**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**


**Môn học: Thực Tập Cơ Sở**

**Báo Cáo Bài Thực Hành 7**

**Cài Đặt Cấu Hình VPN Server**

**Họ và tên:** Trần Thị Thu Phương

**Mã sinh viên:** B21DCAT151

**Nhóm môn học:** 04

**Giảng viên:** Đinh Trường Duy

Hà Nội, 1/2024

# Mục lục

# Danh mục hình ảnh

# 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

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

**a. Tìm hiểu khái quát về VPN**

VPN (Virtual Private Network) là một công nghệ mạng cho phép người dùng tạo một kết nối an toàn qua mạng Internet công cộng. VPN tạo ra một "đường hầm" mã hóa giữa thiết bị của người dùng và một máy chủ VPN, giúp đảm bảo rằng lưu lượng truy cập không thể bị đọc hoặc giả mạo bởi bên thứ ba.

**Cách VPN hoạt động**

- **Khi bạn kết nối đến VPN:**
  + Thiết bị của bạn sẽ giao tiếp với máy chủ VPN.
  + VPN thiết lập một kết nối mã hóa (đôi khi được gọi là đường hầm VPN).
  + Tất cả lưu lượng truy cập của bạn được định tuyến qua đường hầm này.
- **Mã hóa:**
  + Dữ liệu được mã hóa trước khi rời khỏi thiết bị của bạn, đảm bảo rằng không ai có thể theo dõi hoạt động trực tuyến của bạn hoặc đánh cắp thông tin cá nhân.
- **Ẩn danh:**
  + VPN ẩn địa chỉ IP thực của bạn và thay thế nó bằng địa chỉ IP của máy chủ VPN, giúp bạn duyệt web một cách ẩn danh.

**Các tính năng quan trọng của VPN**

- **Mã hóa đầu cuối:** Dữ liệu được mã hóa từ thiết bị của bạn đến máy chủ VPN, không thể bị giải mã cho đến khi đến đích.
- **Chính sách không ghi nhận log:** Một số nhà cung cấp VPN cam kết không lưu trữ bất kỳ thông tin nào về hoạt động trực tuyến của bạn.
- **Kill Switch:** Tính năng tự động ngắt kết nối Internet nếu VPN bị ngắt, để ngăn chặn lộ lọt dữ liệu.
- **Split Tunneling:** Cho phép bạn chọn ứng dụng nào đi qua VPN và ứng dụng nào sử dụng kết nối Internet trực tiếp.

**b. Các mô hình VPN**

Có nhiều loại mô hình VPN (Virtual Private Network) được sử dụng cho các mục đích khác nhau. Dưới đây là một số mô hình phổ biến:

- **Remote Access VPN (RAVPN):**
  + Mô hình này cho phép người dùng từ xa kết nối với mạng của tổ chức từ bất kỳ đâu thông qua internet.
  + Thường sử dụng phần mềm VPN trên thiết bị của người dùng để thiết lập kết nối bảo mật với cổng vào VPN trên mạng của tổ chức.
- **Site-to-Site VPN (S2S VPN):**
  + Mô hình này cho phép kết nối an toàn giữa hai hoặc nhiều mạng văn phòng từ xa.
  + Các thiết bị mạng như router hoặc firewall được cấu hình để thiết lập kết nối VPN với mạng đích.
- **Intranet-based VPN:**
  + Các tổ chức lớn thường xây dựng mạng VPN riêng nội bộ, cho phép các phòng ban hoặc chi nhánh kết nối với nhau một cách bảo mật qua internet.
- **Extranet-based VPN:**
  + Mô hình này mở rộng cơ sở của Intranet VPN bằng cách cho phép các bên thứ ba như đối tác hoặc nhà cung cấp kết nối với hệ thống mạng nội bộ của một tổ chức.
- **Client-to-Site VPN:**
  + Tương tự như Remote Access VPN, nhưng khác biệt ở chỗ mô hình này thường được triển khai bằng cách sử dụng phần mềm VPN trên thiết bị cá nhân của người dùng để kết nối với mạng do tổ chức cung cấp.
- **Full-Mesh VPN:**
  + Mô hình này kết nối mọi điểm mạng với tất cả các điểm mạng khác nhau trong một mạng VPN. Điều này có thể dẫn đến độ phức tạp cao khi số lượng điểm mạng tăng lên.
- **Hybrid VPN:**
  + Kết hợp giữa các mô hình VPN khác nhau để đáp ứng nhu cầu cụ thể của tổ chức, ví dụ như kết hợp Site-to-Site VPN với Remote Access VPN để cung cấp cả kết nối từ xa và kết nối giữa các văn phòng.

### c. Ứng dụng của VPN

- **Bảo mật:**
  + Bảo vệ dữ liệu khi sử dụng mạng Wi-Fi công cộng.
  + Bảo vệ thông tin cá nhân khỏi bị đánh cắp.
- **Quyền riêng tư:**
  + Ngăn chặn ISP (Nhà cung cấp dịch vụ Internet) và các bên thứ ba theo dõi hoạt động trực tuyến của bạn.
  + Tránh bị giám sát và thu thập dữ liệu.
- **Truy cập nội dung:**
  + Vượt qua các hạn chế địa lý và kiểm duyệt để truy cập nội dung và dịch vụ trực tuyến từ bất kỳ nơi nào trên thế giới.

  + VPN cho phép bạn truy cập vào các trang web, dịch vụ hoặc nội dung bị cấm hoặc hạn chế trong quốc gia hoặc mạng của bạn bằng cách thay đổi địa chỉ IP của bạn
- **An toàn khi làm việc từ xa:**
  + Truy cập an toàn vào mạng nội bộ của công ty từ xa.

Một lưu ý khi sử dụng VPN:
- **VPN miễn phí:** Nhiều VPN miễn phí có thể không an toàn và thực sự thu thập dữ liệu của bạn để bán cho bên thứ ba.
- **Luật pháp và quy định:** Một số quốc gia có luật lệ hạn chế hoặc cấm sử dụng VPN.
- **Tương thích:** Đảm bảo VPN tương thích với tất cả thiết bị và hệ điều hành bạn sử dụng.

### 2.1.2. Tìm hiểu về các giao thức tạo đường hầm cho VPN: PPTP, L2TP, L2P, MPLS

**a. PPTP (Point-to-Point Tunneling Protocol):**
- PPTP là một giao thức VPN (Virtual Private Network) được sử dụng để tạo ra kết nối an toàn giữa các máy tính qua Internet.
- Nó hoạt động ở tầng 2 và 3 của mô hình OSI.
- PPTP đã được phát triển sớm (Nó được tạo ra bởi Microsoft và phát hành cùng với Windows 95) và dễ triển khai, nhưng hiện nay ít được sử dụng hơn do các vấn đề liên quan đến bảo mật.
- Bạn không cần phải có bất kỳ chuyên môn kỹ thuật nào để sử dụng PPTP. Tất cả những gì bạn cần là tên người dùng và mật khẩu với địa chỉ máy chủ để thực hiện kết nối. PPTP cũng là giao thức VPN Tunneling nhanh nhất vì mức độ mã hóa của nó quá thấp.

