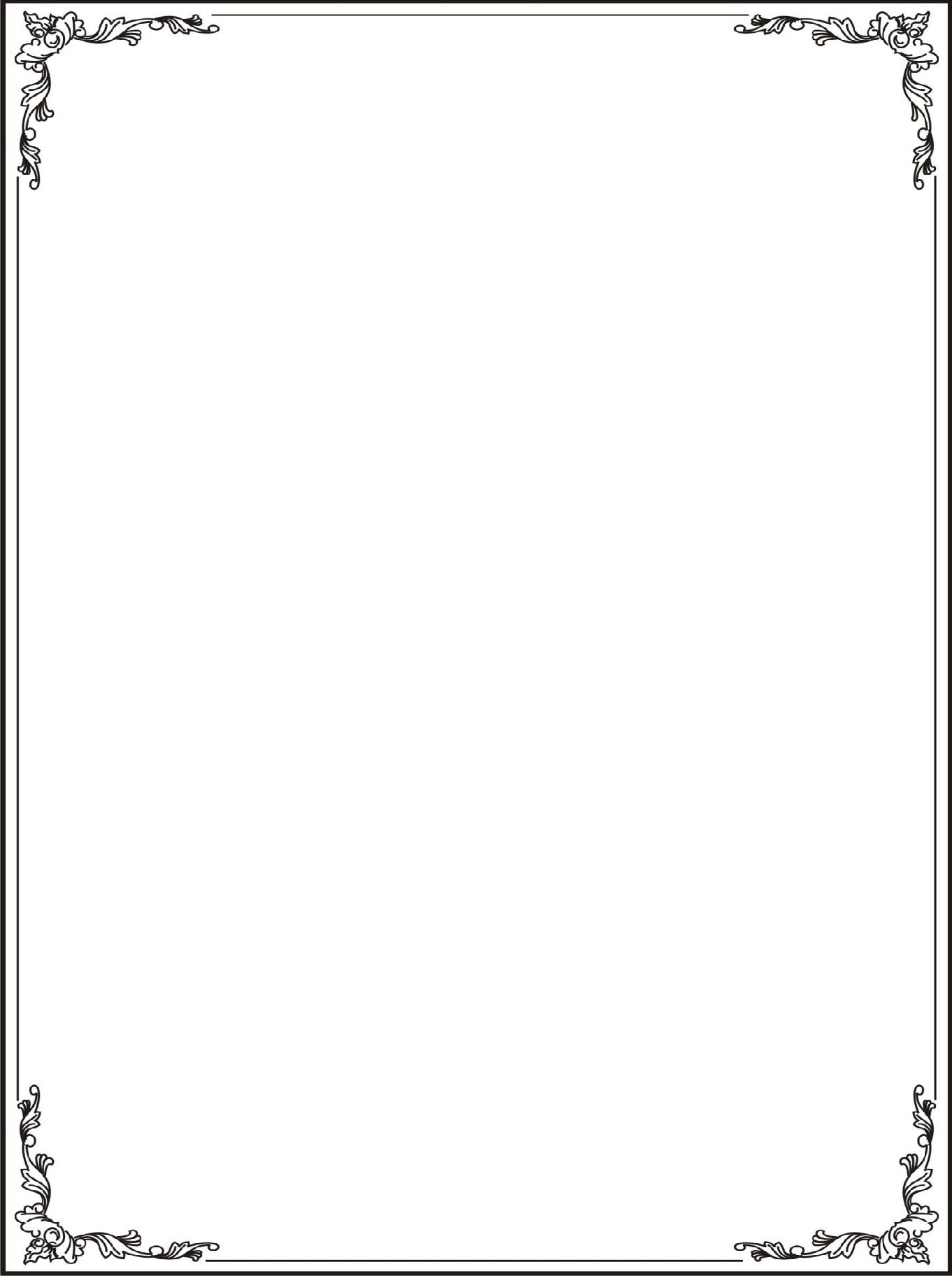
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



BÁO CÁO BÀI THỰC HÀNH THỰC TẬP CƠ SỞ

Bài 07 - Cài đặt cấu hình VPN server

# Họ và tên: Nguyễn Huy Quang

# Mã sinh viên: B20DCAT144

# Giảng viên: Nguyễn Hoa Cương

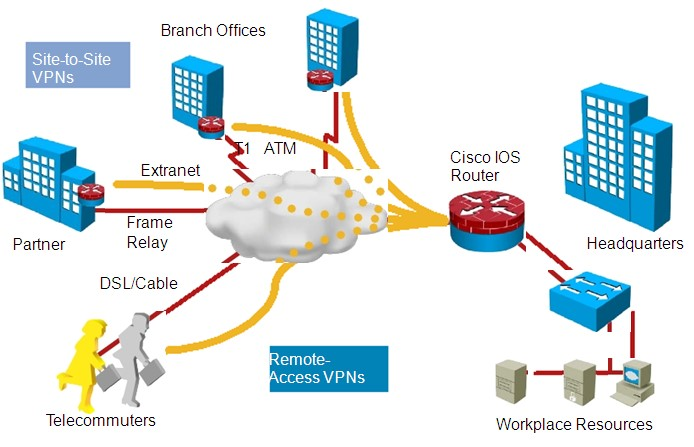
***Hà Nội – 2023***

**I. Lý thuyết:**

* Khái quát về VPN:

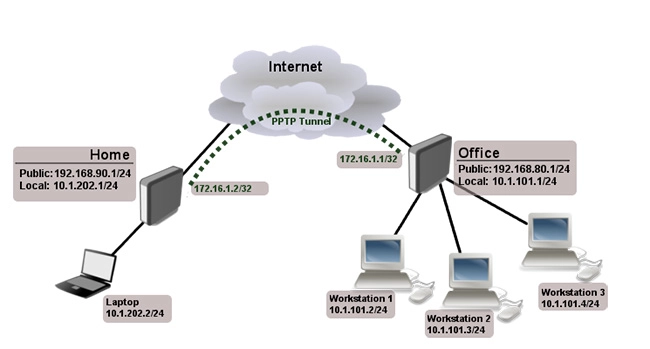
VPN là mạng riêng ảo, Virtual Private Network, là một công nghệ mạng giúp tạo kết nối mạng an toàn khi tham gia vào mạng công cộng như Internet hoặc mạng riêng do một nhà cung cấp dịch vụ sở hữu. Các tập đoàn lớn, các cơ sở giáo dục và cơ quan chính phủ sử dụng công nghệ VPN để cho phép người dùng từ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

* Các mô hình VPN:



* Một số ứng dụng của VPN:
* **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 game 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 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 bạn nên 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 tăng tốc độ tải file. Điều này cũng có ích với các traffic mà ISP của bạn có thể gây trở ngại.
* Tìm hiểu về các giao thức tạo đường hầm cho VPN: PPTP, L2TP, L2F, MPLS,…
* **Point-To-Point Tunneling Protocol (PPTP)**

PPTP không chỉ định giao thức mã hóa nhưng có thể sử dụng một số giao thức như MPPE-128 mạnh mẽ. Việc thiếu sự tiêu chuẩn hóa về giao thức mạng là một rủi ro, vì nó chỉ có thể sử dụng tiêu chuẩn mã hóa mạnh nhất mà cả 2 phía cùng hỗ trợ. Nếu một phía chỉ hỗ trợ tiêu chuẩn yếu hơn thì kết nối phải sử dụng mã hóa yếu hơn người dùng mong đợi



* **L2TP**

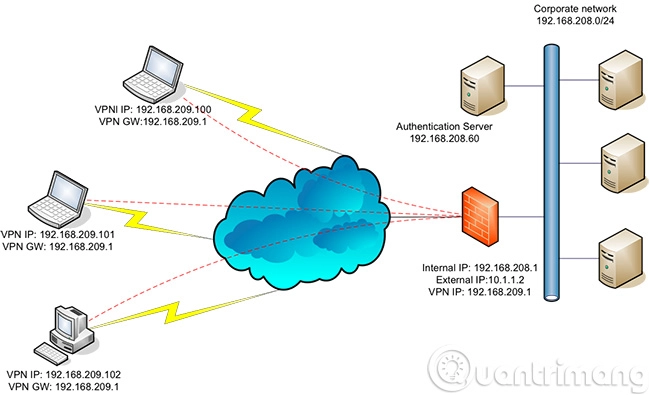
Giao thức L2TP thường hoạt động với thuật toán mã hóa IPSec. Nó mạnh hơn đáng kể so với PPTP nhưng vẫn khiến người dùng lo ngại. Lỗ hổng chính trong L2TP/IPSec là phương thức trao đổi khóa công khai (public key). Trao đổi khóa công khai Diffie-Hellman là cách để hai bên thỏa thuận về khóa mã hóa tiếp theo và không ai được biết về khóa này. Có một phương pháp có thể “bẻ khóa” quá trình này, đòi hỏi sức mạnh điện toán khá lớn, nhưng sau đó nó cho phép truy cập vào tất cả các giao tiếp trên một VPN nhất định.

* 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.

* **Tìm hiểu về SoftEther VPN**

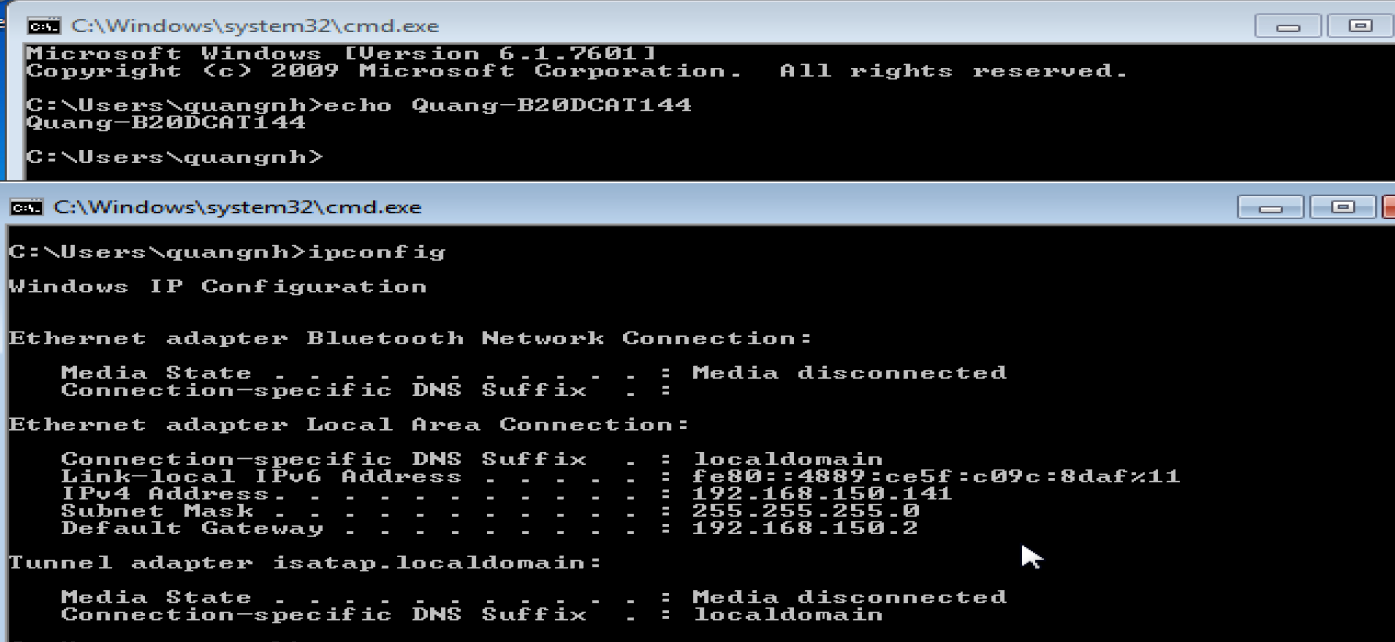
Softether là một dự án VPN tương đối mới giúp công nghệ VPN trở nên an toàn hơn, cho phép người dùng lướt web ẩn danh và BẢO MẬT cao hơn.

