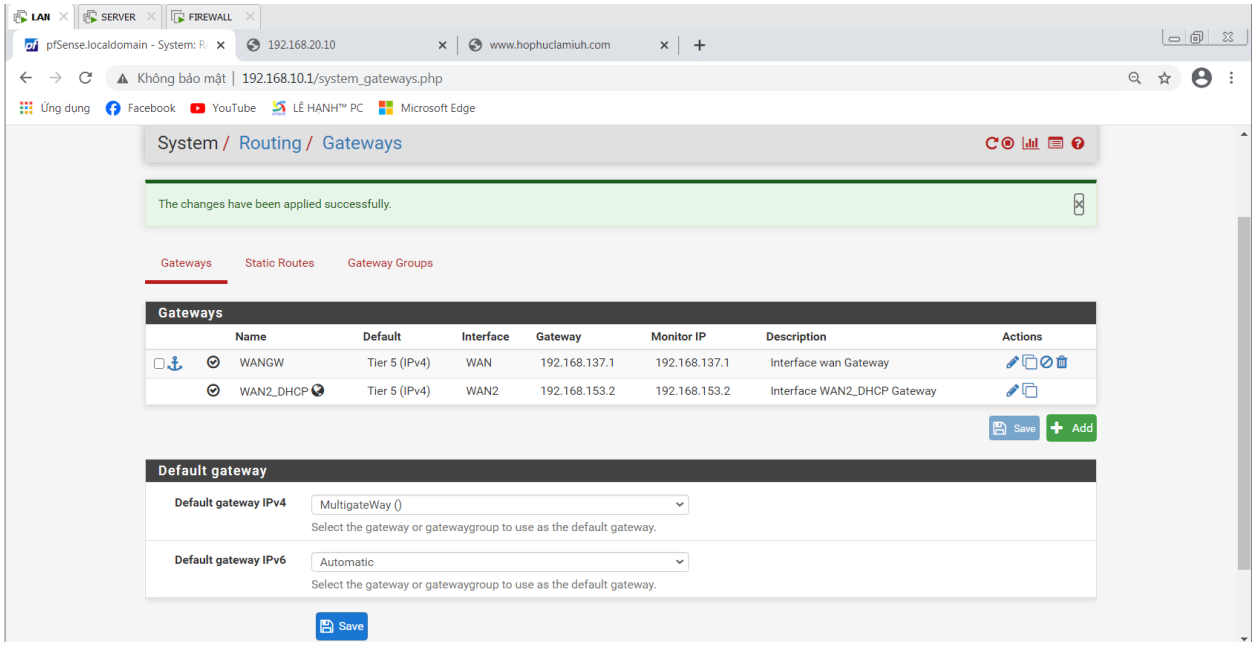


10. Cấu hình MultiGateway WAN1, WAN2 để dự phòng mất kết nối Internet.

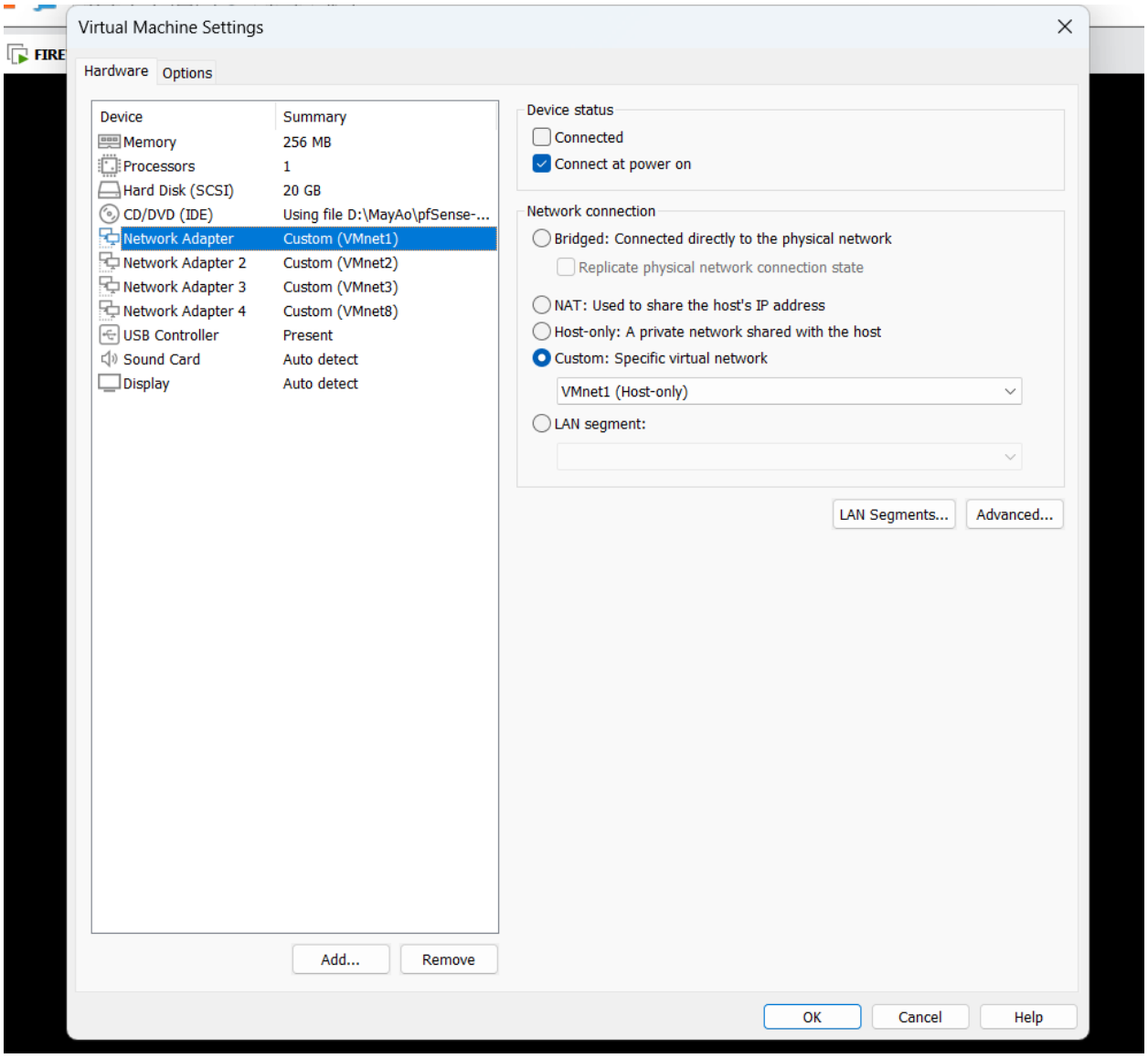


Cấu hình routing để làm dự phòng

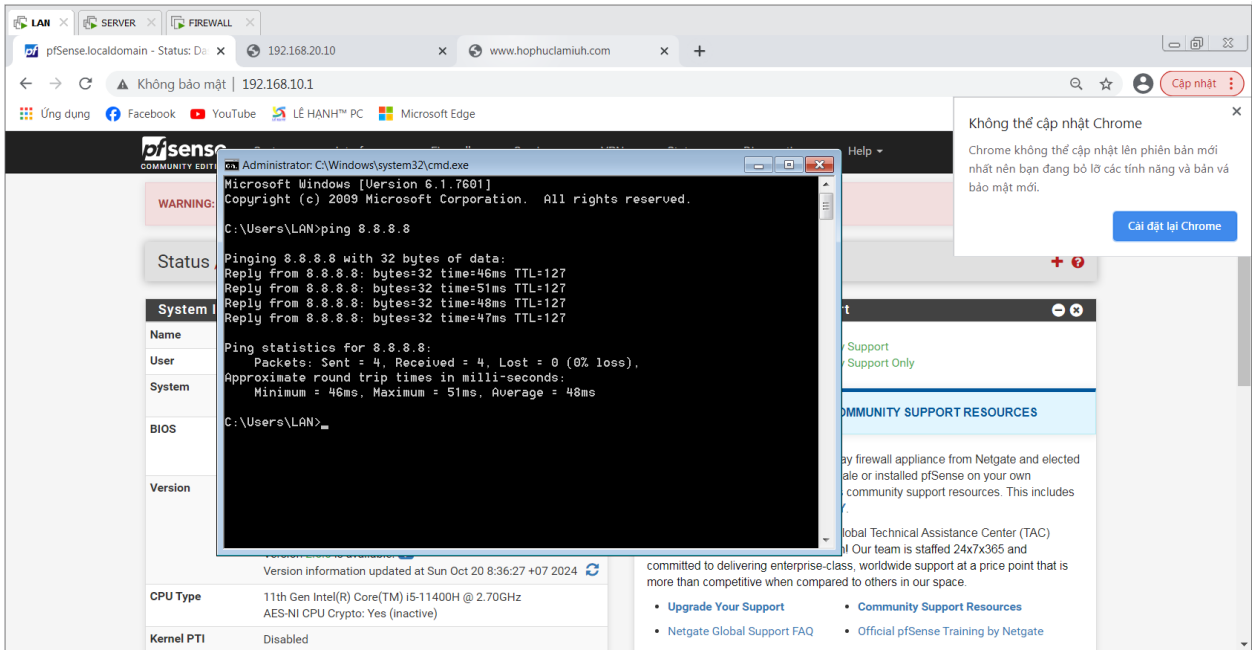



LAN
SERVER
FIREWALL
pfSense.localdomain - System: R
192.168.20.10
www.hophuclamiuh.com
Không bảo mật | 192.168.10.1/system_gateways.php
Ứng dụng