**b. L2TP (Layer 2 Tunneling Protocol):**
- L2TP là một giao thức VPN được sử dụng để tạo ra kết nối an toàn giữa các mạng hoặc máy tính qua Internet.
- L2TP chậm hơn PPTP
- Nó hoạt động ở tầng 2 của mô hình OSI.
- L2TP thường được sử dụng cùng với giao thức bảo mật khác như IPsec để cung cấp một môi trường VPN an toàn và tin cậy.
- L2TP/IPSec cung cấp cho người dùng công nghệ mã hóa tiên tiến nhất, AES-256.
- L2TP là một giao thức phổ biến vì mức độ bảo mật cao nhưng nó không thể vượt qua một số tường lửa hạn chế vì nó sử dụng các cổng cố định để kết nối.

**c. L2F (Layer 2 Forwarding):**

- L2F cũng là một giao thức VPN, được Cisco Systems phát triển.
- Nó hoạt động ở tầng 2 của mô hình OSI.
- L2F đã trở nên ít phổ biến hơn do sự phát triển của các giao thức VPN khác như PPTP và L2TP.

**d. MPLS (Multiprotocol Label Switching):**

- MPLS (Multiprotocol Label Switching) là một công nghệ mạng được sử dụng để chuyển tiếp dữ liệu trong các mạng điều chuyển gói (packet-switched networks). MPLS kết hợp sự linh hoạt của giao thức mạng cùng với khả năng chuyển tiếp nhanh chóng của các mạng điều chuyển gói, nhưng vẫn duy trì được tính toàn vẹn và chất lượng dịch vụ.
- Hoạt động ở tầng 2 và tầng 3 của mô hình OSI
- Trong MPLS, các gói dữ liệu được gán nhãn (label) và chuyển tiếp dựa trên nhãn này thay vì dựa trên các địa chỉ IP đích. Việc sử dụng nhãn giúp giảm bớt thời gian xử lý và chuyển tiếp gói dữ liệu, đồng thời cải thiện hiệu suất và linh hoạt của mạng.
- MPLS được sử dụng rộng rãi trong các mạng lớn, bao gồm các mạng của các nhà cung cấp dịch vụ Internet (ISP) và các doanh nghiệp có yêu cầu cao về hiệu suất mạng. Nó cũng được sử dụng trong các dịch vụ VPN (Virtual Private Network) để cung cấp kết nối mạng an toàn và chất lượng. MPLS cũng là một trong những công nghệ cơ sở cho các dịch vụ mạng cấp cao như MPLS-TE (Traffic Engineering) và MPLS-VPN.

Hiện nay, trong số các giao thức bạn đã liệt kê, MPLS (Multiprotocol Label Switching) đang được sử dụng rộng rãi nhất. MPLS được áp dụng trong nhiều mạng lớn, bao gồm các nhà cung cấp dịch vụ Internet (ISP) và doanh nghiệp, để cung cấp chất lượng dịch vụ (QoS), chuyển tiếp dữ liệu hiệu quả, và hỗ trợ các dịch vụ như MPLS-VPN (MPLS Virtual Private Network) và MPLS-TE (MPLS Traffic Engineering). MPLS giúp cải thiện hiệu suất mạng và đảm bảo một số tính năng như đường ưu tiên cho các ứng dụng nhất định.

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

**a. IPSec**

IPSec (Internet Protocol Security) là một bộ công nghệ bảo mật được sử dụng để bảo vệ việc truyền dữ liệu qua mạng Internet. IPSec được sử dụng để đảm bảo tính toàn vẹn, sự tin cậy và bảo mật của thông tin truyền qua mạng, bằng cách mã hóa và xác thực dữ liệu. Các giao thức trong IPSec cung cấp cơ chế để thiết lập các kênh truyền an toàn giữa các thiết bị mạng, cho phép truyền dữ liệu một cách bảo mật thông qua Internet hoặc các mạng công cộng khác. IPSec thường được sử dụng cho các mạng VPN (Virtual Private Network) để tạo ra một mạng riêng ảo an toàn trên mạng Internet công cộng.

**b. SSL**

SSL (Secure Sockets Layer) là một tiêu chuẩn bảo mật mạng được sử dụng để bảo vệ thông tin truyền qua Internet. SSL được thiết kế để đảm bảo tính bí mật, toàn vẹn và xác thực của dữ liệu truyền qua mạng, bằng cách sử dụng mã hóa và các giao thức bảo mật.

SSL hoạt động bằng cách tạo ra một kênh kết nối bảo mật giữa máy khách (client) và máy chủ (server). Khi một trình duyệt web kết nối đến một trang web được bảo vệ bằng SSL, máy chủ sẽ gửi một chứng chỉ SSL cho trình duyệt web để xác nhận danh tính của mình. Sau đó, máy khách và máy chủ sẽ thỏa thuận một phiên mã hóa để mã hóa dữ liệu được truyền giữa chúng, đảm bảo rằng thông tin không thể bị đánh cắp hoặc thay đổi khi truyền qua mạng.

SSL thường được sử dụng cho các giao thức truyền thông như HTTPS (HTTP Secure), POP3S/IMAPS (POP3/IMAP Secure) để bảo vệ việc truyền thông qua Internet, đặc biệt là trong việc gửi và nhận dữ liệu nhạy cảm như thông tin cá nhân, thông tin tài khoản ngân hàng, mật khẩu, và các dữ liệu quan trọng khác.

**c. TLS**

TLS (Transport Layer Security) là một tiêu chuẩn bảo mật mạng được sử dụng để bảo vệ thông tin truyền qua Internet. TLS là phiên bản nâng cấp của SSL (Secure Sockets Layer) và được sử dụng rộng rãi trong các ứng dụng truyền thông mạng như trình duyệt web, email, truyền tệp và các dịch vụ trực tuyến khác.

Tương tự như SSL, TLS cũng hoạt động bằng cách tạo ra một kênh kết nối bảo mật giữa máy khách (client) và máy chủ (server), bằng cách sử dụng các phương thức mã hóa và giao thức bảo mật. Khi một trình duyệt web kết nối đến một trang web được bảo vệ bằng TLS, máy chủ sẽ gửi một chứng chỉ TLS cho trình duyệt web để xác nhận danh tính của mình và sau đó thiết lập một phiên mã hóa an toàn để bảo vệ dữ liệu truyền qua kênh kết nối.

