

**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:

B22DCAT199 Đỗ Duy Nam

Giảng viên hướng dẫn: TS.Đình Trường Duy

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

MỤC LỤC	2
DANH MỤC CÁC HÌNH VẼ.....	3
CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH	4
1.1 Mục đích.....	4
1.2 Tìm hiểu lý thuyết	4
1.2.1 Khái quát về VPN, các mô hình và ứng dụng của VPN	4
a) Khái quát về VPN	4
b) Các mô hình VPN	4
c) Ứng dụng của VPN	5
1.2.2 Các giao thức tạo đường hầm cho VPN	7
1.2.3 Các giao thức bảo mật cho VPN	9
1.2.4 SoftEther VPN.....	10
a) SoftEther VPN là gì?	10
b) Các giao thức được hỗ trợ	11
c) Cách hoạt động.....	11
d) Ưu điểm.....	11
e) Nhược điểm.....	12
f) Ứng dụng thực tế.....	12
1.3 Kết luận	12
CHƯƠNG 2. NỘI DUNG THỰC HÀNH	13
2.1 Chuẩn bị môi trường	13
2.2 Các bước thực hiện.....	13
2.3 Kết luận	23
KẾT LUẬN	24
TÀI LIỆU THAM KHẢO	25

DANH MỤC CÁC HÌNH VẼ

Hình 1 Đổi tên máy cài VPN Server	13
Hình 2 Đổi tên máy cài VPN Client.....	14
Hình 3 Tải phần mềm Softether VPN Server về máy Linux	15
Hình 4 Giải nén file	16
Hình 5 Chuyển vào thư mục VPN Server	16
Hình 6 Biên dịch và cài đặt VPN Server.....	17
Hình 7 Khởi động máy chủ VPN Server.....	18
Hình 8 Chạy tiện ích quản trị VPN Server.....	19
Hình 9 Tạo Virtual Hub mới	19
Hình 10 Chọn Virtual Hub đã tạo	20
Hình 11 Tạo người dùng VPN mới.....	20
Hình 12 Đặt mật khẩu cho người dùng vừa tạo	20
Hình 13 Thoát khỏi tiện ích quản trị VPN Server.....	21
Hình 14 Tải SoftEther VPN Client cho máy Windows	21
Hình 15 Tạo kết nối mới trên SoftEther VPN Client	22
Hình 16 Kết nối thành công VPN Server từ máy VPN Client	23
Hình 17 Kiểm tra log trên VPN Server	23

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 Khái quát về VPN, các mô hình và ứng dụng của VPN

a) Khái quát về VPN

VPN (Virtual Private Network - Mạng riêng ảo) là một công nghệ cho phép tạo ra một kết nối mạng an toàn qua một mạng công cộng như Internet. VPN mã hóa dữ liệu người dùng và định tuyến nó qua một máy chủ từ xa (VPN server), giúp che giấu địa chỉ IP thực của người dùng và bảo vệ thông tin khỏi bị theo dõi hoặc đánh cắp. Nói đơn giản, VPN hoạt động như một "đường hầm" bảo mật giữa thiết bị của bạn và mạng mà bạn truy cập.

- Cách hoạt động:
 - Dữ liệu được mã hóa trước khi gửi qua Internet, giúp bảo vệ khỏi tin tặc và gián điệp mạng.
 - Địa chỉ IP thực của bạn bị ẩn, thay thế bằng IP của máy chủ VPN, giúp che giấu danh tính và vị trí thực tế.
 - Kết nối giữa thiết bị của bạn và máy chủ VPN được bảo vệ, tránh bị nghe lén hoặc đánh cắp dữ liệu.
- Các giao thức VPN phổ biến:
 - IPsec (Internet Protocol Security): Bảo mật dữ liệu bằng mã hóa và xác thực.
 - OpenVPN: Mã nguồn mở, an toàn và phổ biến nhất.
 - L2TP/IPsec (Layer 2 Tunneling Protocol): Kết hợp giữa L2TP và IPsec để tăng cường bảo mật.
 - WireGuard: Giao thức mới, nhanh và an toàn hơn các giao thức truyền thống.
 - SSL/TLS VPN: Dùng trong VPN Remote Access để truy cập web an toàn.

b) Các mô hình VPN

VPN được phân loại dựa trên mục đích sử dụng, cách triển khai và công nghệ áp dụng. Dưới đây là các mô hình phổ biến:

- **Site-to-Site VPN**
 - Mô tả: Kết nối hai hoặc nhiều mạng nội bộ (LAN) tại các địa điểm khác nhau thông qua Internet, tạo thành một mạng riêng ảo liên kết.
 - Đặc điểm: Không yêu cầu người dùng cuối cài đặt phần mềm VPN trên thiết bị cá nhân; kết nối được thiết lập giữa các bộ định tuyến hoặc tường lửa.
 - Công nghệ: Sử dụng giao thức IPsec (Internet Protocol Security) hoặc MPLS (Multiprotocol Label Switching).
- **Remote Access VPN**
 - Mô tả: Cho phép người dùng cá nhân kết nối từ xa vào một mạng nội bộ hoặc máy chủ thông qua Internet.
 - Đặc điểm: Người dùng cần cài đặt phần mềm VPN hoặc cấu hình thiết bị để truy cập.
 - Công nghệ: Sử dụng các giao thức như PPTP (Point-to-Point Tunneling Protocol), L2TP/IPsec (Layer 2 Tunneling Protocol), hoặc OpenVPN.
- **Client-to-Site VPN**
 - Mô tả: Một dạng của Remote Access VPN, tập trung vào việc người dùng cá nhân kết nối đến một máy chủ VPN cụ thể từ thiết bị của họ.
 - Đặc điểm: Phổ biến trong các dịch vụ VPN thương mại, dễ sử dụng với giao diện thân thiện.
 - Công nghệ: Thường sử dụng OpenVPN, WireGuard, hoặc IKEv2.
- **Peer-to-Peer VPN**
 - Mô tả: Không sử dụng máy chủ trung tâm; các thiết bị kết nối trực tiếp với nhau trong một mạng ngang hàng.
 - Đặc điểm: Phi tập trung, phụ thuộc vào phần mềm chuyên dụng để thiết lập kết nối.
 - Công nghệ: Các công cụ như Hamachi, ZeroTier hoặc Tinc.
- **Cloud VPN**
 - Mô tả: VPN được triển khai trên nền tảng đám mây, kết nối giữa hạ tầng tại chỗ (on-premise) và các dịch vụ đám mây.
 - Đặc điểm: Linh hoạt, dễ mở rộng, tích hợp tốt với các nhà cung cấp dịch vụ đám mây như AWS, Azure.
 - Công nghệ: Dựa trên IPsec hoặc các giải pháp VPN của nhà cung cấp đám mây.

c) **Ứng dụng của VPN**

VPN (Virtual Private Network) có nhiều ứng dụng đa dạng, phục vụ cả cá nhân và tổ chức/doanh nghiệp. Dưới đây là các ứng dụng phổ biến của VPN:

- ❖ **Bảo vệ quyền riêng tư và an toàn dữ liệu**
- **Mục đích:** Che giấu địa chỉ IP thực của người dùng và mã hóa dữ liệu để ngăn chặn việc theo dõi hoặc đánh cắp thông tin.
- **Ứng dụng cụ thể:**
 - Bảo vệ thông tin cá nhân khi sử dụng Wi-Fi công cộng (quán cà phê, sân bay, khách sạn).
 - Ngăn nhà cung cấp dịch vụ Internet (ISP), tin tặc, hoặc chính phủ theo dõi hoạt động trực tuyến.

❖ Truy cập nội dung bị giới hạn địa lý

- Mục đích: Vượt qua các giới hạn khu vực (geo-restrictions) để truy cập dịch vụ hoặc nội dung bị chặn.
- Ứng dụng cụ thể:
 - Xem các nền tảng phát trực tuyến như Netflix, Hulu, hoặc BBC iPlayer từ quốc gia không được hỗ trợ.
 - Truy cập các trang web bị chặn bởi chính phủ hoặc tổ chức (như mạng xã hội ở một số quốc gia).

❖ Hỗ trợ làm việc từ xa

- Mục đích: Cho phép nhân viên truy cập an toàn vào mạng nội bộ hoặc tài nguyên của công ty từ bất kỳ đâu.
- Ứng dụng cụ thể:
 - Truy cập máy chủ công ty, tài liệu nội bộ, hoặc phần mềm quản lý từ nhà hoặc khi đi công tác.
 - Đảm bảo dữ liệu nhạy cảm được truyền tải an toàn qua Internet.