Facebook
YouTube
LÊ HẠNH™ PC
Microsoft Edge
System / Routing / Gateways
The changes have been applied successfully.
Gateways
Static Routes
Gateway Groups
Gateways
Name
Default
Interface
Gateway
Monitor IP
Description
Actions
WANGW
Tier 5 (IPv4)
WAN
192.168.137.1
192.168.137.1
Interface wan Gateway
WAN2_DHCP
Tier 5 (IPv4)
WAN2
192.168.153.2
192.168.153.2
Interface WAN2_DHCP Gateway
Save
Add
Default gateway
Default gateway IPv4
MultigateWay ()
Select the gateway or gatewaygroup to use as the default gateway.
Default gateway IPv6
Automatic
Select the gateway or gatewaygroup to use as the default gateway.
Save

Kiểm tra bằng các tắt VMnet1 của WAN



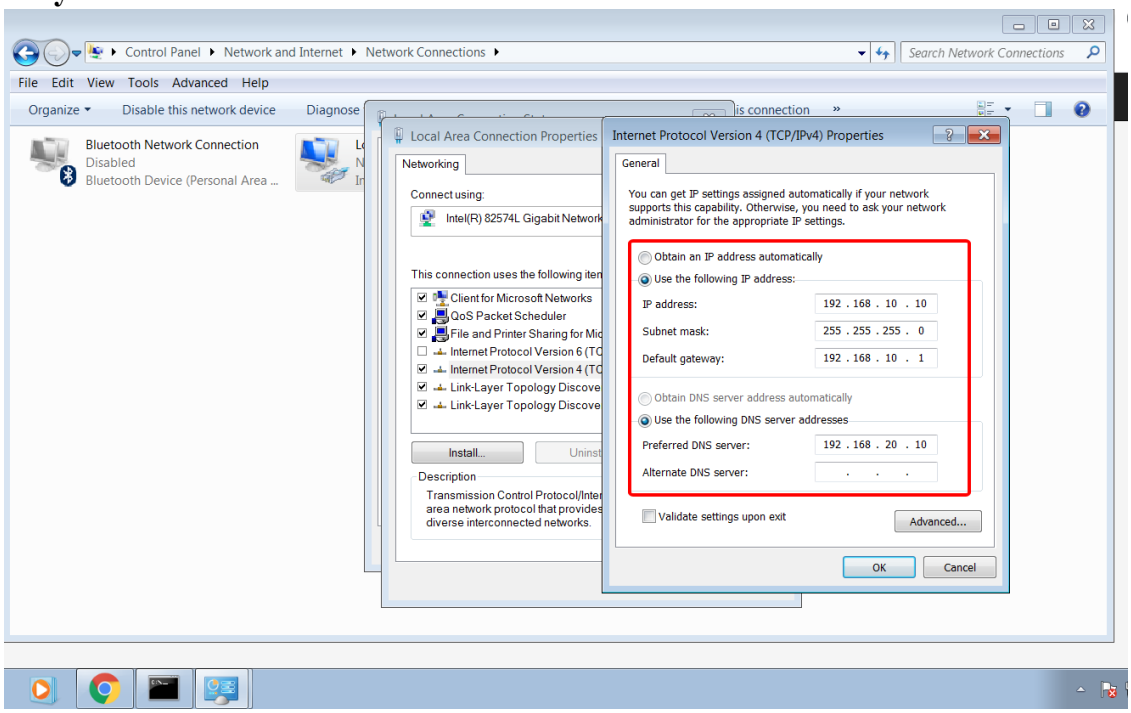
Kết quả là nó chuyển sang VMnet8 và vẫn truy cập đc internet



