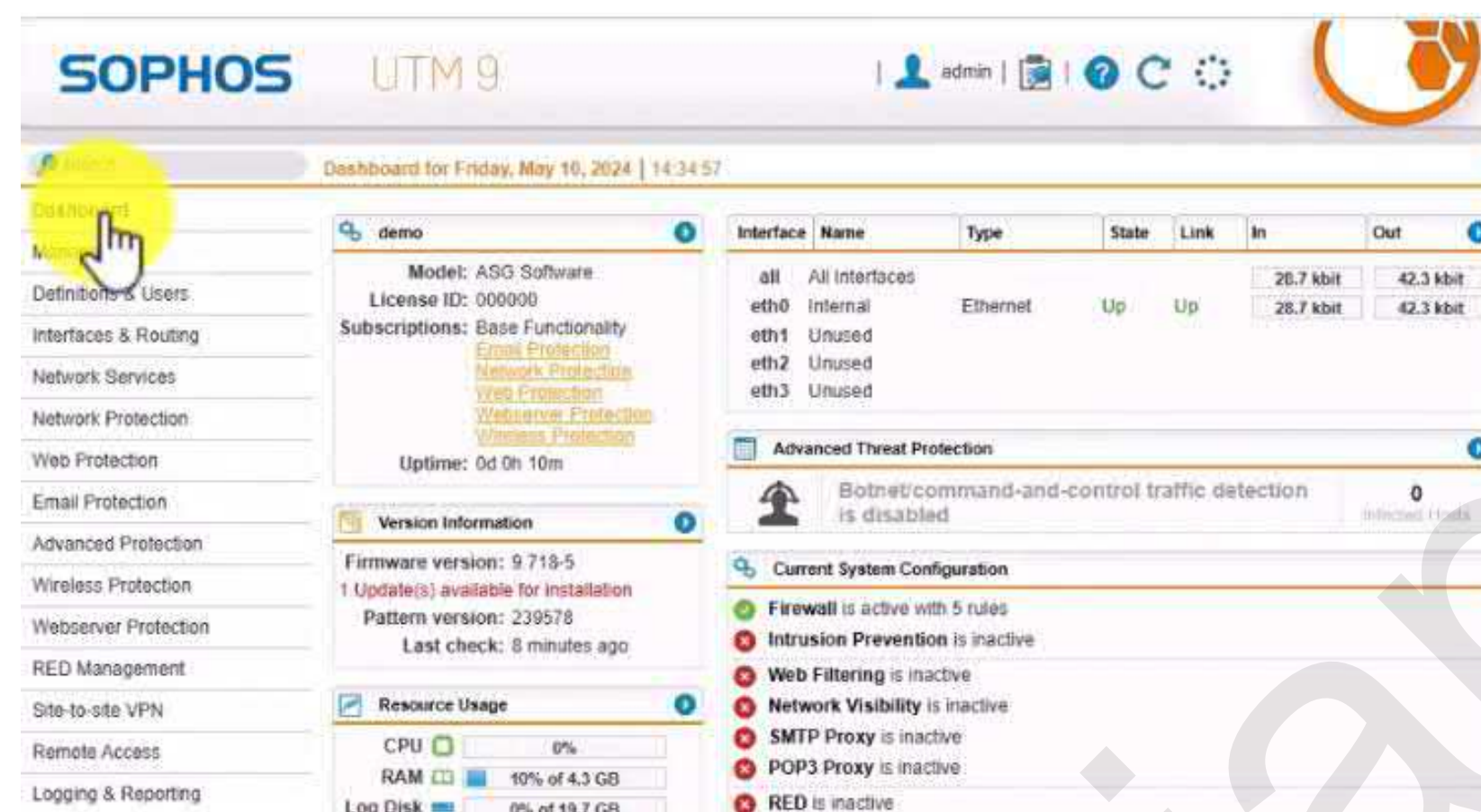


## Cài đặt tường lửa ( Firewall) (SoPhos UTM9 thông qua máy ảo Vmware)



Tường lửa (firewall) là một phần quan trọng trong bảo mật mạng của doanh nghiệp và thường được coi là tuyến phòng thủ đầu tiên trong hệ thống. Dưới đây là một số lợi ích khi sử dụng tường lửa cho doanh nghiệp:

**Bảo vệ dữ liệu và thông tin:** Tường lửa giúp bảo vệ dữ liệu và thông tin của khách hàng, giảm thiểu nguy cơ mất mát dữ liệu.

**Tuân thủ quy định bảo mật:** Sử dụng tường lửa giúp doanh nghiệp tuân thủ các quy định bảo mật và bảo vệ mạng khỏi các vấn đề pháp lý.

**Ngăn chặn cuộc tấn công:** Tường lửa phát hiện và ngăn chặn các cuộc tấn công như từ chối dịch vụ (DoS) và từ chối dịch vụ phân tán (DDoS). Nó cũng giúp phát hiện phần mềm độc hại và virus.

**Lọc nội dung truy cập:** Tường lửa có khả năng lọc nội dung truy cập, ngăn chặn các luồng thông tin không mong muốn.

**Giám sát hoạt động mạng:** Tường lửa giám sát toàn bộ các hoạt động đăng nhập và truy cập vào hệ thống mạng

Trong Phần nội dung này ta tìm hiểu cách cài đặt tường lửa ( Firewall) (SoPhos UTM9 thông qua máy ảo Vmware)



sophos.com/en-us

Discover how ransomware and its business impacts have evolved over the last 12 months. [Read the report](#)

**SOPHOS**

Services & Products Solutions Partners About Support

Experiencing a Cyberattack? Get help now. >

**More companies trust Sophos for MDR than any other cybersecurity provider.**

See How Learn More

Speak with an expert >

Ta vào trình duyệt tải file utm9.iso tại địa chỉ (https://www.sophos.com/ )

I help you

Link tải file utm9 tại đây : <https://www.sophos.com/en-us/support/downloads>



Discover how ransomware and its business impacts have evolved over the last 12 months. [Read the report](#)

SOPHOS

Services & Products ▾

Solutions ▾

Partners ▾

About ▾

Support ▲



# Sophos Support

[Support Portal](#)

## Get Help

[Support Portal](#) >

[Support Packages](#) >

[Partner Care Support](#) >

[Tech Support](#) >

## Resources

[Downloads and Updates](#) >

[Documentation](#) >

[Technical Training](#) >

[Techvids - Training Videos](#) >

[Sophos Status Page](#) >

[Submit a Threat](#) >

## Product Support

[Sophos Community Forums](#) >

[Sophos Firewall](#) >

[Sophos Endpoint](#) >

[Sophos Cloud](#) >

[Sophos Central](#) >

[Sophos Email](#) >

# cybersecurity provider.

[See How](#) ▶

[Learn More](#)

[Speak with an expert](#) >

Tại Tab Resources ta click vào download and update

## Downloads

[Firewall Installers](#) >

[UTM Downloads](#) >

[Sophos Mobile](#) >

[SEC - Endpoint Clients \(End of Life July 2023\)](#) >

[SEC - Sophos Enterprise Console \(End of Life: July 2023\)](#) >

[Sophos Email Appliance and PureMessage \(End of Life July 2023\)](#) >

[Sophos SafeGuard Encryption \(End of Life July 2023\)](#) >

[Virtual Web Appliance \(End of Life July 2023\)](#) >

Tiếp đến ta click vào mục UTM Downloads



**Downloads** Firewall Installers **UTM Downloads** Sophos Mobile SEC – Endpoint Clients [End of Life July 2023] SEC – Sophos Enterprise

9.719-3.1

### Sophos UTM

Platform: UTM v9 hardware appliance

md5

[Download](#)

ssi-9.719-3.1.iso

Size: 1.3 GB

---

9.719-3.1

### Sophos UTM

Platform: UTM v9 software appliance

md5

[Download](#)

