

**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:

B22DCAT034 Trương Quốc Bảo

Giảng viên hướng dẫn: TS. Đinh Trường Duy

**HỌC KỲ 2 NĂM HỌC 2024-2025**

# MỤC LỤC

MỤC LỤC.....	2
DANH MỤC CÁC HÌNH VẼ.....	3
DANH MỤC CÁC TỪ VIẾT TẮT.....	4
<b>CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH.....</b>	<b>5</b>
1.1 Mục đích.....	5
1.2 Tìm hiểu lý thuyết .....	5
1.2.1 VPN – Mạng riêng ảo.....	5
1.2.2 Các giao thức tạo đường hầm cho VPN .....	7
1.2.3 Các giao thức bảo mật cho VPN .....	8
1.2.4 SoftEther VPN.....	10
<b>CHƯƠNG 2. NỘI DUNG THỰC HÀNH .....</b>	<b>11</b>
2.1 Chuẩn bị môi trường .....	11
2.2 Các bước thực hiện.....	11
2.2.1 Chuẩn bị máy tính như mô tả .....	11
2.2.2 Tải và cài đặt SoftEther VPN server .....	12
2.2.3 Tải SoftEther VPN Client .....	17
2.2.4 Tạo và kiểm tra kết nối VPN.....	19
<b>TÀI LIỆU THAM KHẢO.....</b>	<b>23</b>

## DANH MỤC CÁC HÌNH VẼ

Hình 1 Cách VPN hoạt động.....	5
Hình 2 L2TP thường được kết hợp với IPSec.....	8
Hình 3 Hoạt động của IPSec .....	9
Hình 4 Các tùy chọn cài đặt của SoftEther .....	10
Hình 5 Địa chỉ IP máy Ubuntu.....	11
Hình 6 Địa chỉ IP máy Windows .....	12
Hình 7 Tải VPN Server trên máy Ubuntu .....	13
Hình 8 Giải nén file cài đặt .....	14
Hình 9 Cài đặt trình biên dịch gcc.....	14
Hình 10 Cài đặt make.....	15
Hình 11 Khởi động máy chủ VPN .....	15
Hình 12 Chạy tiện tích quản trị VPN Server.....	16
Hình 13 Tạo Hub và User .....	17
Hình 14 Cài đặt VPN Client cho Windows.....	18
Hình 15 Giao diện VPN Client .....	19
Hình 16 Tạo kết nối VPN.....	20
Hình 17 Kết nối VPN thành công .....	21
Hình 18 Kiểm tra kết nối bên máy chủ .....	22

## DANH MỤC CÁC TỪ VIẾT TẮT

<b>Từ viết tắt</b>	<b>Thuật ngữ tiếng Anh/Giải thích</b>	<b>Thuật ngữ tiếng Việt/Giải thích</b>
VPN	Virtual Private Network	Mạng riêng ảo
PPTP	Point-to-Point Tunneling Protocol	Giao thức đường hầm điểm-điểm
L2TP	Layer 2 Tunneling Protocol	Giao thức đường hầm tầng 2
L2F	Layer 2 Forwarding	Chuyển tiếp tầng 2
MPLS	Multiprotocol Label Switching	Chuyển mạch nhãn đa giao thức
SSL	Secure Sockets Layer	Lớp cổng bảo mật
TLS	Transport Layer Security	Bảo mật tầng truyền tải

# 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

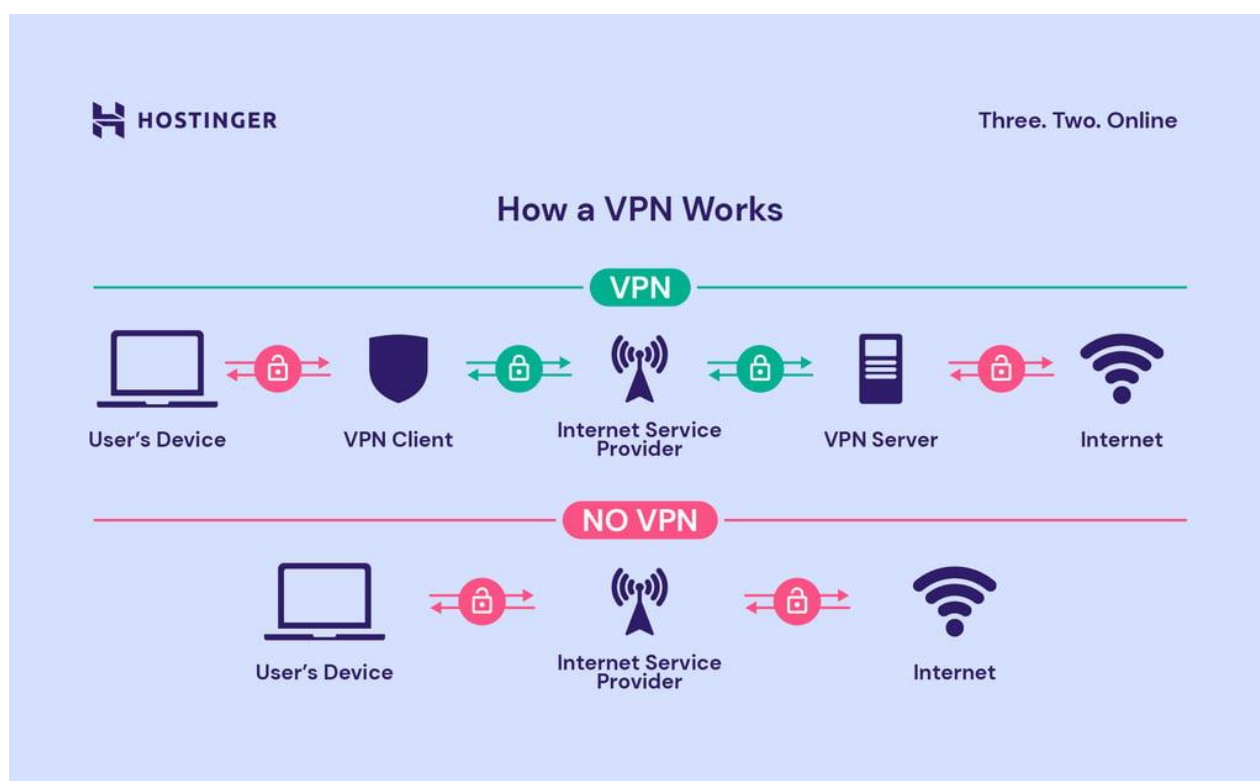
### 1.2.1 VPN – Mạng riêng ảo

#### 1.2.1.1 Khái quát

Mạng riêng ảo hay VPN (virtual private network) là một mạng riêng để kết nối các máy tính của các công ty, tập đoàn hay các tổ chức với nhau thông qua mạng Internet công cộng. Các lợi ích của mạng riêng ảo bao gồm tăng cường chức năng bảo mật và quản lý mạng riêng. Nó cung cấp quyền truy cập vào các tài nguyên không thể truy cập được trên mạng công cộng và thường được sử dụng cho các nhân viên làm việc từ xa.

Công nghệ VPN chỉ rõ 3 yêu cầu cơ bản:

- Cung cấp truy nhập từ xa tới tài nguyên của tổ chức mọi lúc, mọi nơi.
- Kết nối các chi nhánh văn phòng với nhau.
- Kiểm soát truy nhập của khách hàng, nhà cung cấp và các thực thể bên ngoài tới những tài nguyên của tổ chức.



Hình 1 Cách VPN hoạt động

### 1.2.1.2 Các mô hình VPN

Các mô hình VPN bao gồm:

Truy cập từ xa (remote-Access)

Hay cũng được gọi là Mạng quay số riêng ảo (Virtual Private Dial-up Network) hay VPDN, đây là dạng kết nối User-to-Lan áp dụng cho các công ty mà các nhân viên có nhu cầu kết nối tới mạng riêng (private network) từ các địa điểm từ xa và bằng các thiết bị khác nhau.

Khi VPN được triển khai, các nhân viên chỉ việc kết nối Internet thông qua các ISP và sử dụng các phần mềm VPN phía khách để truy cập mạng công ty của họ. Các công ty khi sử dụng loại kết nối này là những hãng lớn với hàng trăm nhân viên thương mại. Các Truy Cập từ xa VPN đảm bảo các kết nối được bảo mật, mã hoá giữa mạng riêng rẽ của công ty với các nhân viên từ xa qua một nhà cung cấp dịch vụ thứ ba (third-party).

Có hai kiểu Truy cập từ xa VPN:

Khởi tạo bởi phía khách (Client-Initiated) – Người dùng từ xa sử dụng phần mềm VPN client để thiết lập một đường hầm an toàn tới mạng riêng thông qua một ISP trung gian.

Khởi tạo bởi NAS (Network Access Server-initiated) – Người dùng từ xa quay số tới một ISP. NAS sẽ thiết lập một đường hầm an toàn tới mạng riêng cần kết nối.

Với Truy cập từ xa VPN, các nhân viên di động và nhân viên làm việc ở nhà chỉ phải trả chi phí cho cuộc gọi nội bộ để kết nối tới ISP và kết nối tới mạng riêng của công ty, tổ chức. Các thiết bị phía máy chủ VPN có thể là Cisco Routers, PIX Firewalls hoặc VPN Concentrators, phía client là các phần mềm VPN hoặc Cisco Routers.

Site-to-Site: Bằng việc sử dụng một thiết bị chuyên dụng và cơ chế bảo mật diện rộng, mỗi công ty có thể tạo kết nối với rất nhiều các site qua một mạng công cộng như Internet.

### 1.2.1.3 Các ứng dụng của VPN

Dịch vụ VPN chủ yếu được sử dụng để gửi dữ liệu một cách an toàn qua Internet. 3 chức năng chính của VPN là:

#### 1. Quyền riêng tư

Nếu không có mạng riêng ảo, dữ liệu cá nhân của bạn như mật khẩu, thông tin thẻ tín dụng và lịch sử duyệt web có thể bị ghi lại và rao bán bởi các bên thứ ba. VPN sử dụng mã hóa để giữ bí mật những thông tin này, đặc biệt là khi bạn kết nối qua mạng Wi-Fi công cộng.