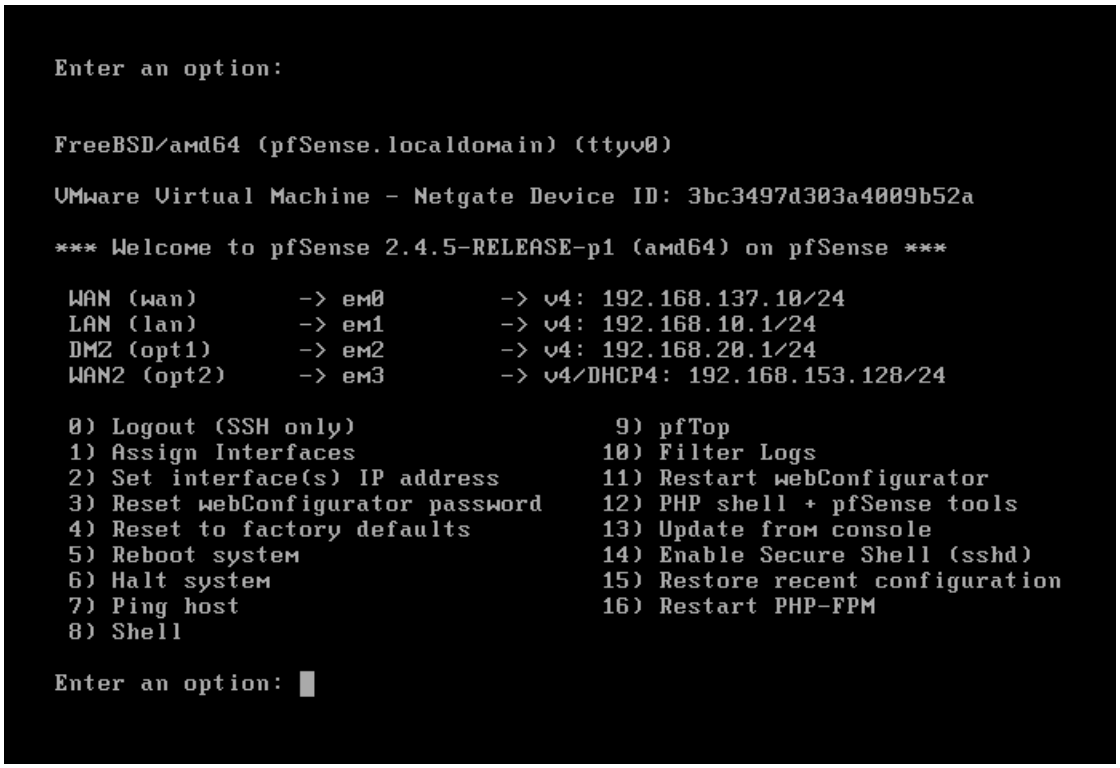
---Kết thúc bài lab---

Làm chi tiết các bước

