HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: THỰC TẬP CƠ SỞ
MÃ HỌC PHẦN: INT13147

BÀI THỰC HÀNH 2.3
TÌM HIỂU VÀ CÀI ĐẶT, CẤU HÌNH MÁY CHỦ VPN

Sinh viên thực hiện: B22DCAT176 Nguyễn Thị Thùy Linh

Giảng viên hướng dẫn: PGS.TS Hoàng Xuân Dậu

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

DANH MỤC HÌNH ẢNH

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Thuật ngữ tiếng Anh/Giải thích	Thuật ngữ tiếng Việt/Giải thích
SIEM	Security Information and Event Management	Giải pháp giám sát, phát hiện và phản ứng nhanh với mối đe dọa.
DNS	Domain Name System	Giao thức tên miền
DHCP	Dynamic Host Configuration Protocol	Giao thức cấp phát địa chỉ IP tự động
IIS	Internet Information Services	Dịch cụ Web Server chính của Microsoft
WAS	Windows Process Activation Service	Dịch vụ hỗ trợ cho IIS

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

I. Mục đích

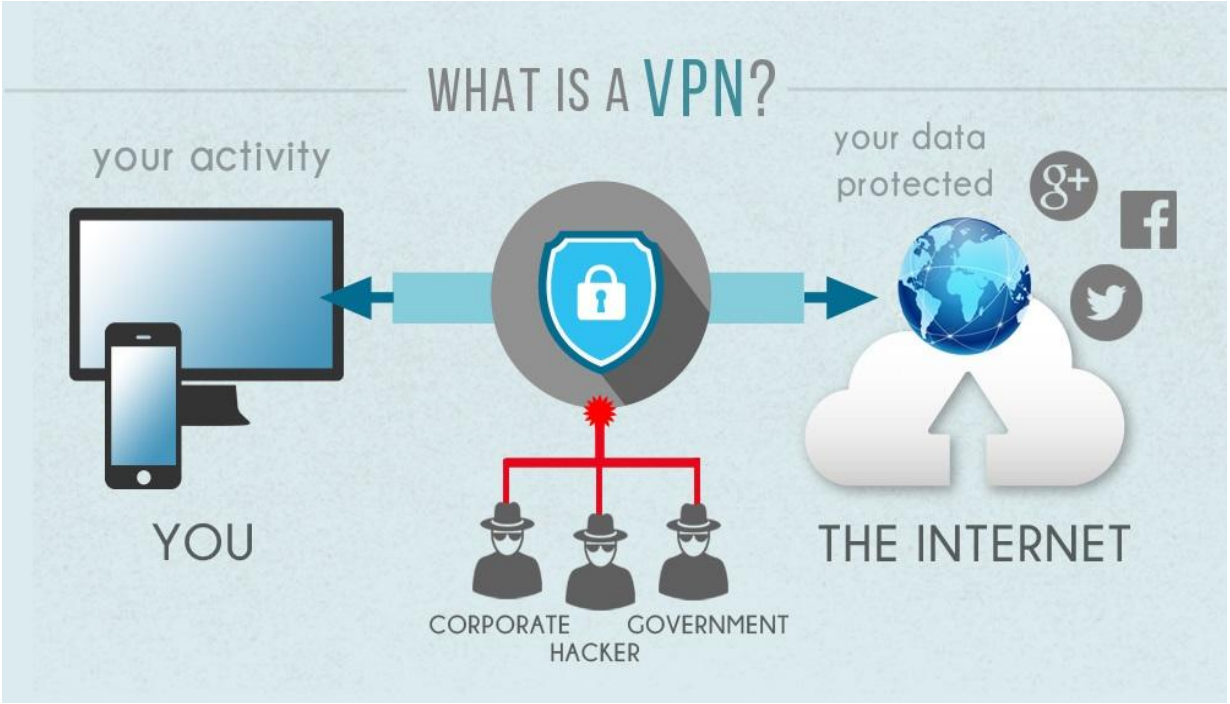
- Tìm hiểu về mạng riêng ảo (VPN – Virtual Private Network), kiến trúc và hoạt động của mạng riêng ảo.
- Luyện tập kỹ năng cài đặt, cấu hình và vận hành máy chủ mạng riêng ảo (VPN server).

II. Tìm hiểu lý thuyết

1. Tìm hiểu khái quát về VPN, các mô hình VPN và ứng dụng của VPN

VPN hay còn gọi là Virtual Private Network (mạng riêng ảo), cho phép người dùng thiết lập mạng riêng ảo với một mạng khác trên Internet.

VPN có thể được sử dụng để truy cập các trang web bị hạn chế truy cập về mặt vị trí địa lý, bảo vệ hoạt động duyệt web của bạn khỏi "sự tò mò" trên mạng Wifi công cộng bằng cách thiết lập mạng riêng ảo của bạn.



Hình ảnh 1: Hình ảnh về VPN.

VPN được ứng dụng để làm rất nhiều thứ như:

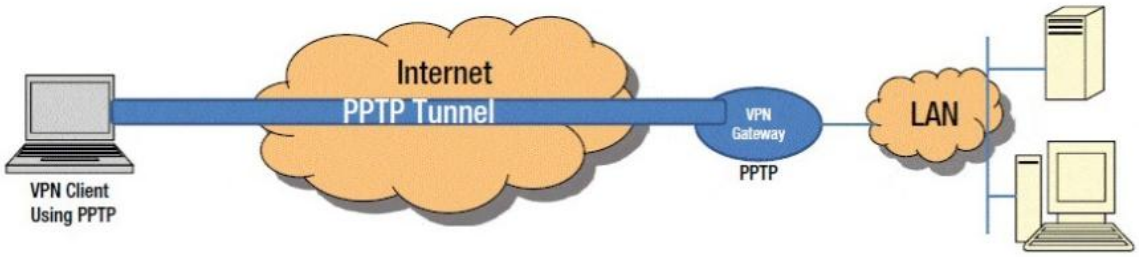
- *Truy cập vào mạng doanh nghiệp khi ở xa*: VPN thường được sử dụng bởi những người kinh doanh để truy cập vào mạng lưới kinh doanh của họ, bao gồm tất cả tài nguyên trên mạng cục bộ, trong khi đang đi trên đường, đi du lịch.. Các nguồn lực trong mạng nội bộ không cần phải tiếp xúc trực tiếp với Internet, nhờ đó làm tăng tính bảo mật.
- *Truy cập mạng gia đình dù không ở nhà*: Bạn có thể thiết lập VPN riêng để truy cập khi không ở nhà. Thao tác này sẽ cho phép truy cập Windows từ xa thông qua Internet, sử dụng tập tin được chia sẻ trong mạng nội bộ, chơi games trên máy tính qua Internet giống như đang ở trong cùng mạng LAN.
- *Duyệt web ẩn danh*: Nếu đang sử dụng Wifi công cộng, duyệt web trên những trang web không phải là HTTPS, thì tính an toàn của dữ liệu trao đổi trong mạng sẽ dễ bị lộ. Nếu muốn ẩn hoạt động duyệt web của mình để dữ liệu được bảo mật hơn thì ta kết nối VPN. Mọi thông tin truyền qua mạng lúc này sẽ được mã hóa.

- *Truy cập đến những website bị chặn* giới hạn địa lý, bỏ qua kiểm duyệt Internet, vượt tường lửa,…
- *Tải tập tin*: Tải BitTorrent trên VPN sẽ giúp tang tốc độ tải file. Điều này cũng có ích với các traffic mà ISP của bạn có thể gây trở ngại.

2. Tìm hiểu về các giao thức tạo đường hầm cho VPN: PPTP, L2TP, L2F, MPLS,..

2.1. Point-To-Point Tunneling Protocol

Point-To-Point Tunneling Protocol (PPTP) là giao thức được dùng để truyền dữ liệu qua các hầm – Tunnel giữa 2 tầng traffic trong Internet. L2TP cũng thường được dùng song song với IPSec (đóng vai trò là Security Layer đã đề cập đến ở phía trên) để đảm bảo quá trình truyền dữ liệu của L2TP qua môi trường Internet được thông suốt.



Hình ảnh 2: Sơ đồ mô tả cách hoạt động của PPTP VPN.

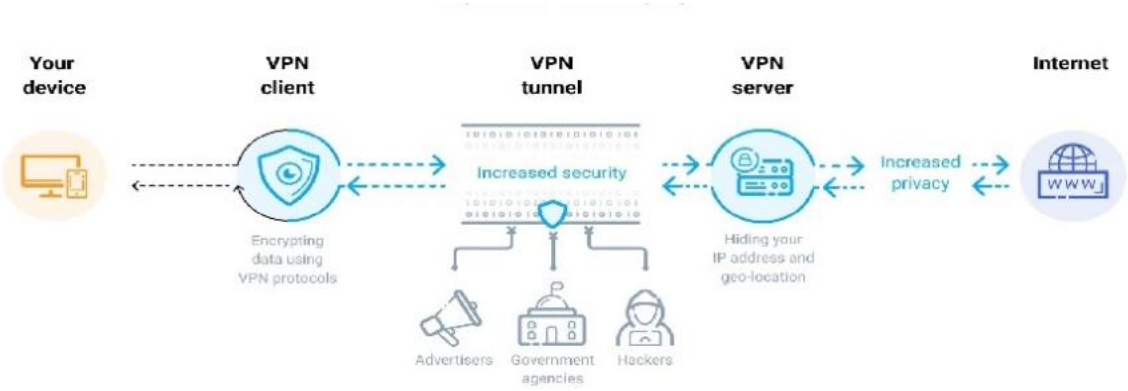
Không giống như PPTP, VPN sẽ "kế thừa" toàn bộ lớp L2TP/IPSec có các key xác thực tài khoản được chia sẻ hoặc là các Certificate.

2.2. Layer 2 Tunneling Protocol

Layer 2 Tunneling Protocol (L2TP) là 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.