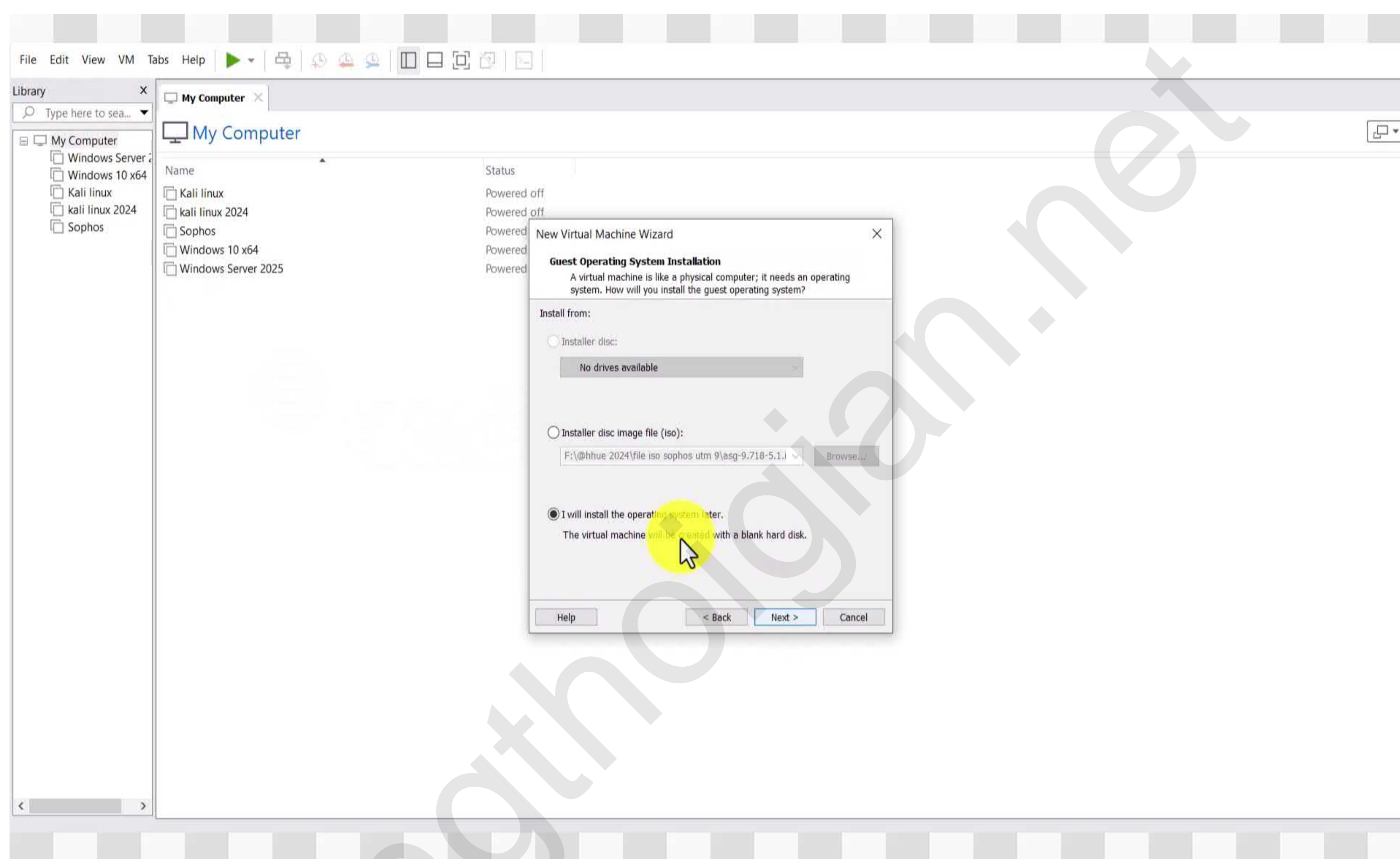
asg-9.719-3.1.iso

Size: 1.3 GB

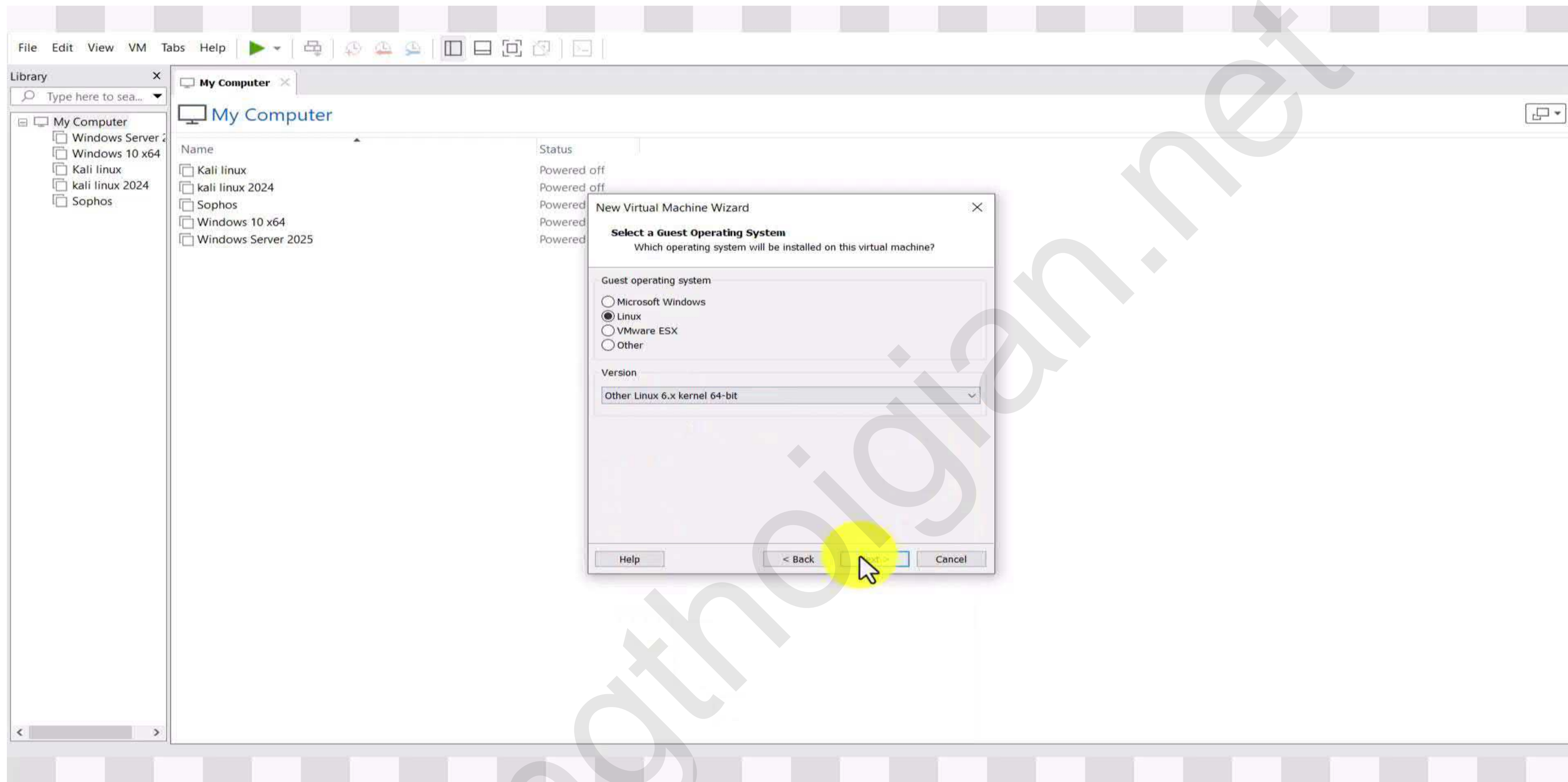
Ta Click vào Download như hình , Sophos yêu cầu đăng ký thông , sau đó sophos sẽ gửi link để Download



