

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



BÁO CÁO THỰC HÀNH

Bài 7: Cài đặt cấu hình VPN server

Họ và tên: Vũ Thành Long

Mã sinh viên: B21DCAT012

Nhóm: 06

Môn học: Thực tập cơ sở

Giảng viên giảng dạy: Nguyễn Hoa Cường

Hà Nội, 2024

Mục Lục

I. Mục đích	3
II. Tìm hiểu lý thuyết.....	3
a, Tìm hiểu về VPN Khái niệm.....	3
b, Tìm hiểu về các giao thức tạo đường hầm cho VPN: PPTP, L2TP, L2F, MPLS....	5
c, Các giao thức bảo mật cho VPN: IPSec, SSL/TLS	6
d, Tìm hiểu về SoftEther VPN	7
III. Các bước thực hiện.....	9
Tài liệu tham khảo	21

Bài thực hành số 7 - Cài đặt cấu hình VPN server

I. 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)

II. Tìm hiểu lý thuyết

a, Tìm hiểu về VPN

Khái niệm

Mạng riêng ảo, hay VPN, là một kết nối được mã hóa qua Internet từ một thiết bị đến một mạng. Kết nối được mã hóa giúp đảm bảo rằng dữ liệu nhạy cảm được truyền đi một cách an toàn. Nó ngăn những người không được phép nghe trộm lưu lượng truy cập và cho phép người dùng tiến hành công việc từ xa. Công nghệ VPN được sử dụng rộng rãi trong môi trường doanh nghiệp.



VPN hoạt động

- Không có VPN

Khi người dùng truy cập một trang web mà không có VPN, người dùng đang được kết nối với trang web đó thông qua nhà cung cấp dịch vụ internet hoặc ISP. ISP chỉ định cho người dùng một địa chỉ IP duy nhất có thể được sử dụng để nhận dạng người dùng với trang web. Vì ISP của người dùng đang xử lý và định hướng tất cả lưu lượng truy cập của người dùng, nên ISP có thể biết người dùng truy cập vào những trang web nào. Và hoạt động của người dùng có thể được liên kết với người dùng bằng địa chỉ IP duy nhất đó.

- Với một VPN

Khi người dùng kết nối Internet bằng VPN, ứng dụng VPN trên thiết bị của người dùng (còn được gọi là máy khách VPN) sẽ thiết lập kết nối an toàn với máy chủ VPN. Lưu lượng truy cập của người dùng vẫn đi qua ISP của người dùng, nhưng ISP của người dùng không thể đọc hoặc nhìn thấy điểm đến cuối cùng của nó nữa. Các trang web người dùng truy cập không còn thấy địa chỉ IP ban đầu của người dùng nữa, chỉ còn địa chỉ IP của máy chủ VPN, được nhiều người dùng khác chia sẻ và thay đổi thường xuyên.

Các mô hình VPN

- VPN site to site là một dạng VPN kết nối 2 hay nhiều mạng riêng với nhau thông qua đường truyền an toàn và bảo mật. VPN site to site giúp mở rộng mạng của doanh nghiệp, giúp cho các chi nhánh ở các nơi khác nhau có thể truy cập đến các ứng dụng hay tài nguyên dùng chung đặt tại head office thông qua 1 đường truyền an toàn và bảo mật dựa trên Internet.
- VPN client to site là loại VPN giúp cho 1 người dùng có thể kết nối đến 1 mạng riêng ở xa thông qua 1 VPN server. Thông thường, để có thể sử dụng VPN client to site, máy tính của người dùng sẽ phải cài đặt 1 phần mềm VPN client để có thể kết nối được đến VPN server. 1 ví dụ điển hình và thông dụng nhất đó là OpenVPN.

Ứng dụng của VPN

- VPN bảo vệ người dùng trên Wi-Fi công cộng

VPN mã hóa dữ liệu của người dùng trực tuyến và giúp bảo mật thông tin cá nhân của người dùng khi sử dụng Wi-Fi tại sân bay, quán cà phê hoặc các địa điểm công

cộng khác. Nó rất hữu ích để che giấu hoạt động trực tuyến của người dùng khi người dùng muốn truy cập thông tin nhạy cảm ở nơi công cộng, chẳng hạn như ngân hàng trực tuyến, nhắn tin hoặc các tập tin điện tử.

- VPN ẩn lịch sử duyệt và ghi Torrenting

Ẩn địa chỉ IP của người dùng là điều cần thiết để đảm bảo quyền riêng tư trực tuyến. Mạng riêng ảo đảm bảo rằng vị trí, thói quen duyệt web và lịch sử torrent không bị ràng buộc trực tiếp với danh tính của người dùng.

- VPN bỏ chặn các trang web bị chặn và kiểm duyệt theo địa lý

Quyền truy cập vào các trang web khác nhau bị hạn chế ở nhiều quốc gia do kiểm duyệt và chặn địa lý. Người dùng có thể bỏ chặn các trang web bằng cách kết nối với máy chủ VPN đặt tại quốc gia khác. Điều này cho phép người dùng vượt qua kiểm duyệt internet, cũng như các hạn chế địa lý khác nhau đối với nội dung, phương tiện truyền thông xã hội

b, Tìm hiểu về các giao thức tạo đường hầm cho VPN: PPTP, L2TP, L2F, MPLS...
PPTP VPN

PPTP là từ viết tắt của Point-to-Point Tunneling Protocol (giao thức tạo đường hầm điểm nối điểm). Giống như tên gọi của mình, mạng riêng ảo PPTP tạo một đường hầm cho dữ liệu đi qua. Người dùng sẽ kết nối đến mạng PPTP VPN bằng đường truyền Internet sẵn có của họ. Loại mạng riêng ảo này phù hợp cho cả doanh nghiệp và người dùng cá nhân. Để truy cập vào mạng PPTP, người dùng sẽ phải đăng nhập bằng mật khẩu. Sở dĩ nói PPTP phù hợp với cả 2 đối tượng trên là vì nó hoàn toàn miễn phí, người dùng không cần cài đặt chương trình khi sử dụng, và các tính năng của dịch vụ này thường được bán dưới dạng phần mềm add on với giá rất rẻ. PPTP được ưa chuộng cũng vì khả năng tương thích với cả 3 hệ điều hành Windows, Mac OS, và Linux.

