BÀI THỰC HÀNH SỐ 7

Môn: MẬT MÃ VÀ AN NINH MẠNG

-o0o-

**CHẾ QUANG HUY – 1812340**

* + 1. **MỤC TIÊU**

Mục tiêu của bài thực hành này cung cấp kiến thức và kỹ năng cơ bản liên quan đến bảo mật hệ thống CNTT thông qua việc tìm hiểu và triển khai bức tường lửa với mã nguồn mở pfSense.

* + 1. **CHUẨN BỊ TRƯỚC KHI THỰC HIỆN BÀI THỰC HÀNH**

Các trang thiết bị và phiên bản phần mềm sử dụng trong bài thực hành:

* 01 máy tính truy cập đến Internet.
* Hệ điều hành: MS Windows 7/10.
* Virtual Box.
* [Tập tin ISO của pfSense](https://www.pfsense.org/download/).

**Tài liệu tham khảo**

# [1]. [VirtualBox Networking](https://www.virtualbox.org/manual/ch06.html)

# [2].

# <https://docs.netgate.com/pfsense/en/latest/>

# [3]. <https://anninhmang.edu.vn/huong-dan-cai-dat-firewall-pfsense/>

# [4]. <https://www.slideshare.net/NetgateUSA/creating-a-dmz-pfsense-hangout-january-2016>

[5]. <https://docs.netgate.com/pfsense/en/latest/recipes/example-basic-configuration.html>

* + 1. **CÁCH THỨC VÀ HẠN CHÓT NỘP BÀI**
* Sinh viên cần trả lời thông tin(văn bản, hình ảnh) vào các phần yêu cầu trong bài thực hành vào lưu lại thành tập tin lab7.doc
* Thời gian làm bài là 14 ngày.
  + 1. **NỘI DUNG THỰC HIỆN**
       - 1. **Đồ hình mạng triển khai**

*Diagram

Description automatically generated*

1. *Thiết lập WAN*

* Tìm hiểu chế độ Bridged trong [1].
* Dự kiến cấu hình giao diện WAN ở chế độ Bridged.

1. *Thiết lập LAN, DMZ*

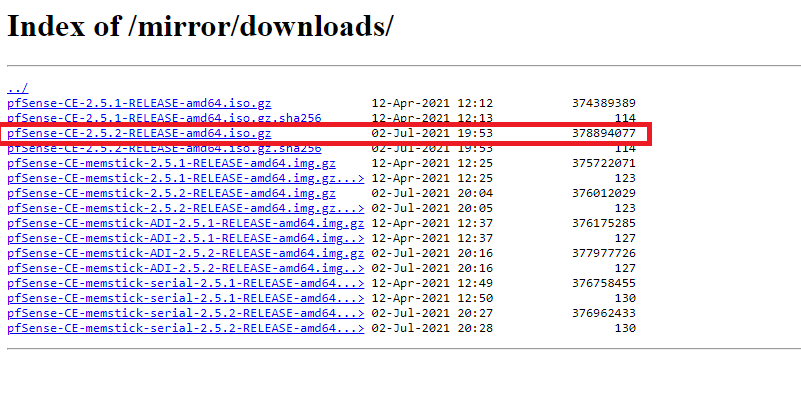
* Tìm hiểu chế độ Host-Only trong [1].
* Thiết lập LAN với Host-Only Network #1 với DHCP Disable.
* Thiết lập mạng DMZ với Host-Only Network #2 với DHCP Disable.
  + - * 1. **Tìm hiểu và cài đặt pfSense**

1. *pfSense là gì*

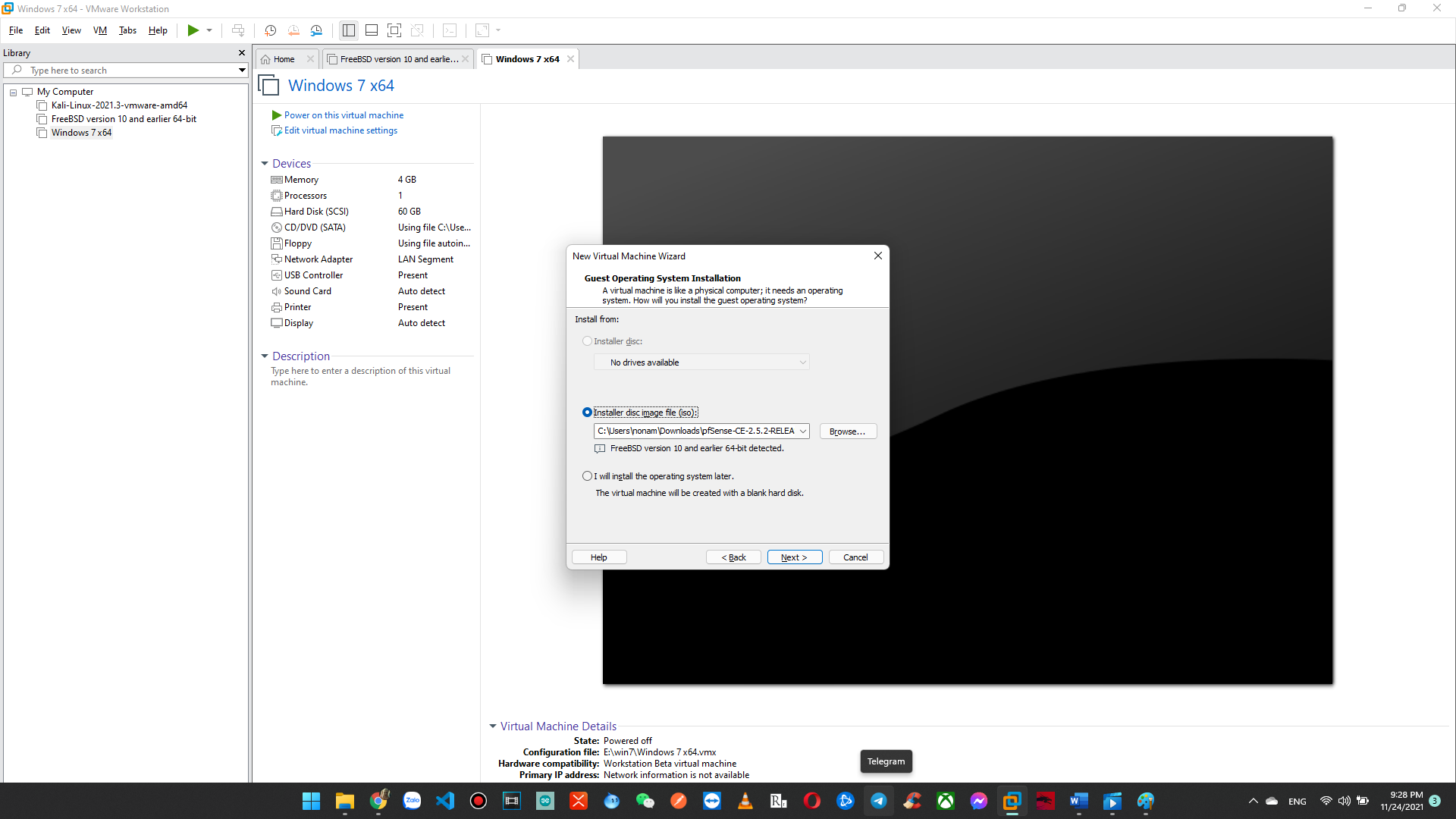
PfSense là phần mềm định tuyến, tường lửa mã nguồn mã nguồn mở miễn phí, được xây dựng dựa trên hệ điều hành FreeBSD. PfSense có thể được cài đặt trên hầu hết các phần cứng và hệ thống nhúng. Pfsense cung cấp giao diện quản trị web giúp người quản trị dễ dàng sử dụng và kiểm soát hệ thống.

1. *Hãy cho biết các bước cài đặt pfSense trên Virtual Box bao gồm vài hình ảnh:*

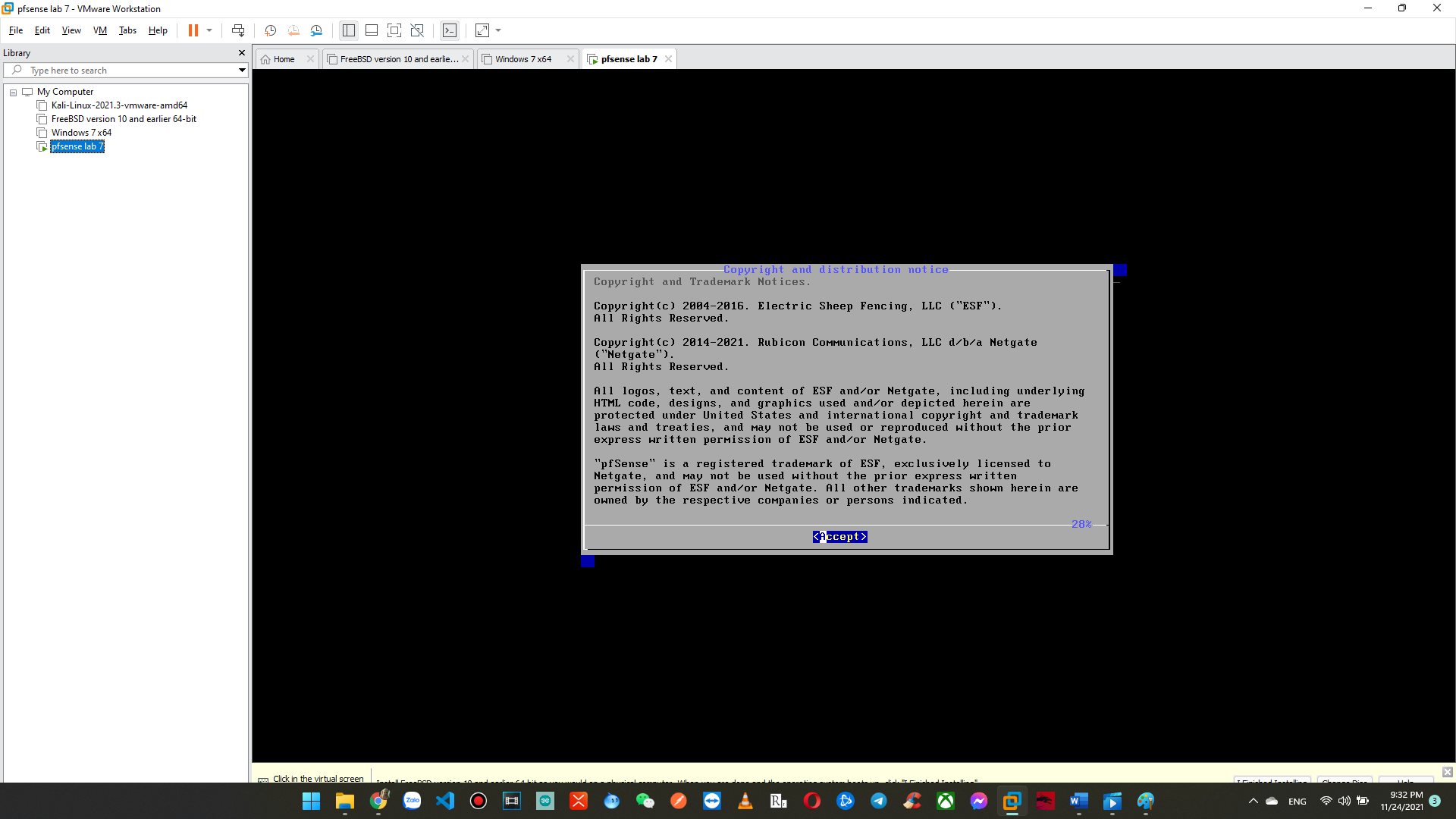
Donwload Pfsense 2.5.2 tại địa chỉ <https://sgpfiles.netgate.com/mirror/downloads/> . Chọn file thứ 3.

**

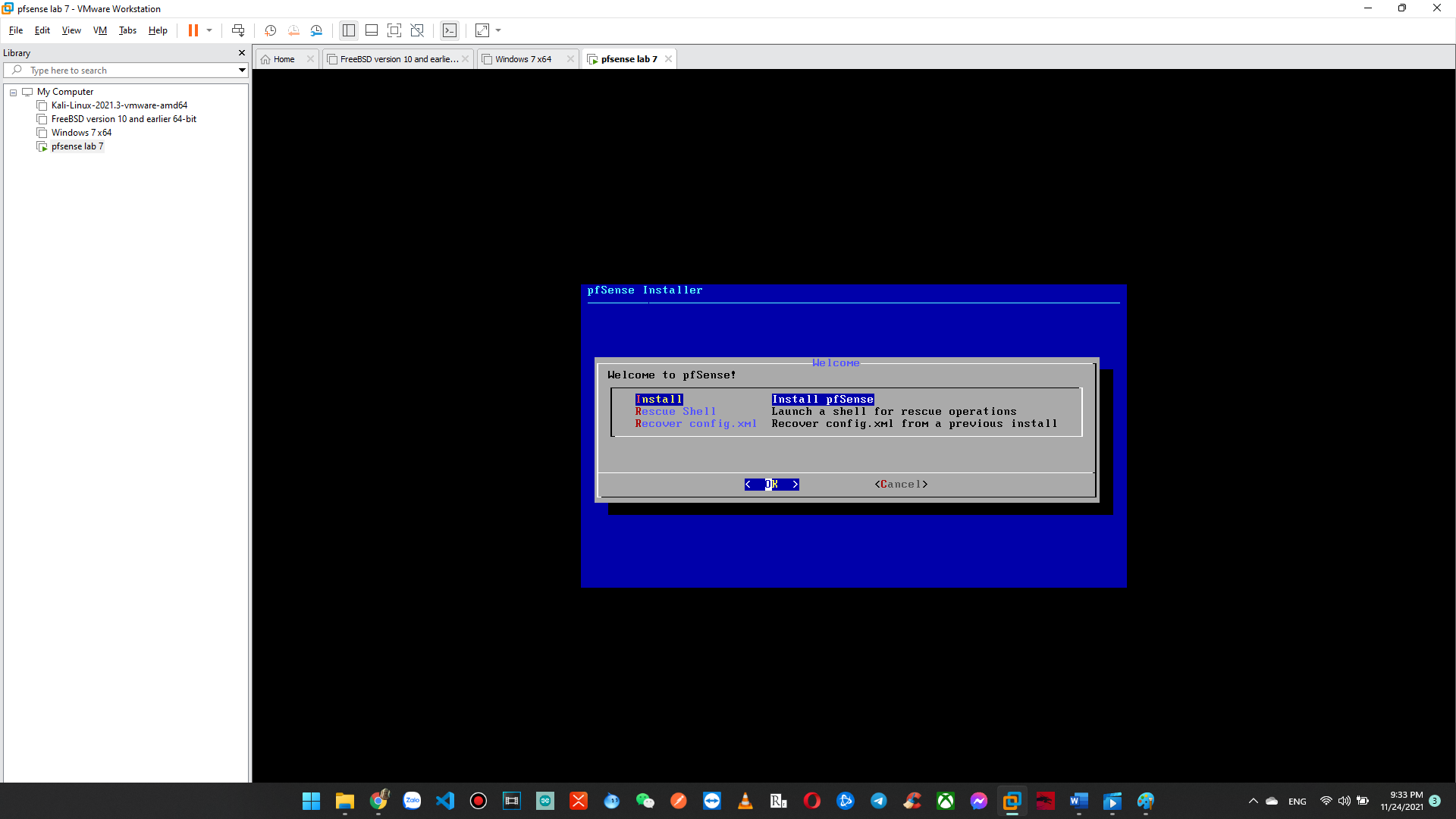
Cài đặt Pfsense trên máy ảo VMWare, ta chọn đường dẫn tới file cài đặt vừa tải về.