❖ Tăng cường bảo mật cho doanh nghiệp

- Mục đích: Bảo vệ dữ liệu và kết nối giữa các văn phòng, chi nhánh hoặc đối tác.
- Ứng dụng cụ thể:
 - Kết nối các mạng nội bộ qua Site-to-Site VPN để chia sẻ tài nguyên an toàn.
 - Bảo mật thông tin liên lạc giữa doanh nghiệp và khách hàng/đối tác.

❖ Chơi game và chia sẻ tệp an toàn

- Mục đích: Tạo môi trường kết nối an toàn hoặc giảm độ trễ khi chơi game, đồng thời bảo vệ quyền riêng tư.
- Ứng dụng cụ thể:
 - Chơi game đa người chơi (multiplayer) qua mạng LAN ảo bằng Peer-to-Peer VPN.
 - Truy cập các máy chủ game ở khu vực khác hoặc giảm ping bằng cách chọn máy chủ VPN gần hơn.
 - Chia sẻ tệp giữa các thiết bị mà không bị theo dõi.

❖ Vượt qua kiểm duyệt Internet

- Mục đích: Truy cập thông tin hoặc dịch vụ bị kiểm duyệt bởi chính phủ hoặc tổ chức.

- Ứng dụng cụ thể:
 - Sử dụng mạng xã hội, ứng dụng nhắn tin (như WhatsApp, Telegram) ở các quốc gia chặn chúng.
 - Đọc tin tức hoặc nghiên cứu thông tin từ các nguồn bị hạn chế.
- ❖ Tiết kiệm chi phí khi mua sắm trực tuyến
 - Mục đích: Thay đổi vị trí ảo để tận dụng giá ưu đãi ở các khu vực khác nhau.
 - Ứng dụng cụ thể:
 - Mua vé máy bay, đặt phòng khách sạn hoặc phần mềm với giá thấp hơn ở quốc gia khác.
- ❖ Phát triển và kiểm thử phần mềm
 - Mục đích: Mô phỏng truy cập từ các vị trí địa lý khác nhau để kiểm tra ứng dụng hoặc website.
 - Ứng dụng cụ thể:
 - Lập trình viên kiểm tra tính năng bị giới hạn theo khu vực.
 - Doanh nghiệp kiểm tra hiệu suất dịch vụ ở các thị trường quốc tế.

1.2.2 Các giao thức tạo đường hầm cho VPN

❖ PPTP (Point-to-Point Tunneling Protocol)

- Mô tả: Là một trong những giao thức VPN lâu đời nhất, được phát triển bởi Microsoft và các đối tác vào những năm 1990. PPTP dựa trên giao thức PPP (Point-to-Point Protocol) và sử dụng GRE (Generic Routing Encapsulation) để tạo đường hầm.
- Ưu điểm:
 - Dễ thiết lập và cấu hình.
 - Tốc độ nhanh do mã hóa nhẹ (thường dùng MS-CHAP v2 hoặc mã hóa 128-bit).
- Nhược điểm:
 - Bảo mật yếu, dễ bị tấn công (đặc biệt với các công cụ hiện đại như khai thác MS-CHAP v2).
 - Không còn được coi là an toàn theo tiêu chuẩn ngày nay, nhiều nhà cung cấp VPN đã ngừng hỗ trợ.
- Ứng dụng: Phù hợp cho các nhu cầu cơ bản như vượt qua giới hạn địa lý, nhưng không nên dùng cho dữ liệu nhạy cảm.

❖ L2TP (Layer 2 Tunneling Protocol)

- Mô tả: Được phát triển bởi Cisco và Microsoft, L2TP là sự kết hợp giữa L2F (của Cisco) và PPTP. Nó thường kết hợp với IPsec để cung cấp mã hóa và bảo mật.
- Ưu điểm:
 - Bảo mật cao hơn PPTP nhờ mã hóa IPsec (thường là AES 256-bit).
 - Ổn định và được hỗ trợ rộng rãi trên nhiều thiết bị.
- Nhược điểm:
 - Tốc độ chậm hơn PPTP do mã hóa kép (double encapsulation): L2TP tạo đường hầm, IPsec mã hóa dữ liệu.
 - Có thể bị chặn bởi tường lửa NAT nếu không cấu hình đúng.
- Ứng dụng: Phổ biến trong VPN thương mại và doanh nghiệp nhờ cân bằng giữa bảo mật và tính tương thích.

❖ L2F (Layer 2 Forwarding)

- Mô tả: Được Cisco phát triển trước L2TP, L2F là giao thức đường hầm cơ bản nhằm hỗ trợ VPN qua mạng dial-up (mạng quay số).
- Ưu điểm:
 - Hỗ trợ đa giao thức (không chỉ IP).
 - Đơn giản và hiệu quả cho thời kỳ đầu của VPN.
- Nhược điểm:
 - Không có mã hóa mạnh mẽ, phụ thuộc vào các lớp bảo mật khác.
 - Đã lỗi thời và bị thay thế bởi L2TP.
- Ứng dụng: Hiện nay hiếm được sử dụng, chủ yếu mang tính lịch sử.

❖ MPLS (Multiprotocol Label Switching)

- Mô tả: Không phải là giao thức VPN truyền thống như các loại trên, MPLS là công nghệ định tuyến dựa trên nhãn (label) thay vì địa chỉ IP. Nó được dùng để tạo các "đường hầm logic" trong mạng nội bộ hoặc VPN cấp nhà cung cấp dịch vụ (ISP).
- Ưu điểm:
 - Tốc độ cao và hiệu suất tốt nhờ chuyển mạch nhãn thay vì định tuyến phức tạp.
 - Hỗ trợ QoS (Quality of Service), ưu tiên lưu lượng theo nhu cầu.
 - Không cần mã hóa mặc định, dựa vào sự tách biệt logic giữa các mạng.
- Nhược điểm:

- Không cung cấp mã hóa nội tại, cần kết hợp IPsec nếu muốn bảo mật mạnh.
- Phức tạp và thường chỉ triển khai trong mạng doanh nghiệp lớn.
- Ứng dụng: Dùng trong VPN cấp doanh nghiệp (MPLS VPN) để kết nối các chi nhánh qua mạng WAN.

1.2.3 Các giao thức bảo mật cho VPN

❖ IPsec (Internet Protocol Security)

- Mô tả: IPsec là bộ giao thức hoạt động ở tầng mạng (Layer 3) trong mô hình OSI, được thiết kế để bảo mật dữ liệu truyền qua mạng IP. Nó thường được kết hợp với các giao thức đường hầm như L2TP hoặc dùng độc lập trong VPN.
- Cách hoạt động:
 - Chế độ:
 - Transport Mode: Chỉ mã hóa phần dữ liệu (payload), không mã hóa header IP. Dùng cho kết nối điểm-đến-điểm.
 - Tunnel Mode: Mã hóa toàn bộ gói tin IP (bao gồm header) và thêm header mới. Phổ biến trong VPN site-to-site.
 - Thành phần chính:
 - AH (Authentication Header): Xác thực dữ liệu, không mã hóa.
 - ESP (Encapsulating Security Payload): Cung cấp cả mã hóa và xác thực.
 - IKE (Internet Key Exchange): Quản lý khóa mã hóa và thiết lập kết nối an toàn.
 - Mã hóa phổ biến: AES (128/256-bit), 3DES.
- Ưu điểm:
 - Bảo mật cao, phù hợp cho VPN site-to-site và remote access.
 - Hoạt động ở tầng mạng, nên bảo vệ toàn bộ lưu lượng IP mà không cần thay đổi ứng dụng.
 - Linh hoạt, có thể kết hợp với nhiều giao thức đường hầm (L2TP, GRE).
- Nhược điểm:
 - Phức tạp trong cấu hình (yêu cầu thiết lập chính sách, khóa, v.v.).
 - Tốc độ có thể chậm hơn do mã hóa toàn bộ gói tin.
 - Dễ bị chặn bởi tường lửa nếu không hỗ trợ NAT traversal.
- Ứng dụng:
 - VPN doanh nghiệp (kết nối chi nhánh).

- Kết hợp với L2TP trong VPN cá nhân (như NordVPN, ExpressVPN).