PPTP có một nhược điểm là nó không sử dụng bộ mã hóa. Trong khi mọi người sử dụng mạng VPN chính vì tính năng đó. Một điểm trừ khác của PPTP là nó sử dụng giao thức PPP để bảo mật đường truyền.

L2TP VPN

L2TP, Layer 2 Tunneling Protocol (giao thức đường hầm lớp 2), là mạng riêng ảo được

phát triển bởi Microsoft và Cisco. L2TP là mạng VPN thường được kết hợp với một giao thức VPN khác để thiết lập một kết nối an toàn hơn. Mạng L2TP hình thành một đường hầm giữa 2 điểm kết nối L2TP, đồng thời một mạng VPN khác (chẳng hạn như giao thức IPSec) sẽ đảm nhận vai trò mã hóa dữ liệu và chú trọng vào việc đảm bảo an toàn cho các thông tin truyền qua đường hầm.

Điểm giống nhau giữa L2TP và PPTP là chúng đều không sử dụng bộ mã hóa mà dựa vào giao thức PPP để bảo mật dữ liệu. Tuy nhiên, L2TP vẫn đảm bảo được tính nhất quán và sự an toàn của dữ liệu, trong khi PPTP thì không.

L2F

Giao thức định hướng lớp 2 L2F do Cisco phát triển độc lập và được phát triển dựa trên giao thức PPP (Point-to-Point Protocol). L2F cung cấp giải pháp cho dịch vụ quay số ảo bằng cách thiết lập một đường hầm bảo mật thông qua cơ sở hạ tầng công cộng như Internet. L2F là giao thức được phát triển sớm nhất, là phương pháp truyền thống để cho những người sử dụng ở xa truy cập vào một mạng công ty thông qua thiết bị truy cập từ xa. L2F cho phép đóng gói các gói PPP trong L2F, định đường hầm ở lớp liên kết dữ liệu MPLS

MPLS là một tập các công nghệ mở dựa vào chuẩn Internet mà kết hợp chuyển mạch lớp 2 và định tuyến lớp 3 để chuyển tiếp gói tin bằng cách sử dụng các nhãn ngắn có chiều dài cố định. MPLS cho phép các ISP hợp nhất các mạng sử dụng các công nghệ khác nhau vào trong một mạng duy nhất, và đặc biệt quan trọng là cho các nhà ISP đạt được việc điều khiển lưu lượng một cách chính xác tại lớp IP.

MPLS sử dụng định tuyến cường bức để xác định các đường mà luồng lưu lượng sẽ đi ngang qua đó và xác định đích tới của các gói chuyển mạch nhãn sử dụng các đường các đường được xác định trước đó.

c, Các giao thức bảo mật cho VPN: IPSec, SSL/TLS

IPSEC

IPSec là từ viết tắt của thuật ngữ Internet Protocol Security (Giao thức bảo mật Internet). IPSec là một giao thức VPN được dùng để đảm bảo an toàn cho việc truyền dữ liệu qua mạng IP. Một đường hầm thiết lập từ xa cho phép người dùng

truy cập đến vị trí trung tâm. Giao thức IPSec bảo vệ đường truyền bằng cách xác minh từng phiên và mã hóa riêng rẽ các gói dữ liệu trong suốt đường truyền. IPSec hoạt động theo 2 chế độ là chế độ vận chuyển và chế độ đường hầm. Cả 2 chế độ đều có cùng tác dụng là bảo vệ dữ liệu trong quá trình chuyển giao giữa 2 mạng lưới. Ở chế độ vận chuyển, thông tin trong gói dữ liệu sẽ được mã hóa. Còn ở chế độ đường hầm, toàn bộ gói dữ liệu đều được mã hóa. Lợi ích của việc sử dụng giao thức IPSec là hỗ trợ các giao thức khác trong việc tăng cường độ an toàn và bảo mật.

Mặc dù IPSec là một giao thức rất hữu dụng, nhưng nhược điểm lớn nhất của nó là người dùng phải mất nhiều thời gian chờ đợi cho quá trình cài đặt chương trình hoàn tất mới có thể bắt đầu sử dụng.

SSL/TLS

SSL là từ viết tắt của Secure Socket Layer (Tầng ổ bảo mật), và TLS là từ viết tắt của Transport Layer Security (Bảo mật lớp vận chuyển). Cả 2 được kết hợp lại thành một giao thức dùng để xây dựng kết nối VPN. Đây là một mạng VPN trong đó trình duyệt web đóng vai trò máy khách và người dùng chỉ được truy cập một số ứng dụng nhất định, thay vì toàn bộ mạng lưới. Giao thức SSL và TLS chủ yếu được dùng trong các trang web bán hàng online và bởi các nhà cung cấp dịch vụ. Mạng VPN SSL và TLS sẽ đảm bảo các phiên truy cập an toàn từ trình duyệt của người dùng đến máy chủ của ứng dụng. Nguyên nhân là do trình duyệt web dễ dàng chuyển sang SSL và người sử dụng không cần phải làm gì cả. Trình duyệt web luôn tương thích với SSL và TLS. Các kết nối SSL sẽ có đường link bắt đầu bằng https thay vì http

