**THỰC HÀNH NHẬP MÔN MÁY TÍNH**

**Lab 3: Thiết lập mô hình tường lửa Sophos**

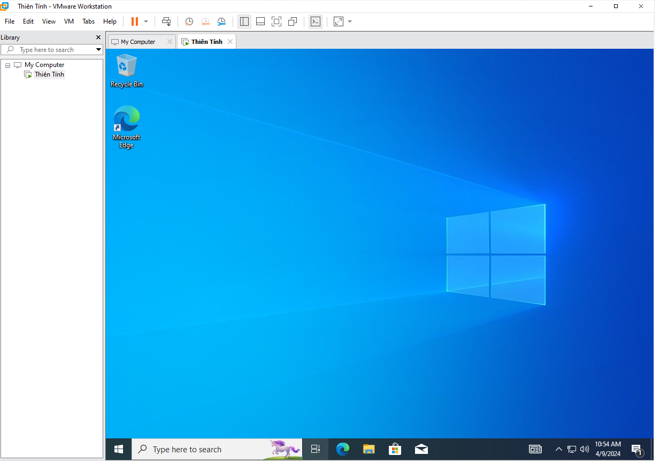
**Họ và tên: Nguyễn Thiên Tính**

**MSSV: 0950080144**

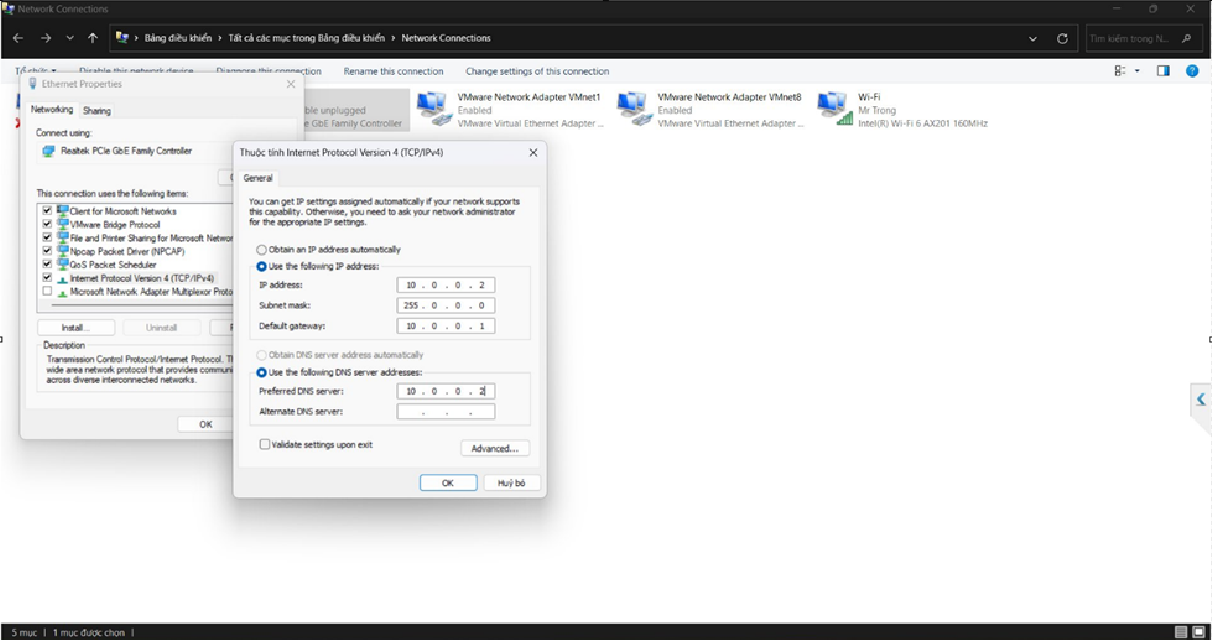
**Lớp: 09\_ĐH\_CNPM3**

**1. Thiết lập máy chć Domain Controller**

• Bước 1: Chuẩn bị máy ảo làm Domain Controller:



Bước 2: Đặt IP cho máy Domain Controller là 10.0.0.2/8

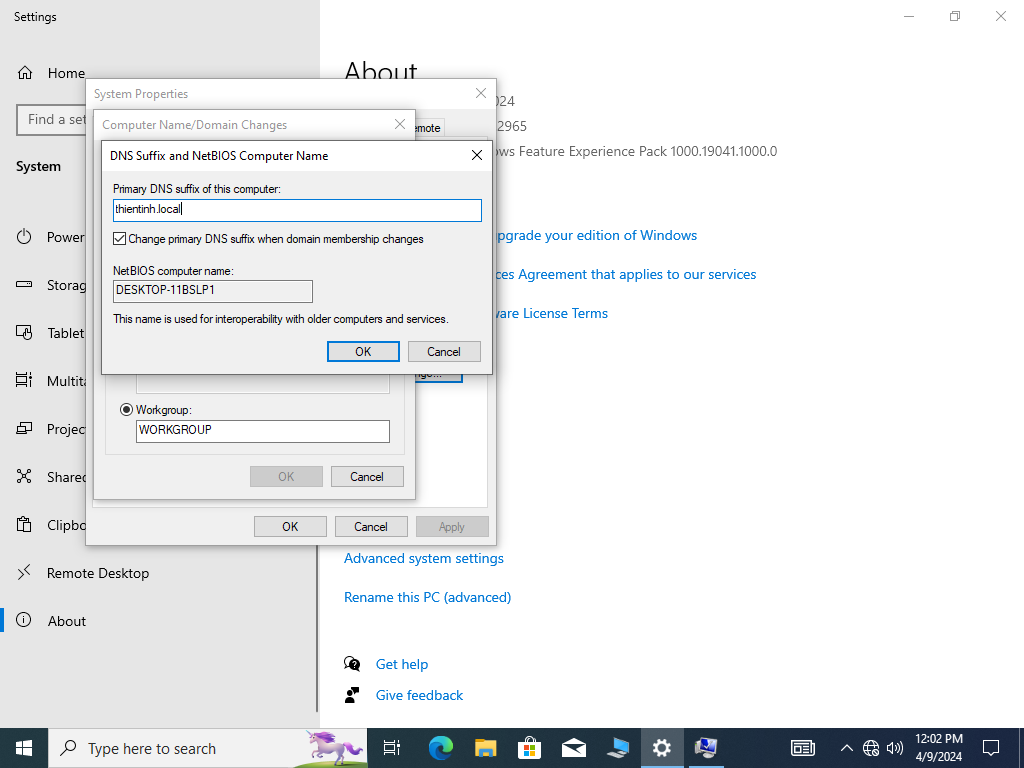


Bước 3: Đặt DNS Suffix bằng cách click phải lên My Computer &gt; Propertites &gt;

Change Setting &gt; Change &gt; chọn More.