❖ SSL/TLS (Secure Sockets Layer / Transport Layer Security)

- Mô tả: SSL/TLS là giao thức bảo mật hoạt động ở tầng ứng dụng (Layer 7) hoặc tầng giao vận (Layer 4), thường được dùng trong VPN dựa trên trình duyệt hoặc ứng dụng (khác với IPSec bảo vệ toàn bộ mạng). OpenVPN là một ví dụ điển hình dùng SSL/TLS.
- Cách hoạt động:
 - Sử dụng cơ chế mã hóa bất đối xứng (RSA) để trao đổi khóa, sau đó chuyển sang mã hóa đối xứng (AES) để truyền dữ liệu.
 - Dựa trên chứng chỉ số (certificate) để xác thực máy chủ và đôi khi cả máy khách.
 - Thường chạy qua cổng 443 (HTTPS), giúp dễ dàng vượt qua tường lửa.
- Ưu điểm:
 - Dễ thiết lập và sử dụng (chỉ cần trình duyệt hoặc ứng dụng hỗ trợ).
 - Linh hoạt, hoạt động tốt trên mạng bị giới hạn (NAT, tường lửa).
 - Tốc độ nhanh hơn IPSec trong một số trường hợp nhờ mã hóa chọn lọc (chỉ mã hóa dữ liệu ứng dụng).
- Nhược điểm:
 - Không bảo vệ toàn bộ lưu lượng mạng mà chỉ mã hóa dữ liệu từ ứng dụng cụ thể (trừ khi dùng OpenVPN full-tunnel).
 - Phụ thuộc vào chứng chỉ và cơ sở hạ tầng PKI (Public Key Infrastructure).
- Ứng dụng:
 - VPN dựa trên trình duyệt (SSL VPN) như Cisco AnyConnect, Fortinet.
 - VPN cá nhân qua OpenVPN (dùng SSL/TLS làm nền tảng bảo mật).

1.2.4 SoftEther VPN

SoftEther VPN là một phần mềm VPN mã nguồn mở, đa nền tảng và đa giao thức, được phát triển bởi Daiyuu Nobori trong khuôn khổ nghiên cứu luận văn thạc sĩ tại Đại học Tsukuba, Nhật Bản. Dự án này được công bố lần đầu vào năm 2014 dưới giấy phép GPLv2, sau đó chuyển sang giấy phép Apache License 2.0 vào năm 2019. SoftEther được thiết kế để cung cấp một giải pháp VPN linh hoạt, mạnh mẽ và dễ sử dụng, phù hợp cho cả người dùng cá nhân lẫn doanh nghiệp.

a) SoftEther VPN là gì?

- Tên gọi: "SoftEther" là viết tắt của "Software Ethernet" (Ethernet phần mềm), ám chỉ khả năng ảo hóa mạng Ethernet thông qua phần mềm.
 - Mục tiêu: SoftEther không chỉ là một giao thức mà còn là một bộ phần mềm hoàn chỉnh, bao gồm SoftEther VPN Server, SoftEther VPN Client, và SoftEther VPN Bridge, hỗ trợ cả kết nối client-to-server (truy cập từ xa) và site-to-site (kết nối giữa các mạng).
-
- Đặc điểm nổi bật: Hỗ trợ nhiều giao thức VPN trong cùng một máy chủ, vượt qua tường lửa hiệu quả, và cung cấp tốc độ cao với mã hóa mạnh mẽ.

b) Các giao thức được hỗ trợ

SoftEther VPN nổi bật nhờ khả năng tích hợp nhiều giao thức VPN phổ biến trong một máy chủ duy nhất, bao gồm:

- SoftEther VPN Protocol: Giao thức độc quyền dựa trên SSL-VPN, sử dụng HTTPS (cổng 443) để vượt qua NAT và tường lửa. Đây là giao thức chính của SoftEther, được tối ưu cho tốc độ và khả năng chống chặn.
- OpenVPN: SoftEther có chức năng "clone" OpenVPN, cho phép sử dụng các client OpenVPN để kết nối.
- L2TP/IPsec: Hỗ trợ các thiết bị như iOS, Android, và macOS thông qua giao thức chuẩn.
- IPSec: Dùng cho VPN site-to-site hoặc kết nối với các thiết bị phần cứng như router Cisco.
- SSTP (Secure Socket Tunneling Protocol): Giao thức của Microsoft, tương thích với Windows.
- EtherIP, L2TPv3: Hỗ trợ kết nối Ethernet cấp độ 2 (Layer 2).

c) Cách hoạt động

- Đường hầm (Tunneling): SoftEther tạo đường hầm VPN bằng cách đóng gói các khung Ethernet (Layer 2) hoặc gói IP (Layer 3) trong giao thức TCP/IP, sau đó mã hóa bằng SSL/TLS.
- Ảo hóa Ethernet: SoftEther sử dụng Virtual Network Adapter (bộ điều hợp mạng ảo) trên client và Virtual Hub (trạm chuyển mạch Ethernet ảo) trên server để mô phỏng mạng Ethernet vật lý.
- Kết nối: Client kết nối đến server qua TCP hoặc UDP, với khả năng NAT traversal (xuyên qua NAT) và Dynamic DNS tích hợp, không cần địa chỉ IP tĩnh.

d) Ưu điểm

- Miễn phí và mã nguồn mở: Có thể tải về và sử dụng miễn phí cho mục đích cá nhân hoặc thương mại.

- Tốc độ cao: Được quảng bá với thông lượng lên đến 1 Gbps, nhờ tối ưu hóa việc xử lý gói tin và giảm thiểu sao chép bộ nhớ.
- Vượt tường lửa: Sử dụng cổng 443 (HTTPS) hoặc các phương thức như VPN over ICMP/DNS để vượt qua các hạn chế mạng nghiêm ngặt.
- Tương thích đa nền tảng: Hỗ trợ Windows, Linux, macOS, FreeBSD, Solaris (server/bridge) và Windows, Linux, macOS (client).
- Mã hóa mạnh mẽ: Sử dụng AES-256 và RSA-4096, dựa trên thư viện OpenSSL.
- Dễ quản lý: Cung cấp giao diện GUI thân thiện và công cụ dòng lệnh (vpncmd) cho quản trị viên.

e) Nhược điểm

- Phức tạp khi thiết lập: So với một số VPN đơn giản hơn như OpenVPN, việc cấu hình SoftEther có thể phức tạp hơn, đặc biệt với người dùng mới.
- Hiệu suất phụ thuộc phần cứng: Tốc độ cao chỉ đạt được trên thiết bị có CPU mạnh, đặc biệt khi dùng mã hóa AES-NI.
- Cộng đồng nhỏ hơn: Dù mã nguồn mở, SoftEther không có cộng đồng lớn như OpenVPN, nên tài liệu và hỗ trợ đôi khi hạn chế.

f) Ứng dụng thực tế

- Cá nhân: Dùng để truy cập mạng gia đình từ xa, vượt qua giới hạn địa lý, hoặc bảo vệ dữ liệu trên Wi-Fi công cộng.
- Doanh nghiệp: Kết nối các chi nhánh (site-to-site VPN), hỗ trợ BYOD (Bring Your Own Device), hoặc cung cấp truy cập từ xa cho nhân viên.
- VPN Gate: SoftEther là nền tảng cho dự án VPN Gate (cũng từ Đại học Tsukuba), một mạng VPN công cộng miễn phí với hàng nghìn máy chủ tình nguyện trên toàn cầu.

1.3 Kết luận

Ở chương này đã tìm hiểu khái quát về VPN, các mô hình và ứng dụng của VPN. Bên cạnh đó cũng tìm hiểu về các giao thức tạo đường hầm và giao thức bảo mật VPN. Và cũng tìm hiểu về SoftEther VPN.

