

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

BỘ MÔN THỰC TẬP CƠ SỞ



BÀI 7:
Cài đặt cấu hình VPN
server

Giảng viên : Nguyễn Ngọc Diệp
Sinh viên : Nguyễn Đức Anh
Mã sinh viên : B21DCAT031
Hệ : Đại học chính quy

Hà Nội, 3/2024

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

a. Tìm hiểu khái quát về VPN, các mô hình VPN và ứng dụng của VPN

VPN hay còn gọi là Virtual Private Network (mạng riêng ảo), cho phép người dùng thiết lập mạng riêng ảo với một mạng khác trên Internet.

VPN có thể được sử dụng để truy cập các trang web bị hạn chế truy cập về mặt vị trí địa lý, bảo vệ hoạt động duyệt web của bạn khỏi “sự tò mò” trên mạng Wifi công cộng bằng cách thiết lập mạng riêng ảo cho bạn.

VPN được ứng dụng để làm rất nhiều thứ như:

- Truy cập vào mạng doanh nghiệp khi ở xa: VPN thường được sử dụng bởi những người kinh doanh để truy cập vào mạng lưới kinh doanh của họ, bao gồm tất cả tài nguyên trên mạng cục bộ, trong khi đang đi trên đường, đi du lịch,... Các nguồn lực trong mạng nội bộ không cần phải tiếp xúc trực tiếp với Internet, nhờ đó làm tăng tính bảo mật.
- Truy cập mạng gia đình dù không ở nhà: Bạn có thể thiết lập VPN riêng để truy cập khi không ở nhà. Thao tác này sẽ cho phép truy cập Windows từ xa thông qua Internet, sử dụng tập tin được chia sẻ trong mạng nội bộ, chơi game trên máy tính qua Internet giống như đang ở trong cùng mạng LAN.
- Duyệt web ẩn danh: Nếu đang sử dụng WiFi công cộng, duyệt web trên những trang web không phải https, thì tính an toàn của dữ liệu trao đổi trong mạng sẽ dễ bị lộ. Nếu muốn ẩn hoạt động duyệt web của mình để dữ liệu được bảo mật hơn thì ta nên kết nối VPN. Mọi thông tin truyền qua mạng lúc này sẽ được mã hóa.
- Truy cập đến những website bị chặn giới hạn địa lý, bỏ qua kiểm duyệt Internet, vượt tường lửa,...
- Tải tập tin: Tải BitTorrent trên VPN sẽ giúp tăng tốc độ tải file. Điều này cũng có ích với các traffic mà ISP của bạn có thể gây trở ngại.

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

• Point-To-Point Tunneling Protocol (PPTP)

- Là giao thức được dùng để truyền dữ liệu qua các hầm - Tunnel giữa 2 tầng traffic trong Internet. L2TP cũng thường được dùng song song với IPSec (đóng vai trò là Security Layer đã đề cập đến ở phía trên) để đảm bảo quá trình truyền dữ liệu của L2TP qua môi trường Internet được thông suốt.
- Không giống như PPTP, VPN sẽ 'kế thừa' toàn bộ lớp L2TP/IPSec có các key xác thực tài khoản được chia sẻ hoặc là các Certificate.

• Giao thức L2TP

- L2TP là viết tắt của Layer 2 Tunneling Protocol, một giao thức tunneling (tạo "đường hầm" truyền dữ liệu qua các mạng). L2TP hỗ trợ tạo mạng riêng ảo VPN hoặc là một thành

phần của mạng phân phối dịch vụ của ISP. L2TP chỉ sử dụng mã hóa cho tin nhắn điều khiển mà không cung cấp bất cứ lớp mã hóa hay bảo mật nào cho nội dung dữ liệu.

***Cách hoạt động của L2TP:**

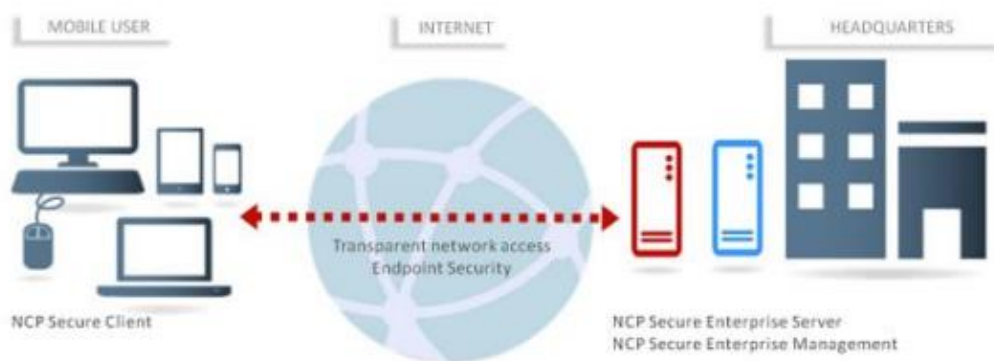
- Các gói tin L2TP bao gồm cả payload và header được gửi đi trong các gói tin UDP (User Datagram Protocol). Một ưu điểm của việc truyền qua UDP (chứ không phải TCP) là nó tránh được vấn đề TCP meltdown – khi hai giao thức truyền dẫn có điều khiển chồng lên nhau và xung đột khi cố sửa chữa vấn đề mất gói tin.
- Hai điểm cuối của đường hầm L2TP được gọi là bộ tập trung truy cập L2TP (LAC - L2TP Access Concentrator) và máy chủ mạng L2TP (LNS - L2TP Network Server). Lưu lượng mạng trong đường hầm là hai chiều, chia thành nhiều session sử dụng các giao thức cấp cao hơn như PPP. Cả LAC và LNS đều có thể khởi động một session, lưu lượng của mỗi session được cách ly bởi L2TP, vì vậy có thể thiết lập nhiều mạng ảo trên một đường hầm.

• Giao thức 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.

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

IP security (IPSec) được dùng để bảo mật các giao tiếp, các luồng dữ liệu trong môi trường Internet (môi trường bên ngoài VPN). Đây là điểm mấu chốt, lượng traffic qua IPSec được dùng chủ yếu bởi các Transport mode, hoặc các tunnel (hay gọi là hầm - khái niệm này hay dùng trong Proxy, SOCKS) để mã hóa dữ liệu trong VPN.



Sự khác biệt giữa các mode này là:

- Transport mode chỉ có nhiệm vụ mã hóa dữ liệu bên trong các gói (data package - hoặc còn biết dưới từ payload). Trong khi các Tunnel mã hóa toàn bộ các data package đó.
- Do vậy, IPSec thường được coi là Security Overlay, bởi vì IPSec dùng các lớp bảo mật so với các Protocol khác.

Secure Sockets Layer (SSL) và Transport Layer Security (TLS):

Có 1 phần tương tự như IPSec, 2 giao thức trên cũng dùng một mật khẩu để đảm bảo an toàn giữa các kết nối trong môi trường Internet.

d. Tìm hiểu về SoftEther VPN

SoftEther (Phần mềm Ethernet) là một trong những đa giao thức mạnh mẽ và dễ sử dụng nhất trên thế giới. Dự án SoftEther VPN khởi đầu là một dự án học thuật tại Đại học Tsukuba và là một Phần mềm VPN đa giao thức đa nền tảng mã nguồn mở miễn phí.