#### 2. Tính ẩn danh

Địa chỉ IP chứa thông tin về vị trí và hoạt động duyệt web của bạn. Tất cả các trang web trên Internet theo dõi dữ liệu này bằng cookie và công nghệ tương tự. Họ có thể nhận dạng bạn bất cứ khi nào bạn ghé thăm trang web của họ. Kết nối VPN sẽ ẩn địa chỉ IP của bạn, để bạn được ẩn danh trên Internet.

#### 3. Bảo mật

Dịch vụ VPN sử dụng mật mã để bảo vệ kết nối Internet của bạn khỏi những truy cập trái phép. VPN cũng có thể hoạt động như một cơ chế tắt, hủy bỏ các chương trình được chọn trước đó phòng khi có hoạt động đáng ngờ trên Internet. Việc này làm giảm khả năng dữ liệu bị xâm phạm. Những tính năng trên cho phép các công ty cấp quyền truy cập từ xa cho người dùng được ủy quyền thuộc mạng lưới kinh doanh của họ.

### ***1.2.2 Các giao thức tạo đường hầm cho VPN***

#### ***1.2.2.1 PPTP***

PPTP là một giao thức tunnelling (giao thức đường hầm), bản thân nó không phải là một giao thức VPN hoàn chỉnh. Mã hóa và xác thực được xử lý bởi Giao thức Point-to-Point (PPP), nhưng PPP không bao gồm cơ chế định tuyến để hướng các gói đến đích của chúng.

PPTP hoạt động trên lớp (dữ liệu) thứ 2 của mô hình OSI. PPTP thiết lập kết nối TCP tới máy chủ VPN qua cổng 1723, đóng gói lại các gói IP PPP bằng cách sử dụng Generic Routing Encapsulation (GRE). Các gói này được mã hóa bằng Point-to-Point Encryption (MPPE) của Microsoft, sử dụng mật mã luồng RSA RC4 với kích thước khóa tối đa là 128-bit.

Xác thực thường đạt được bằng cách sử dụng giao thức MS-CHAP (hiện tại là v2). (Có thể sử dụng AEP-TLS an toàn hơn, nhưng điều này liên quan đến việc triển khai hệ thống chứng chỉ máy chủ, điều này phần lớn phủ nhận những lợi thế của việc sử dụng PPTP ngay từ đầu.)

Công dụng của PPTP:

- Chia sẻ kết nối Internet
- Chia sẻ và chuyển giao dữ liệu

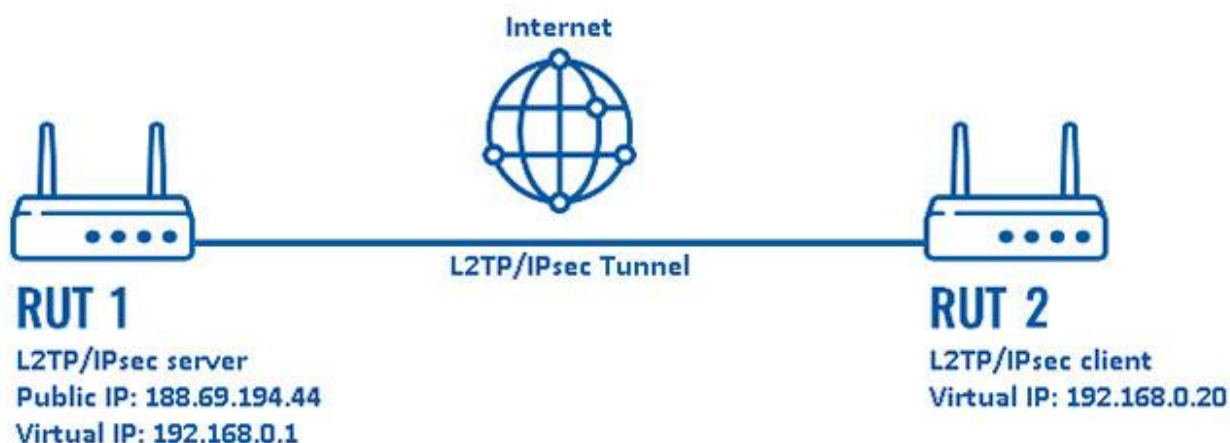
#### ***1.2.2.2 L2TP***

L2TP là viết tắt của Layer 2 Tunneling Protocol, và giống như tên của nó, đây là một giao thức tunneling được thiết kế để hỗ trợ các kết nối VPN. Thật thú vị, L2TP thường được ISP sử dụng để cho phép hoạt động VPN.

L2TP Tunneling bắt đầu bằng cách kết nối LAC (L2TP Access Concentrator) và LNS (L2TP Network Server) - hai điểm cuối của giao thức - trên Internet. Sau khi đạt được điều đó, một layer liên kết PPP được kích hoạt và đóng gói lại, sau đó, lớp liên kết này được chuyển qua web.

Sau đó, kết nối PPP được khởi tạo bởi người dùng cuối (bạn) với ISP. Khi LAC chấp nhận kết nối, liên kết PPP được thiết lập. Sau đó, một vị trí trống trong tunnel mạng được chỉ định và yêu cầu sau đó được chuyển đến LNS.

Cuối cùng, khi kết nối được xác thực và chấp nhận hoàn toàn, một giao diện PPP ảo sẽ được tạo. Tại thời điểm đó, các link frame (đơn vị truyền dữ liệu số trong mạng máy tính) có thể tự do đi qua tunnel. Các frame được LNS chấp nhận, sau đó loại bỏ mã hóa L2TP và tiến hành xử lý chúng như các frame thông thường.



Hình 2 L2TP thường được kết hợp với IPSec

### 1.2.2.3 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.

### 1.2.2.4 MPLS

MPLS là viết tắt của Multi-Protocol Label Switching. Đây là một công nghệ định tuyến mạng được sử dụng để cải thiện hiệu suất và quản lý mạng. MPLS kết hợp nhiều ưu điểm của việc định tuyến dựa trên gói và hoạt động chuyển mạch mạng.

Trong MPLS, khi gói dữ liệu vào mạng được gán một nhãn (label) duy nhất, sau đó được chuyển tiếp theo các đường định tuyến được xác định trước. Nhãn này giúp định tuyến gói dữ liệu một cách nhanh chóng và hiệu quả hơn. Đồng thời cho phép quản lý chất lượng dịch vụ (QoS), ưu tiên dữ liệu và tạo các kết nối ảo (VPN) trên cùng một cơ sở hạ tầng mạng.

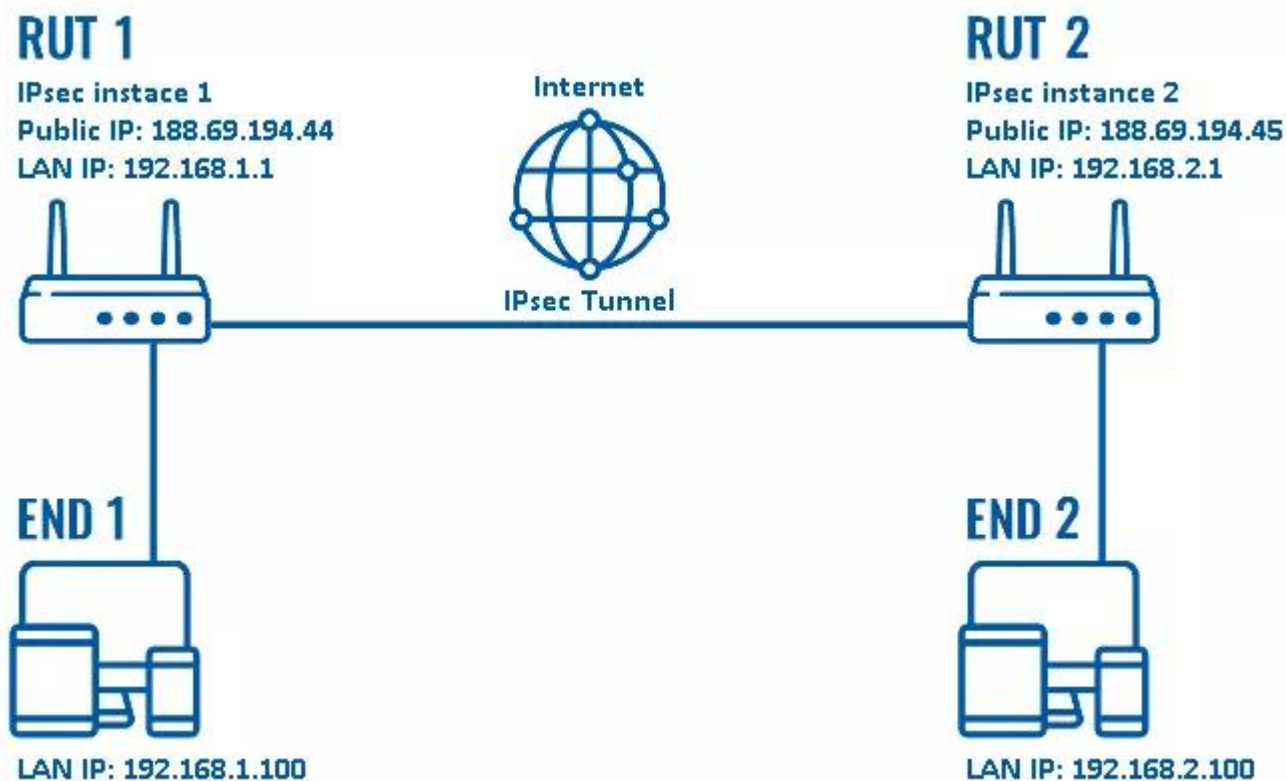
## 1.2.3 Các giao thức bảo mật cho VPN

### 1.2.3.1 IPSec

IPsec là một nhóm giao thức được sử dụng cùng nhau để thiết lập các kết nối được mã hóa giữa các thiết bị. Nó giúp bảo mật dữ liệu được gửi qua public network. Nhóm giao thức này thường được sử dụng để thiết lập VPN. Nó hoạt động bằng cách mã hóa IP packet cùng với việc xác thực nguồn của các packet.