Sau đó nhập DNS Suffix cần đặt. Trong hướng dẫn này sử dụng tên uit.local, để phân

biệt khi thực hiện sinh viên đặt theo dạng tên 2 sinh viên.local. Ví dụ vietnam.local

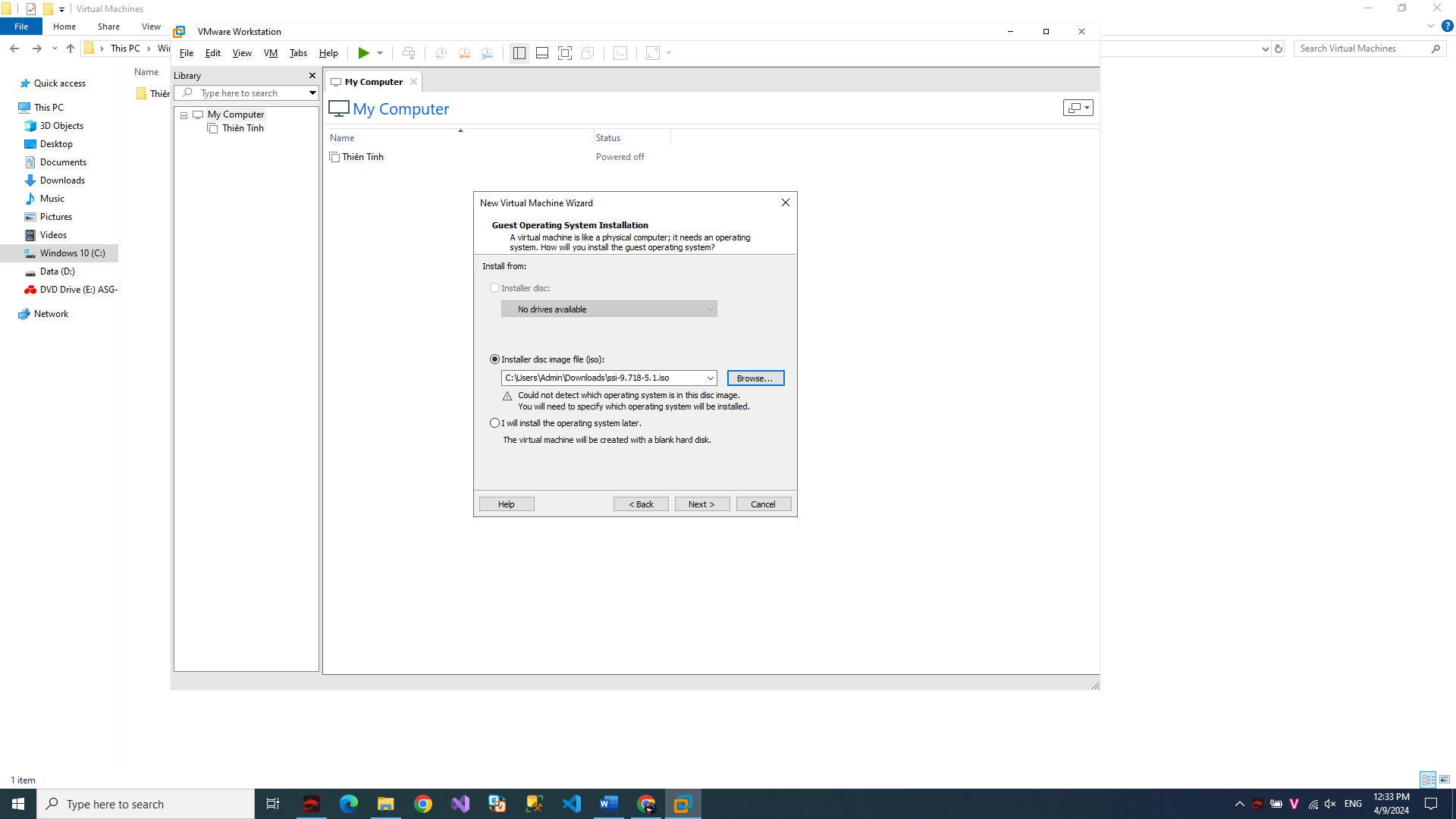


**2. Cài đặt và cấu hình máy Firewall Sophos UTM**

• Bước 1: Tải Sophos UTM 9.4, ta được file ISO cài đặt asg-9.406-3.1.iso

• Bước 2: Tạo máy ảo mới bằng VMware và load file iso của Sophos UTM 9 để

cài đặt tường lửa Sophos UTM.



Máy ảo để Firewall Sophos hoạt động có thông số như sau:

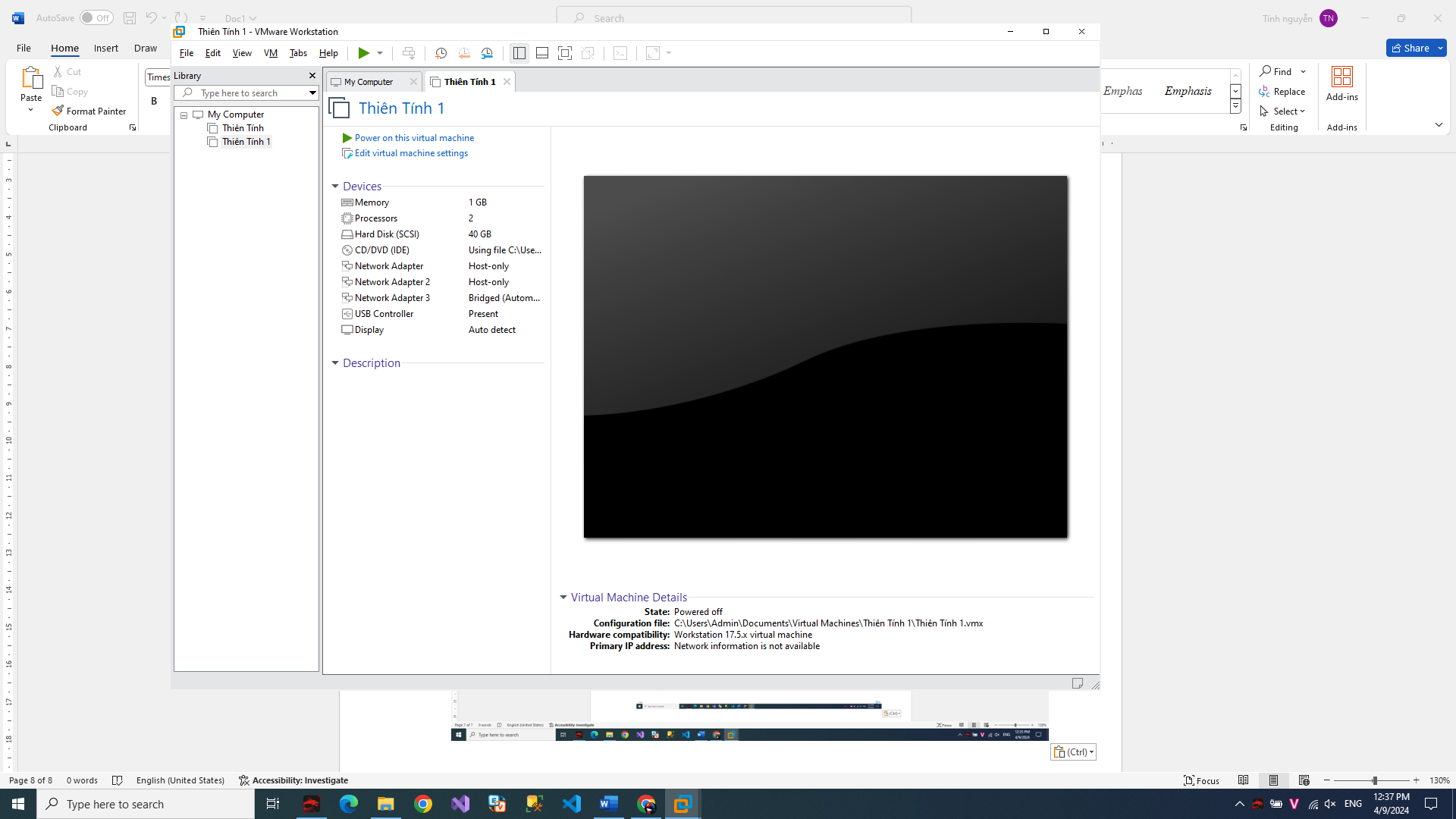
- RAM 1GB (hoặc 2GB)