Hiện tại, SoftEther VPN hỗ trợ Windows, Linux, Mac, Solaris, FreeBSD và thường là một lựa chọn tốt để thay thế cho OpenVPN vì nhanh hơn. SoftEther VPN cũng hỗ trợ Microsoft SSTP VPN cho Windows Vista/7/8.

Bên cạnh ưu điểm nhanh, SoftEther VPN còn sử dụng key certificate AES 256 bit, một cấp độ bảo mật và mã hóa cao. Thêm một điểm cộng lớn cho phần mềm này là nó tích hợp tất cả các tính năng của các giao thức VPN khác nhau như PPTP, L2TP, OpenVPN và SSTP, trong khi loại bỏ nhược điểm của chúng.

Tất cả các tính năng mà SoftEther cung cấp, tăng cường khả năng giúp người dùng điều hướng an toàn và vượt qua mọi tường lửa do các bên chính quyền áp đặt, giúp nó trở thành một giao thức VPN phổ biến.

2.2 Tài liệu tham khảo

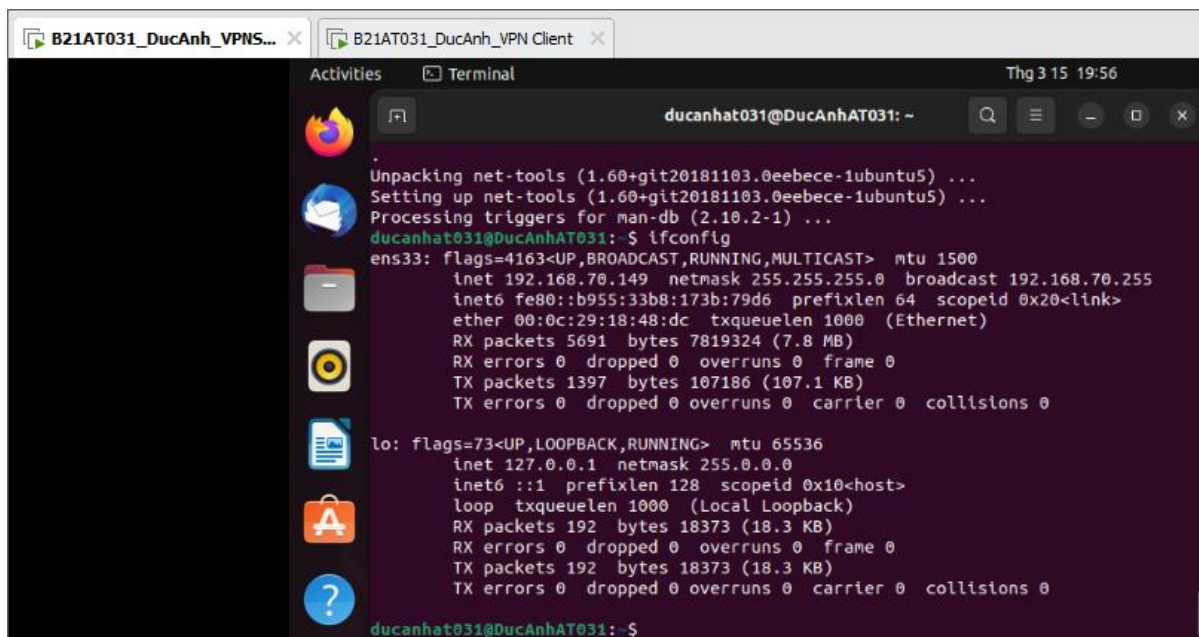
- <https://vncoder.vn/tin-tuc/cong-nghe/tong-quan-ve-vpn>
- <https://br.atsit.in/vi/?p=54681>
- <https://www.hocviendaotao.com/2013/03/giao-thuc-ipsec.html>
- <https://datatracker.ietf.org/doc/html/rfc8446>

2.3 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).
- 01 máy tính (máy thật hoặc máy ảo) chạy Kali Linux (bản 2021 trở lên)
- Bộ phần mềm Snort tải tại <https://www.snort.org/downloads>