Trong thuật ngữ “IPsec”, “IP” là viết tắt của “Internet Protocol” và “sec” là “security”. Internet Protocol là một routing protocol chính được sử dụng trên Internet. Nó chỉ định nơi dữ liệu sẽ đi bằng địa chỉ IP. Nhóm giao thức này an toàn vì nó thêm mã hóa và xác thực vào quá trình này.





*Hình 3 Hoạt động của IPsec*

### 1.2.3.2 SSL/TLS

SSL (Secure Sockets Layer) là một giao thức bảo mật được phát triển để thiết lập một kết nối mã hóa giữa máy chủ và máy khách. SSL được Netscape phát triển lần đầu tiên vào năm 1995 với mục đích đảm bảo quyền riêng tư, tính xác thực và tính toàn vẹn của dữ liệu trong truyền thông Internet.

Tuy nhiên, giống như bất kỳ công nghệ nào, SSL cũng bộc lộ những hạn chế về bảo mật theo thời gian. Các phiên bản SSL 2.0 và 3.0 dần trở nên lỗi thời, tạo cơ hội cho các lỗ hổng bảo mật bị khai thác.

Nhận thức được những hạn chế của SSL, TLS (Transport Layer Security) ra đời như một phiên bản nâng cấp, kế thừa những ưu điểm và khắc phục những lỗ hổng của SSL. Năm 1999, IETF đề xuất một bản cập nhật cho SSL. TLS được xây dựng dựa trên nền tảng của SSL 3.0, đồng thời được bổ sung thêm nhiều tính năng bảo mật tiên tiến, đảm bảo an toàn cho dữ liệu trong môi trường Internet ngày càng phức tạp.

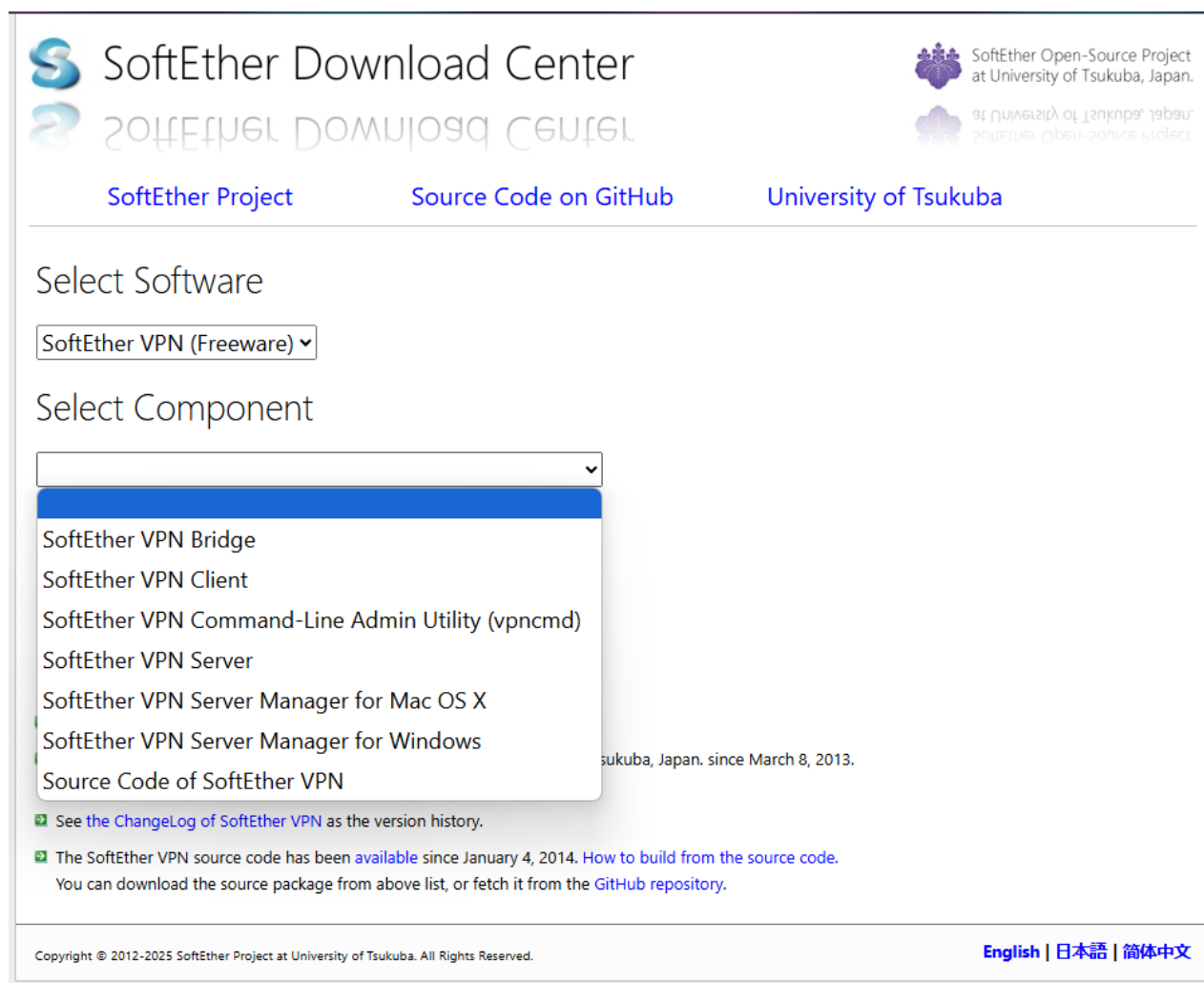
Ngày nay, TLS đã thay thế hoàn toàn SSL, trở thành tiêu chuẩn bảo mật không thể thiếu cho các website và ứng dụng trực tuyến. Khi truy cập một website, bạn hãy chú ý đến biểu tượng ổ khóa trên thanh địa chỉ, đó chính là dấu hiệu cho thấy website đó đang sử dụng TLS để bảo vệ thông tin của bạn.

Khi giao thức SSL được tổ chức IETF chuẩn hóa, nó được đổi tên thành Transport Layer Security (TLS). Mặc dù nhiều người sử dụng tên gọi TLS và SSL thay thế cho nhau, nhưng về mặt kỹ thuật, chúng khác biệt vì mỗi tên đại diện cho một phiên bản khác nhau của giao thức.

### 1.2.4 SoftEther VPN

SoftEther VPN (SoftEther Virtual Private Network) là một phần mềm VPN mã nguồn mở, mạnh mẽ và linh hoạt, do Đại học Tsukuba (Nhật Bản) phát triển. Nó được thiết kế để cung cấp kết nối VPN nhanh, bảo mật cao và hỗ trợ nhiều giao thức khác nhau.

SoftEther VPN hỗ trợ nhiều giao thức VPN như: SoftEther VPN có thể hoạt động như một máy chủ VPN hỗ trợ nhiều giao thức phổ biến, bao gồm: OpenVPN, L2TP/IPsec, SSTP (Secure Socket Tunneling Protocol), SoftEther VPN (giao thức riêng), PPTP (Point-to-Point Tunneling Protocol)



Hình 4 Các tùy chọn cài đặt của SoftEther

## CHƯƠNG 2. NỘI DUNG THỰC HÀNH

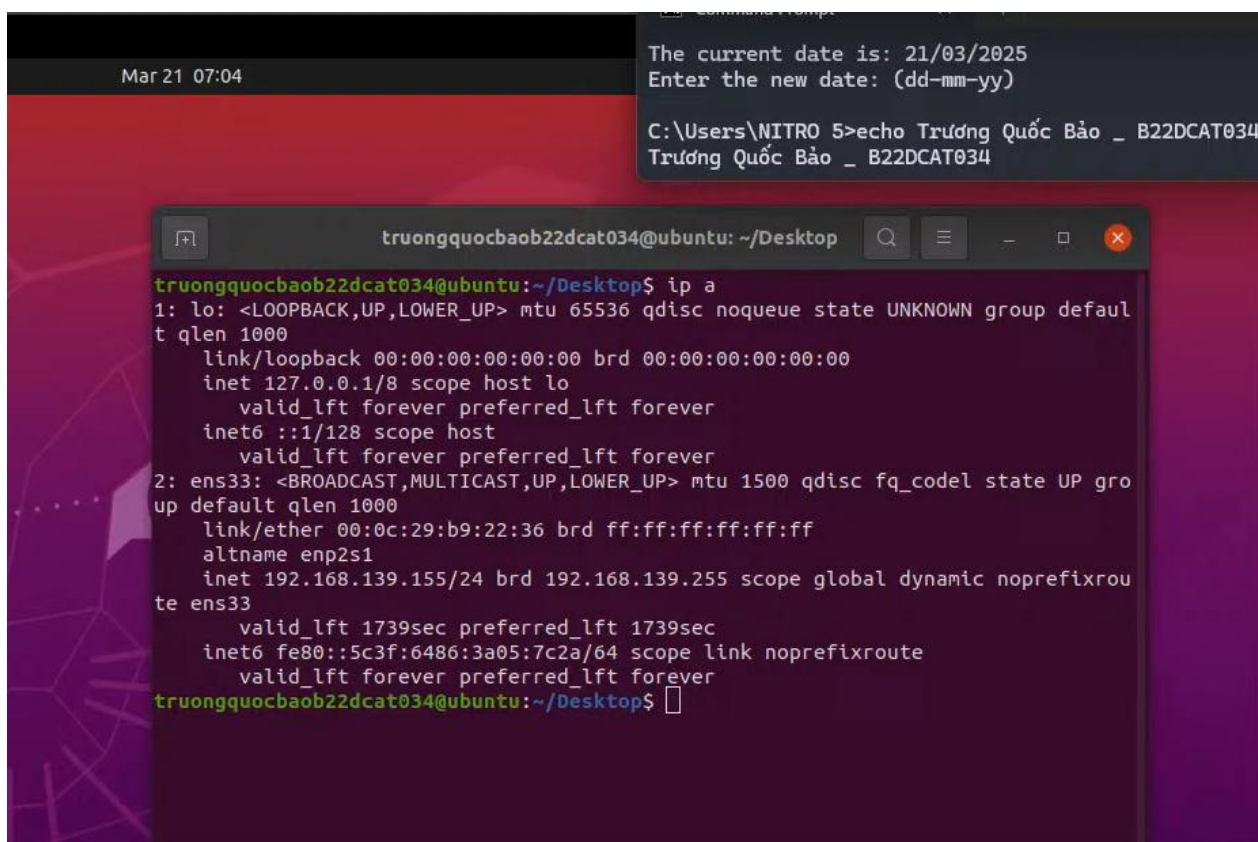
### 2.1 Chuẩn bị môi trường

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

### 2.2 Các bước thực hiện

#### 2.2.1 Chuẩn bị máy tính như mô tả

Máy Ubuntu có kết nối mạng LAN và có địa chỉ IP “192.168.139.155”, kiểm tra bằng lệnh “ip a”



