

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
MÔN THỰC TẬP CƠ SỞ



BÀI THỰC HÀNH 2.3
Tìm hiểu và cài đặt, cấu hình máy chủ VPN

Tên sinh viên: Nguyễn Văn Hùng

Mã sinh viên: B22DCAT136

Nhóm: 09

HÀ NỘI, THÁNG 04/2025

MỤC LỤC

MỤC LỤC	1
DANH MỤC CÁC HÌNH VẼ	2
I. GIỚI THIỆU CHUNG	3
1. Mục đích	3
2. Lý thuyết	3
2.1. Khái quát về VPN	3
2.2. Các giao thức tạo đường hầm cho VPN	4
2.3. Các giao thức bảo mật cho VPN	4
2.4. Tìm hiểu về SoftEther VPN	5
II. NỘI DUNG THỰC HÀNH	6
1. Chuẩn bị môi trường	6
2. Thực hành	6
2.1. Chuẩn bị các máy	6
2.2. Cài đặt và cấu hình SoftEther VPN server trên máy Linux	7
2.3. Cài đặt và cấu hình SoftEther VPN client cho máy Windows	11
2.4. Kiểm tra kết nối VPN	13
TÀI LIỆU THAM KHẢO	17

DANH MỤC CÁC HÌNH VẼ

Hình 1 . Máy Windows VPNClient	6
Hình 2 . Máy Kali Linux VPN Server	7
Hình 3 . Giao diện tải SoftEther VPN	7
Hình 4 . Tùy chọn tải	8
Hình 5 . Chọn version tải VPN Server	8
Hình 6 . Giải nén	9
Hình 7 . Biên dịch vpnserver	9
Hình 8 . Khởi động VPN Server	9
Hình 9 . Chỉnh sửa /etc/hosts	10
Hình 10 . Truy cập công cụ quản lý VPN Server và tạo Virtual Hub	10
Hình 11 . Tạo user VPN	11
Hình 12 . Tùy chọn tải VPN Client	11
Hình 13 . Cài đặt SoftEther VPN Client	12
Hình 14 . Cài đặt thành công	12
Hình 15 . Tạo Virtual Network Adapter	13
Hình 16 . Cấu hình New VPN Connection	13
Hình 17 . Kết nối tới Server	14
Hình 18 . Kiểm tra server_log trên máy Kali Linux	14

I. GIỚI THIỆU CHUNG

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. Lý thuyết

2.1. Khái quát về VPN

VPN (Virtual Private Network - Mạng riêng ảo) là công nghệ giúp tạo kết nối bảo mật giữa hai hay nhiều máy tính qua một mạng công khai như Internet. VPN tạo ra một đường hầm mã hóa giữa các thiết bị, giúp bảo vệ dữ liệu khỏi sự nghe lén và tấn công mạng. Công nghệ này giúp cải thiện quyền riêng tư và bảo mật khi truy cập Internet.

2.1.1. Các mô hình VPN

Remote Access VPN: Cho phép người dùng từ xa kết nối vào mạng nội bộ của doanh nghiệp thông qua một kết nối bảo mật. Được sử dụng phổ biến trong môi trường doanh nghiệp để hỗ trợ làm việc từ xa.

- Ưu điểm: Dễ dàng triển khai, hỗ trợ truy cập linh hoạt.
- Nhược điểm: Có thể làm chậm tốc độ truy cập nếu máy chủ VPN quá tải.

Site-to-Site VPN: Kết nối nhiều mạng nội bộ của doanh nghiệp với nhau thông qua Internet, giúp các chi nhánh có thể truy cập tài nguyên chung một cách an toàn.

- Ưu điểm: Bảo mật tốt, không cần cài đặt phần mềm trên từng thiết bị.
- Nhược điểm: Cấu hình phức tạp, yêu cầu phần cứng và phần mềm chuyên dụng.

Extranet VPN: Cung cấp kết nối bảo mật cho các đối tác kinh doanh, giúp họ truy cập một phần của hệ thống mạng nội bộ mà không ảnh hưởng đến dữ liệu quan trọng khác.

- Ưu điểm: Giúp mở rộng khả năng hợp tác giữa các công ty.
- Nhược điểm: Nguy cơ rò rỉ dữ liệu nếu không quản lý quyền truy cập chặt chẽ.

Intranet VPN: Dùng để kết nối các bộ phận trong cùng một tổ chức trên một nền tảng bảo mật cao, đặc biệt hữu ích với các tập đoàn lớn.

- Ưu điểm: Bảo mật cao, hỗ trợ quản lý tập trung.
- Nhược điểm: Cần đầu tư chi phí cao để thiết lập và duy trì.

2.1.2. Ứng dụng của VPN

- Bảo vệ truy cập Internet công khai: Ngăn chặn các cuộc tấn công khi sử dụng Wi-Fi công cộng.
- Kết nối người dùng từ xa vào mạng doanh nghiệp: Giúp nhân viên làm việc từ xa một cách an toàn.
- Truy cập nội dung bị giới hạn vì địa lý: Cho phép người dùng truy cập nội dung bị chặn ở một số khu vực.
- Bảo vệ dữ liệu khi truyền tải qua Internet: Hạn chế nguy cơ bị đánh cắp dữ liệu quan trọng.
- Giúp truy cập vào hệ thống nội bộ của tổ chức mà không cần phải có mặt trực tiếp tại văn phòng.