- Có 3 card mạng:

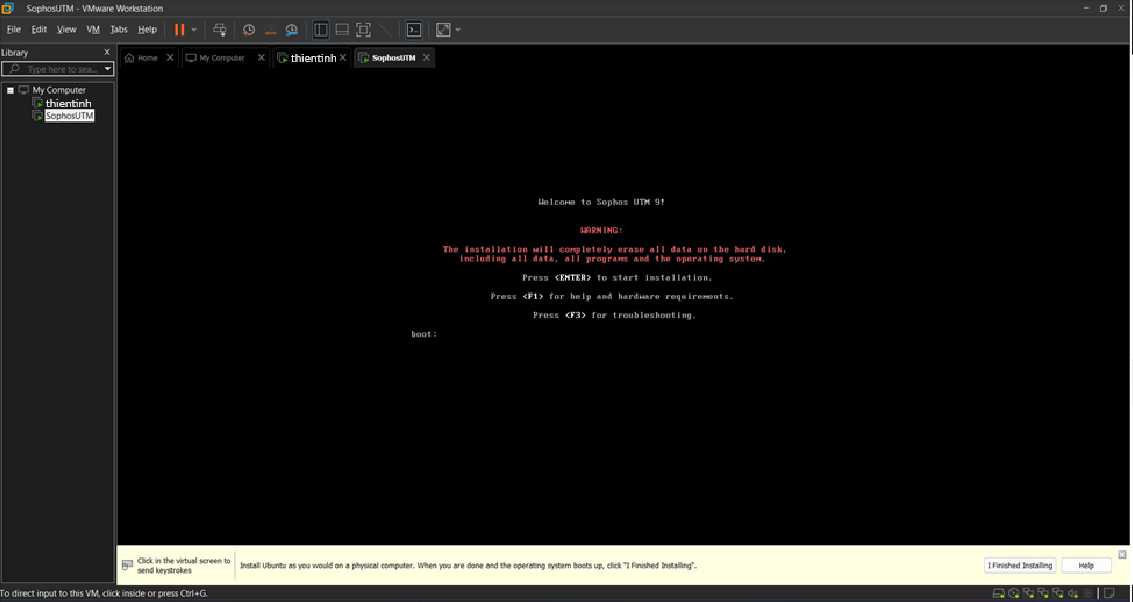
+ Card 1: Host-only

+ Card 2: Host-only

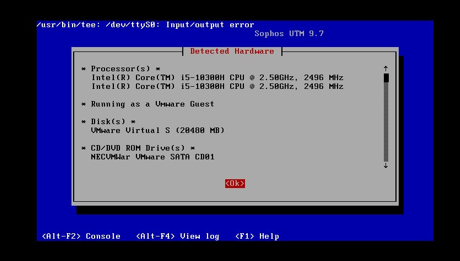
+Card 3: Bridge (kết nối Internet qua máy thật)



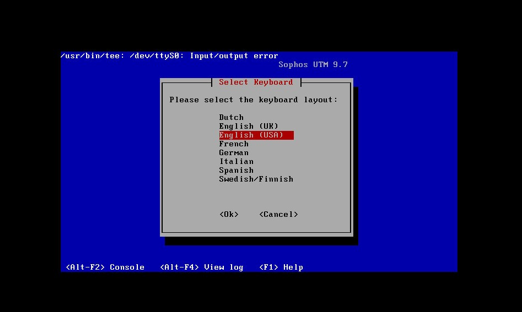
• Bước 3: Khởi động máy ảo và nhấn Enter để bắt đầu cài đặt



