

**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**  
**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**  
**KHOA AN TOÀN THÔNG TIN**

-----



**MÔN HỌC: THỰC TẬP CƠ SỞ**  
**BÁO CÁO BÀI THỰC HÀNH SỐ 7**

**Giảng viên hướng dẫn : PGS.TS Hoàng Xuân Dậu**  
**Sinh viên thực hiện : Nguyễn Nhật Minh**  
**Mã sinh viên : B21DCAT132**

**Hà Nội, tháng 3 năm 2024**

# Môn học Thực tập cơ sở

## Bài 7: Cài đặt cấu hình VPN server

### 1. Mục đích

- Tìm hiểu về mạng riêng ảo VPN, kiến trúc và hoạt động của mạng riêng ảo
- Luyện tập kỹ năng cài đặt, cấu hình và vận hành máy chủ VPN server

### 2. Tìm hiểu lý thuyết

#### 2.1. Mạng riêng ảo VPN là gì

VPN là từ viết tắt của Virtual Private Network, hay còn gọi là mạng riêng ảo, mạng ảo. Đây là một công nghệ mạng giúp tạo nên những kết nối mạng an toàn khi tham gia mạng riêng của nhà cung cấp dịch vụ hoặc mạng công cộng internet, intranet. Mỗi hệ thống mạng riêng ảo có thể kết nối với nhiều site khác nhau dựa trên diện tích địa lý, khu vực. Bởi vậy, ta mới thấy các cơ quan chính phủ có thể cho phép người dùng kết nối an toàn đến mạng riêng của chính phủ, đó là nhờ có mạng riêng ảo VPN. Khái niệm mạng riêng ảo VPN.

Để kết nối vào mạng riêng ảo VPN, bạn cần có một tài khoản với tên và mật khẩu. Đồng thời, bạn cũng sẽ được cấp quyền truy cập thông qua việc xác nhận tài khoản với mã pin. Mã pin đó thường sẽ áp dụng trong khoảng thời gian nhất định từ 30s – 1 phút. Bạn có thể kết nối VPN với máy tính, điện thoại giống như nó đang nằm trên cùng mạng nội bộ. Tất cả traffic đều được gửi qua và kết nối an toàn đến VPN. Do đó, bạn hoàn toàn có thể yên tâm về độ bảo mật tài nguyên mạng nội bộ.

Bên cạnh đó, bạn cũng có thể sử dụng internet như đang ở vị trí VPN, rất tiện cho việc sử dụng wifi public, truy cập web giới hạn địa lý hay bị chặn. Để duyệt web với VPN, máy tính sẽ liên hệ web thông qua kết nối VPN mã hóa. Tất cả thông tin, yêu cầu, dữ liệu trao đổi giữa bạn với website sẽ được bảo vệ trong một kết nối an toàn.

#### 2.2. Các mô hình VPN

Trên thị trường hiện nay có rất nhiều loại mạng riêng ảo. Một số cái tên phổ biến bao gồm: PPTP, Site to Site, L2TP, IPSec, SSL, MPLS, và Hybrid.

##### • PPTP

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. Quả là một cái tên khá dài cho mạng VPN được sử dụng nhiều nhất. 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, bạn 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.

Bên cạnh rất nhiều ưu điểm, 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

- Site to Site VPN

Site to Site VPN còn có tên gọi khác là Router to Router VPN. Nó thường được dùng trong các công ty và tổ chức đoàn thể. Ngày nay, nhiều công ty có văn phòng đặt ở cả trong và ngoài nước; do đó, họ dùng mạng Site to Site VPN để kết nối mạng lưới của văn phòng chính với các văn phòng còn lại. Hình thức kết nối này gọi là "Intranet" (mạng cục bộ). Ngoài ra, mạng Site to Site còn hữu ích trong việc thiết lập đường truyền giữa các công ty với nhau, gọi là "Extranet" (mạng mở rộng). Nói một cách dễ hiểu, Site to Site VPN xây dựng một chiếc cầu ảo kết nối các mạng lưới ở cách xa nhau lại với nhau thông qua đường truyền Internet, đảm bảo việc truyền tải thông tin được an toàn và bảo mật.