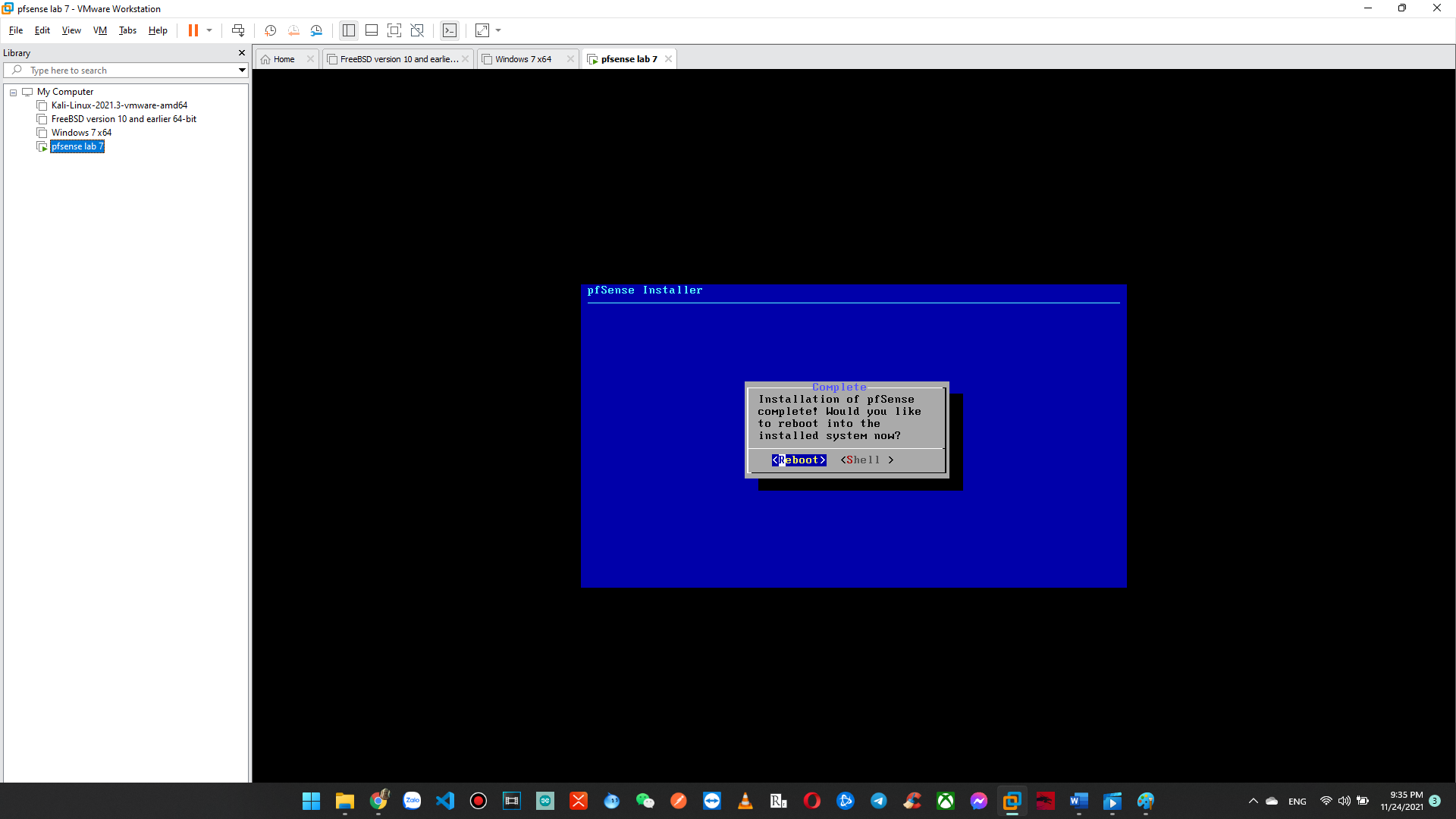
Khởi động máy ảo và tiến hành cài đặt.



Chọn Install



Tiếp tục chọn sử dụng các thiết lập mặc định. Đợi hệ thống cài đặt xong ta chọn reboot.