TLS thường được sử dụng cho các giao thức truyền thông như HTTPS (HTTP Secure), SMTPS/IMAPS (SMTP/IMAP Secure), FTPS (FTP Secure) để bảo vệ việc truyền thông qua Internet. Nó cung cấp một cơ chế an toàn và tin cậy để truyền dữ liệu trực tuyến một cách bảo mật và không thể bị đánh cắp hoặc sửa đổi khi truyền qua mạng.

### 2.1.4. Tìm hiểu về SoftEther VPNz

SoftEther VPN là một bộ phần mềm mã nguồn mở và miễn phí được phát triển bởi Daiyuu Nobori từ Đại học Tsukuba ở Nhật Bản. Nó cung cấp một giải pháp VPN đa năng và linh hoạt, hỗ trợ nhiều giao thức VPN như SSL VPN, L2TP/IPsec, OpenVPN,

và các giao thức VPN tùy chỉnh khác. Dưới đây là một số điểm nổi bật về SoftEther VPN:

- **Đa nền tảng:** SoftEther VPN có thể chạy trên nhiều hệ điều hành khác nhau, bao gồm Windows, Linux, macOS, FreeBSD và Solaris.

- **Tích hợp các giao thức VPN phổ biến:** Nó hỗ trợ nhiều giao thức VPN, cho phép người dùng lựa chọn giao thức phù hợp với nhu cầu cụ thể của họ.

- **Tính linh hoạt và mở rộng:** SoftEther VPN có khả năng mở rộng và tùy chỉnh mạnh mẽ, cho phép bạn tạo và quản lý các mạng VPN phức tạp.

- **Hiệu suất cao và ổn định:** Bộ mã nguồn mở giúp cộng đồng phát triển và kiểm tra SoftEther VPN liên tục, đảm bảo hiệu suất và ổn định cao.

- **Dễ sử dụng:** SoftEther VPN cung cấp giao diện người dùng đồ họa dễ sử dụng, giúp người dùng cài đặt và quản lý mạng VPN một cách dễ dàng.

- **Hỗ trợ cho Remote Access và Site-to-Site VPN:** SoftEther VPN có thể được triển khai để cung cấp kết nối VPN từ xa (Remote Access VPN) hoặc kết nối giữa các văn phòng (Site-to-Site VPN).

- **Bảo mật cao:** SoftEther VPN sử dụng các phương pháp mã hóa mạnh mẽ để bảo vệ dữ liệu khi truyền qua mạng.

Tóm lại, SoftEther VPN là một giải pháp VPN mạnh mẽ, linh hoạt và dễ sử dụng, phù hợp cho cả cá nhân và tổ chức muốn thiết lập một mạng VPN an toàn và hiệu quả.

## 2.2. Nội dung thực hành

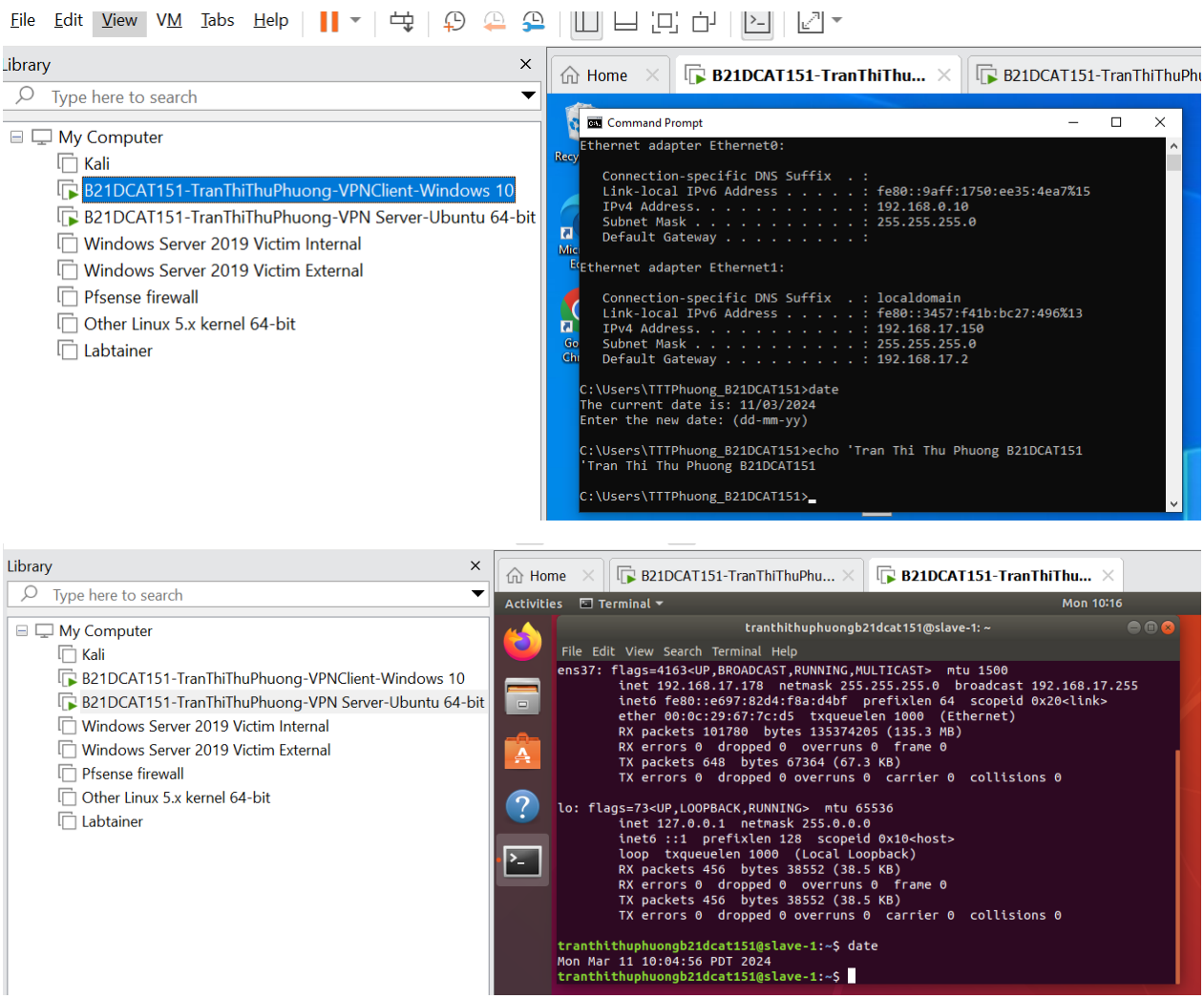
### 2.2.1. Chuẩn bị môi trường, công cụ

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

### 2.2.2. Các bước thực hiện

- **Bước 1:** Chuẩn bị các máy tính như mô tả trong mục 2.2.1
+ Máy Windows được đổi tên thành B21DCAT151-Trần Thị Thu Phương-VPNClient

