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**: PGS.TS.Đỗ Xuân Chợ*
***Họ và tên:** Phạm Thanh Tùng*
***Mã sinh viên:** B20DCAT171*
***Lớp:** D20CQAT03-B*
***Số điện thoại:** 0856915668*

Hà Nội 2023

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*

   - VPN là từ viết tắt của Virtual Private Network, hay còn gọi là mạng riêng ảo, mạng ảo, giúp tạo nên những kết nối mạng an toàn khi tham gia mạng riêng của nhà cung cấp dịch vụ hoặc mạng công cộng internet.
   - Chức năng VPN:
     - Truy cập dễ dàng tới website bị chặn, giới hạn địa lý
     - Truy cập vào mạng gia đình dù không ở nhà
     - Truy cập mạng doanh nghiệp từ xa
     - Duyệt web ẩn danh
   - Các mô hình VPN:
     - PPTP VPN
     - Site-to-Site VPN
     - SSL and TLS
     - L2TP VPN
     - IPsec
     - SSL and TLS
   - Các giao thức tạo đường hầm: giao thức tạo đường hầm cho VPN:
     - PPTP: Ý tưởng cơ sở của giao thức này là tách các chức năng chung và riêng của truy cập từ xa, lợi dụng cơ sở hạ tầng Internet sẵn có để tạo kết nối bảo mật giữa người dùng ở xa (client) và mạng riêng.
     - L2TP: iống như PPTP, L2TP là giao thức đường hầm, nó sử dụng tiêu đề đóng gói riêng cho việc truyền các gói ở lớp 2. Một điểm khác biệt chính giữa L2F và PPTP là L2F không phụ thuộc vào IP và GRE, cho phép nó có thể làm việc ở môi trường vật lý khác.
   - Các giao thức bảo mật cho VPN:
     - IPsec tạo những đường hầm bảo mật xuyên qua mạng Internet để truyền những luồng dữ liệu. Mỗi đường hầm bảo mật là một cặp những kết hợp an ninh để bảo vệ luồng dữ liệu giữa hai Host. IPSec định nghĩa 2 loại tiêu đề cho các gói IP để điều

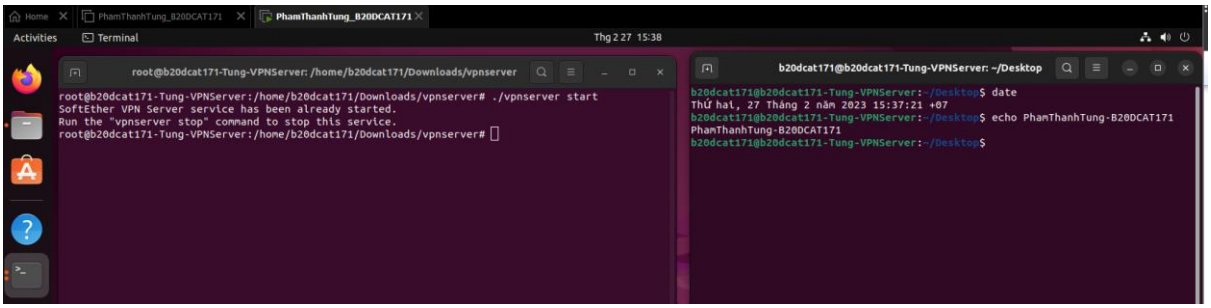
khiển quá trình xác thực và mã hoá: một là xác thực tiêu đề IP – AH (IP Authentication Header) điều khiển việc xác thực và hai là đóng gói tải tin an toàn ESP (Encapsulation Security Payload) cho mục đích mã hoá.

- SSL/TLS: hoạt động bằng cách tích hợp key mã hóa vào thông tin định danh người dùng. Nó sẽ giúp người dùng mã hóa mọi thông tin được truyền mà không bị ảnh hưởng hoặc chỉnh sửa bởi các bên thứ 3. SSL/TLS hoạt động bằng cách sử dụng public và private key, đồng thời các khóa duy nhất của mỗi phiên giao dịch. Mỗi khi khách truy cập điền vào thanh địa chỉ SSL thông tin web browser hoặc chuyển hướng tới trang web được bảo mật, trình duyệt và web server đã thiết lập kết nối.