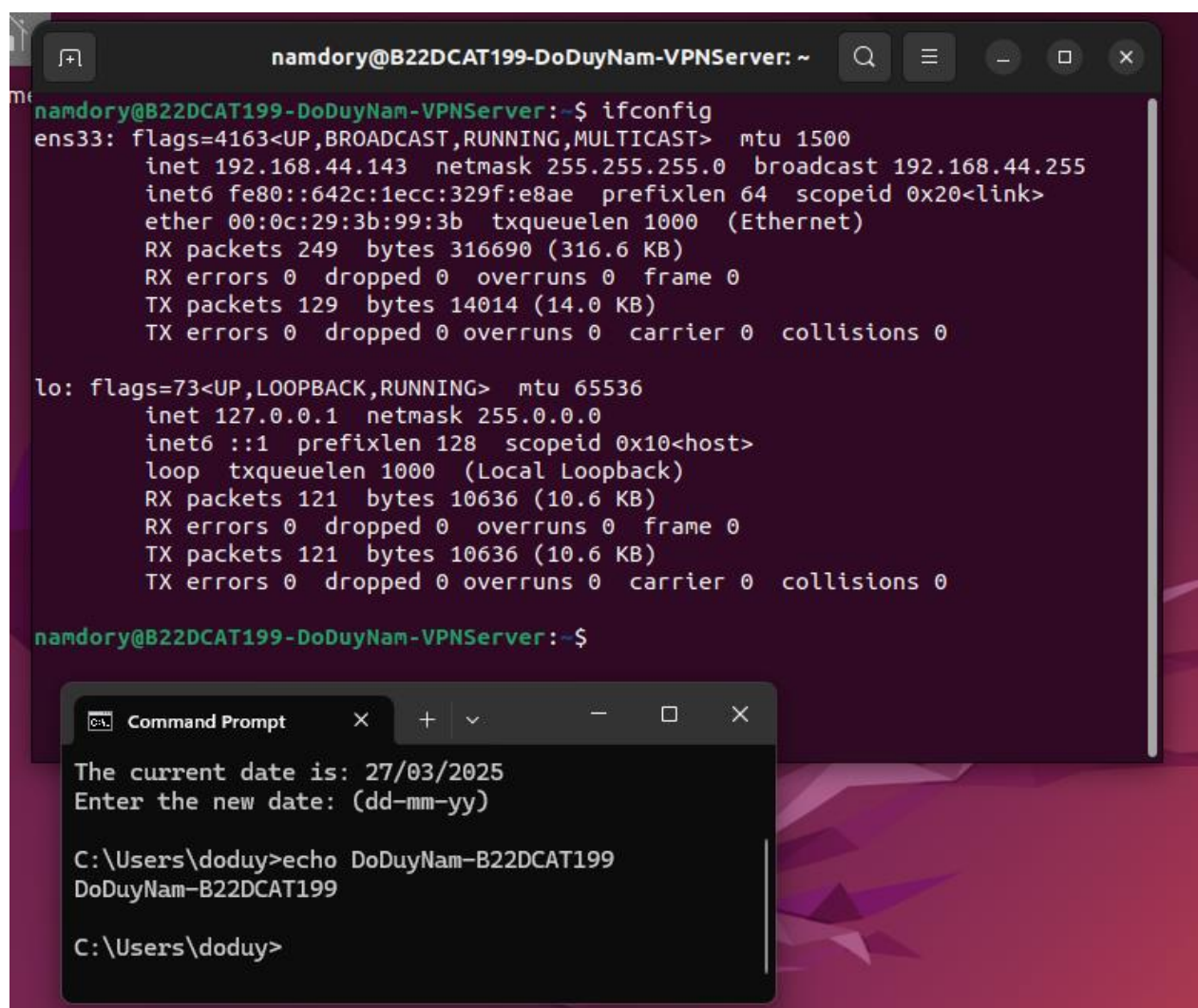
CHƯƠNG 2. NỘI DUNG THỰC HÀNH

2.1 Chuẩn bị môi trường

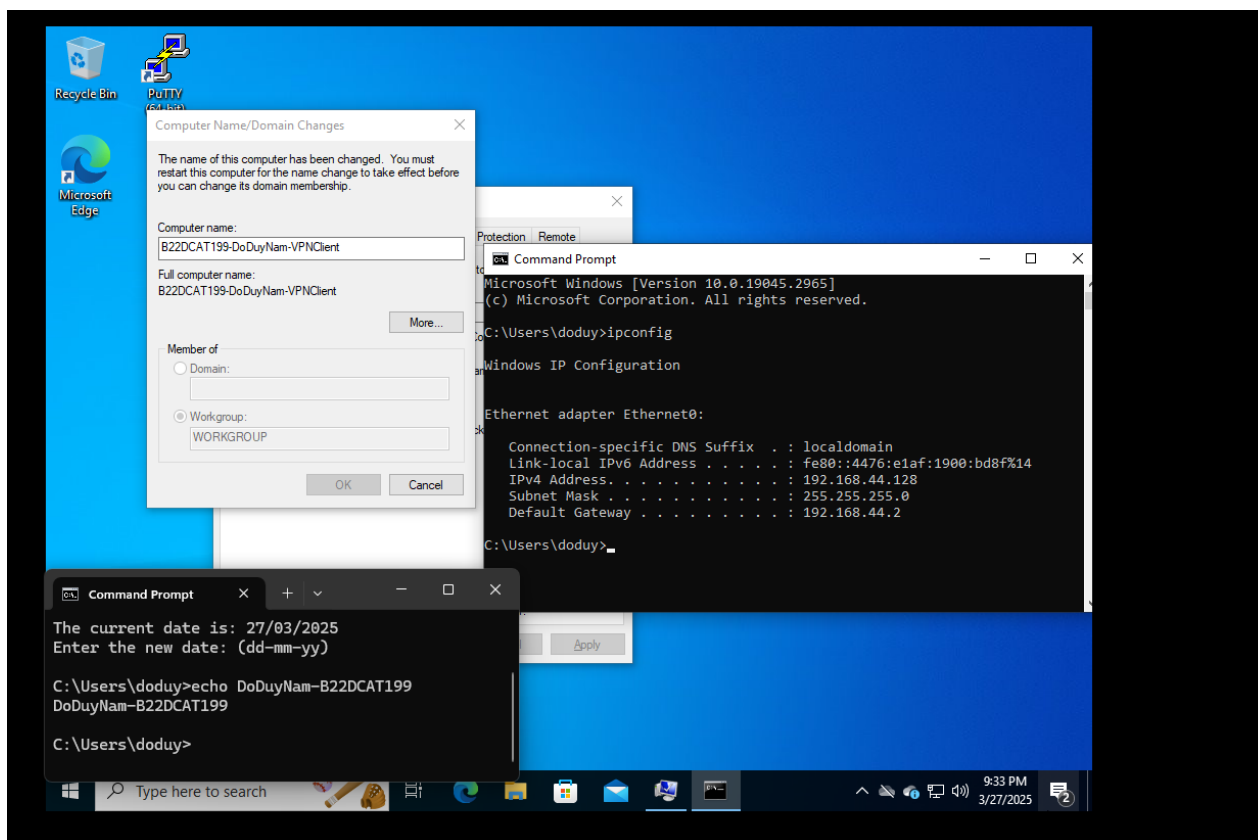
- Máy Linux với RAM tối thiểu 2GB, 10GB đĩa cứng có kết nối mạng để cài đặt VPN Server.
- Máy Windows để cài đặt VPN client.

2.2 Các bước thực hiện

Bước 1: Chuẩn bị các máy tính như mô tả trong mục 2.1. Máy Windows được đổi tên thành B22DCAT199-DoDuyNam-VPNClient và máy cài VPN server thành B22DCAT199-DoDuyNam-VPNServer. Các máy có địa chỉ IP và kết nối mạng LAN.



Hình 1 Đổi tên máy cài VPN Server



Hình 2 Đổi tên máy cài VPN Client

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

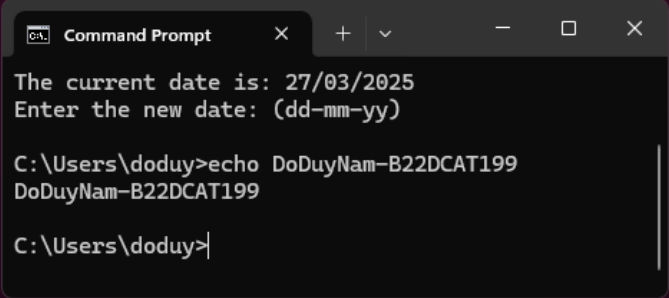
```
namdory@B22DCAT199-DoDuyNam-VPNServer: ~  
namdory@B22DCAT199-DoDuyNam-VPNServer:~$ wget https://www.softether-download.com/files/softether/v4.42-9798-rtm-2023.06.30-tree/Linux/SoftEther_VPN_Server/64bit_-_Intel_x64_or_AMD64/softether-vpnserver-v4.42-9798-rtm-2023.06.30-linux-x64-64bit.tar.gz  
--2025-03-27 21:39:03-- https://www.softether-download.com/files/softether/v4.42-9798-rtm-2023.06.30-tree/Linux/SoftEther_VPN_Server/64bit_-_Intel_x64_or_AMD64/softether-vpnserver-v4.42-9798-rtm-2023.06.30-linux-x64-64bit.tar.gz  
Resolving www.softether-download.com (www.softether-download.com)... 130.158.75.49  
Connecting to www.softether-download.com (www.softether-download.com)|130.158.75.49|:443... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 8398160 (8.0M) [application/x-gzip]  
Saving to: 'softether-vpnserver-v4.42-9798-rtm-2023.06.30-linux-x64-64bit.tar.gz'  
  
softether-vpnserver 100%[=====] 8.01M 1.60MB/s in 5.5s  
  
2025-03-27 21:39:09 (1.45 MB/s) - 'softether-vpnserver-v4.42-9798-rtm-2023.06.30-linux-x64-64bit.tar.gz' saved [8398160/8398160]  
  
namdory@B22DCAT199-DoDuyNam-VPNServer:~$
```

```
Command Prompt  
The current date is: 27/03/2025  
Enter the new date: (dd-mm-yy)  
  
C:\Users\doduy>echo DoDuyNam-B22DCAT199  
DoDuyNam-B22DCAT199  
  
C:\Users\doduy>
```