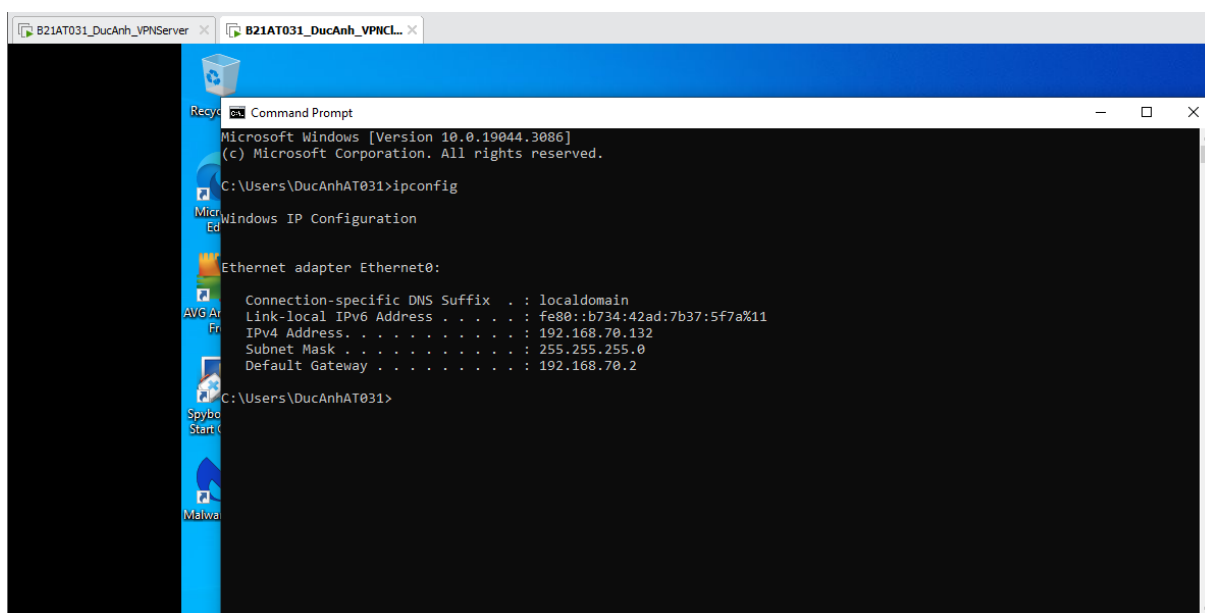
2.4 Các bước thực hiện

Bước 1: Chuẩn bị các máy ảo



The image shows a terminal window on a Linux system. The title bar indicates the user is 'ducanhat031' on a machine named 'DucAnhAT031'. The terminal output shows the installation of 'net-tools' and the execution of 'ifconfig'. The output for 'ens33' shows it is an Ethernet interface with IP 192.168.70.149 and a netmask of 255.255.255.0. The output for 'lo' shows it is a loopback interface with IP 127.0.0.1 and a netmask of 255.0.0.0.

```
ducanhat031@DucAnhAT031: ~  
*  
Unpacking net-tools (1.60+git20181103.0eebece-1ubuntu5) ...  
Setting up net-tools (1.60+git20181103.0eebece-1ubuntu5) ...  
Processing triggers for man-db (2.10.2-1) ...  
ducanhat031@DucAnhAT031: ~$ ifconfig  
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.70.149 netmask 255.255.255.0 broadcast 192.168.70.255  
    inet6 fe80::b955:33b8:173b:79d6 prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:18:48:dc txqueuelen 1000 (Ethernet)  
    RX packets 5691 bytes 7819324 (7.8 MB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 1397 bytes 107186 (107.1 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 192 bytes 18373 (18.3 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 192 bytes 18373 (18.3 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
ducanhat031@DucAnhAT031: ~$
```

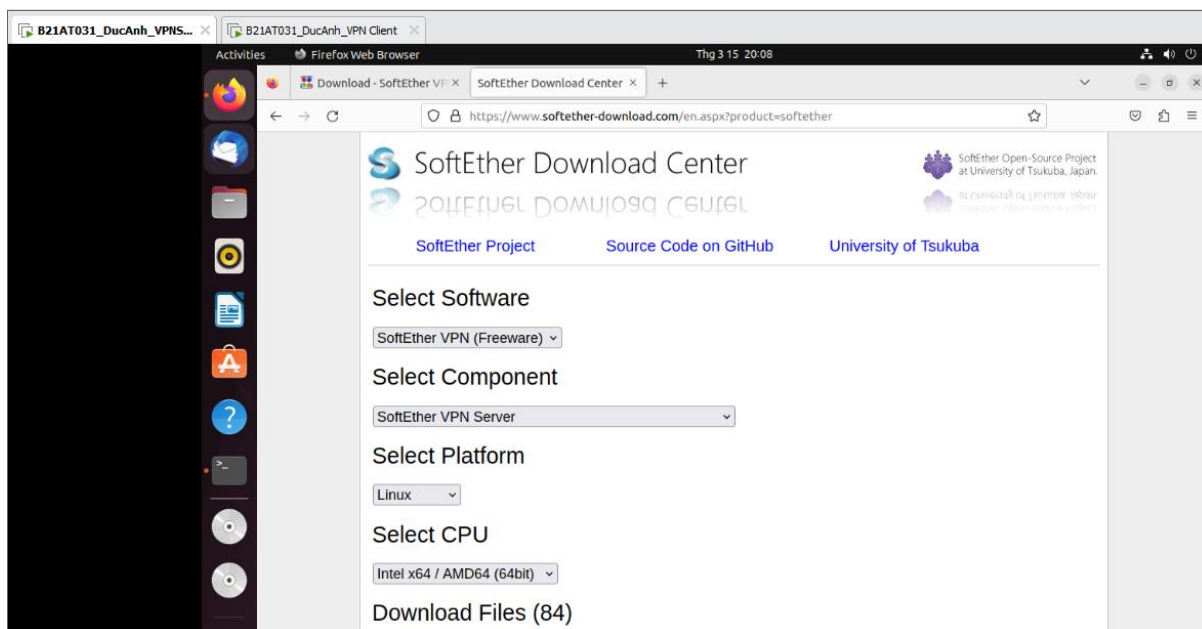


The image shows a Windows Command Prompt window. The title bar indicates the user is 'ducanhat031' on a machine named 'DucAnhAT031'. The command 'ipconfig' has been executed, and the output shows the IP configuration for the Ethernet adapter 'Ethernet0'. The output includes the connection-specific DNS suffix, link-local IPv6 address, IPv4 address, subnet mask, and default gateway.

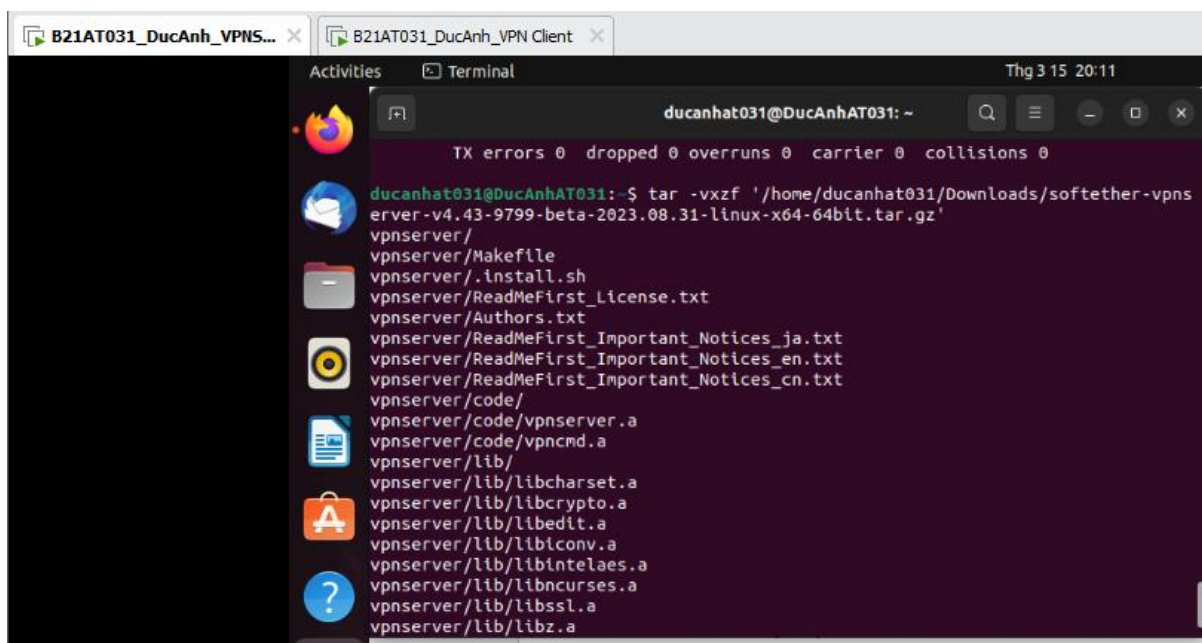
```
Microsoft Windows [Version 10.0.19044.3086]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\DucAnhAT031>ipconfig  
  
Windows IP Configuration  
  
Ethernet adapter Ethernet0:  
  
    Connection-specific DNS Suffix  . : localdomain  
    Link-local IPv6 Address . . . . . : fe80::b734:42ad:7b37:5f7a%11  
    IPv4 Address. . . . . : 192.168.70.132  
    Subnet Mask . . . . . : 255.255.255.0  
    Default Gateway . . . . . : 192.168.70.2  
  
C:\Users\DucAnhAT031>
```

