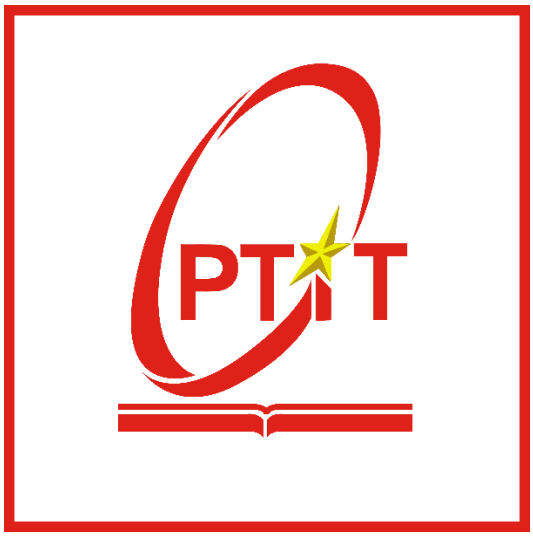
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN



Môn học: **THỰC TẬP CƠ SỞ**

BÁO CÁO BÀI THỰC HÀNH SỐ 7

CÀI ĐẶT CẤU HÌNH VPN SERVER

Sinh viên thực hiện: Lê Anh Tuấn

Mã sinh viên: B21DCAT205

Giảng viên: Ninh Thị Thu Trang

~ Hà Nội, tháng 3/2024 ~

Mục Lục

BÀI 7: Cài đặt, cấu hình VPN server

1 Mục đích

Tìm hiểu về mạng riêng ảo (VPN-Virtual Private Network), kiến trúc và hoạt động của mạng riêng ảo.

Luyện tập kỹ năng cài đặt, cấu hình và vận hành máy chủ mạng riêng ảo (VPN server).

2 Nội dung thực hành

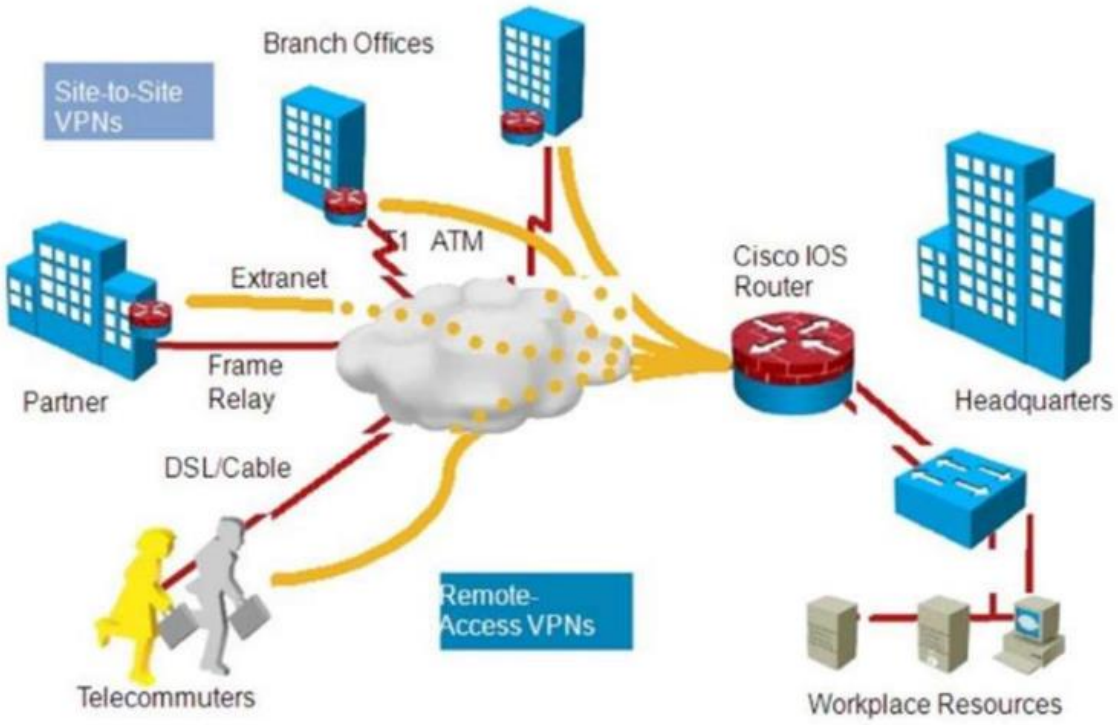
2.1 Tìm hiểu lý thuyết

a) VPN

- Khái quát về VPN:

VPN là mạng riêng ảo, Virtual Private Network, là một công nghệ mạng giúp tạo kết nối mạng an toàn khi tham gia vào mạng công cộng như Internet hoặc mạng riêng do một nhà cung cấp dịch vụ sở hữu. Các tập đoàn lớn, các cơ sở giáo dục và cơ quan chính phủ sử dụng công nghệ VPN để cho phép người dùng từ xa kết nối an toàn đến mạng riêng của cơ quan mình.

- Các mô hình VPN:



Hình 1: mô hình VPN

- Một số ứng dụng của VPN:

+ Truy cập vào mạng doanh nghiệp, gia đình khi ở xa
+ Duyệt web ẩn danh
+ Truy cập đến những website bị chặn giới hạn địa lý
+ Tải tập tin

b) Các giao thức tạo đường hầm cho VPN: PPTP, L2TP, L2F, MPLS...

- *PPTP*

PPTP được xem là một thuật ngữ dùng trong lĩnh vực công nghệ thông tin.

Nó là một dạng cổng kết nối và chia sẻ nguyên liệu từ máy chủ đến các loại máy chia sẻ vật lý trong một đường dây kết nối mạng. PPTP được sáng chế và bắt đầu hoạt động từ những năm đầu của thế kỷ 21.

PPTP dùng trong hệ thống PTC là chủ yếu. Tuy loại giao thức này vẫn còn 1 số hạn chế nhưng là sự đánh dấu thay đổi lớn trong các giao thức mới nhất, trong kỹ thuật chia sẻ nguyên liệu mới hiện nay

- *L2TP*

L2TP là viết tắt của Layer 2 Tunneling Protocol, một giao thức tunneling (tạo "đường hầm" truyền dữ liệu qua các mạng). L2TP hỗ trợ tạo mạng riêng ảo VPN hoặc là một thành phần của mạng phân phối dịch vụ của ISP. L2TP chỉ sử dụng mã hóa cho tin nhắn điều khiển mà không cung cấp bất cứ lớp mã hóa hay bảo mật nào cho nội dung dữ liệu.

- *L2F*

Giao thức định hướng lớp 2 L2F do Cisco phát triển độc lập và được phát triển dựa trên giao thức PPP (Point-to-Point Protocol). L2F cung cấp giải pháp cho dịch vụ quay số ảo bằng cách thiết lập một đường hầm bảo mật thông qua cơ sở hạ tầng công cộng như Internet. L2F là giao thức được phát triển sớm nhất, là phương pháp truyền thống để cho những người sử dụng ở xa truy cập vào một mạng công ty thông qua thiết bị truy cập từ xa. L2F cho phép đóng gói các gói PPP trong L2F, định đường hầm ở lớp liên kết dữ liệu.

- *MPLS*

MultiProtocol Label Switching (MPLS) là một kỹ thuật để tăng tốc kết nối mạng được phát triển lần đầu vào những năm 1990. Internet công cộng hoạt động bằng cách chuyển tiếp các packet từ router này sang router khác đến khi các packet đến đích. Mặt khác, MPLS gửi các packet theo các đường dẫn

c) Các giao thức bảo mật cho VPN: IPSec, SSL/TLS.

IP security (IPSec)

Được dùng để bảo mật các giao tiếp, các luồng dữ liệu trong môi trường Internet (môi trường bên ngoài VPN). Đây là điểm mấu chốt, lượng traffic qua IPSec được dùng chủ yếu bởi các Transport mode, hoặc các tunnel (hay gọi là hầm - khái niệm này hay dùng trong Proxy, SOCKS) để MÃ HÓA dữ liệu trong VPN.