d, Tìm hiểu về SoftEther VPN

Khái niệm

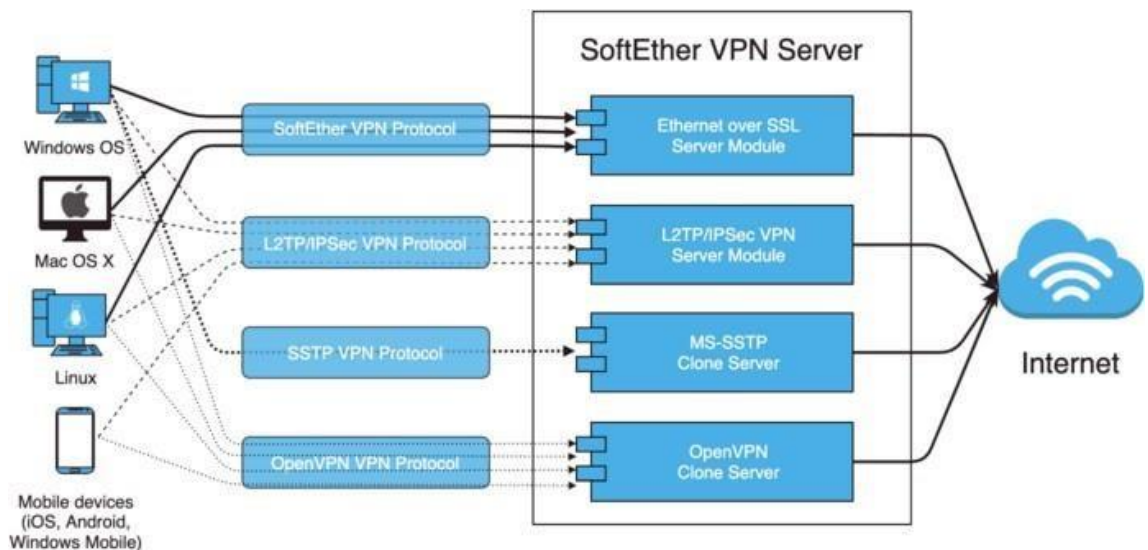
SoftEther VPN ("*SoftEther*" có nghĩa là "*Software Ethernet*") là một trong những phần mềm VPN đa giao thức mạnh mẽ và dễ sử dụng nhất thế giới. Cả giao thức Softether và máy chủ Softether đều có nguồn mở, miễn phí và đa nền tảng. Softether được trình bày như một giải pháp thay thế cho OpenVPN và nó được coi là nhanh hơn.

Một số tính năng quan trọng của SoftEther

- Có sẵn theo giấy phép GNU GPL;
- Sử dụng mã hóa AES 256-bit;
- Hỗ trợ SSL VPN, OpenVPN, EtherIP, L2TP, L2TPv3 và các giao thức SSTP của Microsoft;
- Hỗ trợ IPV6, lọc gói và chức năng DNS động;
- Nó chấp nhận cả kết nối TCP và UDP;
- SoftEther VPN sử dụng xác thực chứng chỉ RSA và chức năng ghi nhật ký gói kiểm tra sâu;
- Phần mềm máy khách SoftEther VPN triển khai Bộ điều hợp mạng ảo và máy chủ SoftEther triển khai Bộ chuyển mạch Ethernet ảo (được gọi là Trung tâm ảo);
- Nó chạy trên Windows, macOS, Linux, FreeBSD, Solaris, iOS và Android.

Phương thức hoạt động

Máy chủ SoftEther VPN là phần trung tâm của kiến trúc SoftEther. Như đã liệt kê ở trên, nó hỗ trợ rất nhiều tính năng và mang lại hiệu suất tuyệt vời. Khía cạnh quan trọng nhất là máy chủ hỗ trợ nhiều giao thức: VPN qua HTTPS (SoftEther), OpenVPN, SSTP, L2TP / IPSec. Do đó, người dùng có thể sử dụng máy chủ SoftEther làm công cho các thiết bị khác nhau (PC, Mac, iPhone / iPad, thiết bị Android, v.v.) và đường hầm VPN.



Giao thức SoftEther sử dụng HTTPS để thiết lập đường hầm VPN và cổng 443 trên TCP / IP làm đích. Cổng này mở cho hầu hết các tường lửa, máy chủ proxy và NAT. Kết quả là giao thức SoftEther có thể được sử dụng để vượt qua kiểm duyệt Internet thành công.

Ưu điểm của SoftEther

- Dự án Softether VPN là nguồn mở. Do đó, miễn phí và cập nhật liên tục.
- Giao thức Softether nhanh chóng, vì nó cung cấp thông lượng vượt trội và độ trễ thấp.
- Lưu lượng Softether có thể xâm nhập vào các bức tường lửa bị giới hạn cao.
- Giao thức sử dụng mã hóa mức cao (AES 256-bit và RSA 4096-bit).
- Softether hỗ trợ đầy đủ cả IPv4 và IPv6.
- Không yêu cầu IP tĩnh hoặc IP cố định cho Softether vì nó hỗ trợ DNS động và chức năng truyền tải NAT.
- Phần mềm máy chủ SoftEther có thể thay thế thành công các bộ định tuyến đắt tiền của Cisco .
- Máy chủ SoftEther có thể cung cấp quyền truy cập từ xa vào mạng LAN hoặc mạng vị trí từ xa bằng mô-đun SoftEther VPN Bridge.