Hình 3 Tải phần mềm Softether VPN Server về máy Linux

- + Giải nén file cài đặt bằng lệnh `tar -vxzf <tên file vpn server>`

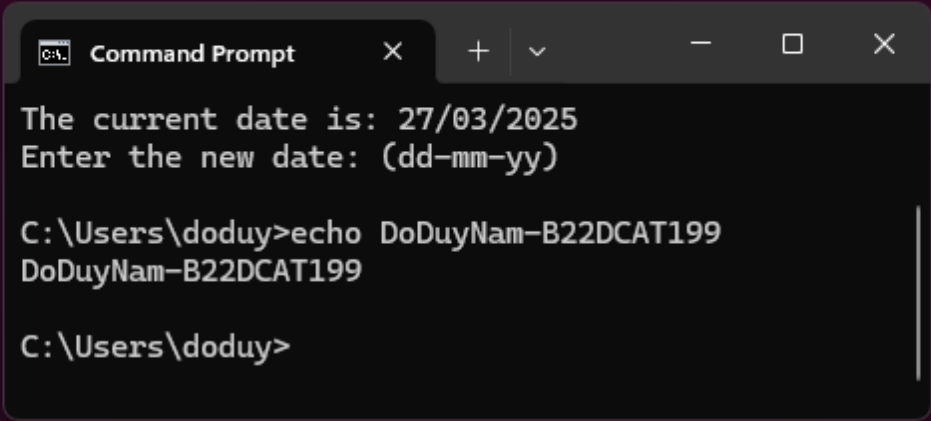
```
namdory@B22DCAT199-DoDuyNam-VPNServer: ~  
namdory@B22DCAT199-DoDuyNam-VPNServer:~$ tar -vxzf softether-vpnserver-v4.42-9798-rtm-2023.06.30  
-linux-x64-64bit.tar.gz  
vpnserver/  
vpnserver/Makefile  
vpnserver/.install.sh  
vpnserver/ReadMeFirst_License.txt  
vpnserver/Authors.txt  
vpnserver/ReadMeFirst_Important_Notices_ja.txt  
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/libintelaes.a  
vpnserver/lib/libncurses.a  
vpnserver/lib/libssl.a  
vpnserver/lib/libz.a  
vpnserver/lib/License.txt  
vpnserver/hamcore.se2  
namdory@B22DCAT199-DoDuyNam-VPNServer:~$
```



Hình 4 Giải nén file

- + Chuyển vào thư mục VPN server: `cd vpnserver`

```
namdory@B22DCAT199-DoDuyNam-VPNServer:~$ cd vpnserver  
namdory@B22DCAT199-DoDuyNam-VPNServer:~/vpnserver$
```



Hình 5 Chuyển vào thư mục VPN Server

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


```
namdory@B22DCAT199-DoDuyNam-VPNServer: ~/vpnservice
namdory@B22DCAT199-DoDuyNam-VPNServer:~/vpnservice$ 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) Daiyu 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 expressed or implied.
See the License for the specific language governing permissions and limitations under the License.

RESPONSIBLE ENTITY
=====

Packetix VPN Server is distributed and operated under the responsibility of SoftEther Corporation (001016519, Tsukuba, Ibaraki, Japan) in cooperation with Tsukuba University, a national university. These products are not intended for use in the national university.

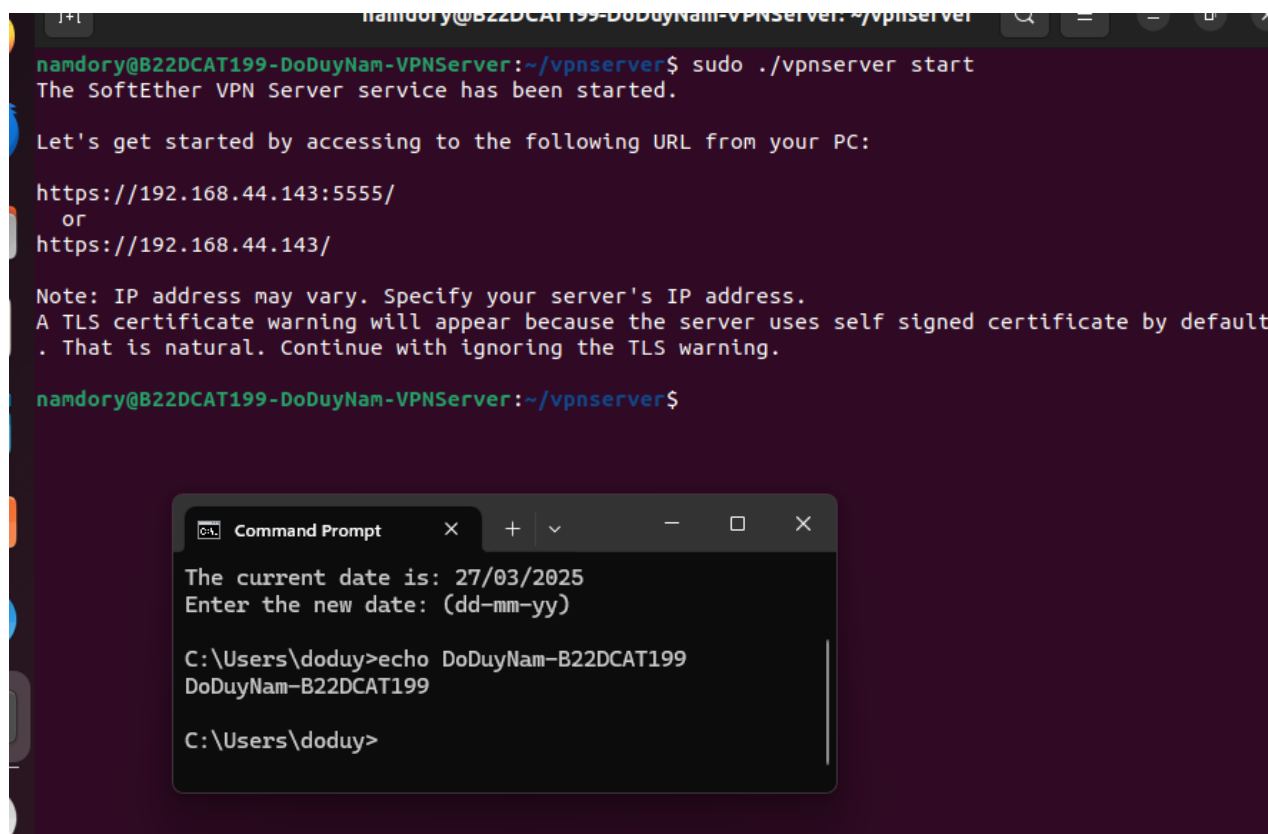
THIS SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN ANY EVENT, UNDER JAPANESE LAWS, YOU MUST AGREE IN ADVANCE TO WAIVE ALL DEFENSES OF LACK OF PERSONAL JURISDICTION AND FORUM NON CONVENIENS. PROCESS MAY BE SERVED ON EITHER PARTY IN THE MANNER AUTHORIZED BY APPLICABLE LAW OR COURT RULE. OF THIS SOFTWARE OR ITS CONTENTS, AGAINST US OR OUR EMPLOYEES, REGARDING, PUBLISHING, DISTRIBUTING, OR OTHERWISE MAKING AS BE CONSTRUED AND CONTROLLED BY JAPANESE LAWS, AND YOU MUST FURTHER CONSENT TO EXCLUSIVE JURISDICTION AND VENUE IN THE COURTS SITTING IN TOKYO, JAPAN. YOU MUST WAIVE ALL DEFENSES OF LACK OF PERSONAL JURISDICTION AND FORUM NON CONVENIENS. PROCESS MAY BE SERVED ON EITHER PARTY IN THE MANNER AUTHORIZED BY APPLICABLE LAW OR COURT RULE.

C:\Users\doduy>echo DoDuyNam-B22DCAT199
DoDuyNam-B22DCAT199

C:\Users\doduy>
```