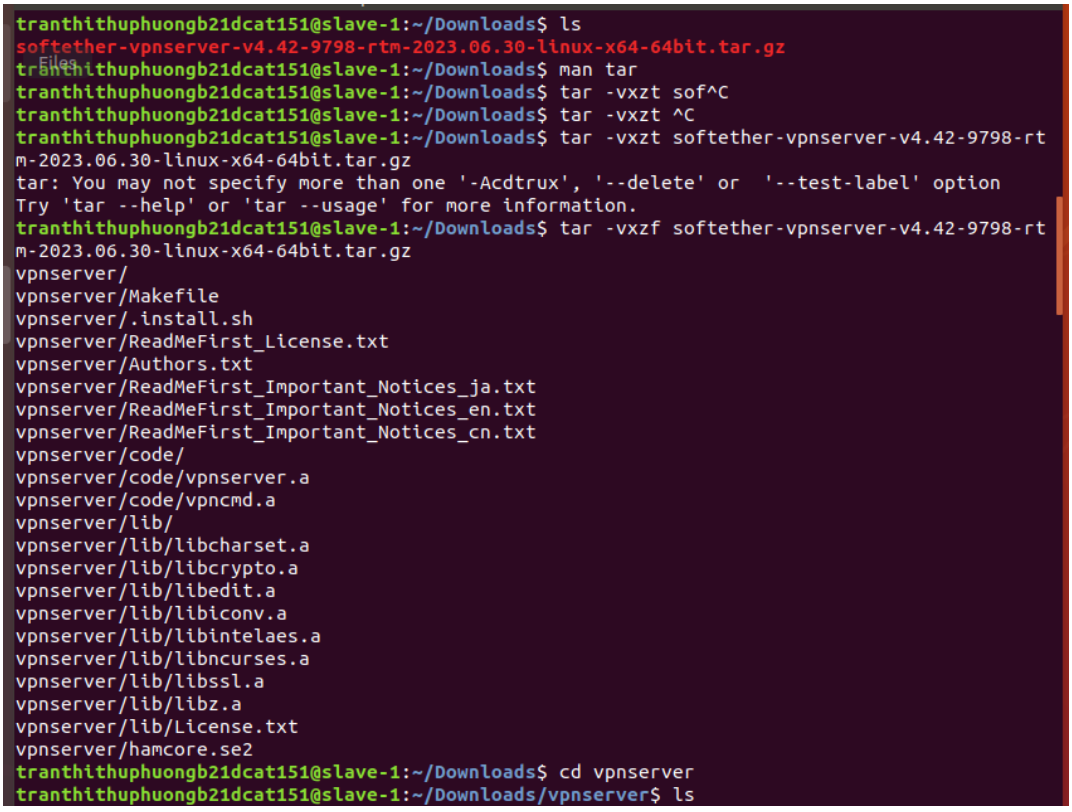
+ Máy cài VPN server thành B21DCAT151-Trần Thị Thu Phương-VPNServer. Các máy có địa chỉ IP và kết nối mạng LAN.




*Đổi tên máy theo yêu cầu*

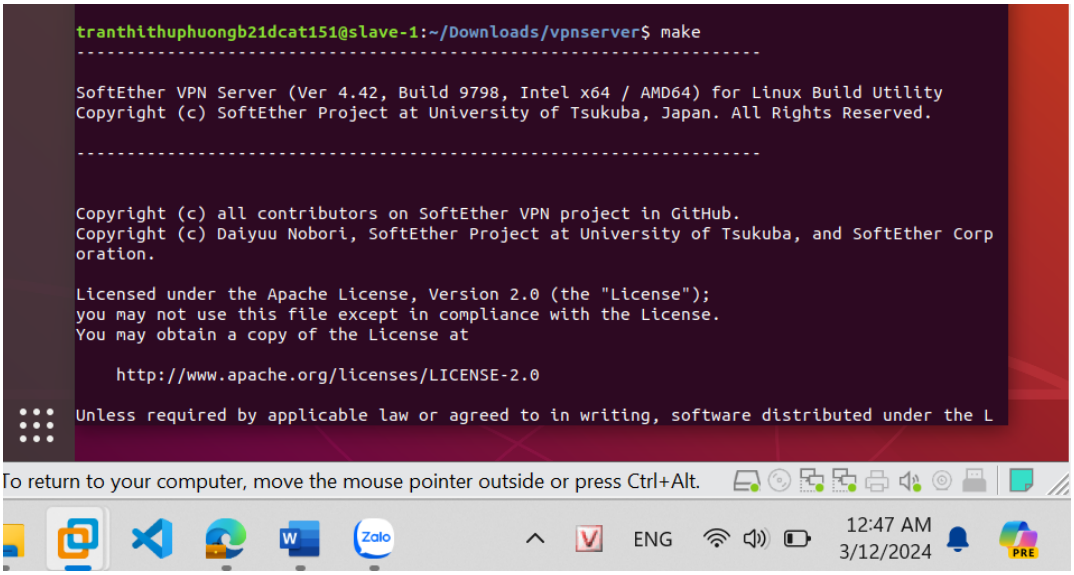
– **Bước 2:** Tải SoftEther VPN server tại https://www.softether.org/5-download. Cài đặt và cấu hình VPN server theo hướng dẫn sau

+ Giải nén file cài đặt bằng lệnh tar -vxzf <tên file vpn server> và chuyển vào thư mục VPN server: cd vpnserver