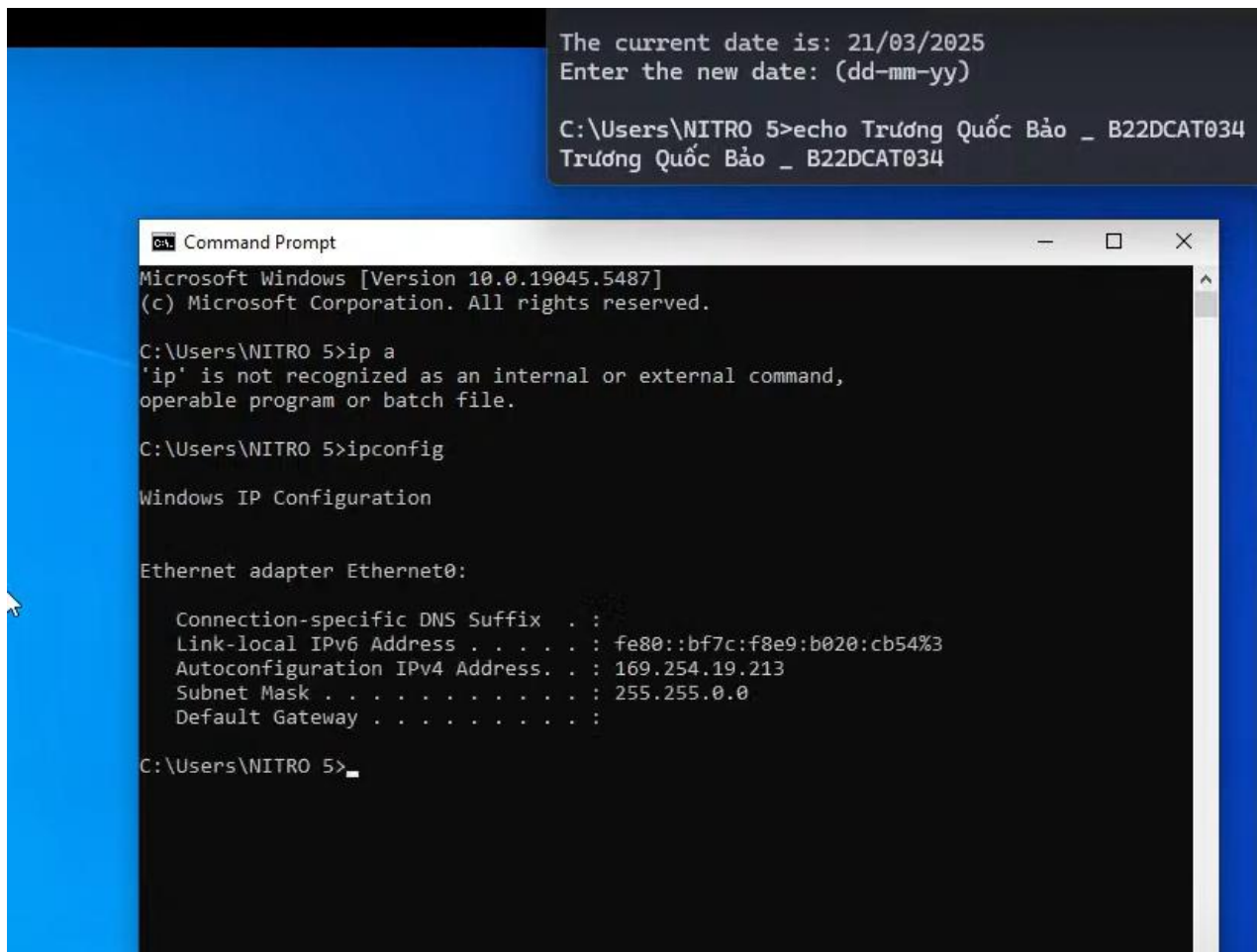
```
Mar 21 07:04
The current date is: 21/03/2025
Enter the new date: (dd-mm-yy)

C:\Users\NITRO 5>echo Trương Quốc Bảo _ B22DCAT034
Trương Quốc Bảo _ B22DCAT034

truongquocbaob22dcat034@ubuntu: ~/Desktop
truongquocbaob22dcat034@ubuntu:~/Desktop$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:b9:22:36 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.139.155/24 brd 192.168.139.255 scope global dynamic noprefixroute ens33
        valid_lft 1739sec preferred_lft 1739sec
    inet6 fe80::5c3f:6486:3a05:7c2a/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
truongquocbaob22dcat034@ubuntu:~/Desktop$
```

Hình 5 Địa chỉ IP máy Ubuntu

Máy Windows có địa chỉ IP và kết nối mạng LAN, gõ “ipconfig” để kiểm tra.



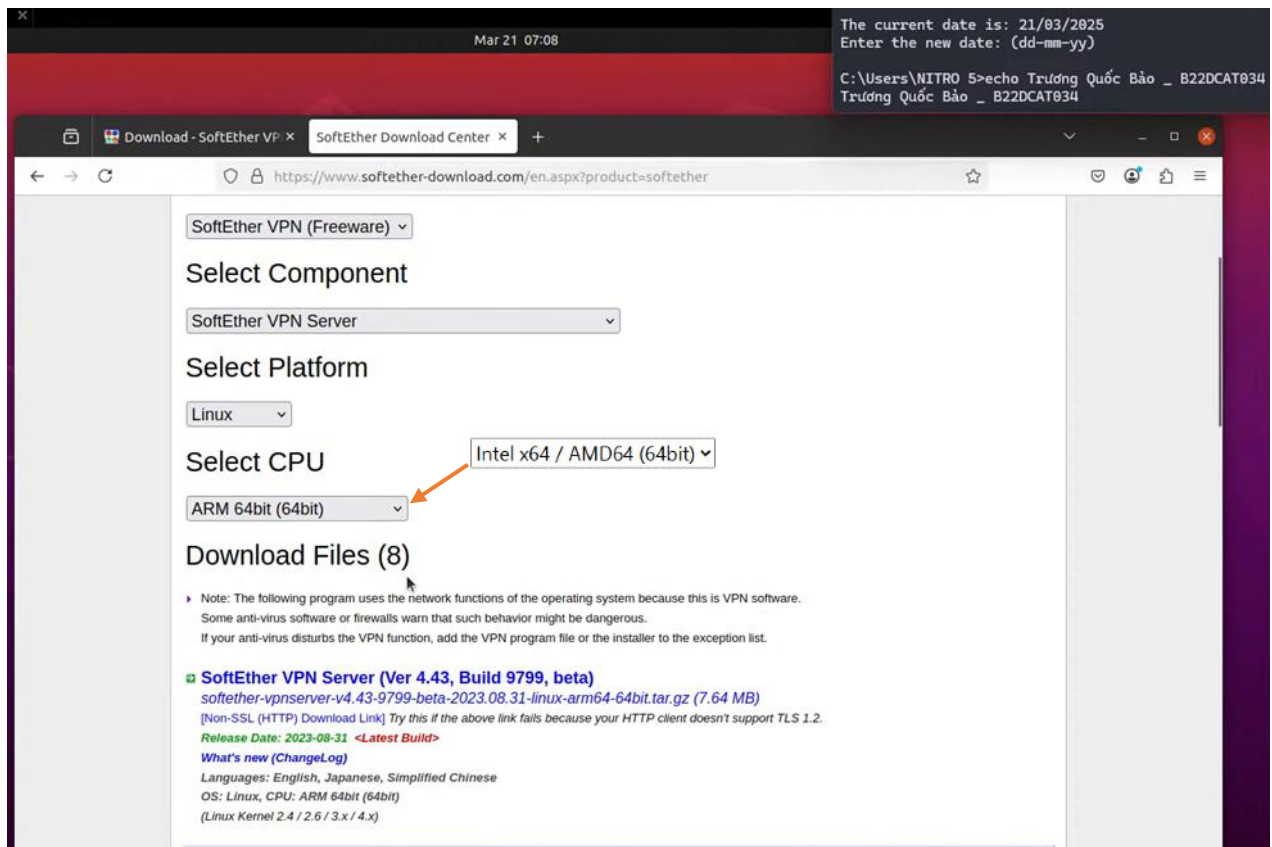
*Hình 6 Địa chỉ IP máy Windows*

### **2.2.2 Tải và cài đặt SoftEther VPN server**

Mở trình duyệt mạng có sẵn trên máy Ubuntu. Tiến hành cài đặt SoftEther VPN tại <https://www.softether.org/5-download>.

Tiến hành chọn để cài đặt VPN Server như hình bên dưới.

Lưu ý, phải đúng phiên bản và mẫu mã của máy.