* Sau đó, nhấn Start để bắt đầu



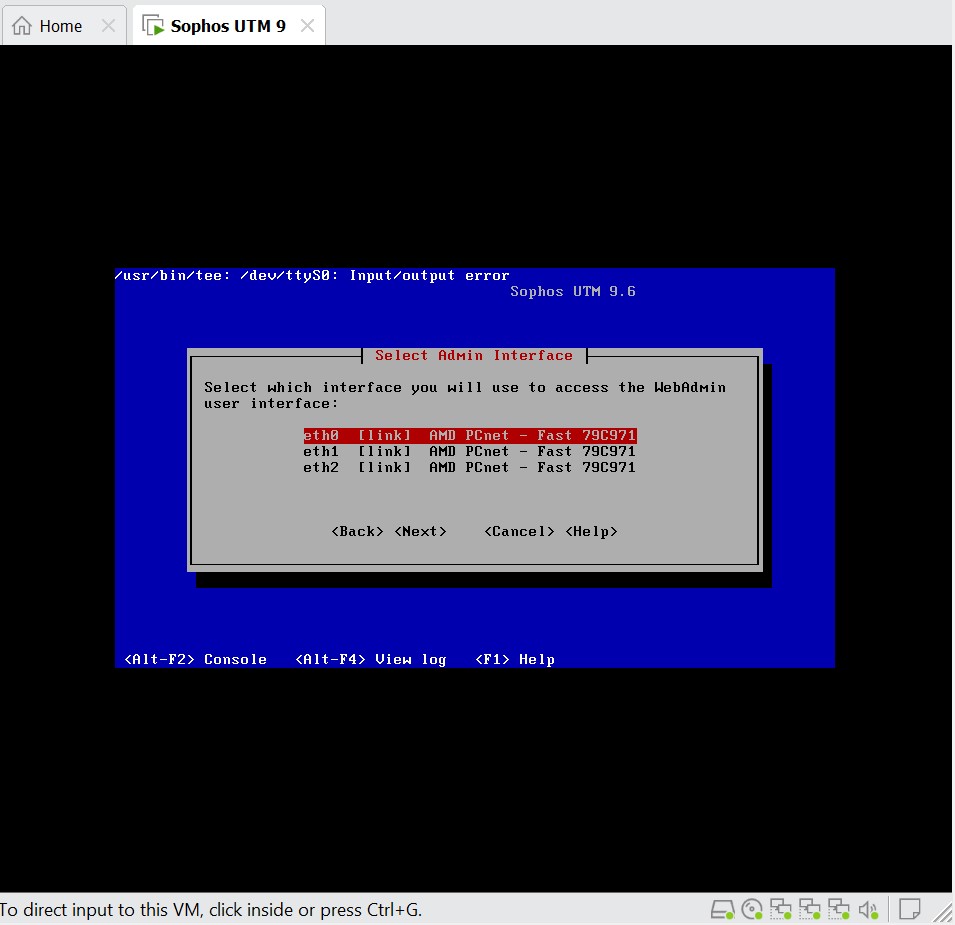
Bước 4: Thiết lập ngôn ngữ và thêm múi giờ



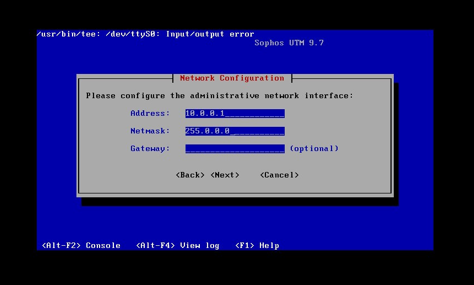


Bước 5: Chọn card mạng eth0 và thiết lập IP mặc định cho trang quản trị

Chọn card mạng eth0 cho WebAdmin của Firewall

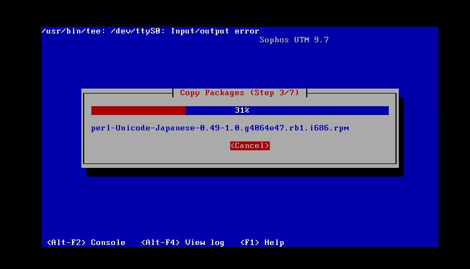


Thiết lập IP quản trị 10.0.0.1 cho Filewall

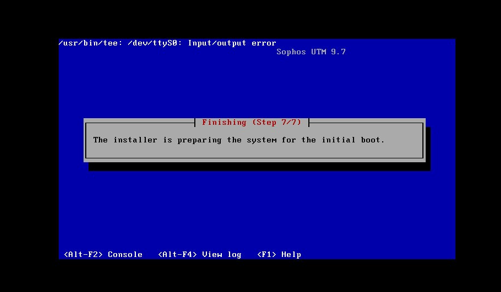


Chọn Yes nếu sử dụng CPU hỗ trợ 64 bit kernel

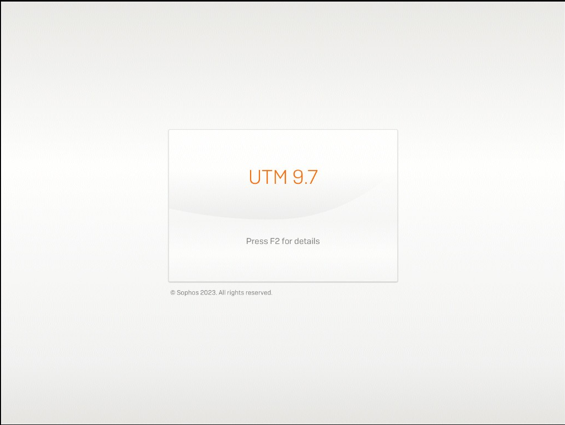
Quá trình cài đặt diễn ra trong 6 bước:



* Sau khi cài đặt thành công sẽ thông báo địa chỉ IP đăng nhập vào trang quản trị WebAdmin là <http://10.0.0.1:4444/>



Bước 6: Khởi động lại Firewall Sophos UTM Quá trình khởi động diễn ra



Khỏi động thành công Firewall

* Sau khi khỏi động thành công, chúng ta sẽ thấy IP được dùng để kết nối v trang quản trị Firewall 10.0.0.1 (tài khoảng mặc định để đăng nhập là root và mật khẩu ở lần đầu tiên, tuy nhiên chúng ta thực hiện các thiết lập cho Firewall qua WebAdmin).

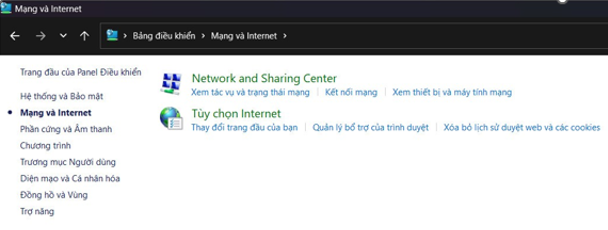


Bước 7: Thiết lập lớp mạng cho VMnet1

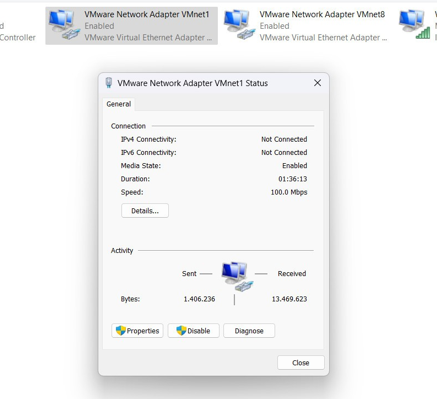
 Vào Control Panel &gt; Network and Internet