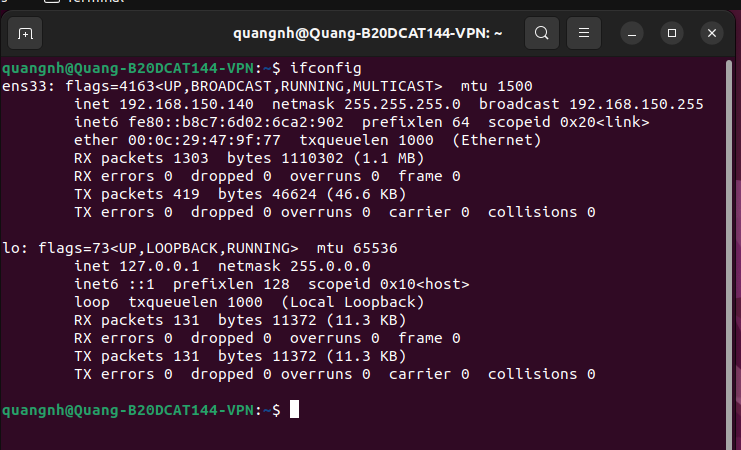
Hiện tại, SoftEther VPN hỗ trợ **Windows, Linux, Mac, Solaris, FreeBSD** và thường là một lựa chọn tốt để thay thế cho OpenVPN vì nhanh hơn. SoftEther VPN cũng hỗ trợ Microsoft SSTP VPN cho Windows Vista/7/8.

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.

**II. BÁO CÁO THỰC HÀNH**

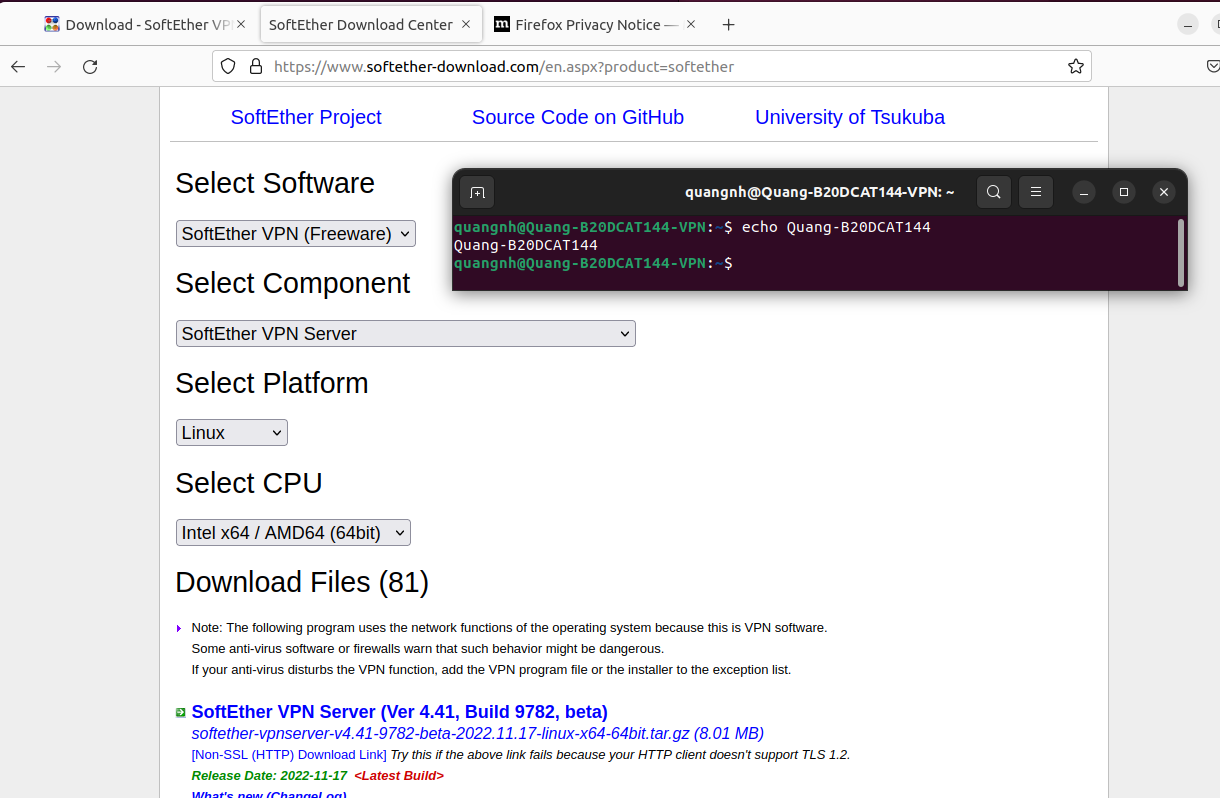
**1.Đổi tên máy và kiểm tra IP ( máy thật win , máy ảo linux)**