**Cách hoạt động của L2TP:*

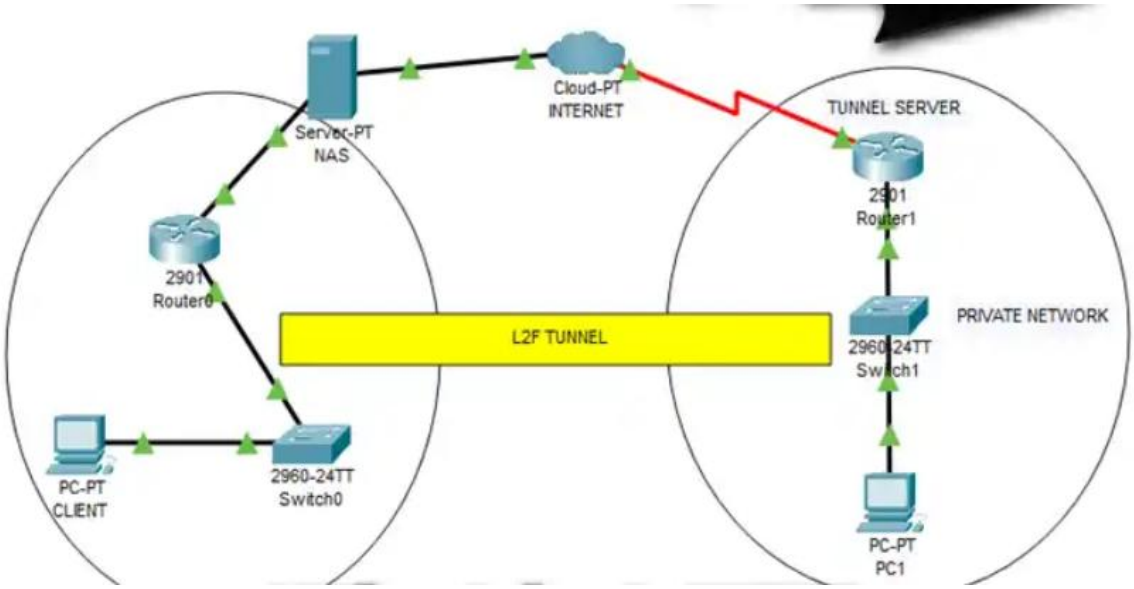
- Các gói tin L2TP bao gồm cả payload và header được gửi đi trong các gói tin UDP (*User Datagram Protocol*). Một ưu điểm của việc truyền qua UDP (chứ không phải TCP) là nó tránh được các vấn đề *TCP meltdown* – khi hai giao thức truyền dẫn có điều khiển chồng lên nhau và xung đột khi cố sửa chữa vấn đề mất gói tin.
- Hai điểm cuối của đường hầm L2TP được gọi là bộ tập trung truy cập L2TP (*LAC – L2TP Access Concentrator*) và máy chủ mạng L2TP (*LNS – L2TP Network Server*). Lưu lượng mạng trong đường hầm là hai chiều, chia thành nhiều session sử dụng các giao thức cấp cao hơn như PPP. Cả LAC và LNS đều có thể khởi động một session, lưu lượng của mỗi session được cách ly bởi L2TP, vì vậy có thể thiết lập nhiều máy ảo trên một đường hầm.



Hình ảnh 3: Sơ đồ cách hoạt động của L2TP.

2.3. Layer 2 Forwarding Protocol

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 tiện 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.

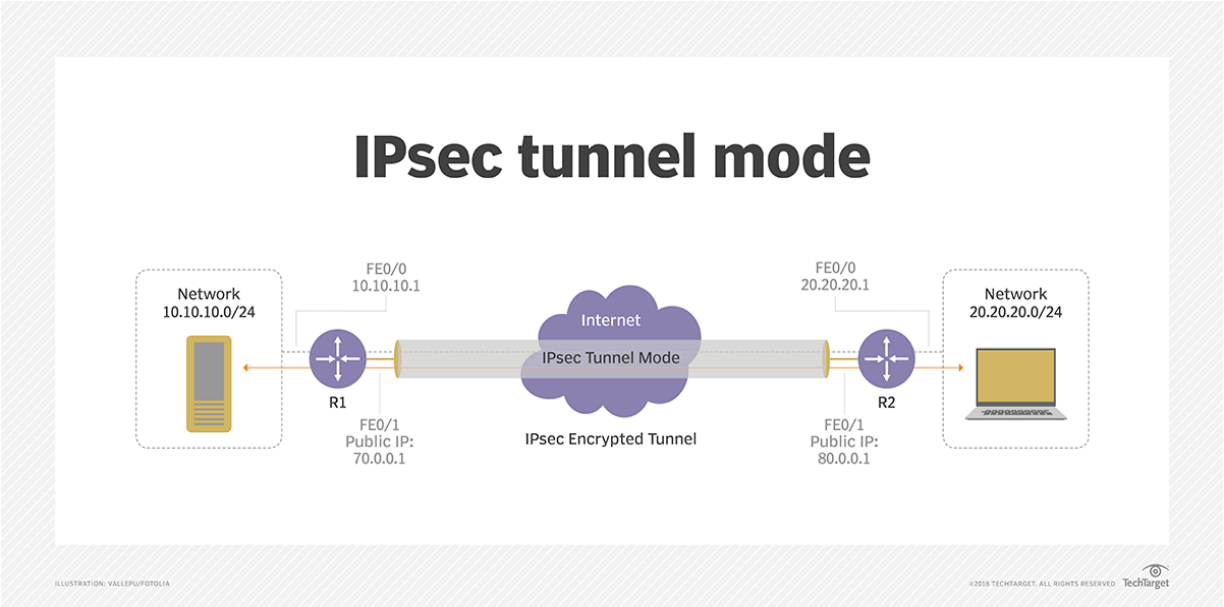


Hình ảnh 4: Sơ đồ cách hoạt đông của L2F.

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

3.1 IPSec:

IP Security (IP Sec) 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.



Hình ảnh 5: Sơ đồ cách thức hoạt động của IPSec.

Sự khác biệt giữa các mode này là:

- *Transport mode* chỉ có nhiệm vụ mã hóa dữ liệu bên trong các gói (*data package* – hoặc còn biết dưới từ *payload*). Trong khi các *Tunnel* mã hóa toàn bộ các data package đó.
- Di vậy, IPSec thường được coi là *Security Overlay*, bởi vì IPSec dùng các lớp bảo mật so với các Protocol khác.

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

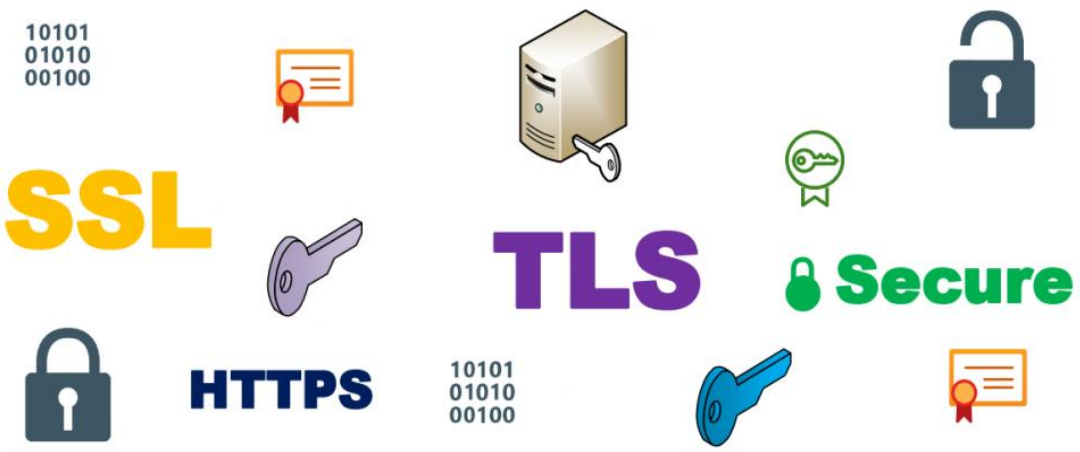
Secure Sockets Layer (SSL) là một loại bảo mật giúp mã hóa liên lạc giữa website và trình duyệt. Công nghệ này đang lỗi thời và được thay thế hoàn toàn bởi TLS. ***Transport Layer Security (TLS)*** cũng là một loại bảo mật thông tin truyền giống như SSL.

Website được cài đặt chứng chỉ *SSL/TLS* có thể dùng giao thức HTTPS để thiết lập kênh kết nối an toàn với server.

Mục tiêu của *SSL/TLS* là bảo mật các thông tin nhạy cảm trong quá trình truyền trên Internet như thông tin cá nhân, thông tin thanh toán, thông tin đăng nhập. Nó là giải pháp thay thế cho phương pháp truyền thông tin văn bản dạng plaintext, văn bản loại này khi truyền trên Internet sẽ không được mã hóa, nên việc áp dụng mã hóa vào sẽ khiến cho các bên thứ 3 không xâm nhập được vào thông tin của bạn, không đánh cắp hay chỉnh sửa được các thông tin đó.

Chứng chỉ *SSL/TLS* hoạt động bằng cách tích hợp key mã hóa vào thông tin định danh công ty. Nó sẽ giúp công ty mã hóa mọi thông tin được truyền vào mã không bị ảnh hưởng hoặc bị chỉnh sửa bởi bên thứ 3.

SSL/TLS hoạt động bằng cách sử dụng public và private key, đồng thời các khóa duy nhất của mỗi phiên giao dịch. Mỗi khi khách truy cập điền vào thanh địa chỉ SSL thông qua web browser hoặc chuyển hướng tới trang web được bảo mật, trình duyệt và web server đã thiết lập kết nối.



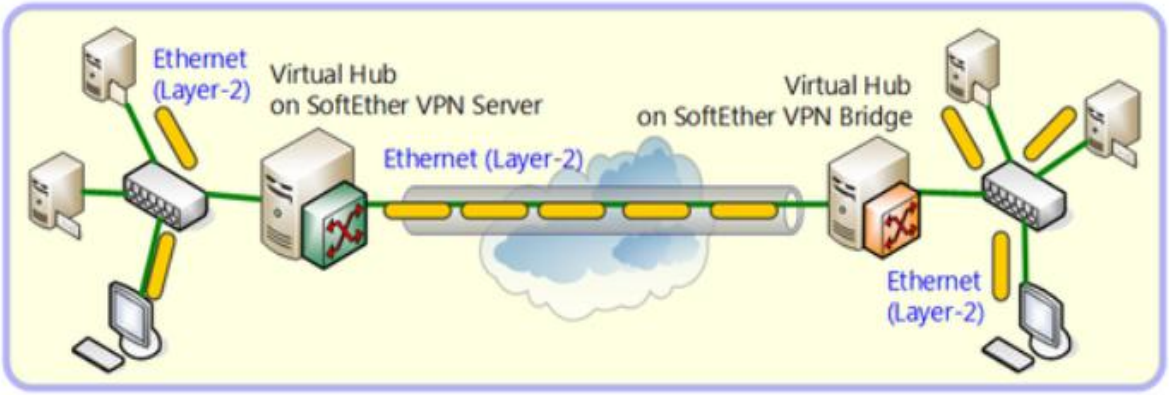
Hình ảnh 6: Sơ đồ cách thức hoạt động của SSL và TLS.