Secure Sockets Layer (SSL) và Transport Layer Security (TLS)

Có 1 phần tương tự như IPSec, 2 giao thức trên cũng dùng mật khẩu để đảm bảo an toàn giữa các kết nối trong môi trường Internet.

Bên cạnh đó, 2 giao thức trên còn sử dụng chế độ Handshake - có liên quan đến quá trình xác thực tài khoản giữa client và server. Để 1 kết nối được coi là thành công, quá trình xác thực này sẽ dùng đến các Certificate - chính là các khóa xác thực tài khoản được lưu trữ trên cả server và client.

d) Tìm hiểu về SoftEther VPN

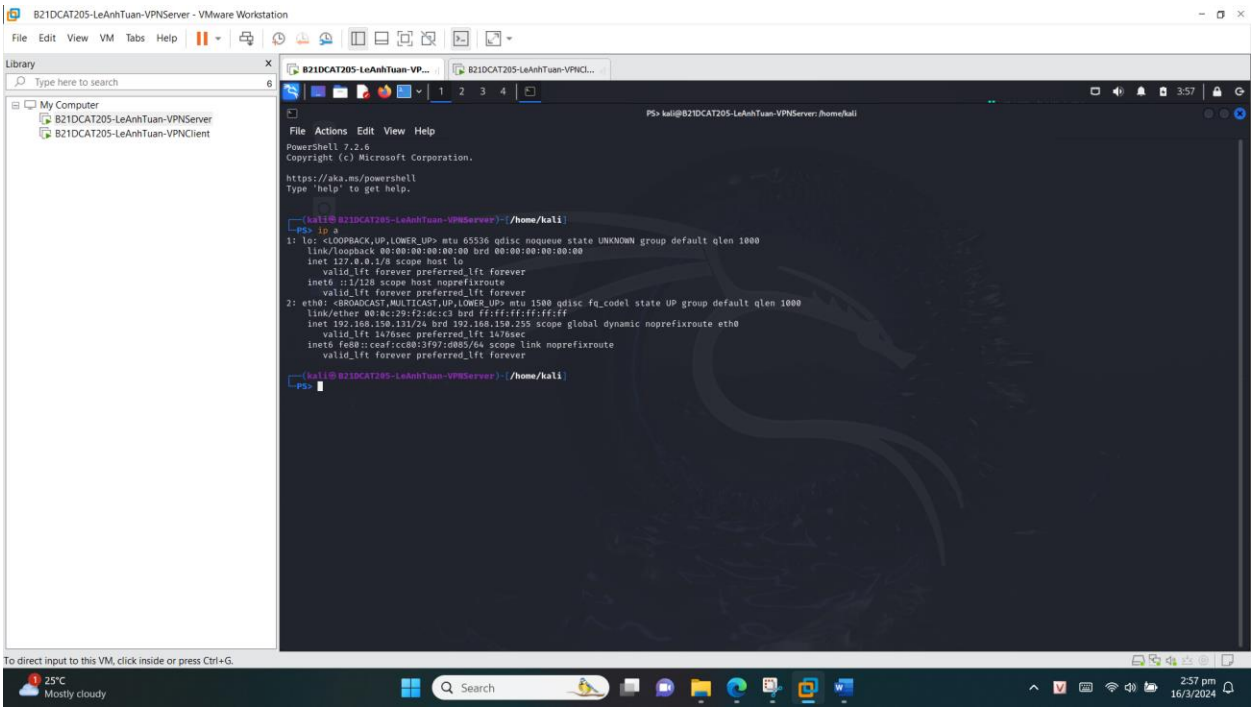
- Softether là một dự án VPN tương đối mới giúp công nghệ VPN trở nên an toàn hơn, cho phép người dùng lướt web ẩn danh và BẢO MẬT cao hơn.

- Hiện tại, SoftEther VPN hỗ trợ Windows, Linux, Mac, Solaris, FreeBSD và thường là một lựa chọn tốt để thay thế cho OpenVPN vì nhanh hơn. SoftEther VPN cũng hỗ trợ Microsoft SSTP VPN cho Windows Vista/7/8.

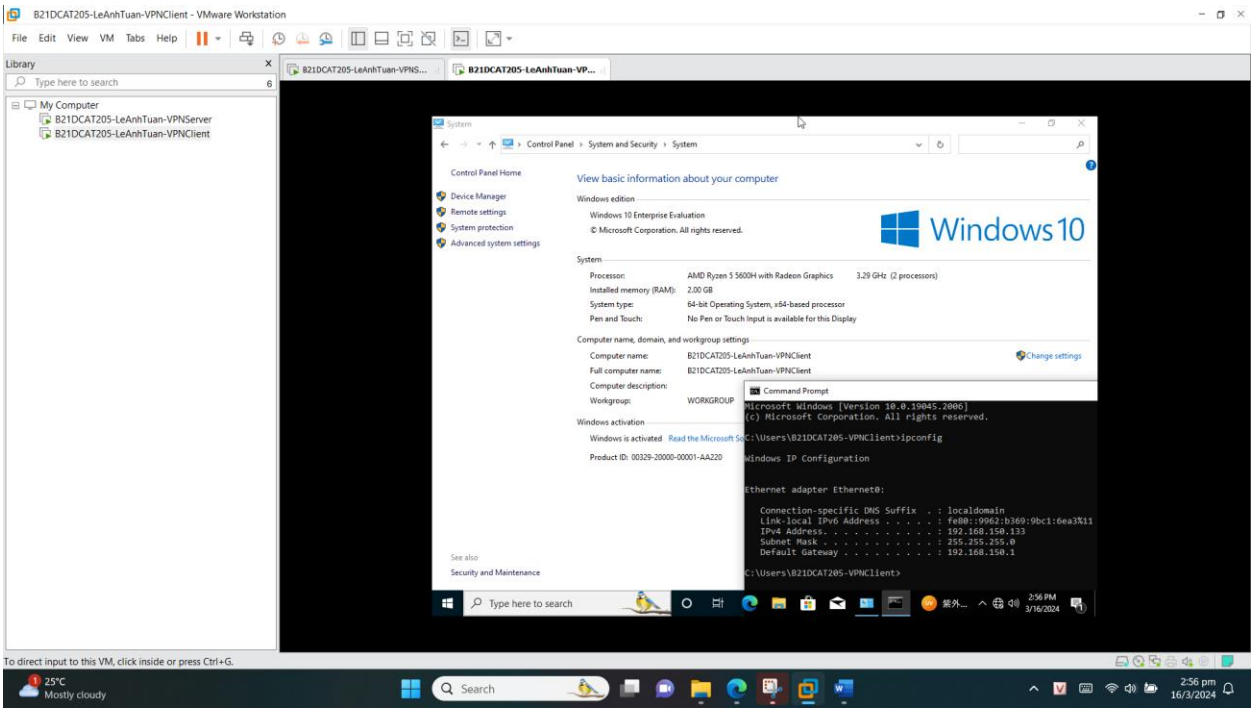
- Bên cạnh ưu điểm nhanh, SoftEther VPN còn sử dụng key certificate AES 256 bit, 1 cấp độ bảo mật và mã hóa cao. Thêm một điểm cộng lớn cho phần mềm này là nó tích hợp tất cả các tính năng của các giao thức VPN khác nhau như PPTP, L2TP, OpenVPN và SSTP, trong khi loại bỏ nhược điểm của chúng.

2.2 Các bước thực hiện

Bước 1: Chuẩn bị các máy. Máy Windows 10 được đổi tên thành **B21DCAT205-LeAnhTuan-VPNClient** và máy **Kali** cài VPN server đổi thành **B21DCAT205-LeAnhTuan--VPNServer**. Các máy có địa chỉ IP và kết nối mạng LAN.