Tương tự như PPTP VPN, Site to Site VPN cũng được dùng để đảm bảo an toàn cho mạng lưới. Tuy nhiên, vì không sử dụng đường line tĩnh nên mọi vị trí trong mạng lưới của công ty đều có thể hợp thành một mạng riêng ảo. Khác với PPTP, quá trình định tuyến, mã hóa, và giải mã đều được thực hiện bởi các bộ định tuyến sử dụng phần cứng hoặc phần mềm đặt ở 2 đầu 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

- Ip sec

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 và 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.

- MPLS VPN

Chuyển mạch nhãn đa giao thức (MPLS) là một công nghệ được dùng nhiều nhất cho kết nối Site to Site. Nguyên nhân là vì MPLS là lựa chọn có tính linh hoạt và khả năng thích nghi cao nhất. MPLS là một nguồn dựa trên các tiêu chuẩn được dùng để tăng tốc độ phân chia các gói mạng lưới thông qua nhiều giao thức khác nhau. Mạng MPLS VPN là những hệ thống mạng VPN điều chỉnh bởi các nhà cung cấp dịch vụ Internet. Mạng VPN điều chỉnh bởi các nhà cung cấp dịch vụ Internet là một mạng lưới được hình thành khi có từ 2 máy trở lên kết nối với nhau và sử dụng cùng 1 nhà cung cấp dịch vụ Internet. Nhược điểm lớn nhất của MPLS là không dễ gì để thiết lập cho 2 mạng VPN tương thích với nhau. Quá trình chỉnh sửa cũng khá khó khăn. Chính vì vậy mà sử dụng MPLS thường đắt tiền hơn các giải pháp khác.

- Hybrid VPN

Mạng VPN lai là sự kết hợp giữa MPLS VPN và IPSec VPN. Dù 2 loại mạng riêng ảo này thường được sử dụng cho các mục đích khác nhau, nhưng chúng ta vẫn có thể kết hợp chúng lại với nhau. Mục đích là dùng IPSec VPN làm phương án dự phòng cho MPLS.

Như tôi đã đề cập, người dùng IPSec cần một số thiết bị để sử dụng dịch vụ. Đó

thường là bộ định tuyến hoặc ứng dụng bảo mật đa nhiệm. Thông qua các thiết bị này, dữ liệu sẽ được mã hóa và hình thành một đường hầm VPN như tôi đã giải thích ở trên. MPLS VPN được dùng bởi các carrier (vật mang), với sự trợ giúp từ các thiết bị trong mạng lưới của carrier.

Để có thể kết hợp IPSec và MPLS, một cổng sẽ được thiết lập để loại bỏ đường hầm IPSec từ một phía và đưa nó vào MPLS ở cuối đầu bên kia, trong khi vẫn phải đảm bảo sự an toàn cho dữ liệu của người dùng.

Mạng VPN lai chủ yếu được dùng trong các công ty, vì MPLS có lẽ không phải là lựa chọn phù hợp nhất. MPLS có rất nhiều ưu điểm so với mạng Internet thông thường, tuy nhiên giá thành rất cao. Vì vậy, sử dụng mạng VPN lai cho phép họ truy cập đến máy chủ trung tâm từ một vị trí khác. Mạng VPN lai cũng không phải là rẻ, nhưng bù lại nó rất linh hoạt.

### 2.3. Ứng dụng của VPN

- Quyền riêng tư

Nếu không có mạng riêng ảo, dữ liệu cá nhân của bạn như mật khẩu, thông tin thẻ tín dụng và lịch sử duyệt web có thể bị ghi lại và rao bán bởi các bên thứ ba. VPN sử dụng mã hóa để giữ bí mật những thông tin này, đặc biệt là khi bạn kết nối qua mạng Wi-Fi công cộng.

- Ẩn danh

Địa chỉ IP chứa thông tin về vị trí và hoạt động duyệt web của bạn. Tất cả các trang web trên Internet theo dõi dữ liệu này bằng cookie và công nghệ tương tự. Họ có thể nhận dạng bạn bất cứ khi nào bạn ghé thăm trang web của họ. Kết nối VPN sẽ ẩn địa chỉ IP của bạn, để bạn được ẩn danh trên Internet.