*Hình 7 Tải VPN Server trên máy Ubuntu*

Sau khi đã cài đặt về máy, mở cmd, di chuyển tới vị trí lưu file và tiến hành giải nén bằng lệnh “*tar -vxzf <tên file>*”



```
Mar 21 07:10
The current date is: 21/03/2025
Enter the new date: (dd-mm-yy)

C:\Users\NITRO 5>echo Trương Quốc Bảo _ B22DCAT034
Trương Quốc Bảo _ B22DCAT034

truongquocbaob22dcat034@ubuntu: ~/Downloads
truongquocbaob22dcat034@ubuntu:~/Downloads$ ls
softether-vpnserver-v4.42-9798-rtm-2023.06.30-linux-arm64-64bit.tar.gz
truongquocbaob22dcat034@ubuntu:~/Downloads$ tar -vxzf softether-vpnserver-v4.42-9798-rtm-2023.06.30-linux-arm64-64bit.tar.gz
vpnserver/
vpnserver/Makefile
vpnserver/.install.sh
vpnserver/ReadMeFirst_License.txt
vpnserver/Authors.txt
vpnserver/ReadMeFirst_Important_Notices_ja.txt
vpnserver/ReadMeFirst_Important_Notices_en.txt
vpnserver/ReadMeFirst_Important_Notices_cn.txt
vpnserver/code/
vpnserver/code/vpnserver.a
vpnserver/code/vpncmd.a
vpnserver/lib/
vpnserver/lib/libcharset.a
vpnserver/lib/libcrypto.a
vpnserver/lib/libedit.a
vpnserver/lib/libiconv.a
vpnserver/lib/libncurses.a
vpnserver/lib/libssl.a
vpnserver/lib/libz.a
vpnserver/lib/License.txt
vpnserver/hamcore.se2
truongquocbaob22dcat034@ubuntu:~/Downloads$
```

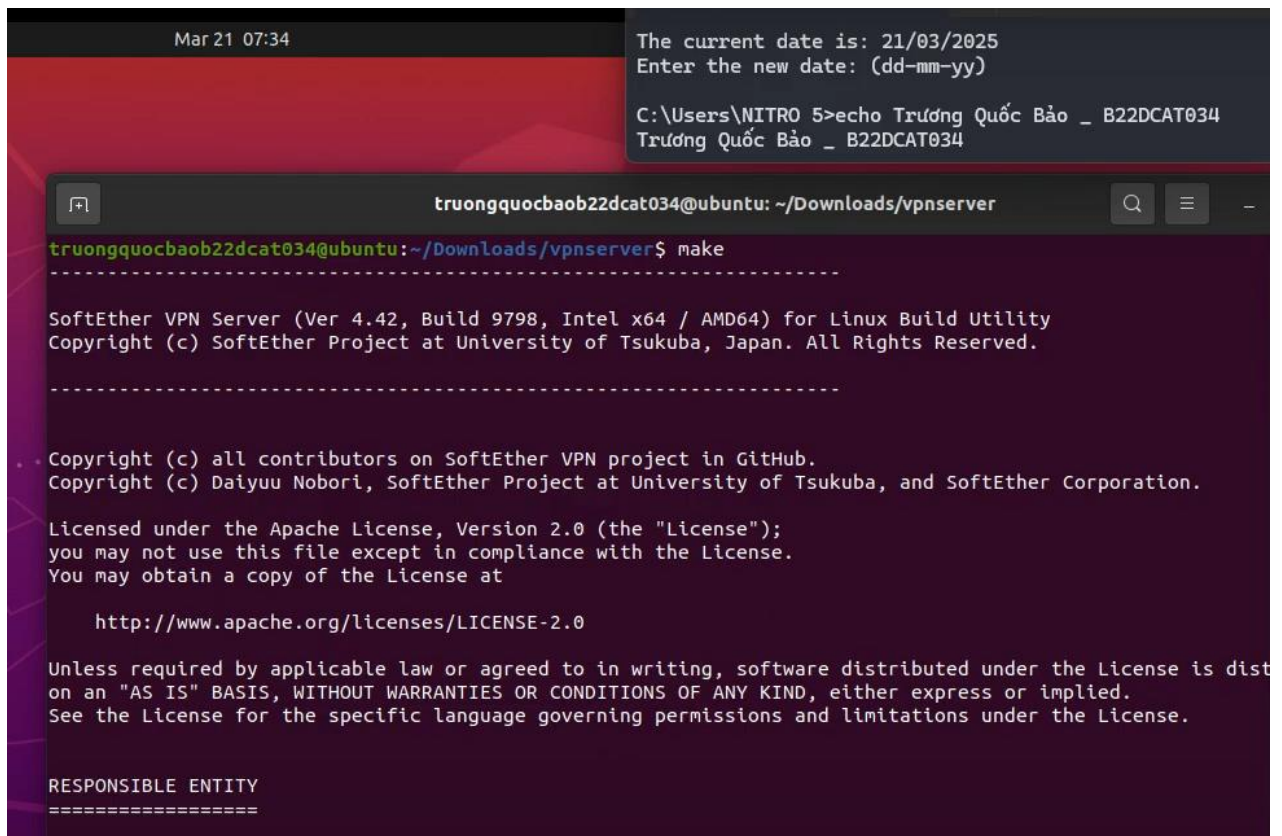
Hình 8 Giải nén file cài đặt

Hãy chắc chắn đã cài đặt trình biên dịch gcc ở hệ thống. Nếu chưa, tiến hành cài đặt bằng lệnh “`sudo apt install gcc make build-essential libssl-dev libreadline-dev zlib1g-dev -y`”

```
truongquocbaob22dcat034@ubuntu:~/Downloads/vpnserver$ sudo apt install gcc make
build-essential libssl-dev libreadline-dev zlib1g-dev -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
gcc is already the newest version (4:9.3.0-1ubuntu2).
libreadline-dev is already the newest version (8.0-4).
make is already the newest version (4.2.1-1.2).
build-essential is already the newest version (12.8ubuntu1.1).
libssl-dev is already the newest version (1.1.1f-1ubuntu2.24).
zlib1g-dev is already the newest version (1:1.2.11.dfsg-2ubuntu1.5).
```

Hình 9 Cài đặt trình biên dịch gcc

Di chuyển đến thư mục “vpnserver”, kiểm tra trình biên dịch bằng lệnh “make”



```
Mar 21 07:34
The current date is: 21/03/2025
Enter the new date: (dd-mm-yy)
C:\Users\NITRO 5>echo Trương Quốc Bảo _ B22DCAT034
Trương Quốc Bảo _ B22DCAT034

truongquocbaob22dcat034@ubuntu: ~/Downloads/vpnserver
truongquocbaob22dcat034@ubuntu:~/Downloads/vpnserver$ make

-----
SoftEther VPN Server (Ver 4.42, Build 9798, Intel x64 / AMD64) for Linux Build Utility
Copyright (c) SoftEther Project at University of Tsukuba, Japan. All Rights Reserved.
-----

Copyright (c) all contributors on SoftEther VPN project in GitHub.
Copyright (c) Daiyuu Nobori, SoftEther Project at University of Tsukuba, and SoftEther Corporation.

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

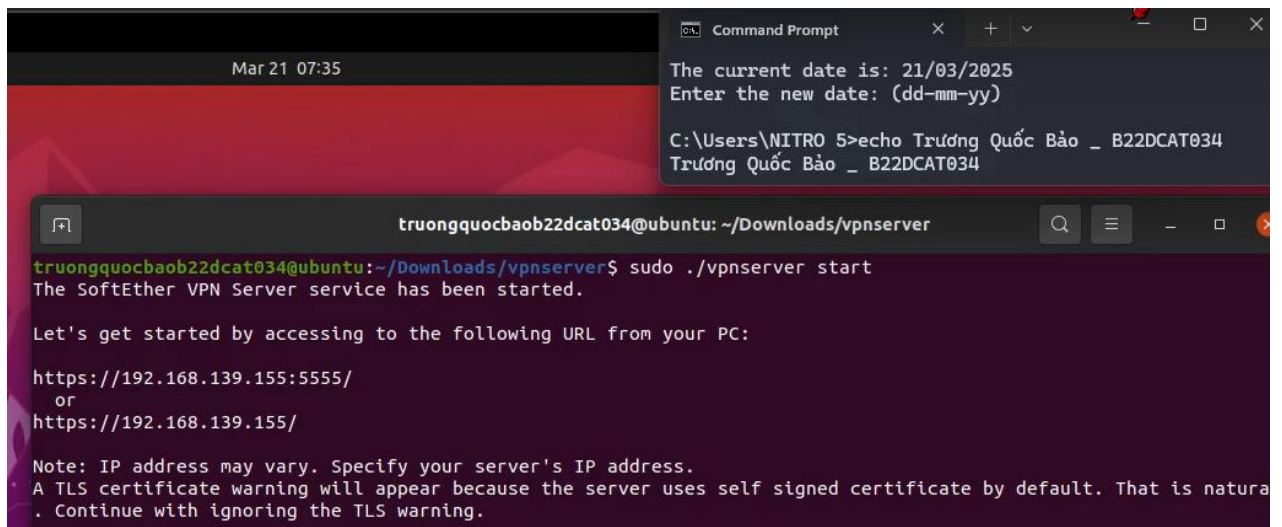
    http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and limitations under the License.

RESPONSIBLE ENTITY
=====
```

