HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

BÀI BÁO CÁO THỰC HÀNH SỐ 7

MÔN THỰC TẬP CƠ SỞ

Cài đặt cấu hình VPN server

Tên sinh viên: Ninh Chí Hướng

Mã sinh viên: B20DCAT094

Giảng viên hướng dẫn : Th.s Ninh Thị Thu Trang

HÀ NỘI, THÁNG 3/2023

Table of Contents

I.KIẾN THỨC LÝ THUYẾT

1. 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 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.

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

Các giao thức thường dùng trong VPN

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 Certificat

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.

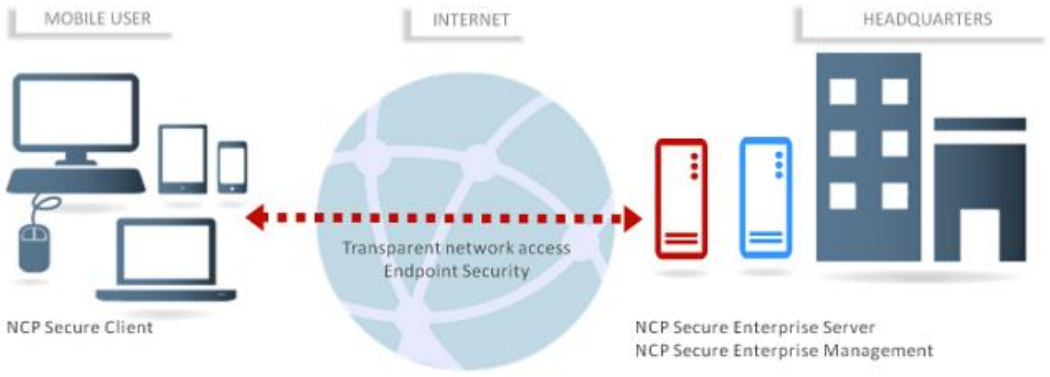
*Cách hoạt động của L2TP:
- Các gói tin L2TP bao gồm cả payload và header được gửi đi trong các gói tin UDP (User Datagram Protocol). Một ưu điểm của việc truyền qua UDP (chứ không phải TCP) là nó tránh được vấn đề TCP meltdown – khi hai giao thức truyền dẫn có điều khiển chồng lên nhau và xung đột khi 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.

3. 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 mật khẩu để đảm bảo an toàn giữa các kết nối trong môi trường Internet.

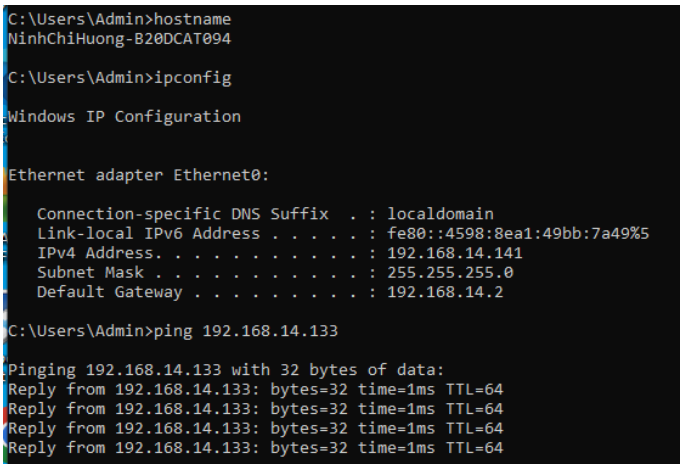
4. Tìm hiểu về SoftEther VPN

- 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,, 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.
- 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.
- SoftEther VPN – Thông số kỹ thuật chi tiết
- Bây giờ chúng ta đã biết SoftEther VPN là gì, tiếp đến chúng ta sẽ kiểm tra các chi tiết kỹ thuật của giao thức:

+Có sẵn theo giấy phép GNU GPL;
+SoftEther VPN hỗ trợ chứng chỉ xác thực RSA và tính năng Deep Inspect Packet Logging; +Hỗ trợ các giao thức OpenVPN, EtherIP, L2TP và Microsoft BST;
+Hỗ trợ IPV6, Packet Filtering và tính năng DNS động;
+Sử dụng mã hóa AES 256-bit;
+SoftEther VPN tuân thủ Virtual Network Adapter, trong khi máy chủ SoftEther VPN tuân thủ Virtual Ethernet Switch;
+Nhúng dynamic-DNS và NAT-traversal;
+Chạy trên Windows, Linux, FreeBSD, Solaris, iOS, Android và Mac OS;
+SoftEther VPN Protocol hỗ trợ đa ngôn ngữ (tiếng Anh, tiếng Nhật và tiếng Trung).