3.3 Tìm hiểu về SoftEther VPN

SoftEther VPN là một trong những đa giao thức mạnh mẽ và dễ sử dụng nhất trên thế giới. Dự án SoftEther VPN khởi đầu là một dự án học thuật tại Đại học Tsukuba và là một Phần mềm VPN đa giao thức đa nền tảng mã nguồn mở miễn phí. Hiện tại, nó có thể 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, một 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 như PPTP, L2TP, OpenVPN và SSTP, trong khi loại bỏ nhược điểm của chúng.

Tất cả các tính năng mà SoftEther cung cấp, tăng cường khả năng giúp người dùng điều hướng an toàn và vượt qua mọi tường lửa do các bên chính quyền áp đặt, giúp nó trở thành một giao thức VPN phổ biến.



Hình ảnh 7: SoftEther VPN khi xây dựng kết nối VPN cơ sở.

CHƯƠNG 2 : NỘI DUNG THỰC HÀNH

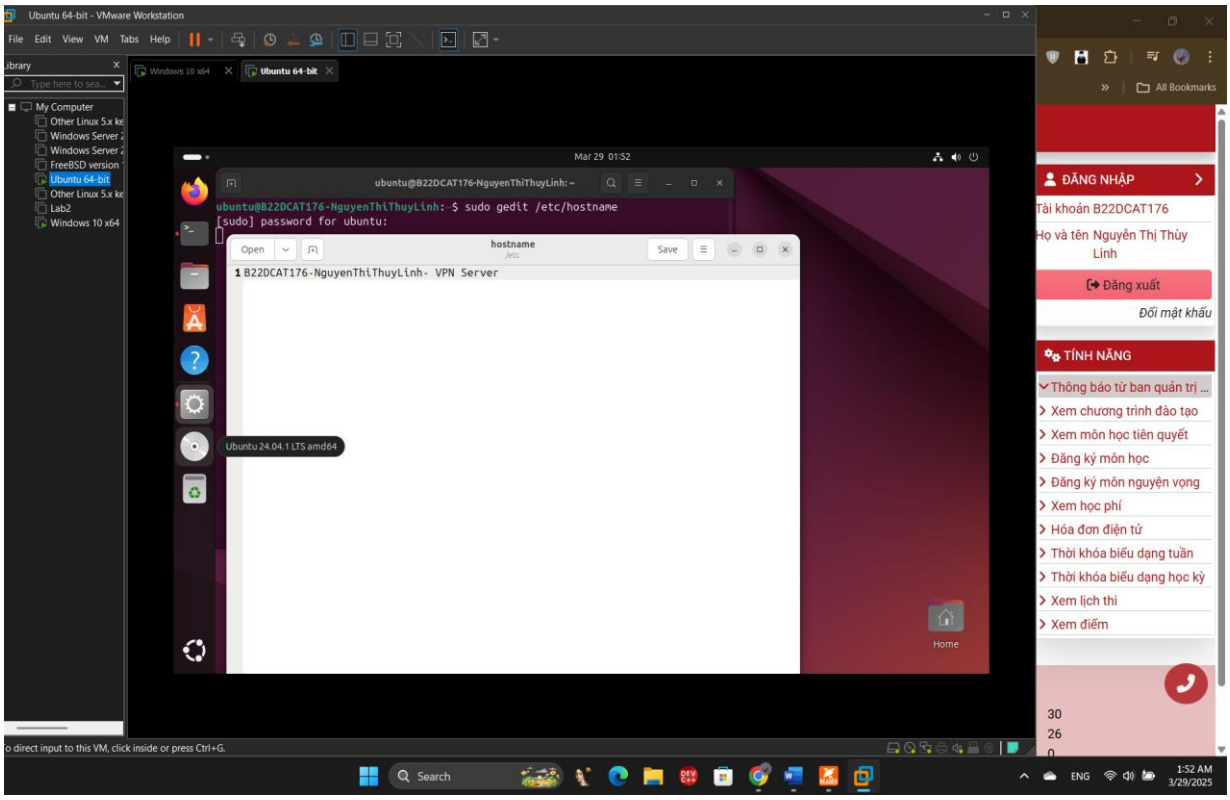
I. Chuẩn bị môi trường

- 01 máy tính (máy thật hoặc máy ảo) chạy Linux với RAM tối thiểu 2GB, 10GB đĩa cứng có kết nối mạng (LAN hoặc Internet).
- 01 máy tính (máy thật hoặc máy ảo) chạy Kali Linux (bản 2021 trở lên).
- Bộ phần mềm Snort tải tại https://www.snort.org/downloads.

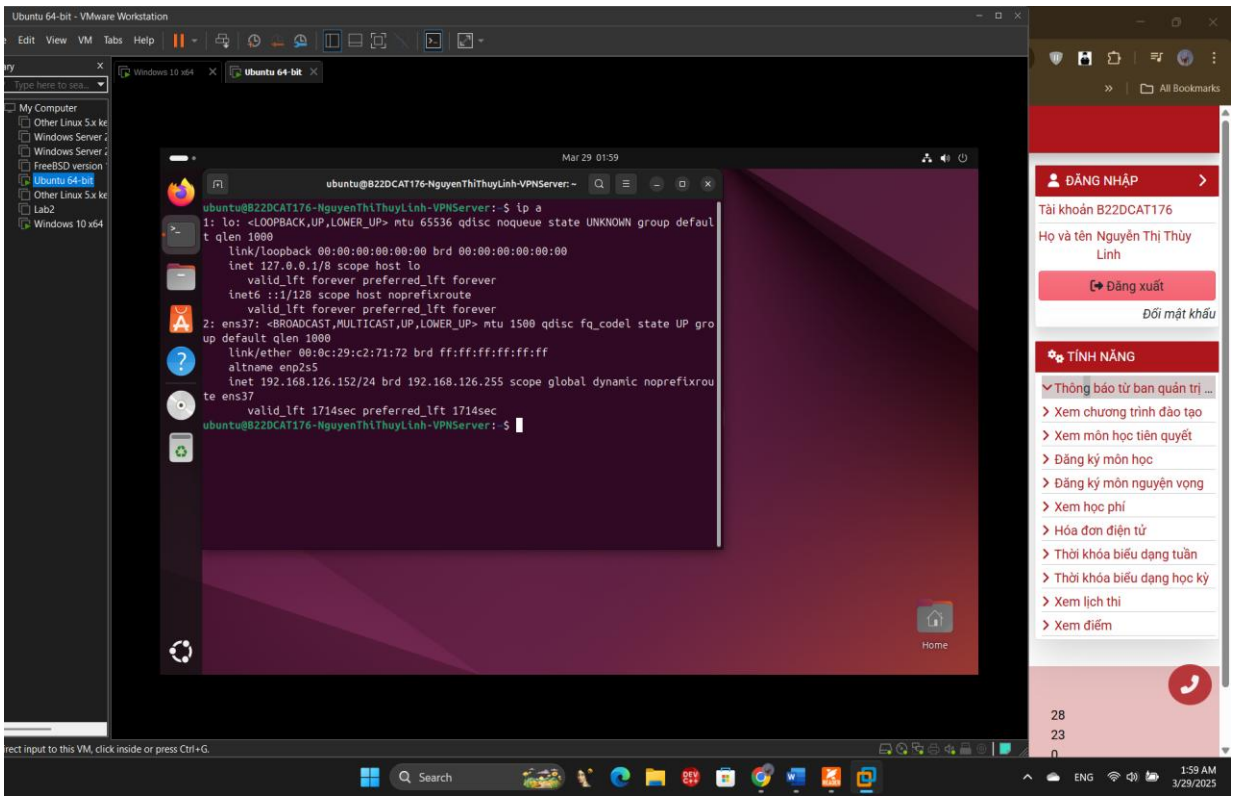
II. Các bước thực hiện

1. Chuẩn bị các máy ảo

Máy Windows được đổi tên thành <*Mã SV-Tên SV*>-VPNClient và máy cài VPN server thành <*Mã SV-Tên SV*>-VPNServer. Các máy có địa chỉ IP và kết nối mạng LAN.