Tiếp đến ta cần cài máy ảo **Vmware** Xem hướng dẫn tại search google

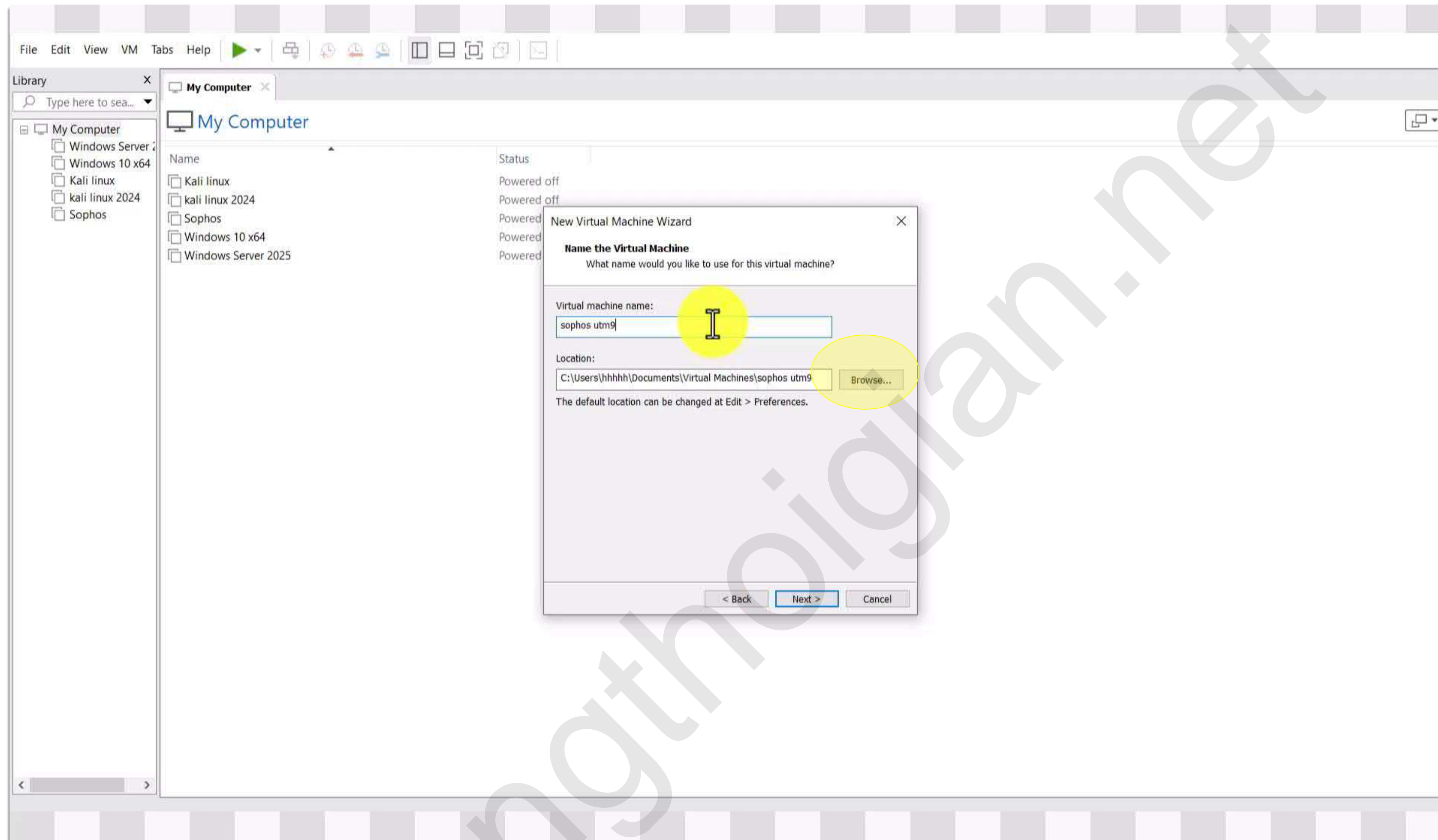


Ta click vào khởi tạo máy ảo mới làm như hình

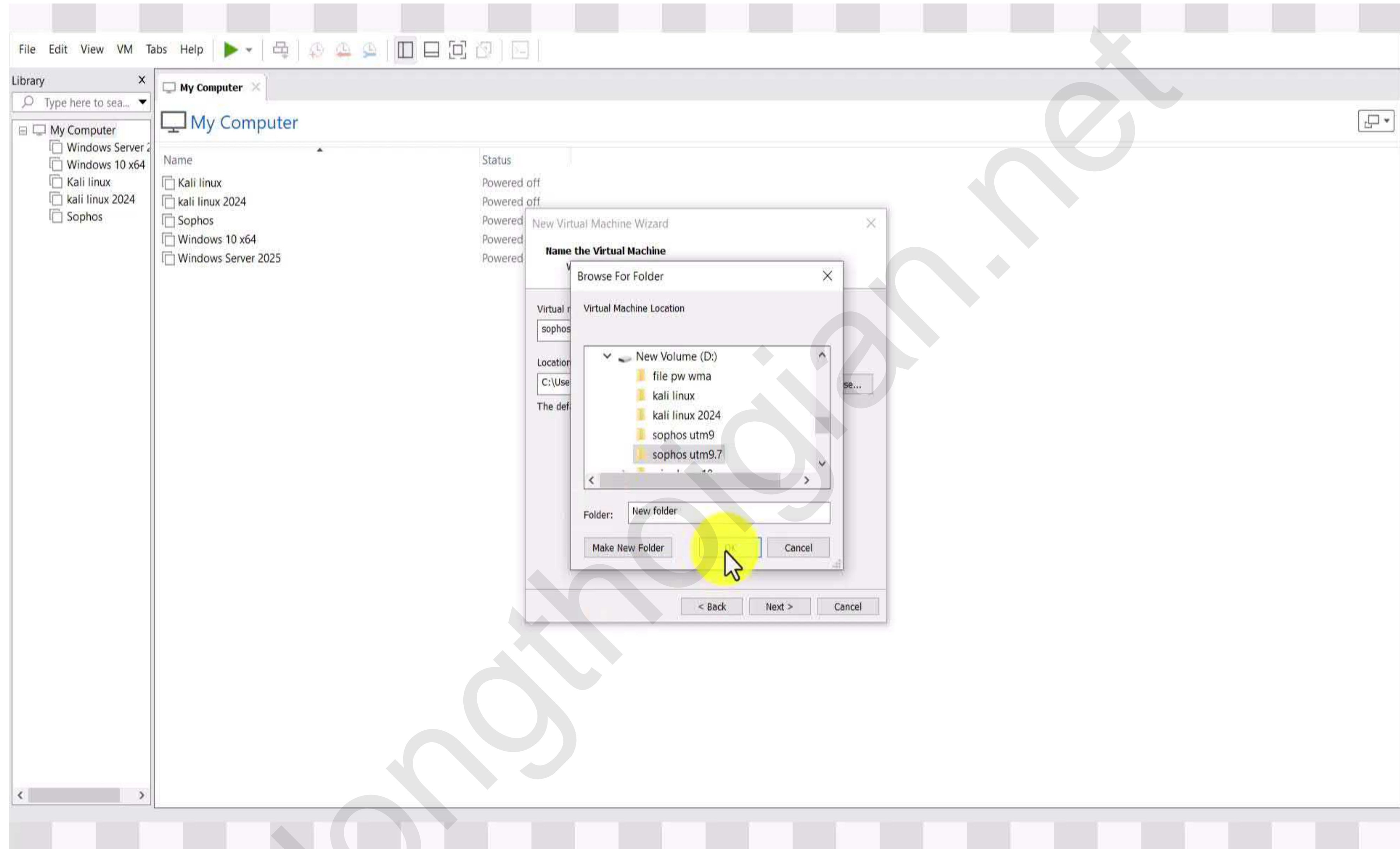


Chọn **Linux** và click tab **Next**



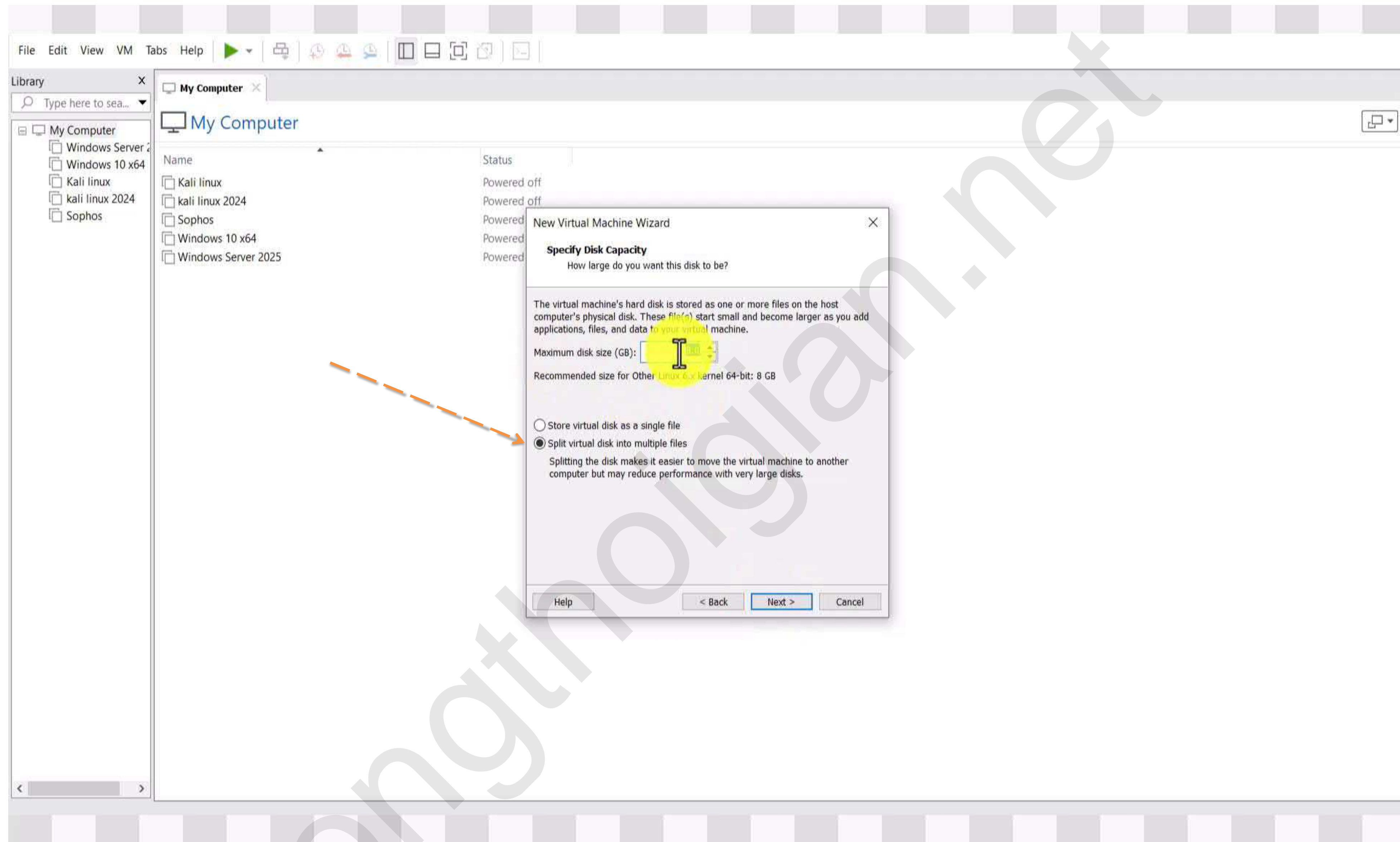


Đặt tên & chọn nơi lưu cho máy ảo và click **next**

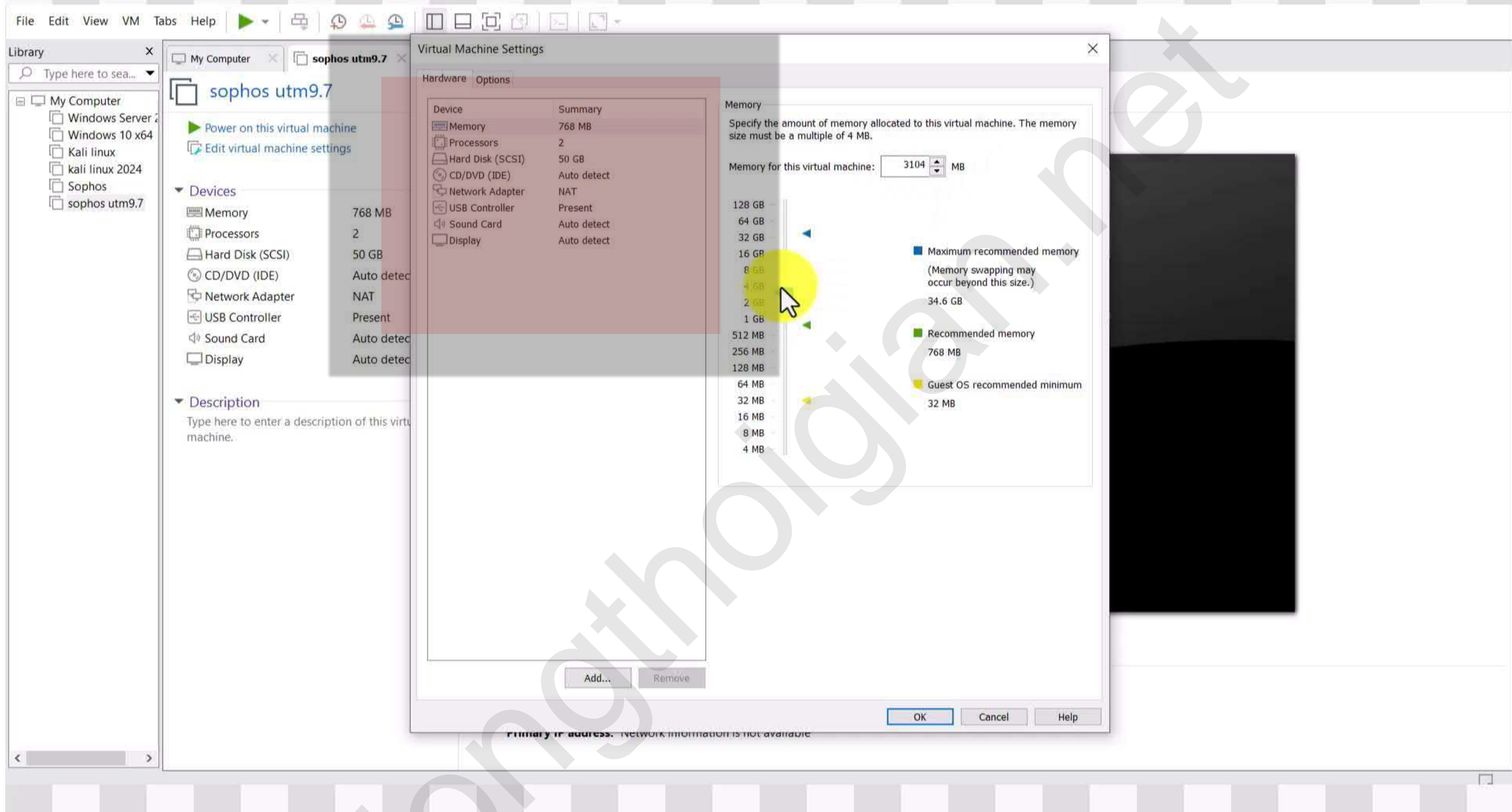


Như hình tôi chọn lưu vào ổ đĩa D và click vào **next**



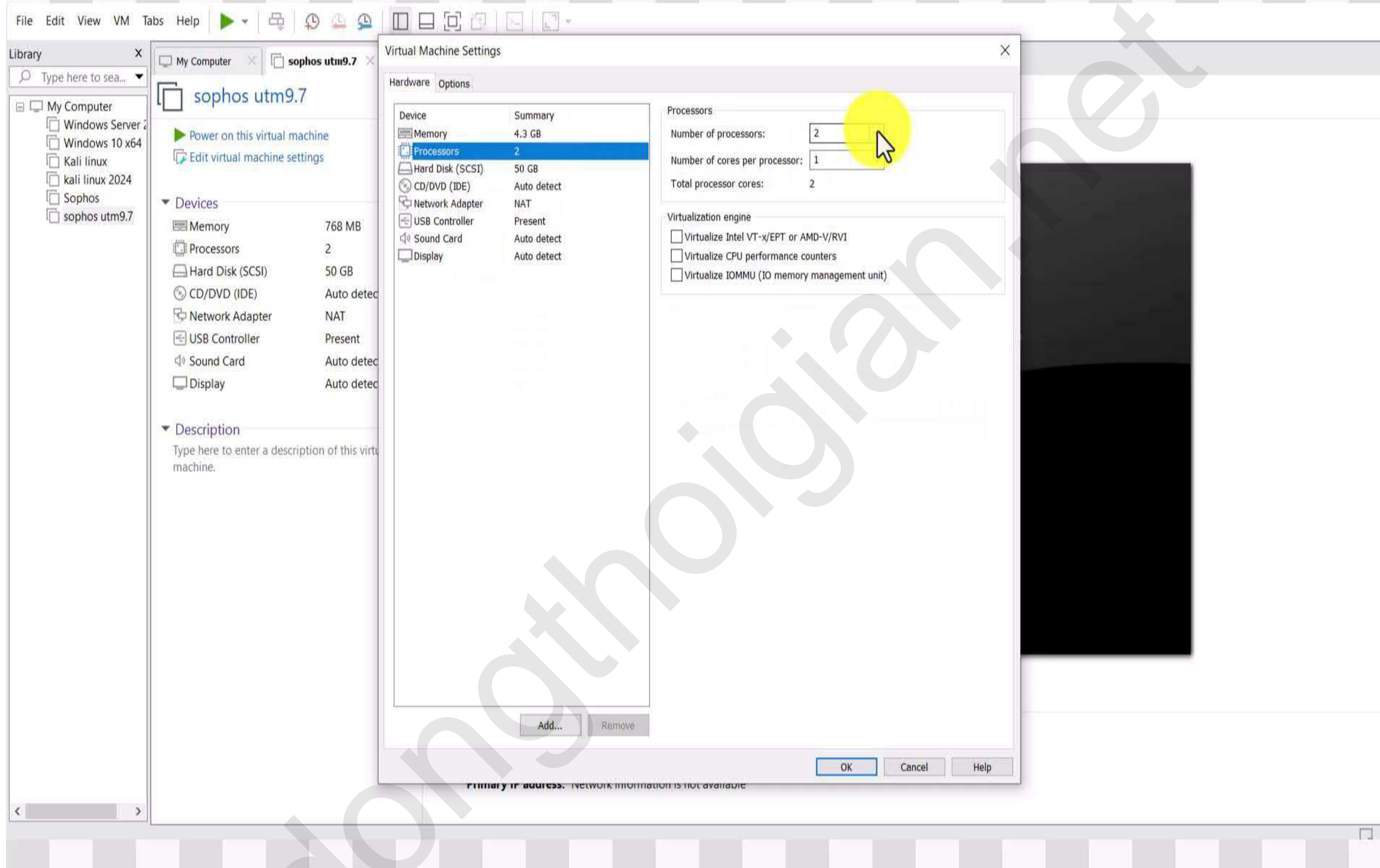


Lựa chọn tích vào ô như hình rồi click vào **next**

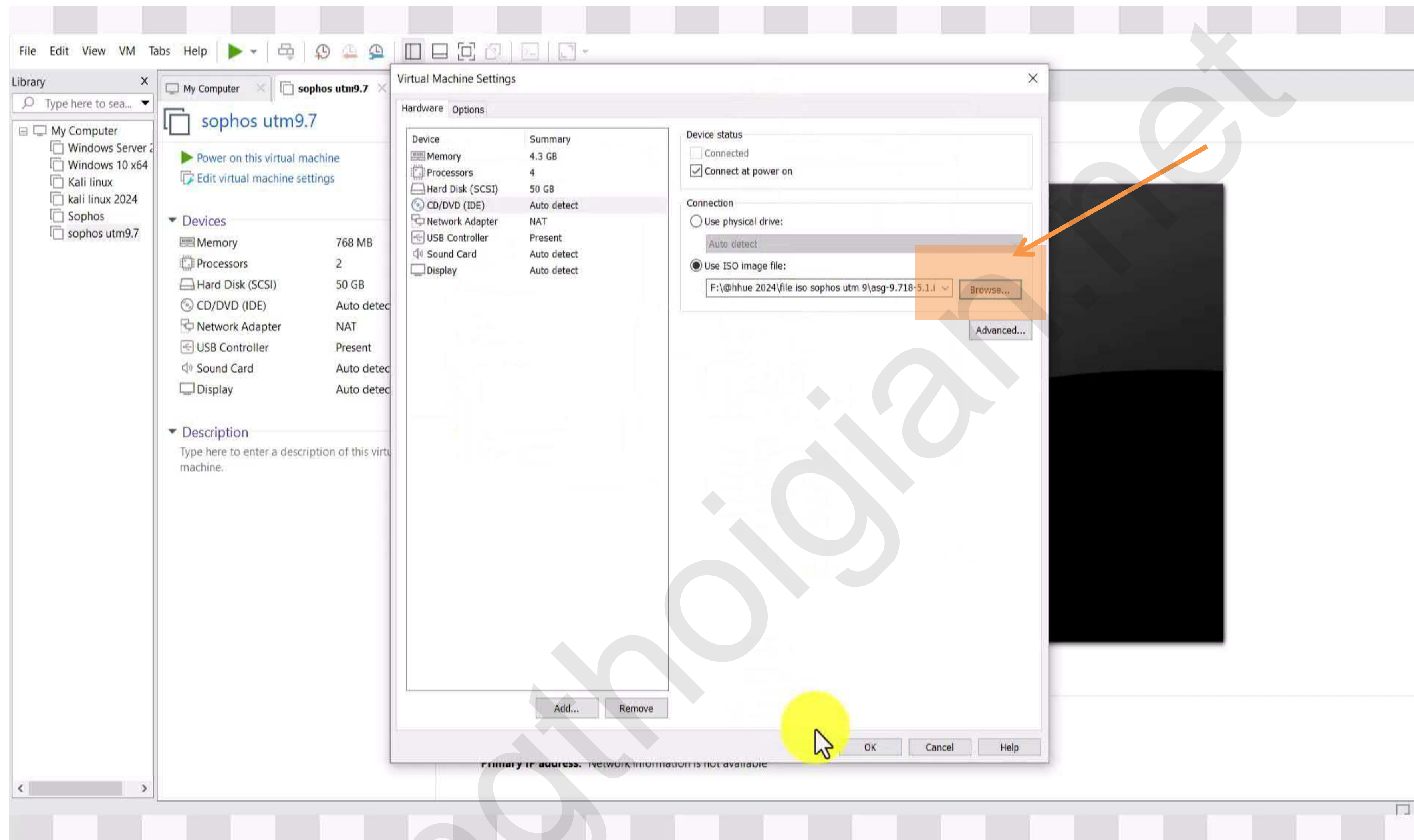


Tại đây ta phân bổ phần cứng cho máy ảo



