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

Môn: Thực tập cơ sở

BÀI BÁO THỰC TẬP CƠ SỞ

Bài 7: Cài đặt cấu hình VPN server

Họ và tên giảng viên:	TS. Đinh Trường Duy
Họ và tên:	Nguyễn Quốc Khánh
Mã sinh viên:	B20DCAT103
Lớp:	D20CQAT03-B
Số điện thoại:	0964137761

Hà Nội 2023

1. Nội dung lý thuyết

a. Khái quát về VPN

VPN (virtual private network) là công nghệ cho phép mở rộng một mạng riêng trên mạng công cộng và cho phép người dùng gửi và nhận dữ liệu trên các mạng dùng chung hoặc mạng công cộng như thể các thiết bị máy tính của họ được kết nối trực tiếp với mạng riêng. Kết nối VPN thường được mã hóa. VPN được tạo ra bằng cách thiết lập một kết nối điểm ảo thông qua việc sử dụng các mạch chuyên dụng hoặc với các giao thức đường hầm qua các mạng hiện có. VPN có sẵn từ Internet công cộng có thể cung cấp một số lợi ích của mạng diện rộng (WAN). Từ góc độ người dùng, các tài nguyên có sẵn trong mạng riêng có thể được truy cập từ xa.

VPN mang lại một số lợi ích như 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 những người làm việc từ xa.

VPN có một số mô hình như truy cập từ xa, kết nối các mạng cục bộ(site-to-site), kết nối các mạng thuộc nhiều tổ chức(extranet site-to-site).

b. Một số giao thức tạo đường hầm cho VPN

PPTP (Point-to-Point Tunneling Protocol) được coi là phương thức đào đường hầm kém an toàn nhất giao thức. Nó cũng là giao thức lâu đời nhất trong số các giao thức. Nó được tạo ra bởi Microsoft và phát hành cùng với Windows 95. Tất cả những gì người dùng cần là tên người dùng và mật khẩu với địa chỉ máy chủ để thực hiện kết nối. PPTP là giao thức đường hầm VPN nhanh nhất vì mức độ mã hóa của nó thấp.

Giao thức đường hầm lớp 2 tốt hơn PPTP về mặt bảo mật, nhưng PPTP

có tốc độ nhanh hơn L2TP. Dữ liệu và lưu lượng đi qua đường hầm này được mã hóa bằng Bảo mật Giao thức Internet (IPSec). 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.

Chuyển đổi nhãn đa giao thức (MPLS) là một công nghệ đường hầm được sử dụng trong nhiều mạng lưới nhà cung cấp dịch vụ. Ứng dụng hỗ trợ MPLS phổ biến nhất được sử dụng hiện nay là VPN MPLS. Các VPN MPLS được phát triển để vận hành trên các mạng MPLS, nhưng chúng cũng có thể chạy trên các mạng IP gốc.

L2F, (Layer 2 Forwarding), là một giao thức đường hầm được phát triển bởi Cisco Systems, Inc. để thiết lập các kết nối mạng riêng ảo qua internet. L2F không cung cấp mã hóa hoặc bảo mật, nó dựa vào giao thức sử dụng đường hầm để cung cấp quyền riêng tư. L2F được thiết kế đặc biệt cho lưu lượng giao thức điểm-điểm (PPP) của đường hầm.

c. Các giao thức bảo mật cho VPN:

Internet Protocol Security (IPsec) là phương pháp bảo mật VPN truyền thống. Được giới thiệu vào những năm 1990, nó được thiết lập tốt, cập nhật thường xuyên và tiếp tục được sử dụng rộng rãi. IPsec yêu cầu phần mềm máy khách(client) của bên thứ ba trên thiết bị của người dùng để truy cập VPN — nó không thể triển khai thông qua trình duyệt web. Các công ty cần mua phần mềm máy khách, cài đặt phần mềm đó trên máy tính của mỗi người dùng, cập nhật phần mềm đó và đôi khi trả tiền để duy trì giấy phép của họ. Điều này làm cho IPsec khá phức tạp để thực hiện và cấu hình. Mục đích của IPsec là cung cấp cho máy tính từ xa quyền truy cập trực tiếp vào mạng trung tâm, biến nó thành một thành viên đầyđủ.