Bước 2: Tải SoftEther VPN server , cài đặt và cấu hình VPN server

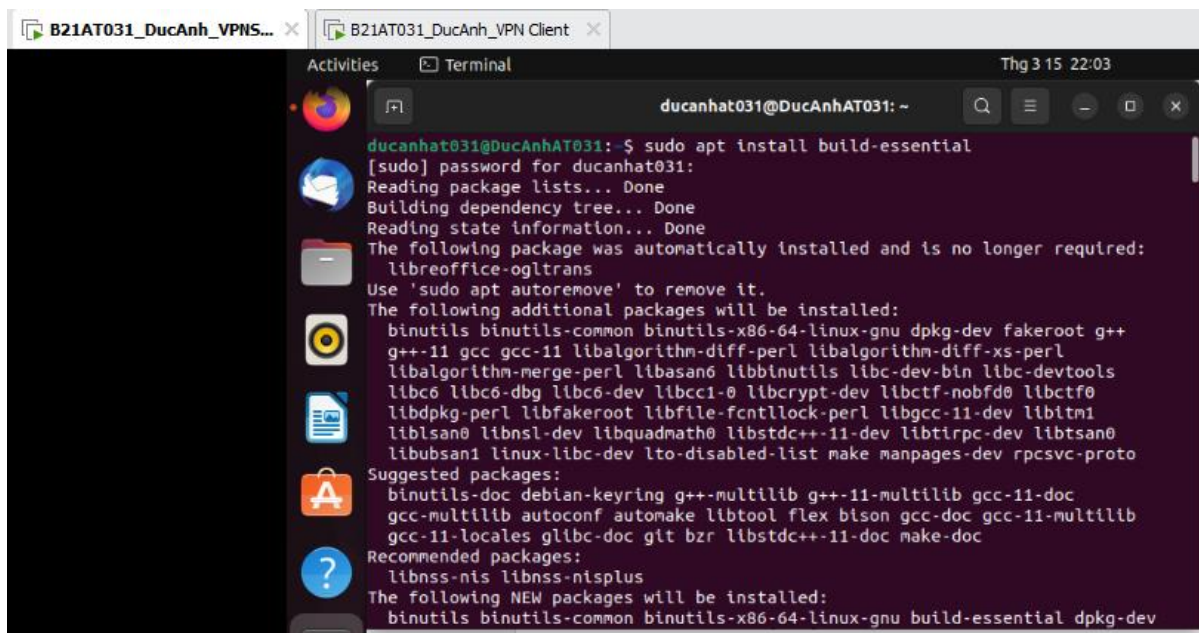
Ta tiến hành tải SoftEther VPN server trên máy Linux



Giải nén file vừa tải



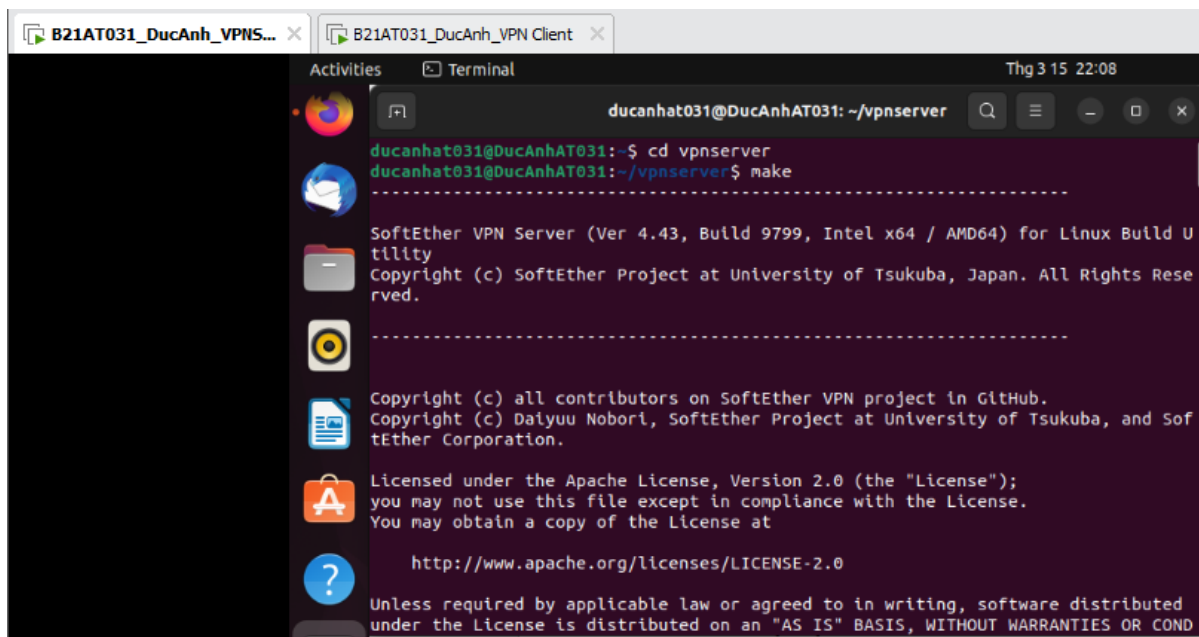
Cài trình dịch GCC



```
ducanhat031@DucAnhAT031: ~  
ducanhat031@DucAnhAT031:~$ sudo apt install build-essential  
[sudo] password for ducanhat031:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following package was automatically installed and is no longer required:  
  libreoffice-ogltrans  
Use 'sudo apt autoremove' to remove it.  
The following additional packages will be installed:  
  binutils binutils-common binutils-x86-64-linux-gnu dpkg-dev fakeroot g++  
  g++-11 gcc gcc-11 libalgorithm-diff-perl libalgorithm-diff-xs-perl  
  libalgorithm-merge-perl libasan6 libbinutils libc-dev-bin libc-devtools  
  libc6 libc6-dbg libc6-dev libcc1-0 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 make 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  
  gcc-11-locales glibc-doc glibc-dev libstdc++-11-doc make-doc  
Recommended packages:  
  libnss-nis libnss-nisplus  
The following NEW packages will be installed:  
  binutils binutils-common binutils-x86-64-linux-gnu build-essential dpkg-dev
```