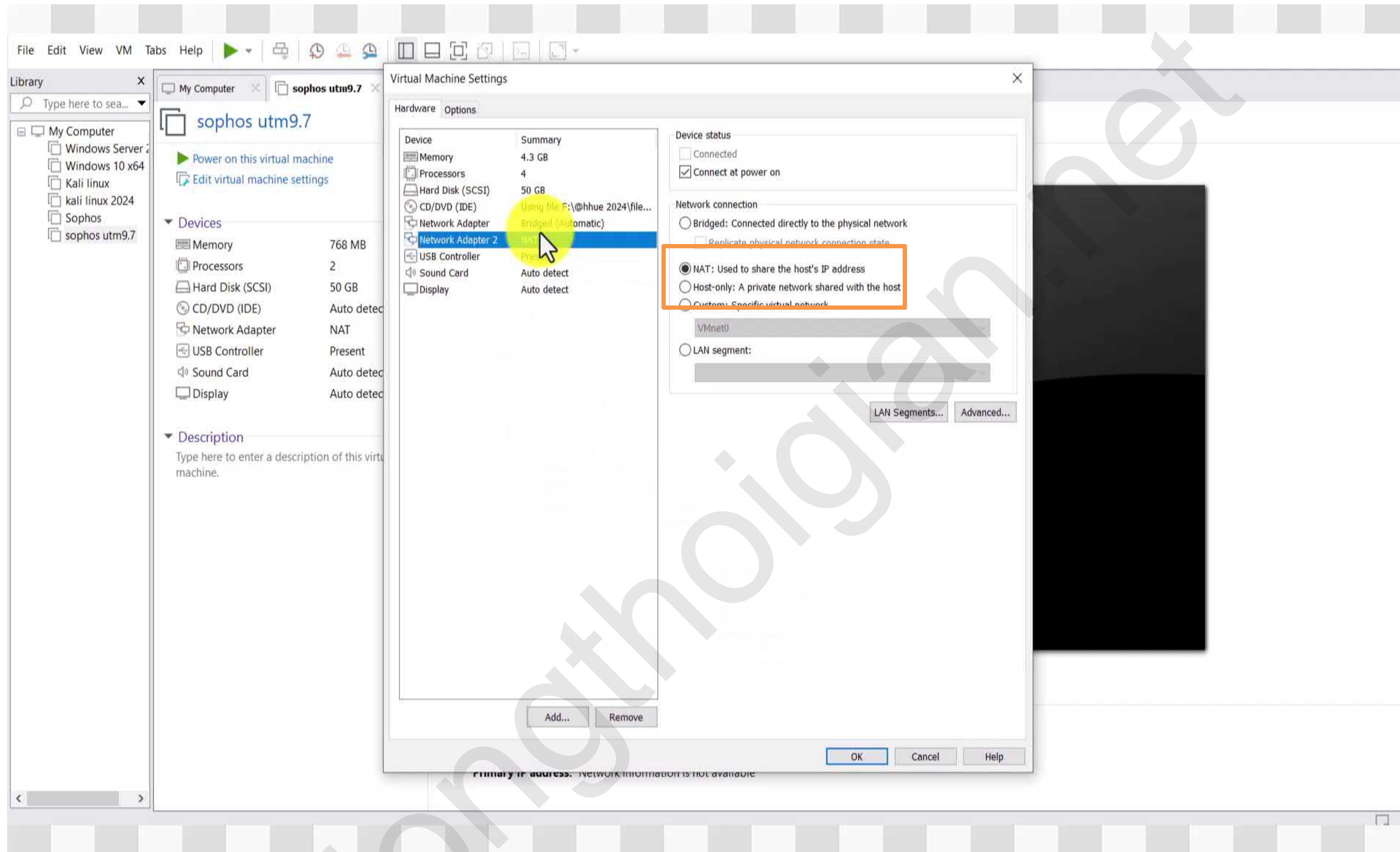


Ta Phân bổ core CPU, Ram , ổ đĩa và các phần cứng mở rộng khác

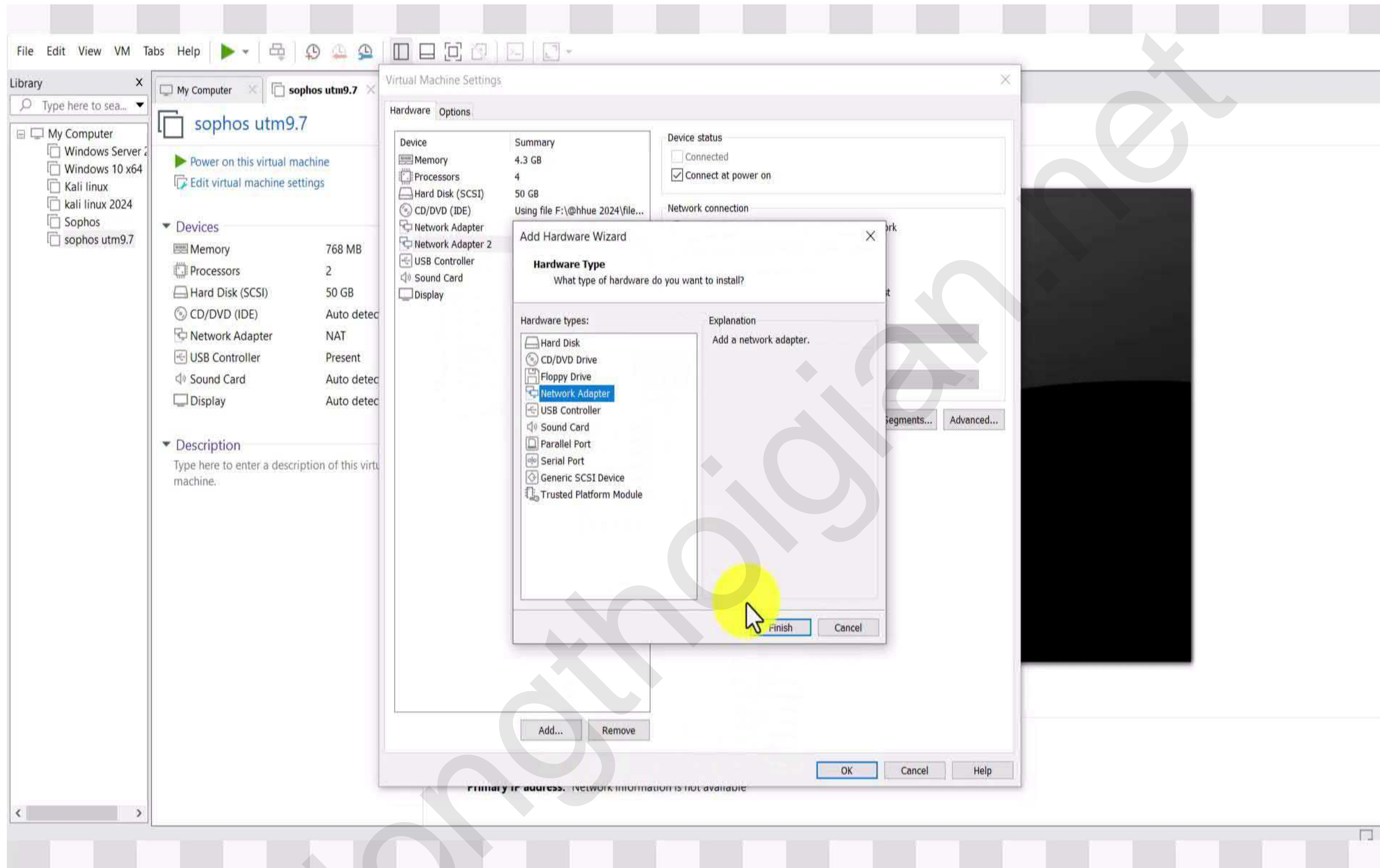


Tại mục use iso image file : Ta **Browse** đến file iso vừa tải



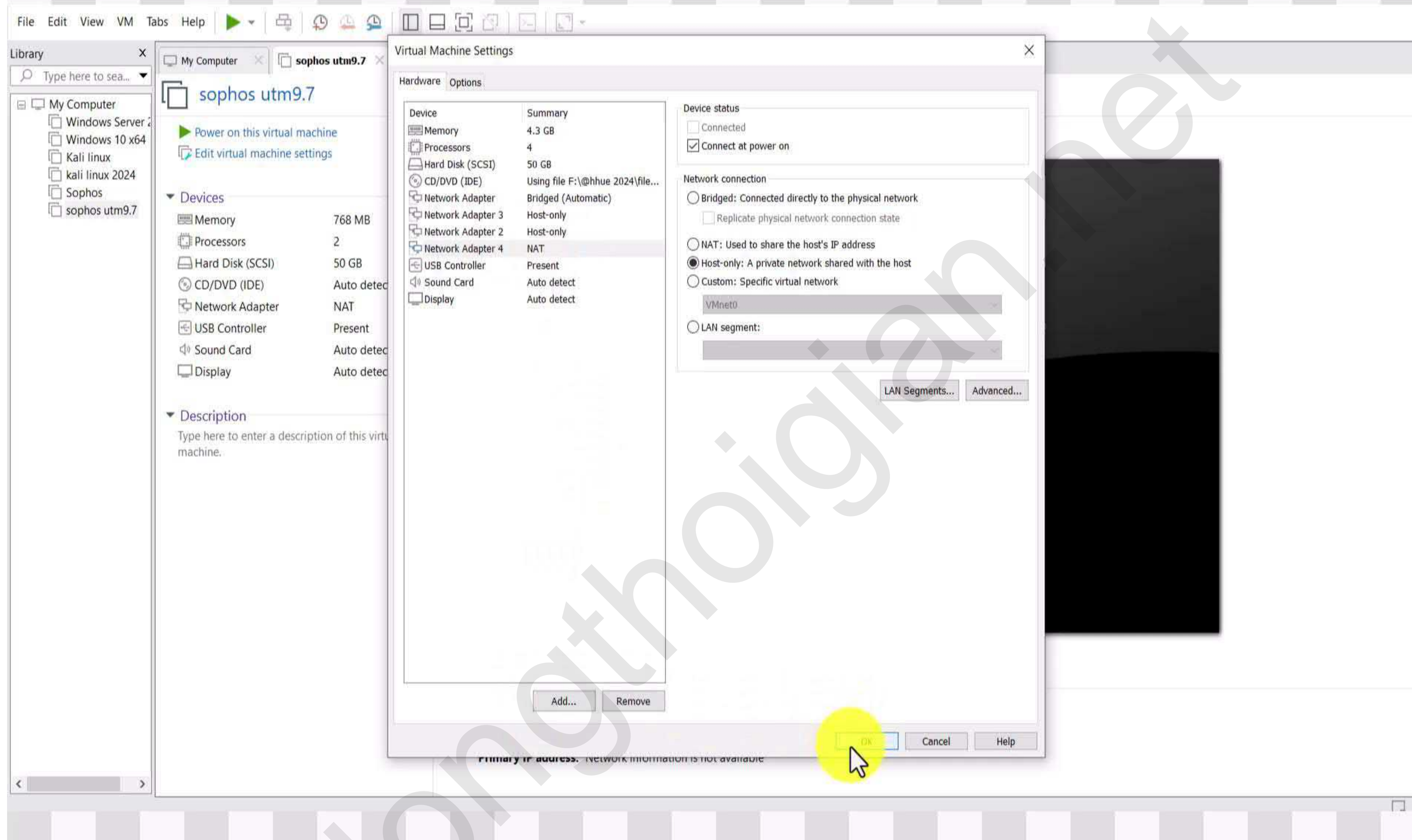


Hình này cho thêm card mạng và cấu hình nat cho card mạng



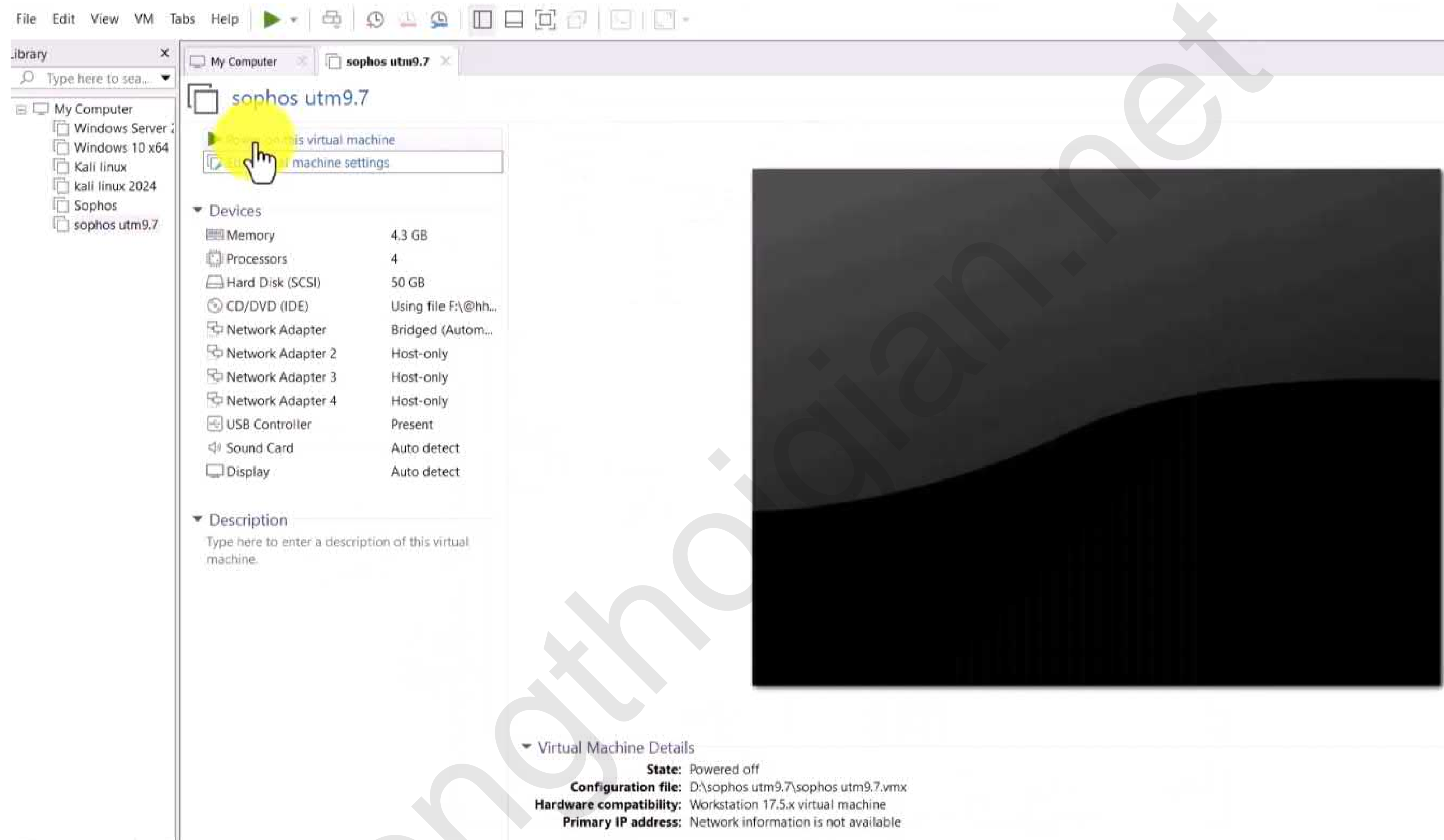
Ta có thể thêm nhiều card mạng ảo





Như hình ta thấy tôi thêm 4 card mạng ảo cho Sophos và Click OK





Tiếp đến ta click vào mục Power on this virtual machine

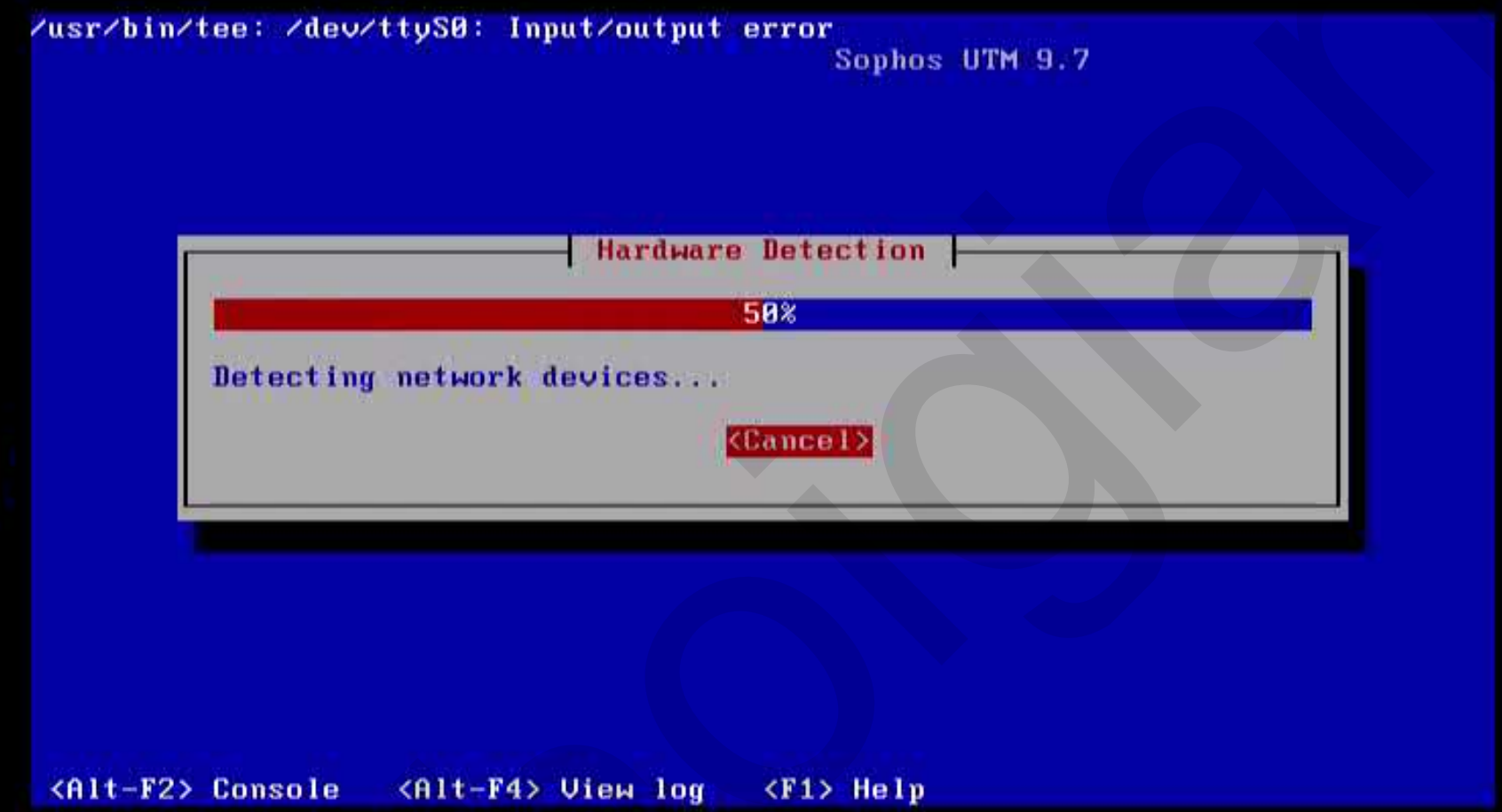


Tiến trình này đang khởi động máy ảo

```
[ 1.692552] pcieport 0000:00:18.6: Signaling PME through PCIe PME interrupt
