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:

B22DCAT251 Đặng Đức Tài

Giảng viên hướng dẫn: TS. Phạm Hoàng Duy

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

DANH MỤC CÁC HÌNH VẼ

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

1.1 Mục đích

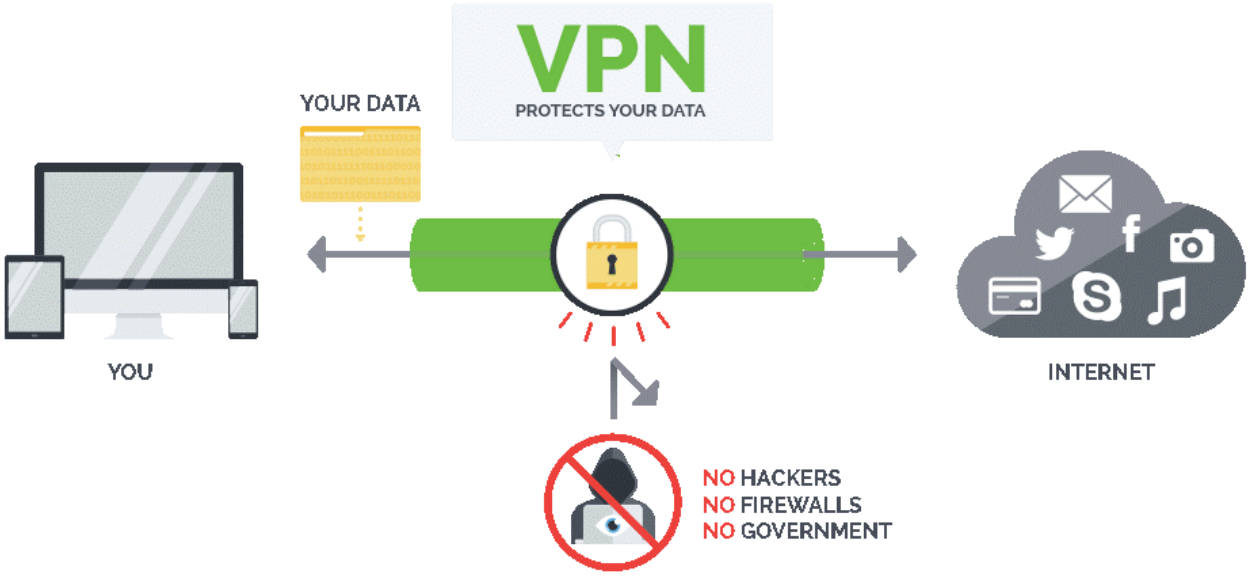
- Tìm hiểu về mạng riêng ảo (VPN-Virtual Private Network), kiến trúc và hoạt động của mạng riêng ảo.
- Luyện tập kỹ năng cài đặt, cấu hình và vận hành máy chủ mạng riêng ảo (VPN server).

1.2 Tìm hiểu lý thuyết

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

1.2.1.1 VPN là gì?

- VPN, viết tắt của Virtual Private Network (Mạng riêng ảo), là một công nghệ tiên tiến cho phép thiết lập một kết nối mạng an toàn thông qua internet hoặc các mạng công cộng khác.
- Khi được kích hoạt, VPN mã hóa toàn bộ dữ liệu gửi đi từ thiết bị của người dùng và truyền chúng qua một "đường hầm" bảo mật đến máy chủ VPN, trước khi dữ liệu đến đích cuối cùng, chẳng hạn như một trang web hoặc dịch vụ trực tuyến.
- Quá trình mã hóa này không chỉ ngăn chặn các bên thứ ba – như nhà cung cấp dịch vụ internet (ISP), tin tặc hoặc cơ quan giám sát – truy cập vào nội dung truyền tải, mà còn che giấu địa chỉ IP thực, khiến hoạt động trực tuyến xuất hiện như thể bắt nguồn từ vị trí của máy chủ VPN. Công nghệ này ra đời từ nhu cầu bảo vệ thông tin nhạy cảm trong thời đại số hóa, đồng thời hỗ trợ vượt qua các rào cản địa lý và truy cập mạng nội bộ từ xa. VPN thường dựa trên các giao thức bảo mật như OpenVPN, L2TP/IPsec hoặc WireGuard để đảm bảo hiệu quả và độ tin cậy.



Hình 1 Tổng quan về VPN

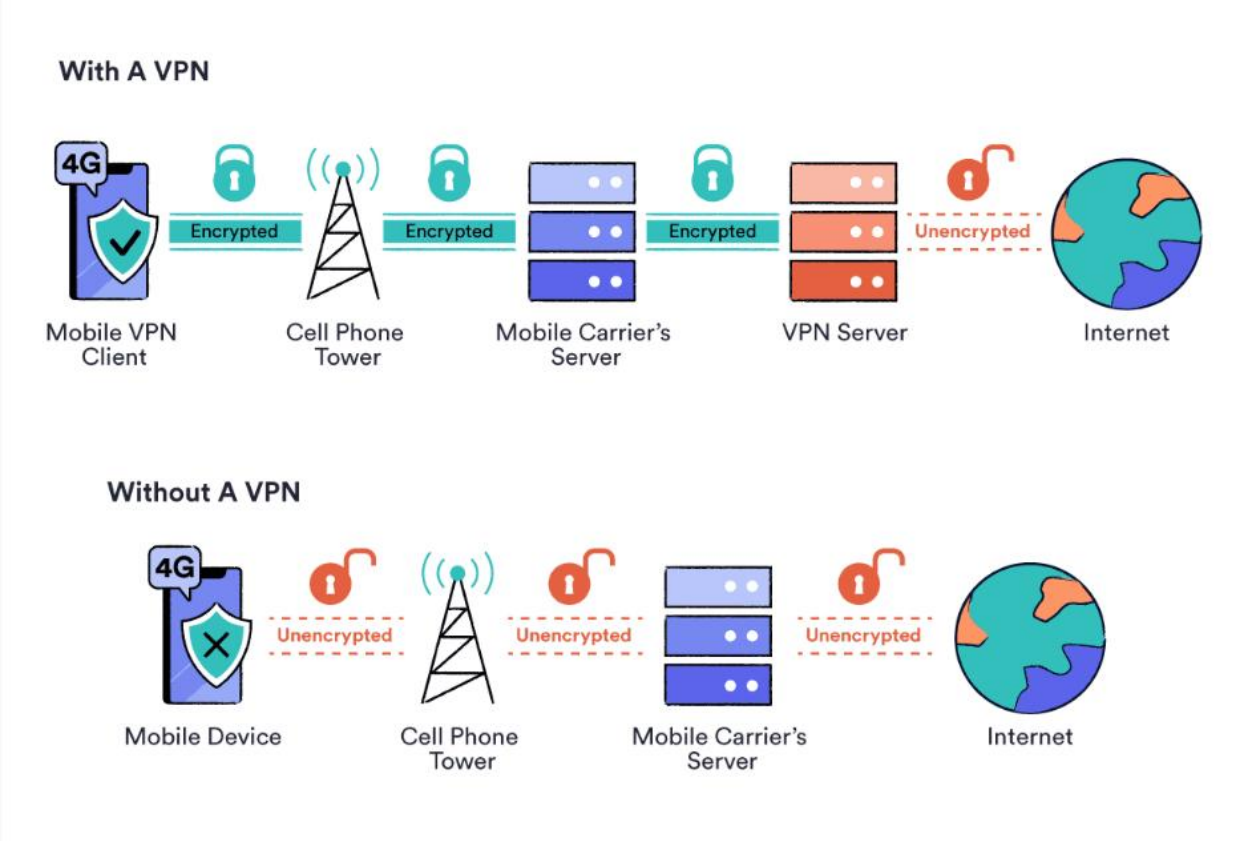
1.2.1.2 Các mô hình VPN

- VPN được triển khai dưới nhiều mô hình khác nhau, mỗi loại đáp ứng một mục đích cụ thể và phù hợp với các đối tượng sử dụng riêng biệt.
- Trước hết, VPN truy cập từ xa (Remote Access VPN) là giải pháp dành cho người dùng cá nhân hoặc nhân viên cần kết nối an toàn đến mạng nội bộ của tổ chức từ các địa điểm bên ngoài. Mô hình này yêu cầu cài đặt phần mềm VPN hoặc cấu hình thủ công trên thiết bị như máy tính, điện thoại thông minh hoặc máy tính bảng. Sau khi kết nối, người dùng có thể truy cập tài nguyên nội bộ – chẳng hạn cơ sở dữ liệu, phần mềm quản lý hoặc tài liệu – như thể đang ở trong văn phòng. Đây là lựa chọn phổ biến cho các công ty hỗ trợ làm việc từ xa hoặc nhân viên thường xuyên di chuyển.
- Tiếp theo, VPN điểm-đến-điểm (Site-to-Site VPN) được thiết kế để kết nối các mạng nội bộ (LAN) tại nhiều địa điểm vật lý khác nhau, chẳng hạn giữa trụ sở chính và chi nhánh của một doanh nghiệp. Thay vì dựa vào phần mềm trên thiết bị cá nhân, mô hình này sử dụng các thiết bị mạng chuyên dụng như bộ định tuyến (router) hoặc cổng (gateway) để tạo một đường hầm mã hóa qua internet. Dữ liệu giữa các mạng được truyền tải liền mạch và an toàn, giúp đồng bộ hóa thông tin và duy trì hoạt động của tổ chức có quy mô lớn, đặc biệt trong các ngành như tài chính, bán lẻ hoặc logistics.
- Một mô hình khác là VPN dựa trên tường lửa (Firewall-based VPN), trong đó chức năng VPN được tích hợp trực tiếp vào hệ thống tường lửa của mạng. Tường lửa không chỉ quản lý lưu lượng truy cập mà còn mã hóa dữ liệu, tạo ra lớp bảo vệ kép trước các mối đe dọa như tấn công mạng hoặc xâm nhập trái phép. Mô hình này thường được các doanh nghiệp vừa và nhỏ triển khai để tối ưu hóa chi phí mà vẫn đảm bảo an ninh mạng hiệu quả.
- Cuối cùng, VPN cá nhân (Personal VPN) là loại phổ biến nhất với người dùng thông thường, được cung cấp bởi các nhà dịch vụ thương mại như NordVPN, ExpressVPN hay Surfshark. Người dùng chỉ cần tải ứng dụng, đăng nhập và chọn máy chủ từ danh sách các quốc gia để kết nối. Loại VPN này tập trung vào việc đơn giản hóa trải nghiệm, đồng thời cung cấp khả năng bảo vệ dữ liệu, ẩn danh trực tuyến và truy cập nội dung bị giới hạn địa lý, chẳng hạn như các chương trình phát trực tuyến hoặc trang web bị chặn.