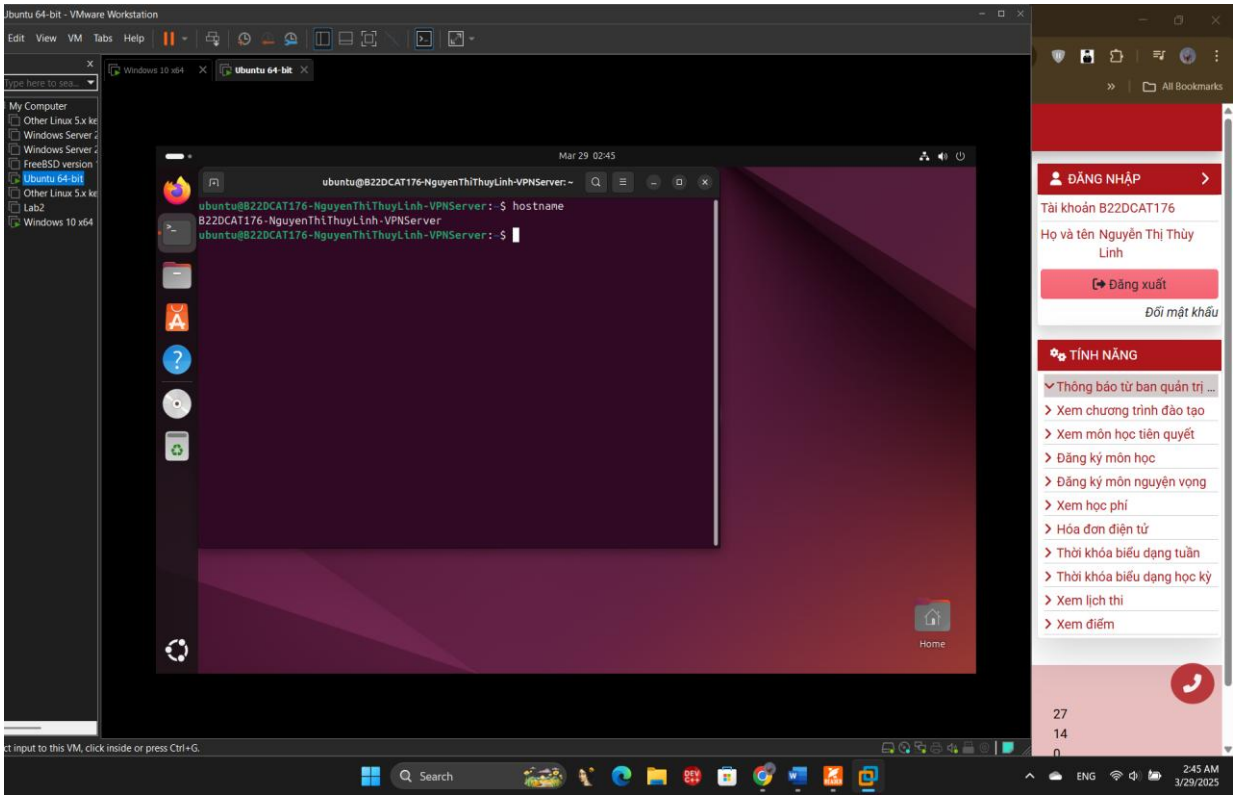


Hình ảnh 8: Đổi tên máy Ubuntu

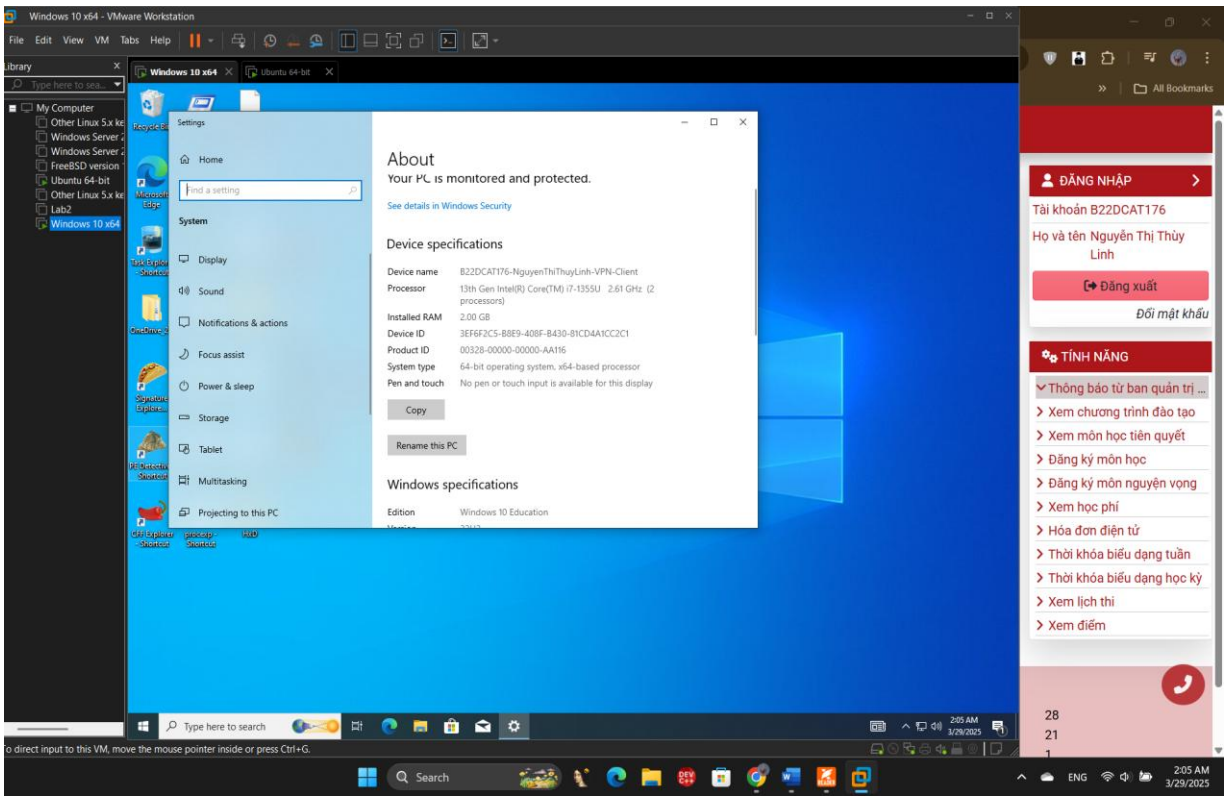


Hình ảnh 9: Địa chỉ IP của máy Ubuntu chuẩn bị.

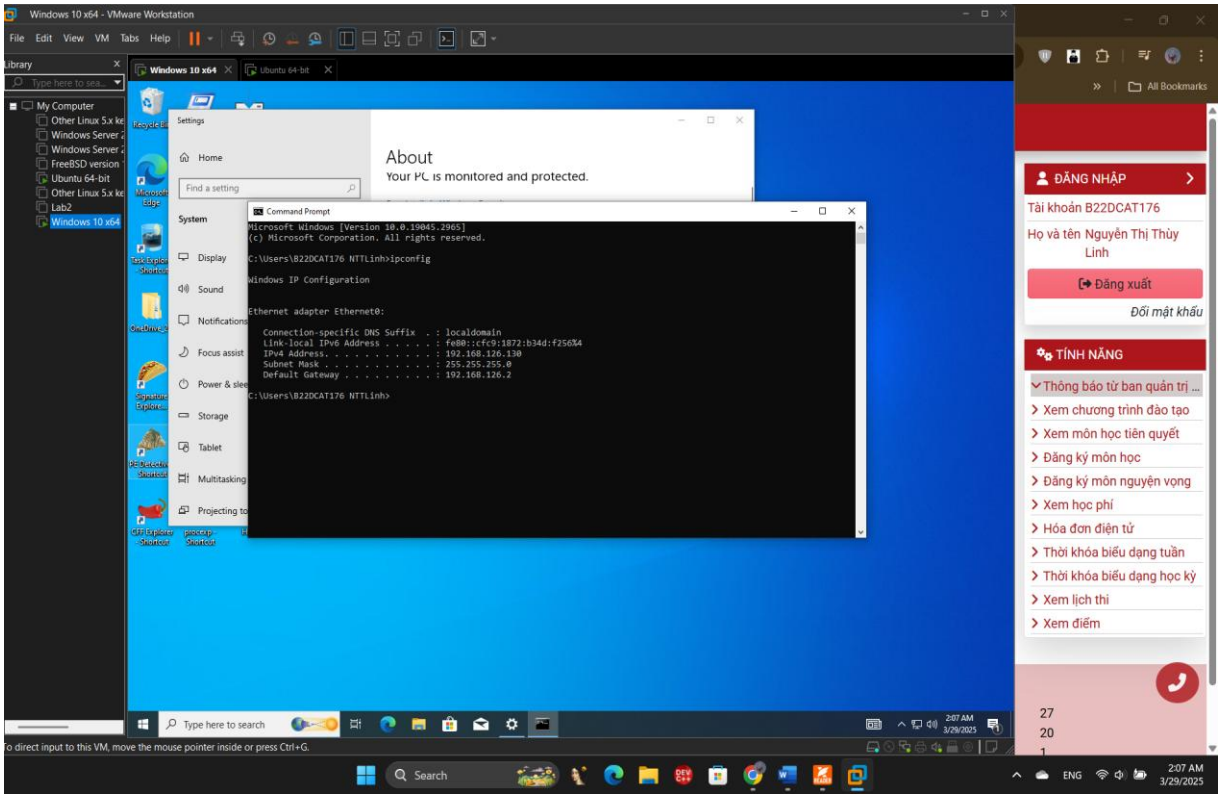
Chạy lệnh hostname để kiểm tra



Hình ảnh 10: Kiểm tra Hostname.



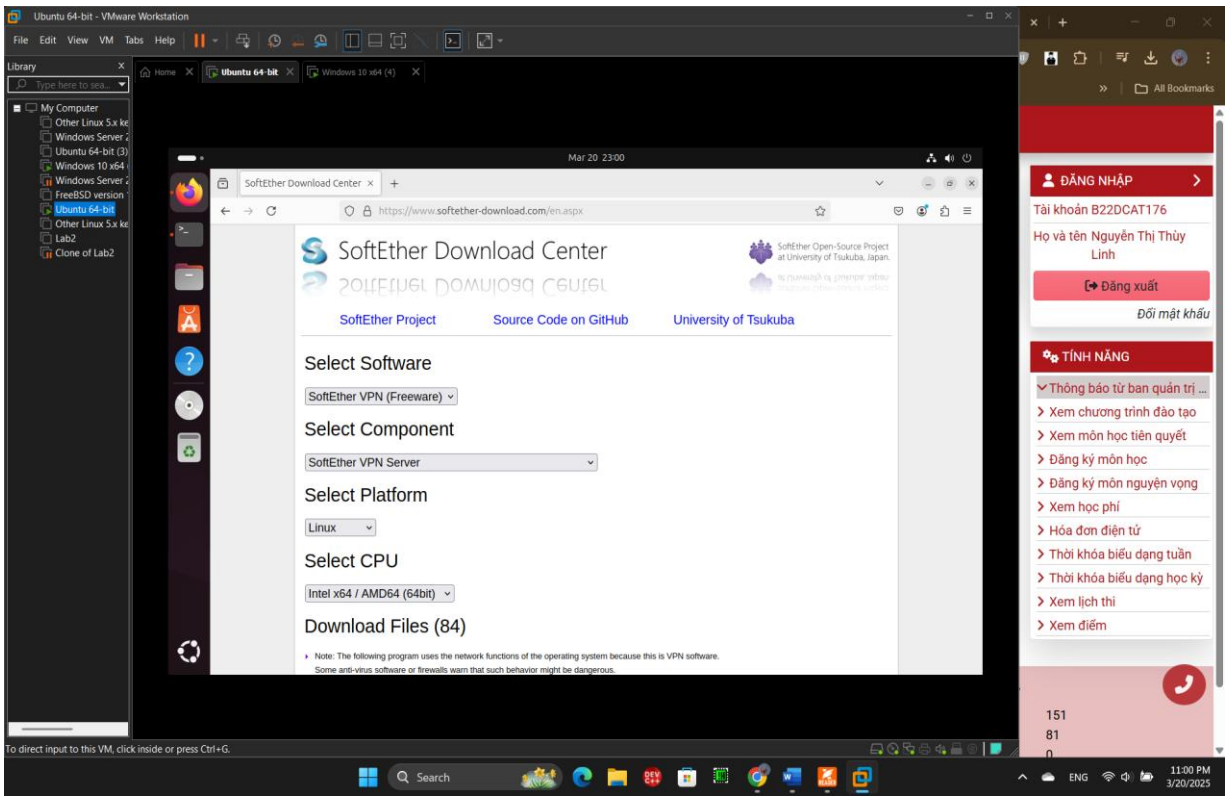
Hình ảnh 11: Đổi tên máy Windows 10.



