

Báo cáo bài thực hành số 7

Môn học

Thực tập cơ sở

Giảng viên : Hoàng Xuân Dậu

Họ tên : Nguyễn Minh Phương

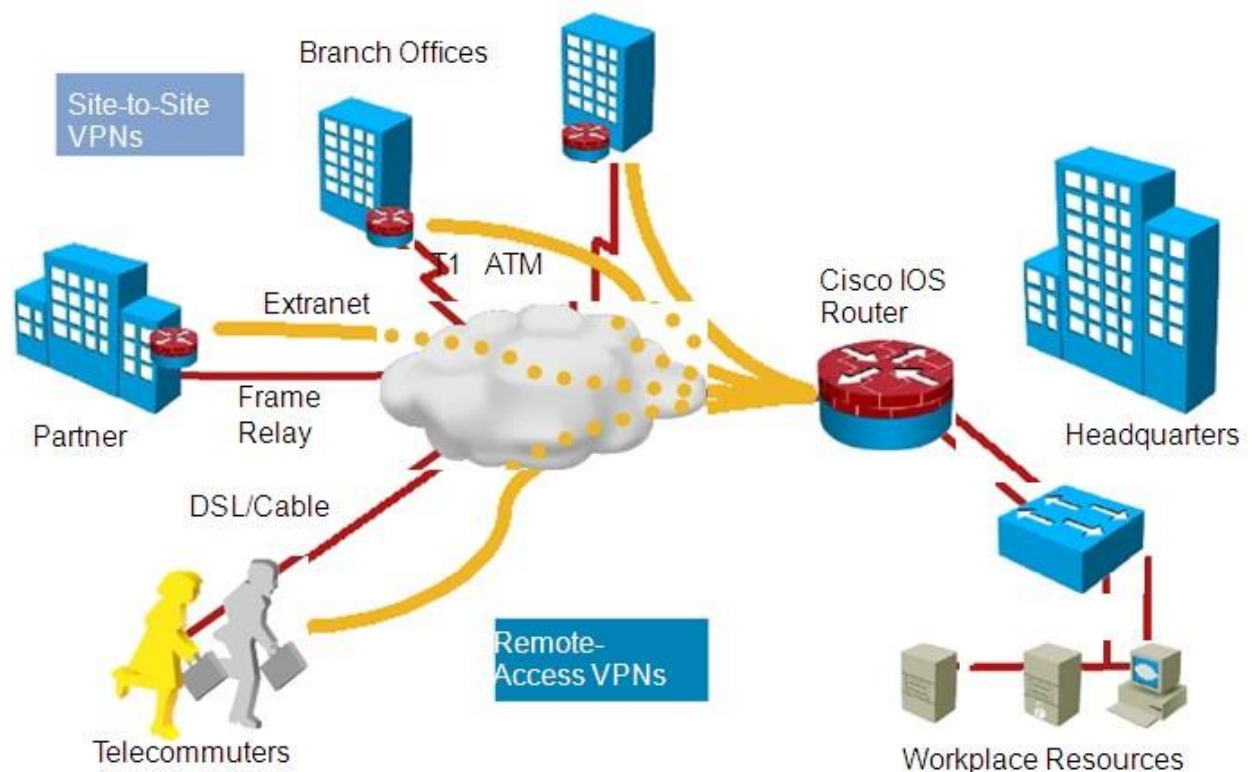
Mã SV: B19DCAT141

I. Lý thuyết:

- Khái quát về VPN:

VPN là mạng riêng ảo, Virtual Private Network, là một công nghệ mạng giúp tạo kết nối mạng an toàn khi tham gia vào mạng công cộng như Internet hoặc mạng riêng do một nhà cung cấp dịch vụ sở hữu. Các tập đoàn lớn, các cơ sở giáo dục và cơ quan chính phủ sử dụng công nghệ VPN để cho phép người dùng từ xa kết nối an toàn đến mạng riêng của cơ quan mình.