1.2.1.3 Ứng dụng của VPN

- VPN mang lại nhiều ứng dụng thực tiễn, đáp ứng nhu cầu đa dạng từ cá nhân đến tổ chức trong bối cảnh kết nối toàn cầu ngày càng gia tăng.

- Một trong những ứng dụng quan trọng nhất là bảo vệ quyền riêng tư. Bằng cách mã hóa dữ liệu và che giấu địa chỉ IP, VPN ngăn chặn nhà cung cấp dịch vụ internet, chính phủ hoặc tin tặc theo dõi lịch sử truy cập, thói quen duyệt web hoặc thông tin cá nhân. Điều này đặc biệt hữu ích trong các tình huống nhạy cảm, như giao dịch tài chính trực tuyến hoặc trao đổi thông tin mật.
- VPN cũng đóng vai trò quan trọng trong việc vượt qua giới hạn địa lý. Nhiều dịch vụ phát trực tuyến như Netflix, Hulu hoặc BBC iPlayer áp dụng chính sách chặn nội dung dựa trên vị trí người dùng. Với VPN, người dùng có thể kết nối đến máy chủ tại quốc gia mong muốn để truy cập các thư viện nội dung khác nhau. Tương tự, công nghệ này giúp vượt qua kiểm duyệt internet tại các quốc gia có chính sách hạn chế, chẳng hạn như truy cập mạng xã hội hoặc trang tin tức bị chặn.
- Trong môi trường doanh nghiệp, VPN là công cụ không thể thiếu để hỗ trợ làm việc từ xa. Nhân viên có thể kết nối an toàn đến mạng công ty từ nhà, khách sạn hoặc bất kỳ đâu, đảm bảo truy cập vào hệ thống nội bộ mà không lo rò rỉ dữ liệu. Điều này đặc biệt quan trọng trong các ngành yêu cầu bảo mật cao như y tế, pháp lý hoặc công nghệ.
- Ngoài ra, VPN tăng cường bảo mật khi sử dụng Wi-Fi công cộng, chẳng hạn tại sân bay, quán cà phê hoặc thư viện. Các mạng này thường dễ bị tấn công bởi tin tặc sử dụng kỹ thuật nghe lén (man-in-the-middle), nhưng VPN mã hóa dữ liệu giúp giảm thiểu nguy cơ bị đánh cắp thông tin như mật khẩu hoặc chi tiết thẻ tín dụng.
- Tuy nhiên, VPN không phải không có hạn chế. Quá trình mã hóa có thể làm giảm tốc độ kết nối, đặc biệt khi máy chủ VPN ở xa hoặc tải nặng. Dịch vụ trả phí chất lượng cao thường đòi hỏi chi phí hàng tháng, trong khi các VPN miễn phí có thể thiếu độ tin cậy hoặc thậm chí khai thác dữ liệu người dùng. Hiệu quả của VPN cũng phụ thuộc lớn vào uy tín và cơ sở hạ tầng của nhà cung cấp.



Hình 2 Mô phỏng khi sử dụng và không sử dụng VPN

1.2.2 Tìm hiểu về các giao thức tạo đường hầm cho VPN

- Công nghệ VPN (Virtual Private Network) phụ thuộc vào các giao thức tạo đường hầm để đảm bảo dữ liệu được truyền tải an toàn qua mạng công cộng như internet. Các giao thức này đóng vai trò thiết lập và duy trì "đường hầm" – một kênh mã hóa kết nối giữa thiết bị người dùng và máy chủ VPN. Trong số các giao thức từng được sử dụng hoặc vẫn đang phổ biến, PPTP, L2TP, L2F và MPLS nổi bật với những đặc điểm riêng biệt về hiệu suất, bảo mật và ứng dụng. Phần sau sẽ phân tích chi tiết từng giao thức để làm rõ vai trò của chúng trong hệ sinh thái VPN.

1.2.2.1 PPTP (Point-to-Point Tunneling Protocol)

- PPTP, hay Giao thức tạo đường hầm điểm-đến-điểm, là một trong những giao thức VPN lâu đời nhất, được Microsoft phát triển vào những năm 1990 và tích hợp sẵn trong nhiều hệ điều hành Windows. Giao thức này dựa trên nền tảng của PPP (Point-to-Point Protocol), một chuẩn truyền thông cơ bản, để đóng gói dữ liệu và tạo đường hầm qua mạng IP. PPTP sử dụng cơ chế mã hóa 128-bit thông qua thuật toán MS-CHAP hoặc GRE (Generic Routing Encapsulation) để bảo vệ dữ liệu trong quá trình truyền tải. Điểm mạnh của PPTP nằm ở tốc độ cao và tính đơn giản, nhờ yêu cầu tài

nguyên xử lý thấp, khiến nó trở thành lựa chọn phổ biến trong giai đoạn đầu của VPN, đặc biệt cho các kết nối quay số (dial-up).

- Tuy nhiên, PPTP ngày nay bị coi là lỗi thời do những lỗ hổng bảo mật nghiêm trọng. Các nghiên cứu đã chỉ ra rằng mã hóa 128-bit của nó dễ bị phá vỡ bởi các cuộc tấn công như nghe lén hoặc giải mã brute-force, đặc biệt khi đối mặt với công nghệ hiện đại. Hơn nữa, PPTP không hỗ trợ các tính năng bảo mật nâng cao như xác thực đa yếu tố hoặc mã hóa mạnh hơn. Vì vậy, dù vẫn được một số thiết bị cũ hỗ trợ, PPTP hầu như không còn được khuyến nghị trong các hệ thống VPN hiện đại, nơi yêu cầu về an ninh mạng ngày càng cao.

1.2.2.2 L2TP (Layer 2 Tunneling Protocol)

- L2TP, hay Giao thức tạo đường hầm lớp 2, là một bước tiến so với PPTP, được phát triển bởi Microsoft và Cisco vào cuối những năm 1990. Giao thức này kết hợp các ưu điểm của PPTP với L2F (sẽ được đề cập sau) để cung cấp khả năng tạo đường hầm mạnh mẽ hơn. L2TP hoạt động ở tầng 2 (Data Link Layer) của mô hình OSI, cho phép đóng gói dữ liệu từ các giao thức như PPP và truyền qua mạng IP. Để tăng cường bảo mật, L2TP thường được triển khai cùng IPsec (Internet Protocol Security), cung cấp mã hóa AES 128-bit hoặc 256-bit, cùng với xác thực và bảo vệ tính toàn vẹn của dữ liệu.
- L2TP/IPsec mang lại độ an toàn cao hơn đáng kể so với PPTP, nhờ khả năng mã hóa kép: một lần ở tầng đường hầm và một lần ở tầng IPsec. Điều này giúp bảo vệ dữ liệu khỏi các mối đe dọa như tấn công trung gian (man-in-the-middle). Tuy nhiên, nhược điểm của L2TP nằm ở hiệu suất, bởi quá trình mã hóa kép đòi hỏi nhiều tài nguyên xử lý hơn, dẫn đến tốc độ kết nối chậm hơn so với các giao thức nhẹ hơn như PPTP. Ngoài ra, L2TP có thể gặp khó khăn khi vượt qua tường lửa hoặc NAT (Network Address Translation), do sử dụng cổng UDP cố định dễ bị chặn. Dù vậy, L2TP vẫn được sử dụng rộng rãi trong VPN cá nhân và doanh nghiệp nhờ sự cân bằng giữa bảo mật và tính tương thích.

1.2.2.3 L2F (Layer 2 Forwarding)

- L2F, hay Chuyển tiếp lớp 2, là giao thức do Cisco phát triển vào giữa những năm 1990, trước khi L2TP ra đời. Mục tiêu chính của L2F là hỗ trợ tạo đường hầm cho các kết nối PPP qua mạng công cộng, đặc biệt trong bối cảnh các nhà cung cấp dịch vụ internet (ISP) cần kết nối người dùng từ xa đến mạng doanh nghiệp. Giống như L2TP, L2F hoạt động ở tầng 2 của mô hình OSI, nhưng nó không tích hợp mã hóa mạnh mẽ như IPsec. Thay vào đó, L2F tập trung vào khả năng chuyển tiếp dữ liệu hiệu quả và hỗ trợ đa giao thức, cho phép kết nối giữa các hệ thống không đồng nhất.

- Tuy nhiên, L2F nhanh chóng bị lu mờ bởi sự xuất hiện của L2TP, vốn kế thừa và cải tiến các tính năng của nó. Một hạn chế lớn của L2F là thiếu cơ chế mã hóa độc lập, khiến dữ liệu dễ bị tổn thương nếu không được bảo vệ bởi lớp bảo mật bổ sung từ thiết bị hoặc mạng. Ngày nay, L2F gần như không còn được sử dụng trong các hệ thống VPN hiện đại, nhưng nó đóng vai trò quan trọng trong lịch sử phát triển công nghệ đường hầm, đặt nền móng cho các giao thức tiên tiến hơn.

1.2.2.4 MPLS (Multiprotocol Label Switching)

- MPLS, hay Chuyển mạch nhãn đa giao thức, là một giao thức khác biệt so với ba loại trên, thường được ứng dụng trong VPN doanh nghiệp hơn là VPN cá nhân. Không giống PPTP, L2TP hay L2F – vốn dựa vào mã hóa để tạo đường hầm – MPLS sử dụng cơ chế gắn nhãn (label) để định tuyến dữ liệu qua mạng. Mỗi gói tin được gán một nhãn khi vào mạng MPLS, và các bộ định tuyến (router) sử dụng nhãn này để chuyển tiếp dữ liệu mà không cần phân tích địa chỉ IP chi tiết. Điều này giúp tăng tốc độ xử lý và giảm độ trễ, đặc biệt trong các mạng quy mô lớn.
- MPLS không tập trung vào mã hóa dữ liệu mà ưu tiên hiệu suất và quản lý lưu lượng. Tuy nhiên, khi kết hợp với VPN (thường gọi là MPLS VPN), nó cung cấp khả năng phân tách lưu lượng giữa các khách hàng hoặc chi nhánh, tạo ra các mạng riêng ảo logic. MPLS thường được các nhà cung cấp dịch vụ viễn thông triển khai để xây dựng mạng WAN (Wide Area Network) cho doanh nghiệp, đảm bảo kết nối ổn định giữa các địa điểm mà không cần mã hóa phức tạp. Dù vậy, vì thiếu mã hóa mặc định, MPLS cần được bổ sung các giao thức như IPsec nếu yêu cầu bảo mật cao.