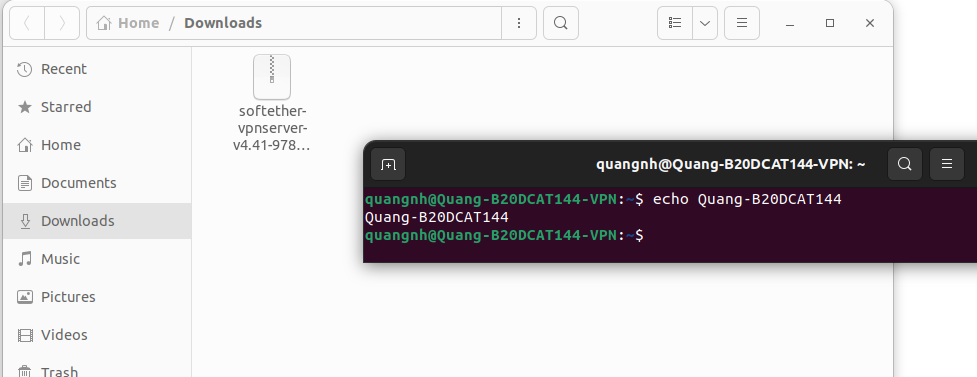


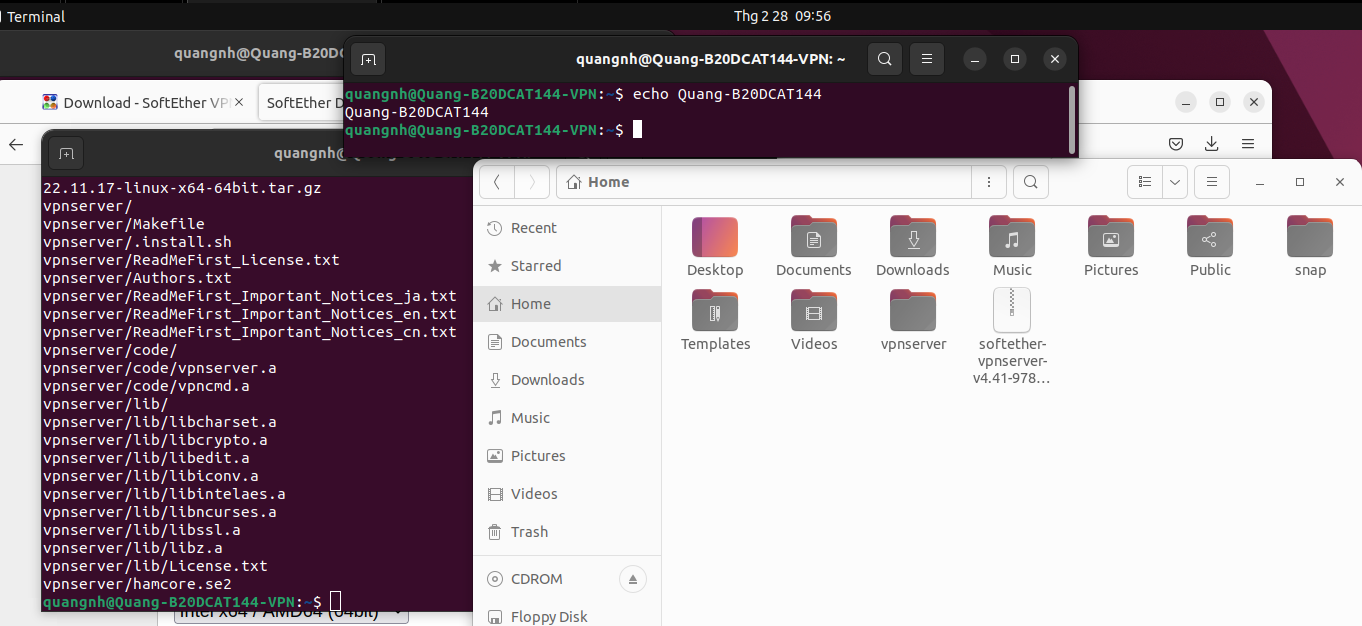


**2.Tải SoftEther VPN server , cài đặt và cấu hình VPN server**

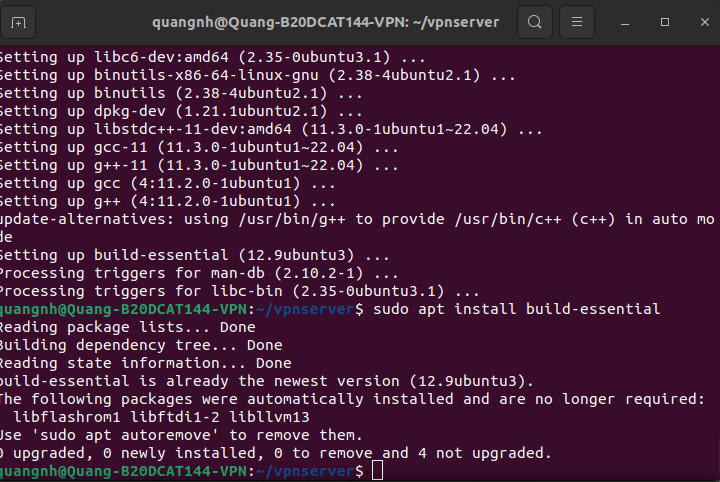
- Tải SoftEther VPN server trên máy Linux



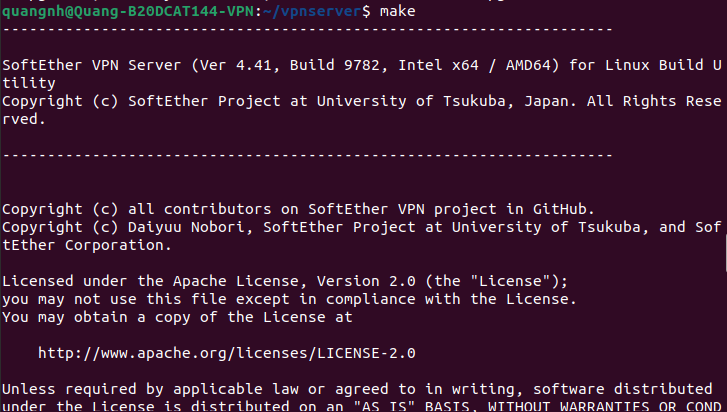




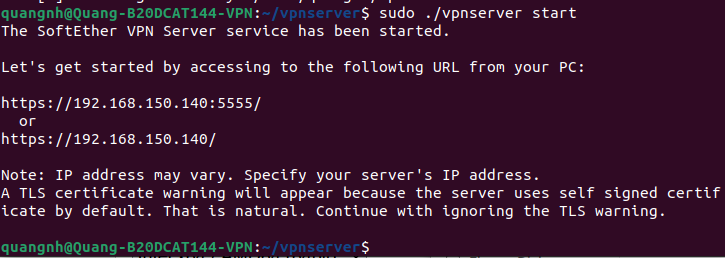