- Bảo mật

Dịch vụ VPN sử dụng mật mã để bảo vệ kết nối Internet của bạn khỏi những truy cập trái phép. VPN cũng có thể hoạt động như một cơ chế tắt, hủy bỏ các chương trình được chọn trước đó phòng khi có hoạt động đáng ngờ trên Internet. Việc này làm giảm khả năng dữ liệu bị xâm phạm. Những tính năng trên cho phép các công ty cấp quyền truy cập từ xa cho người dùng được ủy quyền thuộc mạng lưới kinh doanh của họ

### 2.4. SoftEther VPN

SoftEther VPN, mặc dù có tên gọi có vẻ nhẹ nhàng với tiền tố “Soft,” nhưng thực chất lại là một công cụ VPN vô cùng mạnh mẽ. Bắt nguồn từ một nghiên cứu học thuật tại Đại học Tsukuba, SoftEther không chỉ là một sản phẩm miễn phí mã nguồn mở mà còn là một giải pháp VPN đa giao thức đa nền tảng.

Một trong những điểm đặc trưng của SoftEther là khả năng hỗ trợ nhiều hệ điều hành, từ

Windows đến Linux, Mac, Solaris và FreeBSD. Với tốc độ hoạt động vượt trội, nó thường được xem xét như một phiên bản nâng cấp của OpenVPN. Đặc biệt, SoftEther còn tương thích với giao thức Microsoft SSTP VPN, một tính năng rất có ích cho người dùng Windows Vista/7/8.

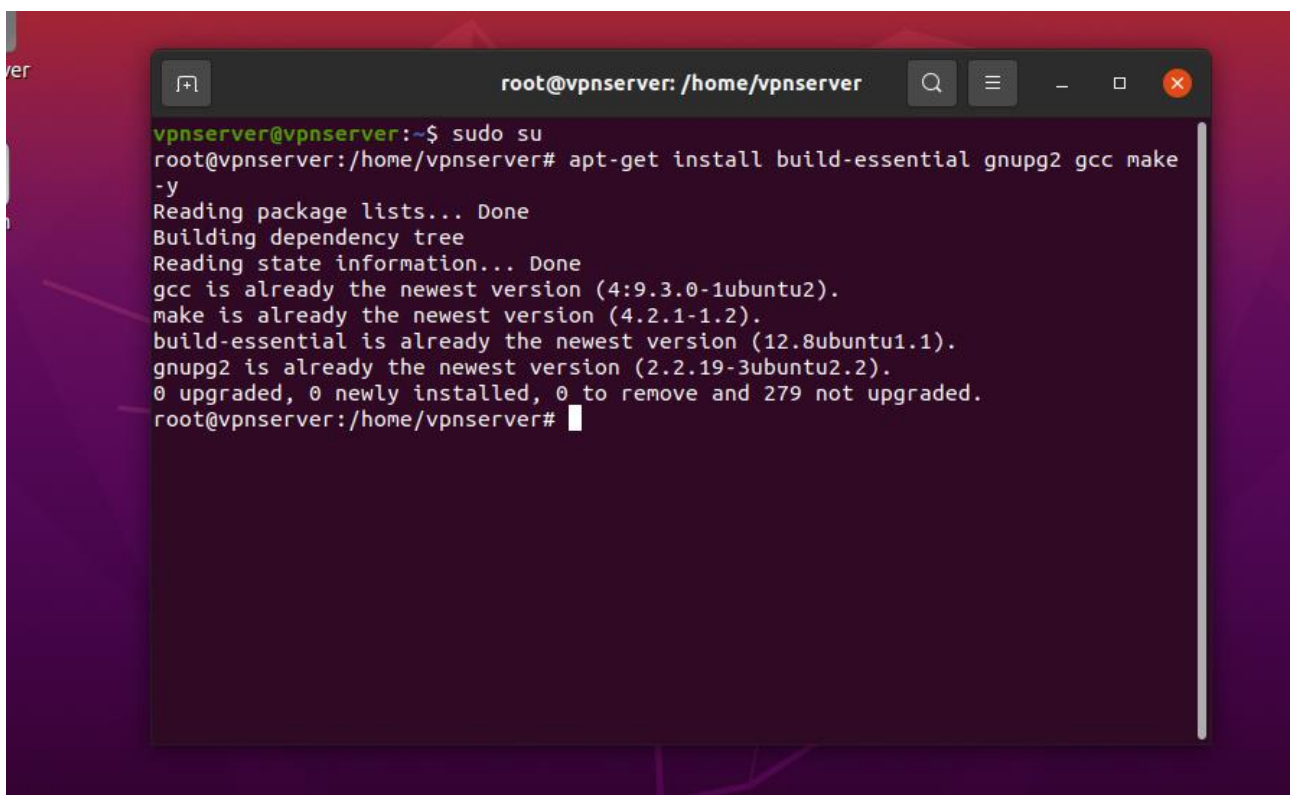
Tính bảo mật của SoftEther cũng đáng kể. Bằng việc sử dụng key certificate AES 256-bit, phần mềm này đảm bảo một cấp độ bảo mật và mã hóa hàng đầu. Điểm mạnh tiếp theo của SoftEther là khả năng kết hợp những tính năng tốt nhất từ các giao thức VPN khác như PPTP, L2TP, OpenVPN và SSTP, trong khi đồng thời loại bỏ đi những hạn chế của chúng.