1.2.3 Các giao thức bảo mật cho VPN

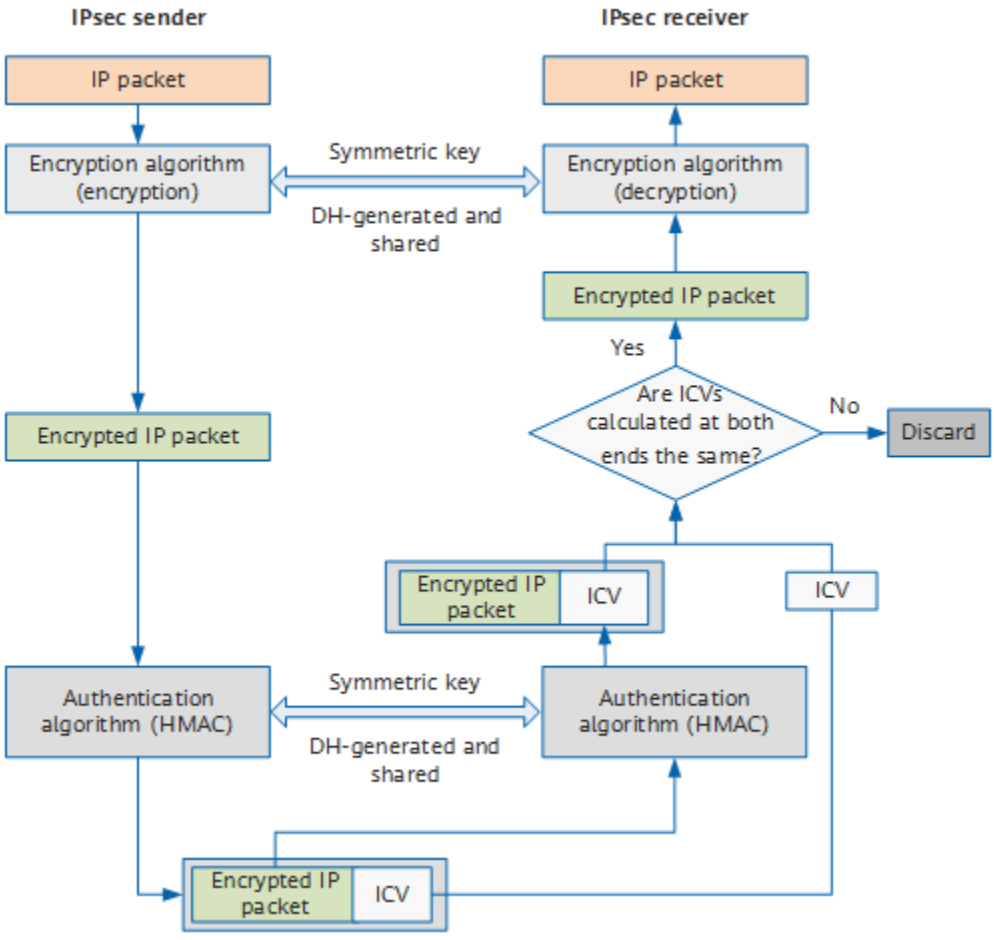
- Bên cạnh các giao thức tạo đường hầm, VPN còn phụ thuộc vào các giao thức bảo mật để đảm bảo dữ liệu được mã hóa và bảo vệ khỏi các mối đe dọa trong quá trình truyền tải qua mạng công cộng. Trong số đó, IPsec (Internet Protocol Security) và SSL/TLS (Secure Sockets Layer/Transport Layer Security) là hai giao thức nổi bật, được ứng dụng rộng rãi trong các hệ thống VPN hiện đại. Mỗi giao thức mang đặc điểm riêng về cách hoạt động, mức độ bảo mật và phạm vi ứng dụng, đóng vai trò quan trọng trong việc duy trì tính an toàn và toàn vẹn của kết nối VPN. Phần sau sẽ phân tích chi tiết từng giao thức để làm rõ vai trò của chúng.

1.2.3.1 IPsec (Internet Protocol Security)

- IPsec là một bộ giao thức bảo mật hoạt động ở tầng mạng (Network Layer) trong mô hình OSI, được thiết kế để bảo vệ dữ liệu ở cấp độ gói tin IP. Được phát triển bởi IETF (Internet Engineering Task Force), IPsec không chỉ là một giao thức đơn

lẻ mà là tập hợp các công cụ và quy trình, bao gồm mã hóa, xác thực và kiểm tra tính toàn vẹn. IPsec thường được triển khai trong hai chế độ chính: chế độ vận chuyển (Transport Mode) – chỉ mã hóa phần dữ liệu của gói tin – và chế độ đường hầm (Tunnel Mode) – mã hóa cả tiêu đề và dữ liệu, thường được dùng trong VPN.

- Cơ chế hoạt động của IPsec dựa trên ba thành phần chính: AH (Authentication Header) để xác thực nguồn gốc và bảo vệ tính toàn vẹn, ESP (Encapsulating Security Payload) để mã hóa dữ liệu và cung cấp thêm xác thực, cùng IKE (Internet Key Exchange) để quản lý khóa mã hóa. IPsec hỗ trợ nhiều thuật toán mã hóa mạnh mẽ như AES (Advanced Encryption Standard) với độ dài khóa 128-bit hoặc 256-bit, kết hợp với các hàm băm như SHA-256 để đảm bảo dữ liệu không bị thay đổi trong quá trình truyền tải. Nhờ tính linh hoạt này, IPsec thường được kết hợp với các giao thức tạo đường hầm như L2TP (Layer 2 Tunneling Protocol) để tạo thành L2TP/IPsec, mang lại khả năng bảo mật toàn diện.



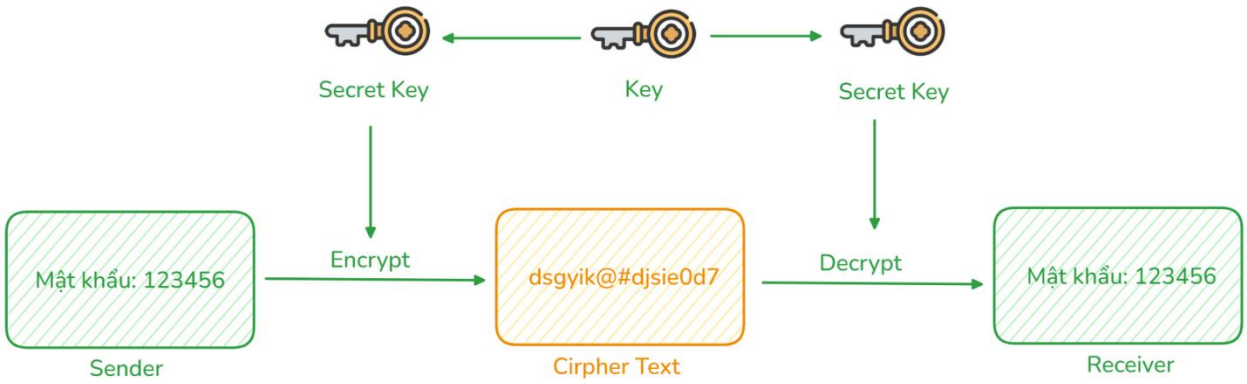
Hình 3 Quy trình xác thực & mã hóa IPSec

- Ưu điểm của IPsec nằm ở khả năng bảo vệ dữ liệu ở cấp độ mạng, phù hợp với VPN điểm-đến-điểm (Site-to-Site VPN) và VPN truy cập từ xa (Remote Access VPN).

Tuy nhiên, nhược điểm của nó là độ phức tạp trong cấu hình và yêu cầu tài nguyên xử lý cao, đặc biệt khi mã hóa toàn bộ lưu lượng mạng. Ngoài ra, IPsec có thể gặp khó khăn khi vượt qua tường lửa hoặc NAT do sử dụng các cổng đặc thù (như UDP 500), đòi hỏi điều chỉnh bổ sung để đảm bảo tính tương thích.

1.2.3.2 SSL/TLS (Secure Sockets Layer/Transport Layer Security)

- SSL/TLS là giao thức bảo mật hoạt động ở tầng ứng dụng (Application Layer) hoặc tầng giao vận (Transport Layer) của mô hình OSI, ban đầu được Netscape phát triển dưới tên SSL vào năm 1995, sau đó tiến hóa thành TLS với các phiên bản cập nhật như TLS 1.3 hiện nay. Không giống IPsec – vốn bảo vệ toàn bộ lưu lượng mạng – SSL/TLS tập trung vào bảo mật dữ liệu cho các ứng dụng cụ thể, chẳng hạn như trình duyệt web, email hoặc phần mềm doanh nghiệp. Trong bối cảnh VPN, SSL/TLS thường được sử dụng trong các giải pháp VPN dựa trên trình duyệt (SSL VPN), cho phép truy cập từ xa mà không cần cài đặt phần mềm phức tạp.
- Cơ chế hoạt động của SSL/TLS dựa trên mã hóa bất đối xứng (asymmetric encryption) để thiết lập kết nối an toàn ban đầu thông qua cái gọi là "bắt tay" (handshake). Trong quá trình này, máy khách và máy chủ trao đổi chứng chỉ số (digital certificate) và khóa công khai để xác thực lẫn nhau, sau đó chuyển sang mã hóa đối xứng (symmetric encryption) với các thuật toán như AES để truyền dữ liệu hiệu quả. SSL/TLS cũng tích hợp các hàm băm như SHA-256 để kiểm tra tính toàn vẹn, đảm bảo dữ liệu không bị can thiệp.