II. BÁO CÁO THỰC HÀNH.

1. Kiểm tra IP (máy ảo win, máy ảo linux)



2.Tải SoftEther VPN server , cài đặt và cấu hình VPN server

- Tải SoftEther VPN server trên máy Linux

Giải nén file vừa tải

```
root@B20DCAT094-NInhChiHuong-Snort:~# tar -vxzf /home/b20at094-ninhchihuong/Downloads/softether-vpnserver-v4.41-
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
```

Cài GCC

```
root@B20DCAT094-NInhChiHuong-Snort:~/vpnserver# apt install build-essential
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libflashrom1 libftdi1-2 libllvm13
Use 'apt autoremove' to remove them.
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-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 git bzr libstdc++-11-doc make-doc
The following NEW packages will be installed:
```

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)

```
root@B20DCAT094-NInhChiHuong-Snort:~/vpnserver# make
--------------------------------------------------------------------

SoftEther VPN Server (Ver 4.41, Build 9787, 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
```

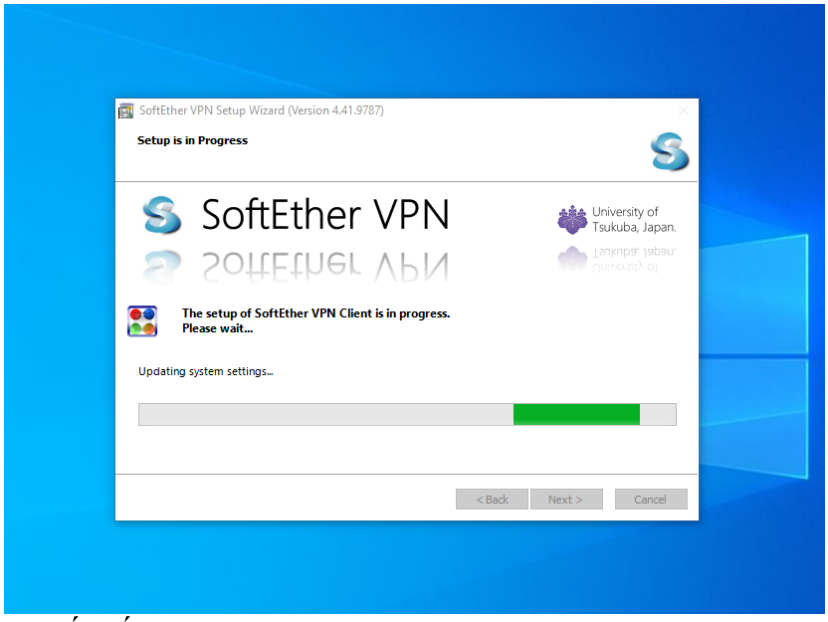
Khởi động máy chủ VPN: sudo ./vpnserver star

```
root@B20DCAT094-NInhChiHuong-Snort:~/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://192.168.14.133:5555/
  or
https://192.168.14.133/
```