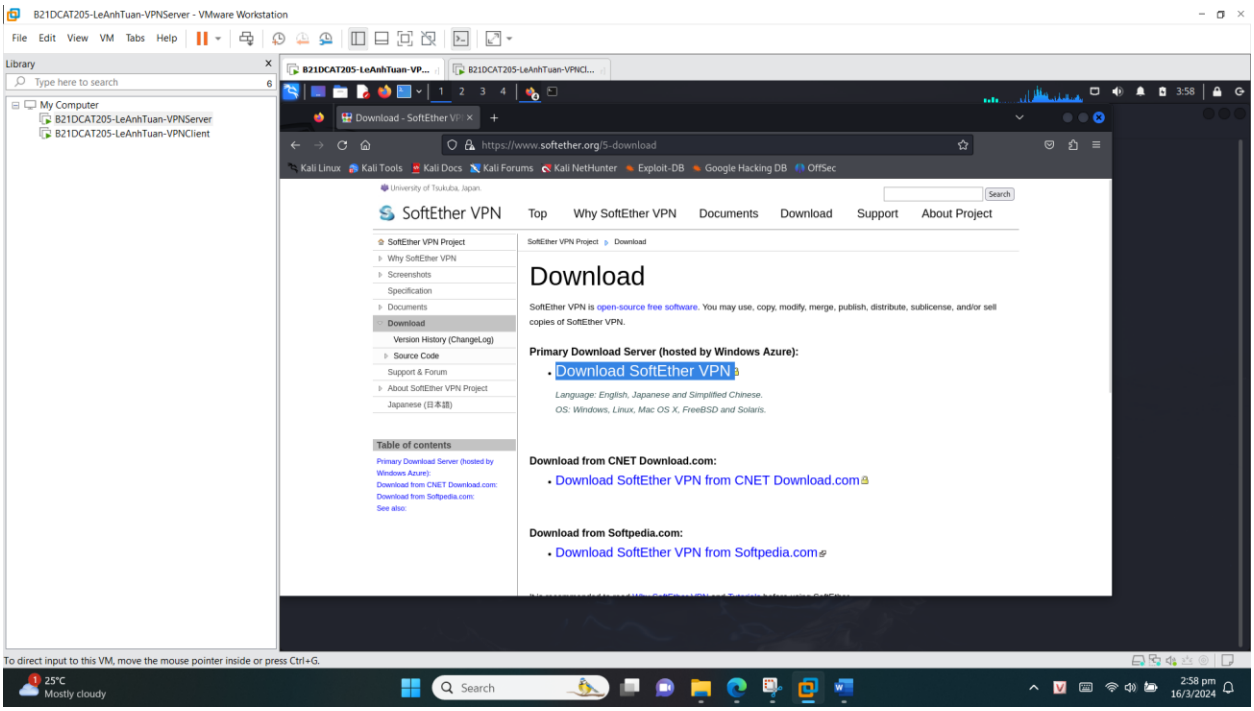


Hình 2: IP máy VPNServer

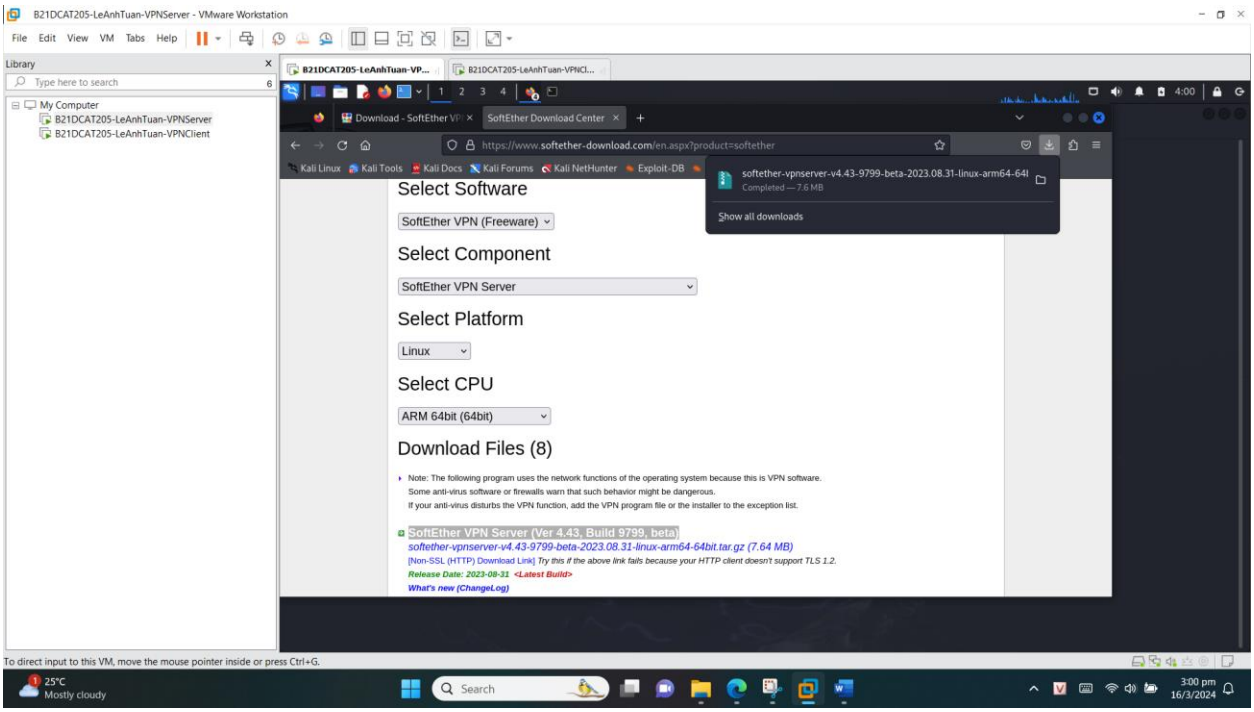


Hình 3: IP máy VPNClient

Bước 2: Tải **SoftEther VPN Server** tại **https://www.softether.org/5-download.**