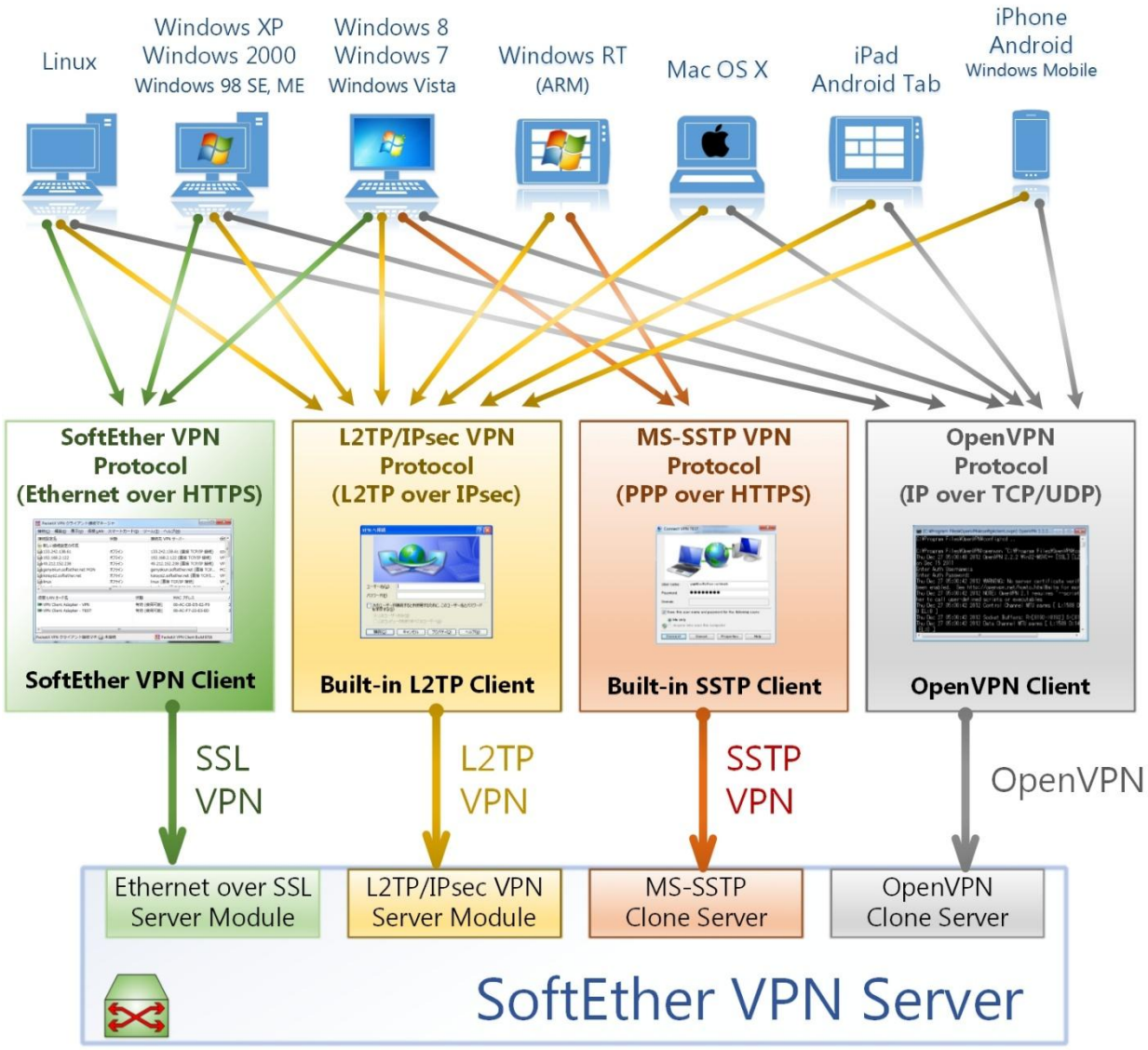
Hình 4 Mã hóa bất đối xứng trong TLS/SSL

- Ưu điểm của SSL/TLS nằm ở tính đơn giản và khả năng tương thích cao. Người dùng chỉ cần một trình duyệt hỗ trợ SSL/TLS để kết nối đến cổng web của VPN (thường là cổng 443 – cổng mặc định của HTTPS), giúp dễ dàng vượt qua tường lửa và NAT mà không cần cấu hình phức tạp. Điều này khiến SSL VPN trở thành lựa chọn phổ biến cho truy cập từ xa vào tài nguyên công ty, chẳng hạn như cổng

thông tin nội bộ hoặc ứng dụng đám mây. Tuy nhiên, hạn chế của SSL/TLS là chỉ bảo vệ dữ liệu ứng dụng cụ thể, không mã hóa toàn bộ lưu lượng mạng như IPsec, do đó ít phù hợp với VPN điểm-đến-điểm quy mô lớn. Ngoài ra, nếu chứng chỉ số không được quản lý tốt, hệ thống có thể dễ bị tấn công giả mạo (spoofing).

1.2.4 Tìm hiểu về SoftEther VPN

- SoftEther VPN là một phần mềm VPN mã nguồn mở, đa giao thức, được phát triển bởi Daiyuu Nobori tại Đại học Tsukuba, Nhật Bản, và ra mắt vào năm 2014. Ban đầu, phần mềm này sử dụng giấy phép GPLv2, nhưng đến năm 2019, nó đã chuyển sang giấy phép Apache License 2.0. Với khả năng hỗ trợ nhiều hệ điều hành như Windows, Linux, macOS, iOS và Android, SoftEther VPN mang lại một giải pháp kết nối an toàn và linh hoạt, phù hợp cho cả cá nhân lẫn doanh nghiệp.
- Mục tiêu của SoftEther VPN là khắc phục những hạn chế của các giao thức VPN truyền thống như PPTP. Tên gọi "SoftEther" (Software Ethernet) phản ánh chính xác chức năng của nó: ảo hóa mạng Ethernet thông qua phần mềm, giúp tạo ra một mạng riêng ảo hoạt động ở tầng 2. Phần mềm này bao gồm ba thành phần chính: máy chủ VPN (VPN Server), cầu nối VPN (VPN Bridge) và ứng dụng khách VPN (VPN Client).
- SoftEther VPN hoạt động bằng cách mô phỏng Ethernet thông qua một Virtual Hub trên máy chủ và một Virtual Network Adapter trên thiết bị khách. Kết nối giữa các thiết bị diễn ra qua giao thức SSL (VPN over HTTPS) trên cổng 443, giúp phần mềm dễ dàng vượt qua các tường lửa và hạn chế mạng. Ngoài ra, SoftEther VPN còn hỗ trợ nhiều giao thức khác như L2TP/IPsec, OpenVPN, và SSTP, đồng thời cung cấp các tính năng như xuyên NAT và sử dụng DNS động, giúp đơn giản hóa quá trình triển khai.



Hình 5 Mô phỏng SoftEther VPN Server

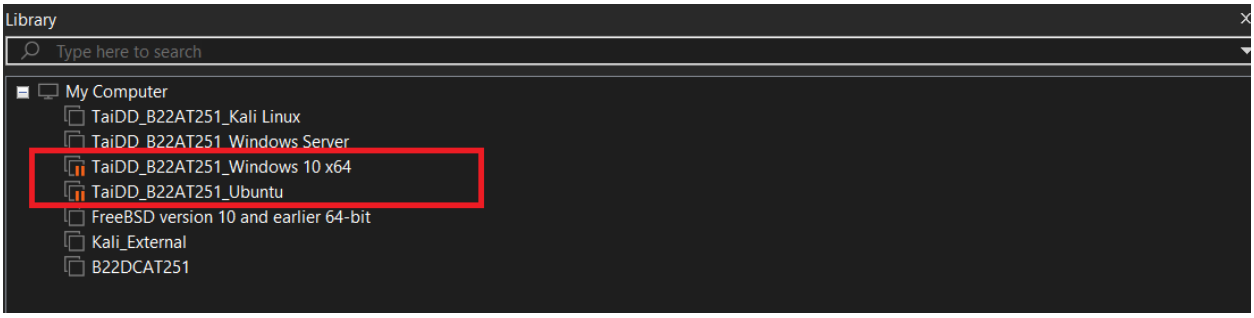
- Một trong những ưu điểm nổi bật của SoftEther VPN là khả năng mã hóa mạnh mẽ với AES 256-bit và RSA 4096-bit, cùng với tính năng vượt tường lửa thông qua ICMP hoặc DNS. Phần mềm này có tốc độ kết nối tối đa lên đến 1 Gbps, hỗ trợ cả IPv4 và IPv6, đồng thời cung cấp giao diện thân thiện với người dùng, bao gồm cả GUI và dòng lệnh. Đặc biệt, nó được thiết kế để hoạt động ổn định, không rò rỉ bộ nhớ và đảm bảo hiệu suất cao.
- Với những tính năng mạnh mẽ như vậy, SoftEther VPN được sử dụng rộng rãi để bảo vệ quyền riêng tư, vượt qua các giới hạn địa lý khi truy cập internet, kết nối từ xa với mạng gia đình hoặc doanh nghiệp, và thiết lập hệ thống VPN cho doanh nghiệp với mô hình Remote Access hoặc Site-to-Site. Nhờ vào khả năng cầu nối

Ethernet và định tuyến IP linh hoạt, SoftEther VPN trở thành một giải pháp lý tưởng cho nhu cầu kết nối an toàn và hiệu quả.

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

2.1 Chuẩn bị môi trường

- 01 máy tính (máy thật hoặc máy ảo) chạy Linux để cài đặt VPN server (Ubuntu).
- 01 máy tính (máy thật hoặc máy ảo) chạy Windows để cài đặt VPN client (Windows 10).