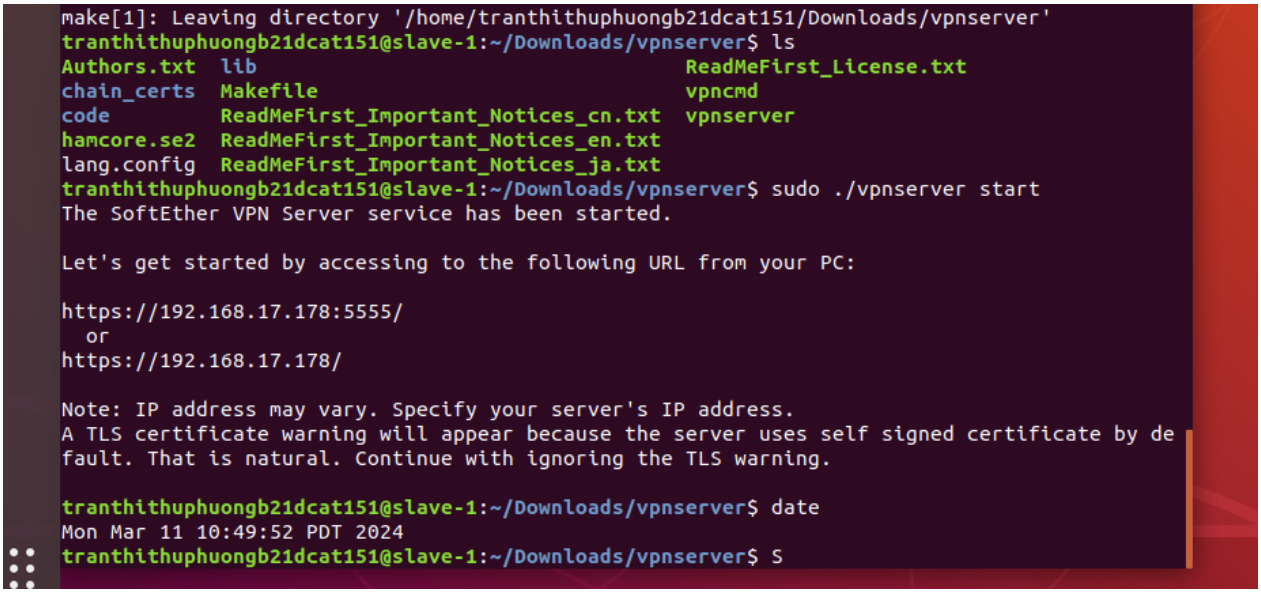

*Giải nén file cài đặt vnpserver*

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



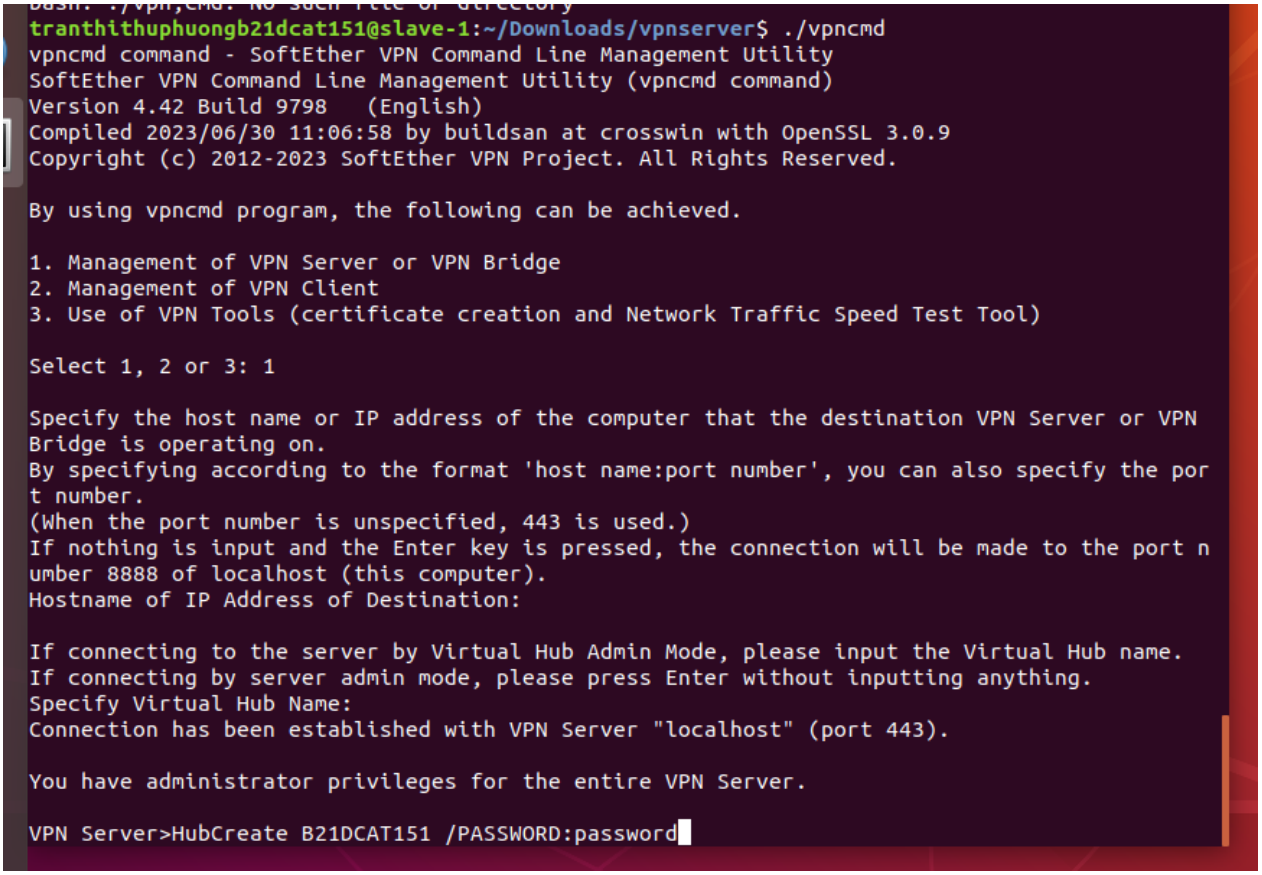

*Biên dịch và cài đặt*

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

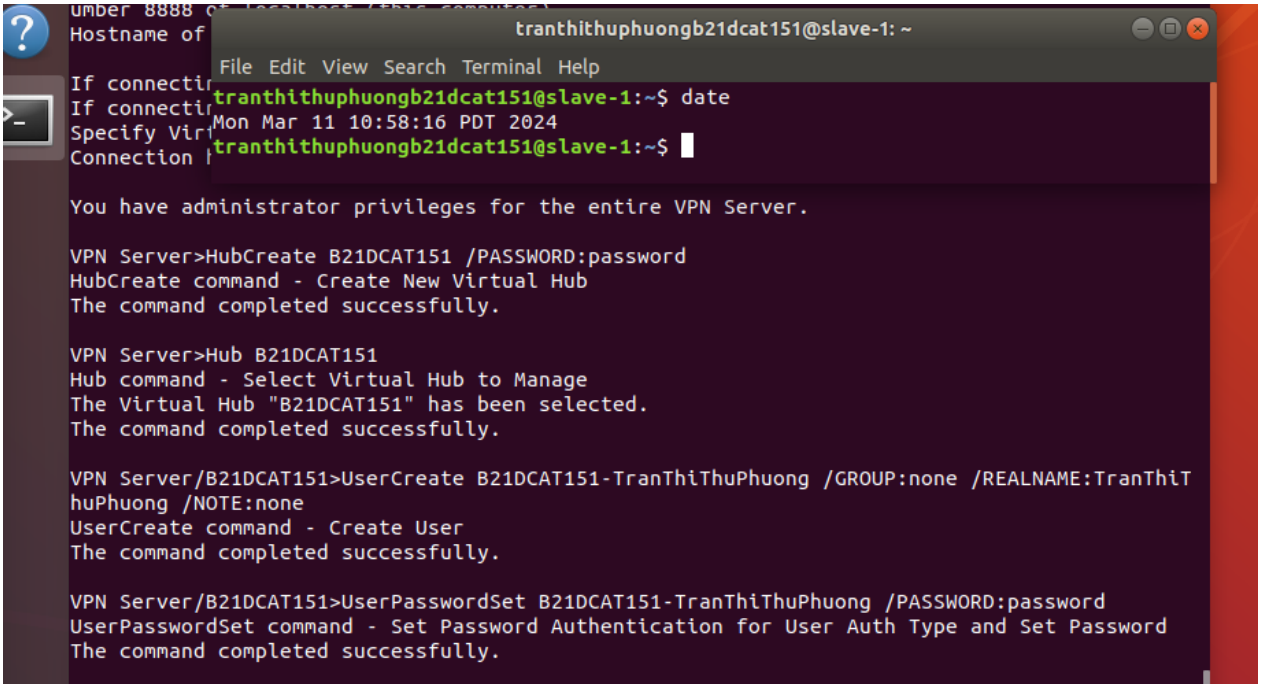



*Khởi động máy chủ VPN*

+ 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:
  - Tạo 1 Virtual Hub mới: HubCreate B21DCAT151 /PASSWORD:password
  - Chọn Virtual Hub đã tạo: Hub B21DCAT151
  - Tạo 1 người dùng VPN mới: UserCreate B21DCAT151-TranThiThuPhuong /GROUP:none /REALNAME:TranThiThuPhuong /NOTE:none
  - Đặt mật khẩu cho người dùng: UserPasswordSet B21DCAT151 /PASSWORD:password
  - Gõ exit để thoát khỏi tiện ích quản trị VPN Server