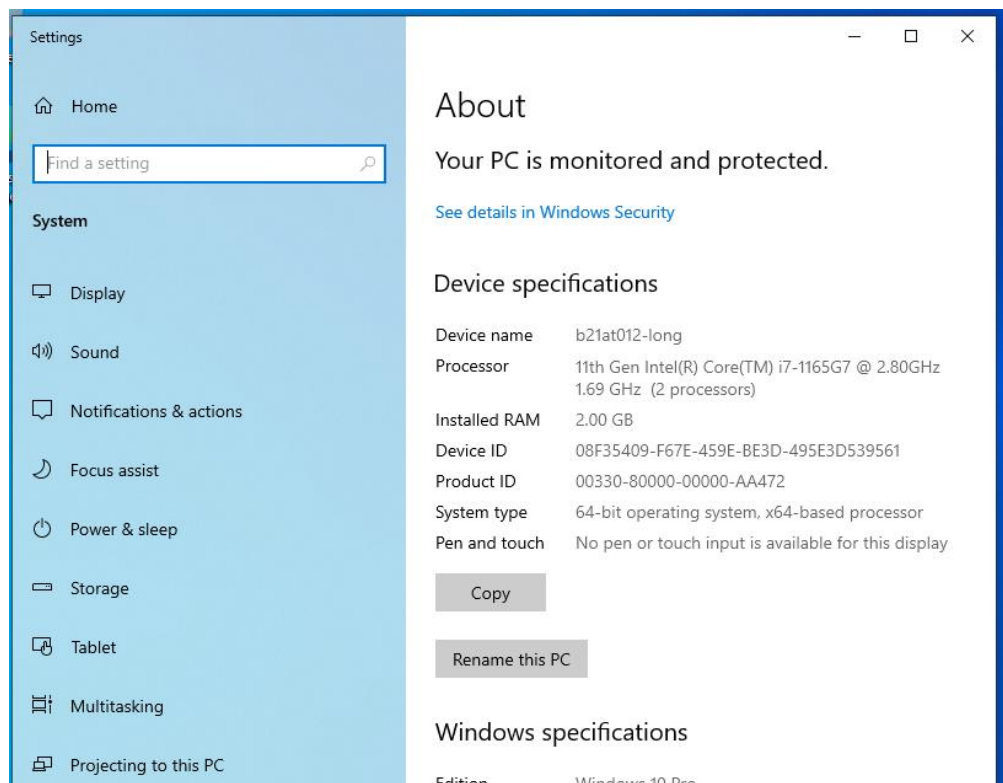
Nhược điểm của SoftEther

- Để được hưởng lợi từ các ưu điểm của giao thức SoftEther, người dùng phải cài đặt và chạy các ứng dụng SoftEther trên các thiết bị dự kiến.
- Khả năng tương thích macOS không tốt.
- Nó là một công nghệ khá mới so với các giao thức khác (OpenVPN, L2TP, SSTP).
- Máy chủ SoftEther không hoặc chưa hỗ trợ giao thức WireGuard.

III.Các bước thực hiện

Bước 1: Chuẩn bị các máy tính như mô tả trong mục 2.2.

- Máy Windows được đổi tên thành b21at012-long



- Máy cài VPN server

```
longvt@B21AT012-LongVT-VPNServer: ~  
longvt@B21AT012-LongVT-VPNServer:~$ hostname  
B21AT012-LongVT-VPNServer  
longvt@B21AT012-LongVT-VPNServer:~$ 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  
        valid_lft forever preferred_lft forever  
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 00:0c:29:db:11:c7 brd ff:ff:ff:ff:ff:ff  
    altname enp2s1  
    inet 192.168.136.134/24 brd 192.168.136.255 scope global dynamic noprefixroute ens33  
        valid_lft 1158sec preferred_lft 1158sec  
    inet6 fe80::5f29:e23a:336d:6d58/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
longvt@B21AT012-LongVT-VPNServer:~$
```

- Các máy có địa chỉ IP và kết nối mạng LAN.

Cập nhật bộ đệm gói của hệ thống lên phiên bản mới nhất. Chạy lệnh **apt-get update -y** để cập nhật tất cả bộ nhớ cache của gói.

```
longvt@B21AT012-LongVT-VPNServer:~$ sudo apt-get update -y
Hit:1 http://vn.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://vn.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:3 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Hit:4 http://vn.archive.ubuntu.com/ubuntu jammy-backports InRelease
Get:5 http://vn.archive.ubuntu.com/ubuntu jammy-updates/main i386 Packages [602 kB]
Get:6 http://vn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [1.519 kB]
Get:7 http://vn.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [293 kB]
Get:8 http://vn.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [1.644 kB]
Get:9 http://vn.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [274 kB]
```

Sau khi hệ thống được cập nhật, hãy cài đặt các phụ thuộc bắt buộc khác bằng lệnh sau:

apt-get install build-essential gnupg2 gcc make -y

```
longvt@B21AT012-LongVT-VPNServer:~$ sudo apt-get install build-essential gnupg2 gcc make -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
make is already the newest version (4.3-4.1build1).
The following additional packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu dpkg-dev fakeroot g++
  g++-11 gcc-11 libalgorithm-diff-perl libalgorithm-diff-xs-perl
  libalgorithm-merge-perl libasan6 libbinutils libc-dev-bin libc-devtools
  LibreOffice Writer 1:0 libcrypt-dev libctf-nobfd0 libctf0 libdpkg-perl
  libfakeroot libfile-fcntllock-perl libgcc-11-dev libitm1 liblsan0 libnsl-dev
  libquadmath0 libstdc++-11-dev libtirpc-dev libtsan0 libubsan1 linux-libc-dev
  lto-disabled-list manpages-dev rpcsvc-proto
Suggested packages:
  binutils-doc debian-keyring g++-multilib g++-11-multilib gcc-11-doc
  gcc-multilib autoconf automake libtool flex bison gcc-doc gcc-11-multilib
```

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

Trước tiên, truy cập trang tải xuống SoftEther VPN và tải xuống phiên bản mới nhất bằng lệnh sau:

wget https://www.softether-download.com/files/softether/v4.43-9799-beta-2023.08.31-tree/Linux/SoftEther_VPN_Server/64bit_-_Intel_x64_or_AMD64/softether-vpnserver-v4.43-9799-beta-2023.08.31-linux-x64-64bit.tar.gz