2.2. Các giao thức tạo đường hầm cho VPN

VPN sử dụng nhiều giao thức để tạo đường hầm an toàn giữa các thiết bị:

- PPTP (Point-to-Point Tunneling Protocol): Giao thức VPN lâu đời, dễ cấu hình nhưng có nhiều lỗ hổng bảo mật.
- L2TP (Layer 2 Tunneling Protocol): Kết hợp giữa PPTP và L2F, không cung cấp mã hóa mặc định nhưng thường được dùng với IPSec để tăng tính bảo mật.
- L2F (Layer 2 Forwarding Protocol): Do Cisco phát triển, chủ yếu được dùng trong mạng dial-up nhưng ít được sử dụng hiện nay.
- MPLS (Multiprotocol Label Switching): Không thực sự là một giao thức VPN nhưng giúp định tuyến dữ liệu hiệu quả trong các mạng doanh nghiệp.

Giao thức	Mức độ bảo mật	Tốc độ	Ứng dụng phổ biến
PPTP	Thấp	Cao	Kết nối nhanh nhưng không an toàn
L2TP/IPsec	Cao	Trung bình	Kết nối doanh nghiệp
OpenVPN	Rất cao	Trung bình	VPN cá nhân và doanh nghiệp
MPLS	Cao	Cao	Mạng doanh nghiệp

2.3. Các giao thức bảo mật cho VPN

VPN sử dụng các giao thức bảo mật để bảo vệ dữ liệu truyền qua đường hầm:

- IPSec (Internet Protocol Security): Cung cấp xác thực và mã hóa cho dữ liệu IP, hỗ trợ chế độ Transport và Tunnel.

- SSL/TLS (Secure Sockets Layer / Transport Layer Security): Chủ yếu dùng trong VPN truy cập từ xa, hoạt động trên trình duyệt web để bảo vệ kết nối Internet.

2.4. Tìm hiểu về SoftEther VPN

SoftEther VPN là một phần mềm mã nguồn mở hỗ trợ nhiều giao thức VPN như SSL-VPN, L2TP/IPSec, OpenVPN và Microsoft SSTP. Đây là một giải pháp thay thế mạnh mẽ cho OpenVPN với hiệu suất cao và dễ triển khai.

Tính năng:

- Hỗ trợ đa giao thức: Chạy được nhiều loại VPN khác nhau trong cùng một hệ thống.
- Bảo mật mạnh mẽ: Hỗ trợ mã hóa AES-256, RSA và xác thực bằng chứng chỉ số.
- Hiệu suất cao: Tốc độ truyền tải nhanh hơn so với nhiều giao thức VPN truyền thống.
- Khả năng tương thích rộng: Chạy trên Windows, Linux, Mac, Android và iOS.

II. NỘI DUNG THỰC HÀNH

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. Thực hành

2.1. Chuẩn bị các máy

- Chuẩn bị máy Windows 10 VPNClient:

```
C:\Users\PC1>hostname
B22AT136NguyenVanHungVPNClient

C:\Users\PC1>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::7f95:7615:3ece:3610%7
    IPv4 Address. . . . . : 192.168.158.130
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.158.2

C:\Users\PC1>ping 192.168.158.133

Pinging 192.168.158.133 with 32 bytes of data:
Reply from 192.168.158.133: bytes=32 time=1ms TTL=64
Reply from 192.168.158.133: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.158.133:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Hình 1. Máy Windows VPNClient

- Chuẩn bị máy Kali Linux VPNServer:

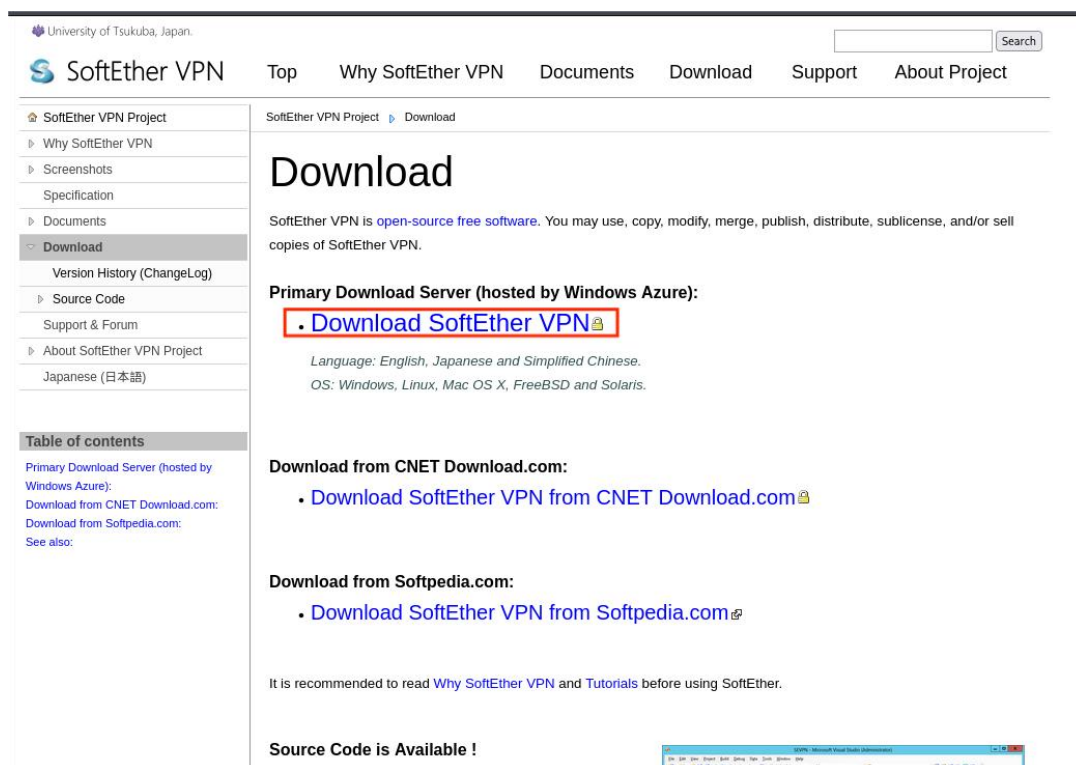