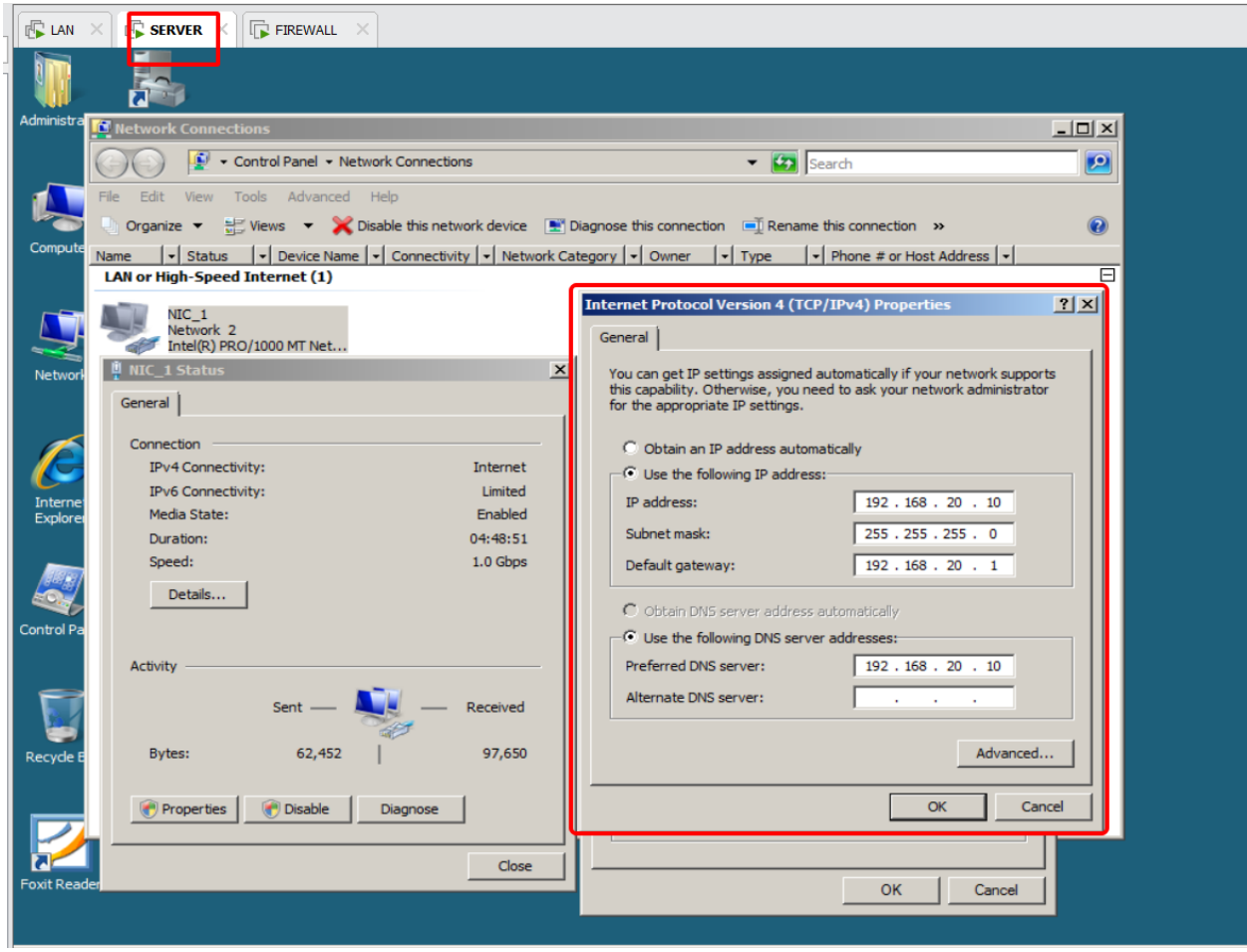
1. **Cấu hình máy LAN DMZ SERVER**
   a. **Máy LAN**