### 3. Chuẩn bị môi trường

- 1 máy ảo ubuntu linux cài đặt VPN server
- 1 máy ảo window cài đặt VPN client

### 4. Thực hành

- Cài đặt trình biên dịch gcc



```
root@vpnserver: /home/vpnserver
vpnserver@vpnserver:~$ sudo su
root@vpnserver:/home/vpnserver# apt-get install build-essential gnupg2 gcc make
-y
Reading package lists... Done
Building dependency tree
Reading state information... Done
gcc is already the newest version (4:9.3.0-1ubuntu2).
make is already the newest version (4.2.1-1.2).
build-essential is already the newest version (12.8ubuntu1.1).
gnupg2 is already the newest version (2.2.19-3ubuntu2.2).
0 upgraded, 0 newly installed, 0 to remove and 279 not upgraded.
root@vpnserver:/home/vpnserver#
```

### - Sử dụng wget tải vpnserver về máy

```
vpnserver@vpnserver:~$ wget http://www.softether-download.com/files/softether/v4.38-9760-rtm-2021.08.17-tree/Linux/SoftEther_VPN_Server/64bit_-_Intel_x64_or_AMD64/softether-vpnserver-v4.38-9760-rtm-2021.08.17-linux-x64-64bit.tar.gz
--2024-03-13 21:08:29-- http://www.softether-download.com/files/softether/v4.38-9760-rtm-2021.08.17-tree/Linux/SoftEther_VPN_Server/64bit_-_Intel_x64_or_AMD64/softether-vpnserver-v4.38-9760-rtm-2021.08.17-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]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7529219 (7,2M) [application/x-gzip]
Saving to: 'softether-vpnserver-v4.38-9760-rtm-2021.08.17-linux-x64-64bit.tar.gz'

softether-v 49%[=====] 3,59M 53,8KB/s eta 52s
```

### - Giải nén bằng lệnh tar

```
vpnserver@vpnserver:~$ ls
Desktop  Downloads  Pictures  softether-vpnserver-v4.38-9760-rtm-2021.08.17-linux-x64-64bit.tar.gz  Videos
Documents Music      Public    Templates

vpnserver@vpnserver:~$ tar -xvzf softether-vpnserver-v4.38-9760-rtm-2021.08.17-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/vpnserver.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
vpnserver@vpnserver:~$
```

### - Mở tệp vpnserver và dùng lệnh make để cài đặt

```
vpnserver@vpnserver:~$ cd vpnserver/
vpnserver@vpnserver:~/vpnserver$ make

-----
SoftEther VPN Server (Ver 4.38, Build 9760, 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
```

```
After you start the server daemon, you can open the HTML5 Web Administration Console is available
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
-----
make[1]: Leaving directory '/home/vpnserver/vpnserver'
vpnserver@vpnserver:~/vpnserver$
```