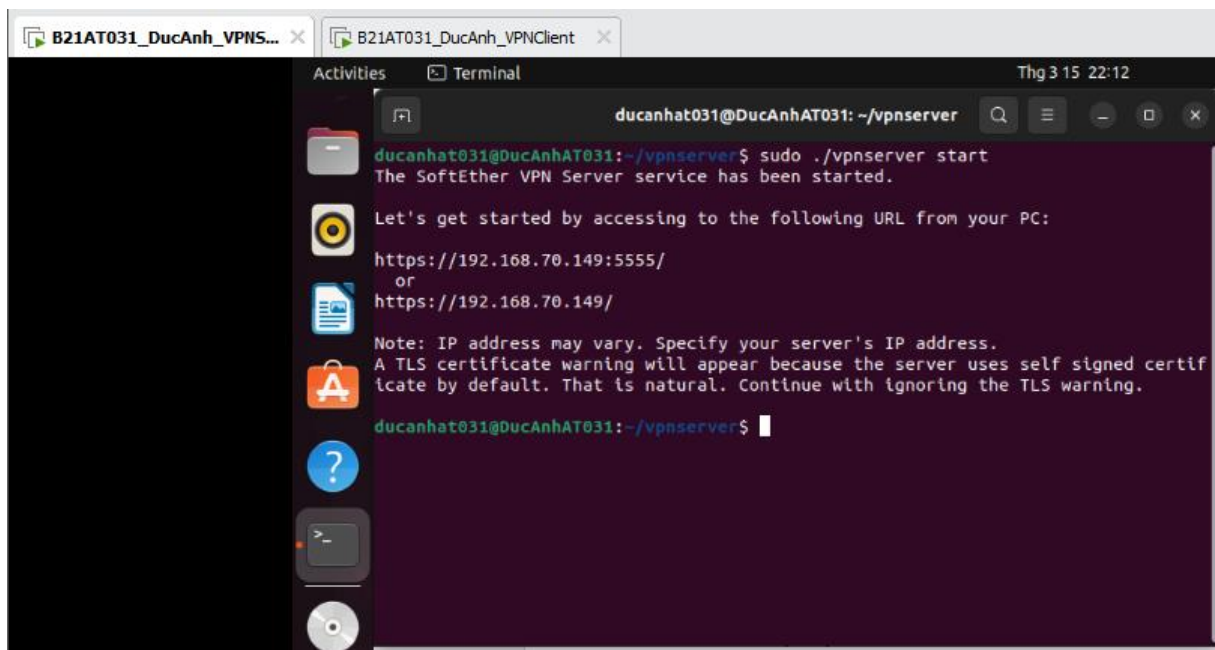
Chuyển vào thư mục VPN server: `cd vpnserver`.

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



```
ducanhat031@DucAnhAT031: ~/vpnserver  
ducanhat031@DucAnhAT031:~/vpnserver$ cd vpnserver  
ducanhat031@DucAnhAT031:~/vpnserver$ make  
-----  
SoftEther VPN Server (Ver 4.43, Build 9799, Intel x64 / AMD64) for Linux Build U  
tility  
Copyright (c) SoftEther Project at University of Tsukuba, Japan. All Rights Rese  
rved.  
-----  
Copyright (c) all contributors on SoftEther VPN project in GitHub.  
Copyright (c) Daiyuu Nobori, SoftEther Project at University of Tsukuba, and Sof  
tEther 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 COND
```

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



A terminal window titled 'ducanh031@DucAnhAT031: ~/vpnservice' showing the execution of the command `sudo ./vpnservice start`. The output indicates that the SoftEther VPN Server service has been started. It provides two URLs for access: `https://192.168.70.149:5555/` or `https://192.168.70.149/`. A note mentions that a TLS certificate warning will appear due to a self-signed certificate, which should be ignored. The prompt returns to `ducanh031@DucAnhAT031:~/vpnservice$`.

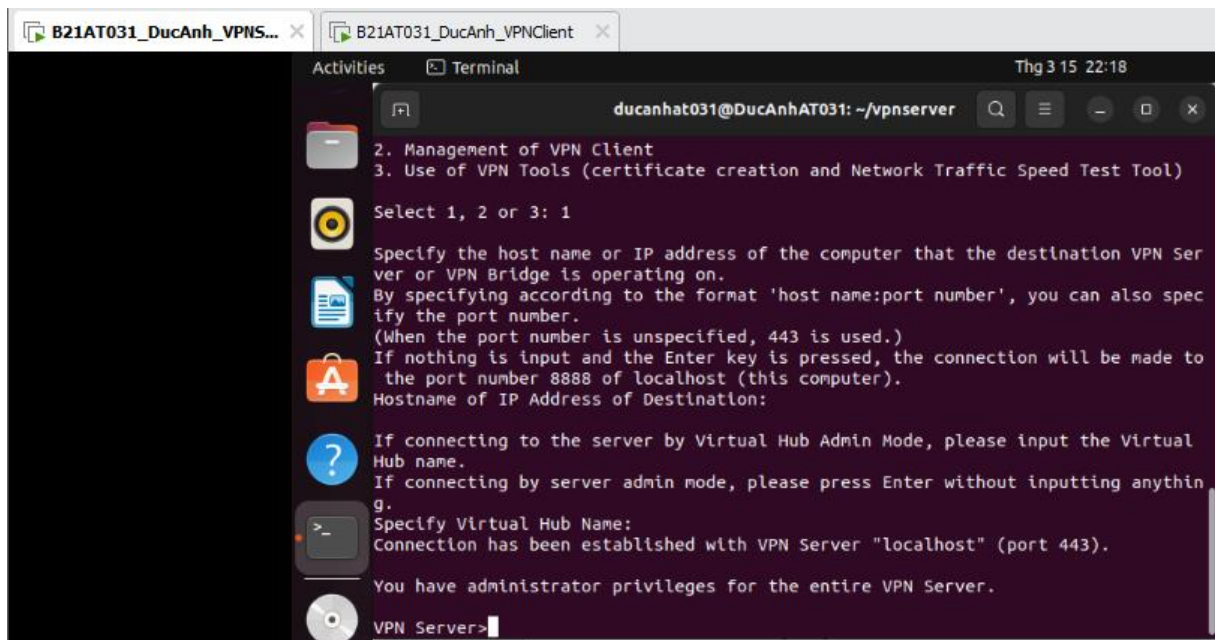
```
ducanh031@DucAnhAT031:~/vpnservice$ sudo ./vpnservice start
The SoftEther VPN Server service has been started.

Let's get started by accessing to the following URL from your PC:
https://192.168.70.149:5555/
or
https://192.168.70.149/

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.

ducanh031@DucAnhAT031:~/vpnservice$
```

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



A terminal window titled 'ducanh031@DucAnhAT031: ~/vpnservice' showing the execution of the command `./vpncmd`. The output displays a menu with three options: '2. Management of VPN Client', '3. Use of VPN Tools (certificate creation and Network Traffic Speed Test Tool)', and 'Select 1, 2 or 3: 1'. It then prompts for the host name or IP address of the destination VPN Server or VPN Bridge, with instructions on the format 'host name:port number'. It specifies that if the port number is unspecified, 443 is used, and if nothing is input and the Enter key is pressed, the connection will be made to the port number 8888 of localhost (this computer). It then prompts for the Virtual Hub name, stating that if connecting by server admin mode, the user should press Enter without inputting anything. It then prompts for the Virtual Hub Name, and the output shows 'Connection has been established with VPN Server "localhost" (port 443)'. It also states 'You have administrator privileges for the entire VPN Server.' and ends with the prompt 'VPN Server>'. The prompt returns to `ducanh031@DucAnhAT031:~/vpnservice$`.