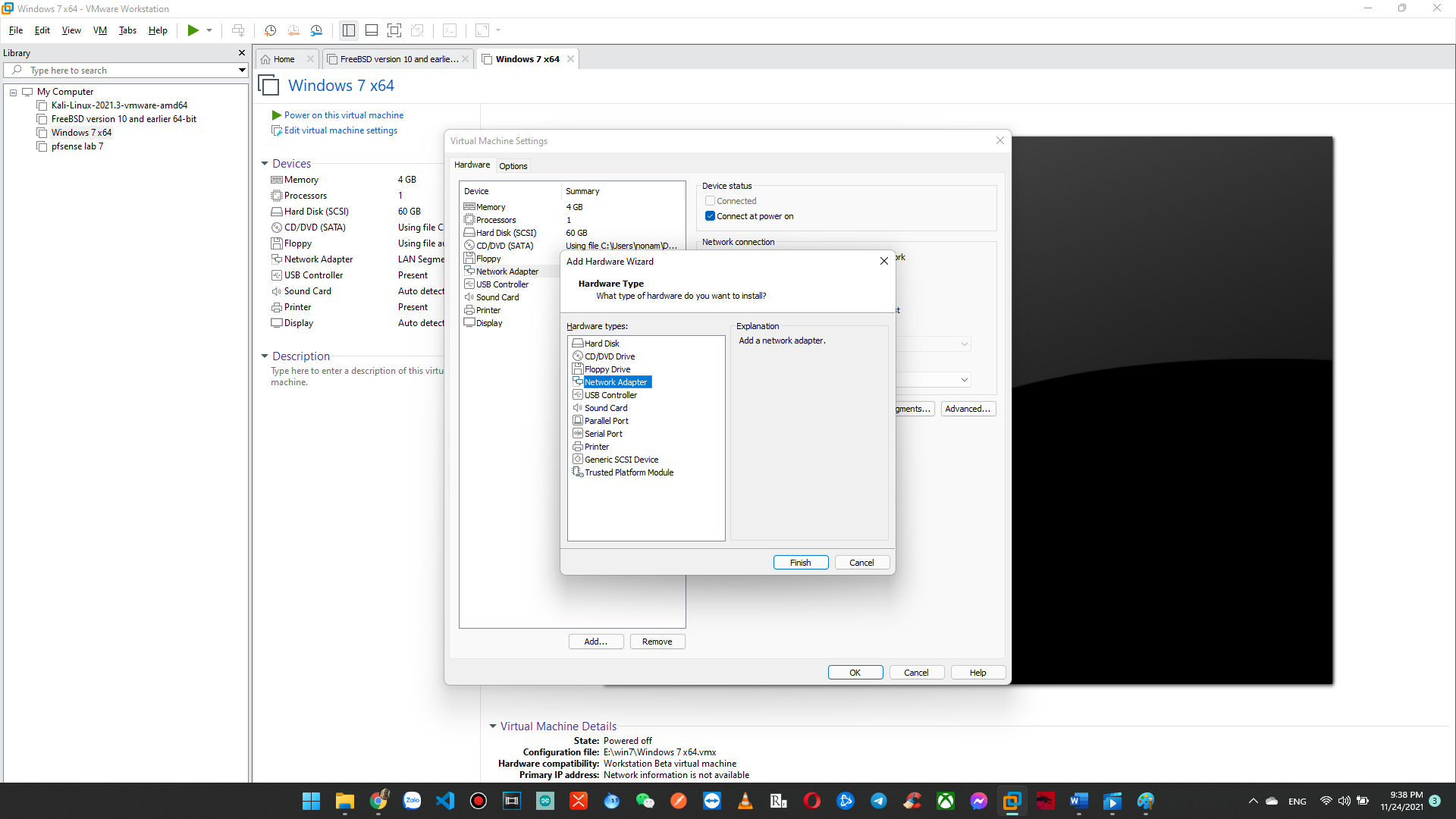


* + - * 1. **Cấu hình *pfSense*, máy trạm, máy chủ**

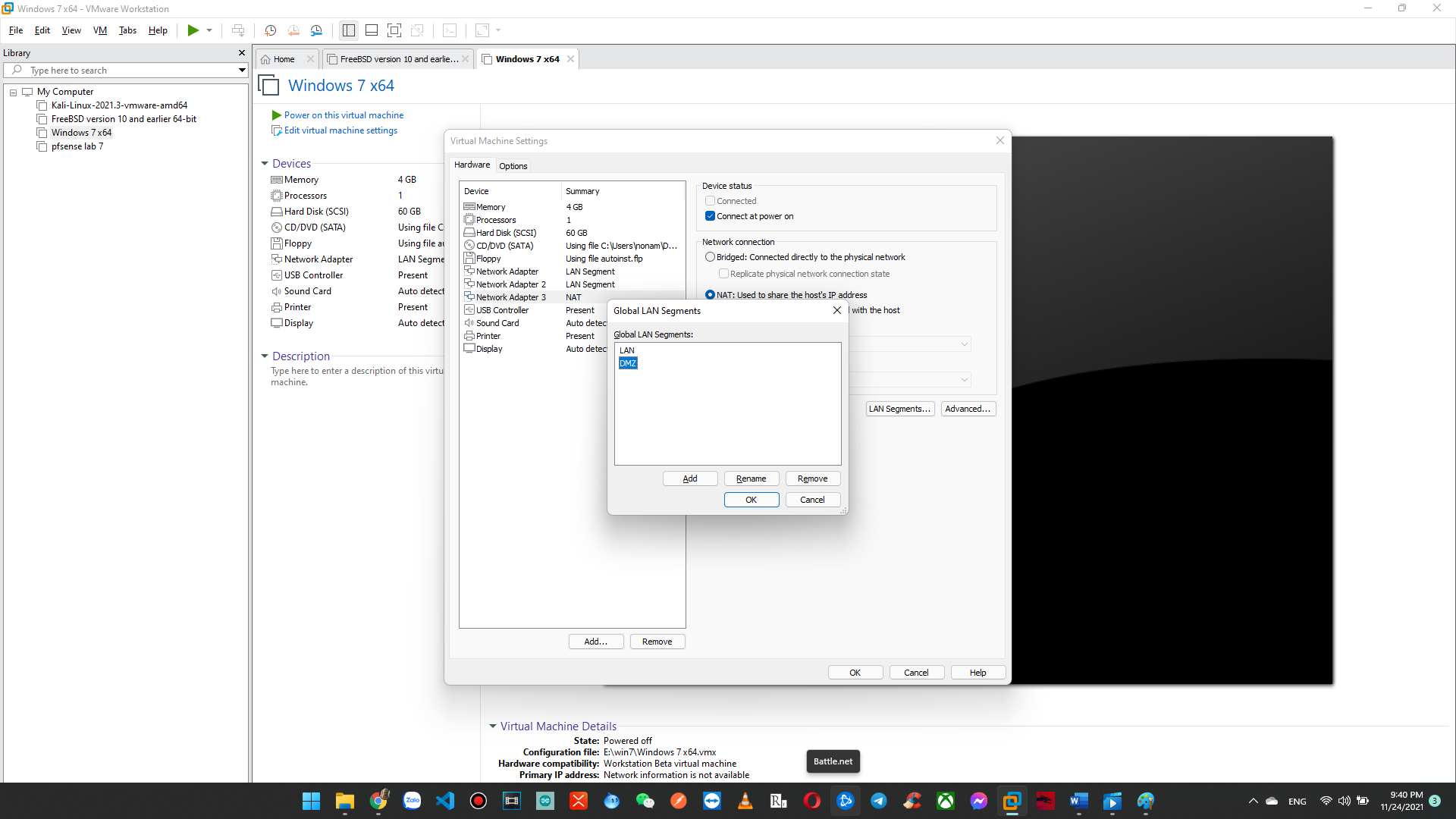
1. *Cấu hình mạng pfSense*

* Cấu hình giao diện WAN chế độ Bridged với giao diện mạng đi Internet

**Chọn Add > Network Adapter để thêm 2 card mạng với card mạng sẵn chúng ta sẽ có 3 card mạng.**

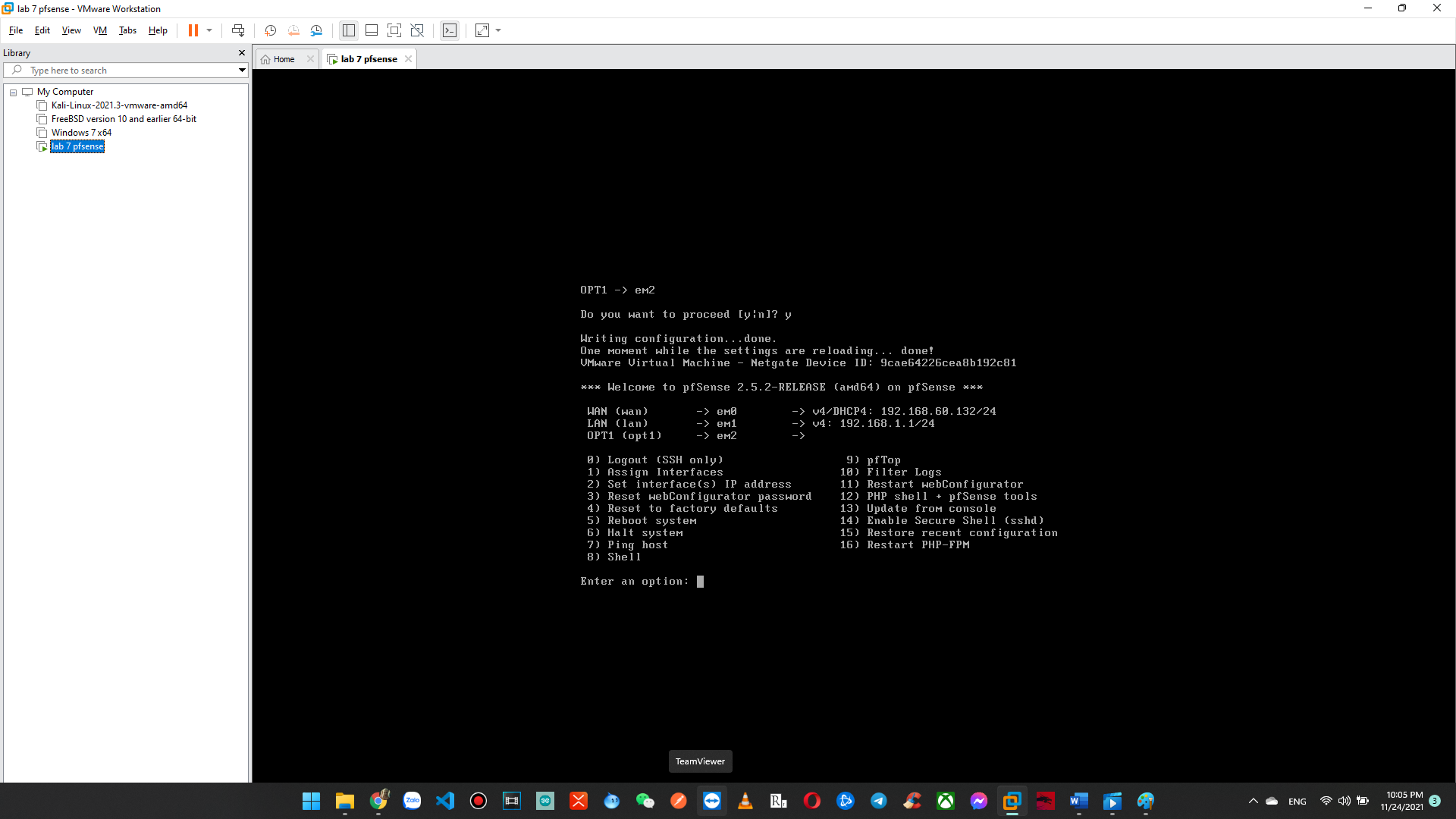


**Chọn LAN Segments tạo 2 card mạng đặt tên là LAN (**Host-Only Nework #1) **và DMZ (**Host-Only Nework #2)**.**

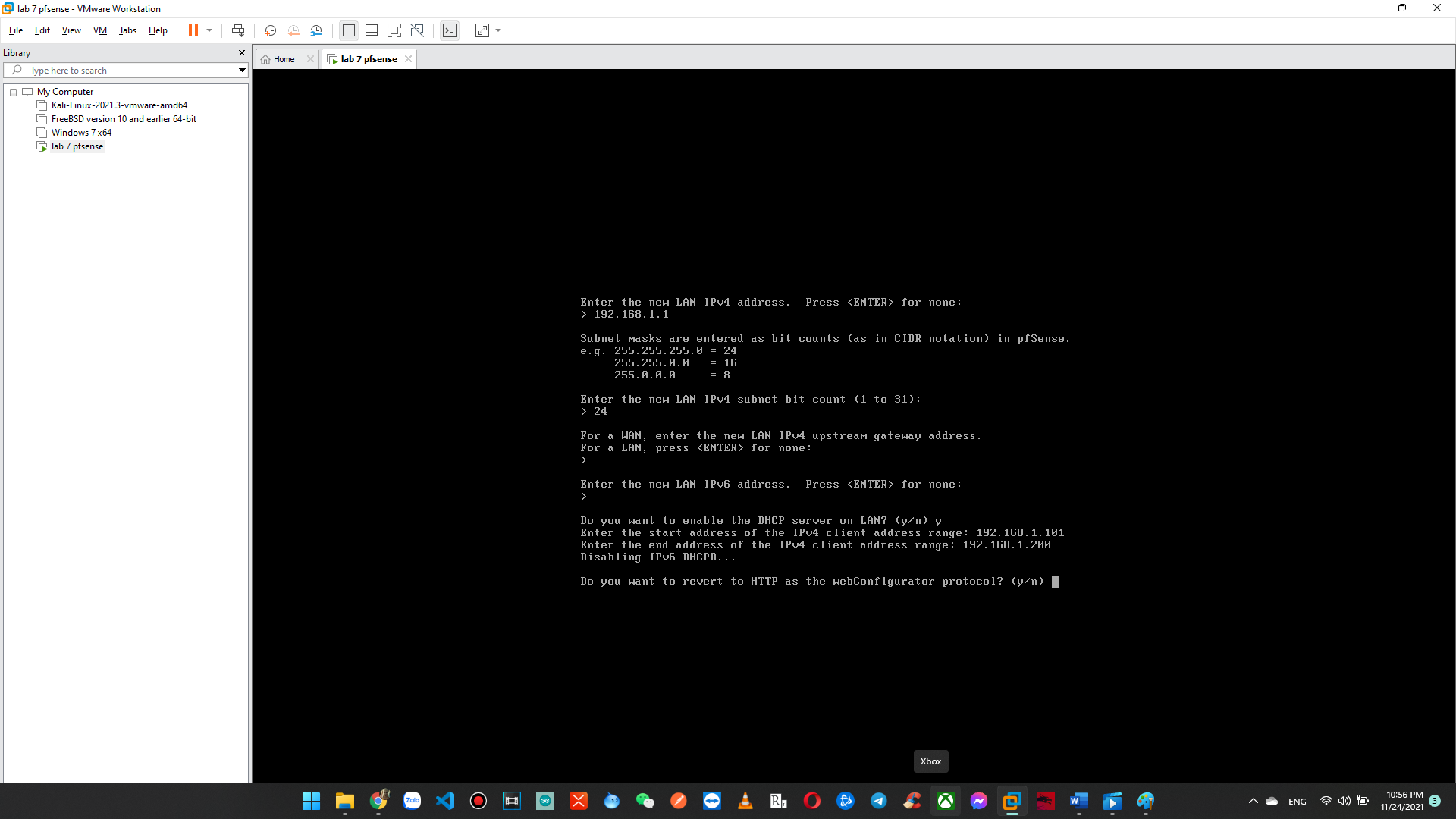


**Network Adapter ta chọn Bridged. Network Adapter 2 ta chọn LAN. Network Adapter 2 ta chọn DMZ.**

**Khởi động máy chủ Pfsense. Chọn 1 (Assign Interfaces ). Gán em0 với WAN , em1 với LAN và OPT1 với em2.**

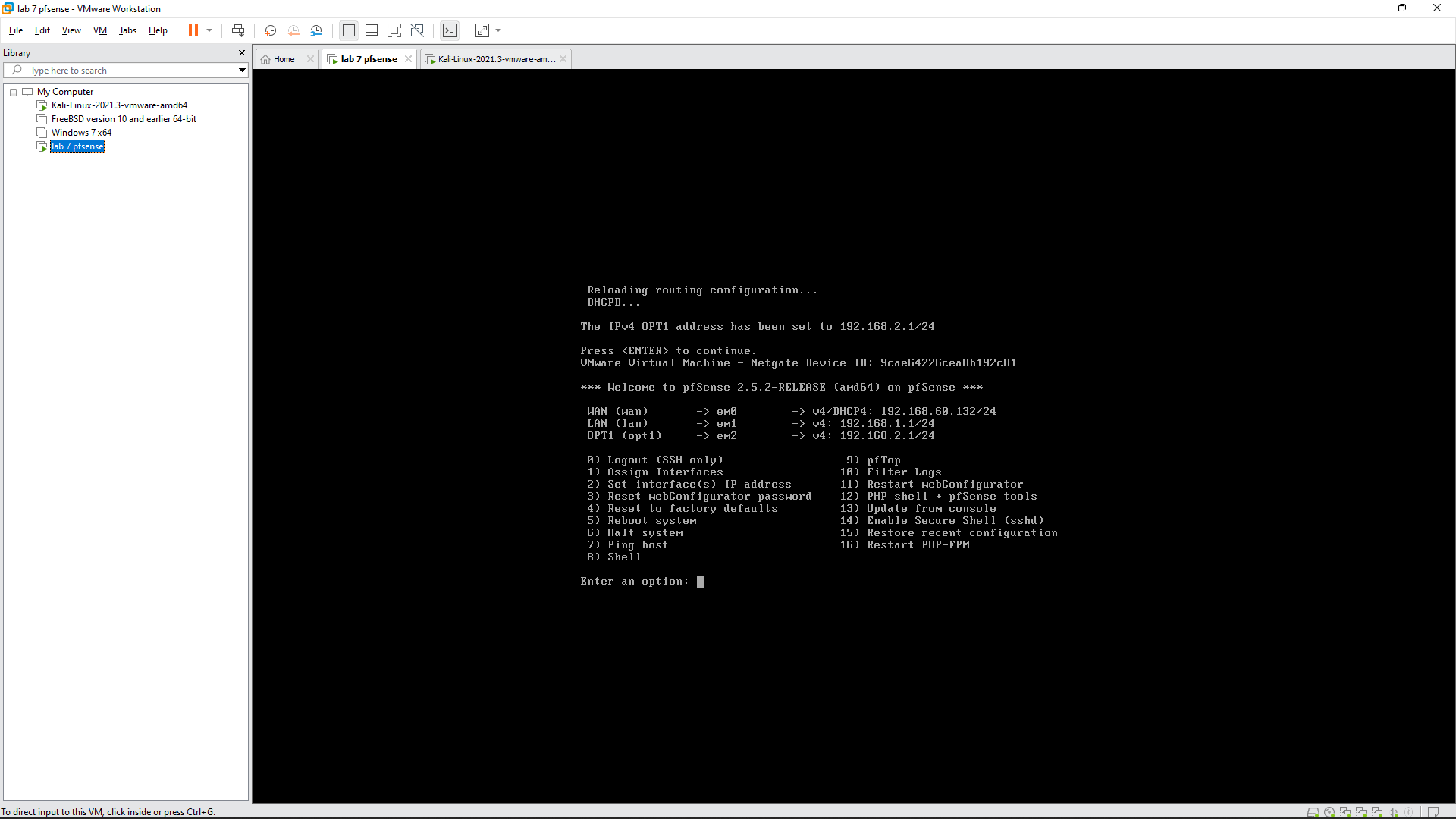


* Cấu hình giao diện LAN thuộc Host-Only Nework #1 với IP tĩnh.
* Chọn 2 ( set interfaces IP address ).
* Sau đó chọn card em1 ( nhấn 2 để chọn ).
* Nhập địa chỉ IP tĩnh 192.168.1.1
* Subnet : 24
* DHCP server on LAN, chọn yes.
* IP range : 192.168.1.101 – 192.168.1.200
* Do you want to revert HTTP as webConfigurator protocal ? Chọn yes.

- Cấu hình giao diện DMZ thuộc Host-Only Nework #2 với IP tĩnh.

* Chọn 2 ( set interfaces IP address ).
* Sau đó chọn card em2 ( nhấn 3 để chọn ).
* Nhập địa chỉ IP tĩnh 192.168.2.1
* Subnet : 24
* DHCP server on LAN, chọn no.
* IP range : 192.168.2.101 – 192.168.2.200
* Cấu hình DHCP Server cho mạng cục bộ (Host-Only Nework #1)

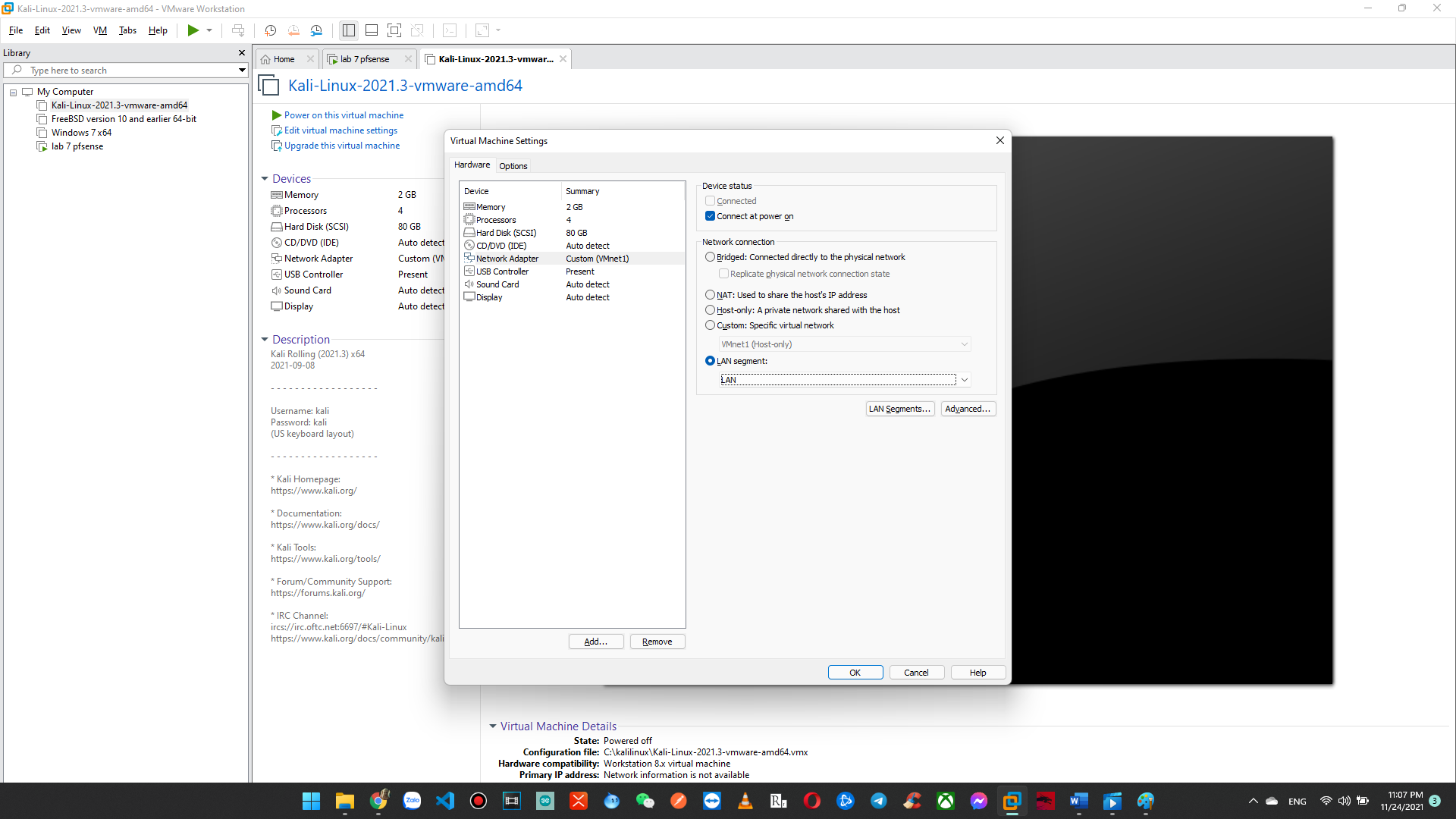
Phần cấu hình DHCP Server đã được cài đặt luôn trong quá trình thiết lập IP tĩnh cho giao diện LAN ở phần trên. Sau khi hoàn tất cấu hình ta được như sau.