Hình ảnh 12 : Kiểm tra IP

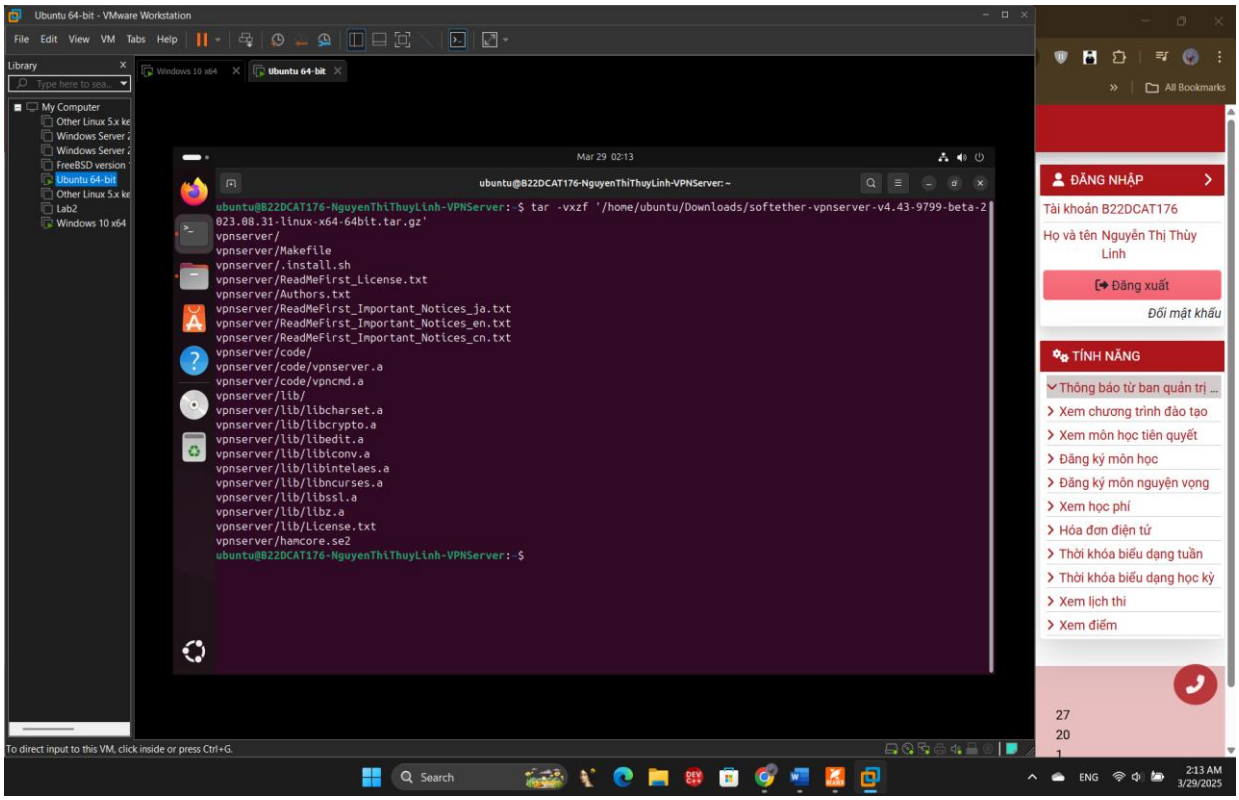
2. Tải SoftEther VPN server, cài đặt và cấu hình VPN Server

- Ta tiến hành tải SoftEther VPN Server trên máy Linux.



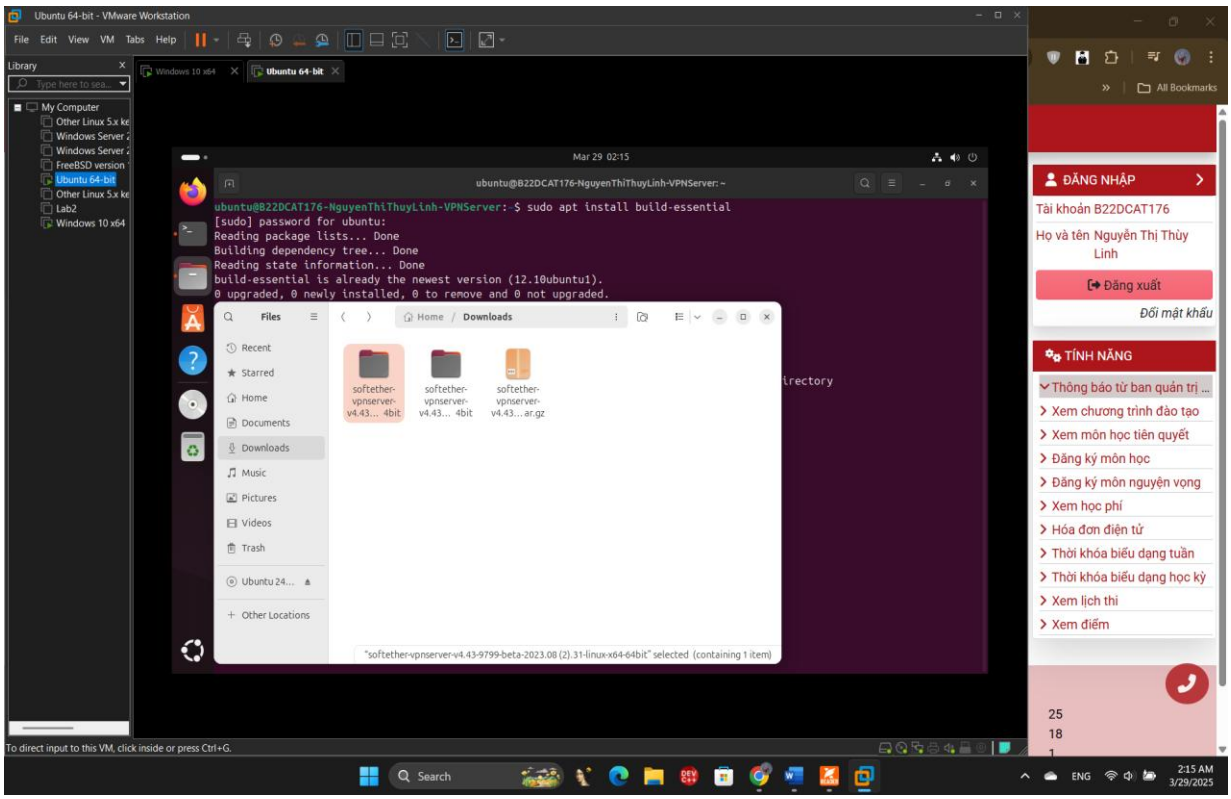
Hình ảnh 13: Tải SoftEther VPN Server.

- Giải nén file vừa tải:



Hình ảnh 14 : Giải nén file vừa tải.

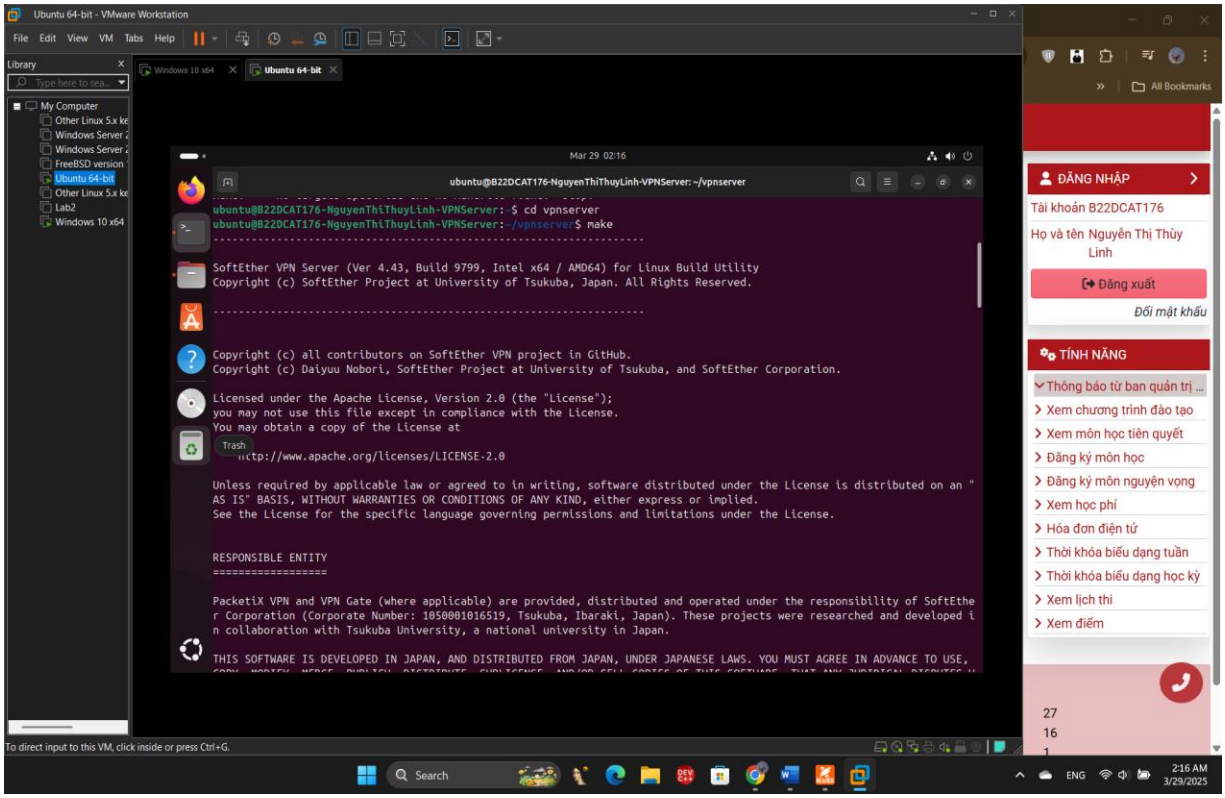
- Cài đặt trình dịch GCC.