- Các mô hình VPN:



- Một số ứng dụng của VPN:

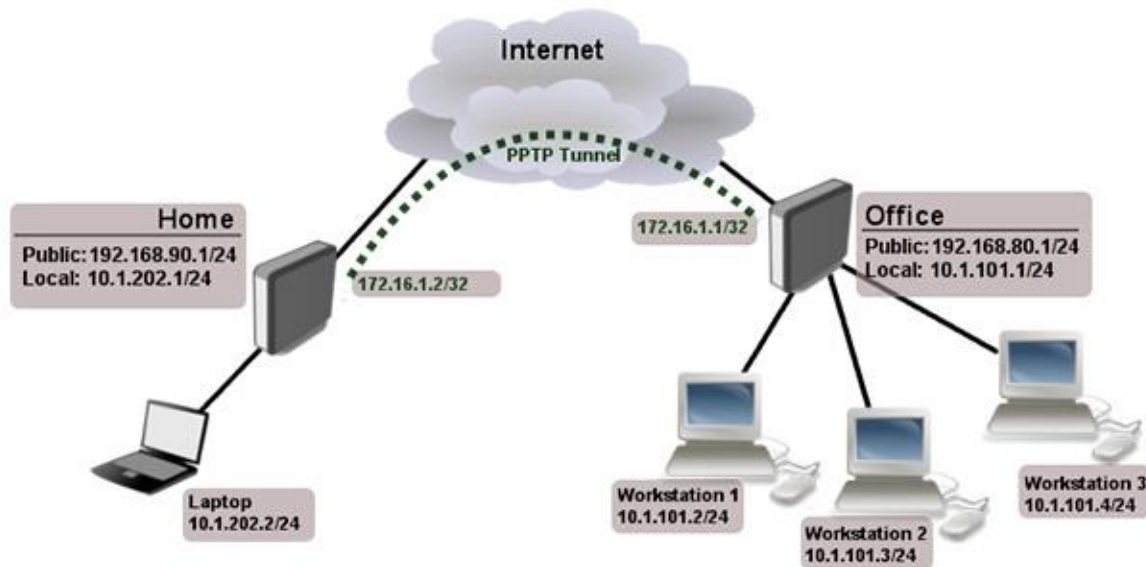
- + **Truy cập vào mạng doanh nghiệp khi ở xa:** VPN thường được sử dụng bởi những người kinh doanh để truy cập vào mạng lưới kinh doanh của họ, bao gồm tất cả tài nguyên trên mạng cục bộ, trong khi đang đi trên đường, đi du lịch,... Các nguồn lực trong mạng nội bộ không cần phải tiếp xúc trực tiếp với 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 bạn 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.
- Tìm hiểu về các giao thức tạo đường hầm cho VPN: PPTP, L2TP, L2F, MPLS,...

- **Point-To-Point Tunneling Protocol (PPTP)**

PPTP không chỉ định giao thức mã hóa nhưng có thể sử dụng một số giao thức như MPPE-128 mạnh mẽ. Việc thiếu sự tiêu chuẩn hóa về giao thức mạng là một rủi ro, vì nó chỉ có thể sử dụng tiêu chuẩn mã hóa mạnh nhất mà cả 2 phía cùng hỗ trợ. Nếu một phía chỉ hỗ trợ tiêu chuẩn yếu hơn thì kết nối phải sử dụng mã hóa yếu hơn người dùng mong đợi



- **L2TP**

Giao thức L2TP thường hoạt động với thuật toán mã hóa IPSec. Nó mạnh hơn đáng kể so với PPTP nhưng vẫn khiến người dùng lo ngại. Lỗi hổng chính trong L2TP/IPSec là phương thức trao đổi khóa công khai (public key). Trao đổi khóa công khai Diffie-Hellman là cách để hai bên thỏa thuận về khóa mã hóa tiếp theo và không ai được biết về khóa này. Có một phương pháp có thể “bẻ khóa” quá trình này, đòi hỏi sức mạnh điện toán khá lớn, nhưng sau đó nó cho phép truy cập vào tất cả các giao tiếp trên một VPN nhất định.