Người dùng từ xa có quyền truy cập vào bất kỳ vị trí lưu trữ tệp, chương trình, máy in và bản sao lưu nào, chính xác như thể họ đang ở trong văn phòng. Do đó, IPsec là một hệ thống mạnh mẽ cung cấp cho người dùng bất kỳ tài nguyên nào họ cần, dù họ ở đâu.

Secure Sockets Layer (SSL) là đối thủ chính của IPsec với tư cách là một giao thức VPN. Mặc dù nguồn gốc của nó cũng bắt nguồn từ những năm 1990, SSL là một phương pháp gần đây hơn để triển khai VPN và nó đang ngày càng trở nên phổ biến. Giao thức SSL đã được thay thế bằng công nghệ kế nhiệm, Transport Layer Security (TLS), vào năm 2015, nhưng các thuật ngữ có thể hoán đổi cho nhau theo cách nói thông thường và "SSL" vẫn được sử dụng rộng rãi. SSL VPN được triển khai thông qua trình duyệt web của người dùng từ xa và không yêu cầu cài đặt phần mềm đặc biệt. Tất cả các trình duyệt web chính — bao gồm Chrome, Firefox, Internet Explorer và Safari — đều có hỗ trợ SSL. Điều này giúp SSL dễ dàng thiết lập và sử dụng, đặc biệt là khi một thành viên trong nhóm cài đặt nó mà không có sự trợ giúp của bộ phận hỗ trợ kỹ thuật.

d. Tìm hiểu về SoftEther VPN

Softether VPN cho đến nay là một trong những phần mềm VPN đa giao thức mạnh mẽ và thân thiện nhất cho người dùng trên thị trường. Được định vị là sự thay thế lý tưởng cho OpenVPN, Softether VPN có chức năng nhân bản cho máy chủ OpenVPN cho phép di chuyển liền mạch từ OpenVPN sang Softether VPN. Các tiêu chuẩn và khả năng bảo mật ấn tượng của Softether được coi là tương đương với những phần mềm phổ biến như NordVPN, nhưng nó có ưu điểm của phần mềm mã nguồn mở.

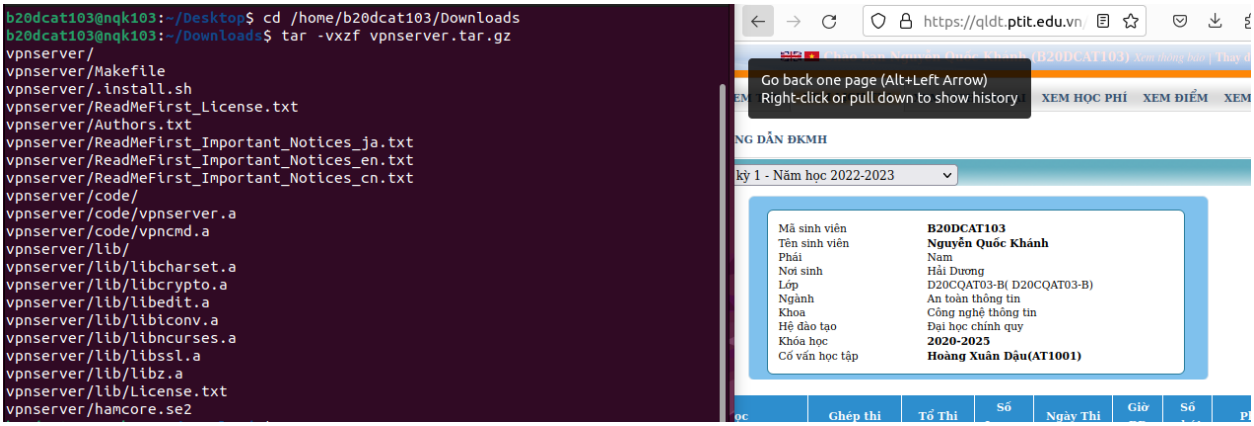
Softether cũng tương thích với các giao thức L2TP và IPSEC, và cho phép tùy chỉnh thêm. Hơn nữa, VPN SoftEther đã được chứng minh là thậm chí còn nhanh hơn OpenVPN, cải thiện trải nghiệm duyệt web. Hạn chế chính hiện