1. *Cấu hình mạng máy trạm, kiểm tra kết nối mạng*

* Cấu hình mạng máy trạm (Kali Linux) thuộc Host-Only Nework #1 với IP động.

Cài đặt Network Adapter cho máy Kali-Linux. Chọn Network Adapter, ở mục LAN segment ta chọn LAN.

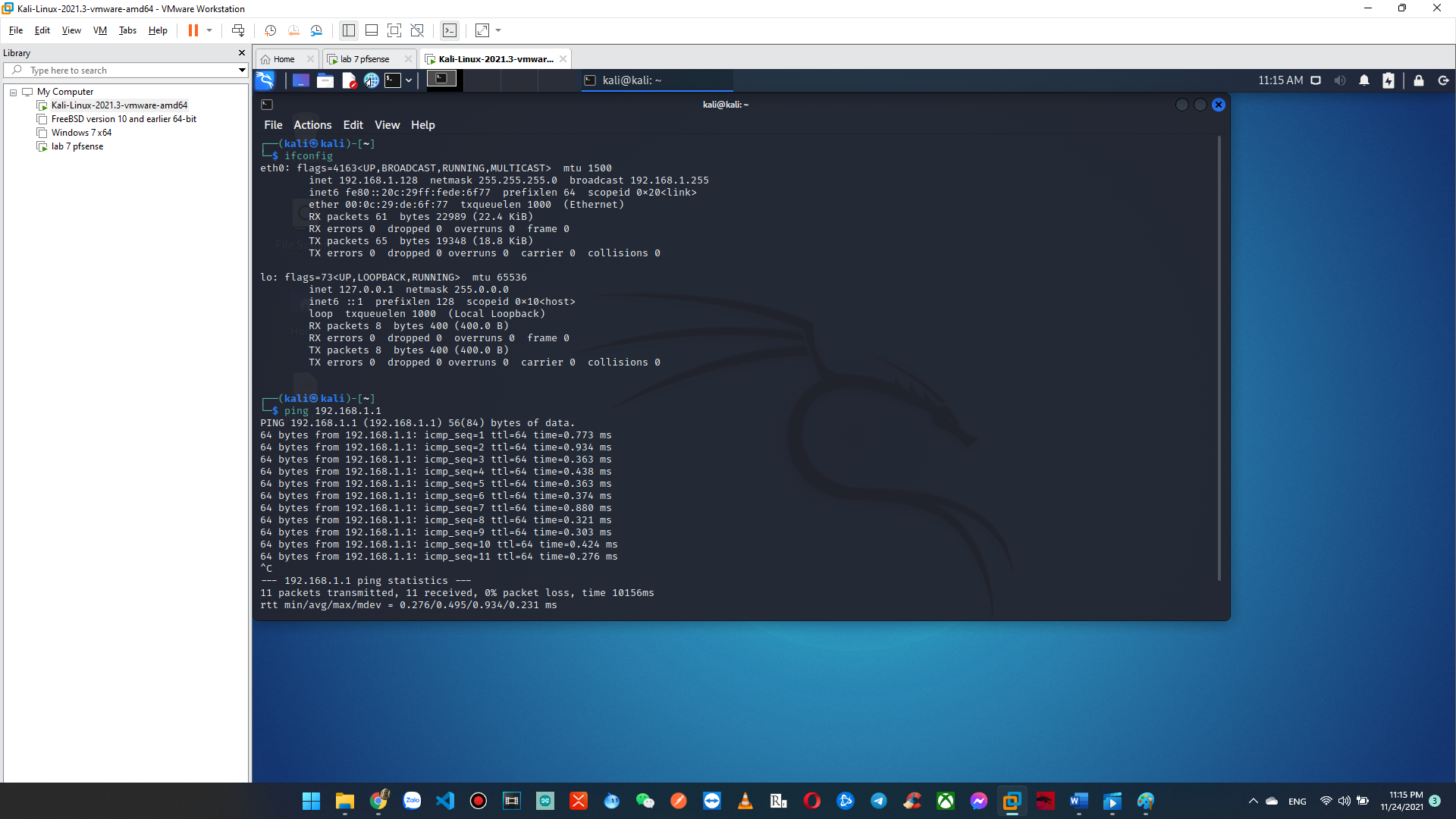


* Kiểm tra kết nối mạng từ máy trạm đến *pfSense*

Dùng lệnh ifconfig ta kiểm tra IP được DHCP server cấp cho máy Kali Linux là 192.168.1.128.

Ping tới địa chỉ 192.168.1.1 ta nhận được phản hồi như hình.

Như vậy là việc kết nối đã thành công.



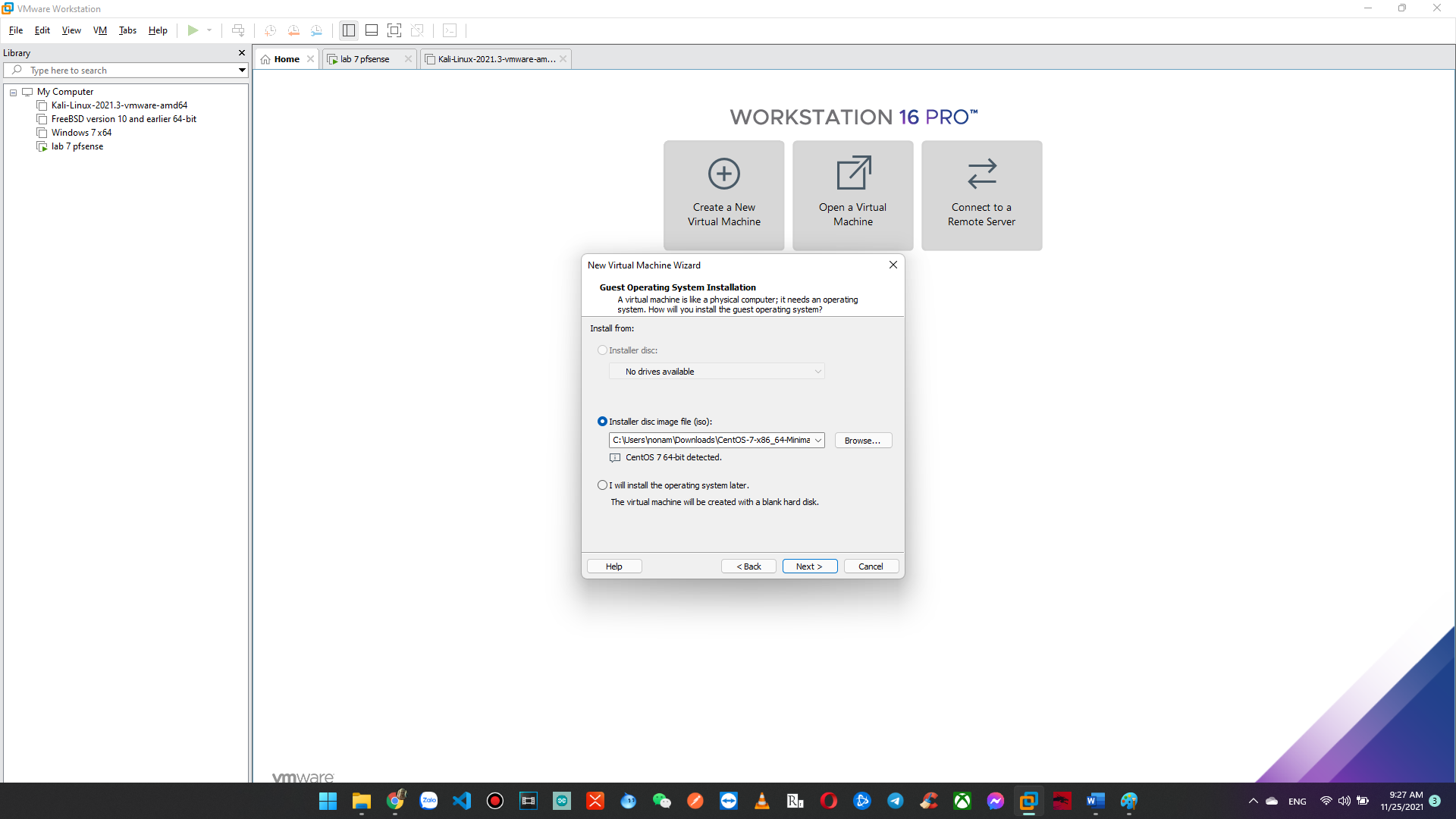
1. *Cấu hình mạng máy chủ, kiểm tra kết nối mạng*

* Cấu hình mạng máy chủ (CentOS7) thuộc Host-Only Nework #2 với IP tĩnh

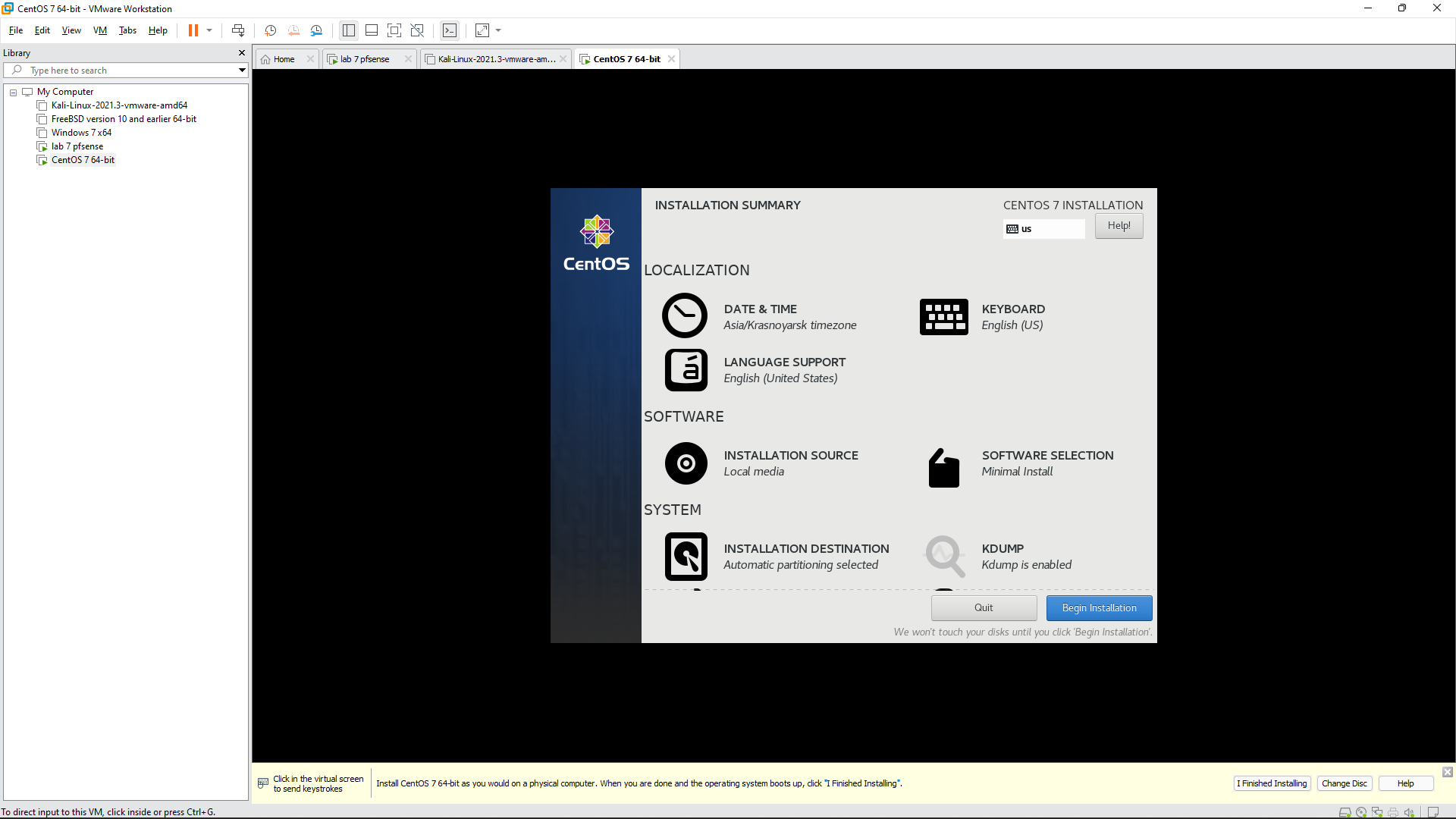
**Download file cài đặt CentOS 7 tại :**

<http://mirrors.cloudfly.vn/centos/7.9.2009/isos/x86_64/>

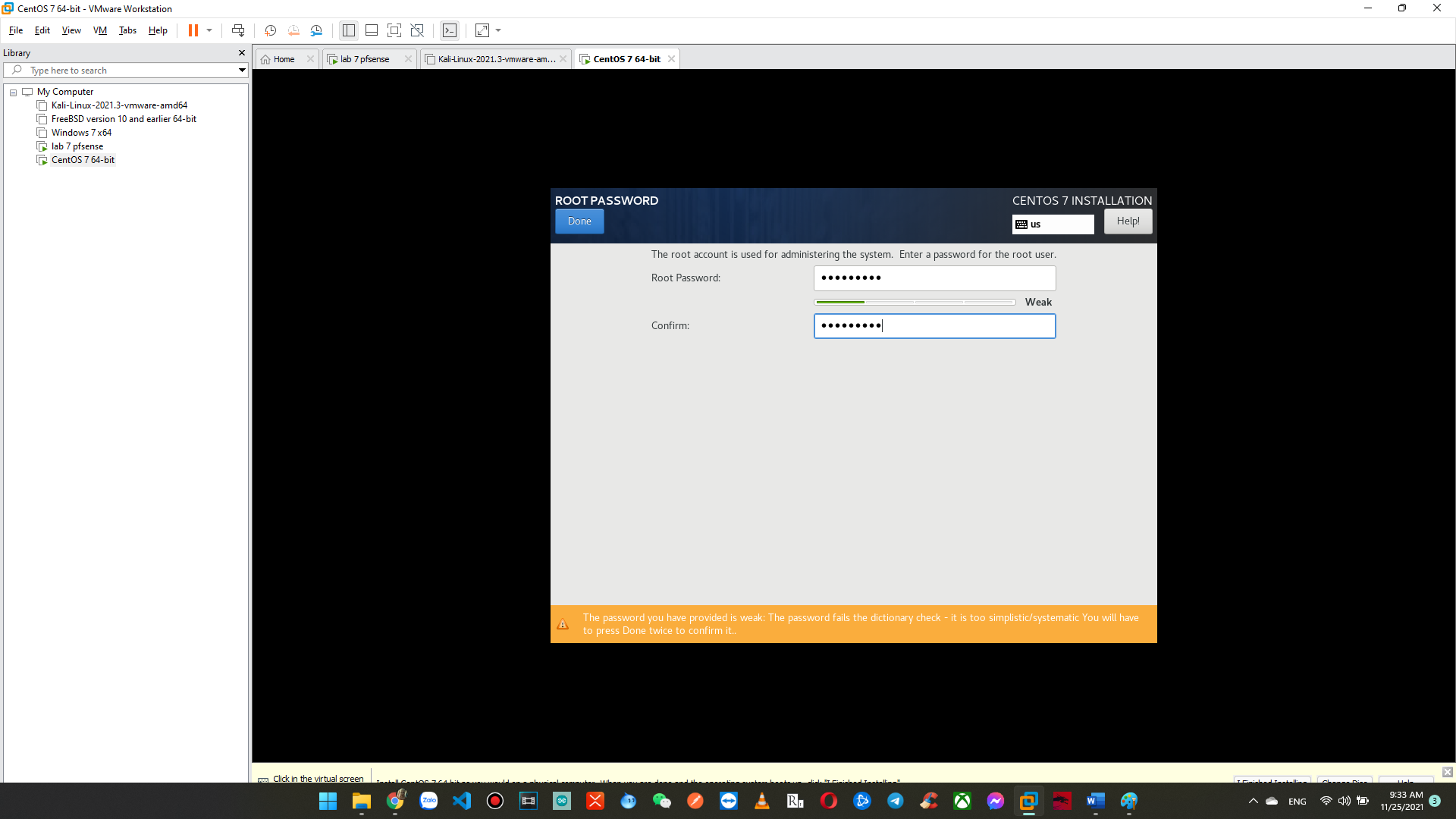
**Tiến hành cài đặt CentOS 7, chọn đường dẫn đến file cài đặt vừa tải về.**