 Chọn Network and Sharing Center



 Chọn VMware Network Adapter VMnet1 &gt; Properties



 Kích đúp chọn Internet Protocol version 4

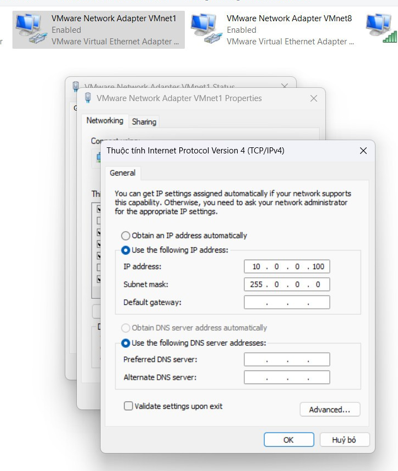


 Tích Chọn Use the following IP address

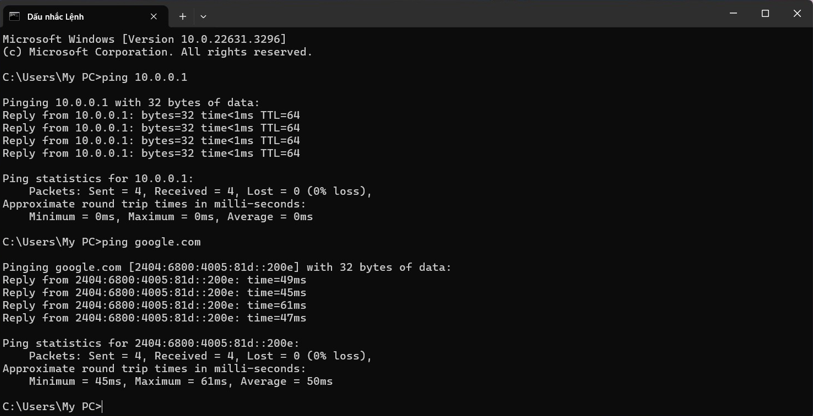
o IP address:10.0.0.100

o Subnet mask: 255.0.0.0

 Hoàn thành thì chọn OK

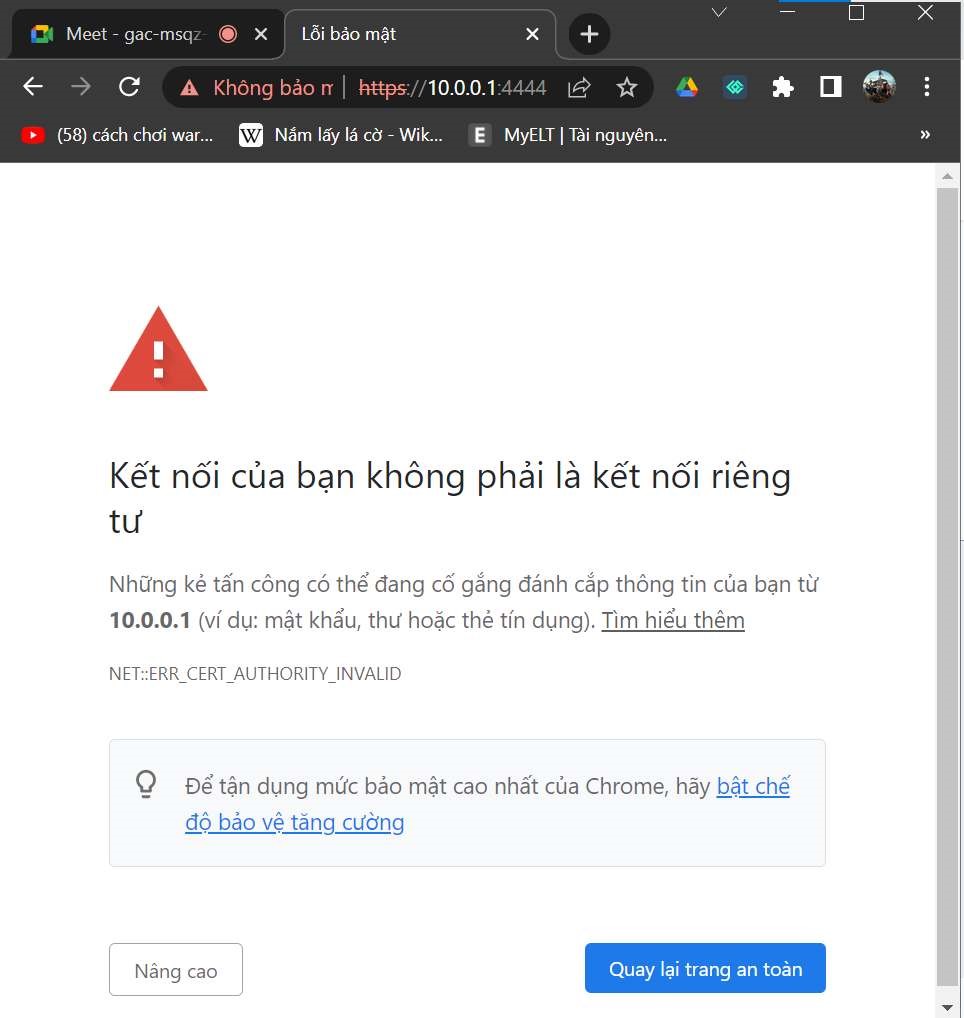


Bước 8: Ở máy thật, Thực hiện lệnh ping 10.0.0.1 trong CMD



Bước 9: Truy cập WebAdmin của Firewall bằng địa chỉ https://10.0.0.1:4444 . Nếu gặp

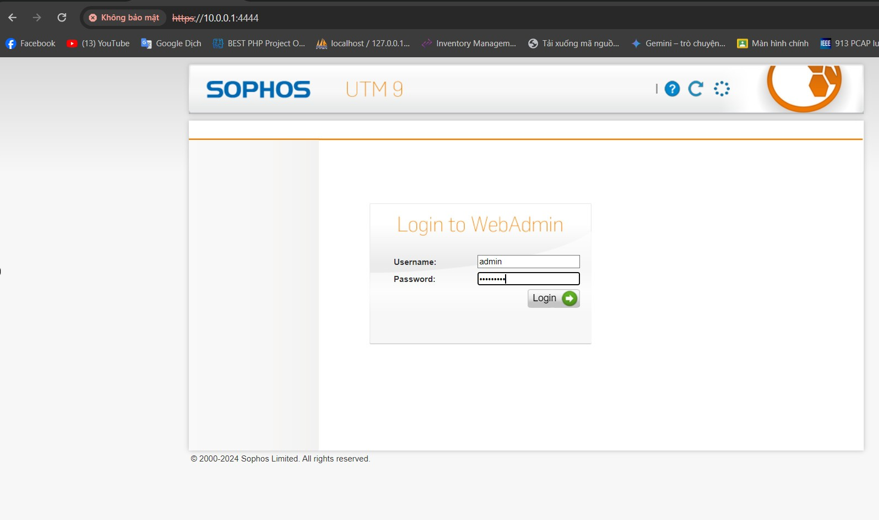
cảnh báo bảo mật của trình duyệt, bỏ qua và tiếp tục truy cập WebAdmin