nay của SoftEther là nó tụt hậu so với những phần mềm khác về khả năng tương thích.

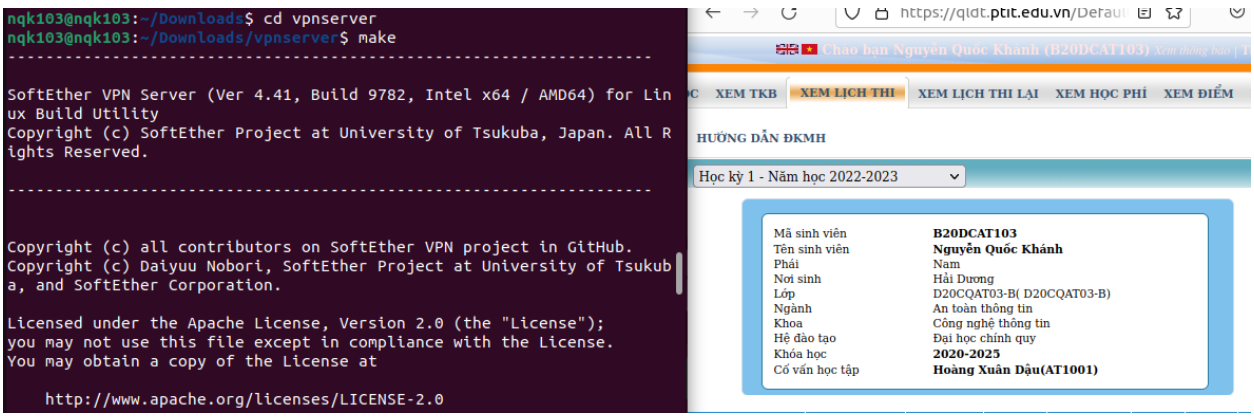
Ngoài Softether VPN, còn có những phần mềm VPN nổi bật khác như OpenVPN, phần mềm mã nguồn mở khả năng bảo mật cao và tương thích với nhiều nền tảng; Tcpcrypt, giải pháp VPN đặc biệt trên Windows và MacOS, không yêu cầu cấu hình, thay đổi đối với các ứng dụng hoặc sự thay đổi đáng chú ý trong kết nối mạng, hoạt động bằng cách sử dụng "mã hóa cơ hội"(opportunistic encryption),...

2. Nội dung thực hành

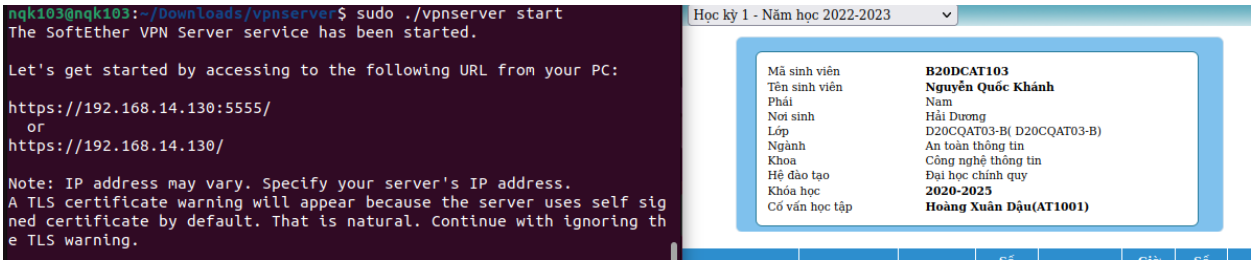
Tải về và giải nén file cài đặt chương trình SoftEther VPN server, và chuyển vào thư mục vpnserver:



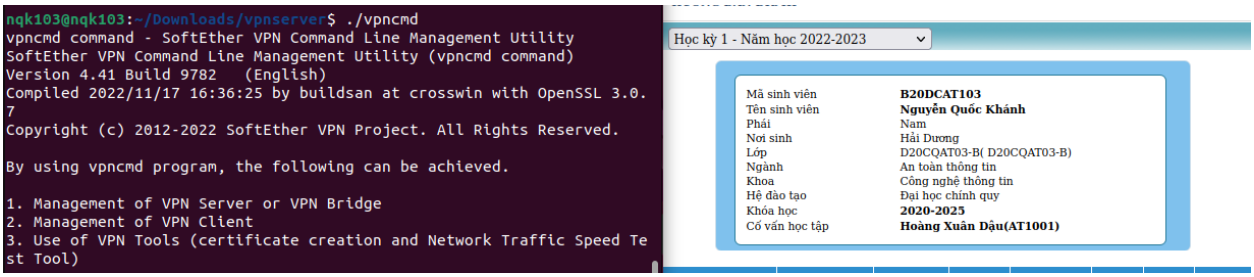
Biên dịch và cài đặt chương trình SoftEther VPN server:



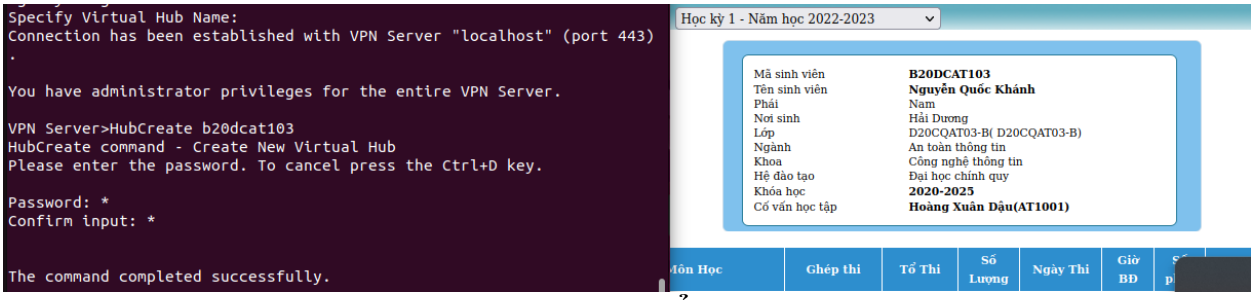
Khởi động máy chủ VPN:



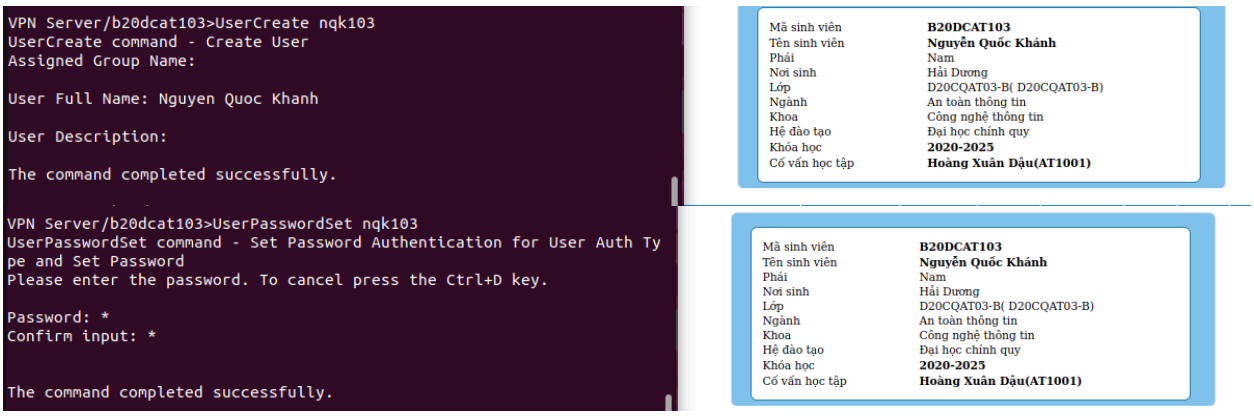
Chạy tiện ích quản trị VPN Server:



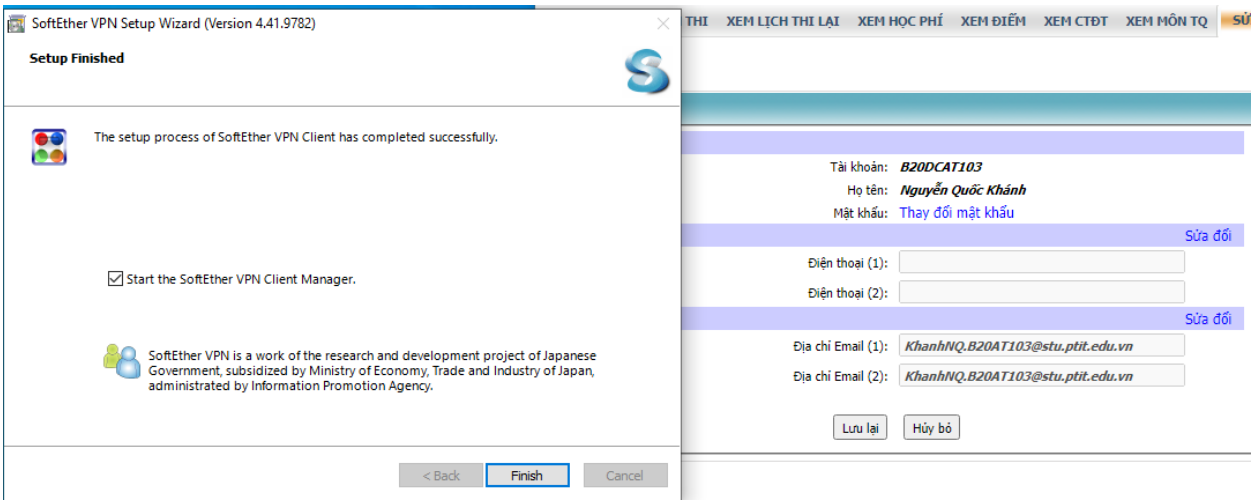
Tạo 1 Virtual Hub mới:



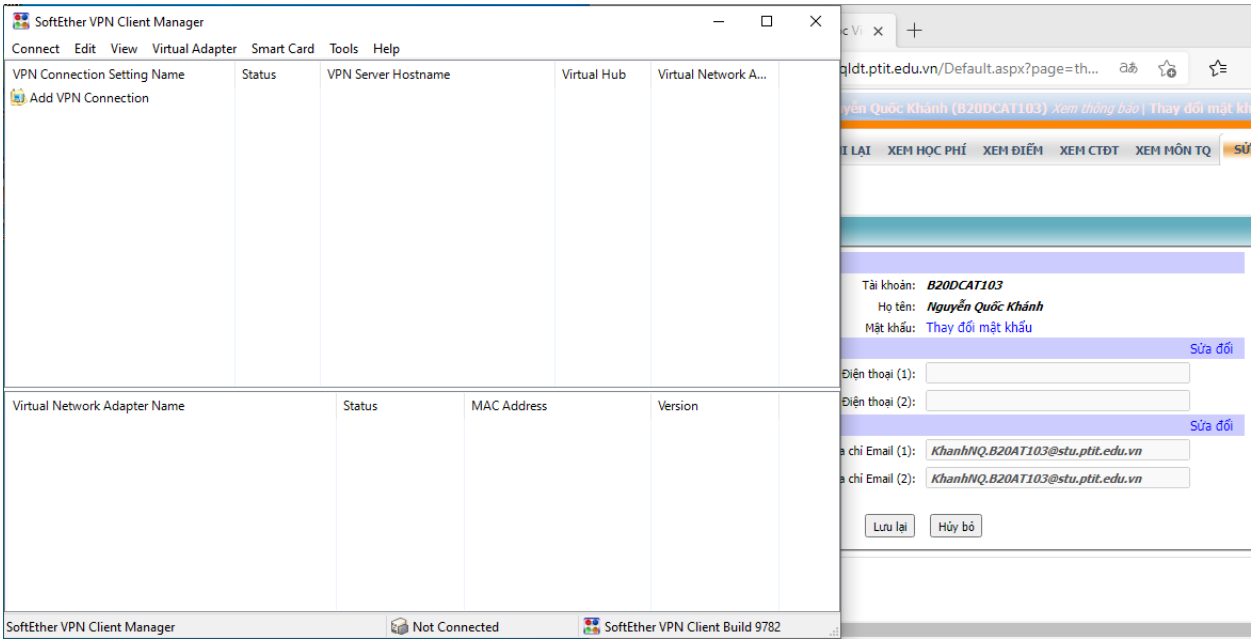
Tạo 1 người dùng VPN mới và đặt mật khẩu cho người dùng:



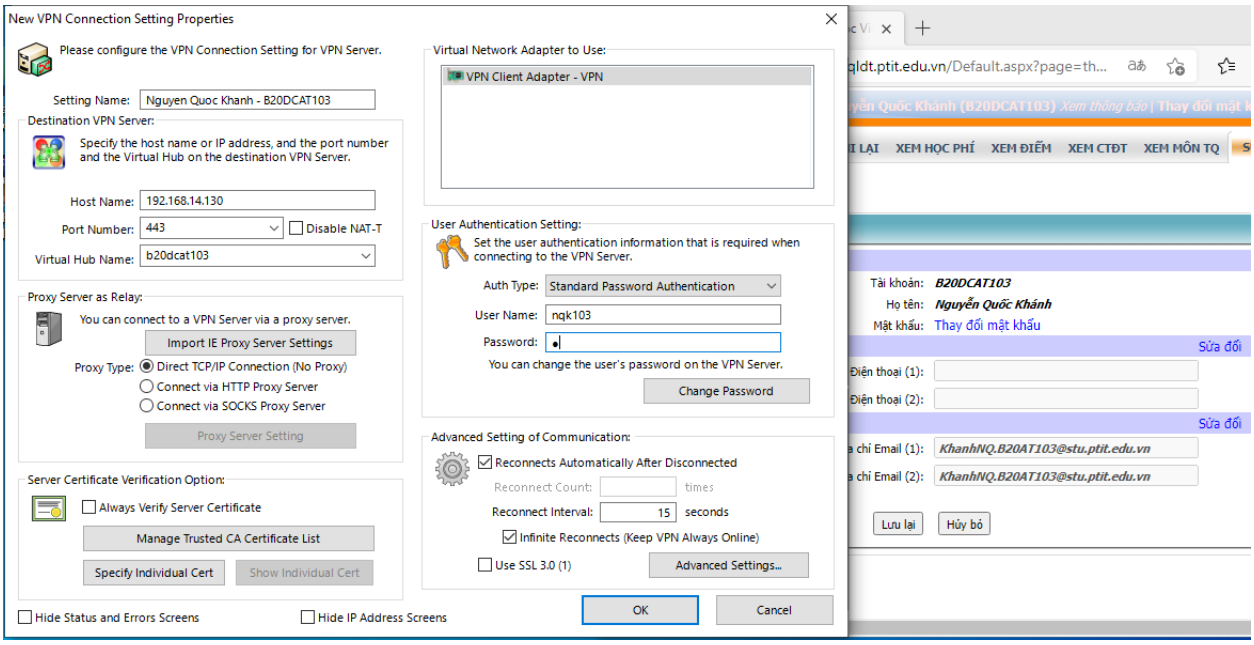
Tải, cài đặt thành công SoftEther VPN client:



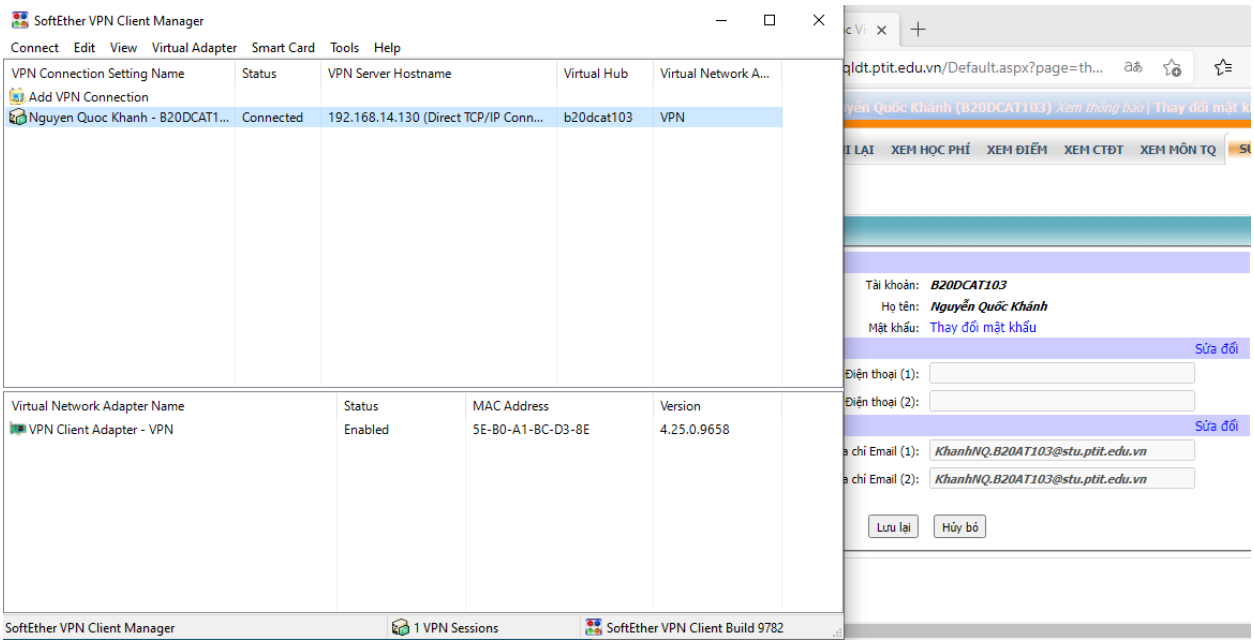
Khởi động thành công SoftEther VPN client:



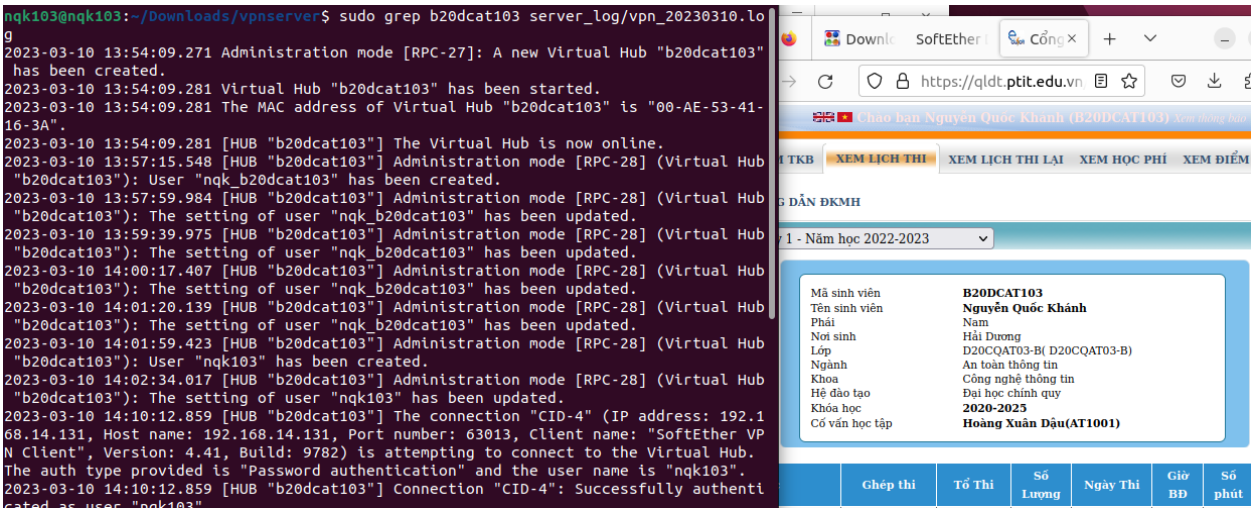
Từ giao diện SoftEther VPN Client Manager, tạo 1 kết nối mới:



Thử kết nối thành công:



Kiểm tra kết nối bên máy chủ thành công, hiển thị các dòng log có liên quan:



```
nqk103@nqk103:~/Downloads/vpnserver$ sudo grep b20dcat103 server_log/vpn_20230310.log
2023-03-10 13:54:09.271 Administration mode [RPC-27]: A new Virtual Hub "b20dcat103" has been created.
2023-03-10 13:54:09.281 Virtual Hub "b20dcat103" has been started.
2023-03-10 13:54:09.281 The MAC address of Virtual Hub "b20dcat103" is "00-AE-53-41-16-3A".
2023-03-10 13:54:09.281 [HUB "b20dcat103"] The Virtual Hub is now online.
2023-03-10 13:57:15.548 [HUB "b20dcat103"] Administration mode [RPC-28] (Virtual Hub "b20dcat103"): User "nqk_b20dcat103" has been created.
2023-03-10 13:57:59.984 [HUB "b20dcat103"] Administration mode [RPC-28] (Virtual Hub "b20dcat103"): The setting of user "nqk_b20dcat103" has been updated.
2023-03-10 13:59:39.975 [HUB "b20dcat103"] Administration mode [RPC-28] (Virtual Hub "b20dcat103"): The setting of user "nqk_b20dcat103" has been updated.
2023-03-10 14:00:17.407 [HUB "b20dcat103"] Administration mode [RPC-28] (Virtual Hub "b20dcat103"): The setting of user "nqk_b20dcat103" has been updated.
2023-03-10 14:01:20.139 [HUB "b20dcat103"] Administration mode [RPC-28] (Virtual Hub "b20dcat103"): The setting of user "nqk_b20dcat103" has been updated.
2023-03-10 14:01:59.423 [HUB "b20dcat103"] Administration mode [RPC-28] (Virtual Hub "b20dcat103"): User "nqk103" has been created.
2023-03-10 14:02:34.017 [HUB "b20dcat103"] Administration mode [RPC-28] (Virtual Hub "b20dcat103"): The setting of user "nqk103" has been updated.
2023-03-10 14:10:12.859 [HUB "b20dcat103"] The connection "CID-4" (IP address: 192.168.14.131, Host name: 192.168.14.131, Port number: 63013, Client name: "SoftEther VPN Client", Version: 4.41, Build: 9782) is attempting to connect to the Virtual Hub.
The auth type provided is "Password authentication" and the user name is "nqk103".
2023-03-10 14:10:12.859 [HUB "b20dcat103"] Connection "CID-4": Successfully authenticated as user "nqk103"
```