```
(nguyenhung@B22DCAT136NguyenVanHungVPNServer)~$ hostname
B22DCAT136NguyenVanHungVPNServer

(nguyenhung@B22DCAT136NguyenVanHungVPNServer)~$ 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 noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:bc:1b:61 brd ff:ff:ff:ff:ff:ff
    inet 192.168.158.133/24 brd 192.168.158.255 scope global dynamic eth0
        valid_lft 1440sec preferred_lft 1440sec
    inet6 fe80::20c:29ff:febc:1b61/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
```

Hình 2. Máy Kali Linux VPN Server

2.2. Cài đặt và cấu hình SoftEther VPN server trên máy Linux

Trên máy Kali Linux, tải SoftEther VPN server tại: <https://www.softether.org/5-download>. Chọn **Download SoftEther VPN**.



Hình 3. Giao diện tải SoftEther VPN

Chọn tùy chọn tải về:

- Select Software: SoftEther VPN (Freeware)
- Select Component: SoftEther VPN Server
- Select Platform: Linux
- Select CPU: Intel x64 / AMD 64 (64bit)

[SoftEther Project](#)
[Source Code on GitHub](#)
[University of Tsukuba](#)

Select Software

SoftEther VPN (Freeware) ▾

Select Component

SoftEther VPN Server ▾

Select Platform

Linux ▾

Select CPU

Intel x64 / AMD64 (64bit) ▾

Download Files (84)

▶ Note: The following program uses the network functions of the operating system because this is VPN software.
 Some anti-virus software or firewalls warn that such behavior might be dangerous.
 If your anti-virus disturbs the VPN function, add the VPN program file or the installer to the exception list.

Hình 4. Tùy chọn tải

Chọn version tải về:

Download Files (84)

▶ Note: The following program uses the network functions of the operating system because this is VPN software.
 Some anti-virus software or firewalls warn that such behavior might be dangerous.
 If your anti-virus disturbs the VPN function, add the VPN program file or the installer to the exception list.

SoftEther VPN Server (Ver 4.43, Build 9799, beta)
[softether-vpnserver-v4.43-9799-beta-2023.08.31-linux-x64-64bit.tar.gz \(8.01 MB\)](#)
[\[Non-SSL \(HTTP\) Download Link\]](#) Try this if the above link fails because your HTTP client doesn't support TLS 1.2.
Release Date: 2023-08-31 <Latest Build>
[What's new \(ChangeLog\)](#)
 Languages: English, Japanese, Simplified Chinese
 OS: Linux, CPU: Intel x64 / AMD64 (64bit)
 (Linux Kernel 2.4 / 2.6 / 3.x / 4.x)

SoftEther VPN Server (Ver 4.42, Build 9798, rtm)
[softether-vpnserver-v4.42-9798-rtm-2023.06.30-linux-x64-64bit.tar.gz \(8.01 MB\)](#)
[\[Non-SSL \(HTTP\) Download Link\]](#) Try this if the above link fails because your HTTP client doesn't support TLS 1.2.
Release Date: 2023-06-30
[What's new \(ChangeLog\)](#)
 Languages: English, Japanese, Simplified Chinese
 OS: Linux, CPU: Intel x64 / AMD64 (64bit)
 (Linux Kernel 2.4 / 2.6 / 3.x / 4.x)

SoftEther VPN Server (Ver 4.41, Build 9787, rtm)
[softether-vpnserver-v4.41-9787-rtm-2023.03.14-linux-x64-64bit.tar.gz \(8.01 MB\)](#)
[\[Non-SSL \(HTTP\) Download Link\]](#) Try this if the above link fails because your HTTP client doesn't support TLS 1.2.

21s left — 2.0 of 8.0 MB (365 KB/sec)

Show all downloads

Hình 5. Chọn version tải VPN Server

Sau khi tải hoàn thành, giải nén: `tar -vxzf softether-vpnserver-*.tar.gz`