Hình 6 Biên dịch và cài đặt VPN Server

- + Khởi động máy chủ VPN: `sudo ./vpnservice start`



Hình 7 Khởi động máy chủ VPN Server

- + 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 B22DCAT199 /PASSWORD:password`
 - Chọn Virtual Hub đã tạo: `Hub B22DCAT199`
 - Tạo 1 người dùng VPN mới:
`UserCreate B22DCAT199-DoDuyNam /GROUP:none /REALNAME:DoDuyNam /NOTE:none`
 - Đặt mật khẩu cho người dùng:
`UserPasswordSet B22DCAT199-DoDuyNam /PASSWORD:password`

```

namdory@B22DCAT199-DoDuyNam-VPNServer:~/vpnserv$ ./vpncmd
vpncmd command - SoftEther VPN Command Line Management Utility
SoftEther VPN Command Line Management Utility (vpncmd command)
Version 4.42 Build 9798 (English)
Compiled 2023/06/30 11:06:58 by buildsan at crosswin with OpenSSL 3.0.9
Copyright (c) 2012-2023 SoftEther VPN Project. All Rights Reserved.

By using vpncmd program, the following can be achieved.

1. Management of VPN Server or VPN Bridge
2. Management of VPN Client
3. Use of VPN Tools (certificate creation and Network Traffic Speed Test Tool)

Select 1, 2 or 3: 1

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>

```

```

Command Prompt
The current date is: 27/03/2025
Enter the new date: (dd-mm-yy)

C:\Users\doduy>echo DoDuyNam-B22DCAT199
DoDuyNam-B22DCAT199

C:\Users\doduy>

```

Hình 8 Chạy tiện ích quản trị VPN Server

```

VPN Server>HubCreate B22DCAT199 /PASSWORD:password
HubCreate command - Create New Virtual Hub
The command completed successfully.

VPN Server>

```

```

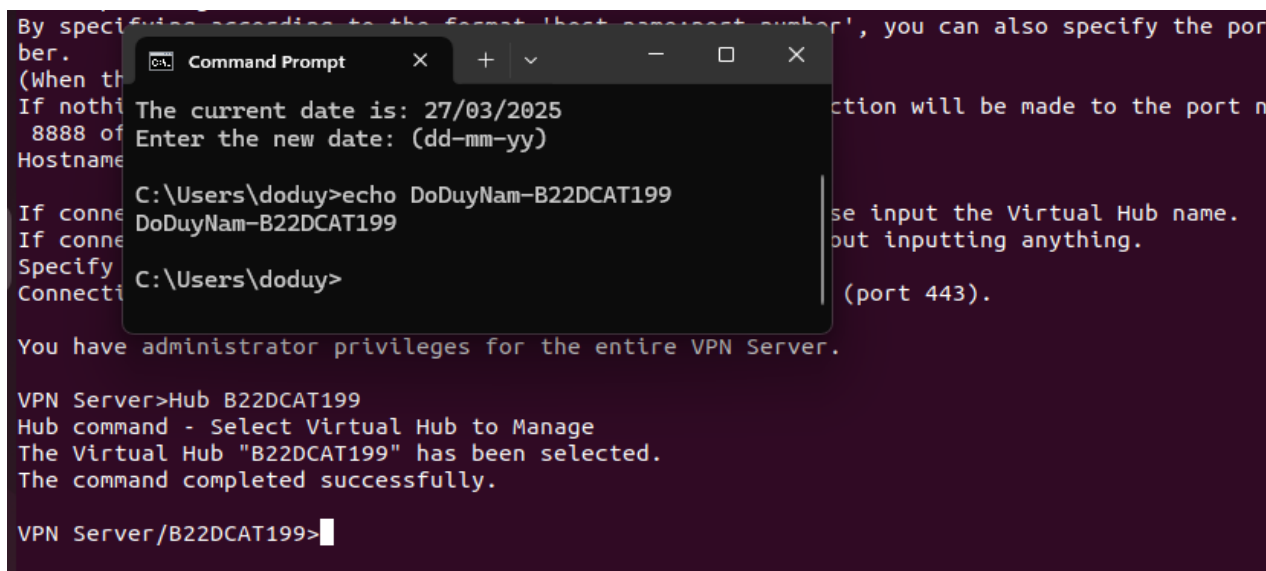
Command Prompt
The current date is: 27/03/2025
Enter the new date: (dd-mm-yy)

C:\Users\doduy>echo DoDuyNam-B22DCAT199
DoDuyNam-B22DCAT199

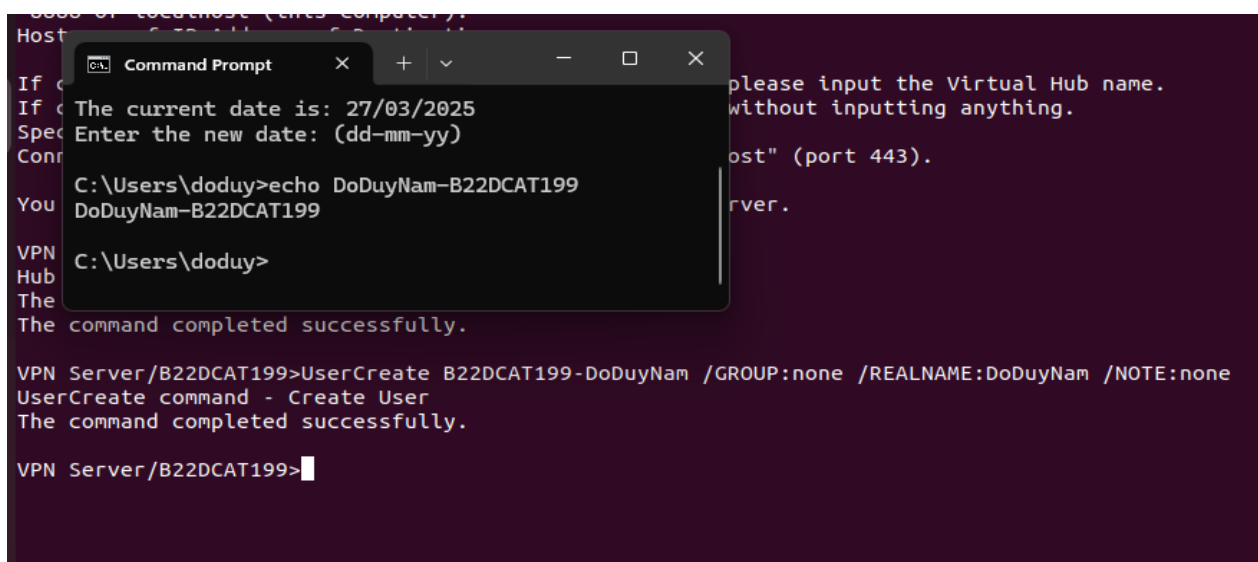
C:\Users\doduy>