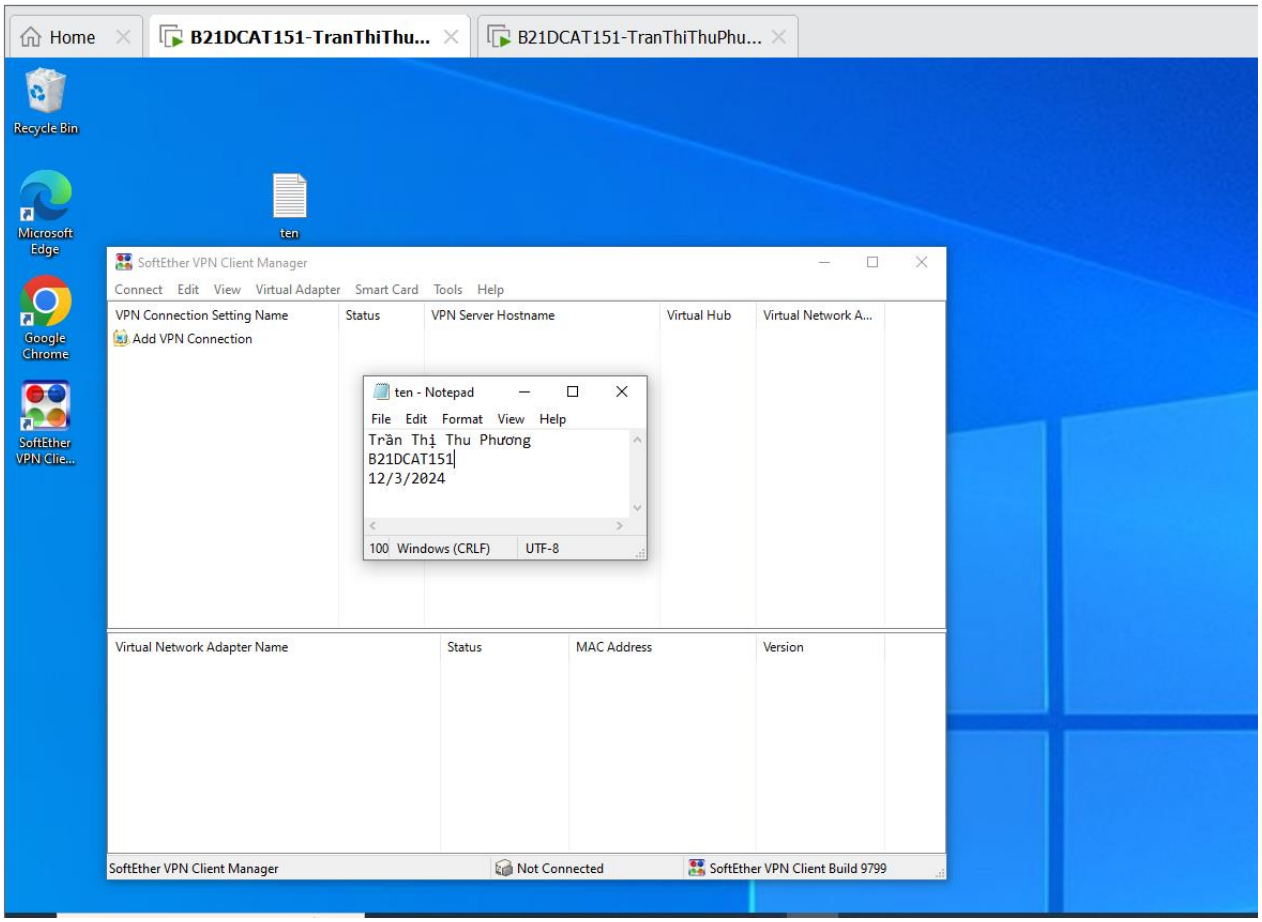



*Chạy tiện ích quản trị VPN Server rồi vào giao diện quản trị*




*Tạo Vitual Hub và tạo tài khoản người dùng VPN trong giao diện quản trị*

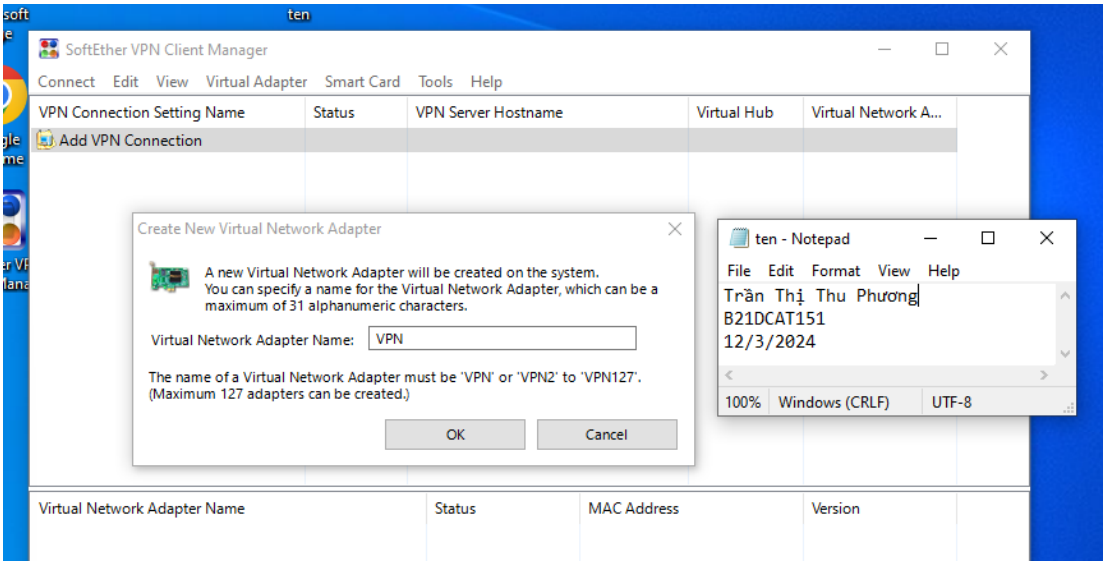