- Chuyển tệp vpnserver vào /usr/local/ và cấp quyền cho thư mục

```
vpnserver@vpnserver:~$ sudo mv vpnserver /usr/local/
vpnserver@vpnserver:~$ cd /usr/local/
vpnserver@vpnserver:/usr/local$ ls
bin  etc  games  include  lib  man  sbin  share  src  vpnserver
vpnserver@vpnserver:/usr/local$ cd vpnserver/
vpnserver@vpnserver:/usr/local/vpnserver$ ls
Authors.txt  hamcore.se2  Makefile  ReadMeFirst_Important_Notices_ja.txt  vpnserver
chain_certs  lang.config  ReadMeFirst_Important_Notices_cn.txt  ReadMeFirst_License.txt
code  lib  ReadMeFirst_Important_Notices_en.txt  vpncmd
vpnserver@vpnserver:/usr/local/vpnserver$ chmod 600 *
vpnserver@vpnserver:/usr/local/vpnserver$ chmod 700 vpnserver
vpnserver@vpnserver:/usr/local/vpnserver$ chmod 700 vpncmd
vpnserver@vpnserver:/usr/local/vpnserver$
```

- Khởi động vpnserser và vpncmd

```
root@vpnserver:/usr/local/vpnserver# ./vpnserver start
The SoftEther VPN Server service has been started.

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

https://192.168.1.183:5555/
or
https://192.168.1.183/

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.

root@vpnserver:/usr/local/vpnserver# ./vpncmd
vpncmd command - SoftEther VPN Command Line Management Utility
SoftEther VPN Command Line Management Utility (vpncmd command)
Version 4.38 Build 9760 (English)
Compiled 2021/08/17 22:32:49 by buildsan at crosswin
Copyright (c) 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)

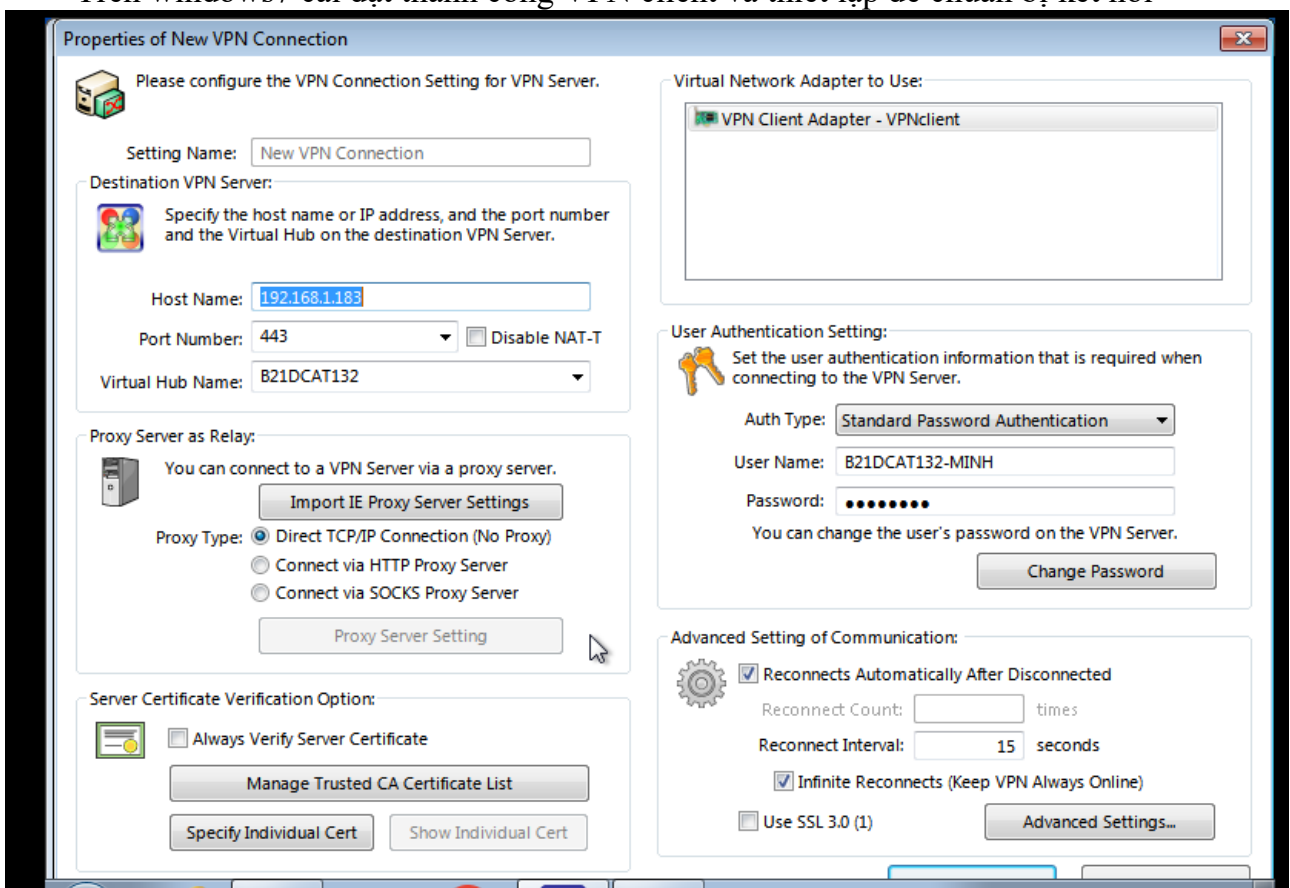
Select 1, 2 or 3:
```