```

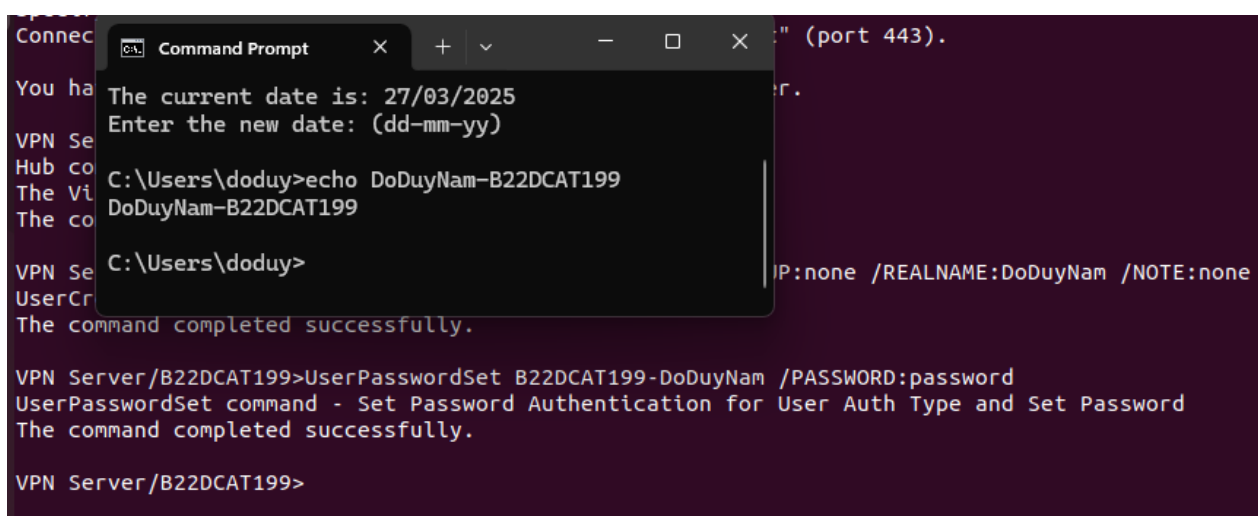
Hình 9 Tạo Virtual Hub mới



Hình 10 Chọn Virtual Hub đã tạo

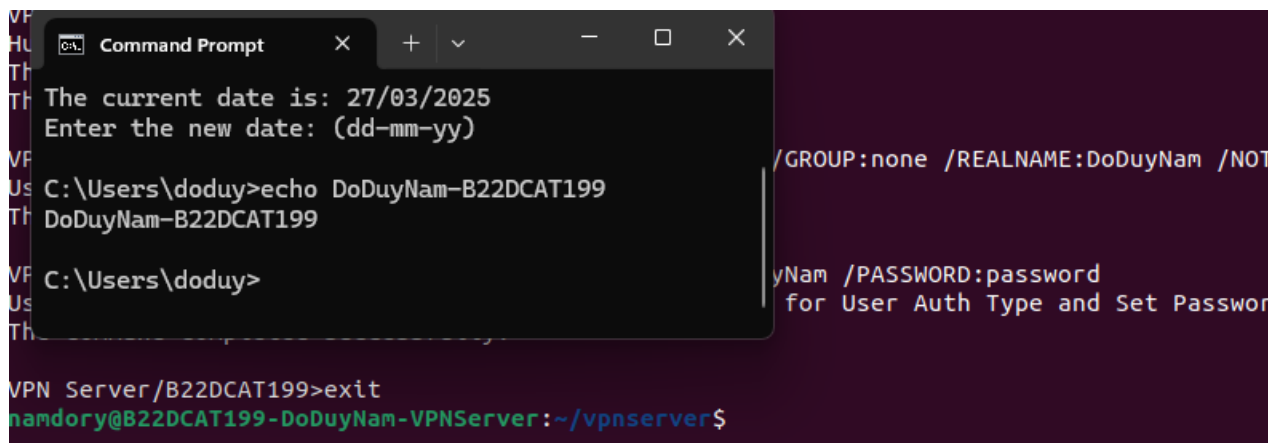


Hình 11 Tạo người dùng VPN mới



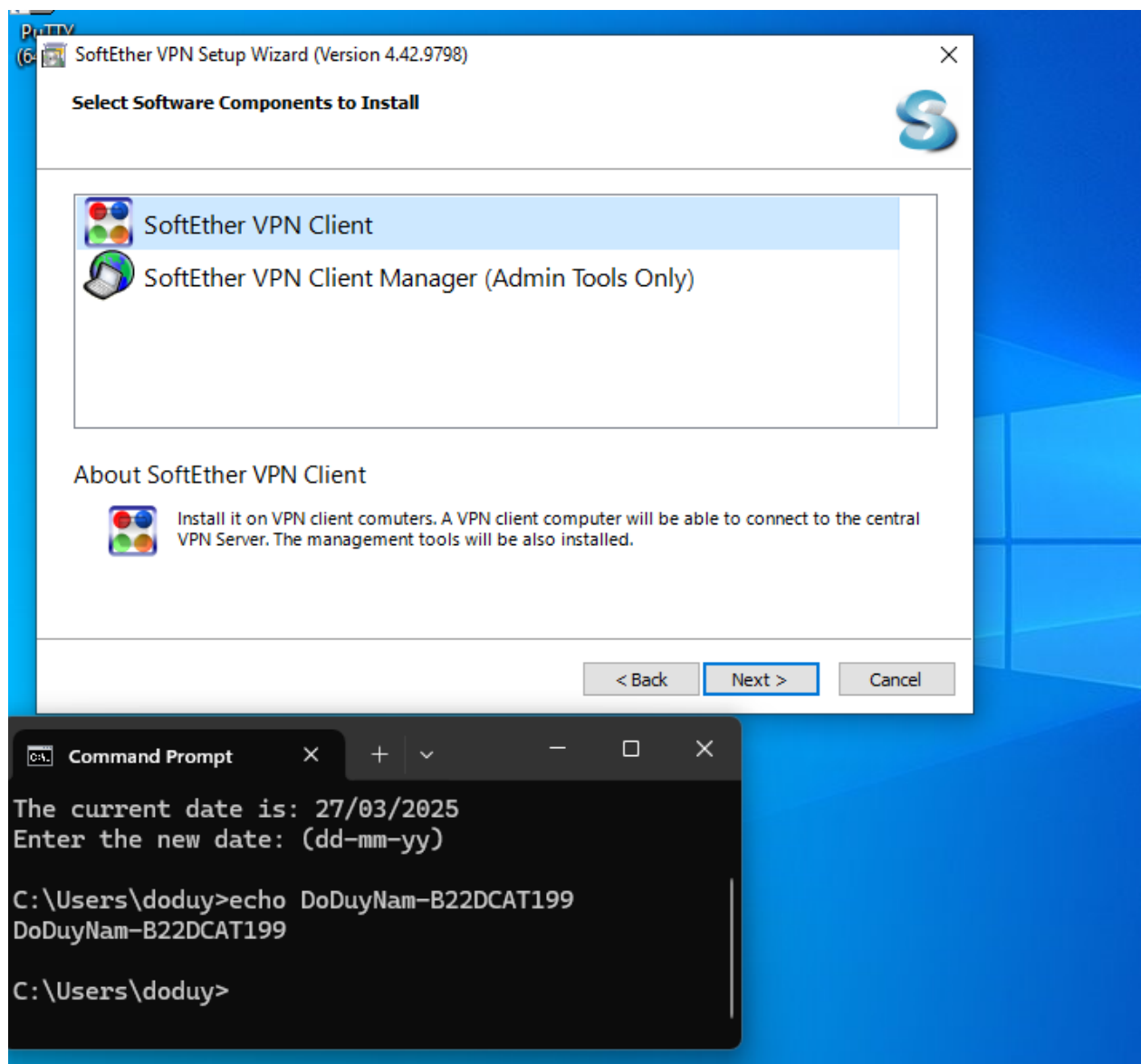
Hình 12 Đặt mật khẩu cho người dùng vừa tạo

- + Gõ exit để thoát khỏi tiện ích quản trị VPN Server



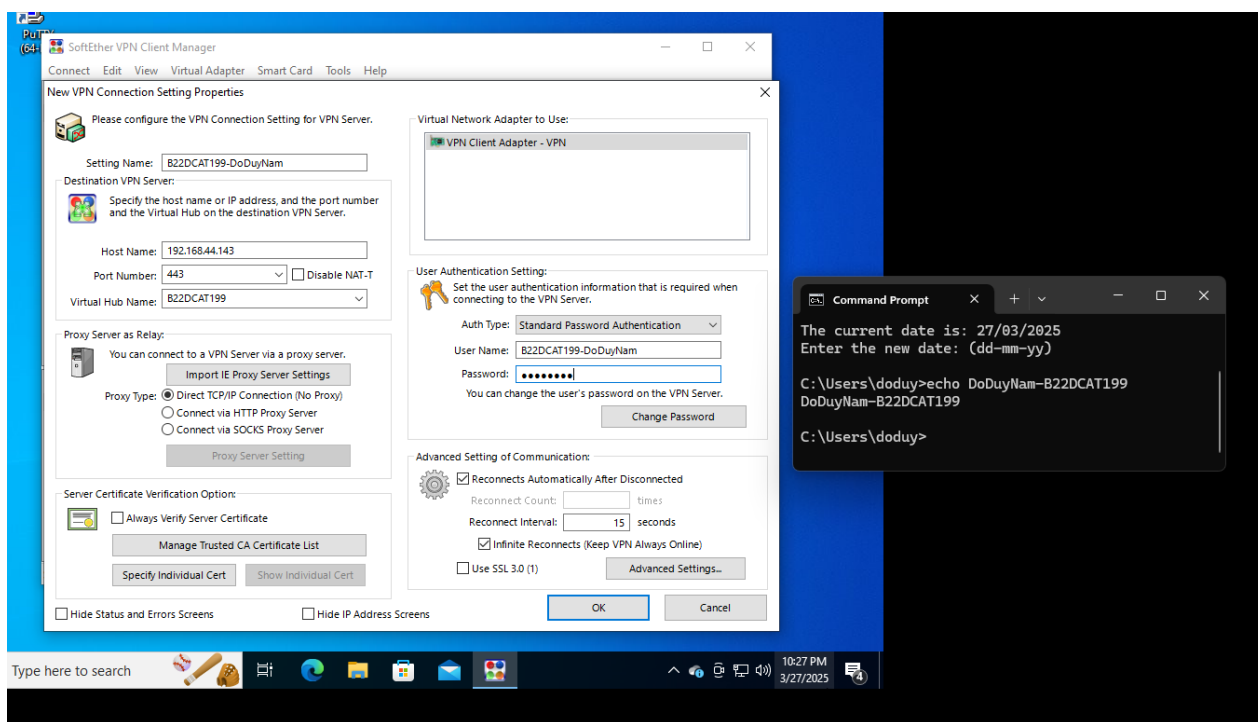
Hình 13 Thoát khỏi tiện ích quản trị VPN Server