– **Bước 3:** Tải SoftEther VPN client cho Windows tại https://www.softether.org/5-download. Cài đặt VPN client.



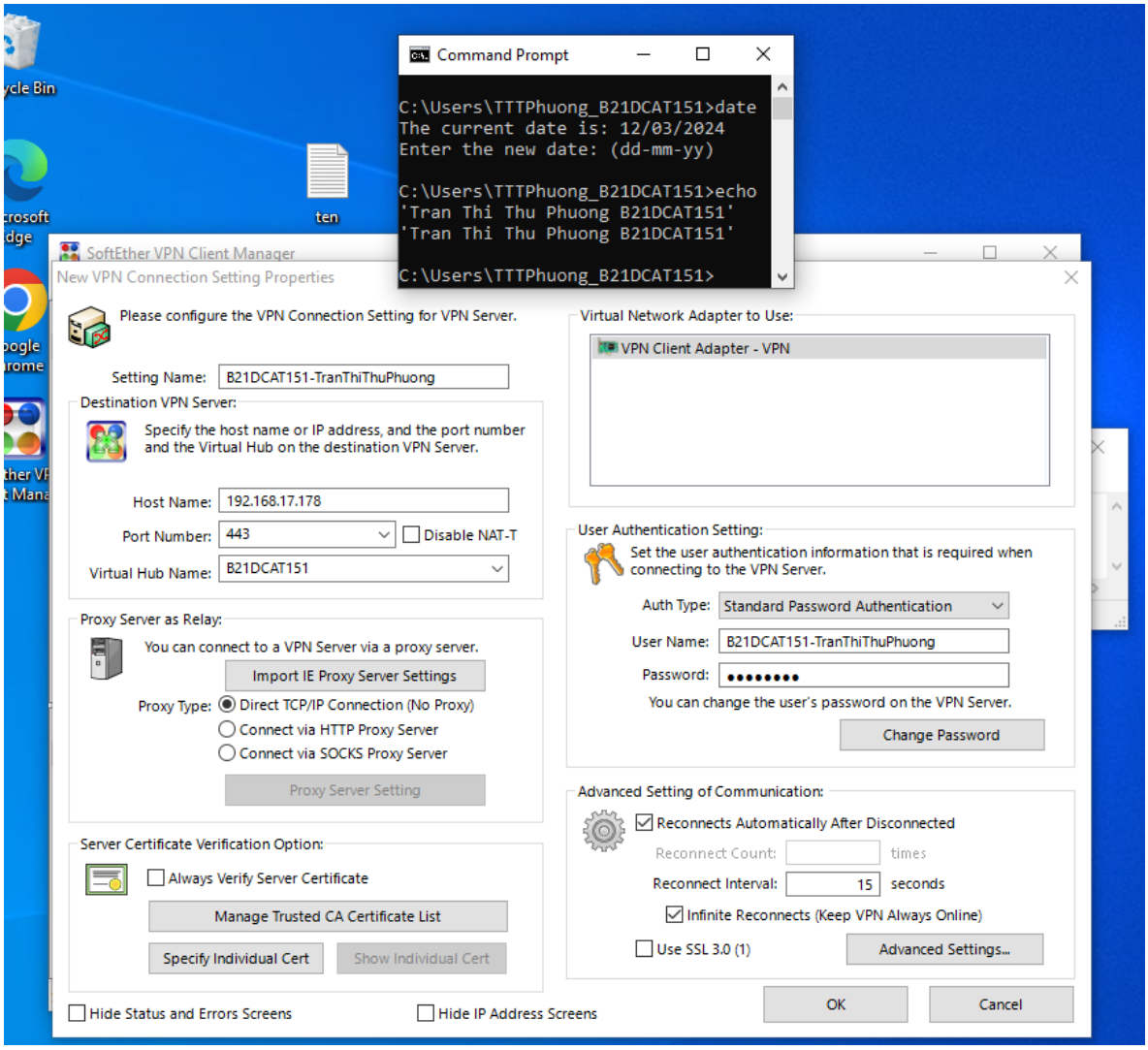

*Giao diện SoftEther VPN Client Manager*

– **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. Đặt tên kết nối là B21DCAT151-TranThiThuPhuong