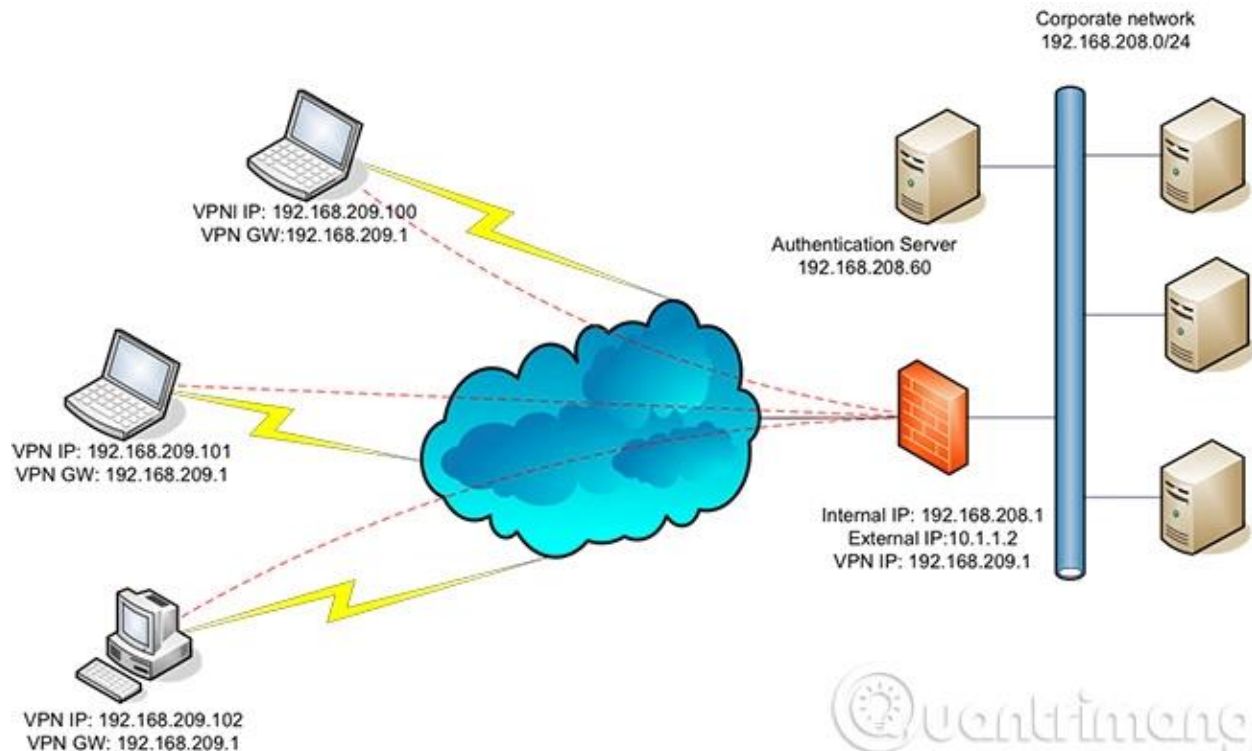
- Các giao thức bảo mật cho VPN: IPSec, SSL/TLS

- **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.

- **Secure Sockets Layer (SSL) và Transport Layer Security (TLS)**

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



Bên cạnh đó, 2 giao thức trên còn sử dụng chế độ **Handshake** - có liên quan đến quá trình xác thực tài khoản giữa client và server. Để 1 kết nối được coi là thành

công, quá trình xác thực này sẽ dùng đến các **Certificate** - chính là các khóa xác thực tài khoản được lưu trữ trên cả server và client.