[ 1.692651] pcieport 0000:00:18.7: Signaling PME through PCIe PME interrupt
[ 1.746046] Serial: 8250/16550 driver, 4 ports, IRQ sharing enabled
[ 1.747451] Linux agpgart interface v0.103
[ 1.747500] agpgart-intel 0000:00:00.0: Intel 440BX Chipset
[ 1.747975] agpgart-intel 0000:00:00.0: AGP aperture is 256M @ 0x0
[ 1.751567] brd: module loaded
[ 1.751617] hv_vmbus: registering driver hv_netvsc
[ 1.751906] usbcore: registered new interface driver usbserial
[ 1.752038] usbcore: registered new interface driver usbserial_generic
[ 1.752215] usbserial: USB Serial support registered for generic
[ 1.752506] i8042: PNP: PS/2 Controller [PNP0303:KBC,PNP0f13:MOUS] at 0x60,0x
64 irq 1,12
[ 1.753176] serio: i8042 KBD port at 0x60,0x64 irq 1
[ 1.753227] serio: i8042 AUX port at 0x60,0x64 irq 12
[ 1.753765] mousedev: PS/2 mouse device common for all mice
[ 1.754362] hidraw: raw HID events driver (C) Jiri Kosina
[ 1.754463] TCP: cubic registered
[ 1.754512] Key type dns_resolver registered
[ 1.755833] Using IPI Shortcut mode
[ 1.755890] input: AT Translated Set 2 keyboard as /devices/platform/i8042/se
rio0/input/input0
[ 1.769310] drivers/rtc/hctosys.c: unable to open rtc device (rtc0)
[ 1.776197] Freeing unused kernel memory: 408K (804ca000 - 80530000)
-
```