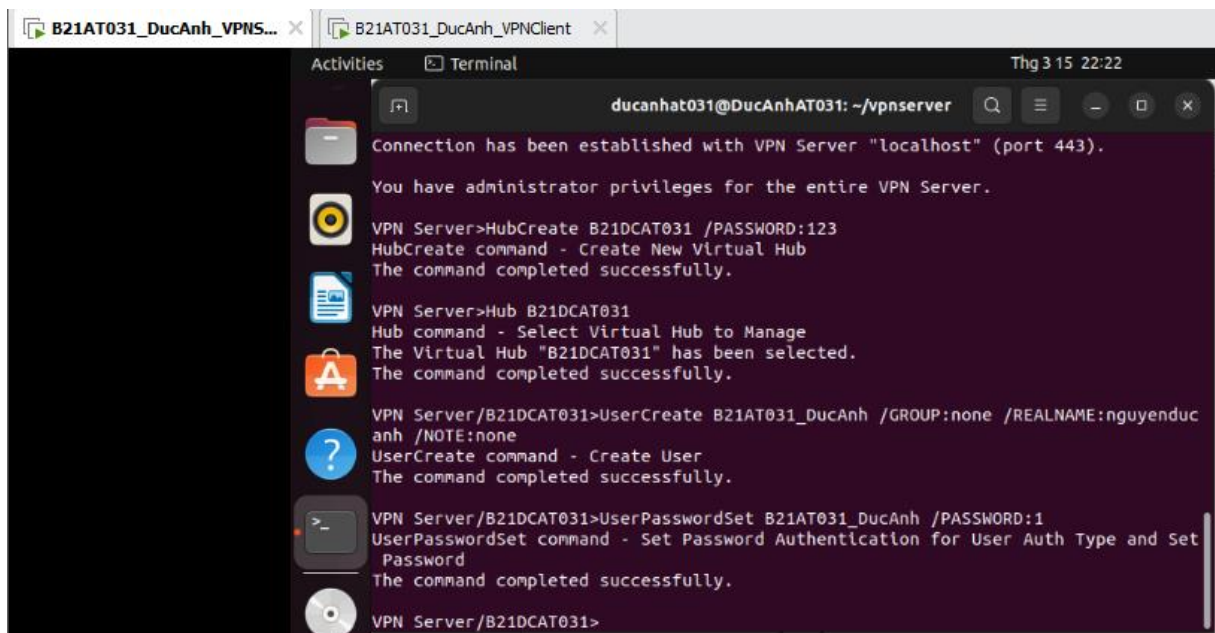
```
2. Management of VPN Client
3. Use of VPN Tools (certificate creation and Network Traffic Speed Test Tool)
Select 1, 2 or 3: 1

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>

ducanh031@DucAnhAT031:~/vpnservice$
```

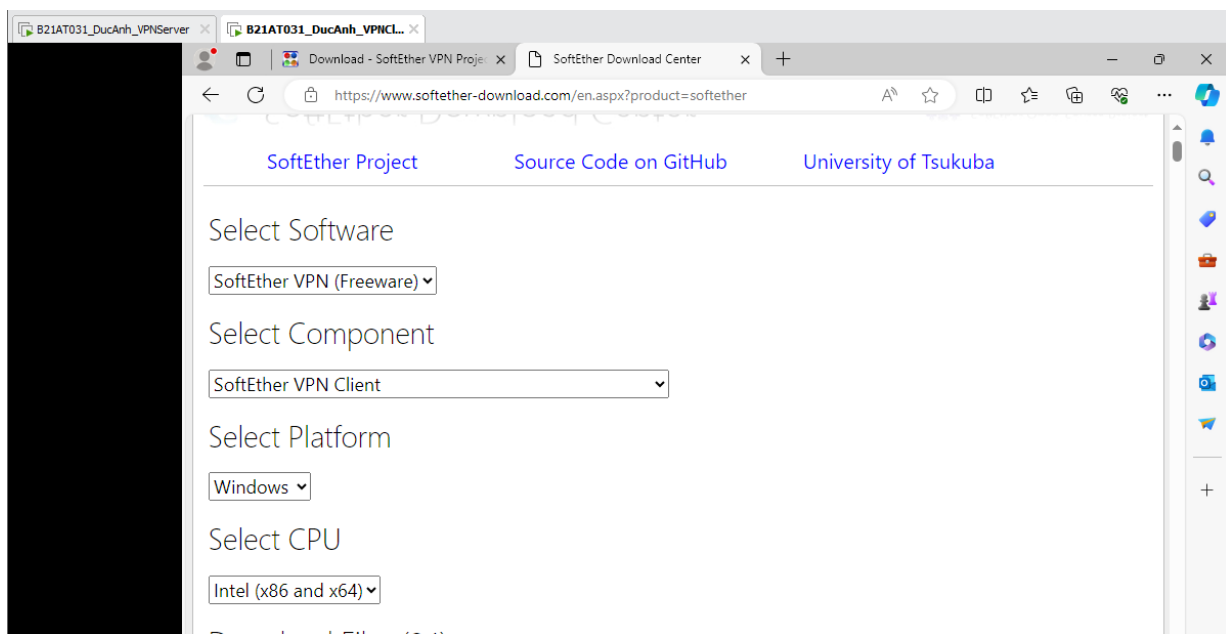
Tiếp theo tiến hành tạo Hub mới, tạo User trong Hub và thiết lập mật khẩu cho user.