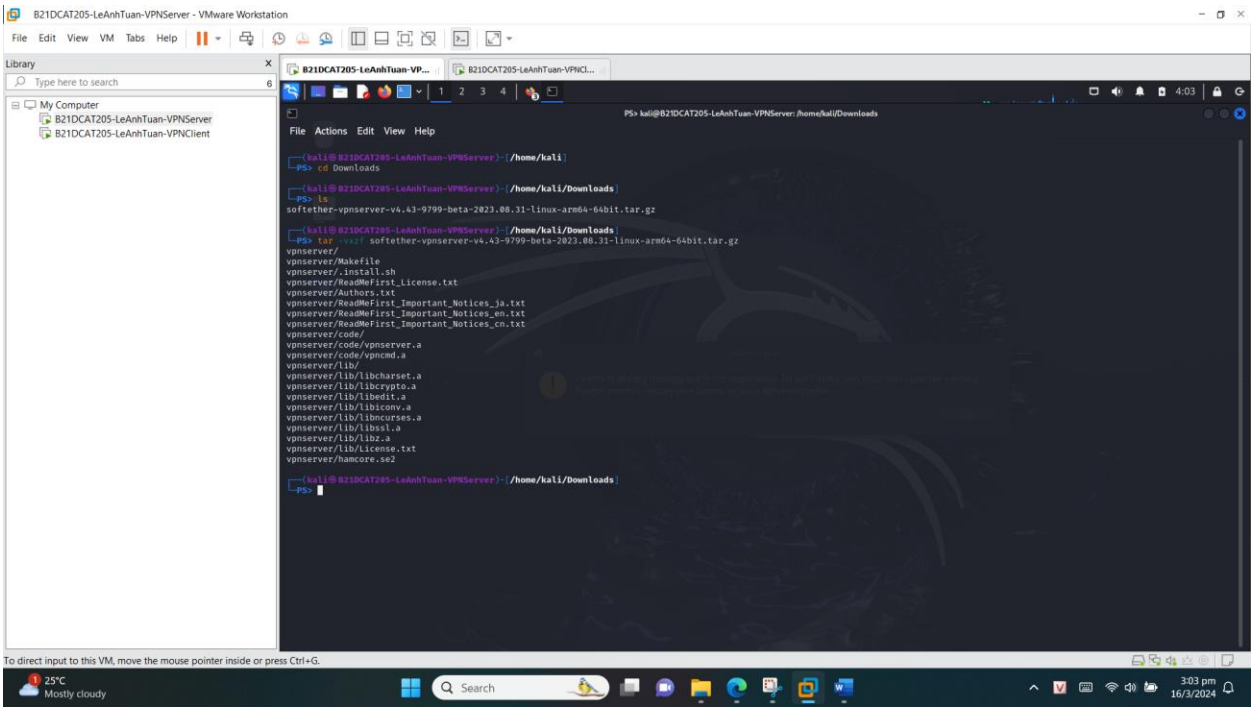


Hình 4: Chọn Download SoftEther VPN



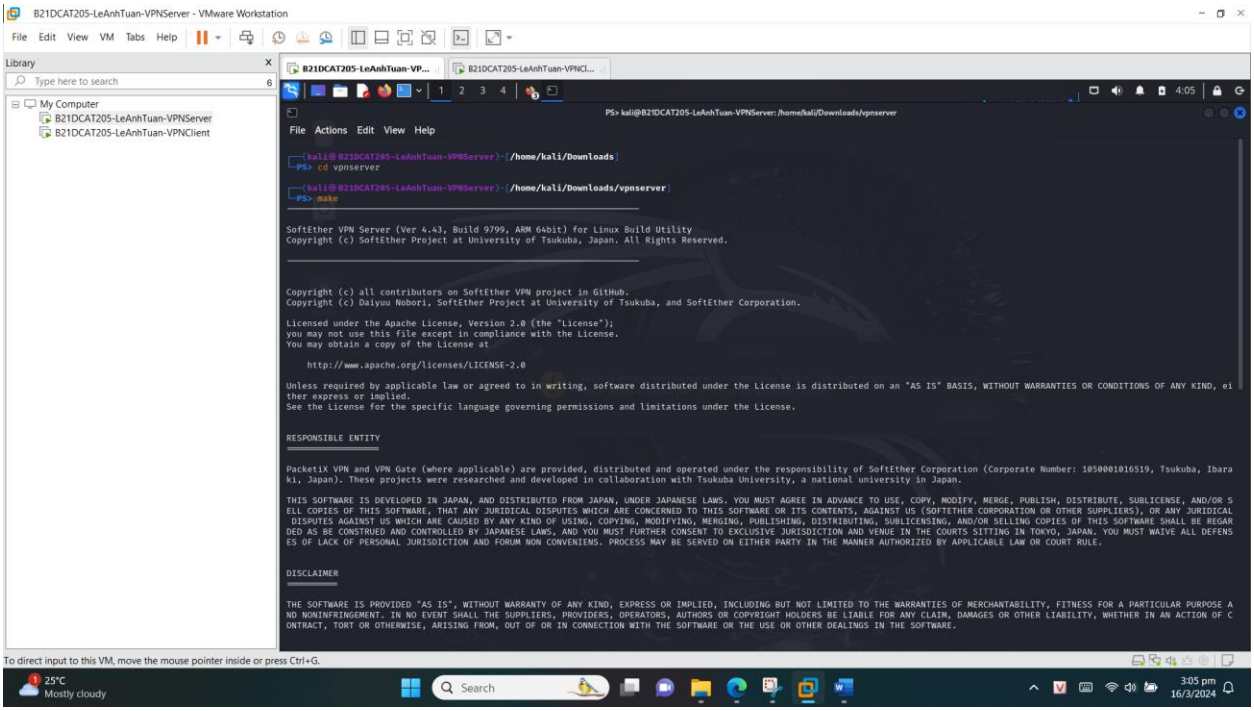
Hình 5: Chọn phiên bản SoftEther VPN Server

Giải nén file cài đặt bằng lệnh **tar -vxzf <tên file>**



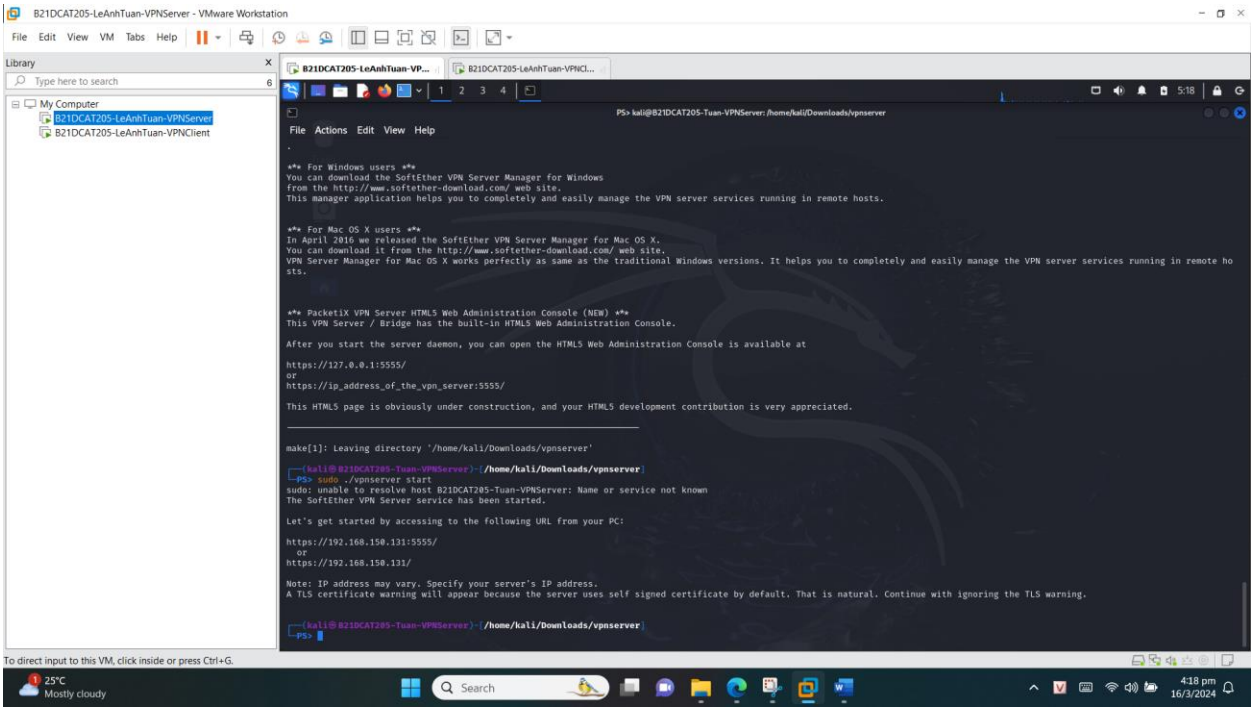
Hình 6: Giải nén file vừa tải

Chuyển vào thư mục VPN server: **cd vpnserver**
Biên dịch và cài đặt: **make** (lưu ý hệ thống phải có sẵn trình biên dịch gcc)