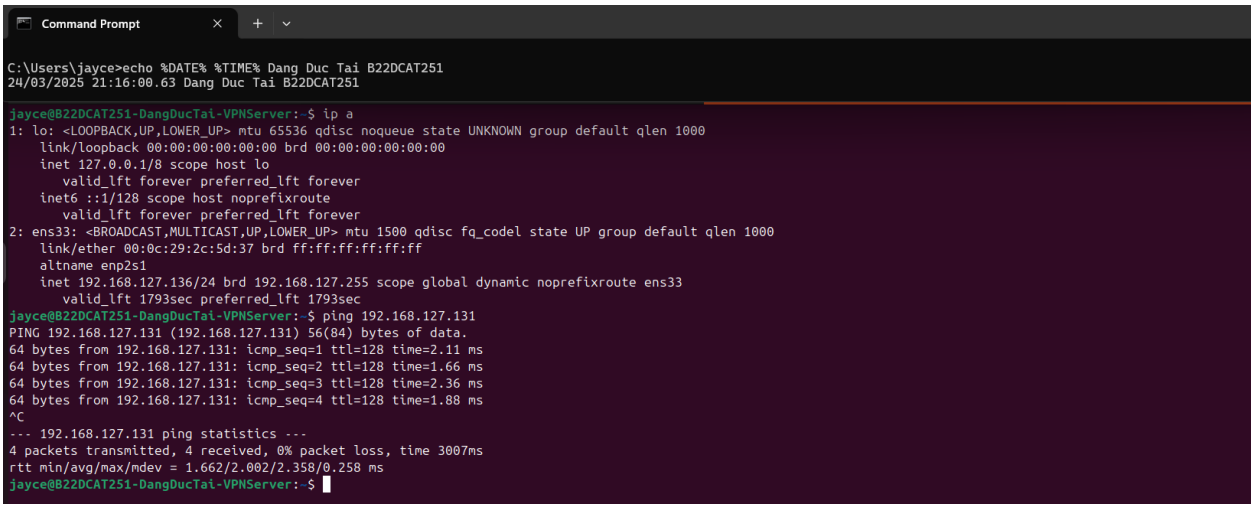
Hình 6 Chuẩn bị môi trường

2.2 Các bước thực hiện

2.2.1 Cài đặt môi trường

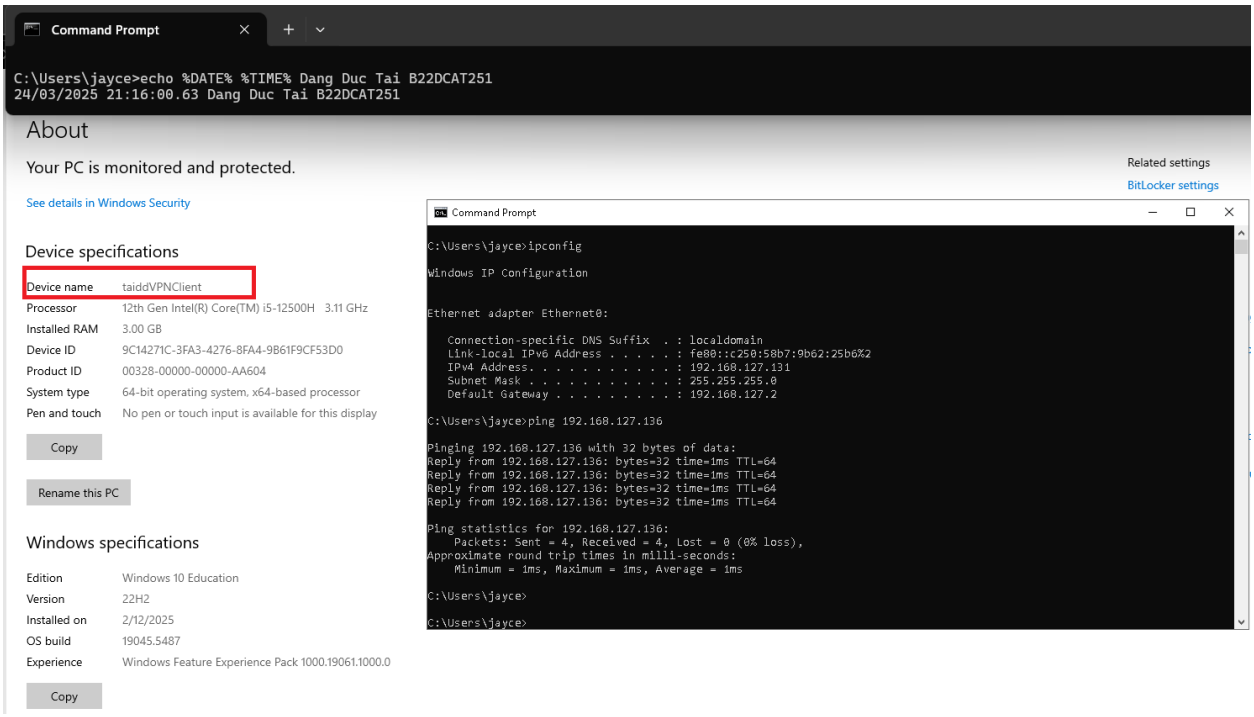
- Chuẩn bị các máy tính như mô tả trong mục 2.1. Thực hiện đổi tên các máy theo format: máy Windows được đổi tên thành <Mã SV-Tên SV>-VPNClient và máy cài VPN server thành <Mã SV-Tên SV>-VPNServer. Các máy có địa chỉ IP và kết nối mạng LAN (Ping để kiểm tra kết nối).

- Máy VPNServer (Ubuntu)



Hình 7 Máy VPNServer

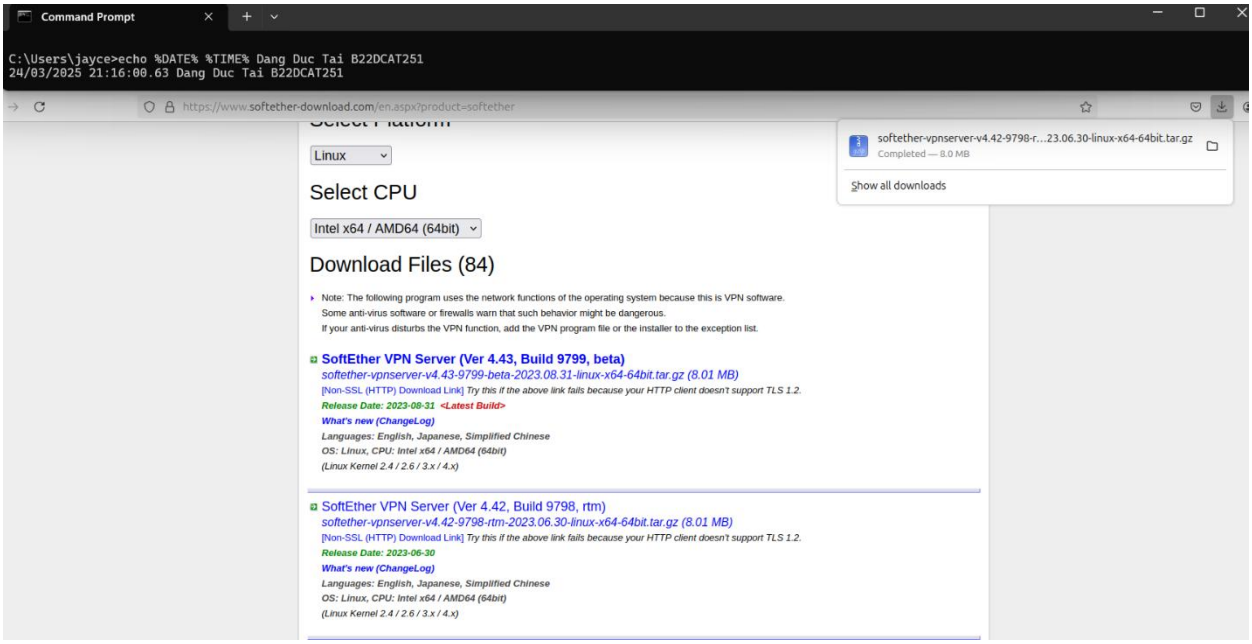
- Máy VPNClient (Windows 10)



Hình 8 Máy VPNClient

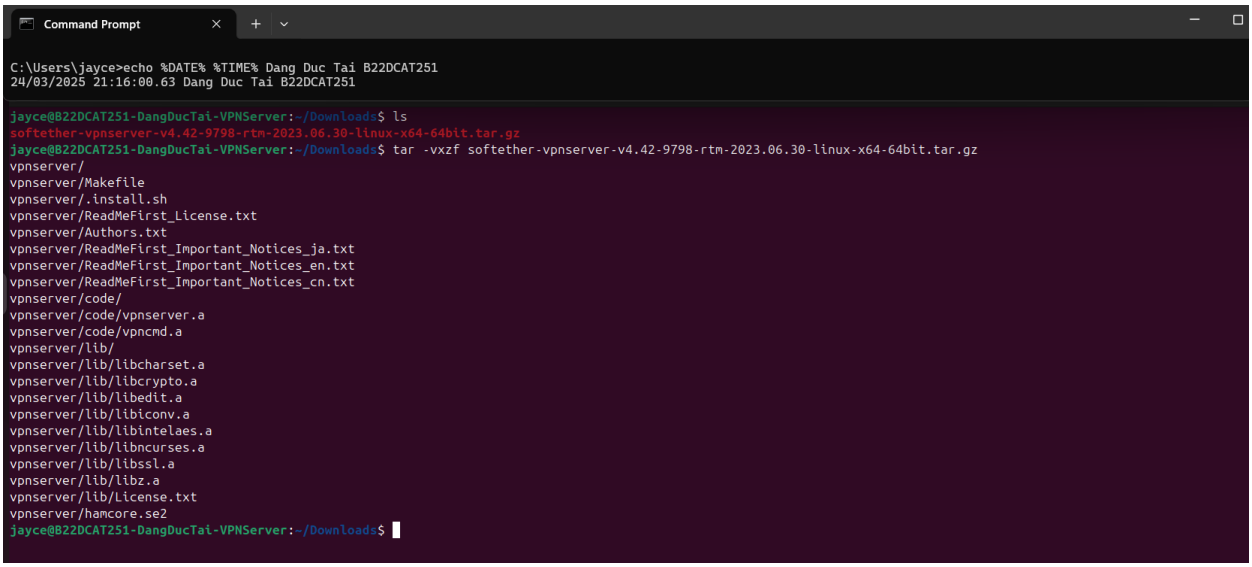
2.2.2 Cấu hình VPN Server

- Trên máy Ubuntu, tải SoftEther VPN Server tại https://www.softether.org/5-download