Sau khi quá trình tải xuống hoàn tất, hãy giải nén tệp đã tải xuống bằng lệnh sau:

```
tar -xvzf softether-vpnserver-v4.43-9799-beta-2023.08.31-linux-x64-64bit.tar.gz
```

```
root@B21AT012-LongVT-VPNServer:/home/longvt# tar -xvzf softether-vpnserver-v4.43-9799-beta-2023.08.31-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
```

Tiếp theo, điều hướng đến thư mục đã giải nén và cài đặt SoftEther VPN bằng lệnh sau:

```
cd vpnserver
```

```
make
```

```
root@B21AT012-LongVT-VPNServer: /home/longvt/vpnserver
root@B21AT012-LongVT-VPNServer:/home/longvt# cd vpnserver/
root@B21AT012-LongVT-VPNServer:/home/longvt/vpnserver# make
-----

SoftEther VPN Server (Ver 4.43, Build 9799, 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.
```

Khi quá trình cài đặt hoàn tất, người dùng sẽ nhận được kết quả sau:

```
You can download it from the http://www.softether-download.com/ web site.
VPN Server Manager for Mac OS X works perfectly as same as the traditional Windows versions. It helps you to completely and easily manage the VPN server services running in remote hosts.

*** PacketIX VPN Server HTML5 Web Administration Console (NEW) ***
This VPN Server / Bridge has the built-in HTML5 Web Administration Console.

After you start the server daemon, you can open the HTML5 Web Administration Console is available at

https://127.0.0.1:5555/
or
https://ip_address_of_the_vpn_server:5555/

This HTML5 page is obviously under construction, and your HTML5 development contribution is very appreciated.

-----

make[1]: Leaving directory '/home/longvt/vpnserver'
root@B21AT012-LongVT-VPNServer:/home/longvt/vpnserver#
```

Khởi động máy chủ VPN: `sudo ./vpnserver start`

```
longvt@B21AT012-LongVT-VPNServer:~$ cd vpnserver/
longvt@B21AT012-LongVT-VPNServer:~/vpnserver$ sudo ./vpnserver start
The SoftEther VPN Server service has been started.

Let's get started by accessing to the following URL from your PC:

https://192.168.136.134:5555/
or
https://192.168.136.134/

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.

longvt@B21AT012-LongVT-VPNServer:~/vpnserver$
```

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:

```
longvt@B21AT012-LongVT-VPNServer:~/vpnservice$ ./vpncmd
vpncmd command - SoftEther VPN Command Line Management Utility
SoftEther VPN Command Line Management Utility (vpncmd command)
Version 4.43 Build 9799 (English)
Compiled 2023/08/31 10:50:49 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:

Tạo 1 Virtual Hub mới: **HubCreate b21at012 /PASSWORD: 15042003**

Chọn Virtual Hub đã tạo: **Hub b21at012**

```
VPN Server>HubCreate b21at012 /PASSWORD: 15042003
HubCreate command - Create New Virtual Hub
The command completed successfully.

VPN Server>Hub b21at012
Hub command - Select Virtual Hub to Manage
The Virtual Hub "b21at012" has been selected.
The command completed successfully.

VPN Server/b21at012>
```

Tạo 1 người dùng VPN mới: **UserCreate b21at012-long /GROUP:none /REALNAME: vuthanhlone /NOTE:none**

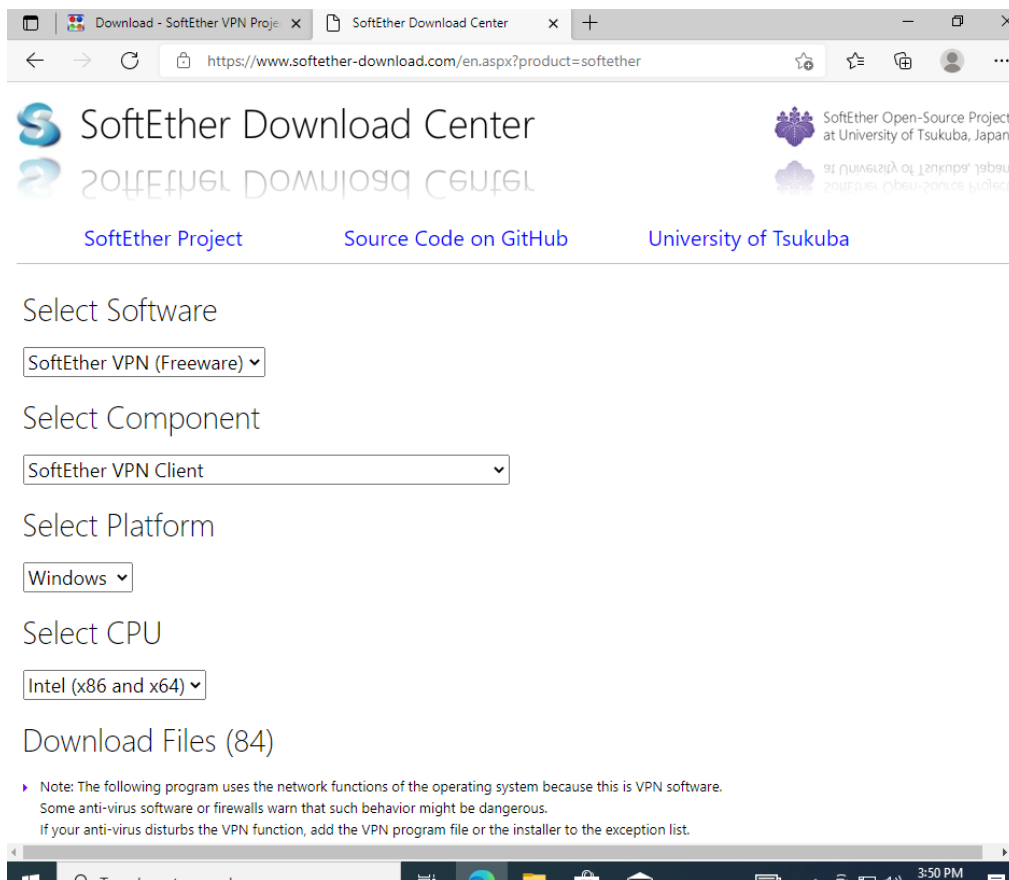