```
(nguyenhung@ B22DCAT136NguyenVanHungVPNServer)~[~/Downloads]
$ ll
total 8204
-rw-rw-r-- 1 nguyenhung nguyenhung 8398160 Apr  2 14:35 softether-vpnserver-v4.42-9798-rtm-2023.06.30-linux-x64-64bit.tar.gz

(nguyenhung@ B22DCAT136NguyenVanHungVPNServer)~[~/Downloads]
$ 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

(nguyenhung@ B22DCAT136NguyenVanHungVPNServer)~[~/Downloads]
$ ll
total 8208
-rw-rw-r-- 1 nguyenhung nguyenhung 8398160 Apr  2 14:35 softether-vpnserver-v4.42-9798-rtm-2023.06.30-linux-x64-64bit.tar.gz
drwxrwxr-x 4 nguyenhung nguyenhung  4096 Jun 29  2023 vpnserver
```

Hình 6. Giải nén

Chuyển đến vpnserver và biên dịch:

- `cd vpnserver`
- `make`

```
(nguyenhung@ B22DCAT136NguyenVanHungVPNServer)~[~/Downloads]
$ cd vpnserver

(nguyenhung@ B22DCAT136NguyenVanHungVPNServer)~[~/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 expressed or implied.
See the License for the specific language governing permissions and limitations under the License.

RESPONSIBLE ENTITY

PacketIX VPN and VPN Gate (where applicable) are provided, distributed and operated under the responsibility of SoftEther Corporation (Corporate Number: 1050001016519, Tsukuba, Ibaraki, Jap
```

Hình 7. Biên dịch vpnserver

Khởi động VPN Server: `sudo ./vpnserver start`

```
(nguyenhung@ B22DCAT136NguyenVanHungVPNServer)~[~/Downloads/vpnserver]
$ sudo ./vpnserver start
sudo: unable to resolve host B22DCAT136NguyenVanHungVPNServer: Name or service not known
[sudo] password for nguyenhung:
Sorry, try again.
[sudo] password for nguyenhung:
The SoftEther VPN Server service has been started.

Let's get started by accessing to the following URL from your PC:
https://192.168.158.133:5555/
or
https://192.168.158.133/

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 8. Khởi động VPN Server

Thông báo gặp phải:

sudo: unable to resolve host B22DCAT136NguyenVanHungVPNServer: Name or service not known

→ Do đổi tên máy nhưng chưa cập nhật đầy đủ file cấu hình hệ thống, mở file /etc/hosts chỉnh sửa bản ghi ánh xạ giữa địa IP local và hostname mới.

```
GNU nano 8.3 /etc/hosts *
127.0.0.1    localhost
127.0.1.1    B22DCAT136NguyenVanHungVPNServer

# The following lines are desirable for IPv6 capable hosts
::1    localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Hình 9. Chỉnh sửa /etc/hosts

Áp dụng thay đổi: *sudo systemctl restart systemd-hostnamed*

Truy cập công cụ quản trị VPN Server: *.\vpncmd*

Trong giao diện vpncmd:

- Chọn "1" (Management of VPN Server or VPN Bridge)
- Nhấn Enter 2 lần
- Tạo Virtual Hub: *HubCreate B22DCAT136*. Nhập mật khẩu Virtual Hub.

```
(nguyenhung@ B22DCAT136NguyenVanHungVPNServer)~[/Downloads/vpnserver]
$ ./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 buildsant 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>HubCreate B22DCAT136
HubCreate command - Create New Virtual Hub
Please enter the password. To cancel press the Ctrl+D key.

Password: *****
Confirm input: *****

The command completed successfully.

VPN Server>
```

Hình 10. Truy cập công cụ quản lý VPN Server và tạo Virtual Hub

- Chọn Virtual Hub vừa tạo: *Hub B22DCAT136*

- Tạo user VPN: `UserCreate B22DCAT136NguyenVanHung /GROUP:none /REALNAME:Nguyen Van Hung /NOTE:none`
- Đặt mật khẩu cho user:
`UserPasswordSet B22DCAT136NguyenVanHung /PASSWORD:password`
- Thoát: `exit`

```
VPN Server>Hub B22DCAT136
Hub command - Select Virtual Hub to Manage
The Virtual Hub "B22DCAT136" has been selected.
The command completed successfully.

VPN Server/B22DCAT136>UserCreate B22DCAT136NguyenVanHung /GROUP:none /REALNAME:Nguyen Van Hung /NOTE:none
UserCreate command - Create User
The command completed successfully.

VPN Server/B22DCAT136>UserPasswordSet B22DCAT136NguyenVanHung /PASSWORD:password
UserPasswordSet command - Set Password Authentication for User Auth Type and Set Password
The command completed successfully.