- 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)
- Chọn Virtual Hub đã tạo: Hub <ten Virtual Hub>
- Tạo 1 người dùng VPN mới: UserCreate <msv-ten> /GROUP:none /REALNAME:Tên sinh viên /NOTE:none
-Đặt mật khẩu cho người dùng: UserPasswordSet <msv> /PASSWORD:password

```
root@B20DCAT094-NInhChiHuong-Snort: ~/vpnserver
alhost (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 B20DCAT094 /PASSWORD:password
HubCreate command - Create New Virtual Hub
The command completed successfully.

VPN Server>Hub B20DCAT094
Hub command - Select Virtual Hub to Manage
The Virtual Hub "B20DCAT094" has been selected.
The command completed successfully.

VPN Server/B20DCAT094>UserCreate B20DCAT094-NinhChiHuong /GROUP:none /REALNAME:NinhChiHuo
ng /NOTE:none
UserCreate command - Create User
The command completed successfully.

VPN Server/B20DCAT094>UserPasswordSet B20DCAT094 /PASSWORD:password
UserPasswordSet command - Set Password Authentication for User Auth Type and Set Password
Error occurred. (Error code: 29)
Object not found.
VPN Server/B20DCAT094>UserPasswordSet B20DCAT094-NinhChiHuong /PASSWORD:password
UserPasswordSet command - Set Password Authentication for User Auth Type and Set Password
The command completed successfully.

VPN Server/B20DCAT094>
```

3.Tải SoftEther VPN client cho Windows



Tạo và kiểm tra kết nối VPN:

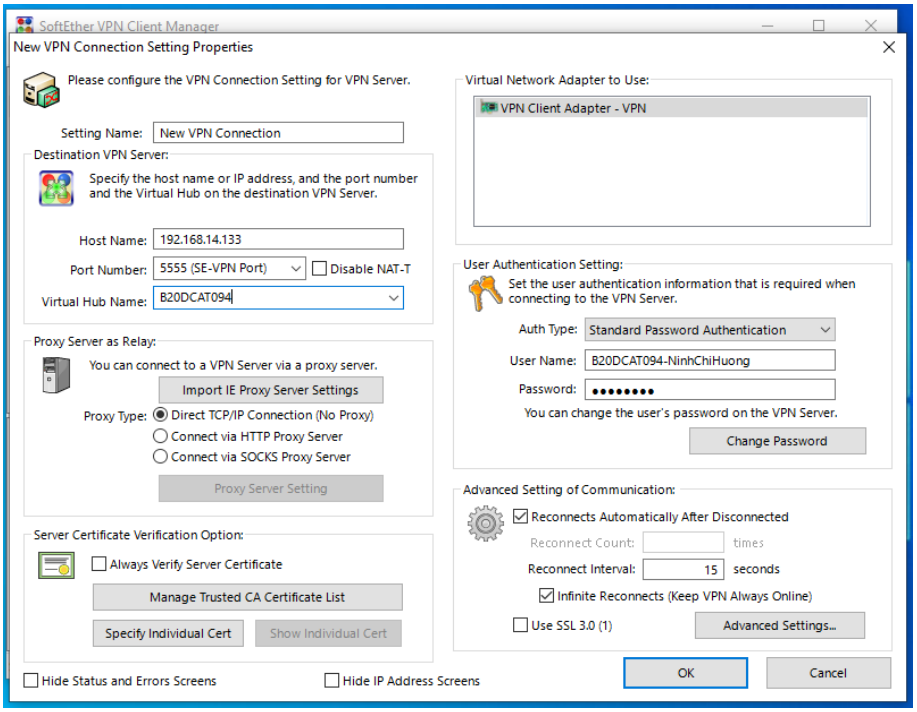
-Từ giao diện SoftEther VPN Client Manager tạo 1 kết nối mới (Add New Connection)