```
VPN Server/b21at012>UserCreate b21at012-long /GROUP:none /REALNAME: vuthanhlong /NOTE:none
UserCreate command - Create User
The command completed successfully.
```

Đặt mật khẩu cho người dùng: **UserPasswordSet b21at012-long /PASSWORD: 15042003**

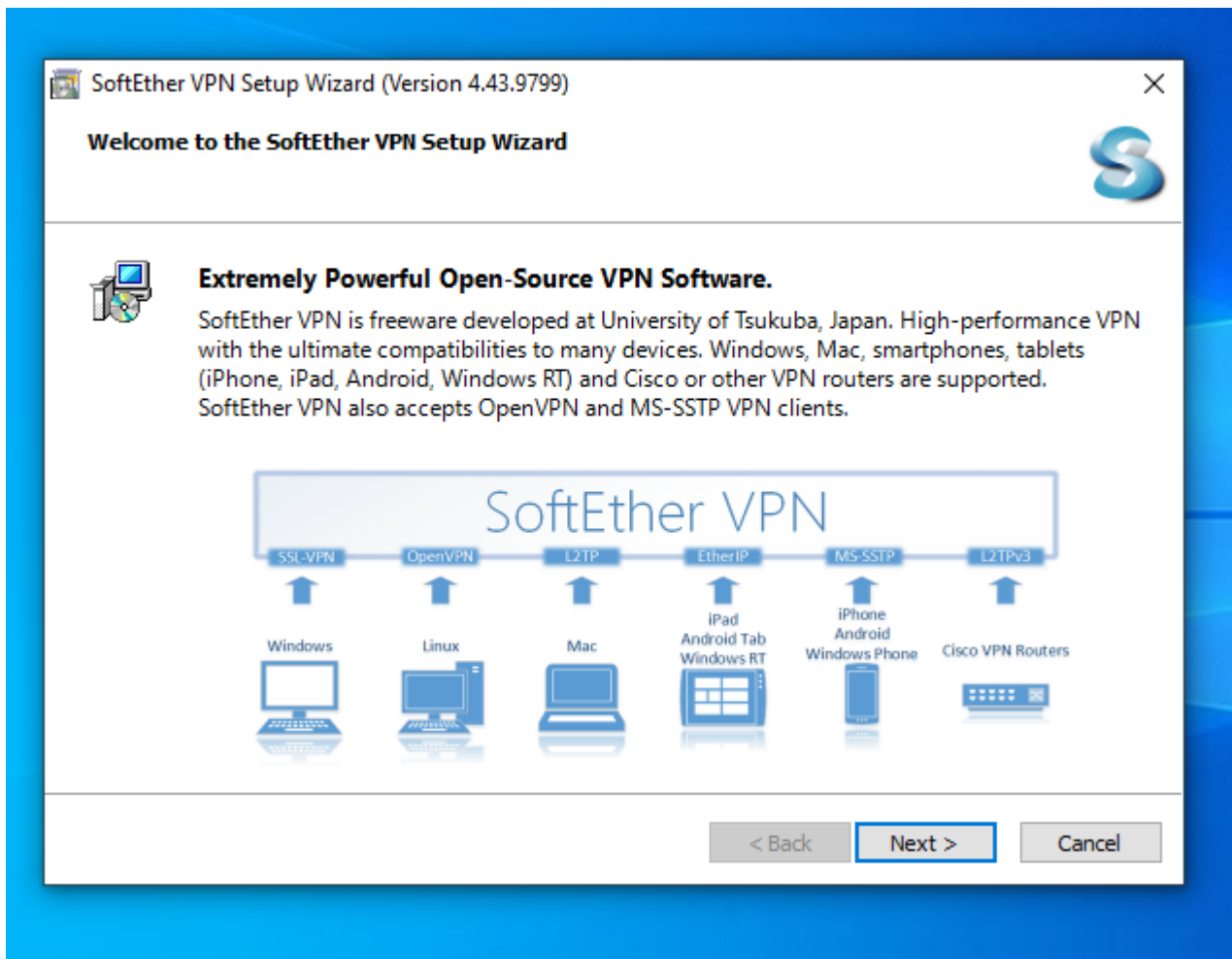
```
VPN Server/b21at012>UserPasswordSet b21at012-long /PASSWORD: 15042003
UserPasswordSet command - Set Password Authentication for User Auth Type and Set Password
The command completed successfully.