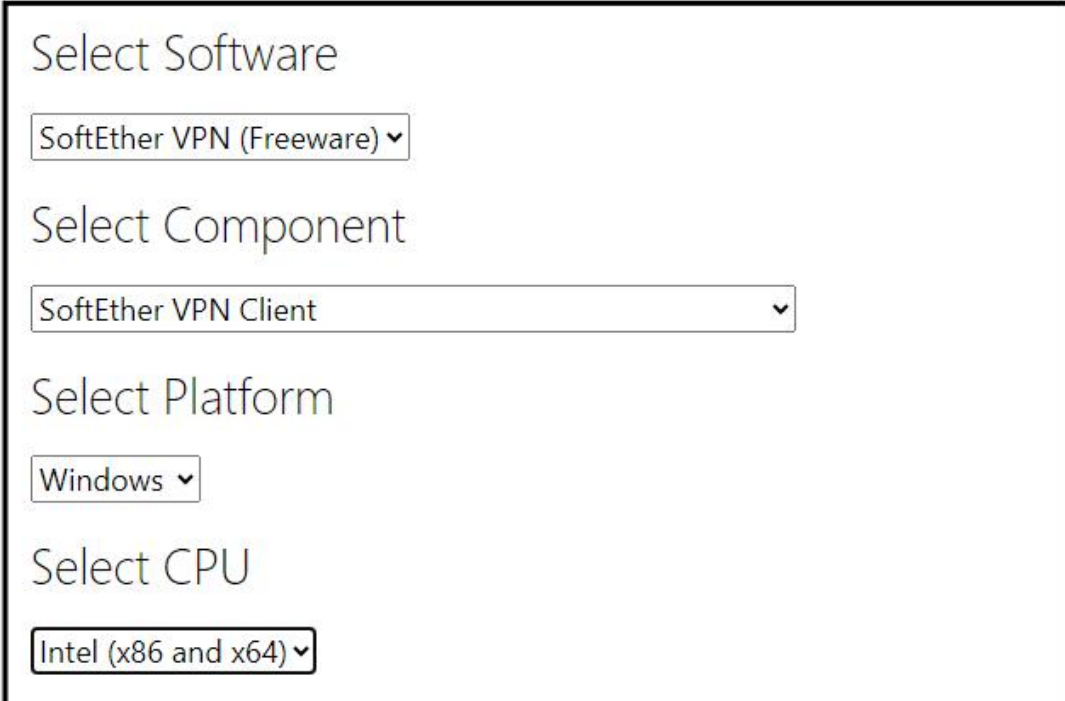
VPN Server/B22DCAT136>exit

nguyenhung@ B22DCAT136NguyenVanHungVPNServer ]-[~/Downloads/vpnserver]
```

Hình 11. Tạo user VPN

2.3. Cài đặt và cấu hình SoftEther VPN client cho máy Windows

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



Select Software

SoftEther VPN (Freeware) ▼

Select Component

SoftEther VPN Client ▼

Select Platform

Windows ▼

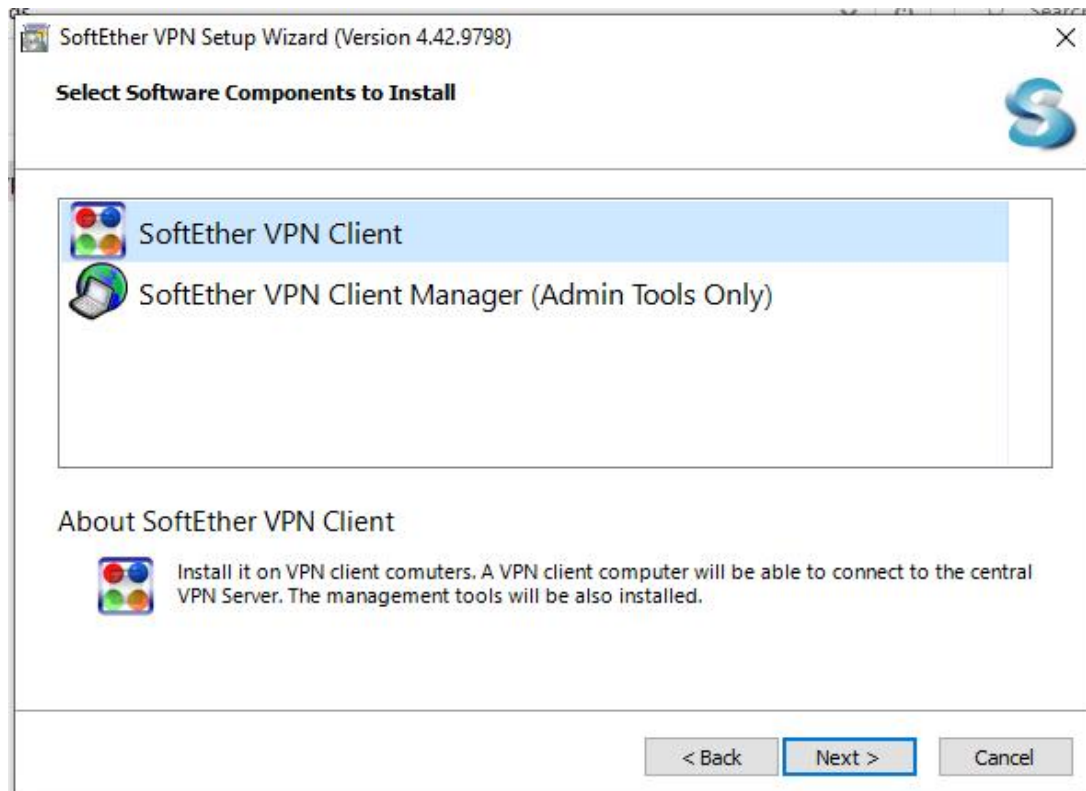
Select CPU

Intel (x86 and x64) ▼

Hình 12. Tùy chọn tải VPN Client

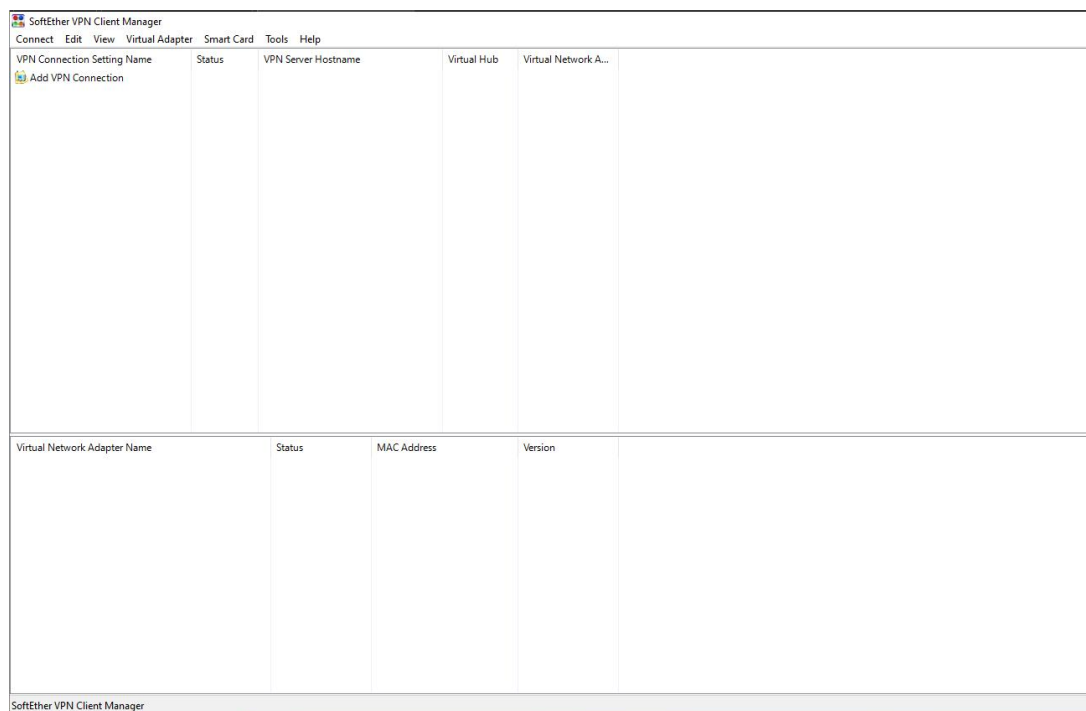
Sau khi tải thành công, thực hiện cài đặt.

Tại bước **Select Software Components to Install**: Chọn **SoftEther VPN Client**
→ **Next**



Hình 13. Cài đặt SoftEther VPN Client

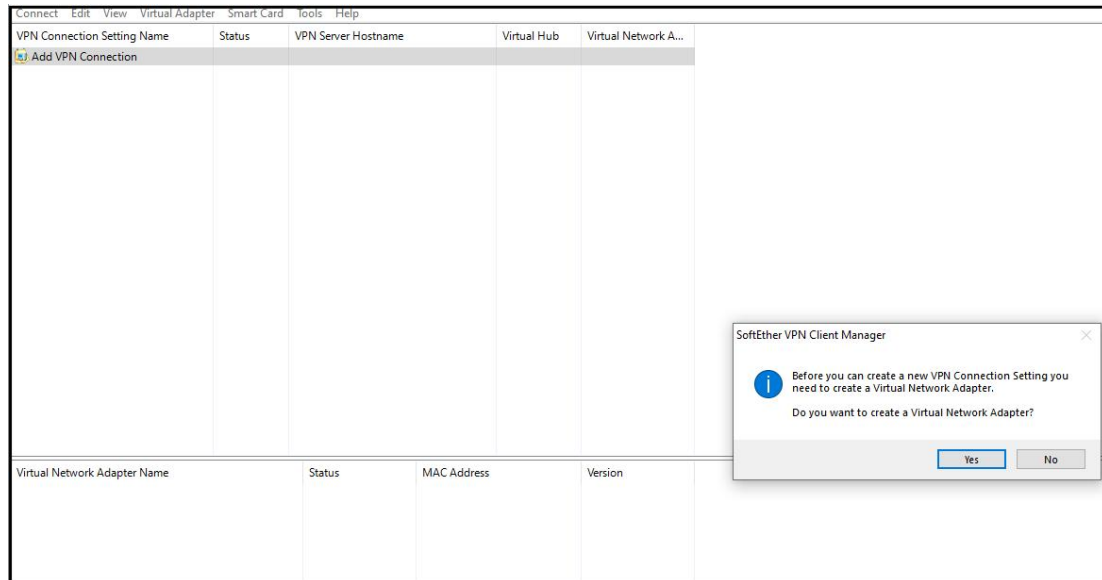
Cài đặt thành công:



Hình 14. Cài đặt thành công

Tạo kết nối mới: Add VPN Connection

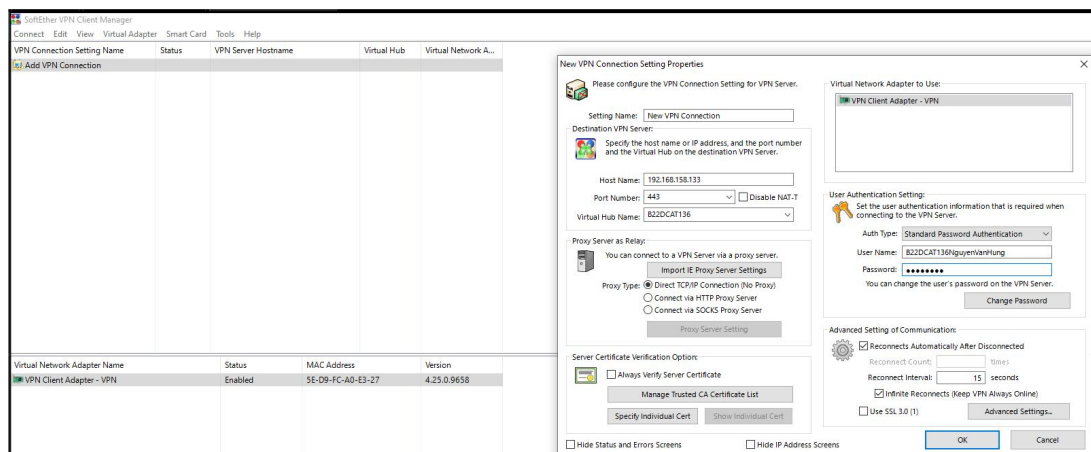
- Tạo **Virtual Network Adapter**



Hình 15. Tạo Virtual Network Adapter

- Tại **New VPN Connection Setting Properties**:

- Host Name: 192.168.158.133 → IP của máy VPN Server
- Virtual Hub Name: B22DCAT136 → Tên Virtual Hub bạn đã tạo
- Username: B22DCAT136NguyenVanHung → User VPN
- Password: password
- Nhấn OK

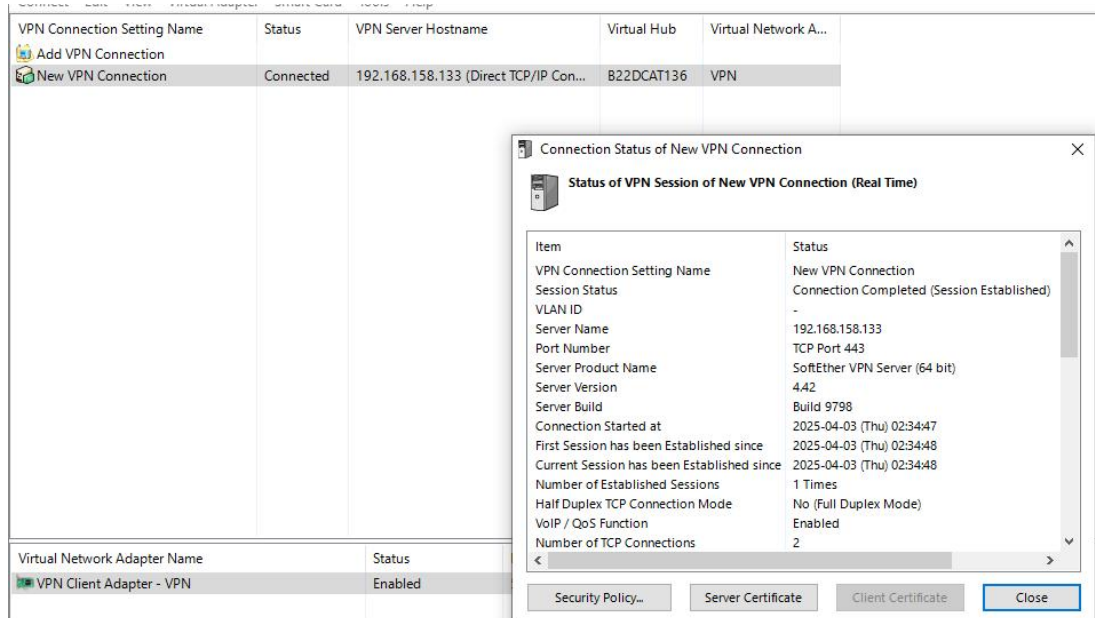


Hình 16. Cấu hình New VPN Connection

2.4. Kiểm tra kết nối VPN