* Cài đặt GCC



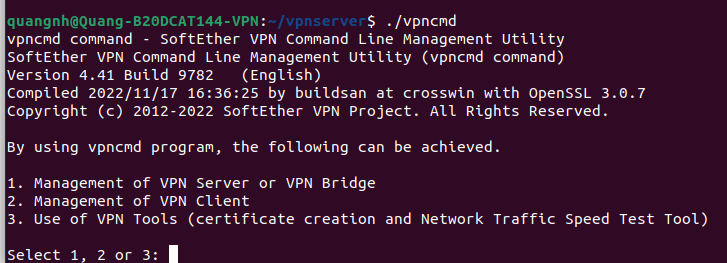
* Chuyển vào thư mục VPN server: cd vpnserver. Biên dịch và cài đặt: make (lưu ý hệ thống phải có sẵn trình biên dịch gcc)

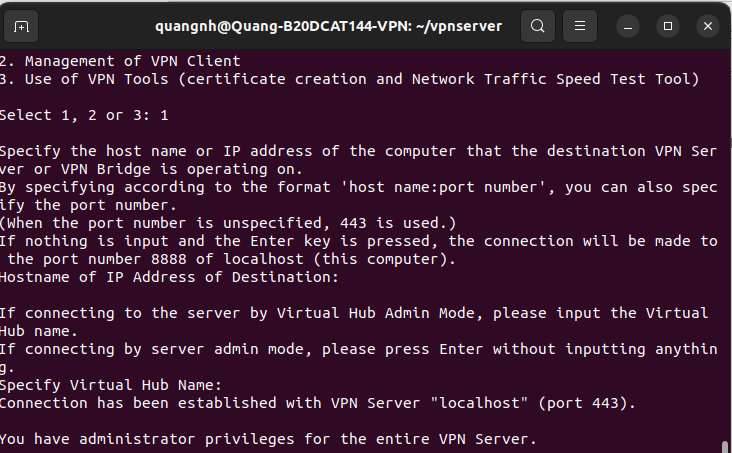


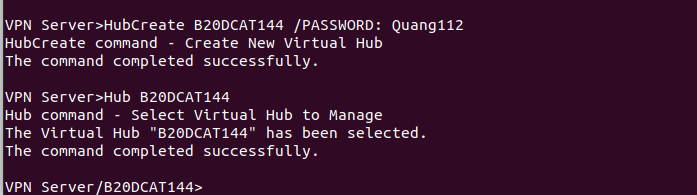
* Khởi động máy chủ VPN: sudo ./vpnserver star