-Với địa chỉ IP của máy chủ VPN

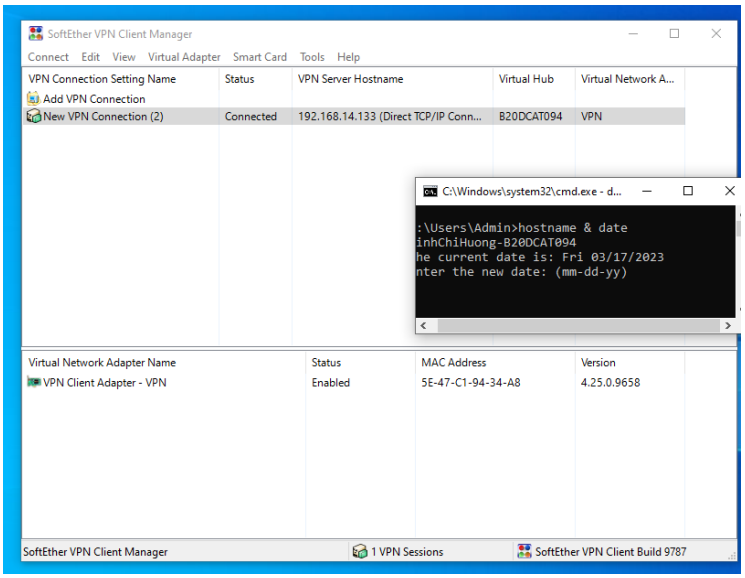
-Tên Virtual Hub

-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:

sudo grep <msv> bai7ttcs/vpnserver/server_log/*.log

==> Hiển thị các dòng log có liên quan đến <msv>

```
root@b20at094ninhchihuong-virtual-machine:~/vpnserver#  grep B20DCAT094 server_log/*.log
2023-03-17 03:15:40.868 Administration mode [RPC-28]: A new Virtual Hub "B20DCAT094" has been created.
2023-03-17 03:15:40.879 Virtual Hub "B20DCAT094" has been started.
2023-03-17 03:15:40.879 The MAC address of Virtual Hub "B20DCAT094" is "00-AE-D3-1E-6B-04".
2023-03-17 03:15:40.879 [HUB "B20DCAT094"] The Virtual Hub is now online.
2023-03-17 03:18:18.932 [HUB "B20DCAT094"] Administration mode [RPC-28] (Virtual Hub "B20DCAT094"): User "B20DCAT094-NinhChiHuong" has been created.
2023-03-17 03:19:01.775 [HUB "B20DCAT094"] Administration mode [RPC-28] (Virtual Hub "B20DCAT094"): The setting of user "B20DCAT094-NinhChiHuong" has been updated.
2023-03-17 03:19:57.364 [HUB "B20DCAT094"] The connection "CID-3" (IP address: 192.168.14.141, Host name: NINHCHIHUONG-B2, Port number: 49997, Client name: "SoftEther VPN
Client", Version: 4.41, Build: 9787) is attempting to connect to the Virtual Hub. The auth type provided is "Password authentication" and the user name is "B20DCAT094-Nin
ChiHuong".
2023-03-17 03:19:57.364 [HUB "B20DCAT094"] Connection "CID-3": Successfully authenticated as user "B20DCAT094-NinhChiHuong".
2023-03-17 03:19:57.364 [HUB "B20DCAT094"] Connection "CID-3": The new session "SID-B20DCAT094-NINHCHIHUONG-1" has been created. (IP address: 192.168.14.141, Port number:
49997, Physical underlying protocol: "Standard TCP/IP (IPv4)")
2023-03-17 03:19:57.364 [HUB "B20DCAT094"] Session "SID-B20DCAT094-NINHCHIHUONG-1": The parameter has been set. Max number of TCP connections: 2, Use of encryption: Yes,
se of compression: No, Use of Half duplex communication: No, Timeout: 20 seconds.
2023-03-17 03:19:57.374 [HUB "B20DCAT094"] Session "SID-B20DCAT094-NINHCHIHUONG-1": VPN Client details: (Client product name: "SoftEther VPN Client", Client version: 441,
Client build number: 9787, Server product name: "SoftEther VPN Server (64 bit)", Server version: 441, Server build number: 9787, Client OS name: "Windows 10", Client OS v
rsion: "Build 18363, Multiprocessor Free (18362.19h1_release.190318-1202)", Client product ID: "--", Client host name: "NinhChiHuong-B20DCAT094", Client IP address: "192.
68.14.141", Client port number: 49997, Server host name: "192.168.14.133", Server IP address: "192.168.14.133", Server port number: 5555, Proxy host name: "", Proxy IP ad
ress: "0.0.0.0", Proxy port number: 0, Virtual Hub name: "B20DCAT094", Client unique ID: "2DAB839BBCF72D1C505D88EE81D8942E")
root@b20at094ninhchihuong-virtual-machine:~/vpnserver#
```

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

+ https://www.softether.org/4-docs