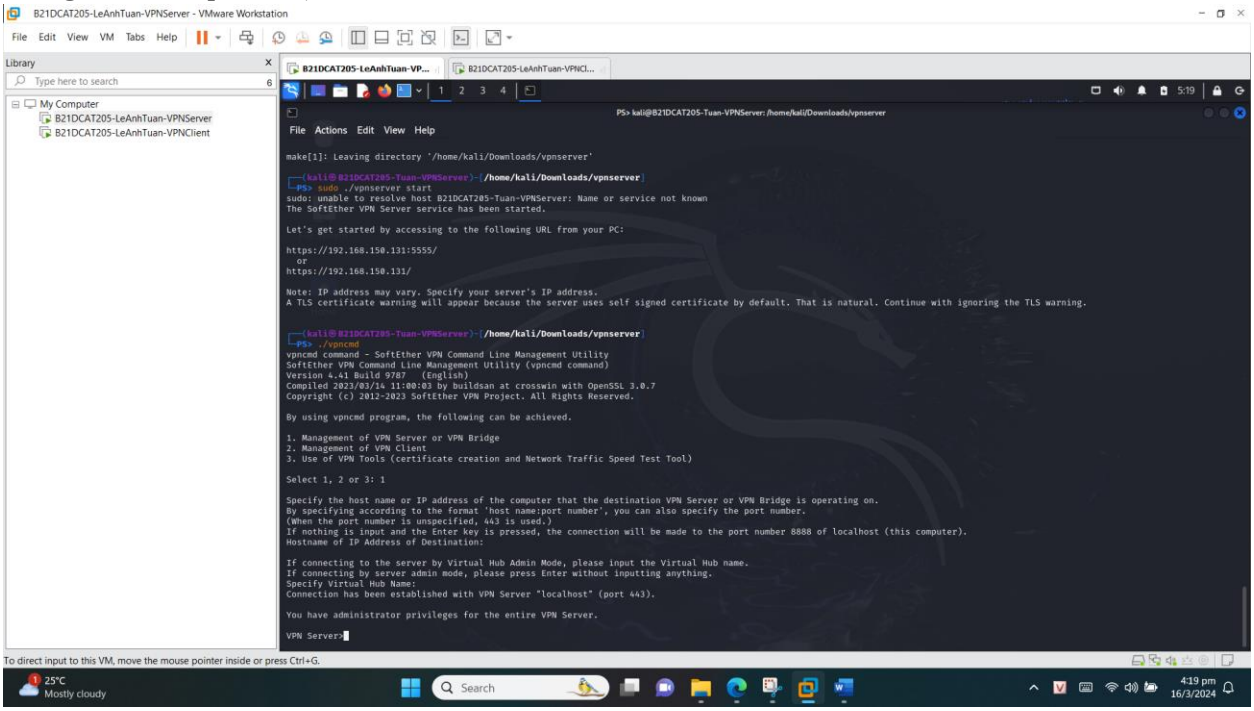
Hình 7: Biên dịch và cài đặt

Khởi động máy chủ VPN: **sudo ./vpnserver start**



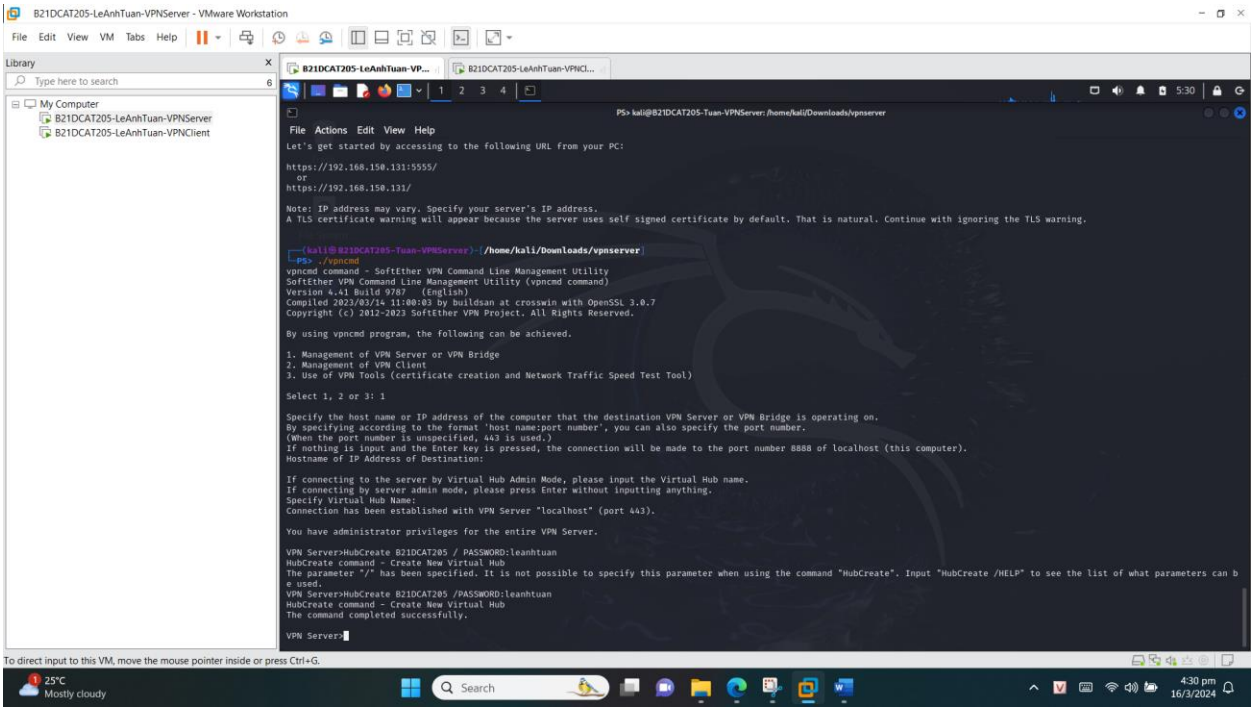
Hình 8: Khởi động máy chủ thành công

Chạy tiện ích quản trị VPN Server: **./vpncmd** (chọn chức năng số 1 và gõ Enter 2 lần để vào giao diện quản trị).



Hình 9: Giao diện quản trị cmd của VPN

Tạo 1 Virtual Hub mới: **HubCreate** (là tên Virtual Hub - dùng mã sinh viên làm tên Virtual Hub)