- **Tìm hiểu về SoftEther VPN**

Softether là một dự án VPN tương đối mới giúp công nghệ VPN trở nên an toàn hơn, cho phép người dùng lướt web ẩn danh và BẢO MẬT cao hơn.

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**, 1 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.

II. Thực hành:

- Chuẩn bị các máy tính như mô tả trong mục 2.2. Máy Windows được đổi tên thành <Mã SV-Tên SV>-VPNClient và máy cài VPN server thành <Mã SV-Tên SV>-VPNServer. Các máy có địa chỉ IP và kết nối mạng LAN.

```
phuongnm-b19dcat141@phuongnm-b19dcat141-vpnserver: ~  
phuongnm-b19dcat141@phuongnm-b19dcat141-vpnserver:~$ ifconfig  
ens33      Link encap:Ethernet  HWaddr 00:0c:29:34:50:41  
            inet addr:192.168.240.129  Bcast:192.168.240.255  Mask:255.255.255.0  
            inet6 addr: fe80::90bd:4960:d2d5:f37b/64 Scope:Link  
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
            RX packets:111 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:114 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:1000  
            RX bytes:25989 (25.9 KB)  TX bytes:13046 (13.0 KB)  
            Interrupt:19 Base address:0x2000  
  
lo          Link encap:Local Loopback  
            inet addr:127.0.0.1  Mask:255.0.0.0  
            inet6 addr: ::1/128 Scope:Host  
            UP LOOPBACK RUNNING  MTU:65536  Metric:1  
            RX packets:204 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:204 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:1000  
            RX bytes:15181 (15.1 KB)  TX bytes:15181 (15.1 KB)
```

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\phuongnm>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::7001:d4d3:4623:57d3%11
    IPv4 Address. . . . . : 192.168.240.130
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.240.2

Tunnel adapter isatap.localdomain:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
```

- Tải SoftEther VPN server tại <https://www.softether.org/5-download>. Cài đặt và cấu hình VPN server theo hướng dẫn sau:
 - + Giải nén file cài đặt bằng lệnh `tar -vxzf <tên file vpn server>`

```
phuongnm-b19dcat141@phuongnm-b19dcat141-vpnserver: ~/Downloads
phuongnm-b19dcat141@phuongnm-b19dcat141-vpnserver:~/Downloads$ tar -vxzf 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/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
```

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


```

phuongnm-b19dcat141@phuongnm-b19dcat141-vpnserver: ~/Downloads/vpnserver
phuongnm-b19dcat141@phuongnm-b19dcat141-vpnserver:~/Downloads/vpnserver$ make
-----
SoftEther VPN Server (Ver 4.38, Build 9760, Intel x64 / AMD64) for Linux Build U
tality
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
ITIONS OF ANY KIND, either express or implied.

```

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

```

root@phuongnm-b19dcat141-vpnserver: /home/phuongnm-b19dcat141/Downloads/vpnse
root@phuongnm-b19dcat141-vpnserver: /home/phuongnm-b19dcat141/Downloads/vpnse
# 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://192.168.240.129:5555/
or
https://192.168.240.129/

Note: IP address may vary. Specify your server's IP address.
A TLS certificate warning will appear because the server uses self signed certif
icate by default. That is natural. Continue with ignoring the TLS warning.

```

- + 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 <name> </PASSWORD:password>`

(<name> là tên Virtual Hub - dùng mã sinh viên làm tên Virtual Hub)

```

VPN Server>HubCreate
HubCreate command - Create New Virtual Hub
Name of Virtual Hub to be created: B19DCAT141

Please enter the password. To cancel press the Ctrl+D key.

Password: *
Confirm input: *

The command completed successfully.

VPN Server>

```

- Chọn Virtual Hub đã tạo: Hub <tên Virtual Hub>

```

VPN Server>Hub B19DCAT141
Hub command - Select Virtual Hub to Manage
The Virtual Hub "B19DCAT141" has been selected.
The command completed successfully.