Hình 10 Cài đặt make

Khởi động máy chủ VPN bằng lệnh “*sudo ./vpnserver start*”



```
Mar 21 07:35
The current date is: 21/03/2025
Enter the new date: (dd-mm-yy)
C:\Users\NITRO 5>echo Trương Quốc Bảo _ B22DCAT034
Trương Quốc Bảo _ B22DCAT034

truongquocbaob22dcat034@ubuntu: ~/Downloads/vpnserver
truongquocbaob22dcat034@ubuntu:~/Downloads/vpnserver$ sudo ./vpnserver start
The SoftEther VPN Server service has been started.

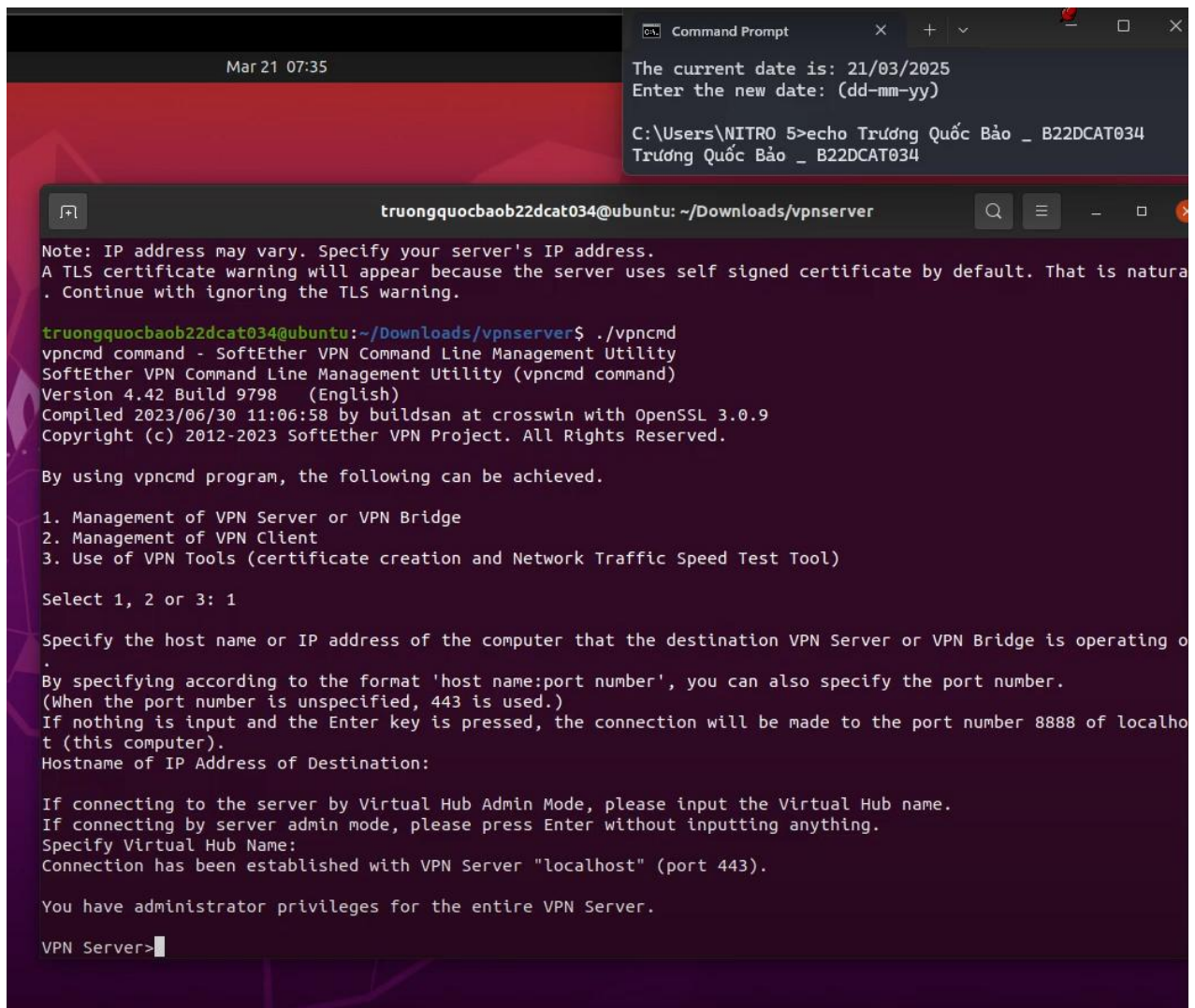
Let's get started by accessing to the following URL from your PC:

https://192.168.139.155:5555/
or
https://192.168.139.155/

Note: IP address may vary. Specify your server's IP address.
A TLS certificate warning will appear because the server uses self signed certificate by default. That is natural.
Continue with ignoring the TLS warning.
```

Hình 11 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).



Hình 12 Chạy tiện ích quản trị VPN Server

Tạo Virtual Hub và tài khoản người dùng VPN trong giao diện quản trị:

Tạo 1 Virtual Hub mới:

*HubCreate <name> </PASSWORD:password>*

Chọn Virtual Hub đã tạo:

*Hub <tên Virtual Hub>*

Tạo 1 người dùng VPN mới:

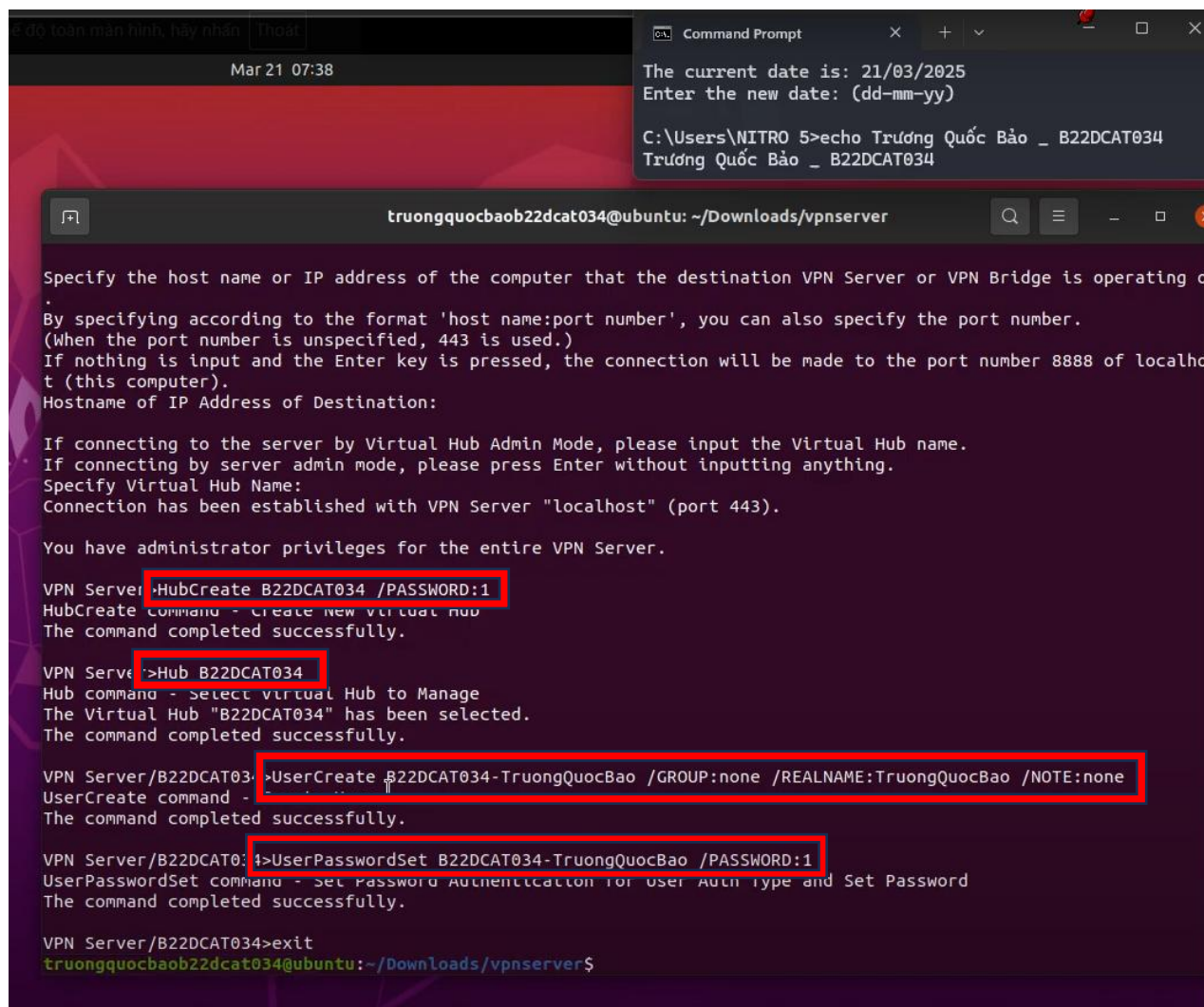
*UserCreate <mã sv-tên> /GROUP:none /REALNAME:Tên sinh viên /NOTE:none*

Đặt mật khẩu cho người dùng:

*UserPasswordSet <mã sv-tên> </PASSWORD:password>*

Gõ *exit* để thoát khỏi tiện ích quản trị VPN Server





```
Mar 21 07:38

Command Prompt
The current date is: 21/03/2025
Enter the new date: (dd-mm-yy)
C:\Users\NITRO 5>echo Trương Quốc Bảo _ B22DCAT034
Trương Quốc Bảo _ B22DCAT034

truongquocbaob22dcat034@ubuntu: ~/Downloads/vpnserver

Specify the host name or IP address of the computer that the destination VPN Server or VPN Bridge is operating on.
By specifying according to the format 'host name:port number', you can also specify the port number.
(When the port number is unspecified, 443 is used.)
If nothing is input and the Enter key is pressed, the connection will be made to the port number 8888 of localhost (this computer).
Hostname of IP Address of Destination:

If connecting to the server by Virtual Hub Admin Mode, please input the Virtual Hub name.
If connecting by server admin mode, please press Enter without inputting anything.
Specify Virtual Hub Name:
Connection has been established with VPN Server "localhost" (port 443).

You have administrator privileges for the entire VPN Server.

VPN Server>HubCreate B22DCAT034 /PASSWORD:1
HubCreate command - Create new virtual hub
The command completed successfully.

VPN Server>Hub B22DCAT034
Hub command - Select virtual Hub to Manage
The Virtual Hub "B22DCAT034" has been selected.
The command completed successfully.

VPN Server/B22DCAT034>UserCreate B22DCAT034-TruongQuocBao /GROUP:none /REALNAME:TruongQuocBao /NOTE:none
UserCreate command - 
The command completed successfully.

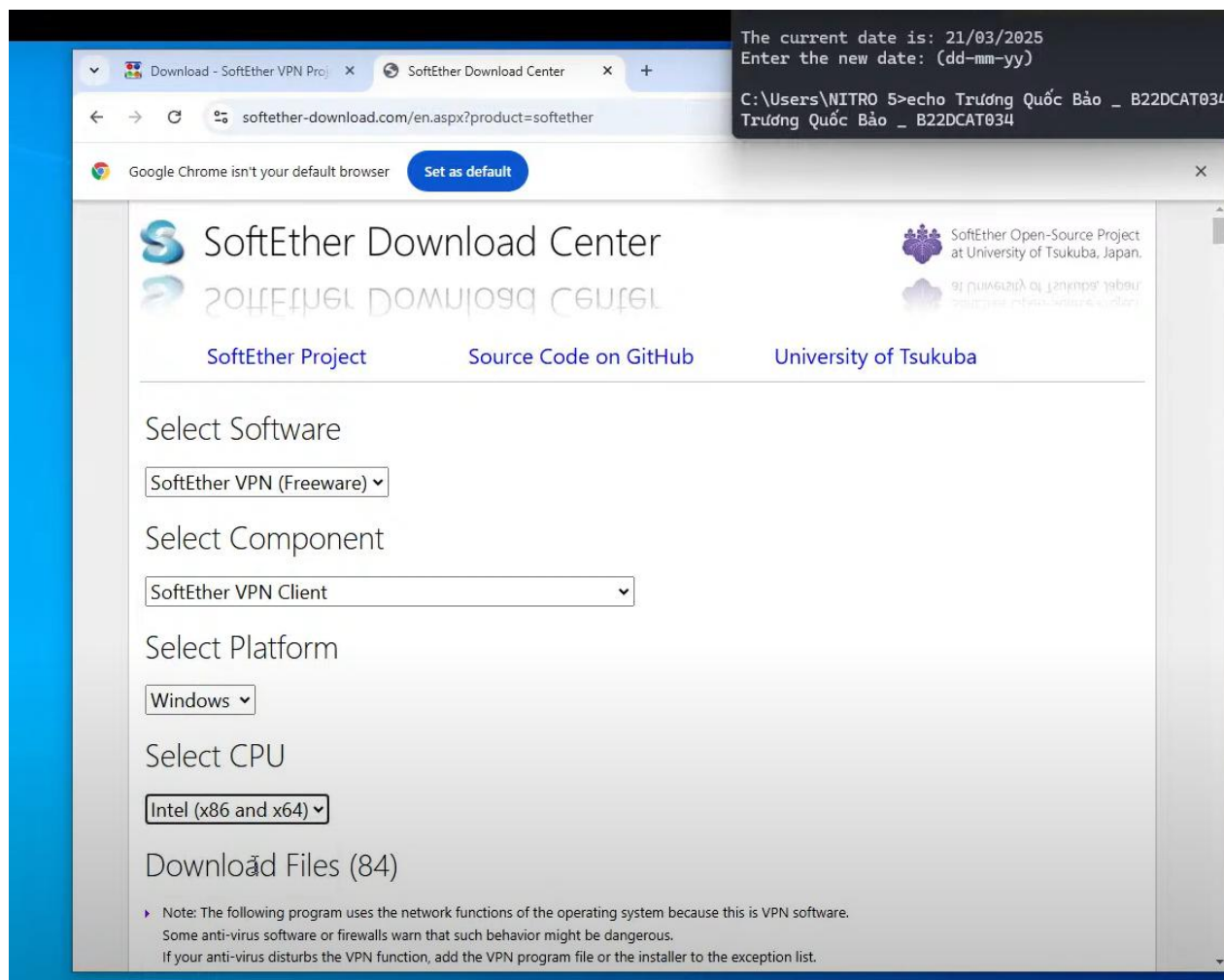
VPN Server/B22DCAT034>UserPasswordSet B22DCAT034-TruongQuocBao /PASSWORD:1
UserPasswordSet command - Set Password Authentication for user Auth type and Set Password
The command completed successfully.

VPN Server/B22DCAT034>exit
truongquocbaob22dcat034@ubuntu: ~/Downloads/vpnserver$
```

Hình 13 Tạo Hub và User

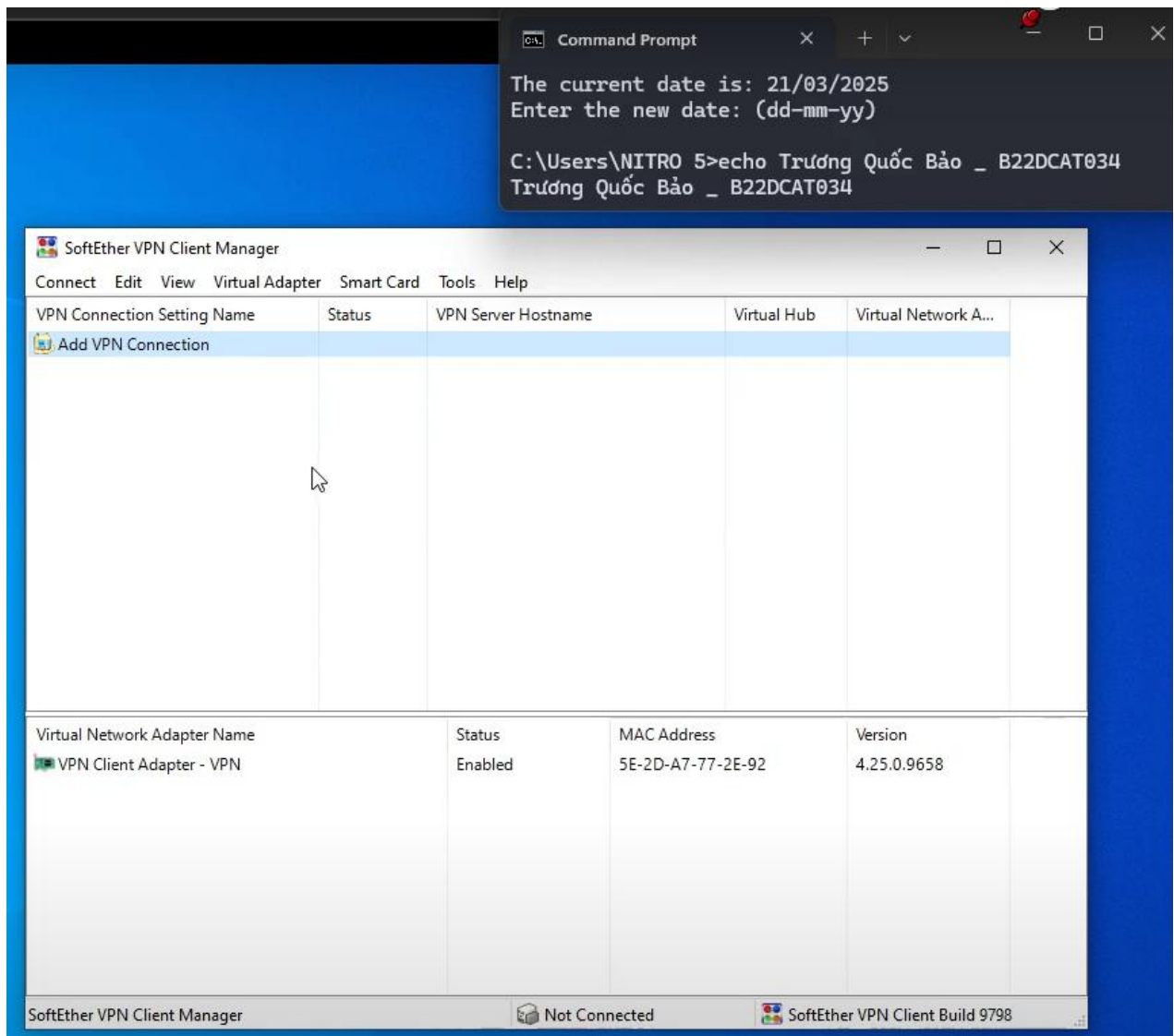
### 2.2.3 Tải SoftEther VPN Client

Ở máy Windows, truy cập <https://www.softether.org/5-download> để tải xuống VPN Client. Lưu ý chọn phiên bản cấu hình cho phù hợp.



*Hình 14 Cài đặt VPN Client cho Windows*

Tiến hành cài đặt và mở phần mềm. Giao diện làm việc sẽ như ở bên dưới.



*Hình 15 Giao diện VPN Client*

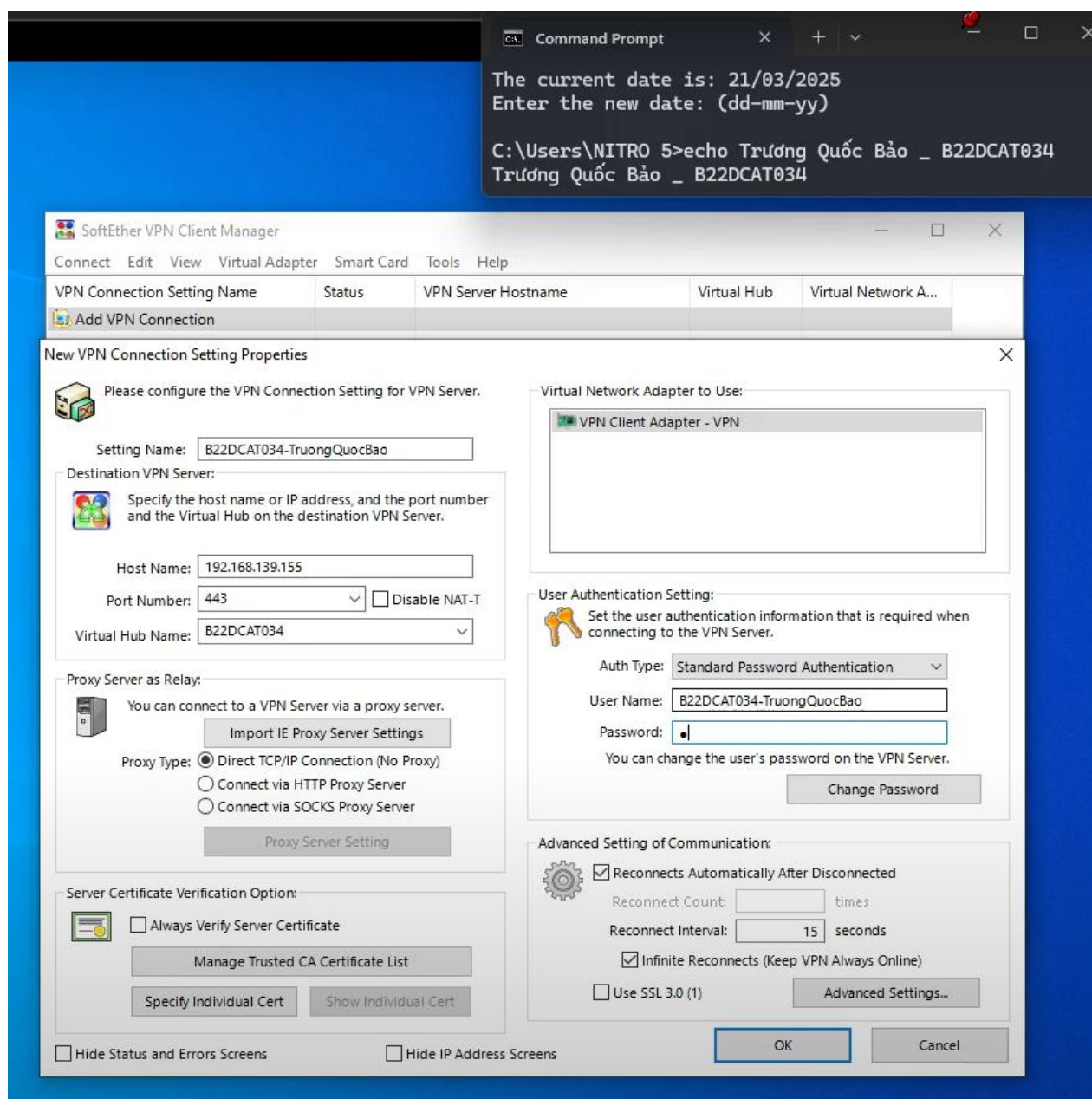
## **2.2.4 Tạo và kiểm tra kết nối VPN**

Nháy chuột phải vào Add New Connection để tạo kết nối mới

Đặt tên kết nối, địa chỉ Host ( địa chỉ máy Ubuntu ), cổng 443, Virtual Hub Name là mã sinh viên đã tạo trước đó.