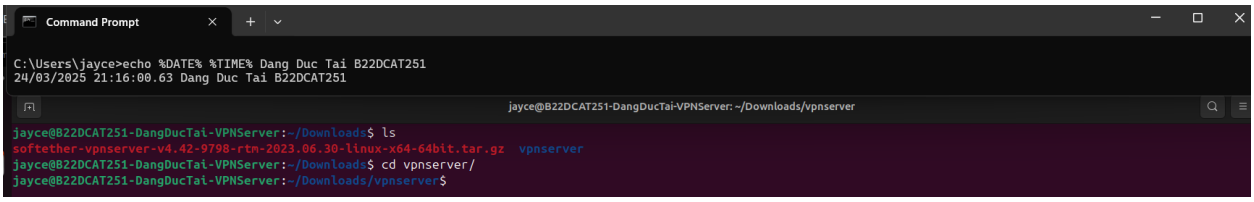
Hình 9 Tải SoftEther VPN Server

- Giải nén vào thư mục bằng lệnh
  tar -vxzf <tên file VPN Server>



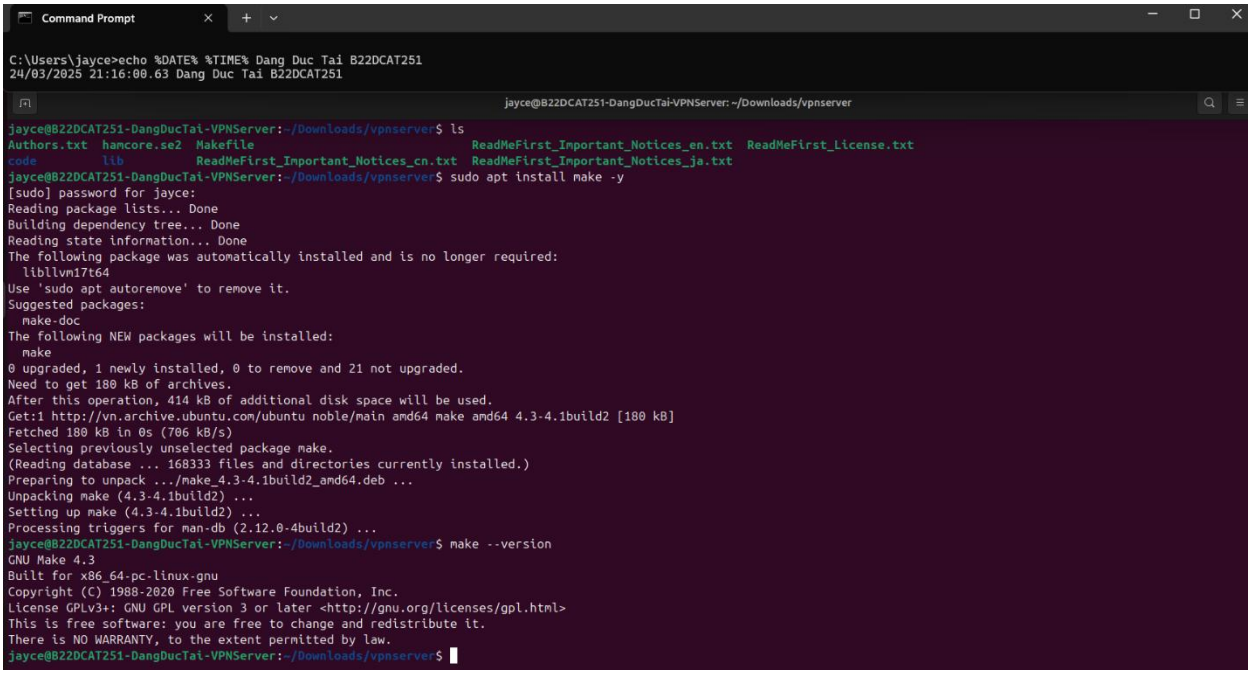
Hình 10 Giải nén file cài đặt

- Chuyển hướng tới thư mục chứa file cài đặt
  cd vpnserver



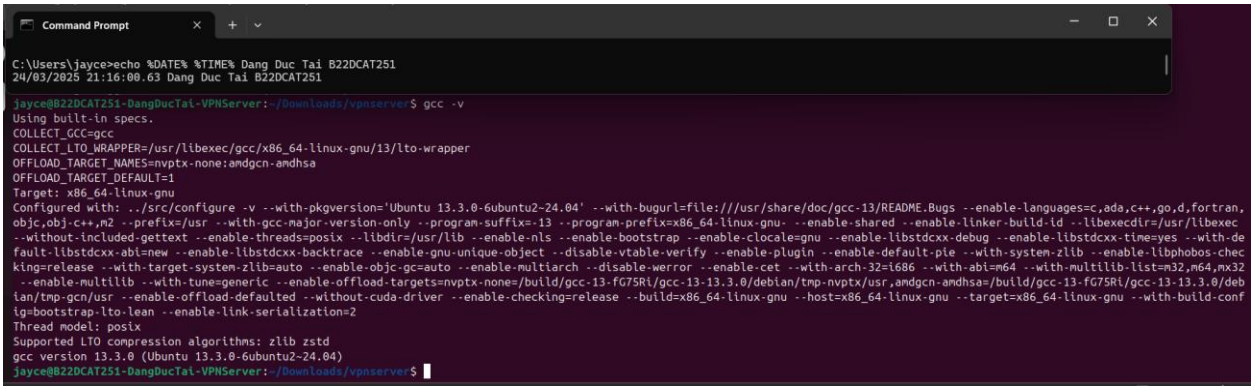
Hình 11 Chuyển hướng tới thư mục vpnserver

- Cài đặt make
  sudo apt install make -y



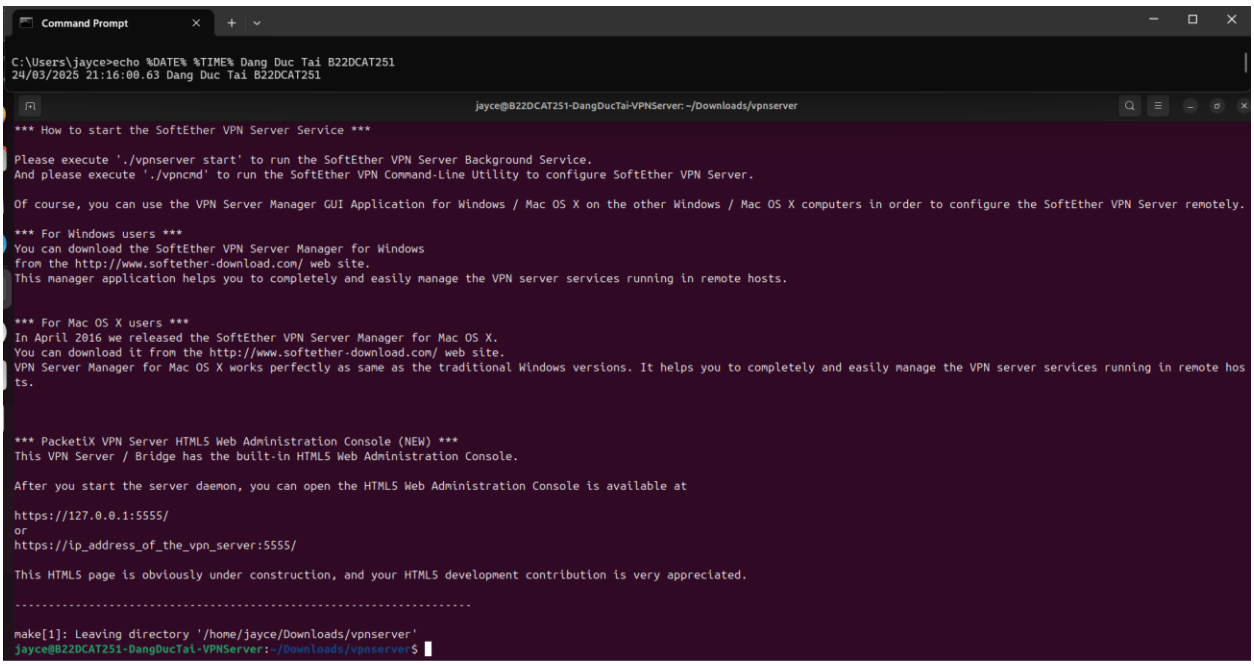
Hình 12 Cài đặt make

- Kiểm tra phiên bản gcc
  gcc -v
- Nếu chưa có gcc, cài đặt bằng câu lệnh
  sudo apt install gcc -y



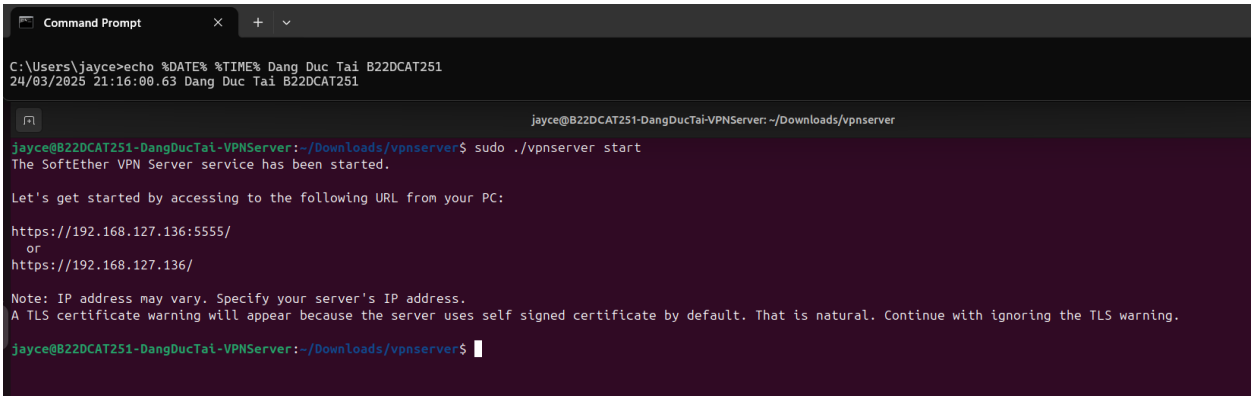
Hình 13 Kiểm tra phiên bản gcc

- Cài đặt thư viện OpenSSL và các thư viện hỗ trợ để biên dịch SoftEther VPN Server
  sudo apt install -y build-essential libssl-dev libreadline-dev zlib1g-dev -y
- Biên dịch make sau khi đã cài đặt môi trường
  make