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

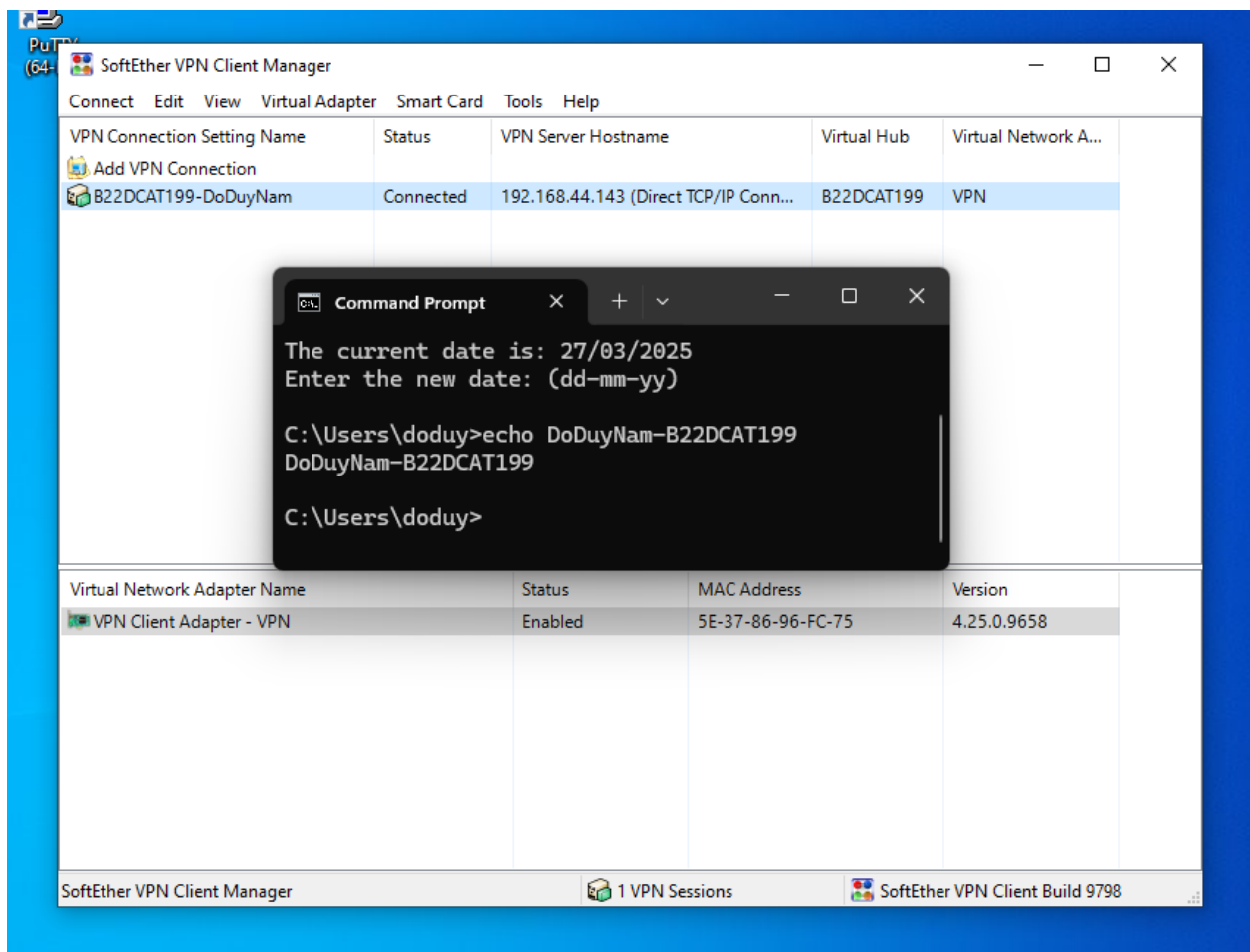


Hình 14 Tải SoftEther VPN Client cho máy Windows

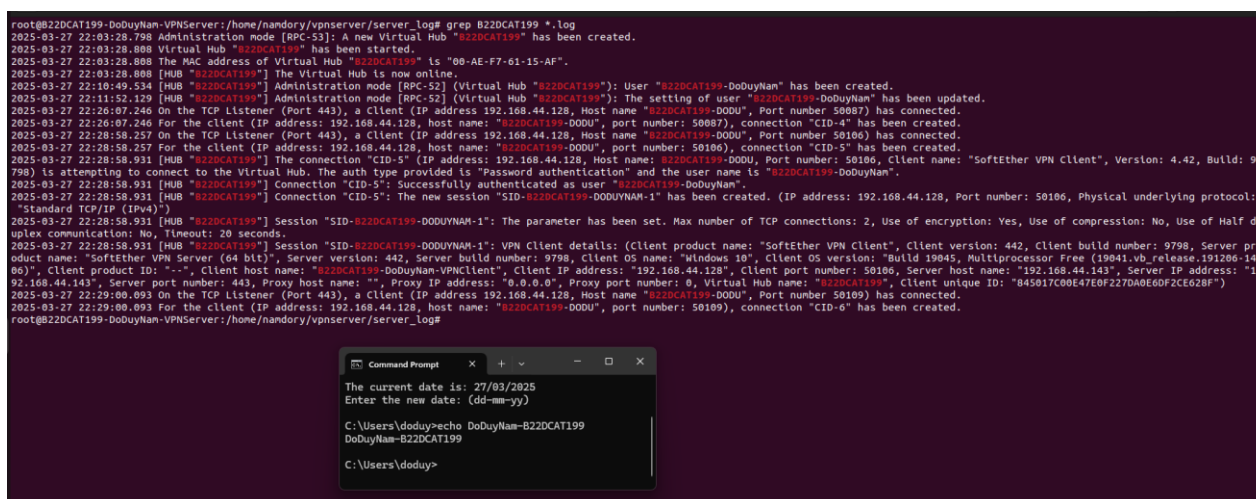
- Bước 4: Tạo và kiểm tra kết nối VPN.
 - + Từ giao diện SoftEther VPN Client Manager, tạo 1 kết nối mới (Add New Connection) với địa chỉ IP của máy chủ VPN, tên Virtual Hub, tên và mật khẩu người dùng. Đặt tên kết nối là B22DCAT199-DoDuyNam
 - + Thử kết nối: Nếu thành công sẽ báo connected.
 - + Kiểm 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 B22DCAT199 vpnserver/server_log/*.log`
 ==> Hiện thị các dòng log có liên quan đến B22DCAT199



Hình 15 Tạo kết nối mới trên SoftEther VPN Client



Hình 16 Kết nối thành công VPN Server từ máy VPN Client



Hình 17 Kiểm tra log trên VPN Server

2.3 Kết luận

Ở chương này đã thực hiện các bước mà bài thực hành yêu cầu. Từ việc chuẩn bị máy để cài đặt VPN Server và VPN Client đến tạo người dùng mới và kết nối từ máy Client đến máy Server.

KẾT LUẬN

- Tìm hiểu khái quát về VPN, các mô hình và ứng dụng của VPN.
- Tìm hiểu về các giao thức tạo đường hầm và giao thức bảo mật cho VPN.
- Tìm hiểu về SoftEther VPN.
- 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 từ máy VPN Client đến máy VPN Server

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>