Quá trình cài đặt bắt đầu

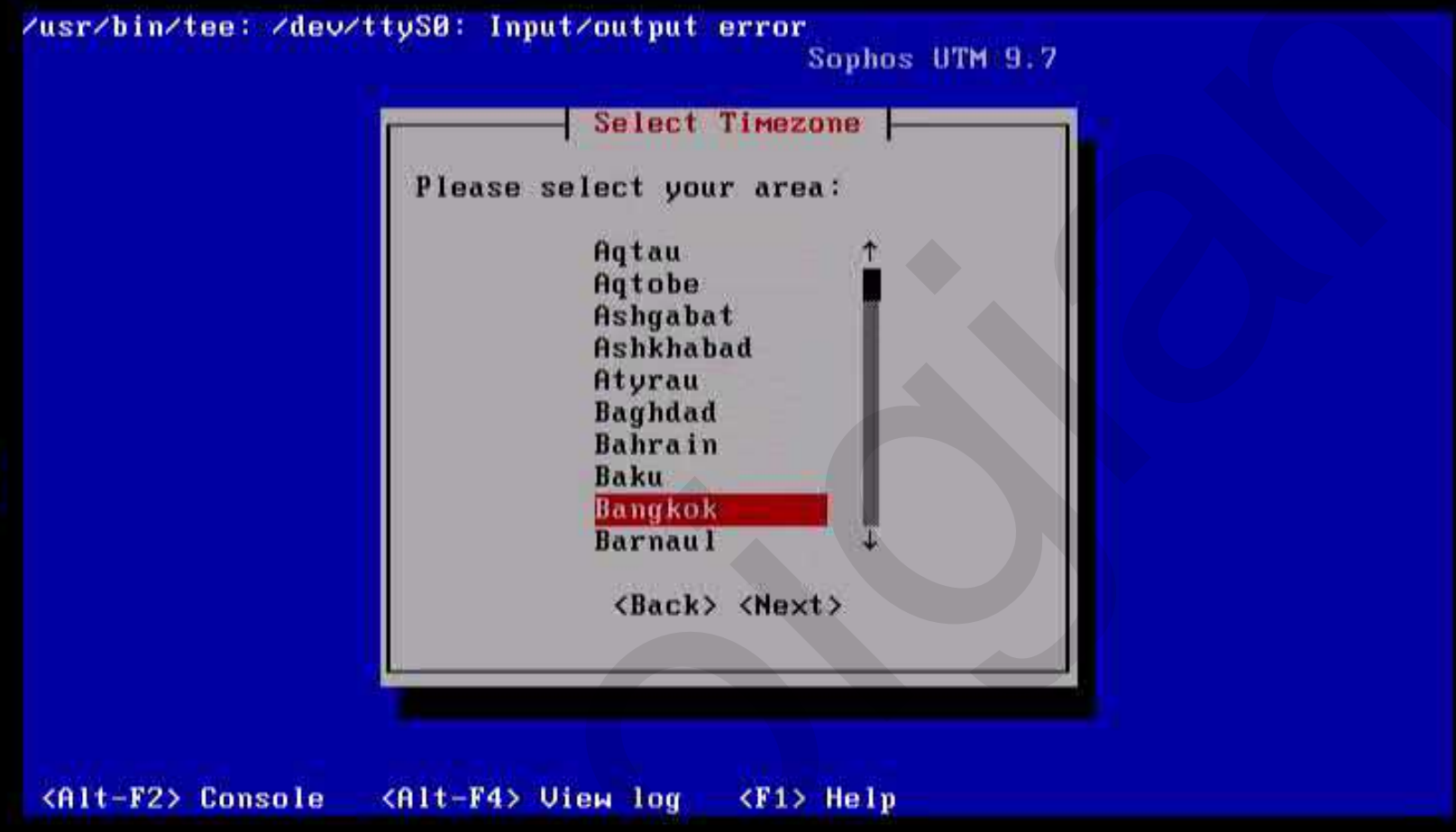




Quá trình cài đặt đang kiểm tra card mạng



Chọn ngôn ngữ bàn phím



Chọn quốc gia



```
/usr/bin/tee: /dev/ttyS0: Input/output error
Sophos UTM 9.7
```

Date and Time

Date: 05/04/24

Local Time: 23:38:59

Host clock is UTC

<Back> **<Next>** <Cancel> <Help>

```
<Alt-F2> Console <Alt-F4> View log <F1> Help
```

Đặt lại thời gian

```
/usr/bin/tee: /dev/ttyS0: Input/output error
Sophos UTM 9.7

|----- Select Admin Interface -----|
Select which interface you will use to access the WebAdmin
user interface:
eth0 [link] VMware PRO/1000 MT Single Port Adapter
eth1      VMware PRO/1000 MT Single Port Adapter
eth2      VMware PRO/1000 MT Single Port Adapter
eth3      VMware PRO/1000 MT Single Port Adapter

<Back> <Next> <Cancel> <Help>

<Alt-F2> Console <Alt-F4> View log <F1> Help
```

Lựa chọn card mạng để kết nối



Ta có thể đặt lại IP để đăng nhập vào phần quản lý



```
/usr/bin/tee: /dev/ttyS0: Input/output error
Sophos UTM 9.7

Network Configuration
Please configure the administrative network interface:
Address: 192.168.0.101
Netmask: 255.255.255.0
Gateway: 192.168.0.1 (optional)
<Back> <Next> <Cancel>

<Alt-F2> Console <Alt-F4> View log <F1> Help
```

Ta nên đặt lớp mạng theo ip router nhà cung cấp

```
/usr/bin/tee: /dev/ttyS0: Input/output error
Sophos UTM 9.7

Installation: Partitioning

The next step will erase all existing data on '/dev/sda'
(UMware Virtual S).

Would you like to proceed?

<Back> <Yes> <No>

<Alt-F2> Console <Alt-F4> View log <F1> Help
```

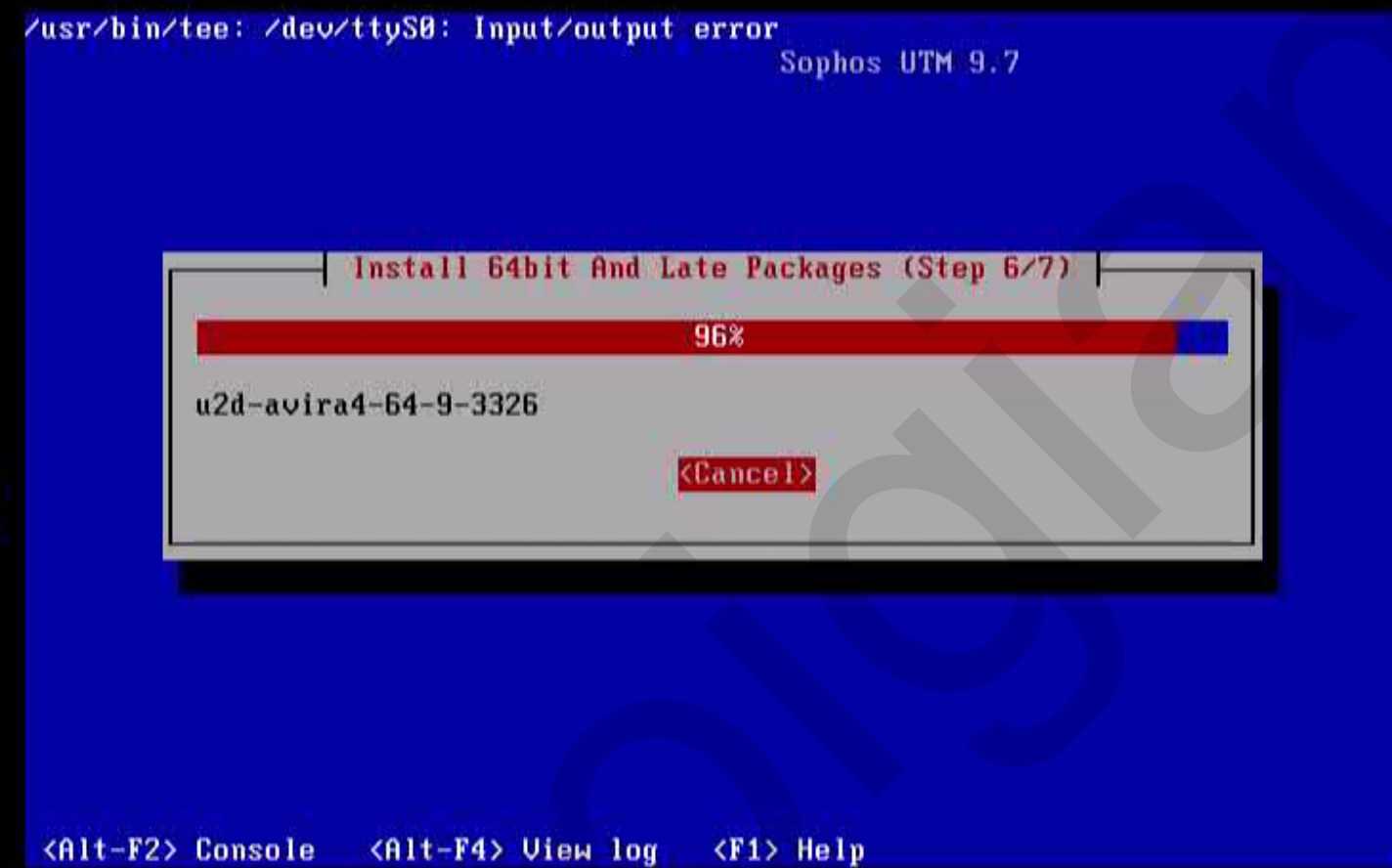


Chọn Yes



Xem tiến trình cài đặt bao gồm 7 bước





Xem tiến trình cài đặt đến bước 6

```
/usr/bin/tee: /dev/ttyS0: Input/output error
Sophos UTM 9.7
```

Finishing (Step 7/7)  
The installer is preparing the system for the initial boot.

```
<Alt-F2> Console <Alt-F4> View log <F1> Help
```

Quá Trình cài đã thành công

```
/usr/bin/tee: /dev/ttyS0: Input/output error
Sophos UTM 9.7

Installation Finished

Please remove the CD-ROM or unplug the USB device, connect the
selected administrative network interface to your local network
or PC, and restart the system by pressing the Reboot button.

After the system has restarted, open

https://192.168.0.101:4444/

in a web browser to access the WebAdmin user interface and
finish the setup.

<Reboot> <Support>

<Alt-F2> Console <Alt-F4> View log <F1> Help
```

Ta click vào tab Reboot như hình



```
Booting 'Sophos UTM 9.7 (3.12.74-0.434058663.g1ba2494.rb7-smp64)'
```

```
root (hd0,0)  
Filesystem type is ext2fs, partition type 0x83  
kernel /boot/vmlinuz-3.12.74-0.434058663.g1ba2494.rb7-smp64 root=/dev/disk/by-label/root vga=791 rootflags=data=ordered splash=silent  
[Linux-bzImage, setup=0x3c00, size=0x2bb490]  
initrd /boot/initrd-3.12.74-0.434058663.g1ba2494.rb7-smp64
```