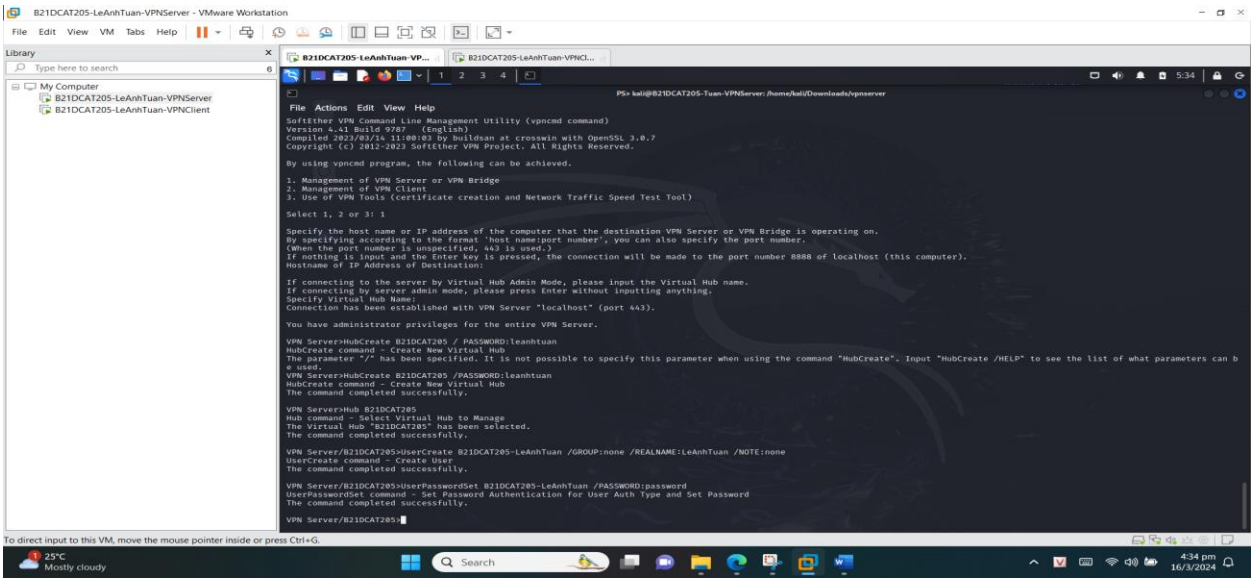


Hình 10: Tạo Virtual Hub B21DCAT205

Chọn Virtual Hub đã tạo: **Hub <tên Virtual Hub>**

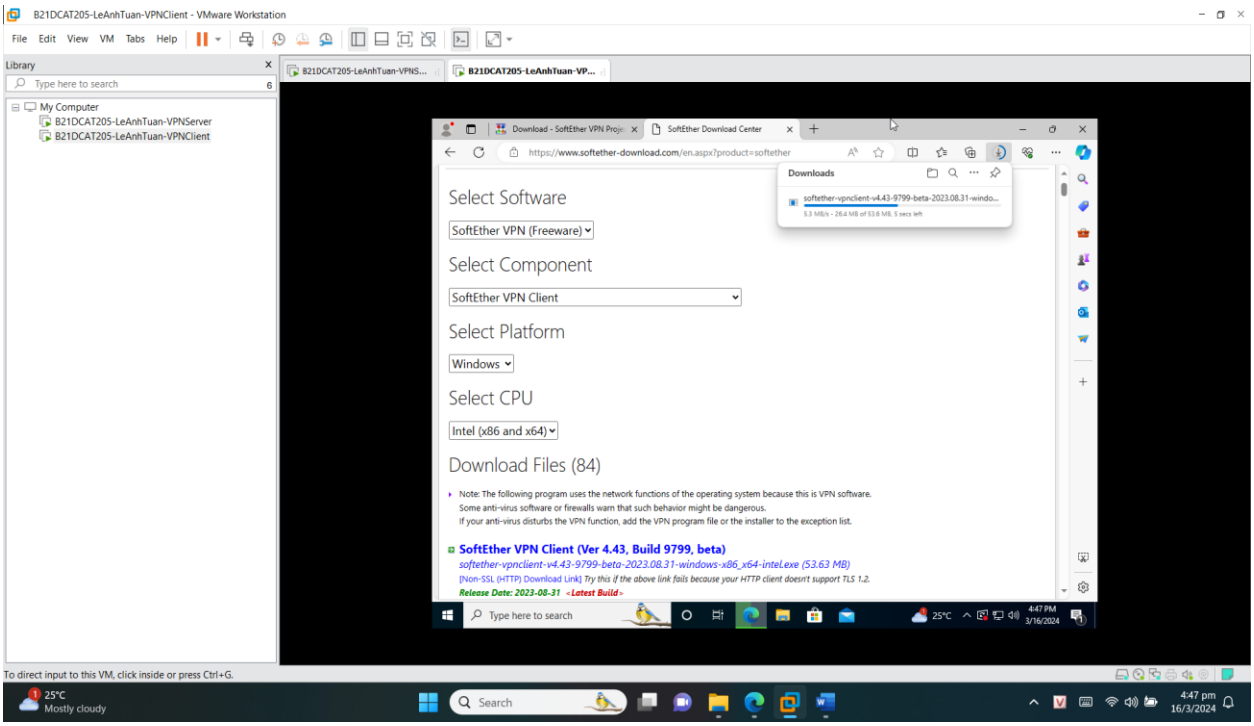
Tạo 1 người dùng VPN mới: **UserCreate <mã sv-tên> /GROUP:none /REALNAME:Tên sinh viên /NOTE:none**

Đặt mật khẩu cho người dùng: **UserPasswordSet <mã sv-tên> </PASSWORD:password>**

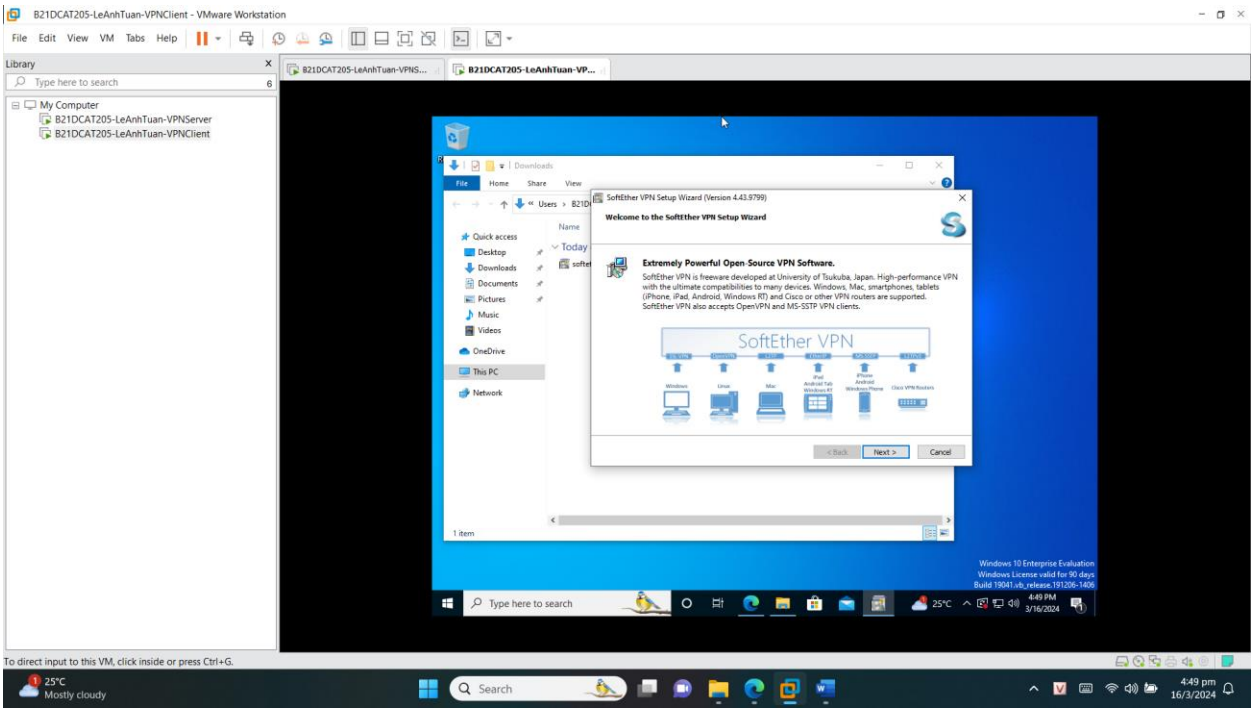


Hình 11: Tạo người dùng VPN B21DCAT205-LeAnhTuan

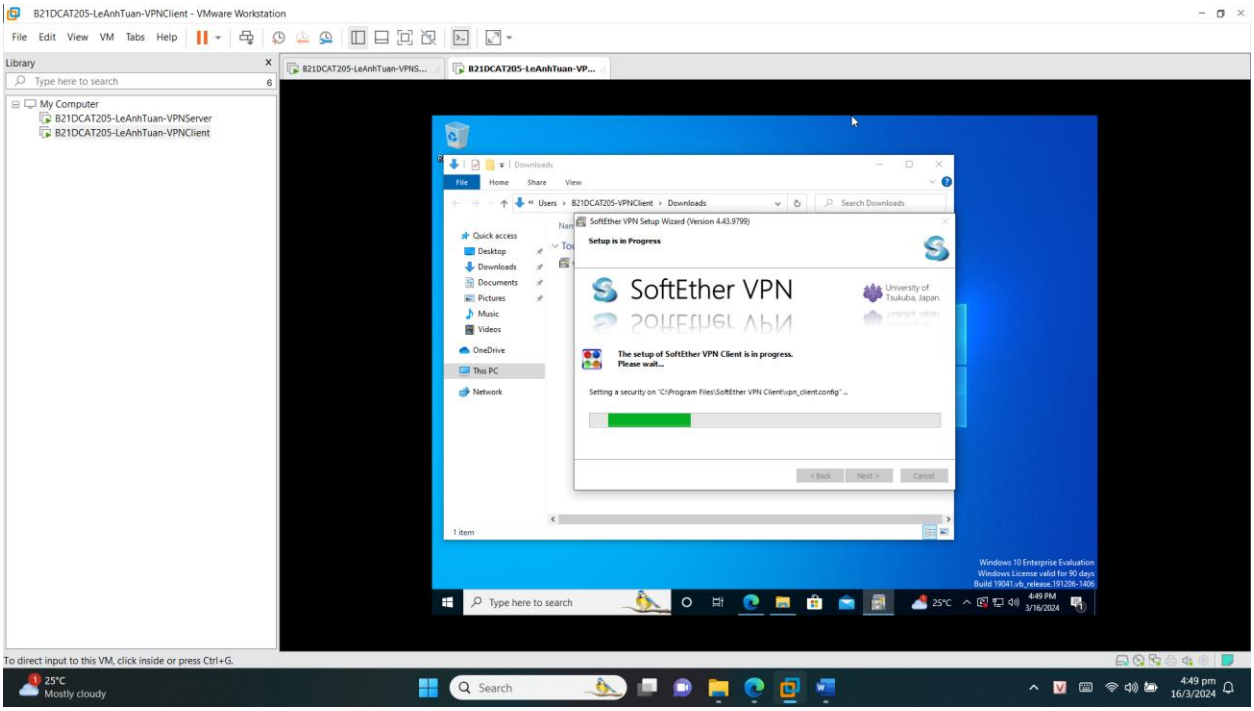
Bước 3: Tải **SoftEther VPN client** cho Windows tại **https://www.softether.org/5-download**.Cài đặt VPN client.