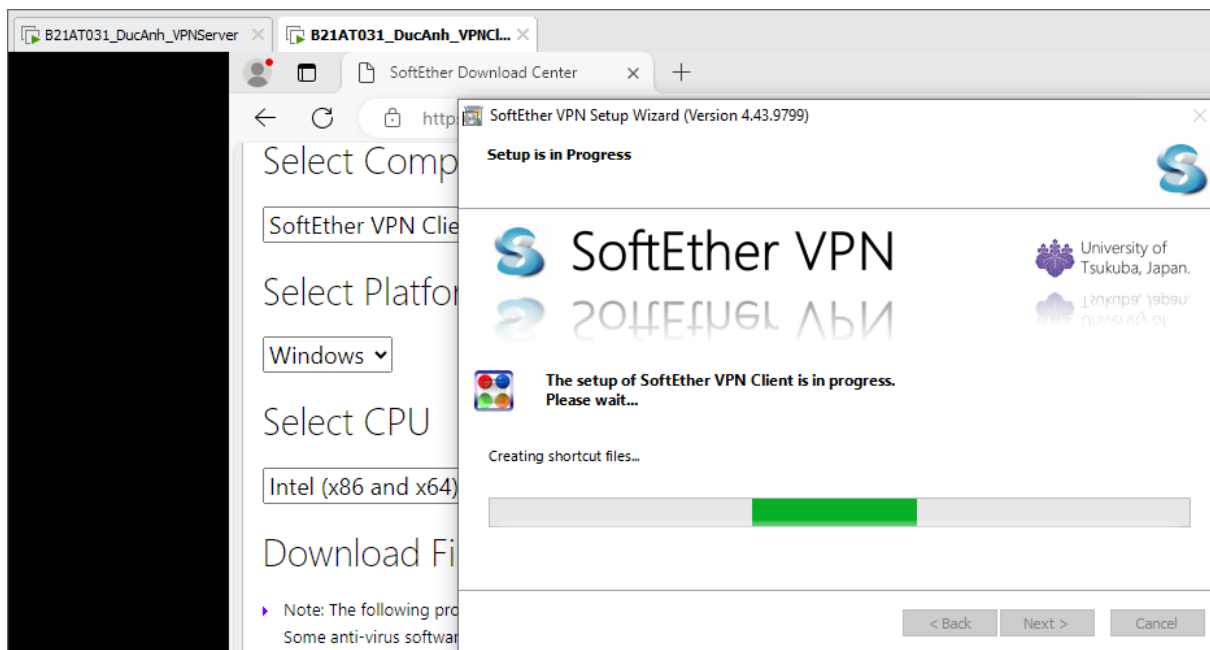


```
ducanhat031@DucAnhAT031: ~/vpnsrvr
Connection has been established with VPN Server "localhost" (port 443).
You have administrator privileges for the entire VPN Server.
VPN Server>HubCreate B21DCAT031 /PASSWORD:123
HubCreate command - Create New Virtual Hub
The command completed successfully.
VPN Server>Hub B21DCAT031
Hub command - Select Virtual Hub to Manage
The Virtual Hub "B21DCAT031" has been selected.
The command completed successfully.
VPN Server/B21DCAT031>UserCreate B21AT031_DucAnh /GROUP:none /REALNAME:nguyenduc
anh /NOTE:none
UserCreate command - Create User
The command completed successfully.
VPN Server/B21DCAT031>UserPasswordSet B21AT031_DucAnh /PASSWORD:1
UserPasswordSet command - Set Password Authentication for User Auth Type and Set
Password
The command completed successfully.
VPN Server/B21DCAT031>
```

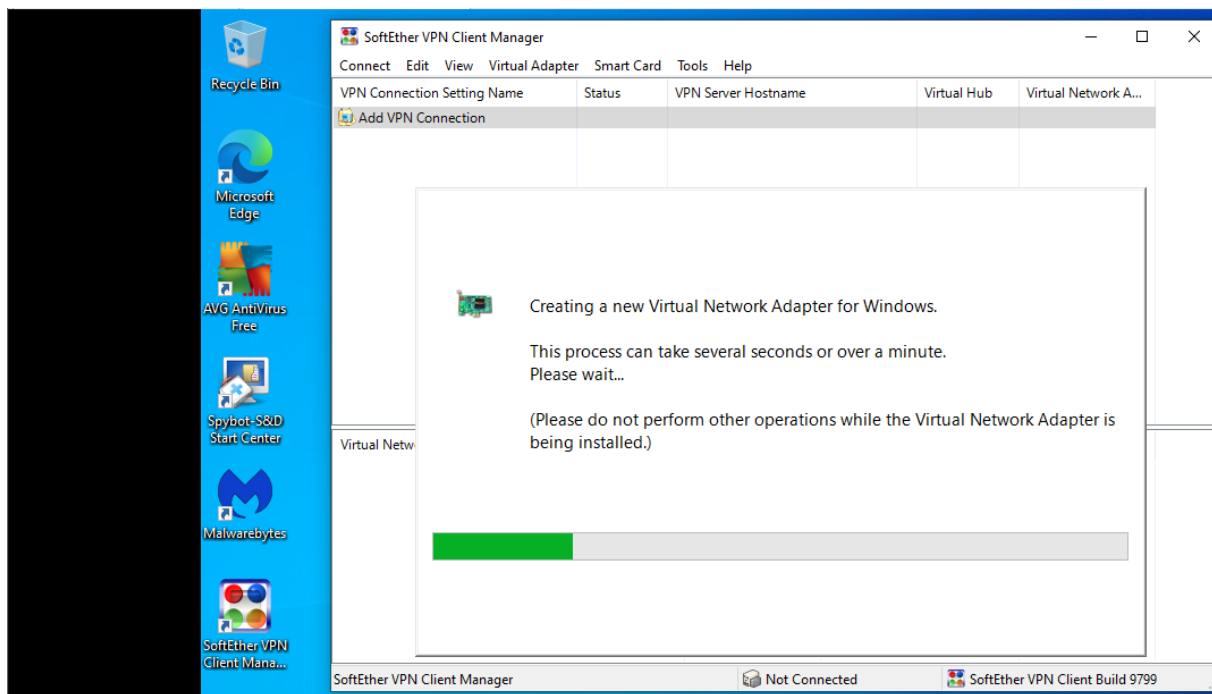
Bước 3: Tải SoftEther VPN client cho Windows

Tiến hành tải và cài đặt VPN client cho máy Windows.