VPN Server/B19DCAT141>

```

- Tạo 1 người dùng VPN mới:

UserCreate <mã sv-tên> /GROUP:none /REALNAME:Tên sinh viên /NOTE:none

```

VPN Server/B19DCAT141>UserCreate
UserCreate command - Create User
User Name: B19DCAT141-NguyenMinhPhuong

Assigned Group Name:

User Full Name: Nguyen Minh Phuong

User Description:

The command completed successfully.

VPN Server/B19DCAT141>

```

- UserPasswordSet <mã sv-tên> </PASSWORD:password>+ Gõ exit để thoát khỏi tiện ích quản trị VPN Server


```

VPN Server/B19DCAT141>UserPasswordSet B19DCAT141-NguyenMinhPhuong
UserPasswordSet command - Set Password Authentication for User Auth Type and Set
Password
Please enter the password. To cancel press the Ctrl+D key.

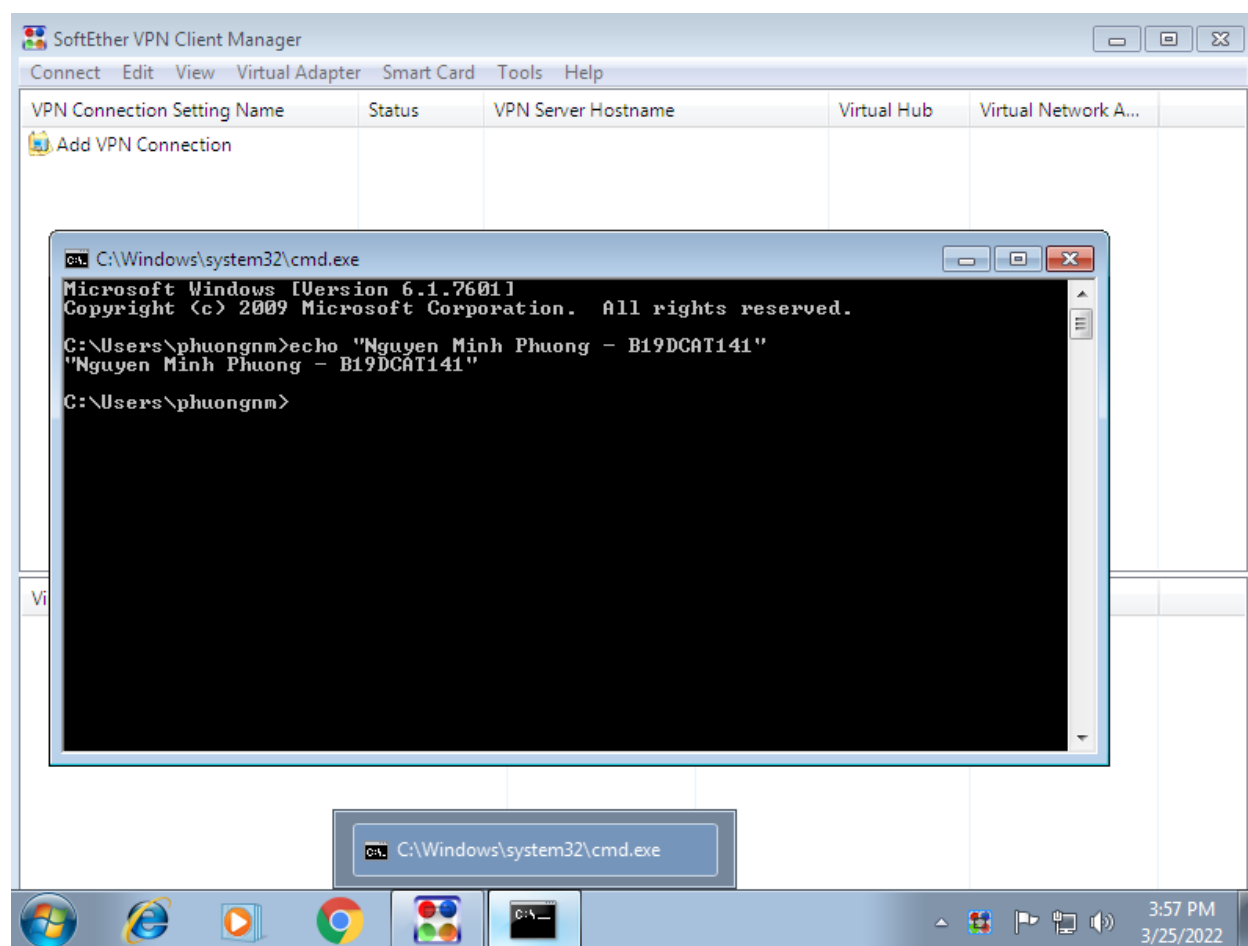
Password: *
Confirm input: *

The command completed successfully.

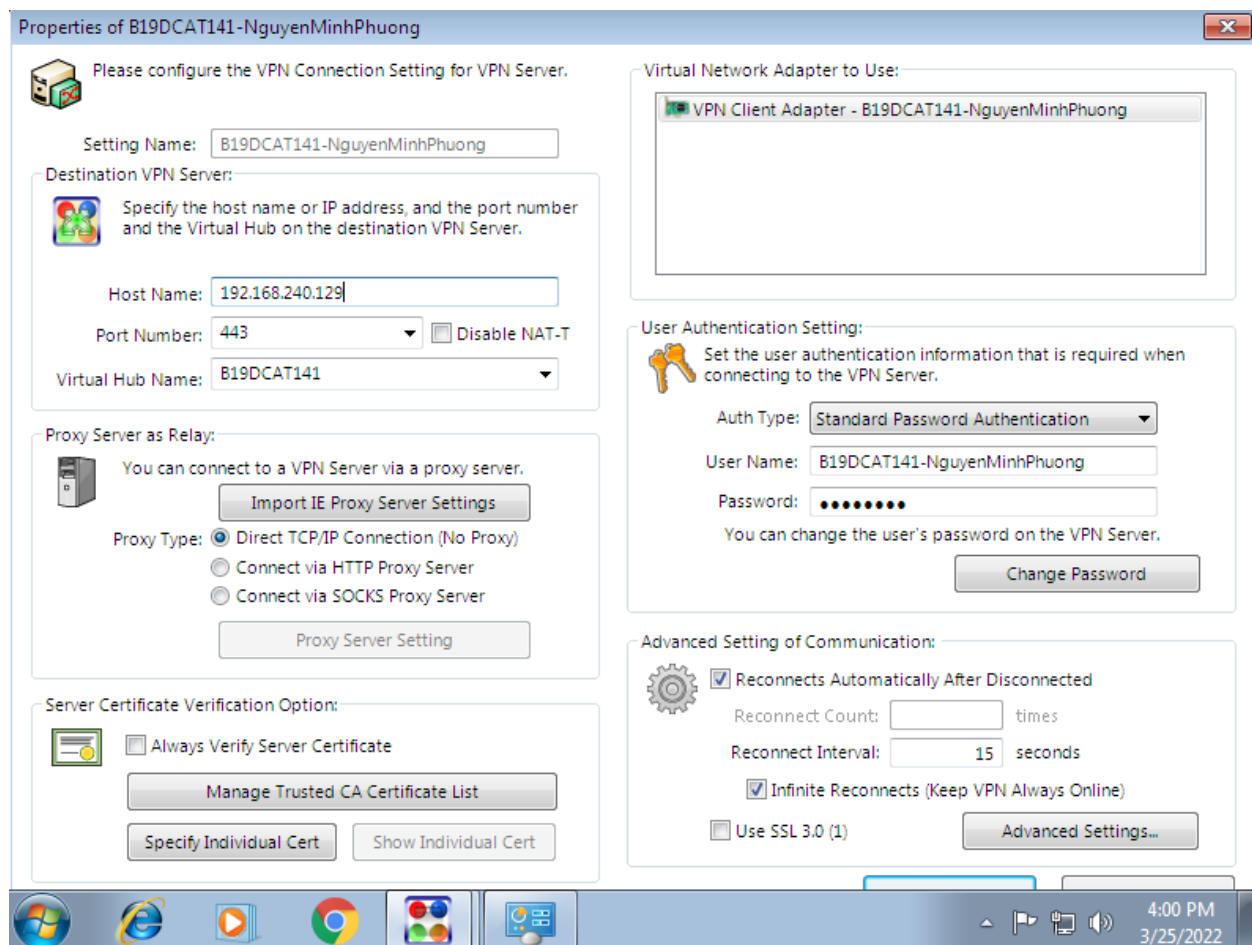
VPN Server/B19DCAT141>

```

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



- 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 <Mã sinh viên>-<Họ tên>



- Thử kết nối: Nếu thành công sẽ báo connected.

VPN Connection Setting Name	Status	VPN Server Hostname	Virtual Hub	Virtual Network A...
Add VPN Connection				
B19DCAT141-NguyenMinhPhuong	Connected	192.168.240.129 (Direct TCP/IP Con...	B19DCAT141	B19DCAT141-Ng...

- + 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 <mã sinh viên> vpnserver/server_log/*.log`

=> Hiển thị các dòng log có liên quan đến <mã sinh viên>