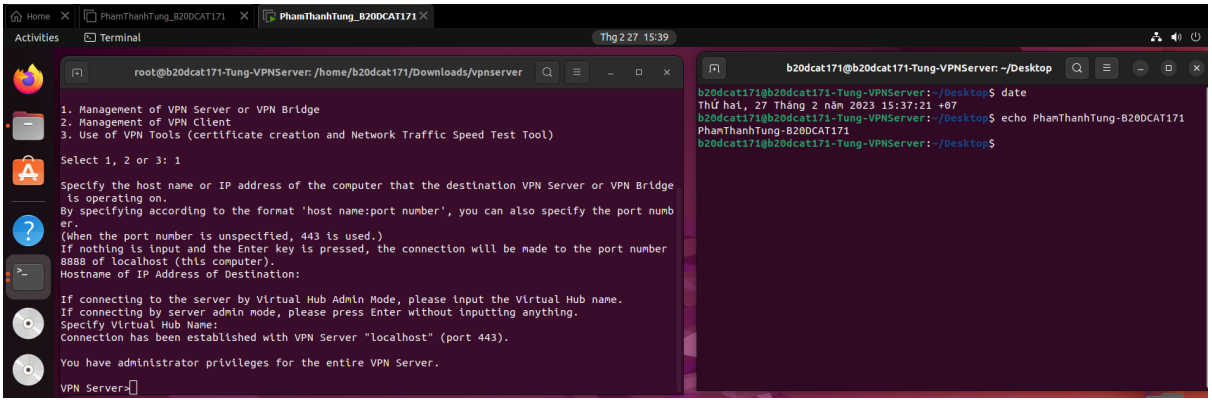
- SoftEther VPN: là phần mềm máy chủ VPN và máy khách VPN đa giao thức, mã nguồn mở , đa nền tảng, miễn phí, được phát triển như một phần của nghiên cứu luận văn thạc sĩ của Daiyuu Nobori tại Đại học Tsukuba .
    - SoftEther VPN tối ưu hóa hiệu suất bằng cách sử dụng toàn bộ khung Ethernet, giảm hoạt động sao chép bộ nhớ, truyền song song và phân cụm. Cùng với nhau, những điều này làm giảm độ trễ thường được kết hợp với các kết nối VPN đồng thời tăng thông lượng.

2.2. Các bước thực hiện:

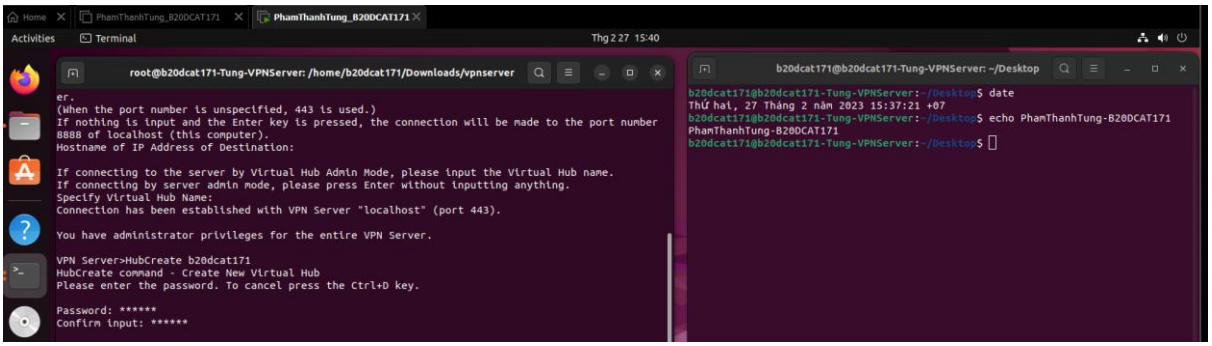
- Tải SoftEther VPN server tại https://www.softether.org/5-download.
    - Giải nén file cài đặt
    - Chuyển vào thư mục VPN server
    - Khởi động máy chủ VPN