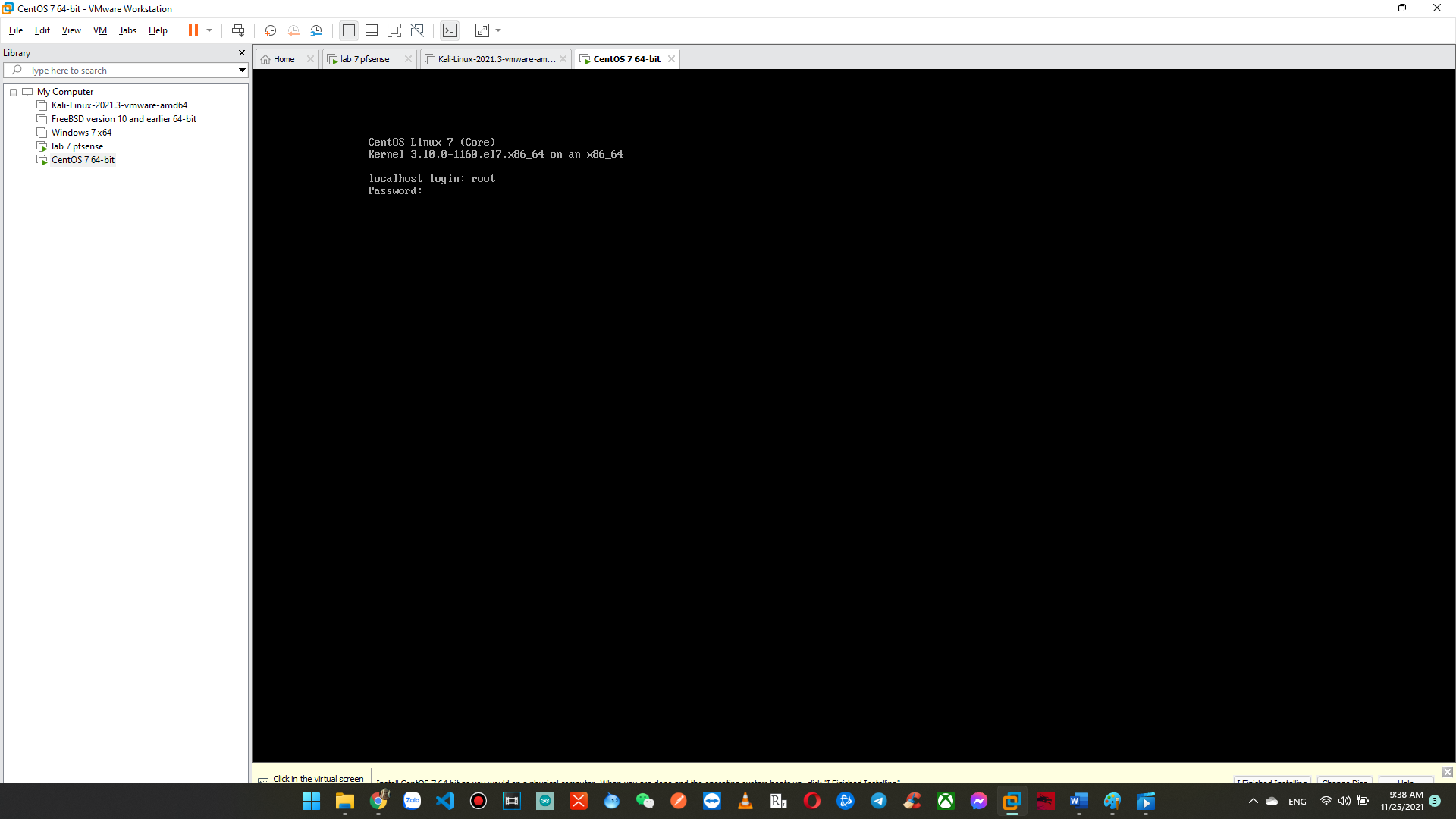
**Chọn Begin Installation.**



**Thiết lập root password**



**Sau khi cài đặt xong, chọn reboot. Sau đó đăng nhập với locahost login là root password được tạo trong quá trình cài đặt.**



**Thực hiện :**

* **cd /etc/sysconfig/network-scripts/**
* **vi ifcfg-ens33**

**Sau đó tiến hành chỉnh sửa như sau:**

* **Sửa BOOTPROTOL : static**
* **Thêm vào cuối:**

**IPADDR=192.168.2.111**

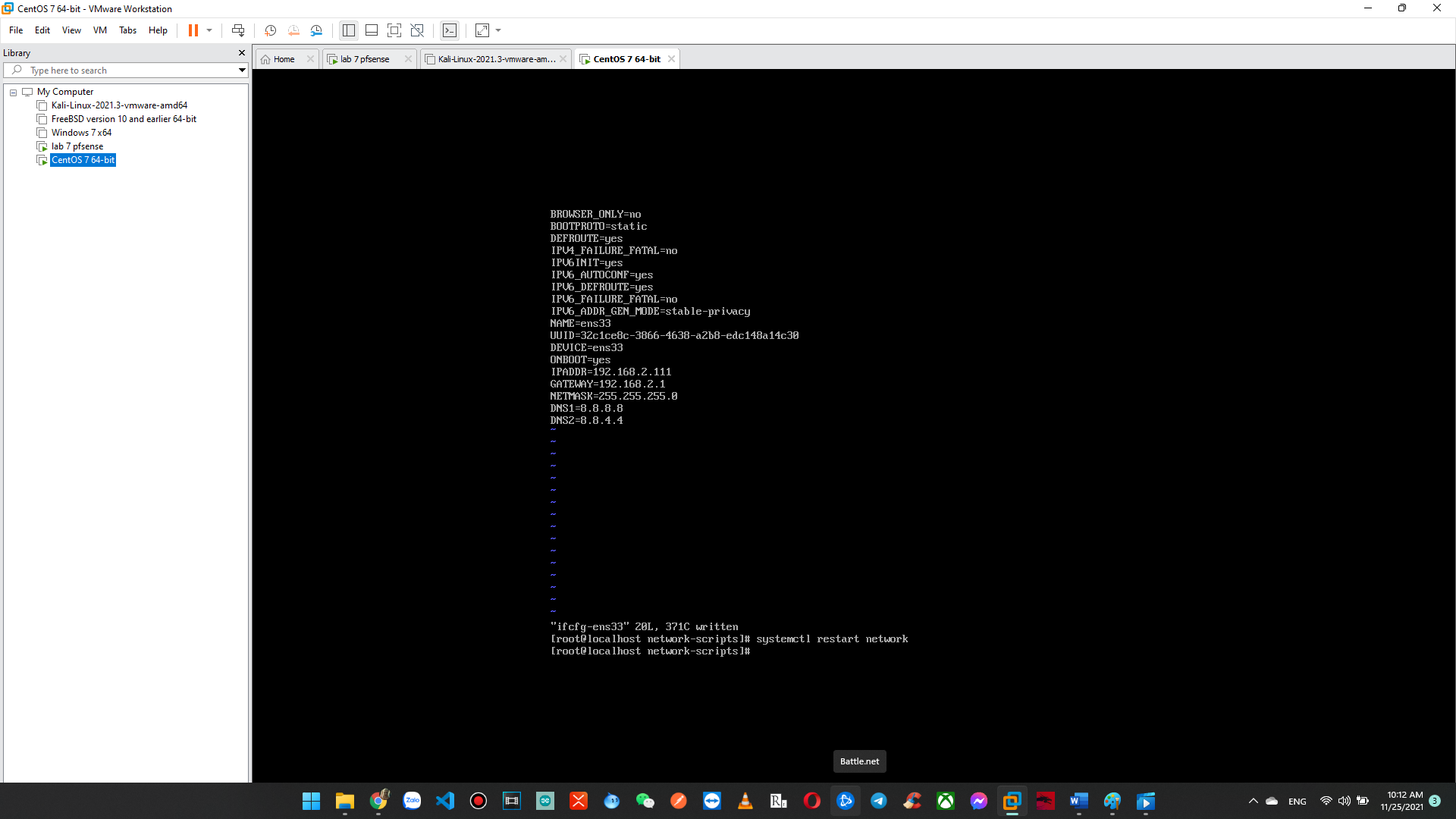
**GATEWAY=192.168.2.1**

**NETMASK=255.255.255.0**

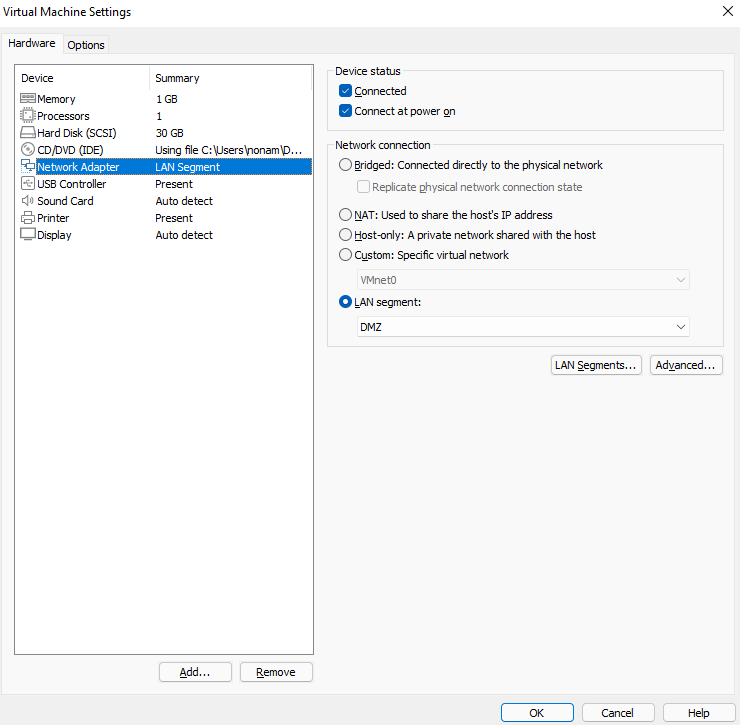
**DNS1=8.8.8.8**

**DNS2=8.8.4.4**

**Sau đó lưu lại và restart ( systemctl restart network ).**



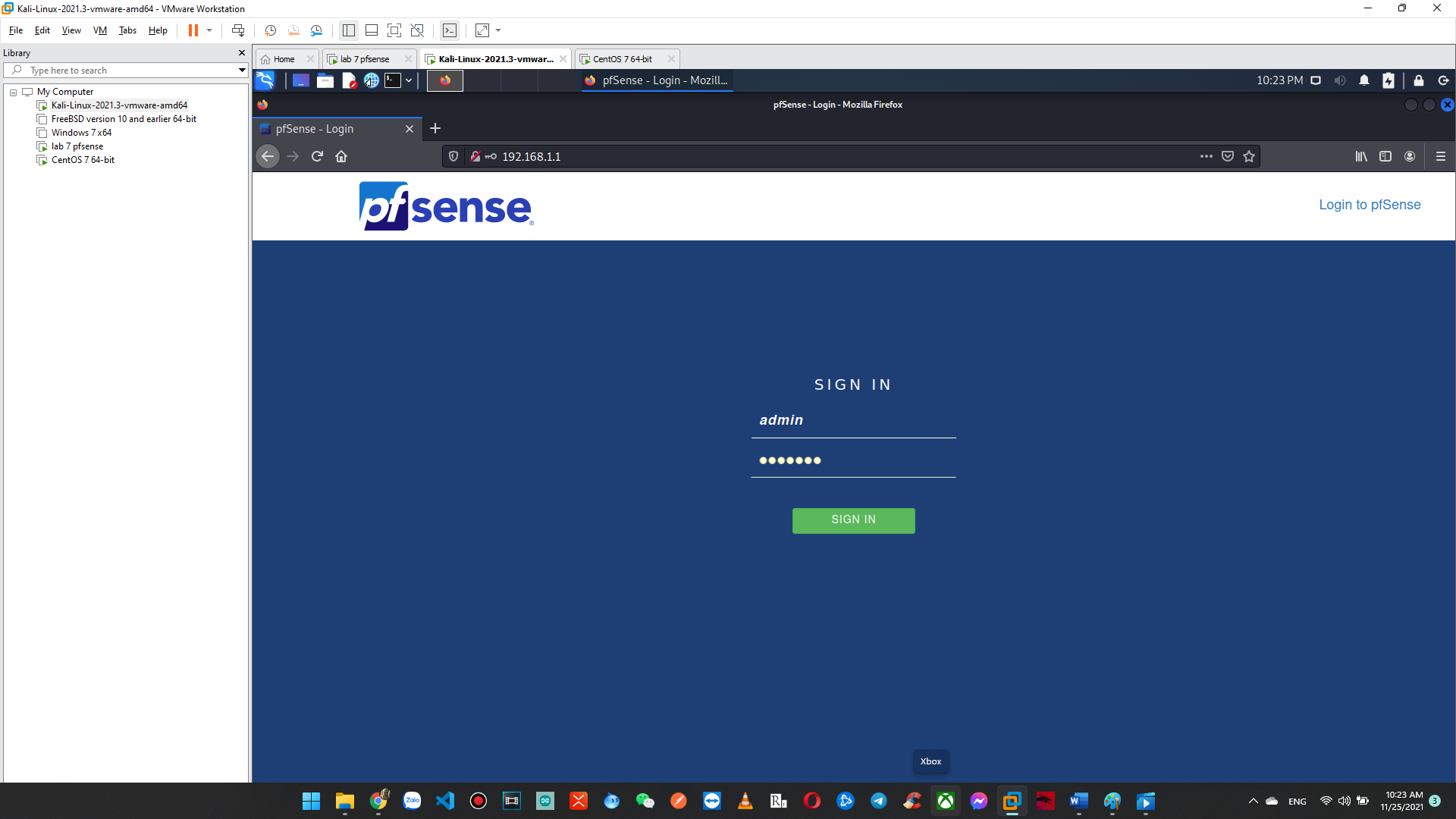
**Ta tắt máy CentOS đi và cài đặt card mạng như hình bên dưới. LAN Segment ta cho DMZ.**