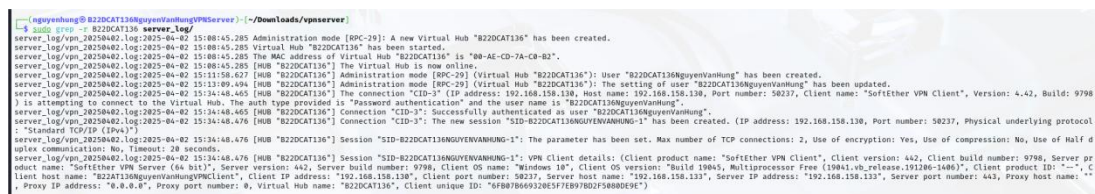
Trên giao diện VPN Client, chọn kết nối vừa tạo.

Nếu trạng thái hiển thị **Connected** thì đã kết nối thành công.



Hình 17. Kết nối tới Server

Mở Kali Linux VPN Server, kiểm tra log trong `vpnservice/server_log`:
`sudo grep -r B22DCAT136 server_log/`



Hình 18. Kiểm tra server_log trên máy Kali Linux

Giải thích các log VPN Server:

2025-04-02 15:08:45.285 Administration mode [RPC-29]: A new Virtual Hub "B22DCAT136" has been created.

2025-04-02 15:08:45.285 Virtual Hub "B22DCAT136" has been started.

2025-04-02 15:08:45.285 The MAC address of Virtual Hub "B22DCAT136" is "00-AE-CD-7A-C0-B2".

2025-04-02 15:08:45.285 [HUB "B22DCAT136"] The Virtual Hub is now online.

→ Log tạo virtual Hub

- Tạo thành công Virtual Hub với tên "B22DCAT136"
- Hub được gán MAC address 00-AE-CD-7A-C0-B2
- Hub đã khởi động và sẵn sàng hoạt động

2025-04-02 15:11:58.627 [HUB "B22DCAT136"] Administration mode [RPC-29] (Virtual Hub "B22DCAT136"): User "B22DCAT136NguyenVanHung" has been created.

2025-04-02 15:13:09.494 [HUB "B22DCAT136"] Administration mode [RPC-29] (Virtual Hub "B22DCAT136"): The setting of user "B22DCAT136NguyenVanHung" has been updated.

→ Log tạo user VPN

- Tạo user "B22DCAT136NguyenVanHung" trong Hub
- Sau đó đã cập nhật cài đặt cho user này