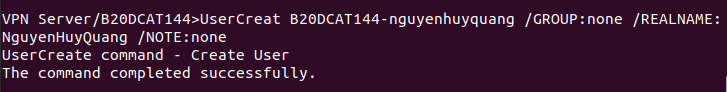
* Chạy tiện ích quản trị VPN Server: ./vpncmd (chọn chức năng số 1 và gõ Enter 2 lần để vào giao diện quản trị). Tạo Virtual Hub và tài khoản người dùng VPN trong giao diện quản trị:
* Tạo 1 -Virtual Hub mới: HubCreate ( là tên Virtual Hub - dùng mã sinh viên làm tên Virtual Hub)
* Chọn Virtual Hub đã tạo: Hub - Tạo 1 người dùng VPN mới: UserCreate /GROUP:none /REALNAME:Tên sinh viên /NOTE:none

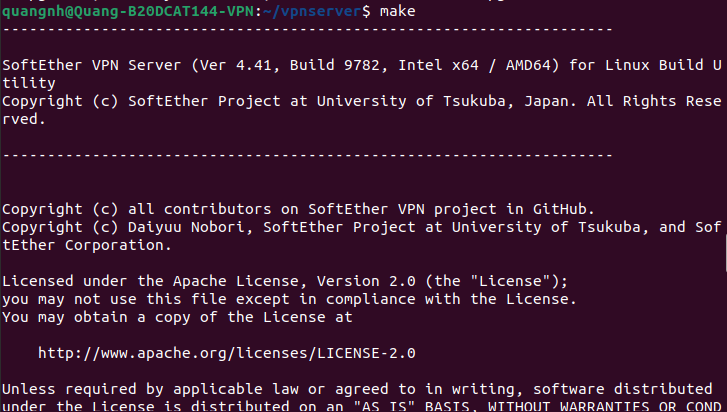




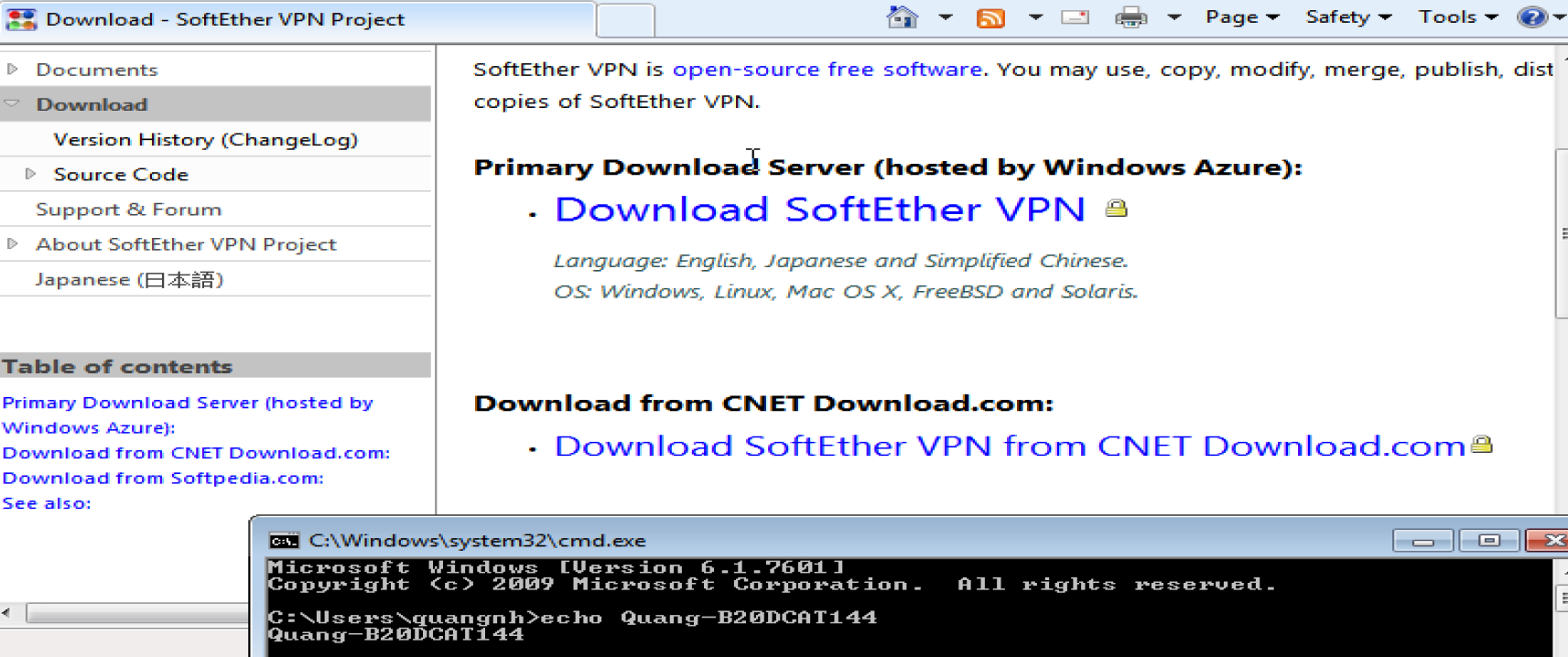


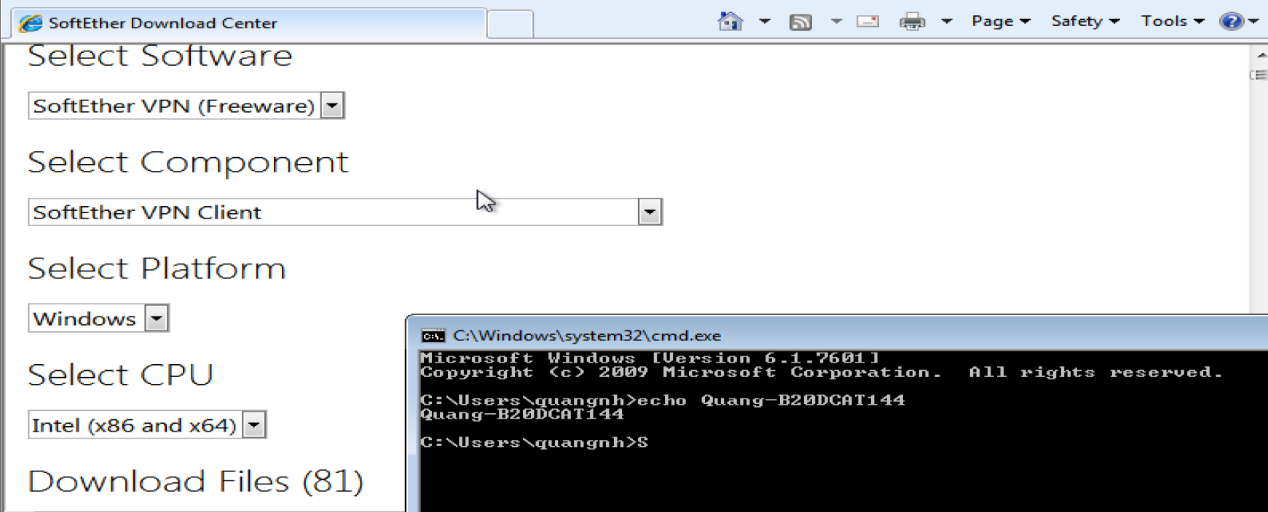
* Đặt mật khẩu cho người dùng: UserPasswordSet