Hình 12: Tải file cài đặt SoftEther VPN Client



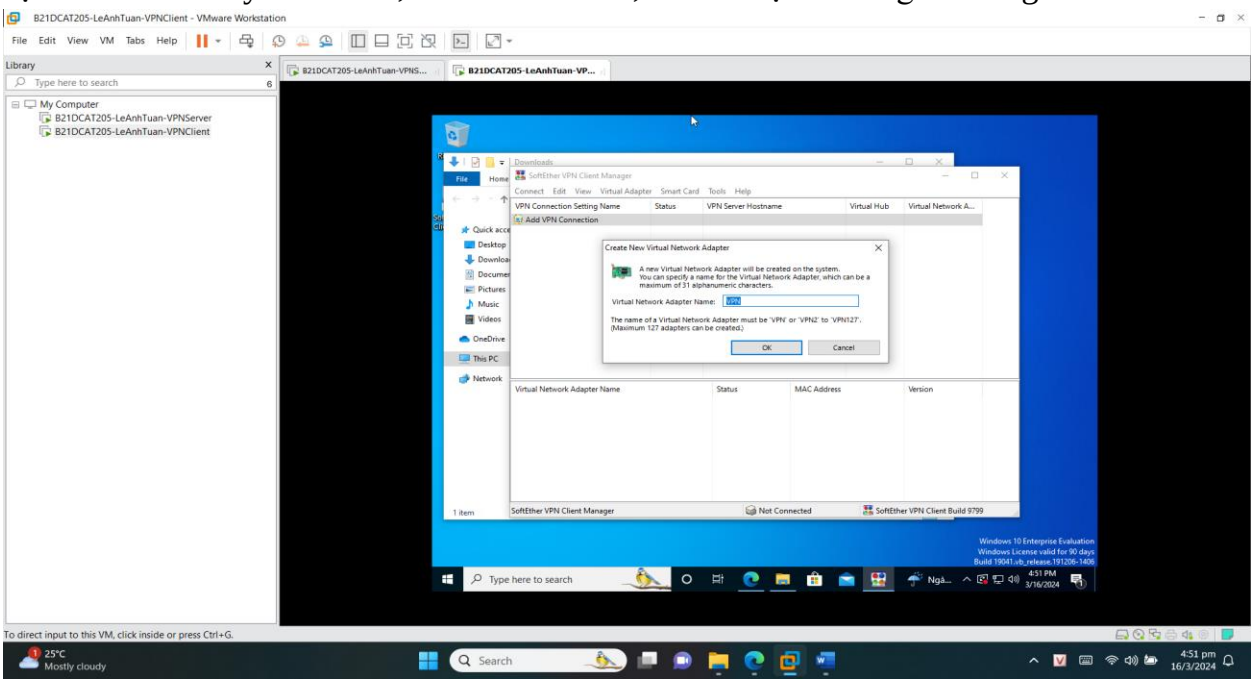
Hình 13: Tiến hành cài đặt chọn Next



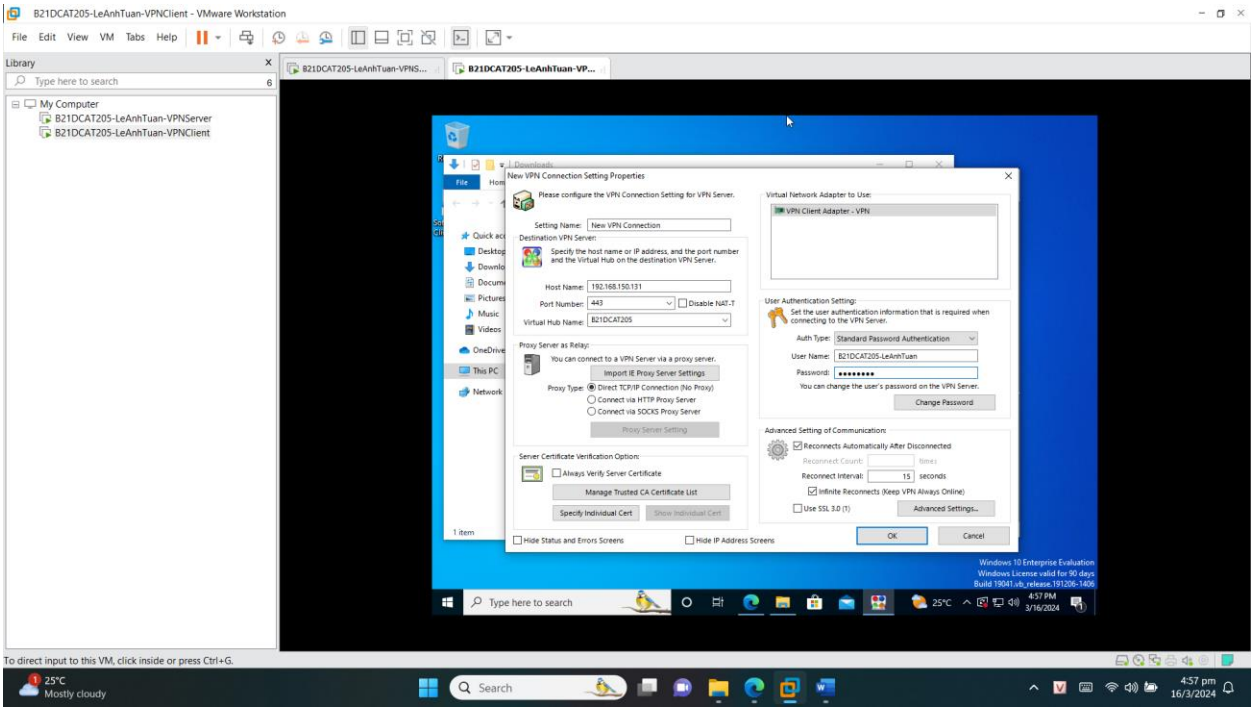
Hình 14: Tiến hành cài đặt

Bước 4: Tạo và kiểm tra kết nối VPN

Từ giao diện SoftEther VPN Client Manager, tạo 1 kết nối mới (Add New Connection) với địa chỉ IP của máy chủ VPN, tên Virtual Hub, tên và mật khẩu người dùng.

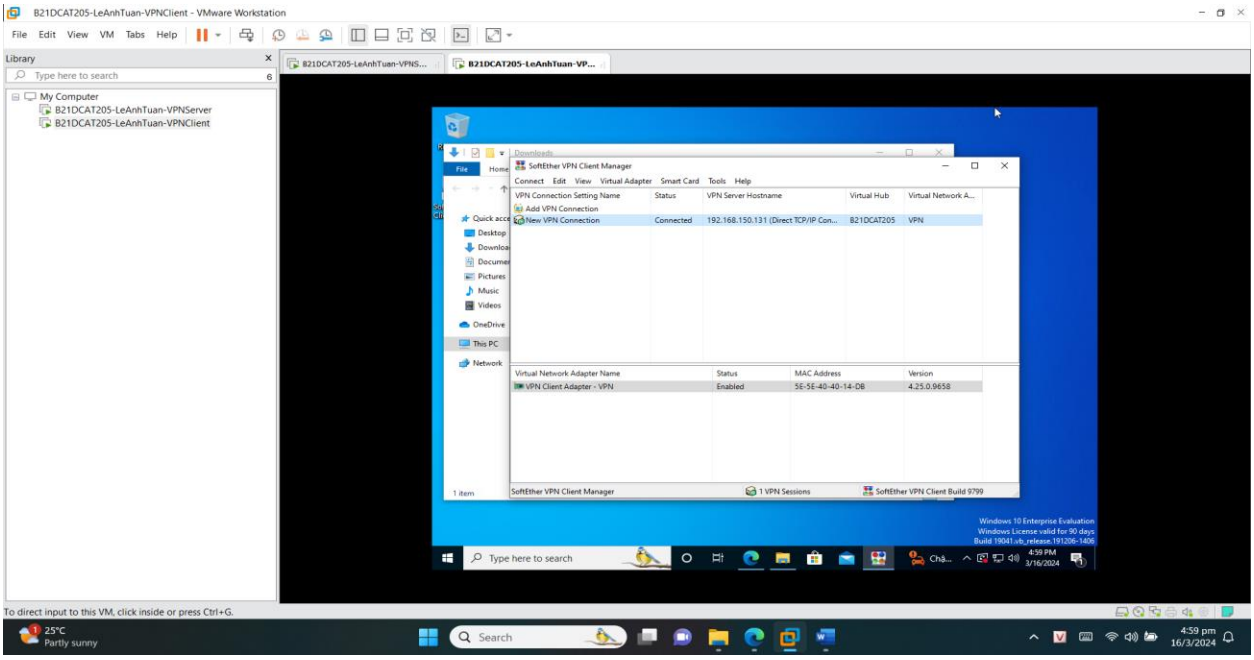


Hình 15: Giao diện SoftEther VPN Client (Tạo mới Virtual Network Adapter)