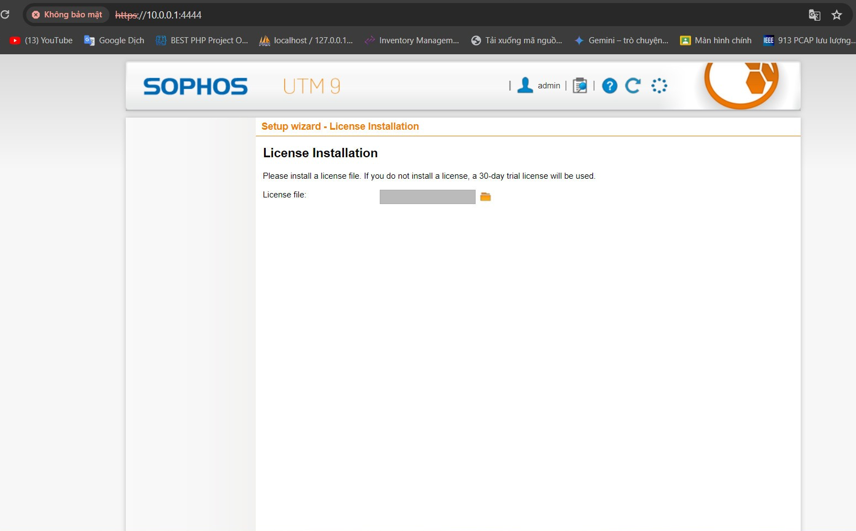
Bước 10: Thiết lập các thông tin cơ bản cho Firewall Sophos và đặt

mật khẩu cho tài khoảng admin

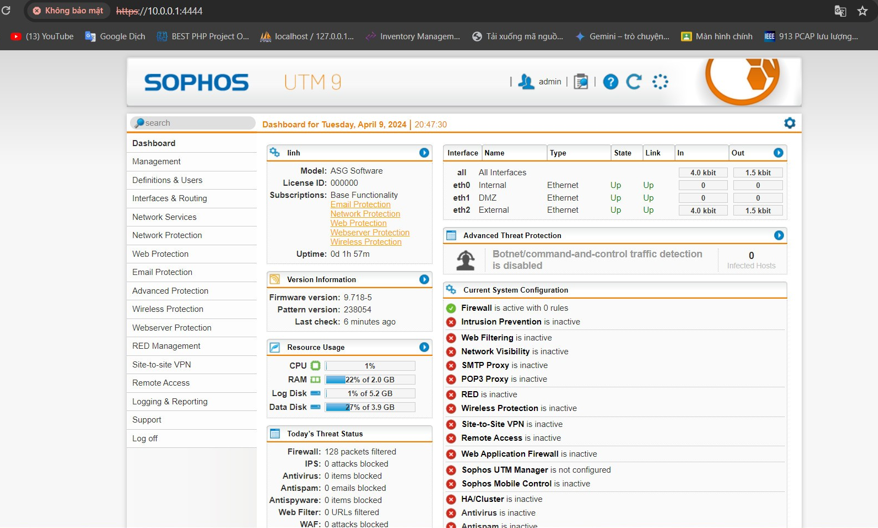
Bước 11: sau đó đăng nhập với user và pass vừa mới thiết lập



Bước 12: Sau khi đăng nhập thành công chọn Cancel để bỏ qua Wizad



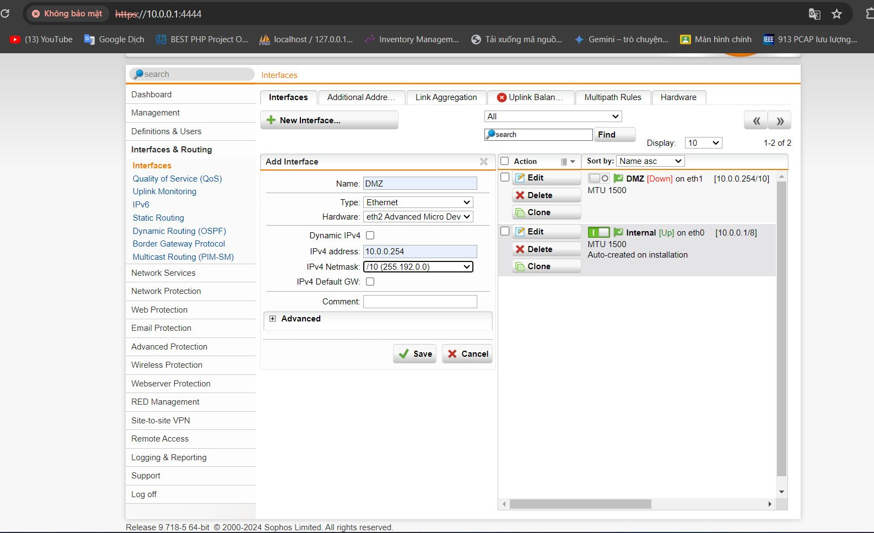
* Giao diện quản lý Firewall



Bước 13: Cấu hình các interface cho các Firewall theo đúng mô hình triển khai. Vào Interface & Routing để thiết lập các interface

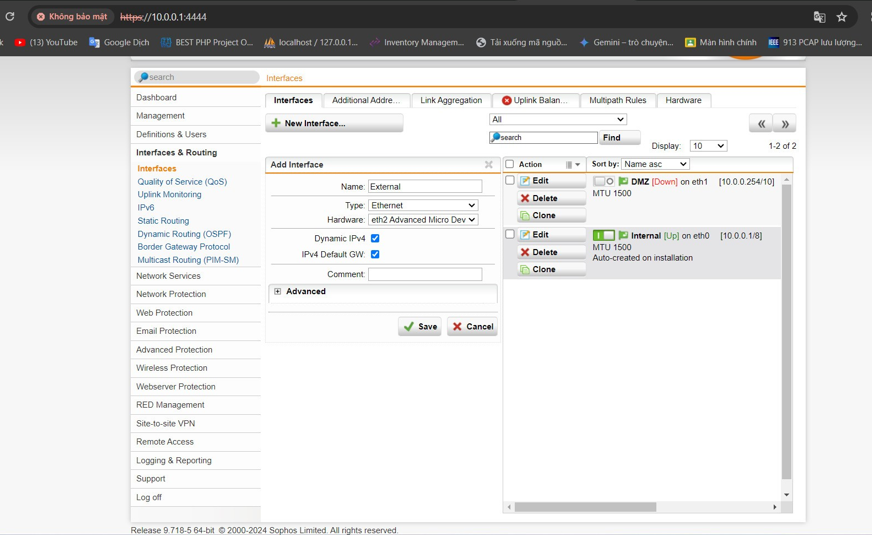
* Tạo interface cho vùng DMZ

Chọn New Interface và thiết lập như sau



* Tạo Interface External để kết nối Internet:

Chọn New Interface và thiết lập như sau

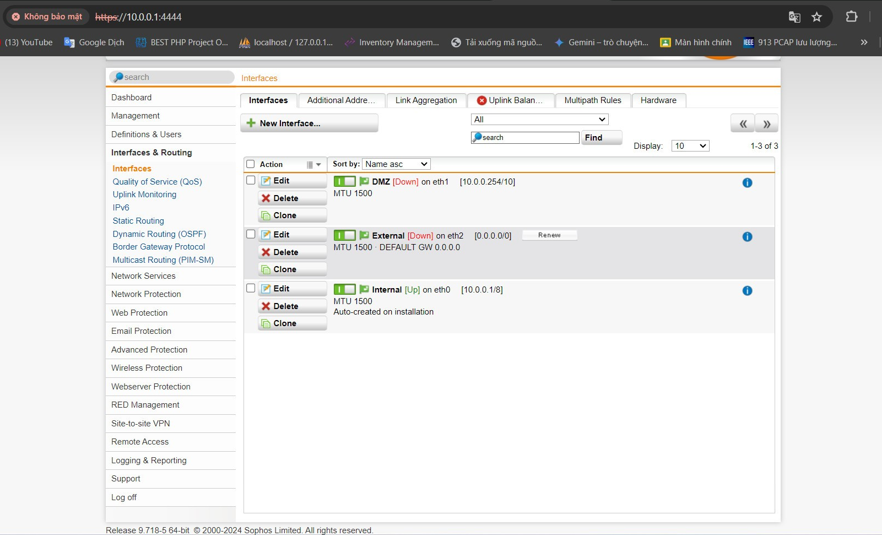


* eth1: là card mạng thứ 2 của máy ảo Sophos firewall UTM 9

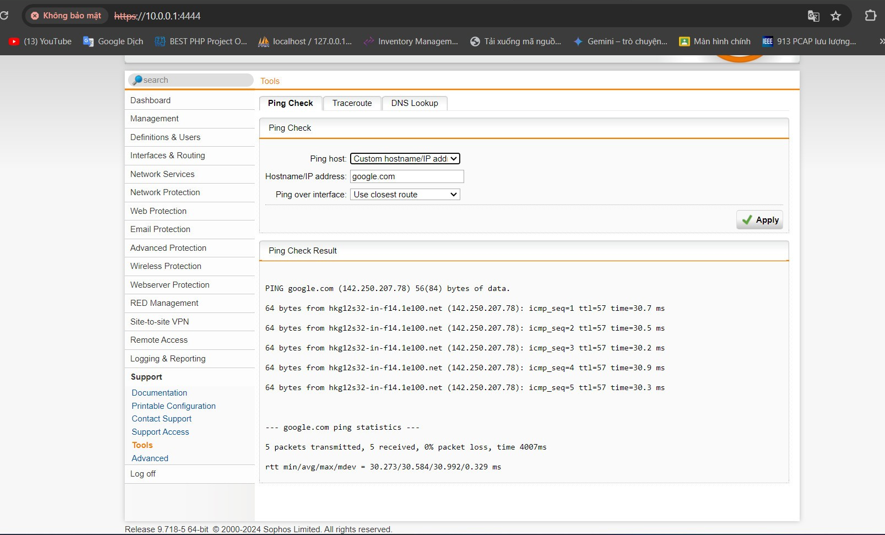
(VMnet1)

* eth2: là card mạng thứ 3 của máy ảo Sophos firewall UTM 9 (VMnet0) chính là card internet

Bước 14: Bật cả 3 interface và đặc biệt interface External đã nhận được IP từ DHCP Server hay chưa



* Kiểm tra xem Firewall có kết nối được internet hay không bằng cách vào Support > Tool > dùng tool Ping check để ping google.com dùng interface External

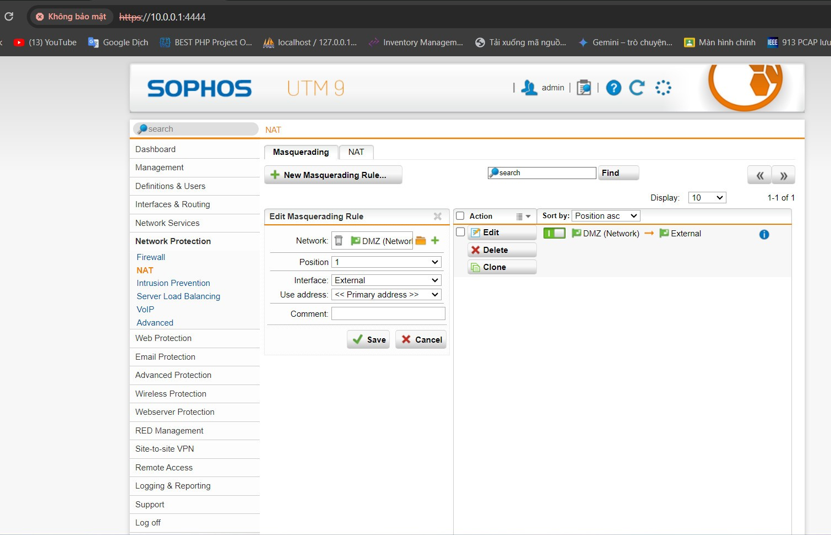


Thành công

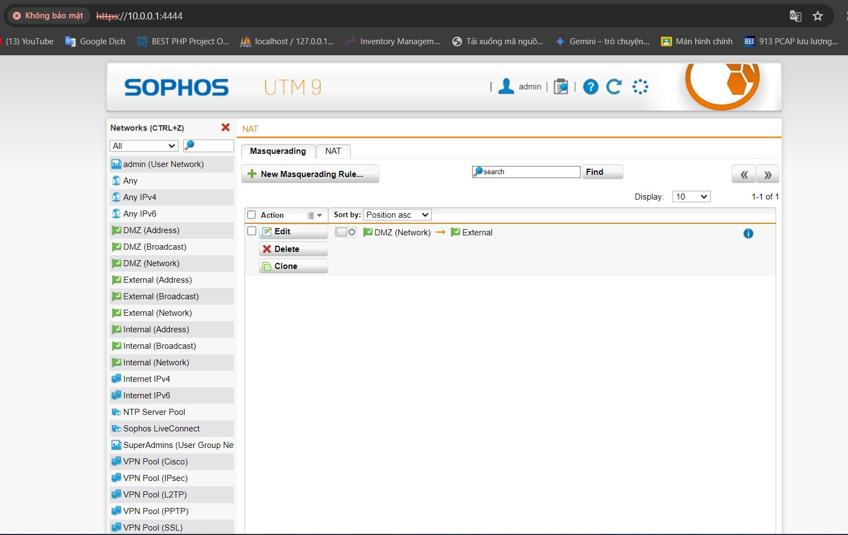
Lưu ý: Nếu không kết nối được hay interface External không nhận được IP thì cần kiểm tra lại cấu hình hoặc restart lại Firewall

Bước 15: Cấu hình NAT outbound. Cơ chế NAT sẽ xác định mạng nào sẽ NAT mạng ra ngoài Internet.