2025-04-02 15:34:48.465 [HUB "B22DCAT136"] The connection "CID-3" (IP address: 192.168.158.130, Host name: 192.168.158.130, Port number: 50237, Client name: "SoftEther VPN Client", Version: 4.42, Build: 9798) is attempting to connect to the Virtual Hub. The auth type provided is "Password authentication" and the user name is "B22DCAT136NguyenVanHung".

2025-04-02 15:34:48.465 [HUB "B22DCAT136"] Connection "CID-3": Successfully authenticated as user "B22DCAT136NguyenVanHung".

→ Log kết nối từ client

- Client từ IP 192.168.158.130 (cổng 50237) đã thử kết nối
- Client sử dụng phiên bản SoftEther VPN Client 4.42 (build 9798)
- Đã xác thực thành công với username "B22DCAT136NguyenVanHung"

2025-04-02 15:34:48.476 [HUB "B22DCAT136"] Connection "CID-3": The new session "SID-B22DCAT136NGUYENVANHUNG-1" has been created. (IP address: 192.168.158.130, Port number: 50237, Physical underlying protocol: "Standard TCP/IP (IPv4)")

2025-04-02 15:34:48.476 [HUB "B22DCAT136"] Session "SID-B22DCAT136NGUYENVANHUNG-1": The parameter has been set. Max number of TCP connections: 2, Use of encryption: Yes, Use of compression: No, Use of Half duplex communication: No, Timeout: 20 seconds.

→ Log tạo session VPN

- Session VPN mới đã được tạo với ID "SID-B22DCAT136NGUYENVANHUNG-1"
- Thông số kết nối:
 - Sử dụng encryption (mã hóa)
 - Không dùng compression

- Timeout: 20 giây