Hình ảnh 15: Cài đặt trình dịch GCC.

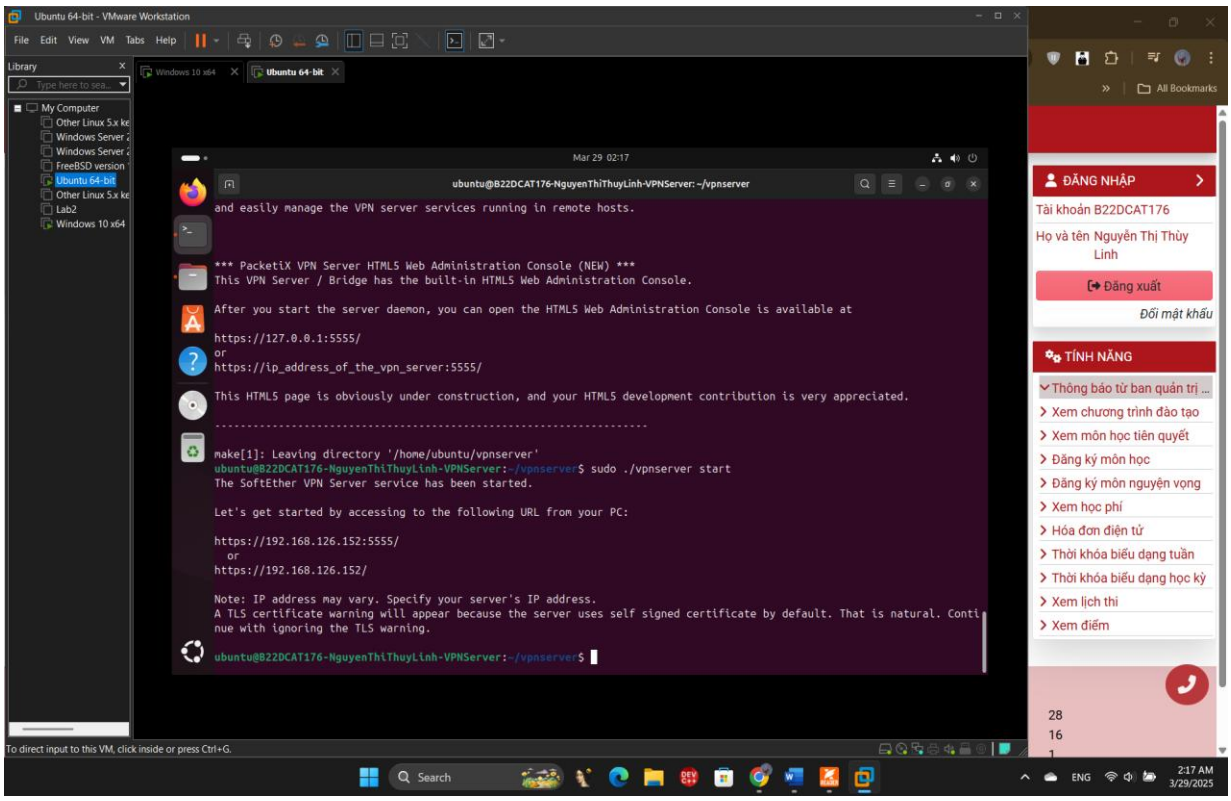
-Chuyển vào thư mục VPN server: *cd vpnserver.*

Biên dịch và cài đặt: *make* (lưu ý hệ thống phải có sẵn trình biên dịch GCC)



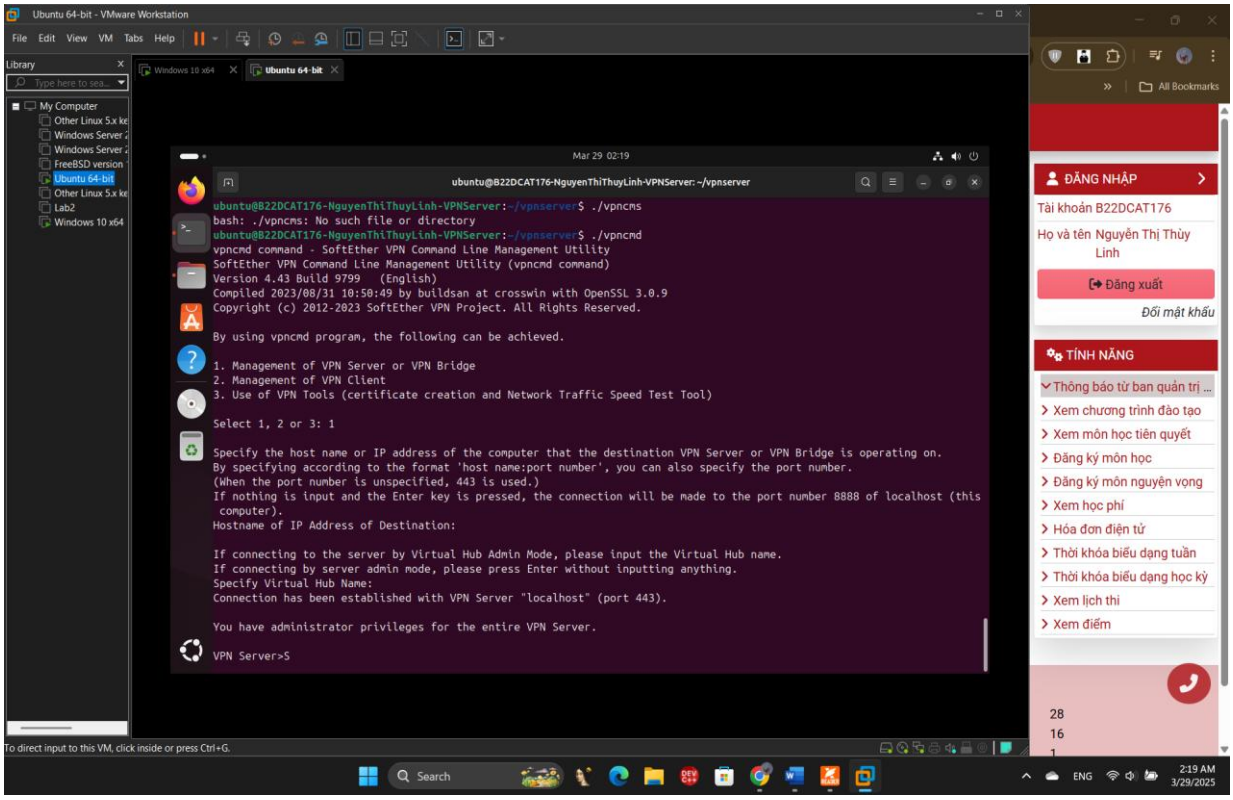
Hình ảnh 16: Chuyển vào thư mục vpnserver.

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



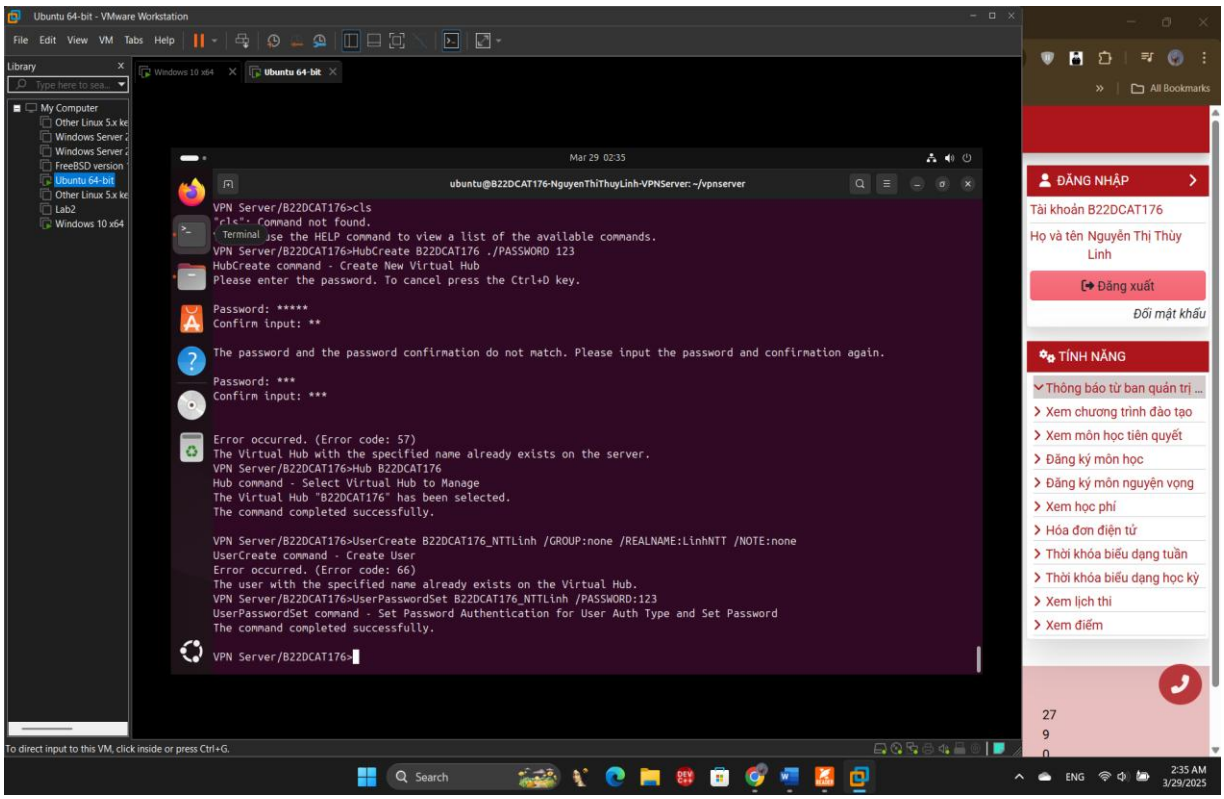
Hình ảnh 17: Khởi động máy chủ VPN Server.

-Chạy tiện ích quản trị VPN Server: *./vpncmd* (chọn chức năng số 1 và gõ *Enter* 2 lần để vào giao diện quản trị). Tạo Virtual Hub và tài khoản người dùng VPN trong giao diện quản trị.