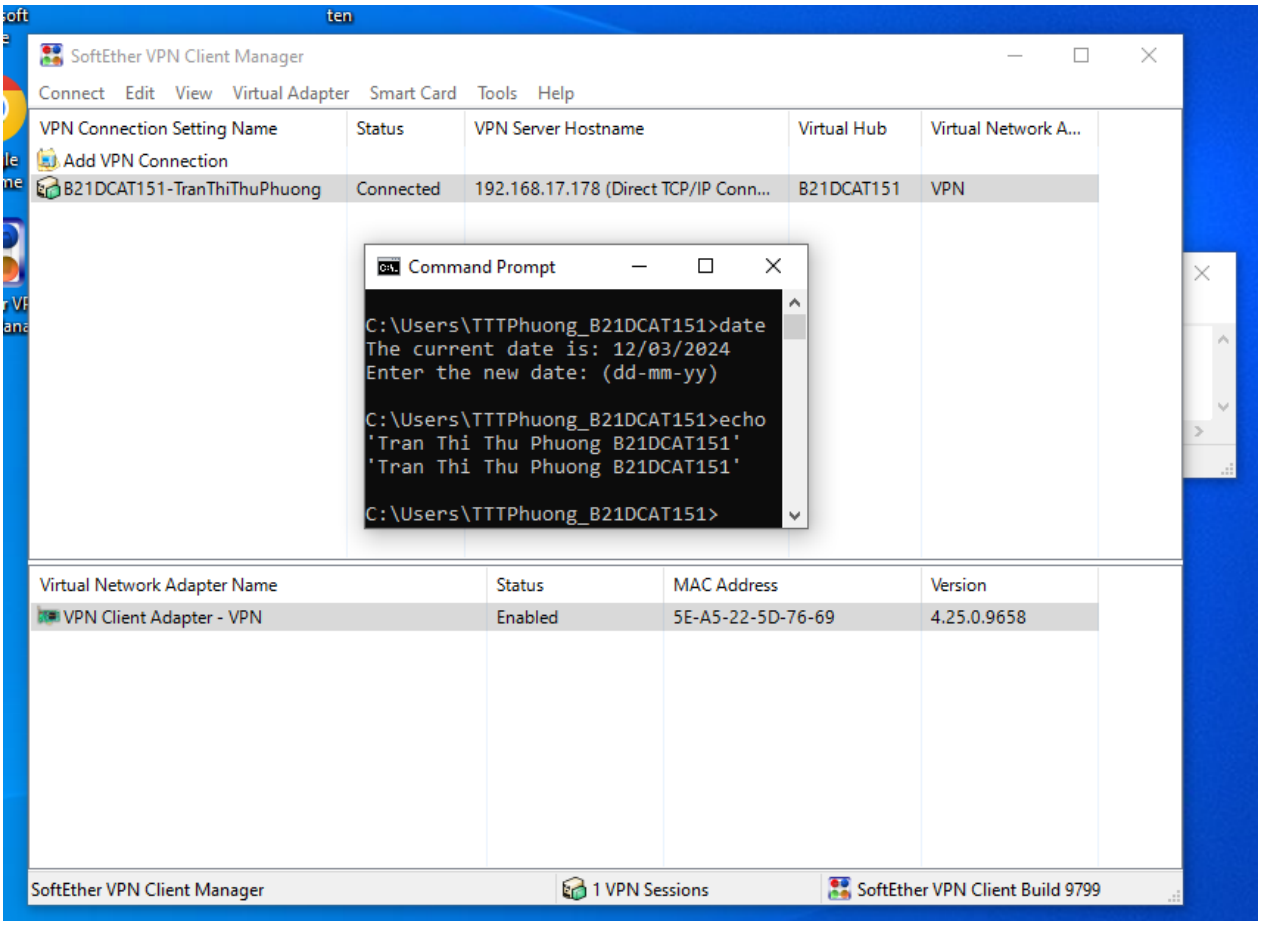



*Thêm 1 kết nối VPN*




*Cấu hình các thuộc tính của kết nối VPN*

+ Thử kết nối: Nếu thành công sẽ báo connected.

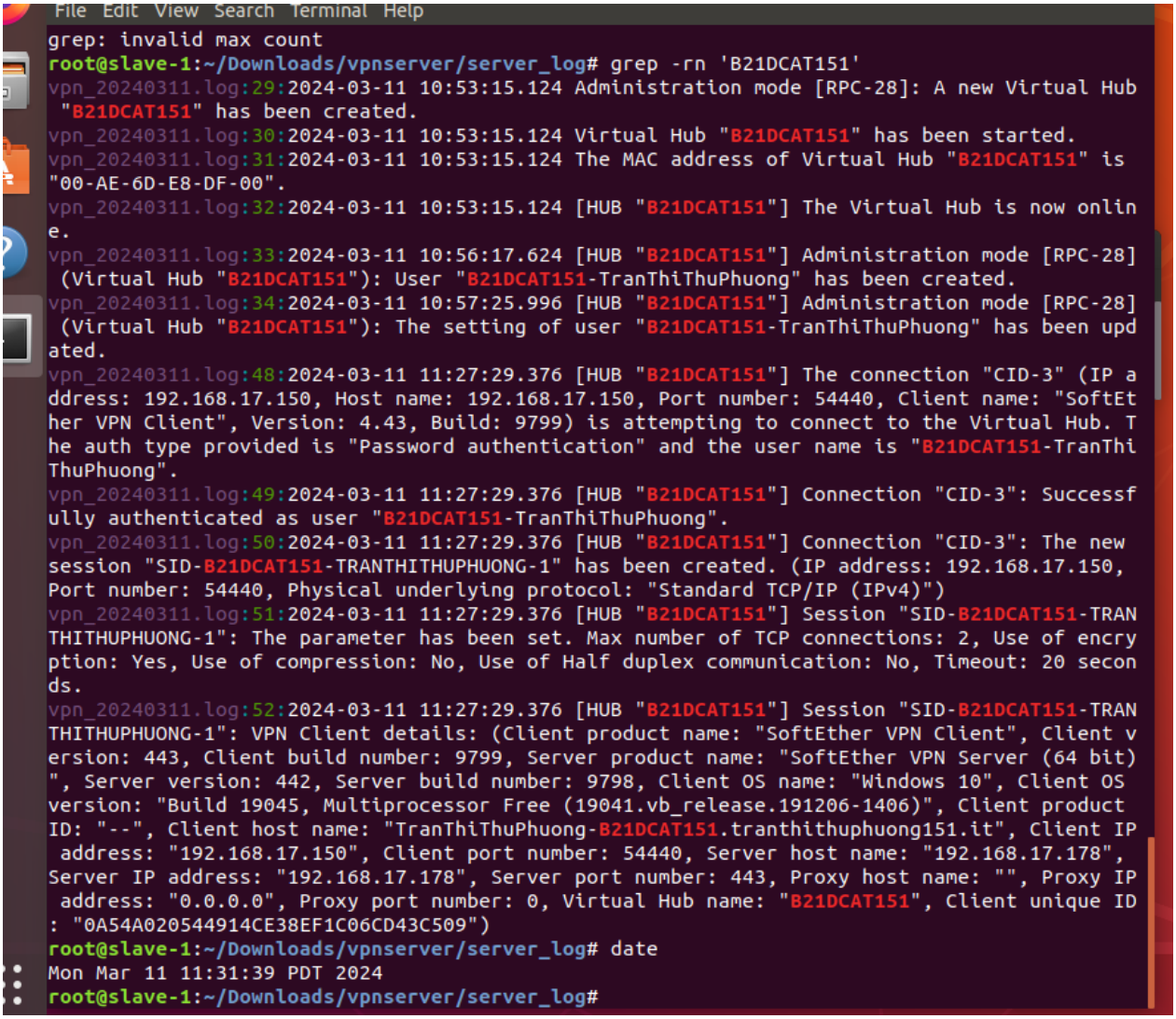



*Kết nối thành công VPN Server từ máy Client*

+ 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:

sudo grep B21DCAT151 vpnserver/server_log/*.log

⇨ Hiển thị các dòng log có liên quan đến B21DCAT151




*Kiểm tra kết nối VPN bằng file log của vpnserver*

## 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

## 4. 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