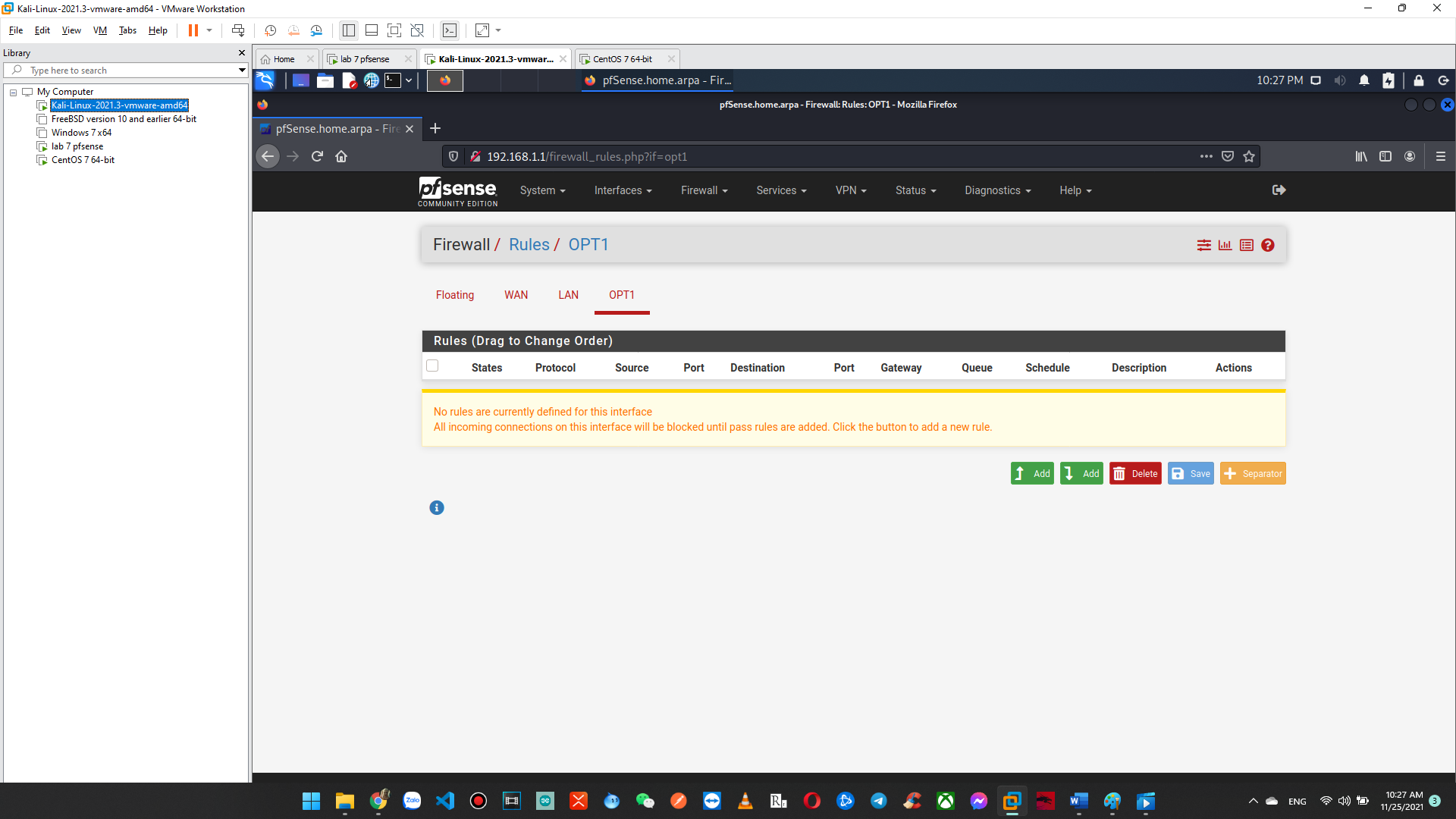
**Bấm OK và start lại máy CentOS**

* Kiểm tra kết nối mạng từ máy chủ đến pfSense

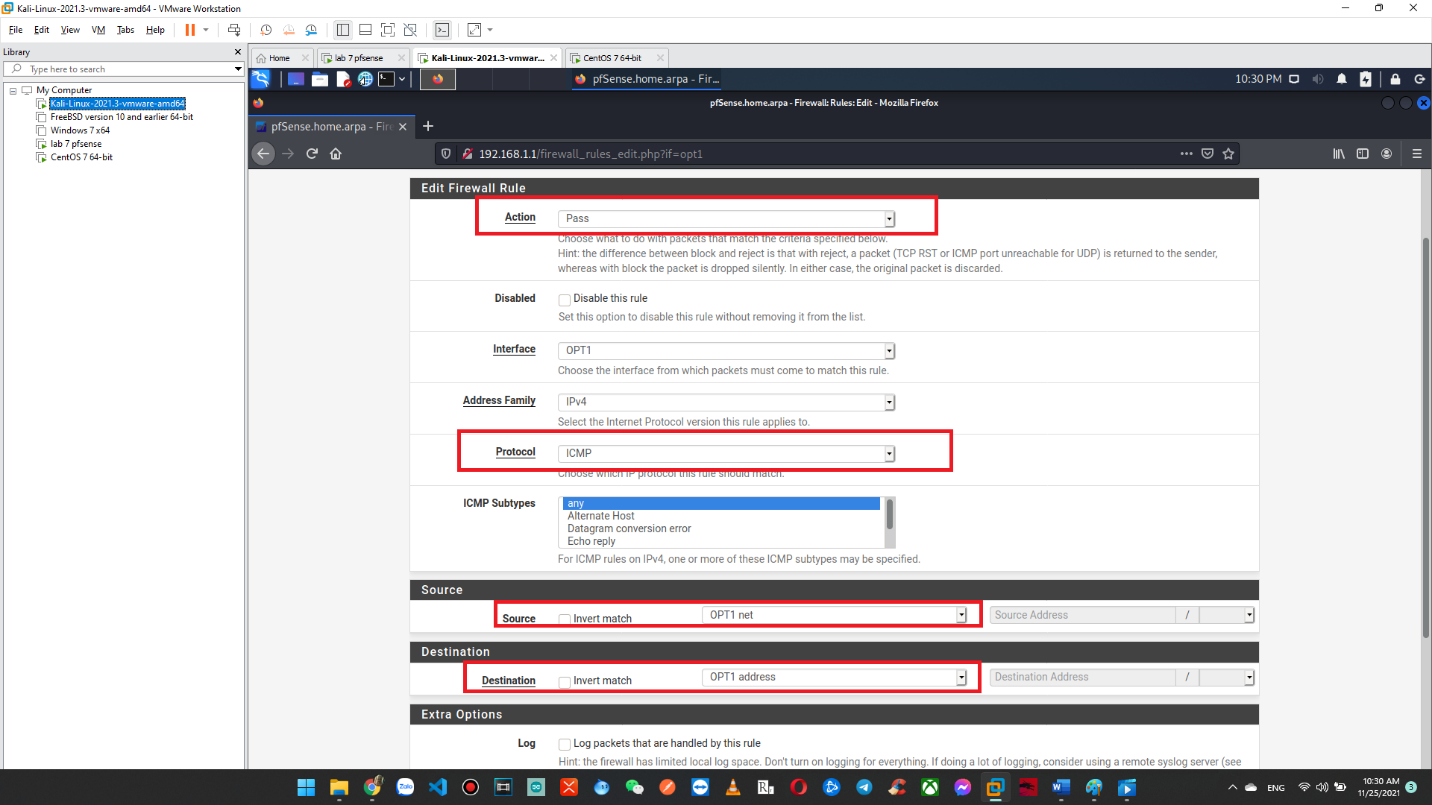
**Quay lại máy kali linux , truy cập địa chỉ 192.168.1.1 đăng nhập pfsense để thiết lập rules cho DMZ. Đăng nhập với username và password mặc định là (admin – pfsense).**



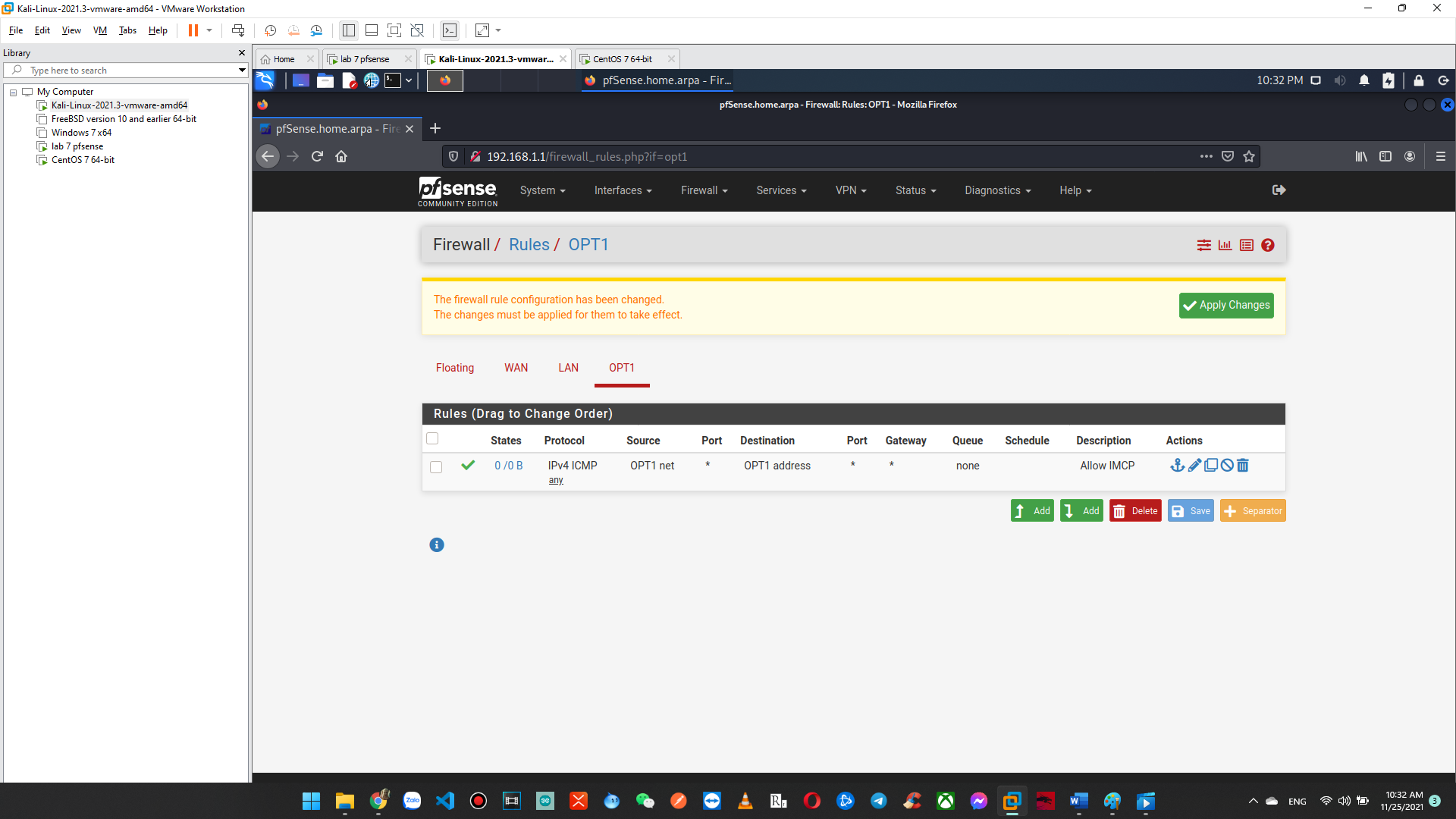
**Thiết lập rules cho OPT1 , ta chọn nút add.**



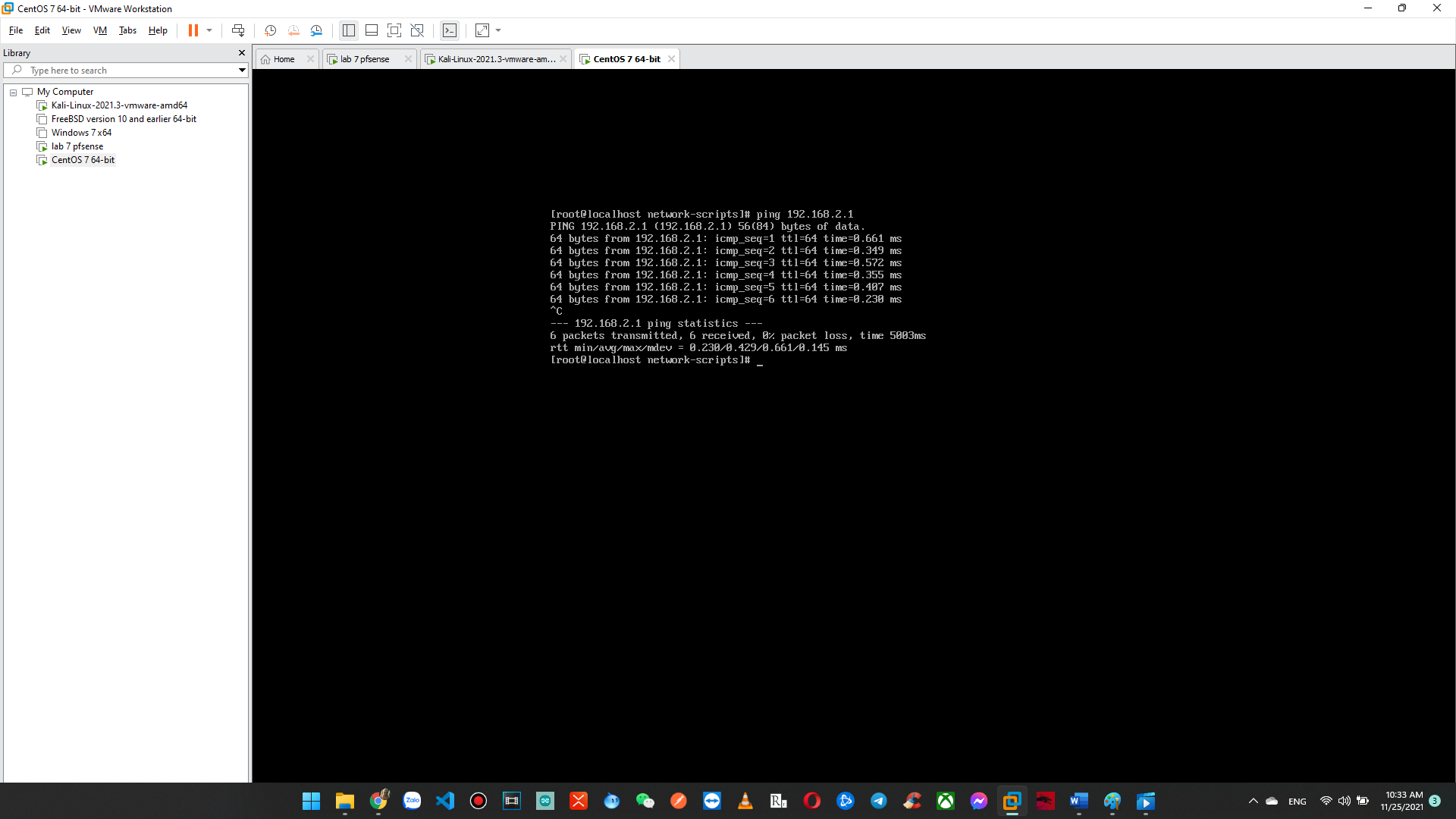
**Thiết lập cho phép giao thức giao thức ICMP như hình và bấm lưu.**