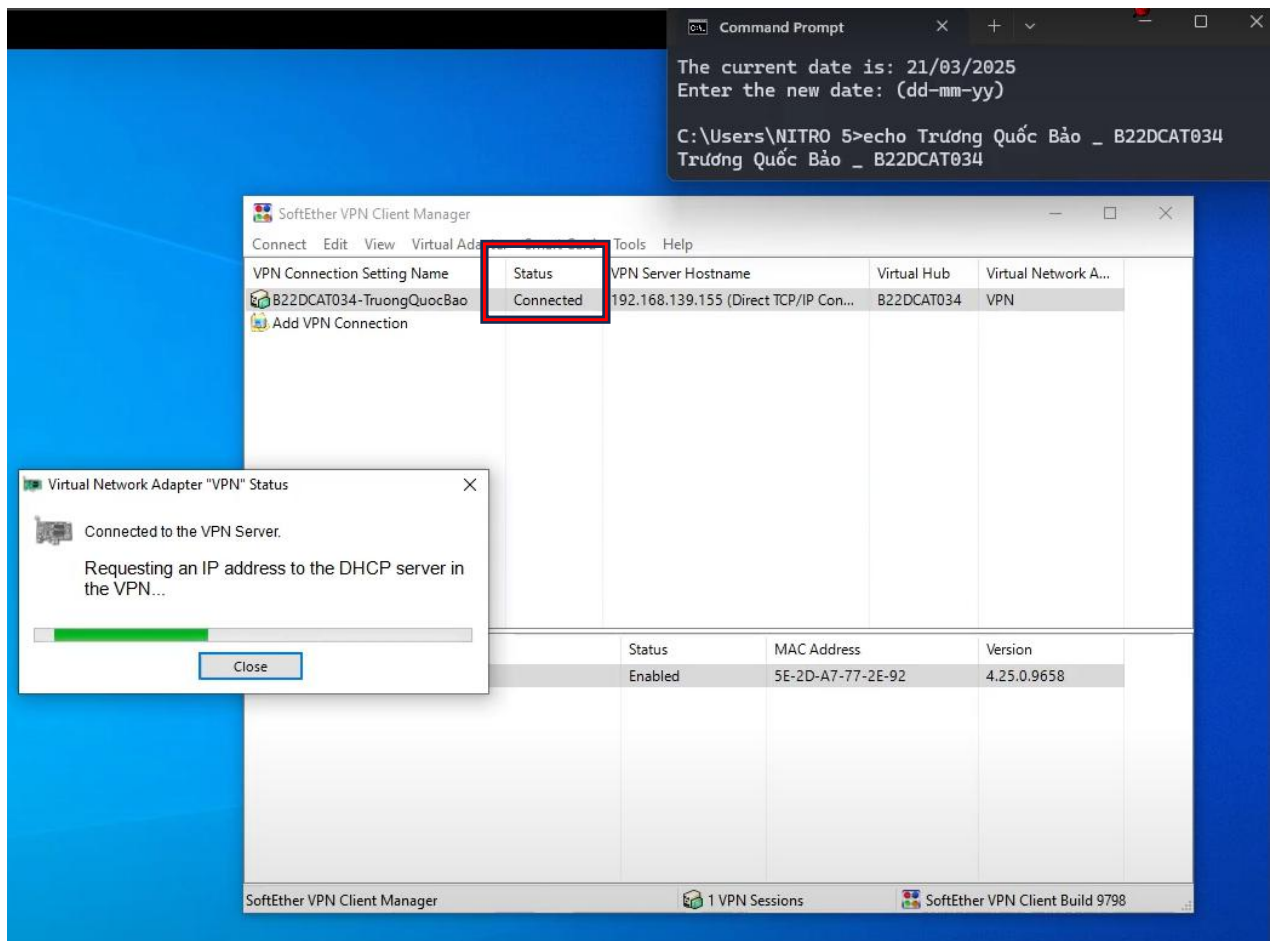
Xác thực bằng cách đăng nhập User đã tạo và nhập mật khẩu tương ứng

Nhấn OK để tiến hành kết nối.



*Hình 16 Tạo kết nối VPN*

Hệ thống sẽ tự động kết nối, sau một khoảng thời gian, *Status* sẽ chuyển thành *Connected* nếu thành công.



Hình 17 Kết nối VPN thành công

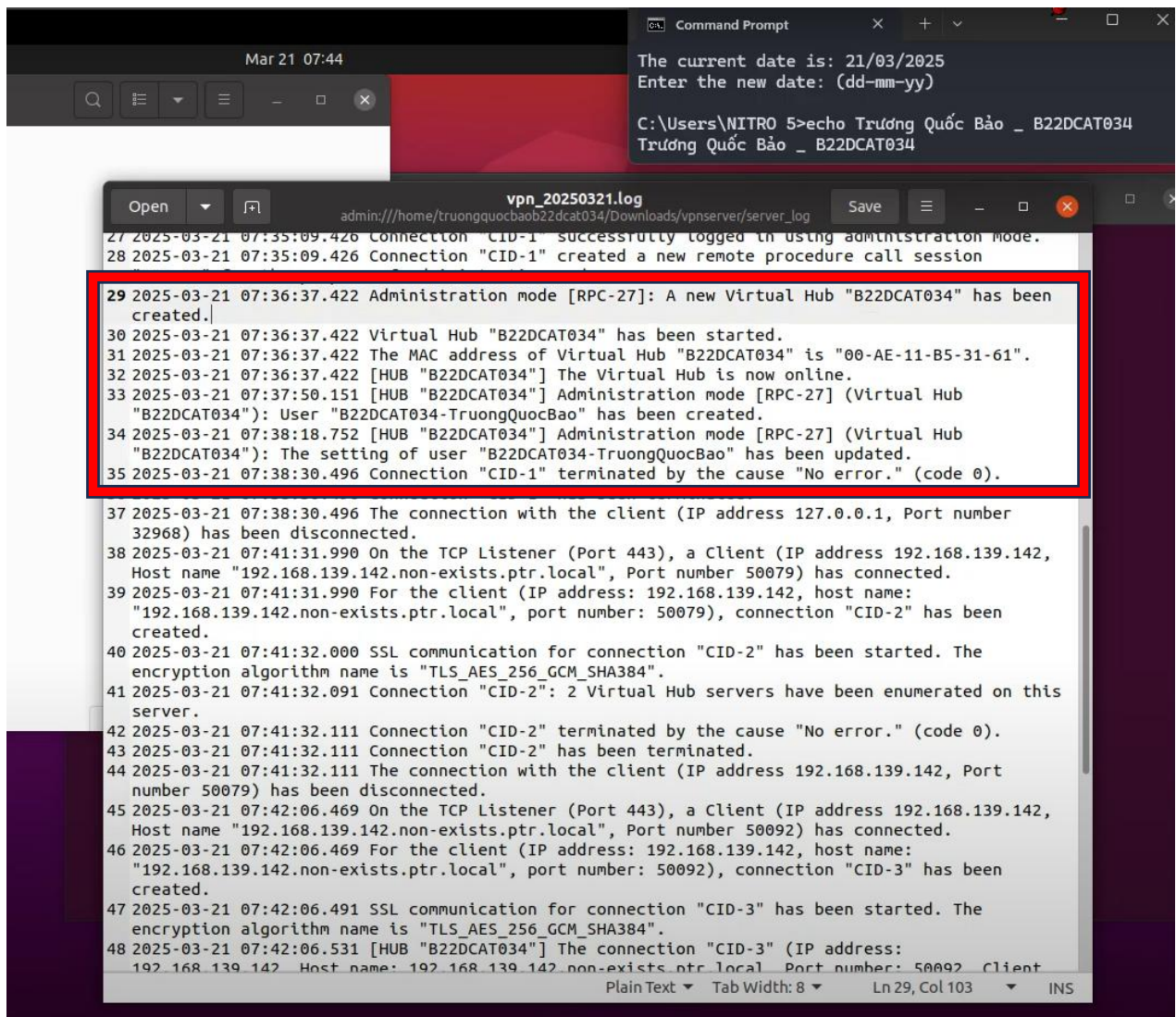
+ Kiểm tra kết nối bên máy chủ: Chuyển sang máy chủ VPN, mở 1 terminal mới chuyển đến thư mục vpnserver/server\_log để kiểm tra log trên VPN server:

```
sudo grep <mã sinh viên> vpnserver/server_log/*.log
```

Hoặc trực tiếp kiểm tra file server\_log đã lưu trong thư mục tương ứng

Ta sẽ thấy hiện thông tin kết nối cụ thể theo thời gian và hành động.





Hình 18 Kiểm tra kết nối bên máy chủ

## **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>