```

root@phuongnm-b19dcat141-vpnserver: /usr/local/vpnserver/server_log
tion" and the user name is "B19DCAT141-NguyenMinhPhuong".
vpn_20220325.log:46:2022-03-25 02:00:36.749 [HUB "B19DCAT141"] Connection "CID-3
": Successfully authenticated as user "B19DCAT141-NguyenMinhPhuong".
vpn_20220325.log:47:2022-03-25 02:00:36.749 [HUB "B19DCAT141"] Connection "CID-3
": The new session "SID-B19DCAT141-NGUYENMINHPHUONG-1" has been created. (IP add
ress: 192.168.240.130, Port number: 64766, Physical underlying protocol: "Standar
d TCP/IP (IPv4)")
vpn_20220325.log:48:2022-03-25 02:00:36.749 [HUB "B19DCAT141"] Session "SID-B19D
CAT141-NGUYENMINHPHUONG-1": The parameter has been set. Max number of TCP connec
tions: 2, Use of encryption: Yes, Use of compression: No, Use of Half duplex com
munication: No, Timeout: 20 seconds.
vpn_20220325.log:49:2022-03-25 02:00:36.749 [HUB "B19DCAT141"] Session "SID-B19D
CAT141-NGUYENMINHPHUONG-1": VPN Client details: (Client product name: "SoftEther
VPN Client", Client version: 438, Client build number: 9760, Server product nam
e: "SoftEther VPN Server (32 bit)", Server version: 438, Server build number: 97
60, Client OS name: "Windows 7", Client OS version: "Build 7601, Multiprocessor
Free, Service Pack 1 (7601.win7sp1_rtm.101119-1850)", Client product ID: "--", C
lient host name: "Phuong-B19DCAT141.phuongnmb19dcat141.it", Client IP address: "
192.168.240.130", Client port number: 64766, Server host name: "192.168.240.129"
, Server IP address: "192.168.240.129", Server port number: 443, Proxy host name
: "", Proxy IP address: "0.0.0.0", Proxy port number: 0, Virtual Hub name: "B19D
CAT141", Client unique ID: "E090E7A4C5140AFEF5AFE87A4E4B7B69")
root@phuongnm-b19dcat141-vpnserver: /usr/local/vpnserver/server_log#

```

III. Kết quả cần đạt:

- 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 (có ảnh chụp màn hình minh chứng bên máy khách và log bên máy chủ).