**Chọn “Apply Changes”**

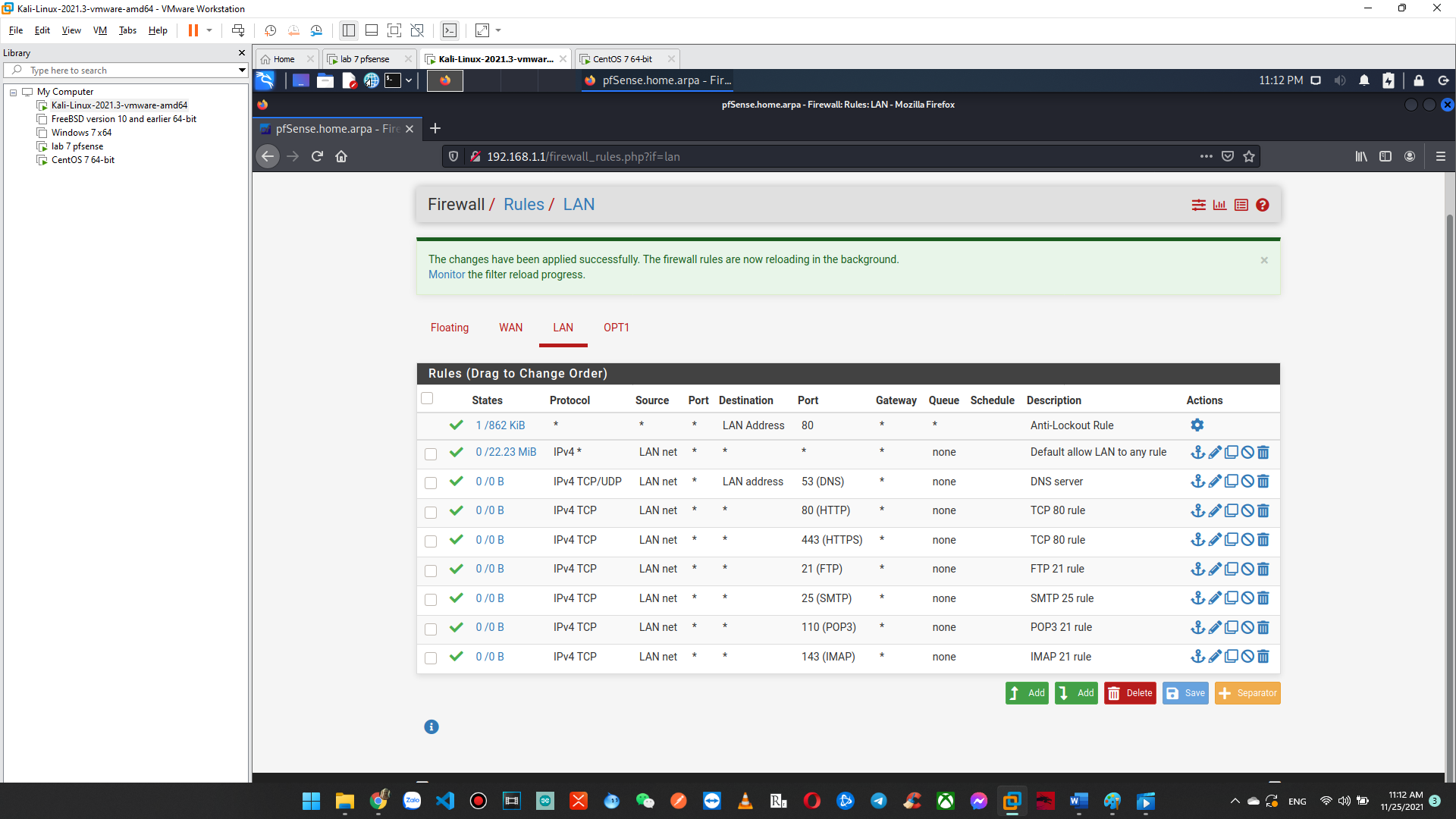


**Sau đó ta quay lại máy CentOS 7 và thử ping 192.168.2.1 Kết quả là ping thành công.**

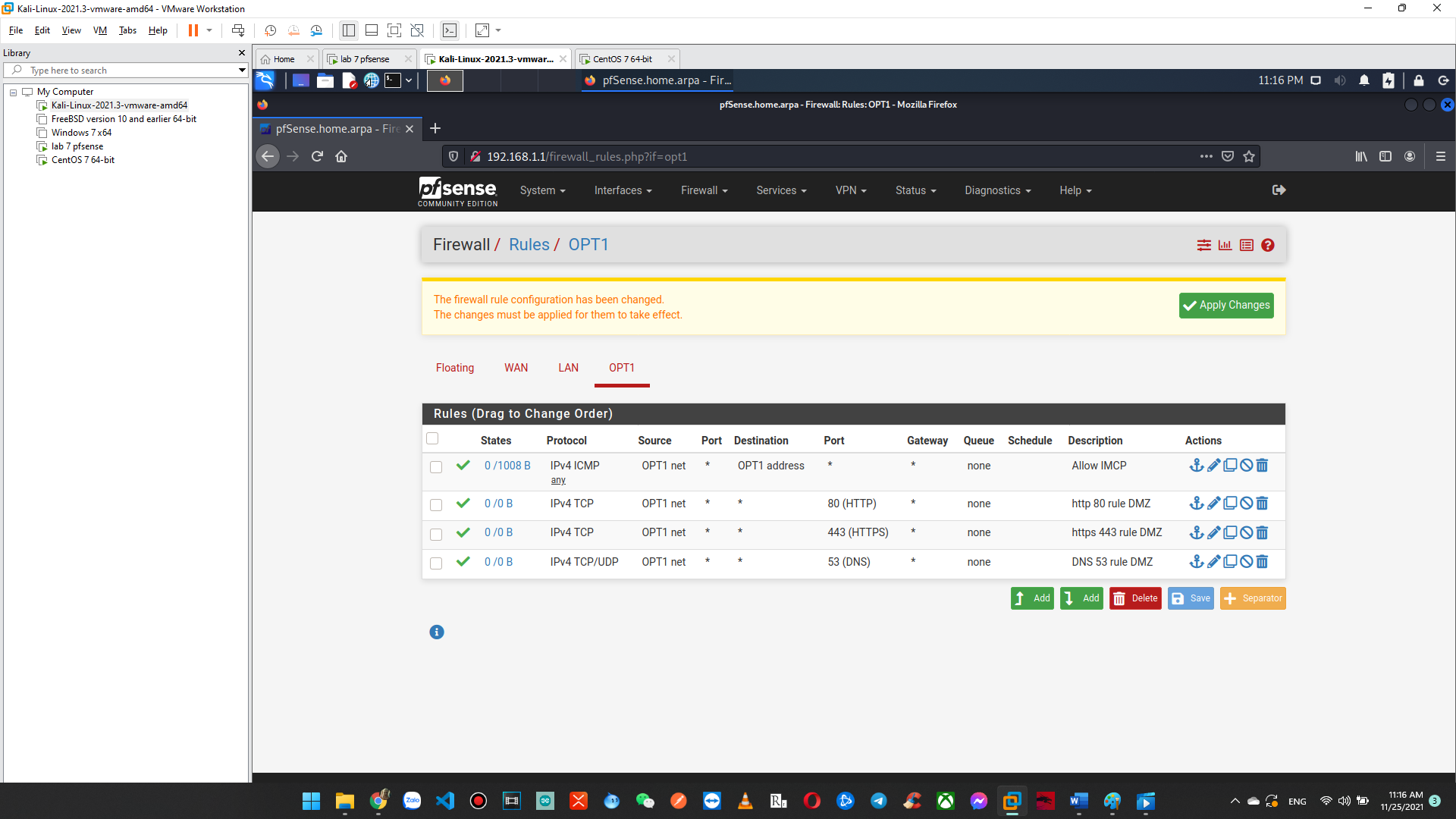


* + - * 1. **Cấu hình cơ bản bức tường lửa từ máy trạm (Kali Linux)**
* Tham khảo ví dụ về cấu hình bức tường lửa cơ bản trên *pfSense* trong [5]
* Cấu hình Outbound LAN

Tham khảo ví dụ về cấu hình bức tường lửa cơ bản trên *pfSense* trong [5] ta cấu hình như sau cho LAN.