Hình ảnh 18: Chạy tiện ích quản trị VPN Server.

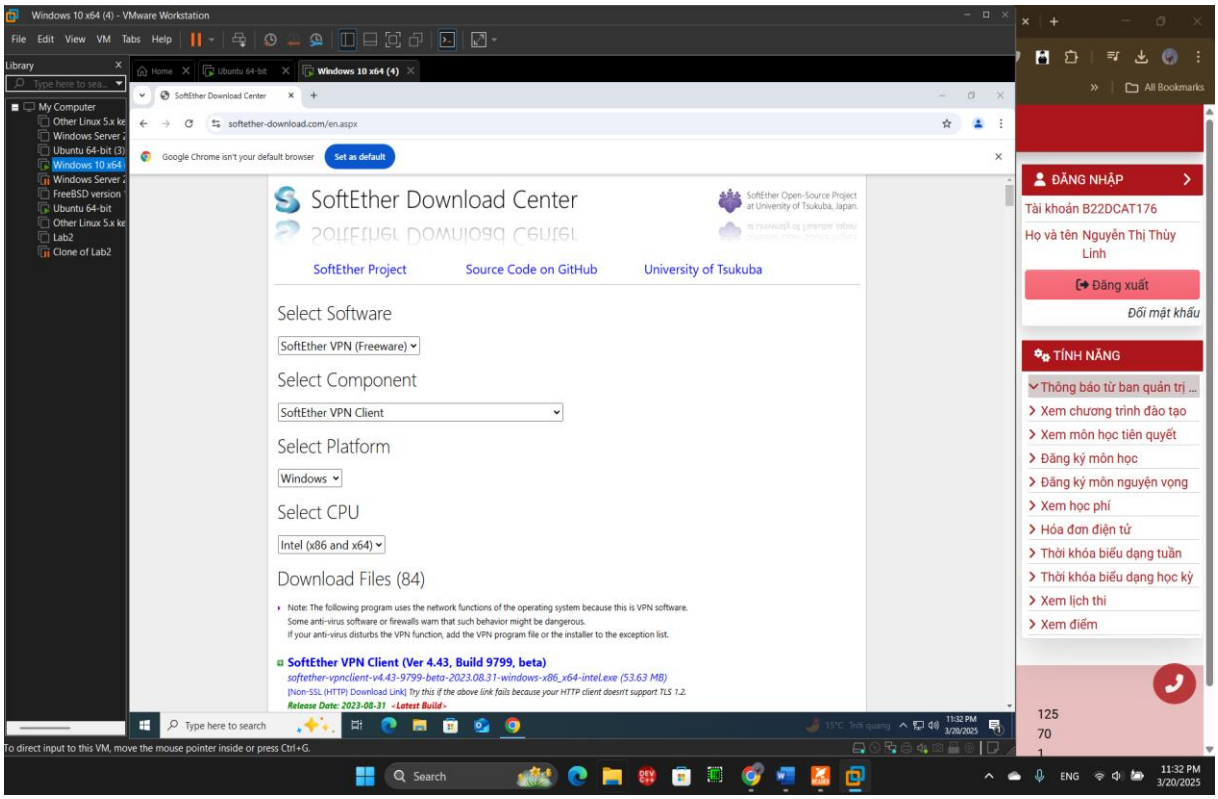
-Tiếp theo tiến hành tạo Hub mới, tạo User trong Hub và thiết lập mật khẩu cho user.



Hình ảnh 19: Tiến hành tạo Hub mới.

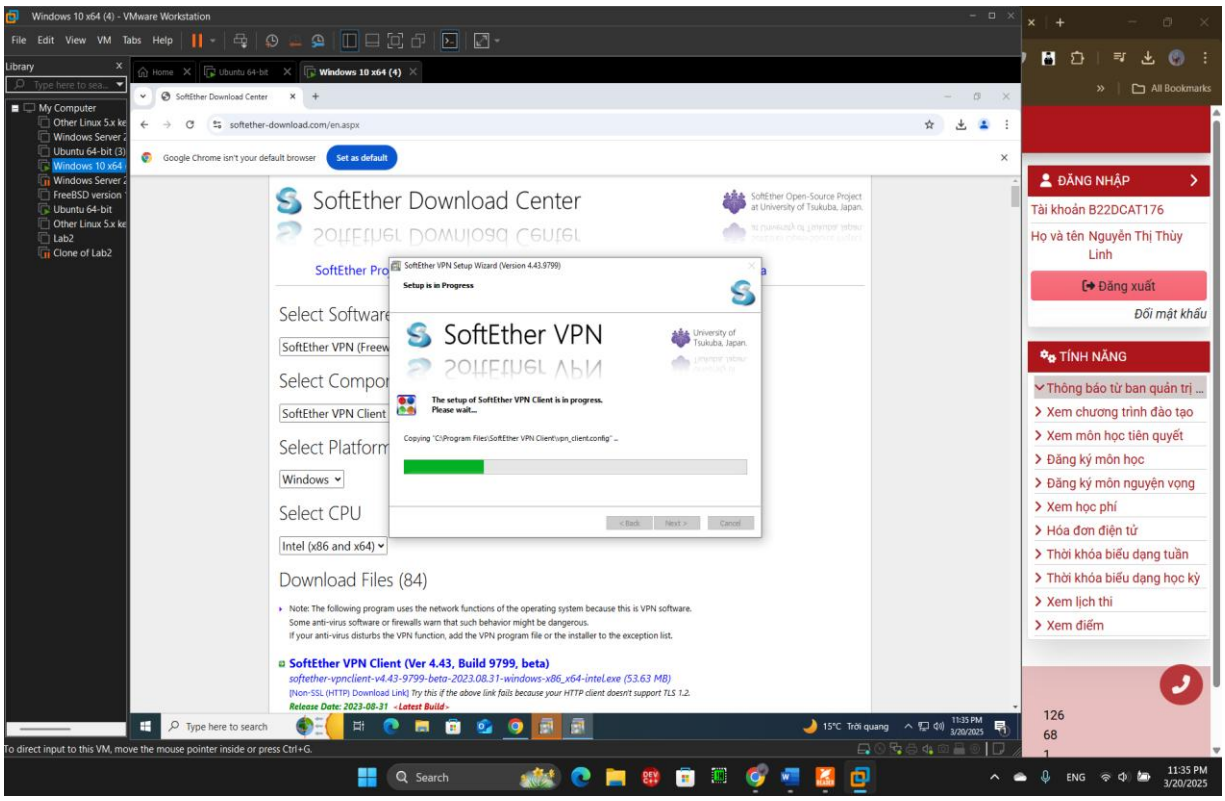
3.Tải SoftEther VPN client cho Windows

-Tiến hành tải và cài đặt VPN client cho máy Windows.



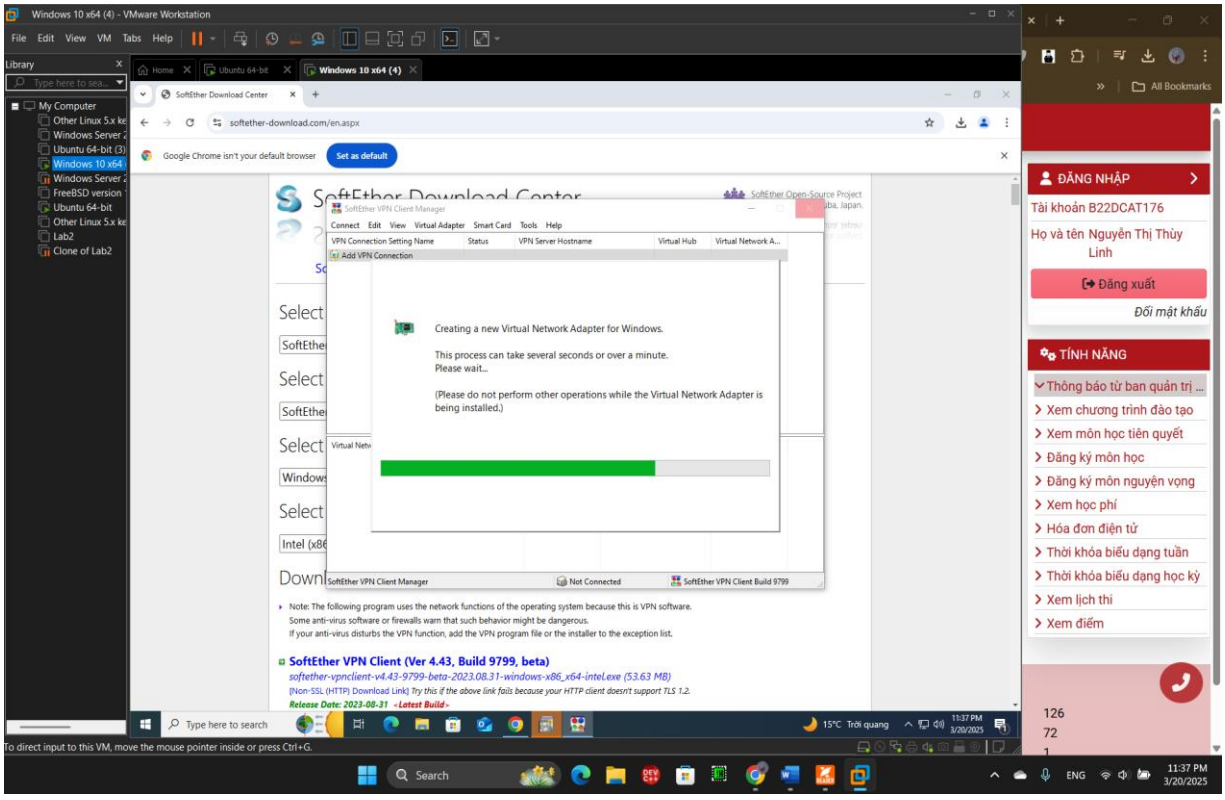
Hình ảnh 20: Tải VPN client.

- Sau khi tải, tiến hành ấn *Next* để cài đặt *VPN Client* trên Windows 10.



Hình ảnh 21: Cài đặt VPN client.

- Trước hết ta tạo một *Virtual Network Adapter* mới.



Hình ảnh 22: Tạo một Virtual Network Adapter mới.