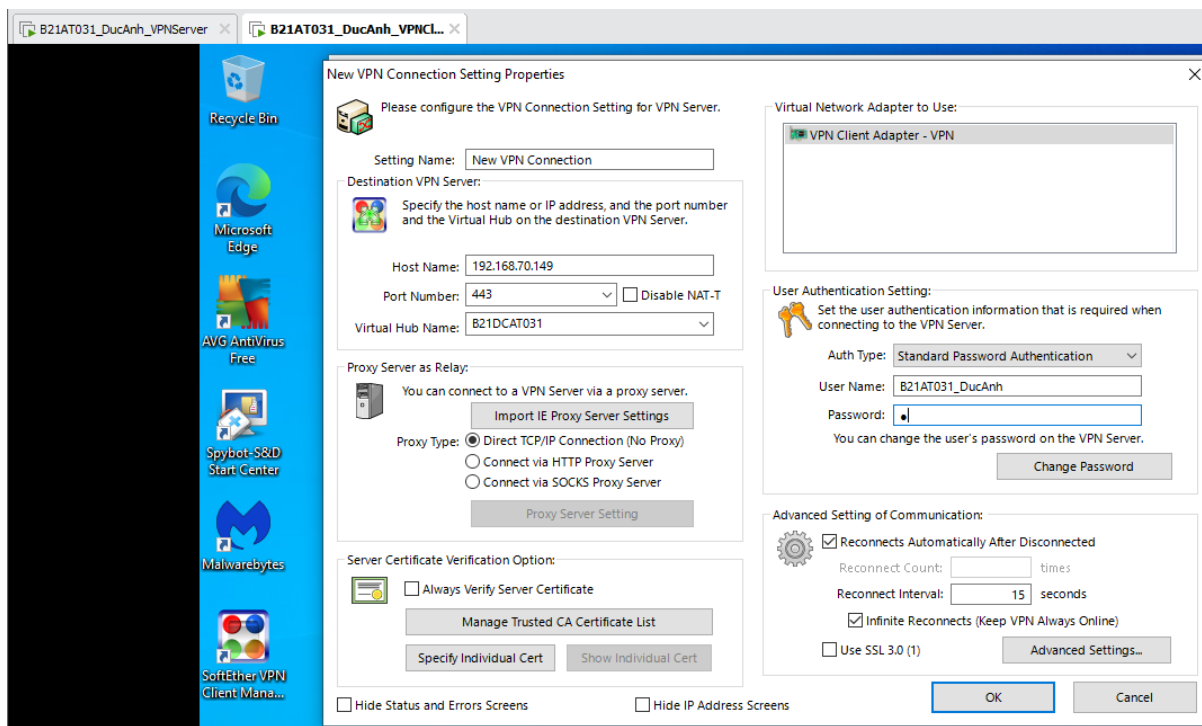


Trước hết ta tạo một Virtual Network Adapter mới

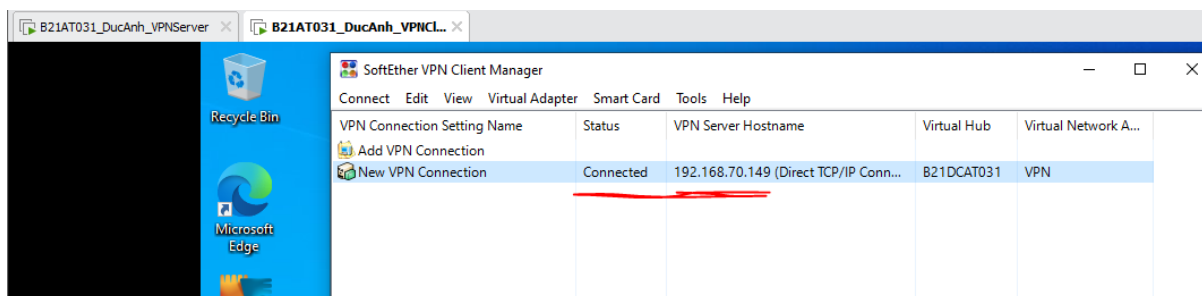


Tạo và kiểm tra kết nối VPN:

- 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



Thử kết nối: Nếu thành công sẽ báo connected

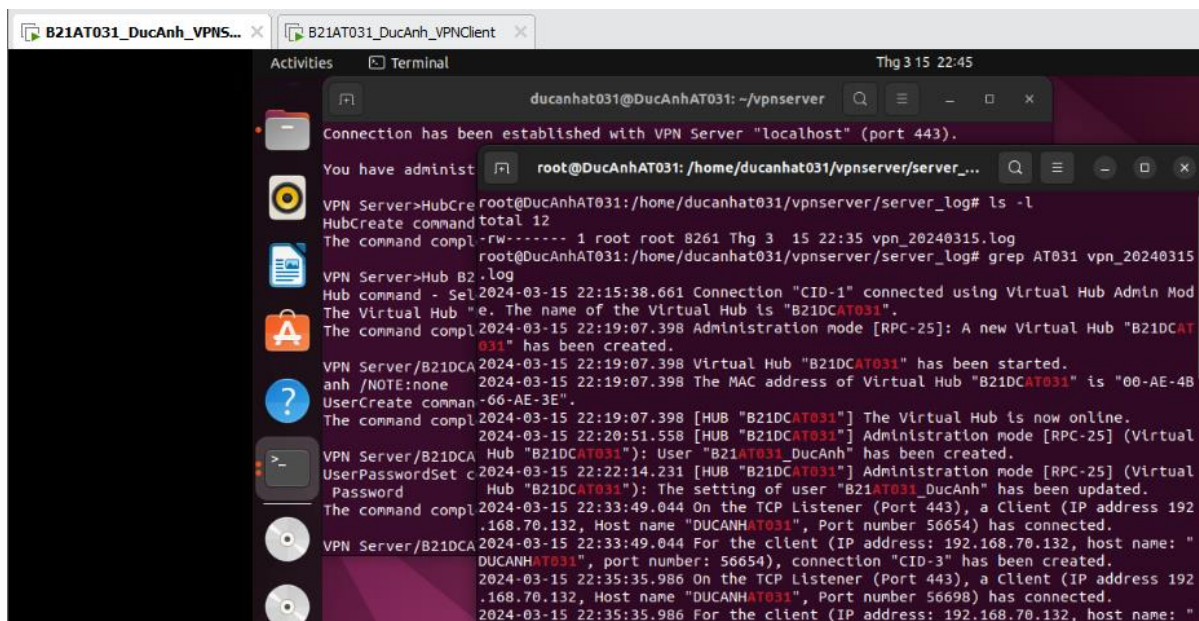


Kiểm tra kết nối bên máy chủ: Chuyển sang máy chủ VPN, mở 1 terminal mới chuyển đến thư mục bai7ttcs/vpnserver/server_log để kiểm tra log trên VPN server:

```
cd vpnserver/server_log
```

```
sudo grep AT031 20240315.log
```

Ta sẽ có thể xem được các dòng log có liên quan đến AT031



```
ducanhat031@DucAnhAT031: ~/vpnsrvr
Connection has been established with VPN Server "localhost" (port 443).
You have administ
VPN Server>HubCre
HubCreate command total 12
The command compl
root@DucAnhAT031: /home/ducanhat031/vpnsrvr/server_log# ls -l
root@DucAnhAT031: /home/ducanhat031/vpnsrvr/server_log# grep AT031 vpn_20240315.log
VPN Server>Hub B2
Hub command - Sel
The Virtual Hub "e. The name of the Virtual Hub is "B21DCAT031".
The command compl
2024-03-15 22:19:07.398 Administration mode [RPC-25]: A new Virtual Hub "B21DCAT031" has been created.
VPN Server/B21DCA
2024-03-15 22:19:07.398 Virtual Hub "B21DCAT031" has been started.
anh /NOTE:none
2024-03-15 22:19:07.398 The MAC address of Virtual Hub "B21DCAT031" is "00-AE-4B
UserCreate comman
-66-AE-3E".
The command compl
2024-03-15 22:19:07.398 [HUB "B21DCAT031"] The Virtual Hub is now online.
2024-03-15 22:20:51.558 [HUB "B21DCAT031"] Administration mode [RPC-25] (Virtual
VPN Server/B21DCA
Hub "B21DCAT031"): User "B21AT031_DucAnh" has been created.
UserPasswordSet c
2024-03-15 22:22:14.231 [HUB "B21DCAT031"] Administration mode [RPC-25] (Virtual
Hub "B21DCAT031"): The setting of user "B21AT031_DucAnh" has been updated.
Password
The command compl
2024-03-15 22:33:49.044 On the TCP Listener (Port 443), a Client (IP address 192
.168.70.132, Host name "DUCANHAT031", Port number 56654) has connected.
VPN Server/B21DCA
2024-03-15 22:33:49.044 For the client (IP address: 192.168.70.132, host name: "
DUCANHAT031", port number: 56654), connection "CID-3" has been created.
2024-03-15 22:35:35.986 On the TCP Listener (Port 443), a Client (IP address 192
.168.70.132, Host name "DUCANHAT031", Port number 56698) has connected.
2024-03-15 22:35:35.986 For the client (IP address: 192.168.70.132, host name: "
```

3. 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