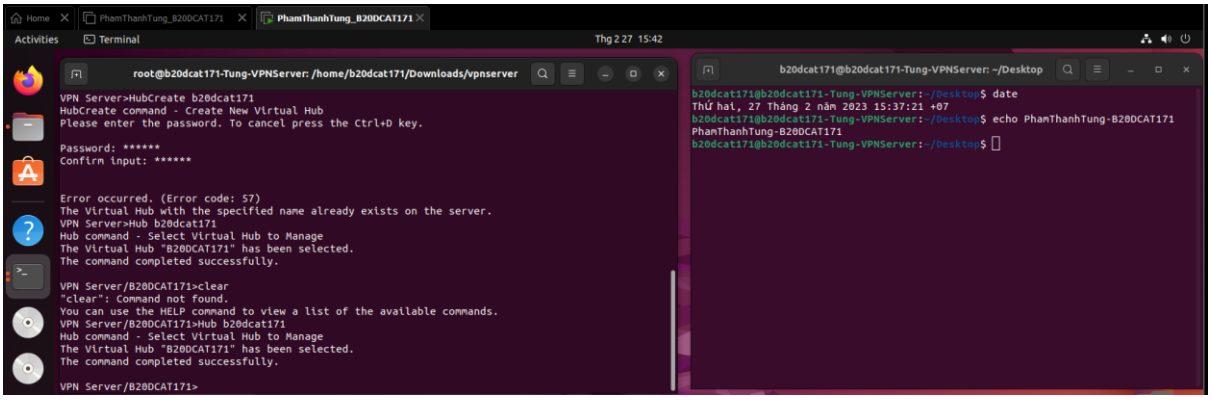
- Chạy tiện ích quản trị VPN Server: ./vpncmd (chọn chức năng số 1 và gõ Enter 2 lần để vào giao diện quản trị). Tạo Virtual Hub và tài khoản người dùng VPN trong giao diện quản trị



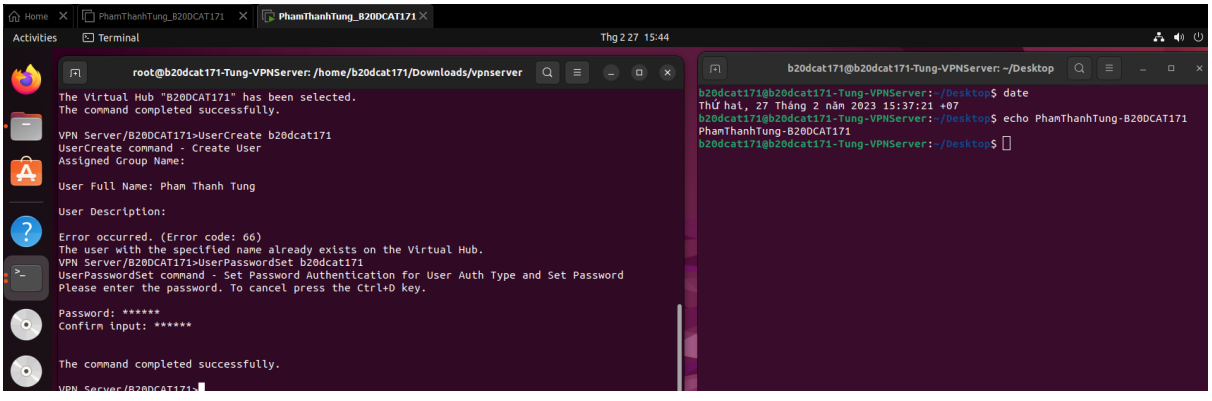
- Tạo 1 Virtual Hub mới:



- Chọn Virtual Hub đã tạo



- Tạo 1 người dùng VPN mới, đặt mật khẩu cho người dùng:



- Tải SoftEther VPN client cho Windows:
- Tạo và kiểm tra kết nối VPN.