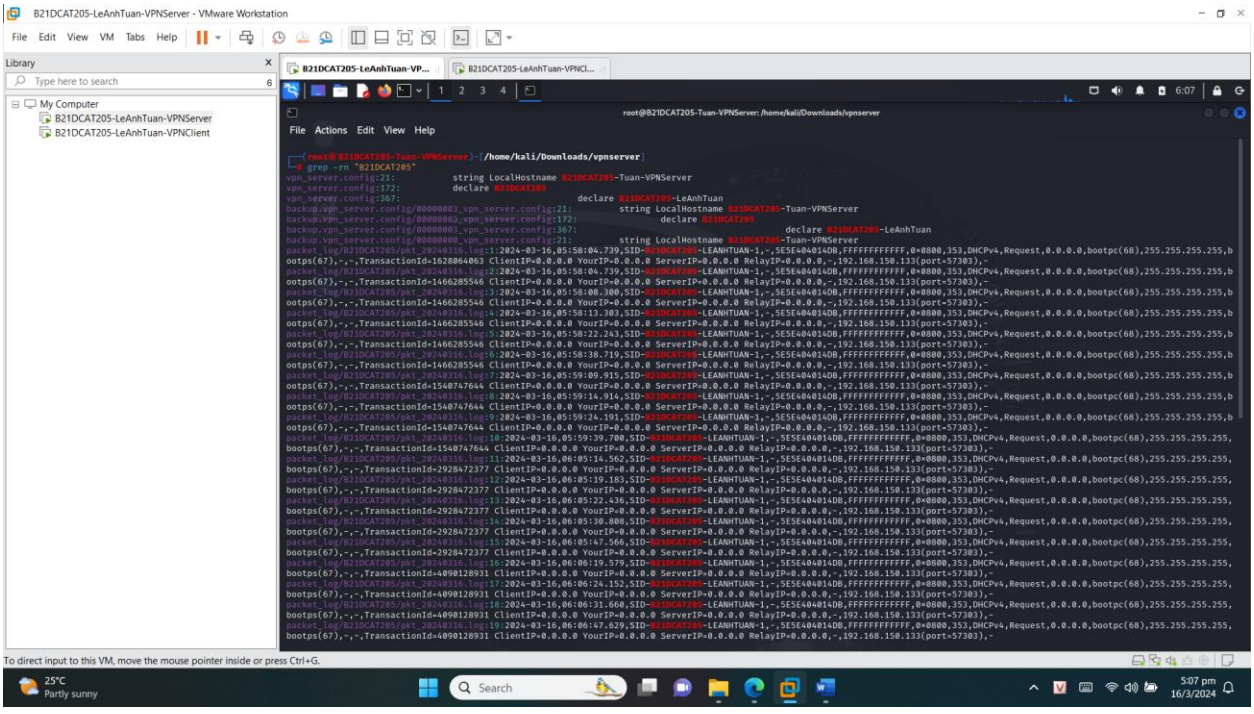
Hình 16: Cấu hình SoftEther VPN Client

Thử kết nối: Nếu thành công sẽ báo **connected**

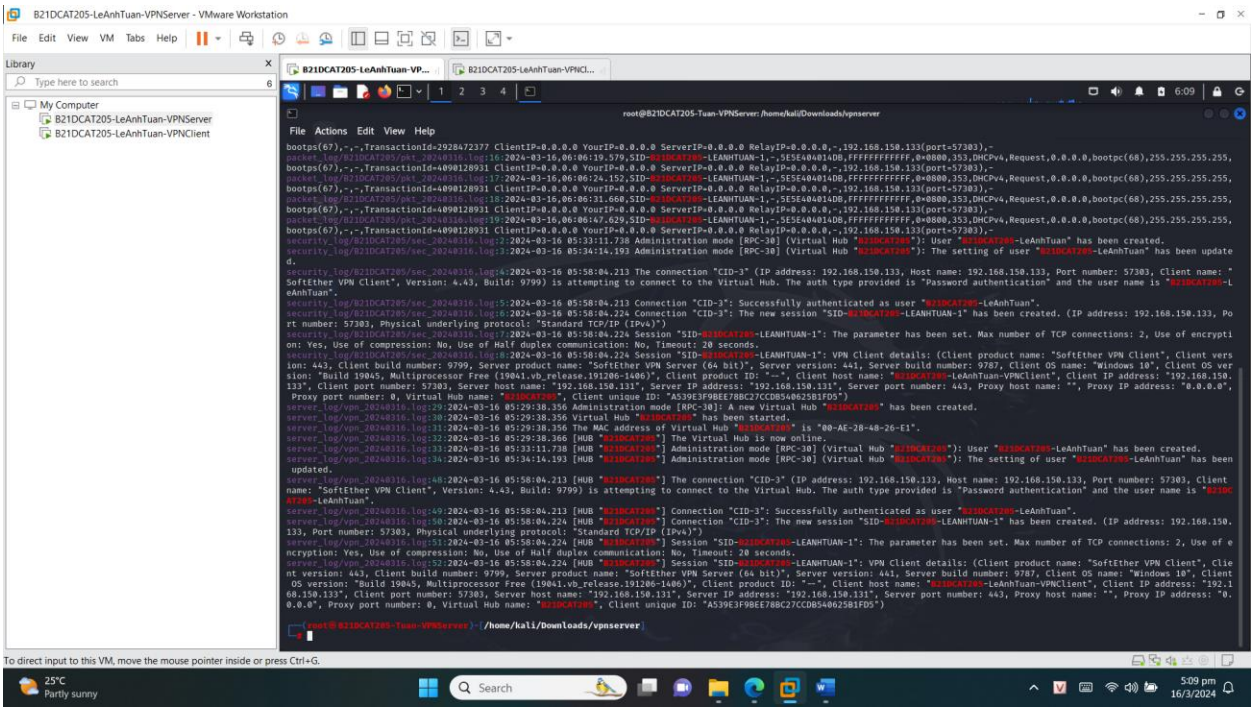


Hình 17: Kết nối thành công

Kiểm tra kết nối bên máy chủ: Chuyển sang máy chủ VPN, mở 1 terminal mới chuyển đến thư mục **vpnserver/server_log** để kiểm tra log trên VPN server:



Hình 18: Kết nối thành công (ảnh 1)



Hình 19: Kết nối thành công (ảnh 2)

3 Kết luận

- Cài đặt thành công VPN server và VPN client
- Tạo Virtual Hub, tài khoản người dùng VPN trên máy chủ VPN
- Tạo kết nối và kết nối thành công đến máy chủ (có ảnh chụp màn hình minh chứng bên máy khách và log bên máy chủ).

4 Tài liệu tham khảo

- https://vncoder.vn/tin-tuc/cong-nghe/tong-quan-ve-vpn
- https://br.atsit.in/vi/?p=54681
- https://www.hocviendaotao.com/2013/03/giao-thuc-ipsec.html
- https://datatracker.ietf.org/doc/html/rfc8446
- https://www.softether.org/4-docs