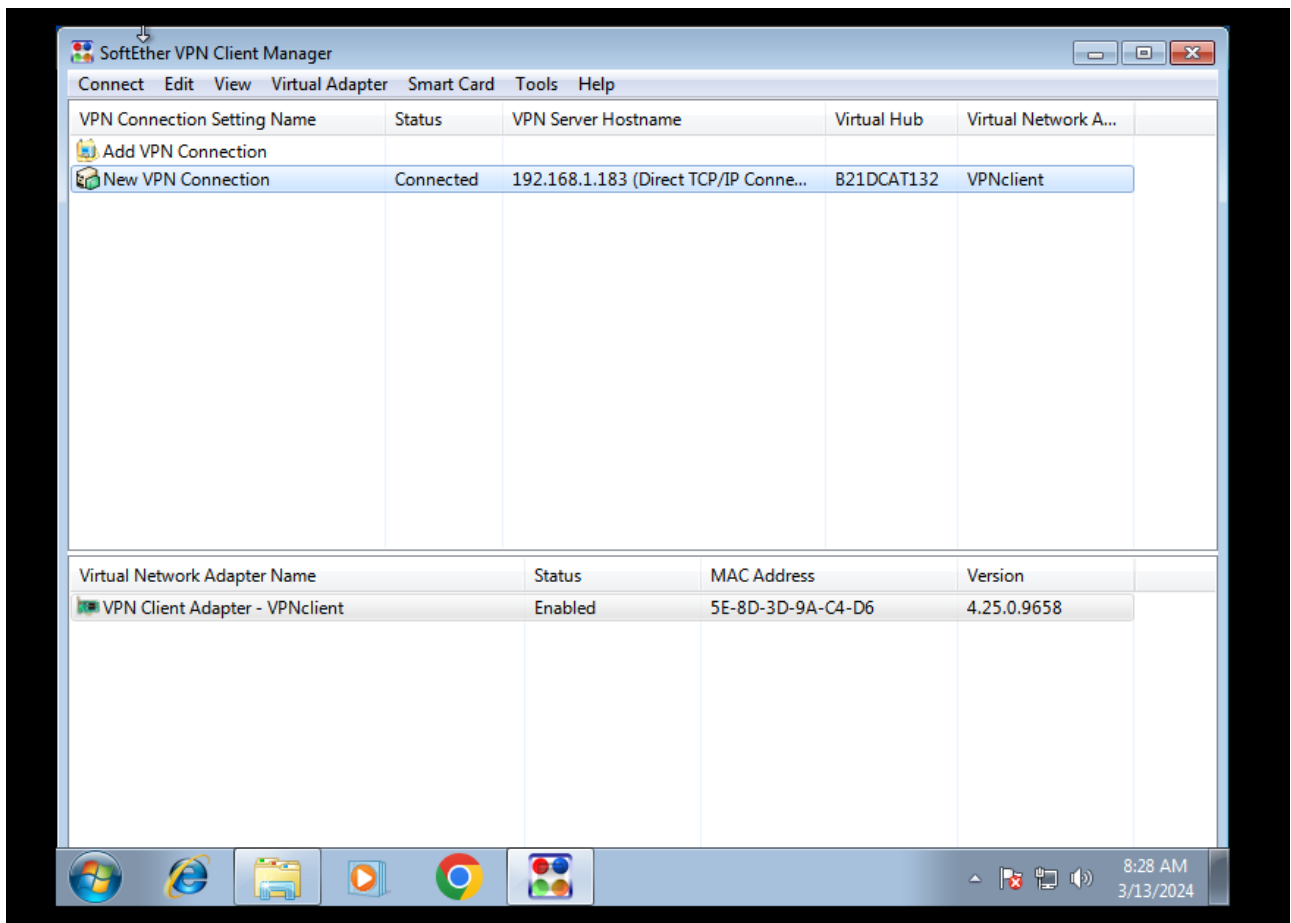


- Tạo Virtual Hub mới: B21DCAT132 mật khẩu là 3153
- Tạo người dùng mới: B21DCAT132-MINH mật khẩu là minh3153



- Trên windows7 cài đặt thành công VPN client và thiết lập để chuẩn bị kết nối





- Trên máy ubuntu phần vpnlog đã có phiên kết nối của client với địa chỉ ip trùng khớp

```
2024-03-13 22:28:01.244 [HUB "B21DCAT132"] The connection "CID-8" (IP address: 192.168.1.58, Host name: vpnclient-PC, P
ort number: 49476, Client name: "SoftEther VPN Client", Version: 4.43, Build: 9799) is attempting to connect to the Vir
tual Hub. The auth type provided is "Password authentication" and the user name is "B21DCAT132-MINH".
2024-03-13 22:28:01.244 [HUB "B21DCAT132"] Connection "CID-8": Successfully authenticated as user "B21DCAT132-MINH".
2024-03-13 22:28:01.254 [HUB "B21DCAT132"] Connection "CID-8": The new session "SID-B21DCAT132-MINH-1" has been created
. (IP address: 192.168.1.58, Port number: 49476, Physical underlying protocol: "Standard TCP/IP (IPv4)")
2024-03-13 22:28:01.254 [HUB "B21DCAT132"] Session "SID-B21DCAT132-MINH-1": The parameter has been set. Max number of T
CP connections: 2, Use of encryption: Yes, Use of compression: No, Use of Half duplex communication: No, Timeout: 20 se
conds.