VPN Server/b21at012>
```

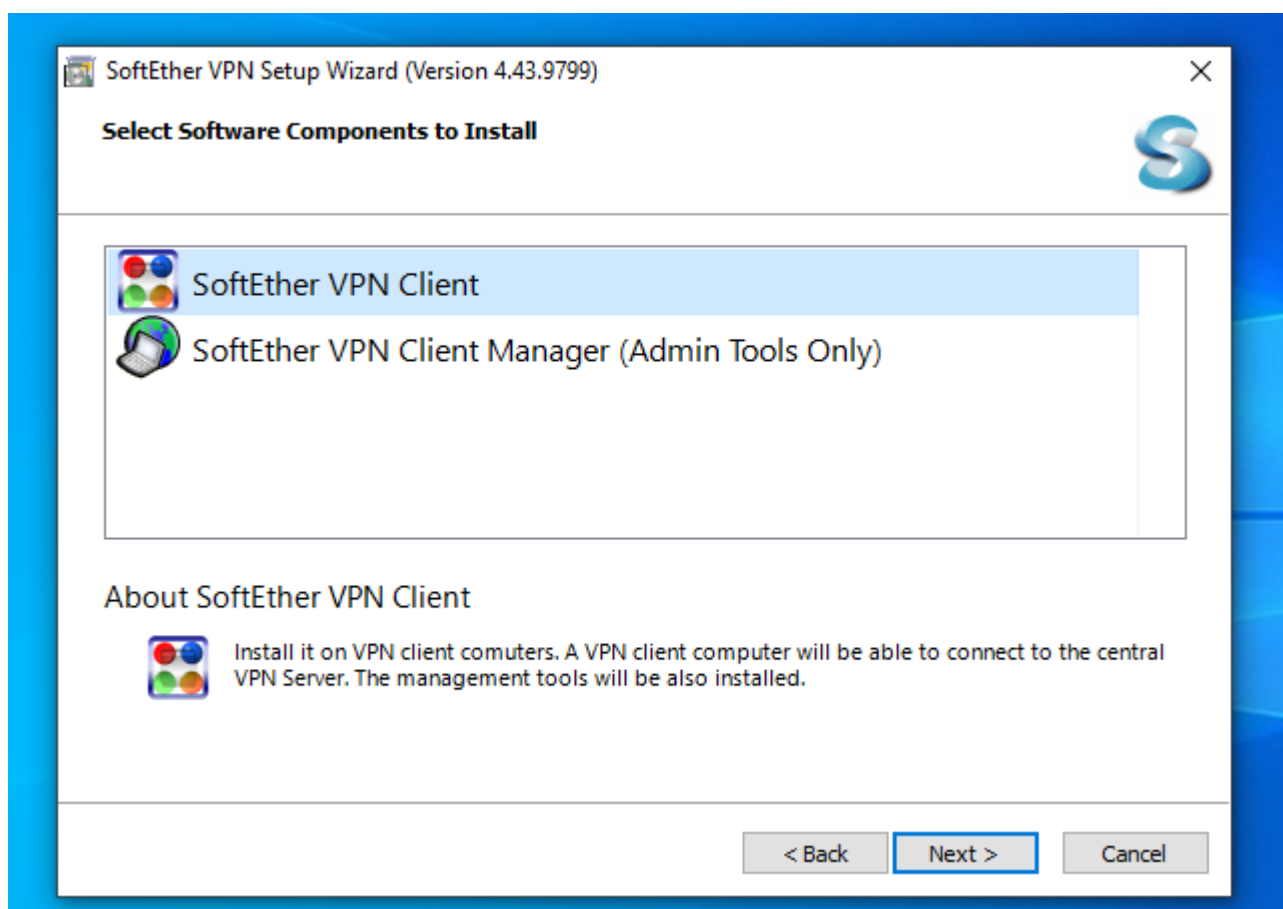
Bước 3: Tải SoftEther VPN client cho Windows tại <https://www.softether.org/5-download>. Cài đặt VPN client



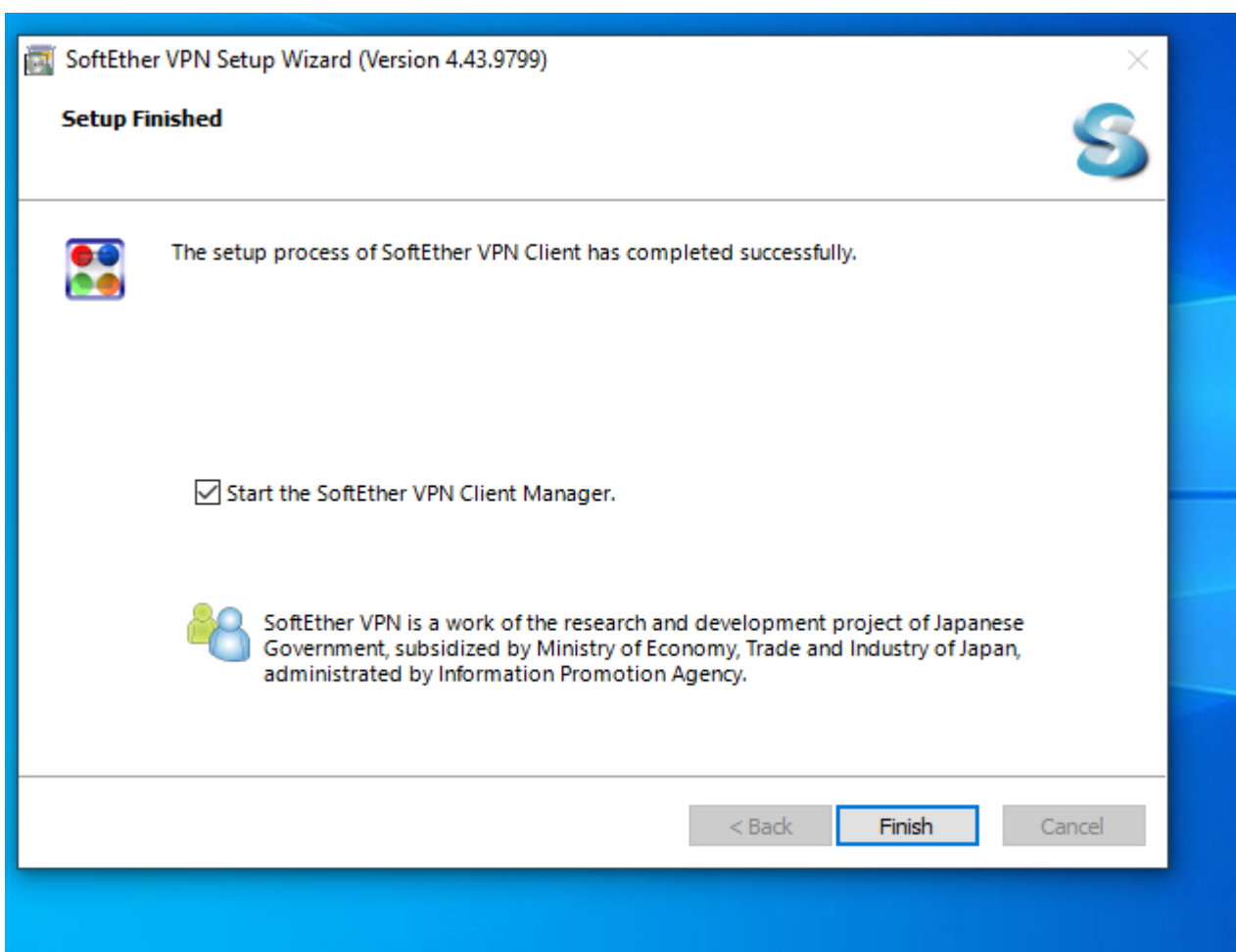
Màn hình khởi động ban đầu



Chọn **SoftEther VPN Client** rồi ấn **Next**



Đồng ý 1 số điều khoản và ấn **Finish** để kết thúc



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.