2025-04-02 15:34:48.476 [HUB "B22DCAT136"] Session "SID-B22DCAT136NGUYENVANHUNG-1": VPN Client details: (Client product name: "SoftEther VPN Client", Client version: 442, Client build number: 9798, Server product name: "SoftEther VPN Server (64 bit)", Server version: 442, Server build number: 9798, Client OS name: "Windows 10", Client OS version: "Build 19045, Multiprocessor Free (19041.vb_release.191206-1406)", Client product ID: "--", Client host name: "B22AT136NguyenVanHungVPNClient", Client IP address: "192.168.158.130", Client port number: 50237, Server host name: "192.168.158.133", Server IP address: "192.168.158.133", Server port number: 443, Proxy host name: "", Proxy IP address: "0.0.0.0", Proxy port number: 0, Virtual Hub name: "B22DCAT136", Client unique ID: "6FB07B669320E5F7EB97BD2F5080DE9E")

→ Thông tin chi tiết client

- Client đang chạy trên Windows 10 (Build 19045)
- Tên máy client: "B22AT136NguyenVanHungVPNClient"
- Kết nối từ IP 192.168.158.130 tới server 192.168.158.133 qua cổng 443
- Client và server cùng phiên bản 4.42 (build 9798)
- ID duy nhất của client: "6FB07B669320E5F7EB97BD2F5080DE9E"

TÀI LIỆU THAM KHẢO

- [1] <https://www.hocviendaotao.com/2013/03/giao-thuc-ipsec.html>
- [2] <https://datatracker.ietf.org/doc/html/rfc8446>
- [3] <https://www.softether.org/4-docs>
- [4] <https://aws.amazon.com/vi/what-is/vpn/>