2024-03-13 22:28:01.254 [HUB "B21DCAT132"] Session "SID-B21DCAT132-MINH-1": VPN Client details: (Client product name: "
SoftEther VPN Client", Client version: 443, Client build number: 9799, Server product name: "SoftEther VPN Server (64 b
it)", Server version: 438, Server build number: 9760, Client OS name: "Windows 7", Client OS version: "Build 7601, Mult
iprocessor Free, Service Pack 1 (7601.win7sp1_rtm.101119-1850)", Client product ID: "--", Client host name: "vpnclient-
PC", Client IP address: "192.168.1.58", Client port number: 49476, Server host name: "192.168.1.183", Server IP address
: "192.168.1.183", Server port number: 443, Proxy host name: "", Proxy IP address: "0.0.0.0", Proxy port number: 0, Vir
tual Hub name: "B21DCAT132", Client unique ID: "40BDD64AAF37F2B2239DF8872E1290E9")
root@vpnserver: /usr/local/vpnserver/server log# ls
vpn 20240313.log
```

```
Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::dd1d:32ea:7931:c432%11
IPv4 Address. . . . . : 192.168.1.58
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1

Tunnel adapter isatap.{EA15B3E3-98C2-4EB8-BE81-D1048A5F7160}:

```

## 5. Kết quả

Bài thực hành hoàn thành vào ngày 13/03/2024

```
TX errors 0 dropped 0 overruns 0 carrier 0 collision
vpnsver@vpnsver:~$ date
Thứ tư, 13 Tháng 3 năm 2024 22:37:12 +07
vpnsver@vpnsver:~$ nguyen nhat minh b21dcat132
```