```
VPN Server/b21at012>UserCreate b21at012-long /GROUP:none /REALNAME: vuthanhlong /NOTE:none
UserCreate command - Create User
The command completed successfully.

VPN Server/b21at012>UserPasswordSet b21at012-long /PASSWORD: 15042003
UserPasswordSet command - Set Password Authentication for User Auth Type and Set Password
The command completed successfully.

VPN Server/b21at012>
```

New VPN Connection Setting Properties

Please configure the VPN Connection Setting for VPN Server.

Setting Name:

b21at012-vuthanlong

Destination VPN Server:

Specify the host name or IP address, and the port number and the Virtual Hub on the destination VPN Server.

Host Name:

192.168.136.134

Port Number:

443

☐ Disable NAT-T

Virtual Hub Name:

b21at012

Proxy Server as Relay:

You can connect to a VPN Server via a proxy server.

Import IE Proxy Server Settings

Proxy Type:

☒ Direct TCP/IP Connection (No Proxy)
☐ Connect via HTTP Proxy Server
☐ Connect via SOCKS Proxy Server

Proxy Server Setting

Server Certificate Verification Option:

☐ Always Verify Server Certificate

Manage Trusted CA Certificate List

Specify Individual Cert

Show Individual Cert

Virtual Network Adapter to Use:

VPN Client Adapter - VPN

User Authentication Setting:

Set the user authentication information that is required when connecting to the VPN Server.

Auth Type:

Standard Password Authentication

User Name:

b21at012-long

Password:

••••••••

You can change the user's password on the VPN Server.

Change Password

Advanced Setting of Communication:

☒ Reconnects Automatically After Disconnected

Reconnect Count:

times

Reconnect Interval:

5

seconds

☒ Infinite Reconnects (Keep VPN Always Online)

☐ Use SSL 3.0 (1)

Advanced Settings...






☐ Hide Status and Errors Screens

☐ Hide IP Address Screens

OK

Cancel

Thử kết nối: Nếu thành công sẽ báo connected.

SoftEther VPN Client Manager				
Connect Edit View Virtual Adapter Smart Card Tools Help				
VPN Connection Setting Name	Status	VPN Server Hostname	Virtual Hub	Virtual Network A...
 Add VPN Connection				
 b21at012-vuthanhlong	Connected	192.168.136.134 (Direct TCP/IP Con...	b21at012	VPN
Virtual Network Adapter Name		Status	MAC Address	Version
 VPN Client Adapter - VPN		Enabled	5E-AC-32-4D-6D-95	4.25.0.9658
SoftEther VPN Client Manager		 1 VPN Sessions		 SoftEther VPN Client Build 9799

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

```
2024-03-28 16:15:17.737 [HUB "b21at012"] Connection "CID-40": The new session "SID-B21AT012-LONG-1" has been created. (IP address: 192.168.136.131, Port number: 62536, Physical underlying protocol: "Standard TCP/IP (IPv4)")
2024-03-28 16:15:17.737 [HUB "b21at012"] Session "SID-B21AT012-LONG-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.
2024-03-28 16:15:17.748 [HUB "b21at012"] Session "SID-B21AT012-LONG-1": VPN Client details: (Client product name: "SoftEther VPN Client", Client version: 443, Client build number: 9799, Server product name: "SoftEther VPN Server (64 bit)", Server version: 443, Server build number: 9799, Client OS name: "Windows 10", Client OS version: "Build 19045, Multiprocessor Free (19041.vb_release.191206-1406)", Client product ID: "--", Client host name: "b21at012-long", Client IP address: "192.168.136.131", Client port number: 62536, Server host name: "192.168.136.134", Server IP address: "192.168.136.134", Server port number: 443, Proxy host name: "", Proxy IP address: "0.0.0.0", Proxy port number: 0, Virtual Hub name: "b21at012", Client unique ID: "10B73C0ED8E5770F7628403101A6B4E8")
2024-03-28 16:15:19.160 On the TCP Listener (Port 443), a Client (IP address 192.168.136.131, Host name "B21AT012-LONG", Port number 62538) has connected.
2024-03-28 16:15:19.160 For the client (IP address: 192.168.136.131, host name: "B21AT012-LONG", port number: 62538), connection "CID-41" has been created.
2024-03-28 16:15:19.185 SSL communication for connection "CID-41" has been started. The encryption algorithm name is "TLS_AES_256_GCM_SHA384".
2024-03-28 16:15:19.185 Connection "CID-41" has been terminated.
root@B21AT012-LongVT-VPNServer:/home/longvt/vpnserver/server_log#
```

Kết quả đạt được:

- 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 đến máy chủ

Tài liệu tham khảo

<https://cloudinfrastructureservices.co.uk/how-to-install-softether-vpn-server-on-ubuntu-20-04/>

<https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html#~types-of-vpns>

<https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn>

<https://www.expressvpn.com/what-is-vpn>