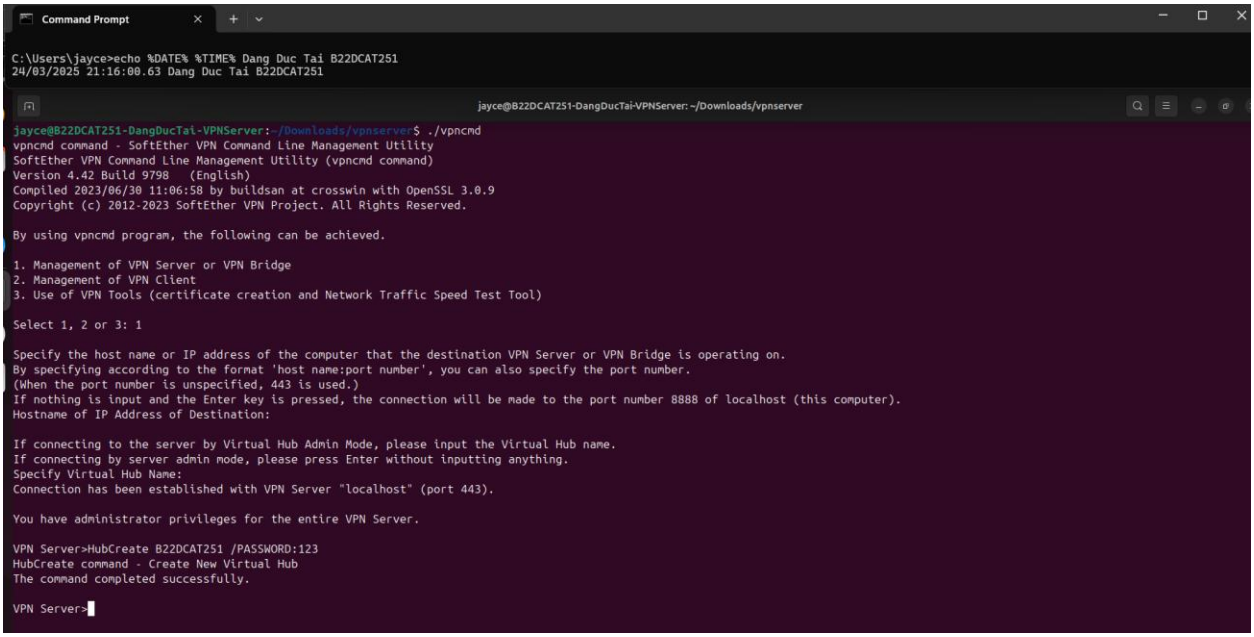
Hình 14 Biên dịch make

- Khởi động máy chủ vpn sau khi đã biên dịch môi trường
  sudo ./vpnserver start



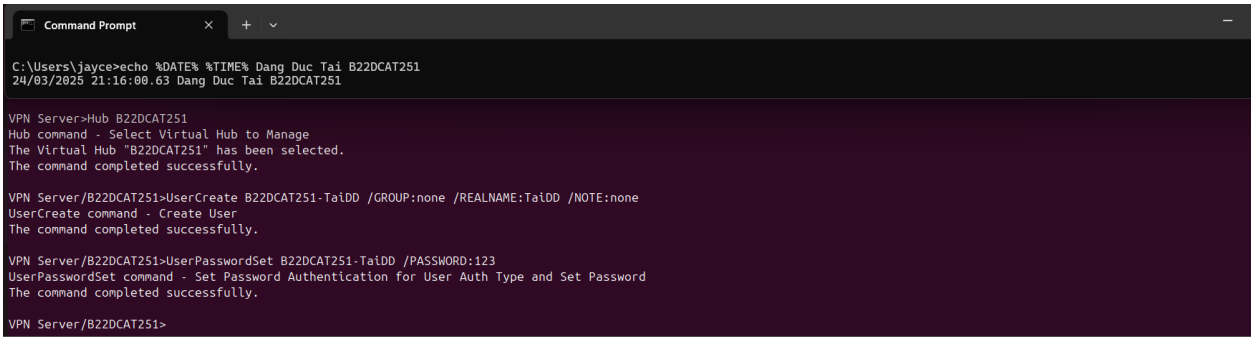
Hình 15 Khởi động máy chủ vpn

- Chạy tiện ích quản trị VPN Server
  ./vpncmd
- Chọn 1, gõ enter 2 lần để vào giao diện quản trị. Tạo Virtual Hub và tài khoản người dùng VPN trong giao diện quản trị
  HubCreate B22DCAT251 /PASSWORD:123



Hình 16 Tạo Virtual Hub mới

- Tạo 1 người dùng mới & đặt mật khẩu cho người dùng
  UserCreate B22DCAT251-TaiDD /Group:none /REALNAME:TaiDD /NOTE:none
  UserPasswordSet B22DCAT251-TaiDD /PASSWORD:123