Tiến Trình đang khởi động



Tiến trình đang load vào giao diện Sophos utm9.7

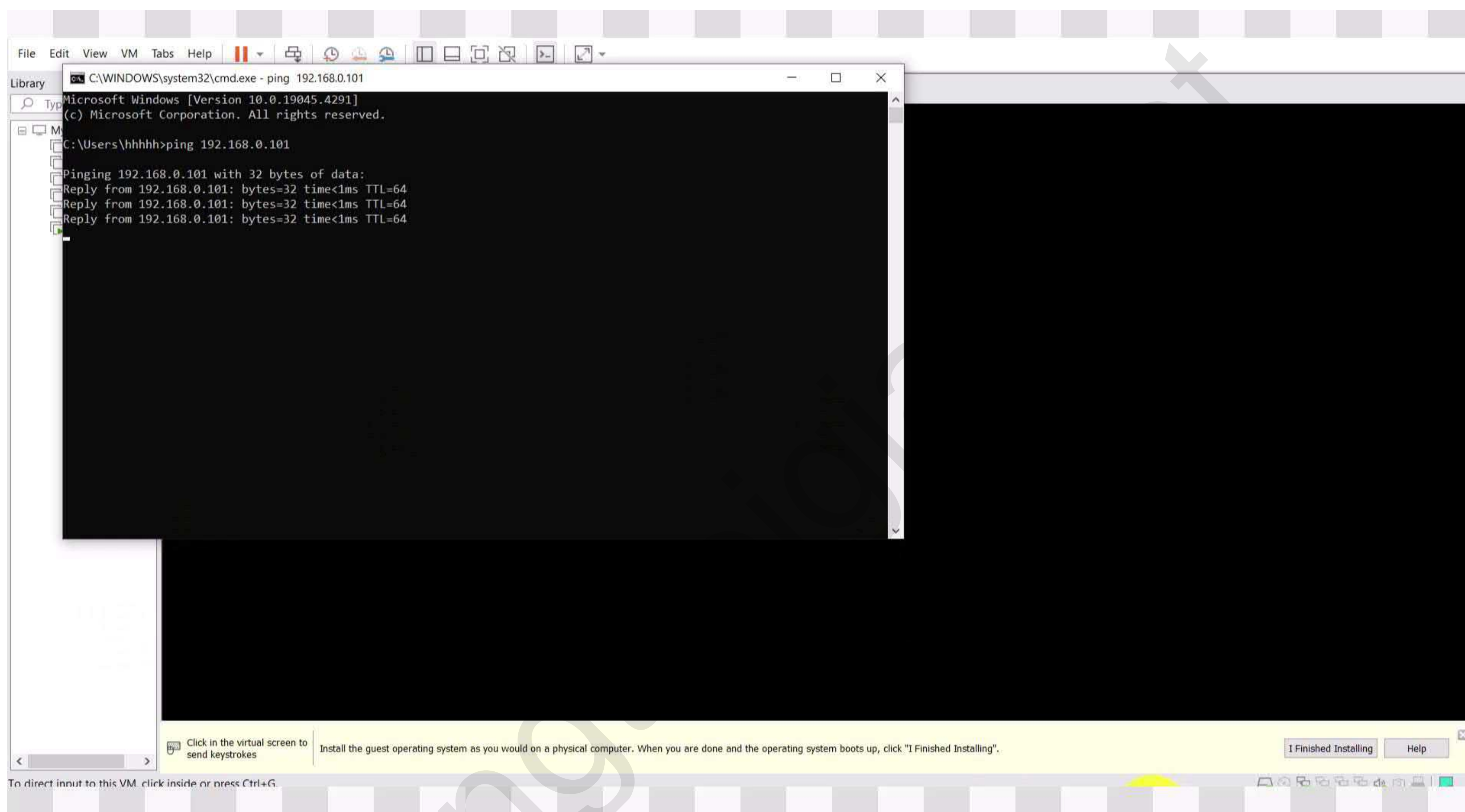
All configuration is done with WebAdmin. Go to <https://192.168.0.101:4444>  
in your browser.

192.168.0.101  
login: \_

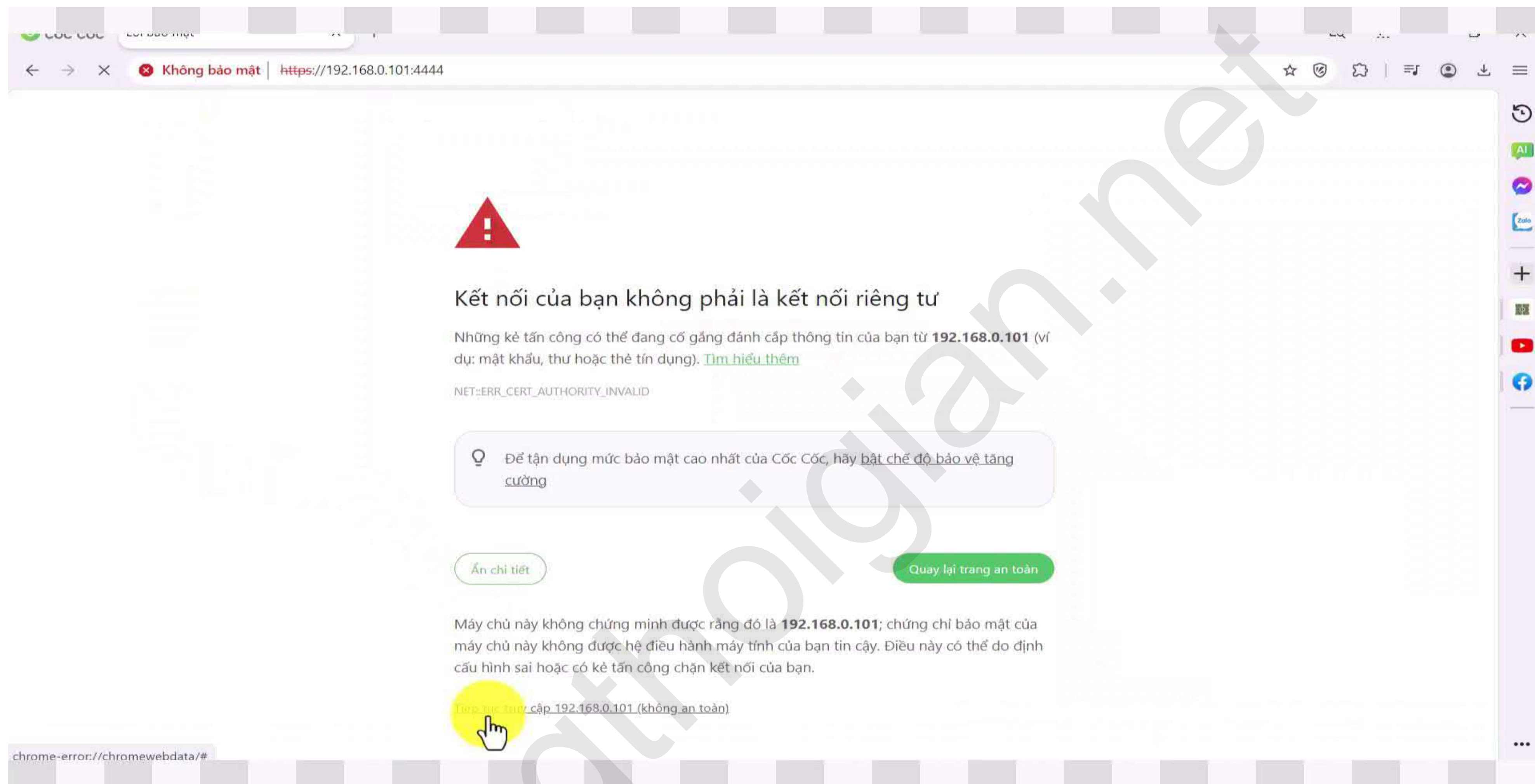


Như hình Hệ thống Sophos yêu cầu đăng nhập





Kiểm tra ip vừa rồi ta add vào như hình



Đăng Nhập Vào phần Quản Lý Sophos thông qua địa chỉ IP và thêm port 4444



**SOPHOS** UTM 9 | admin | ? | C | ⚙️

Dashboard for Friday, May 10, 2024 | 14:34:57

**demo**

Model: ASG Software  
License ID: 000000  
Subscriptions: Base Functionality  
Email Protection  
Network Protection  
Web Protection  
Webserver Protection  
Wireless Protection  
Uptime: 0d 0h 10m

Interface	Name	Type	State	Link	In	Out
all	All Interfaces				28.7 kbit	42.3 kbit
eth0	Internal	Ethernet	Up	Up	28.7 kbit	42.3 kbit
eth1	Unused					
eth2	Unused					
eth3	Unused					

**Advanced Threat Protection**

Botnet/command-and-control traffic detection is disabled 0 infected hosts

**Current System Configuration**

- Firewall is active with 5 rules
- Intrusion Prevention is inactive
- Web Filtering is inactive
- Network Visibility is inactive
- SMTP Proxy is inactive
- POP3 Proxy is inactive
- RED is inactive
- Wireless Protection is inactive
- Site-to-Site VPN is inactive
- Remote Access is inactive
- Web Application Firewall is inactive
- Sophos UTM Manager is not configured
- Sophos Mobile Control is inactive
- HA/Cluster is inactive
- Antivirus is inactive
- Antispam is inactive
- Antispyware is inactive

**Version Information**

Firmware version: 9.718-5  
1 Update(s) available for installation  
Pattern version: 239578  
Last check: 8 minutes ago

**Resource Usage**

CPU 0%  
RAM 10% of 4.3 GB  
Log Disk 0% of 19.7 GB  
Data Disk 8% of 14.9 GB

**Today's Threat Status**

Firewall: 79 packets filtered  
IPS: 0 attacks blocked  
Antivirus: 0 items blocked  
Antispam: 0 emails blocked  
Antispyware: 0 items blocked  
Web Filter: 0 URLs filtered  
WAF: 0 attacks blocked  
Sandstorm: 0 malicious items detected

Dashboard | Management | Definitions & Users | Interfaces & Routing | Network Services | Network Protection | Web Protection | Email Protection | Advanced Protection | Wireless Protection | Webserver Protection | RED Management | Site-to-site VPN | Remote Access | Logging & Reporting | Support | Log off

Giao Diện Tường lửa (Fireware) SoPhos