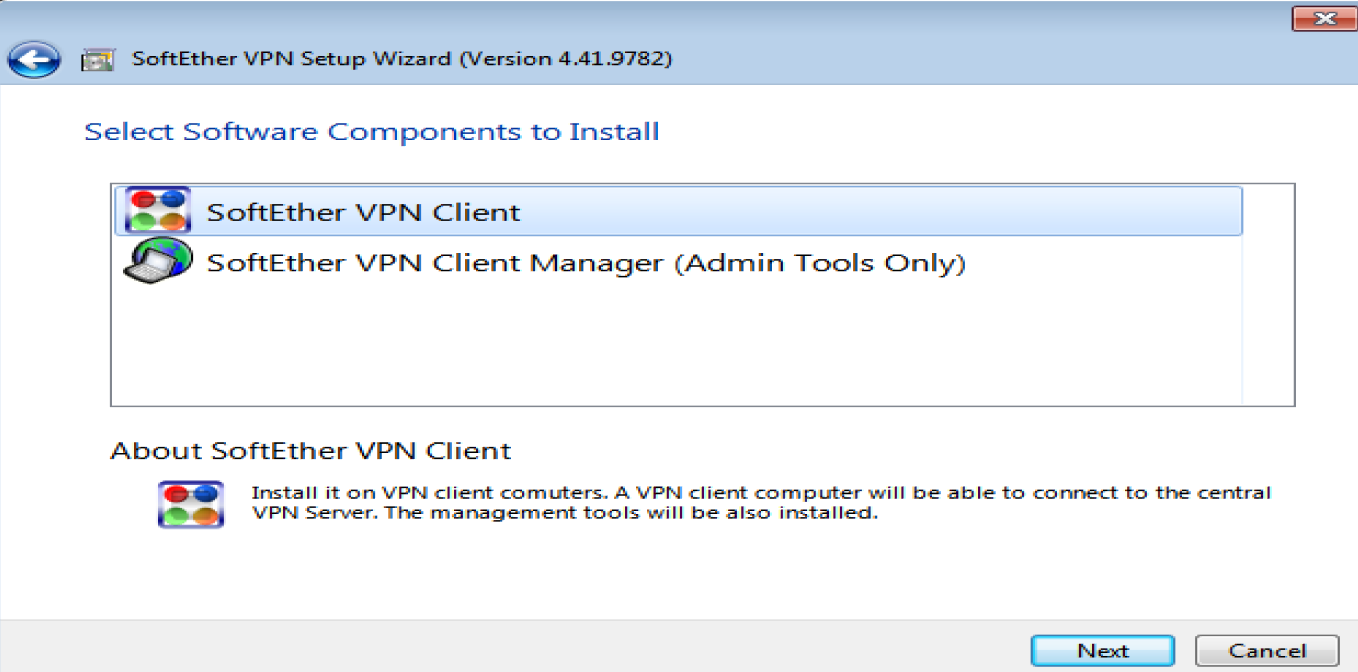


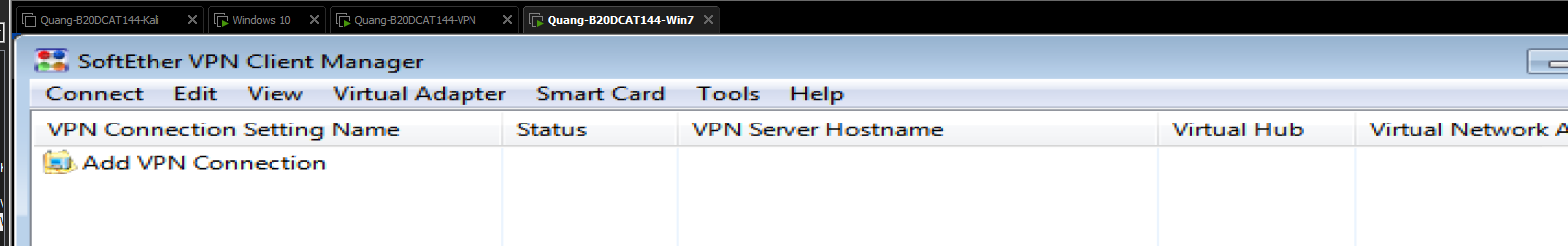


**3.Tải SoftEther VPN client cho Windows**









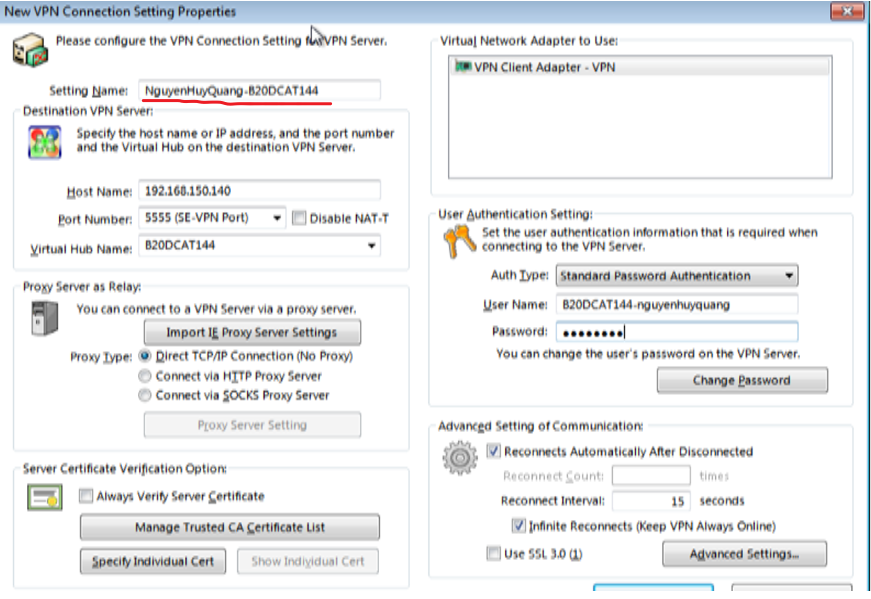
1. Tạo và kiểm tra kết nối VPN

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

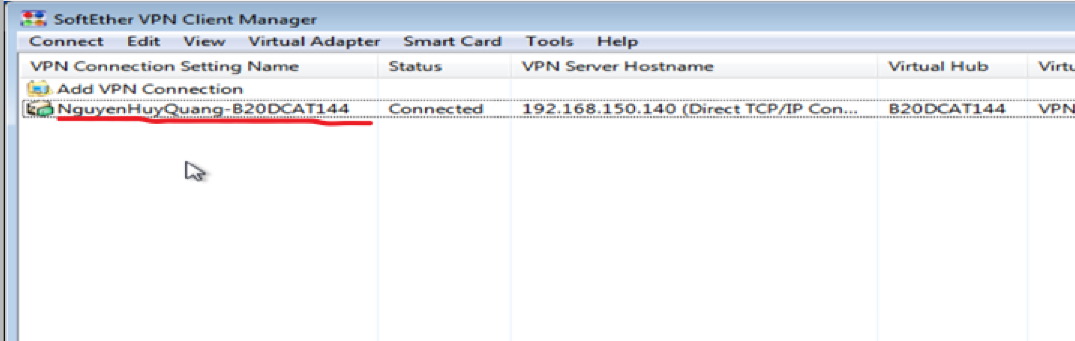
Với địa chỉ IP của máy chủ VPN − tên Virtual Hub,