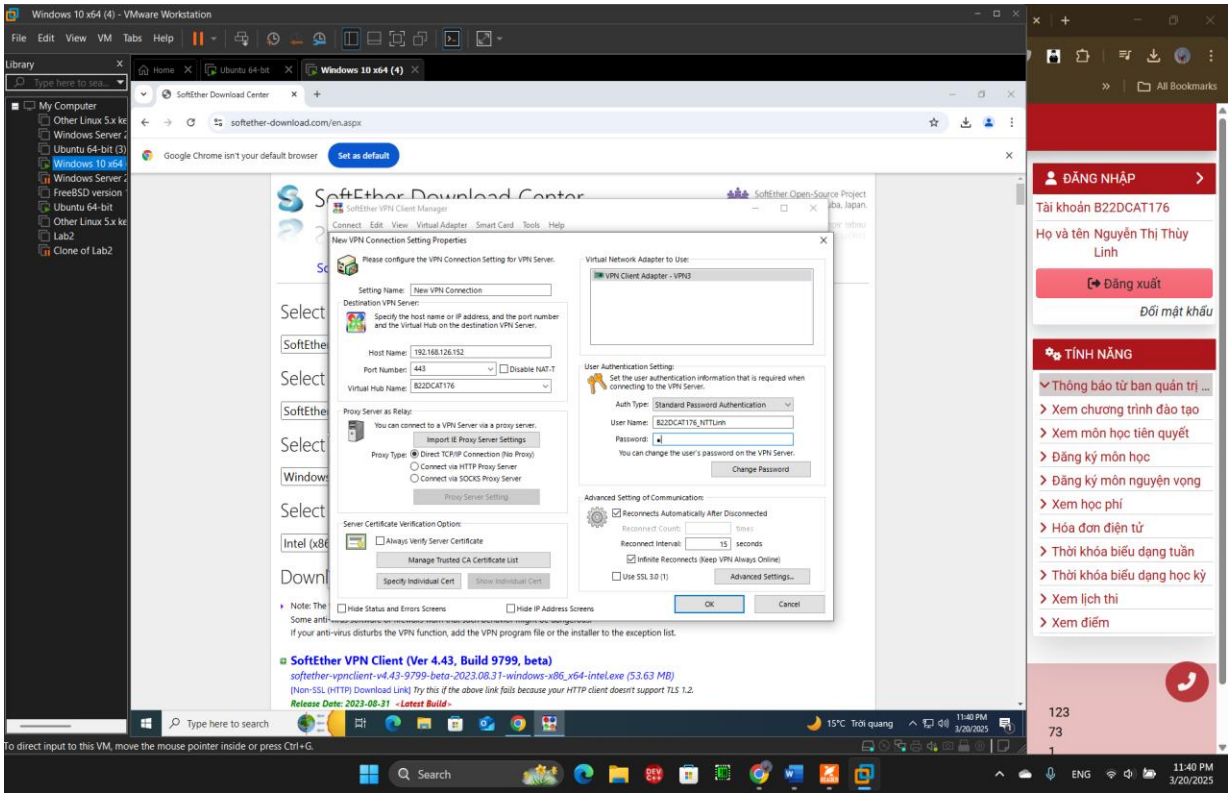
- Tạo và kiểm tra kết nối VPN:

* Từ giao diện *SoftEther VPN Client Manager* tạo 1 kết nối mới (*Add New Connection*)

* Với địa chỉ IP của máy chủ VPN.

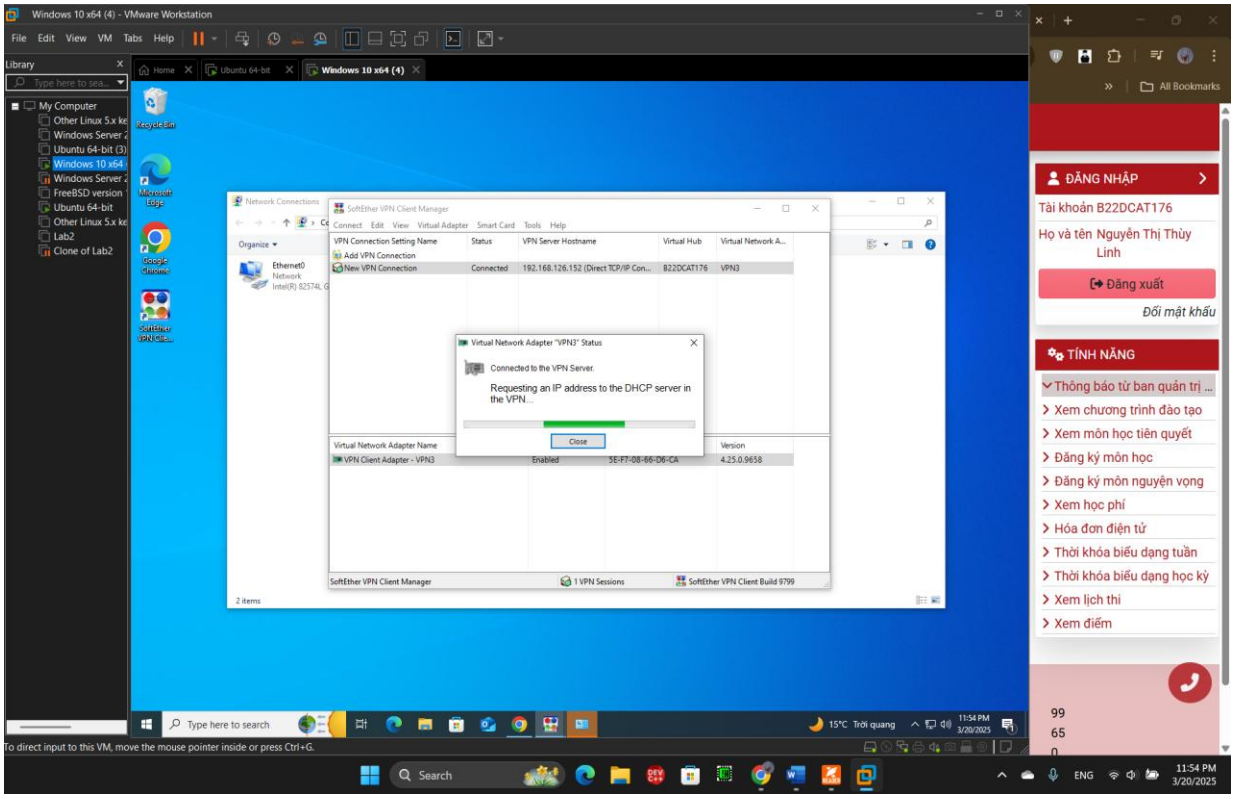
* Tên Virtual Hub, Tên và mật khẩu người dùng

* Đặt tên kết nối



Hình 23: Tạo và kiểm tra kết nối VPN.

-Thử kết nối: Nếu thành công sẽ báo *Connected*.

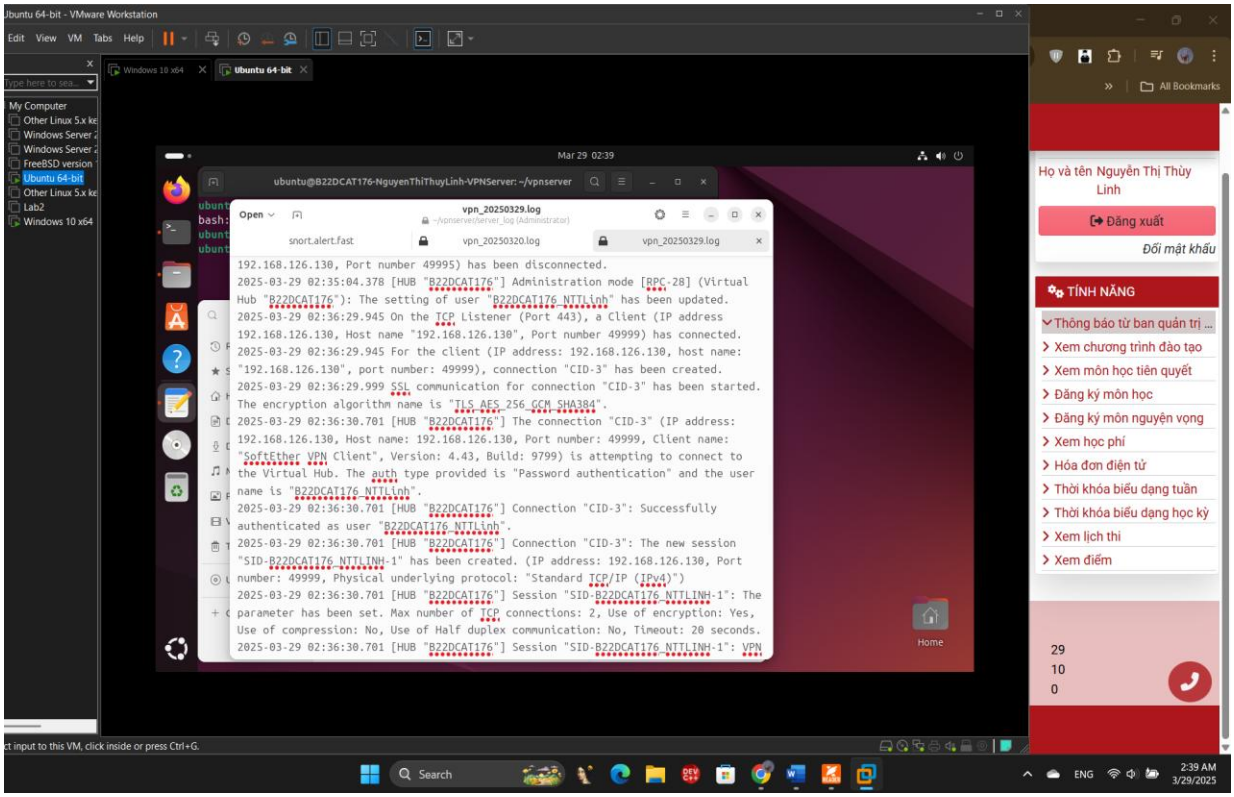


Hình ảnh 24: Thông báo kết nối thành công Connected.

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

-Đọc nội dung file *vpn_20250329.log*

-Ta sẽ có thể xem được các dòng log có liên quan đến *B22DCAT176.*



Hình ảnh 25: Xem các dòng log liên quan đến B22DCAT176.

TÀI LIỆU THAM KHẢO

[1] Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2016.

[2] Tom Carpenter, Microsoft Windows Server Operating System Essentials, Sybex, 2011.

[3] Wale Soyinka, Linux Administration A Beginners Guide, McGraw-Hill Osborne Media, 2012.