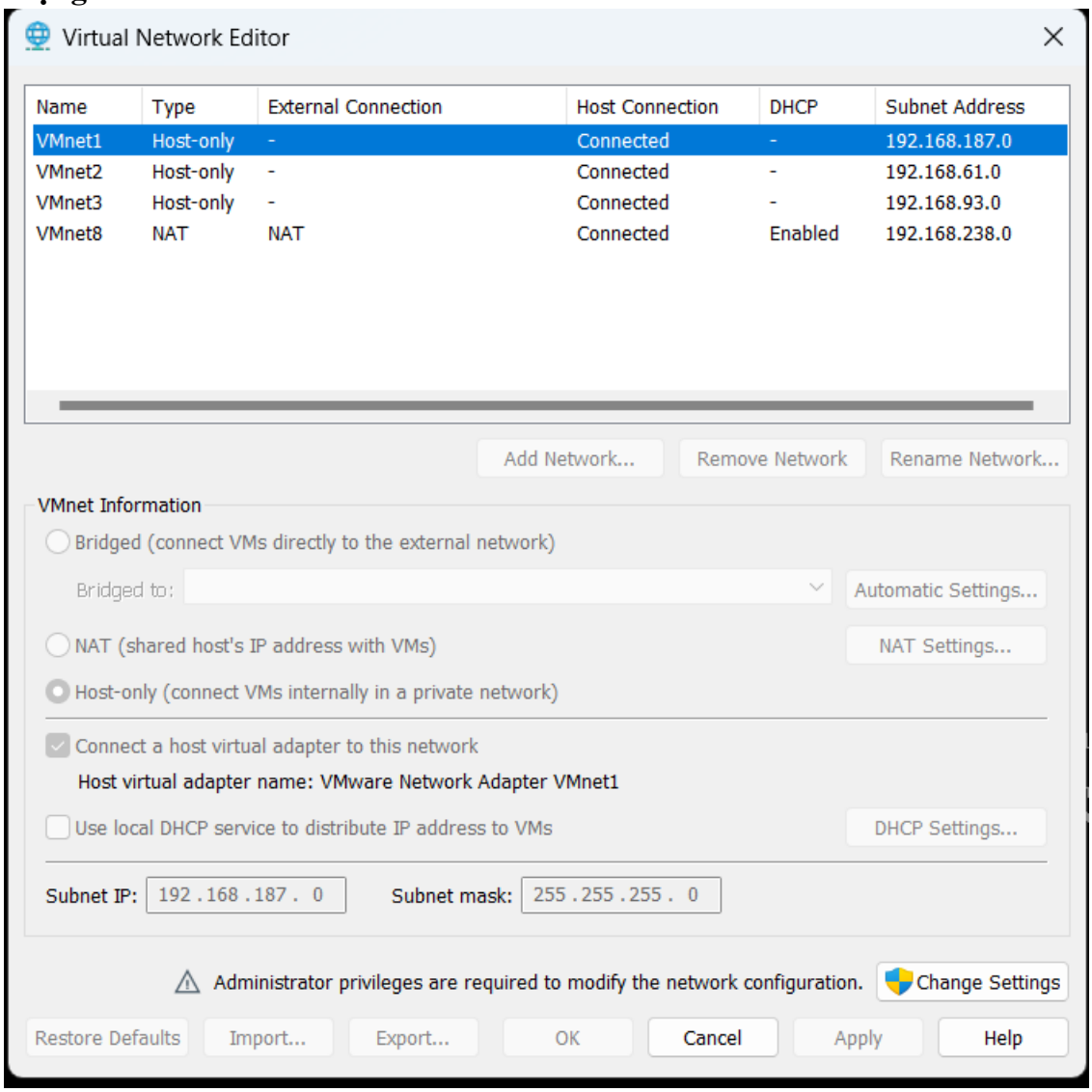
   b.
   c. **Firewall**



d. Máy server


LAN
SERVER
FIREWALL
Network Connections
Control Panel ▸ Network Connections
Search
File Edit View Tools Advanced Help
Organize Views Disable this network device Diagnose this connection Rename this connection
Name Status Device Name Connectivity Network Category Owner Type Phone # or Host Address
LAN or High-Speed Internet (1)
NIC_1
Network 2
Intel(R) PRO/1000 MT Net...
NIC_1 Status
General
Connection
IPv4 Connectivity: Internet
IPv6 Connectivity: Limited
Media State: Enabled
Duration: 04:48:51
Speed: 1.0 Gbps
Details...
Activity
Sent Received
Bytes: 62,452 97,650
Properties Disable Diagnose
Close
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 20 . 10
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 20 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 20 . 10
Alternate DNS server:
Advanced...
OK Cancel
OK Cancel

e. Mạng VMnet


Virtual Network Editor
Name Type External Connection Host Connection DHCP Subnet Address
VMnet1 Host-only - Connected - 192.168.187.0
VMnet2 Host-only - Connected - 192.168.61.0
VMnet3 Host-only - Connected - 192.168.93.0
VMnet8 NAT NAT Connected Enabled 192.168.238.0
Add Network...
Remove Network
Rename Network...
VMnet Information
Bridged (connect VMs directly to the external network)
Bridged to:
Automatic Settings...
NAT (shared host's IP address with VMs)
NAT Settings...
Host-only (connect VMs internally in a private network)
Connect a host virtual adapter to this network
Host virtual adapter name: VMware Network Adapter VMnet1
Use local DHCP service to distribute IP address to VMs
DHCP Settings...
Subnet IP: 192 . 168 . 187 . 0
Subnet mask: 255 . 255 . 255 . 0
Administrator privileges are required to modify the network configuration.
Change Settings
Restore Defaults
Import...
Export...
OK
Cancel
Apply
Help