* Vào Network Protection > NAT > New Masquerading Rule và cấu hình như sau:
* DMZ là vùng mạng cho tổ chức nhỏ là VMnet1 để chia cho các máy có card mạng vùng VMnet1

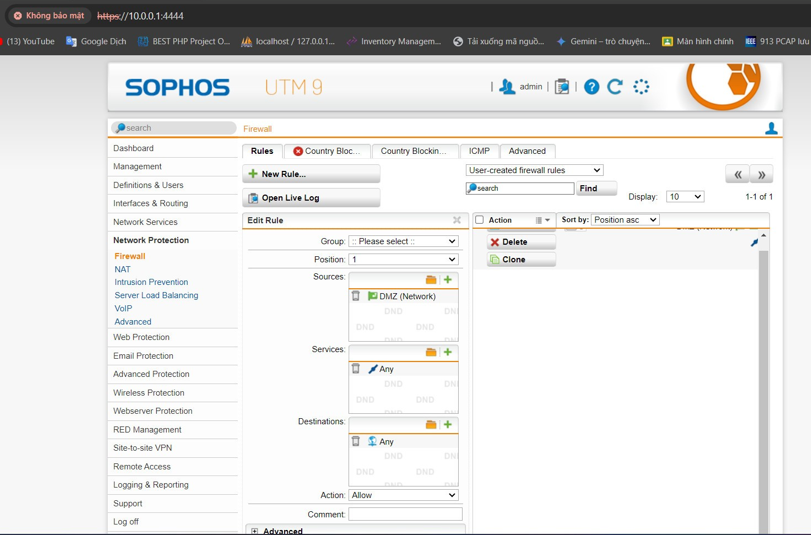


Sau khi kích hoạt Masquerading này. Kết quả sau khi cấu hình



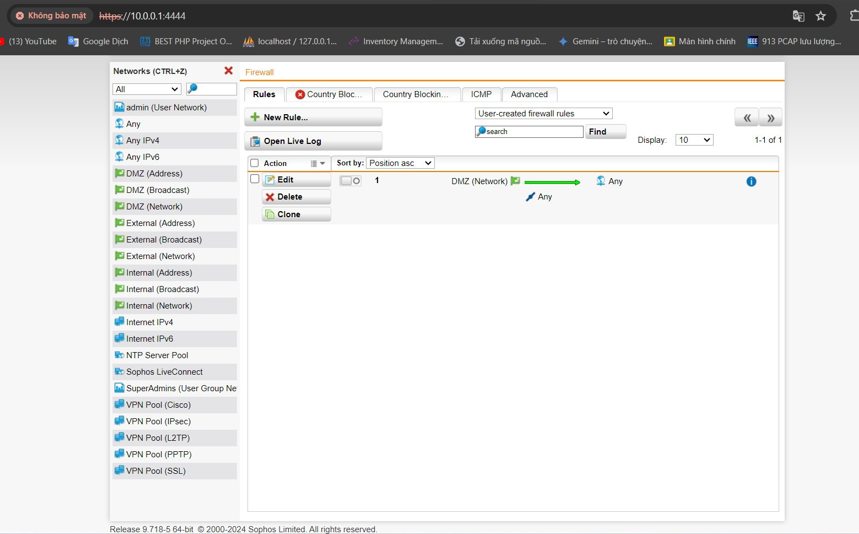
Bước 16: Cấu hình Rule để máy chủ Domain Controller kết nối được internet bình thường. Vào Network Protection > Firewall >

New Rule

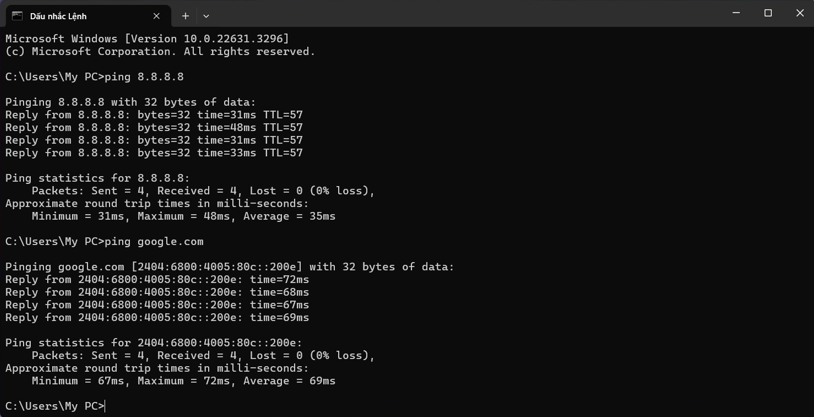


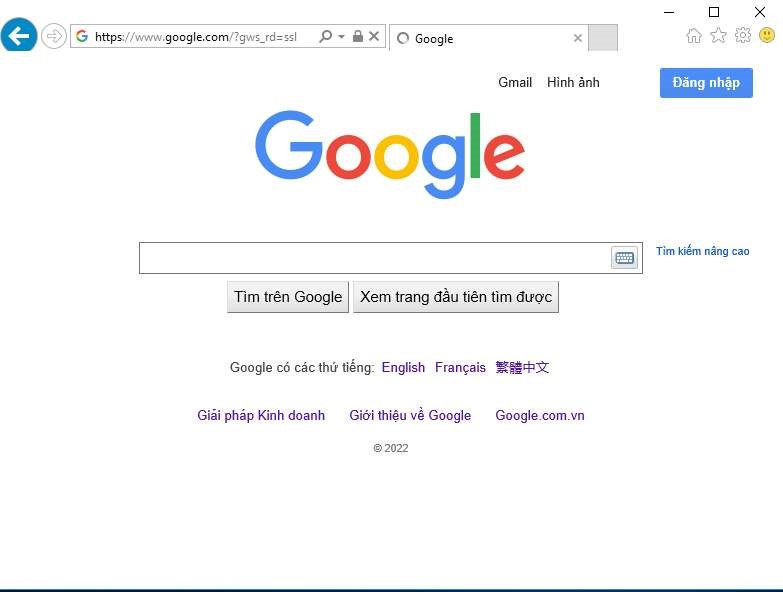
* Sources: là vùng mạng DMZ (đầu)
* Services: là dịch vụ của mạng đó
* Destinations: là vùng muốn được truyền mạng DMZ (cuối)

Kết quả



Bước 17: Kiểm tra kết nối Internet của máy chủ Domain Controller





Bước 18: Quay lại trang WebAdmin của Firewall thử tắt Rule

Firewall và một vào Rule vừa thiết lập và quay lại máy Domain Controller để truy cập Internet và kết luận rằng