* Cấu hình Outbound DMZ

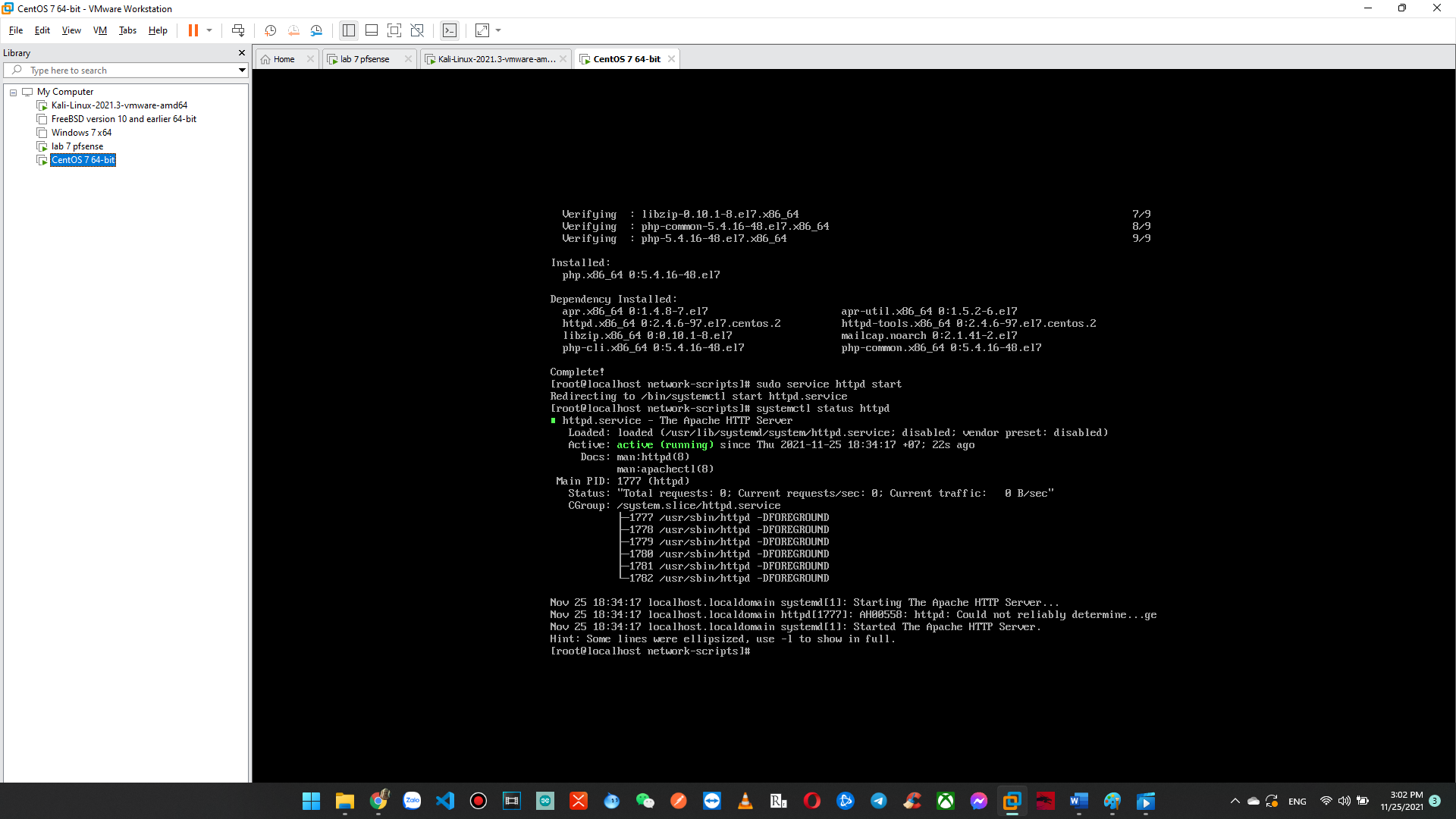


* Cấu hình bổ sung Outbound LAN

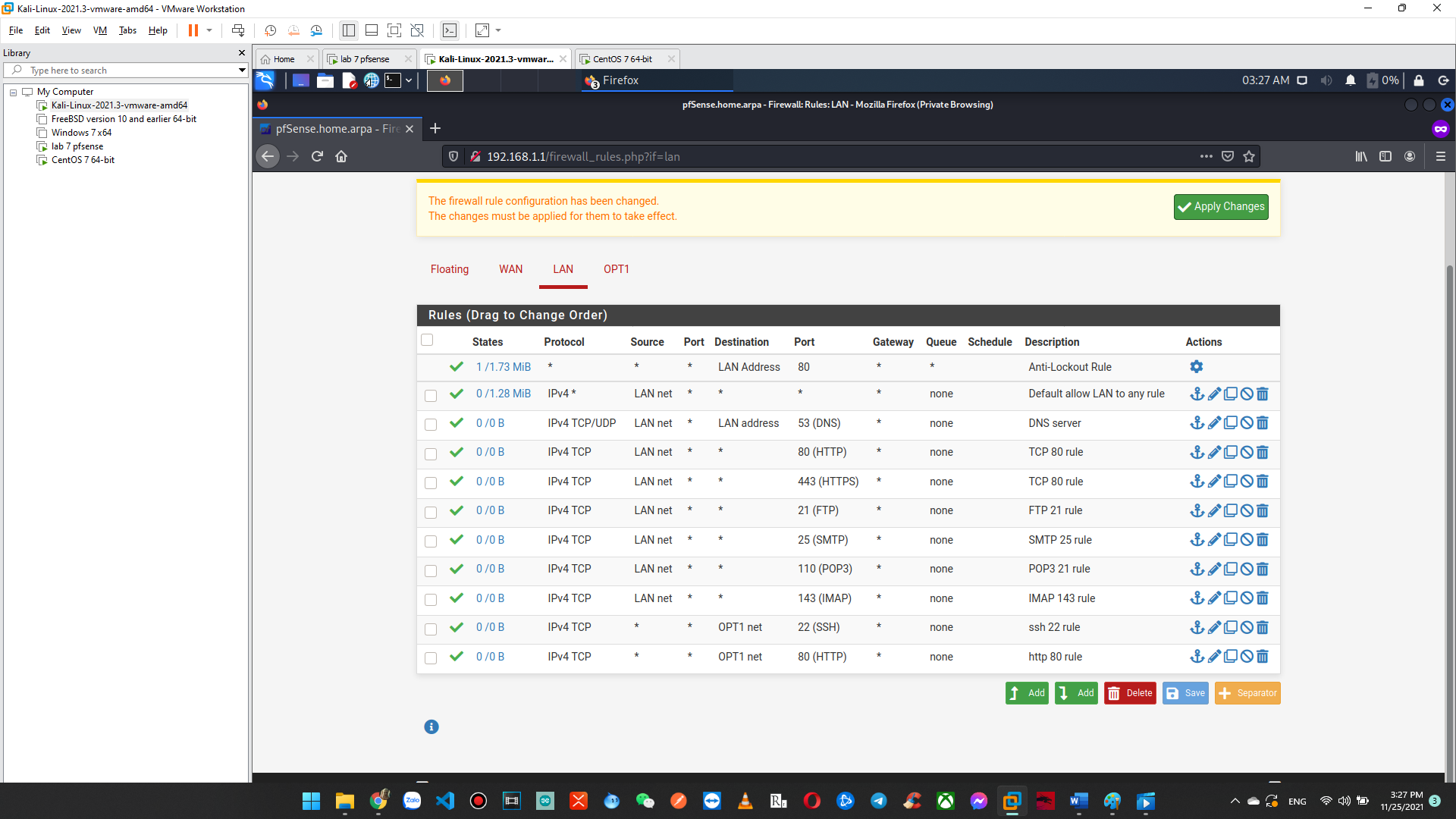
Cài đặt và start httpd trên centOS 7 :

* Yum update
* Yum install httpd
* systemctl start httpd
* systemctl enable httpd
* firewall-cmd --permanent --zone=public --add-service=http
* firewall-cmd --permanent --zone=public --add-service=https
* firewall-cmd --reload

Chạy lệnh systemctl status httpd để kiểm tra httpd serice đã hoạt động chưa.

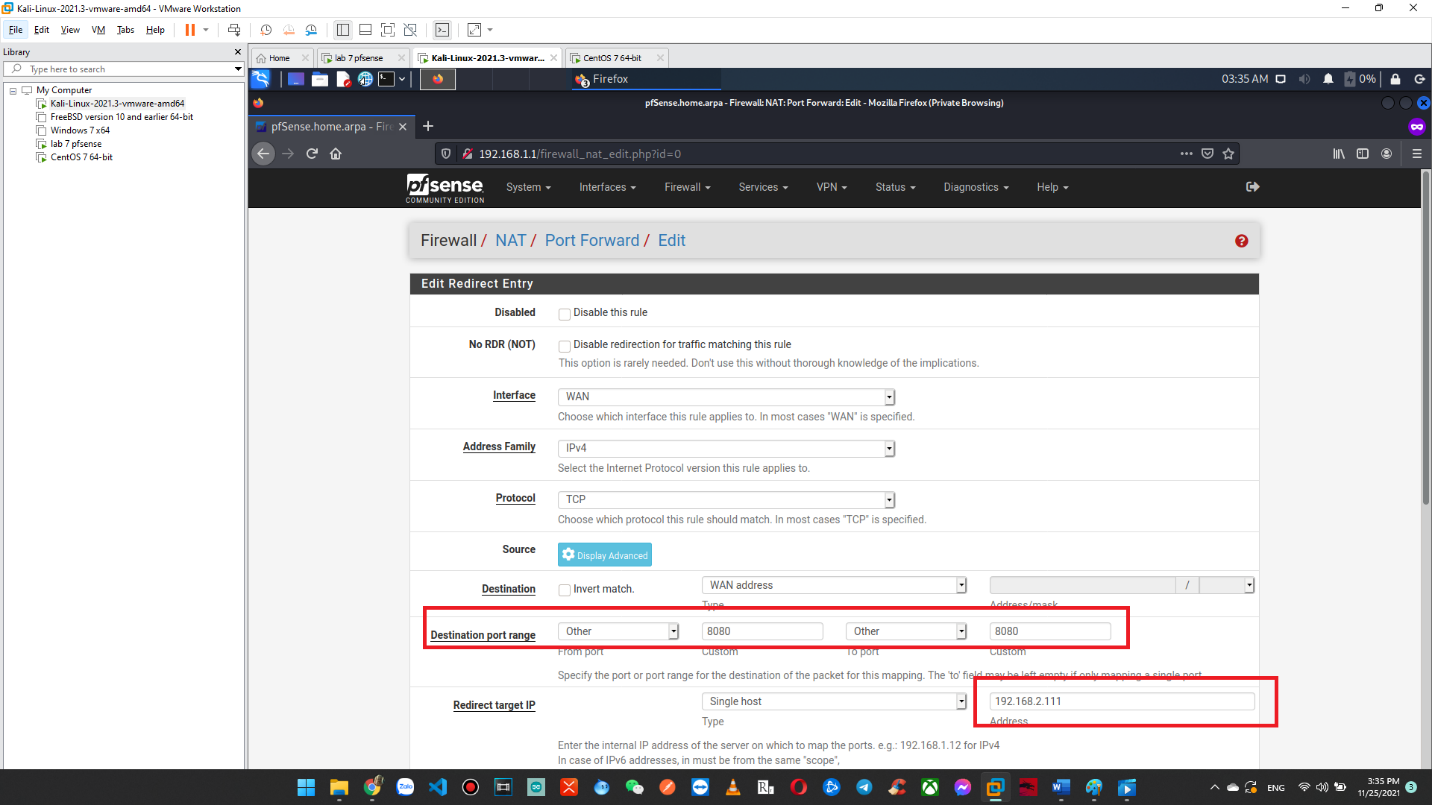


Thiết lập thêm mộ số rule như hình bên dưới



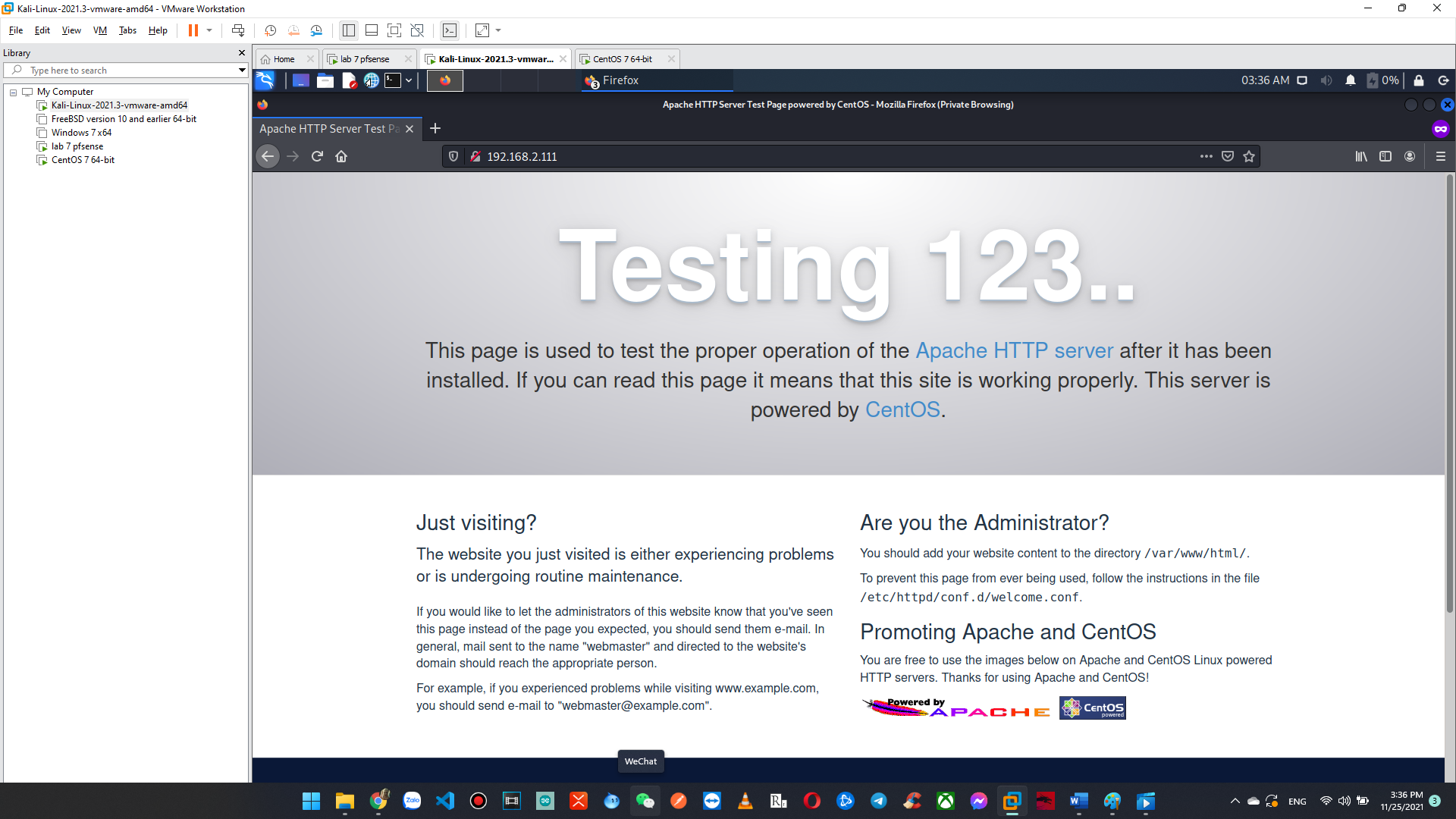
* Cấu hình bổ sung Outbound DMZ

Vào Firewall > NAT >Port forward. Nhấn vào add để thêm rules vào cấu hình như sau.



* **Kiểm tra hoạt động của bức tường lửa *pfSense***

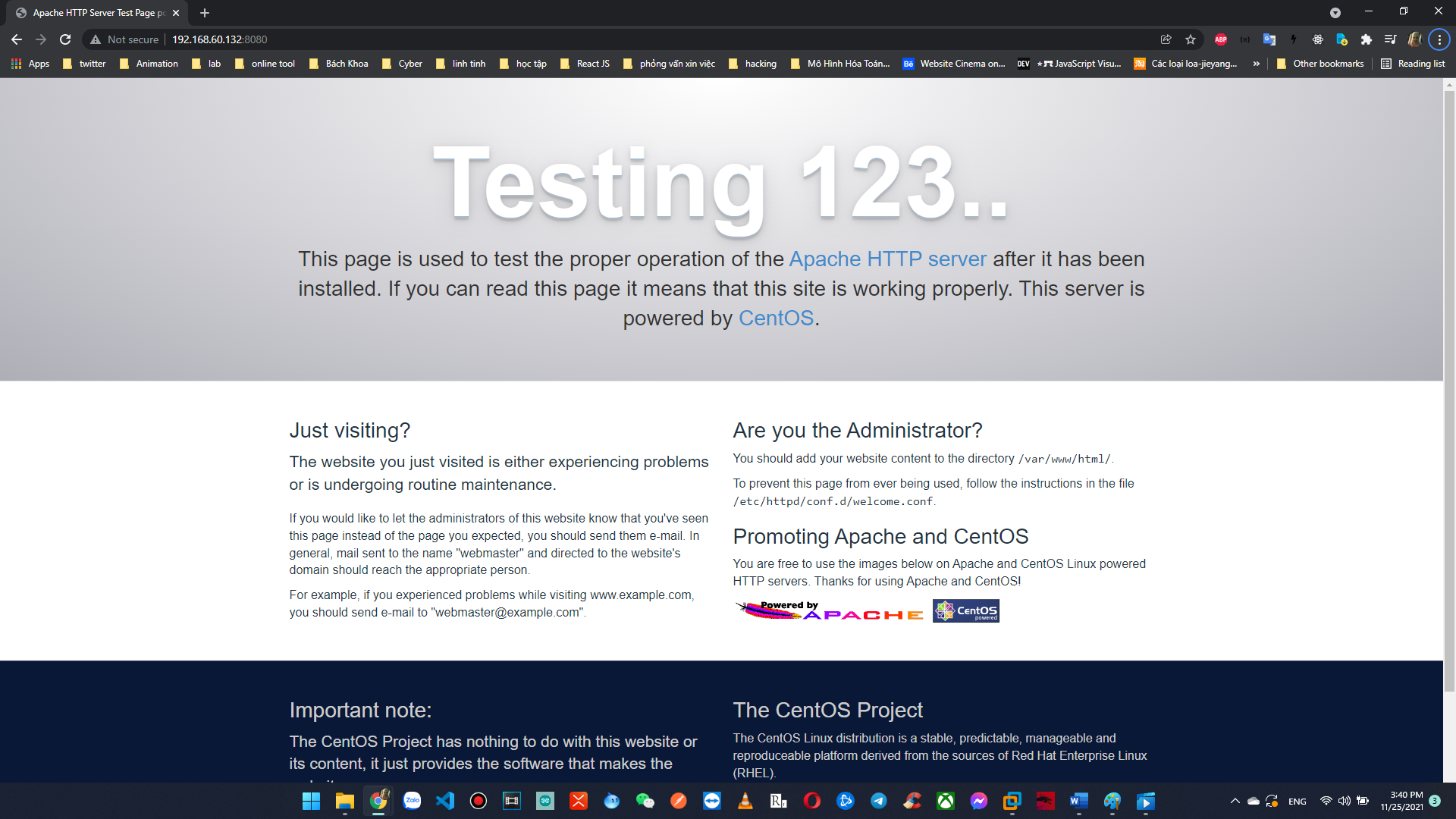
**Trên máy Kali Linux truy cập 192.168.2.111 ta được như sau.**



Trên máy tính cá nhân truy cập 192.168.60.132:8080 ( 192.168.60.132 là địa chỉ của WAN trên pfsense)



Ta được như sau:



Vậy là tưởng lửa pfsense đã hoạt động.

-HẾT-