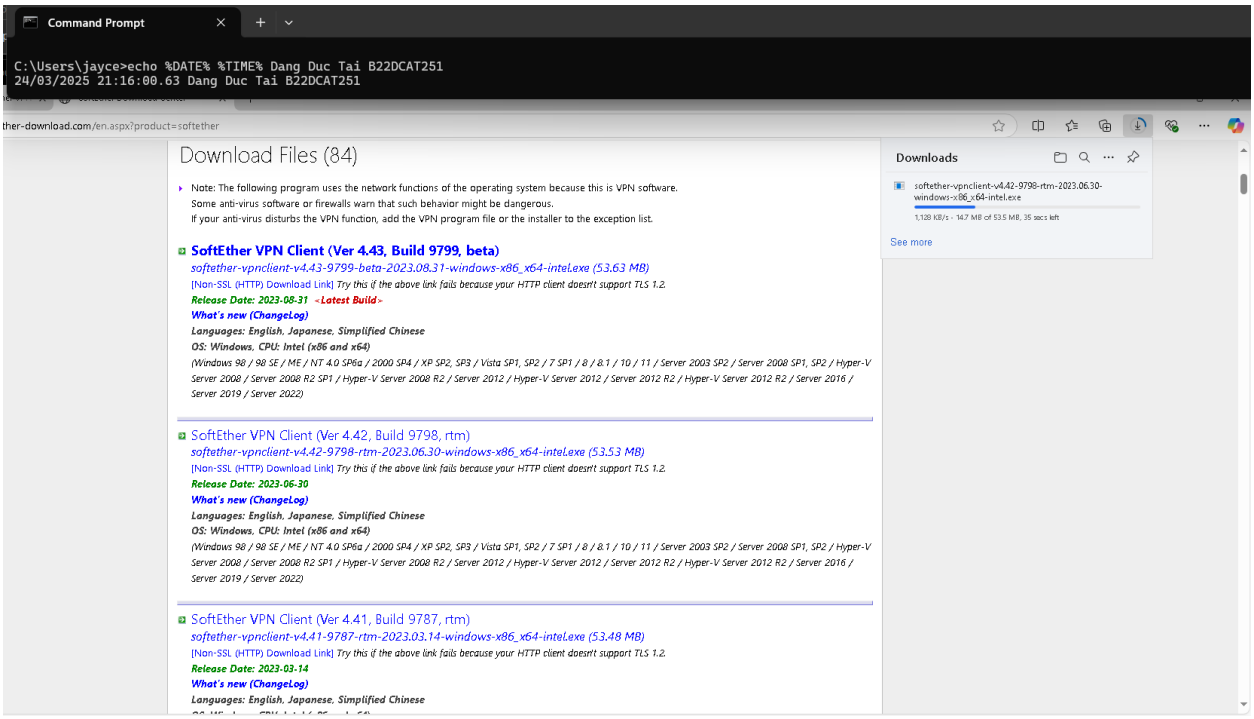


Hình 17 Tạo tài khoản người dùng VPN mới

- Sau khi tạo thành công, gõ exit để thoát khỏi tiện ích quản trị VPN Server

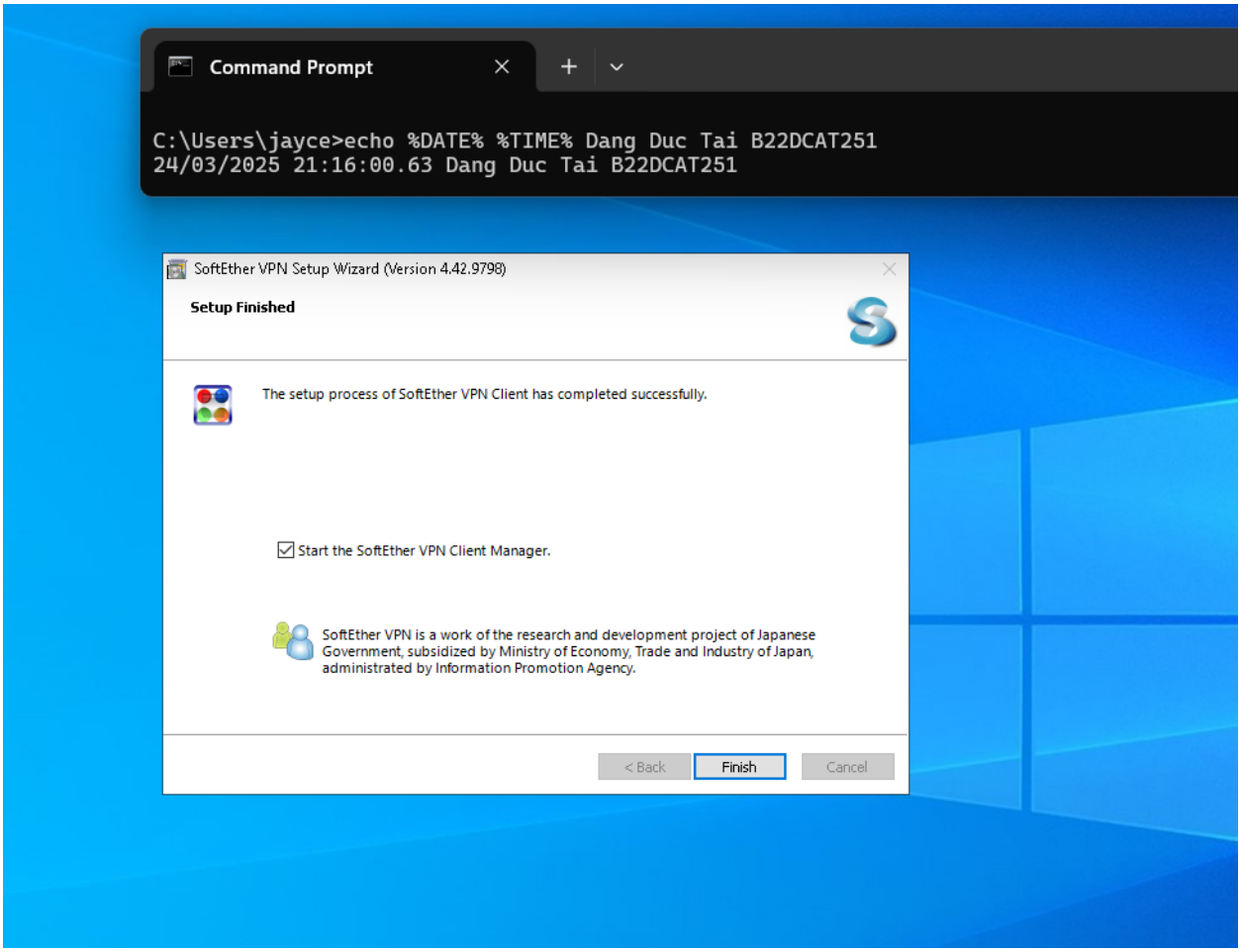
2.2.3 Cấu hình VPN Client

- Tải SoftEther VPN client cho Windows tại https://www.softether.org/5-download



Hình 18 Tải SoftEther VPN Client

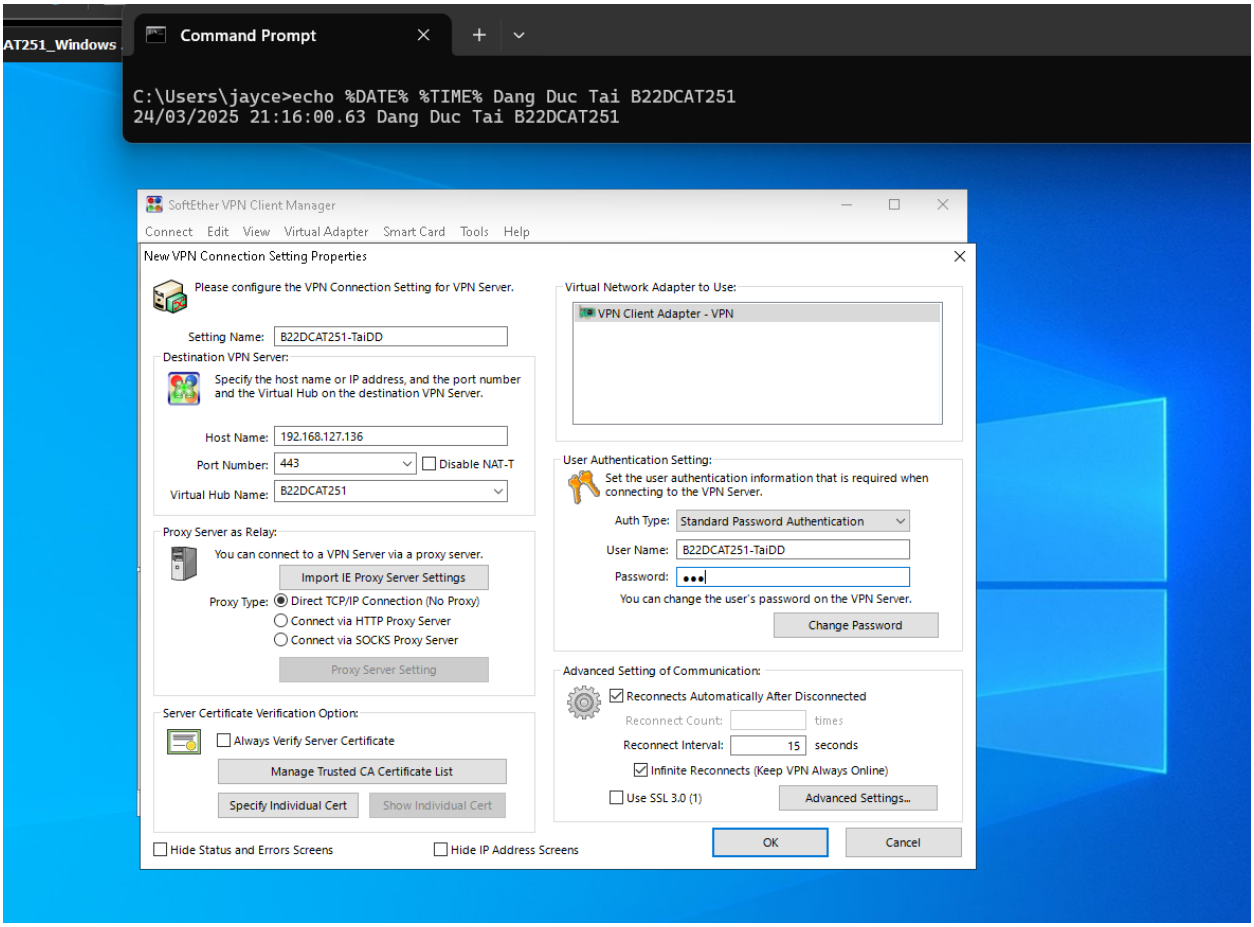
- Sau khi tải, tiến hành setup SoftEther VPN Client



Hình 19 Setup thành công SoftEther VPN Client

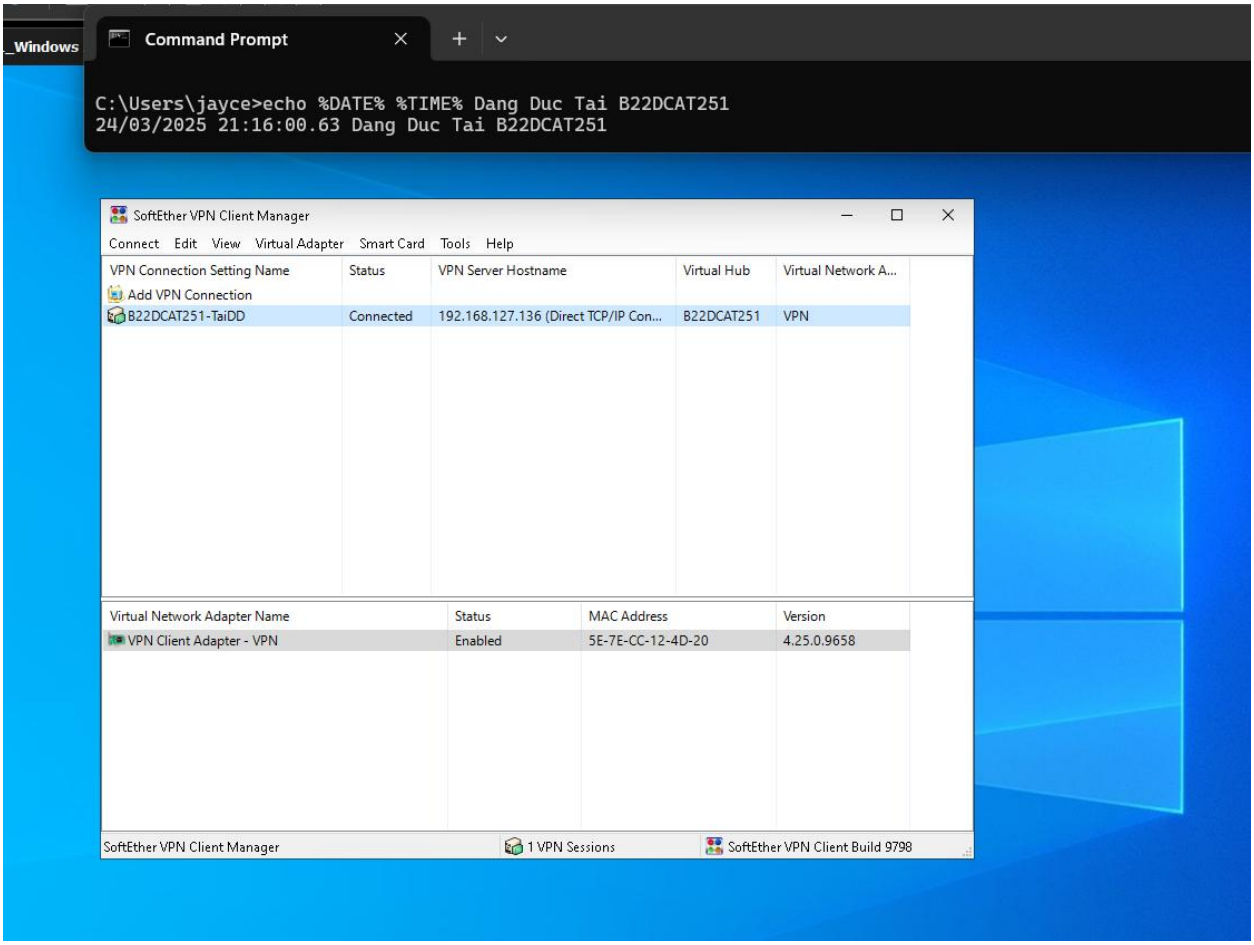
- Tạo kết nối tới VPN Server

- Từ giao diện SoftEther VPN Client Manager, tạo 1 kết nối mới (Add New Connection) với địa chỉ IP của máy chủ VPN (192.168.127.136) , tên Virtual Hub, tên và mật khẩu người dùng. Đặt tên kết nối là <Mã sinh viên>-<Họ tên>



Hình 20 Tạo kết nối tới VPN Server

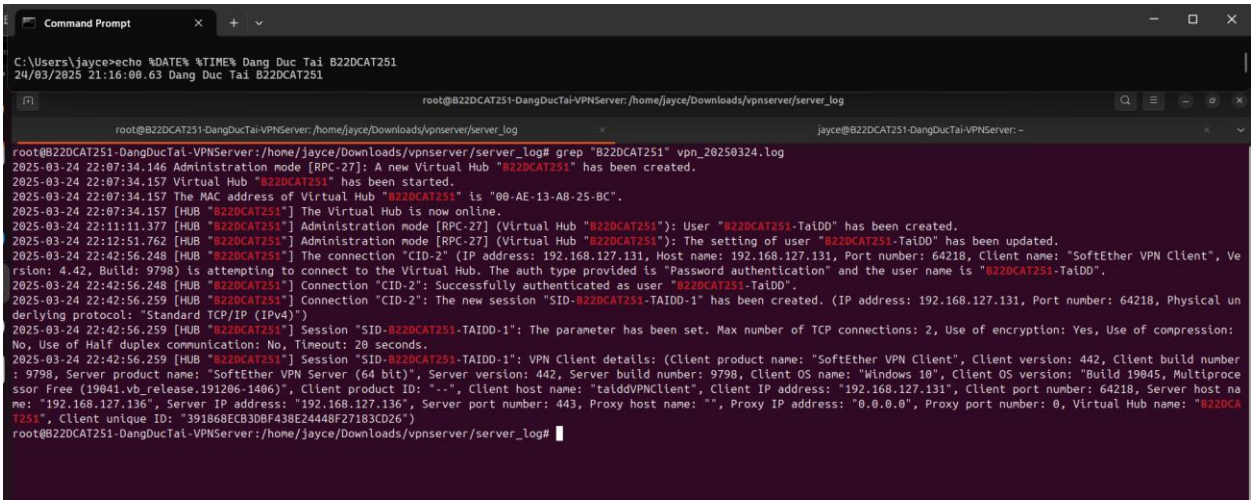
- Kết nối thành công, trạng thái *connected*



Hình 21 Kết nối thành công tới VPN Server

- Kiểm tra file log trên Server (Lưu ý, phải sử dụng quyền sudo/root cho tác vụ này)

- Chuyển tới thư mục chứa file log (server_log) trên VPN Server
  cd vpnserver/server_log
- Hiển thị các dòng log có liên quan
  *grep "B22DCAT251" *.log*



Hình 22 Xem file log trên VPN Server

TÀI LIỆU THAM KHẢO

[1] https://vncoder.vn/tin-tuc/cong-nghe/tong-quan-ve-vpn

[2] https://br.atsit.in/vi/?p=54681

[3] https://www.hocviendaotao.com/2013/03/giao-thuc-ipsec.html

[4] https://datatracker.ietf.org/doc/html/rfc8446

[5] https://www.softether.org/4-docs