tên và mật khẩu người dùng.

Đặt tên kết nối là <Mã sinh viên> - <Họ tên>

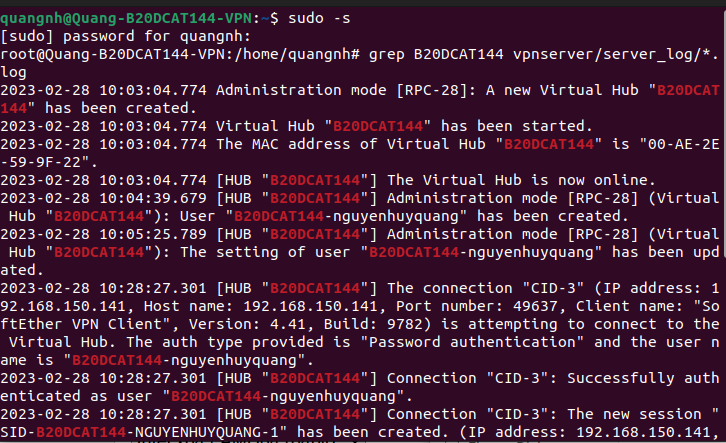


* Thử kết nối: Nếu thành công sẽ báo connected

****

* 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

==> Hiển thị các dòng log có liên quan đến <Mã sinh viên>



* Xem file server\_log bằng cách thay đổi quyền

