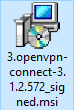
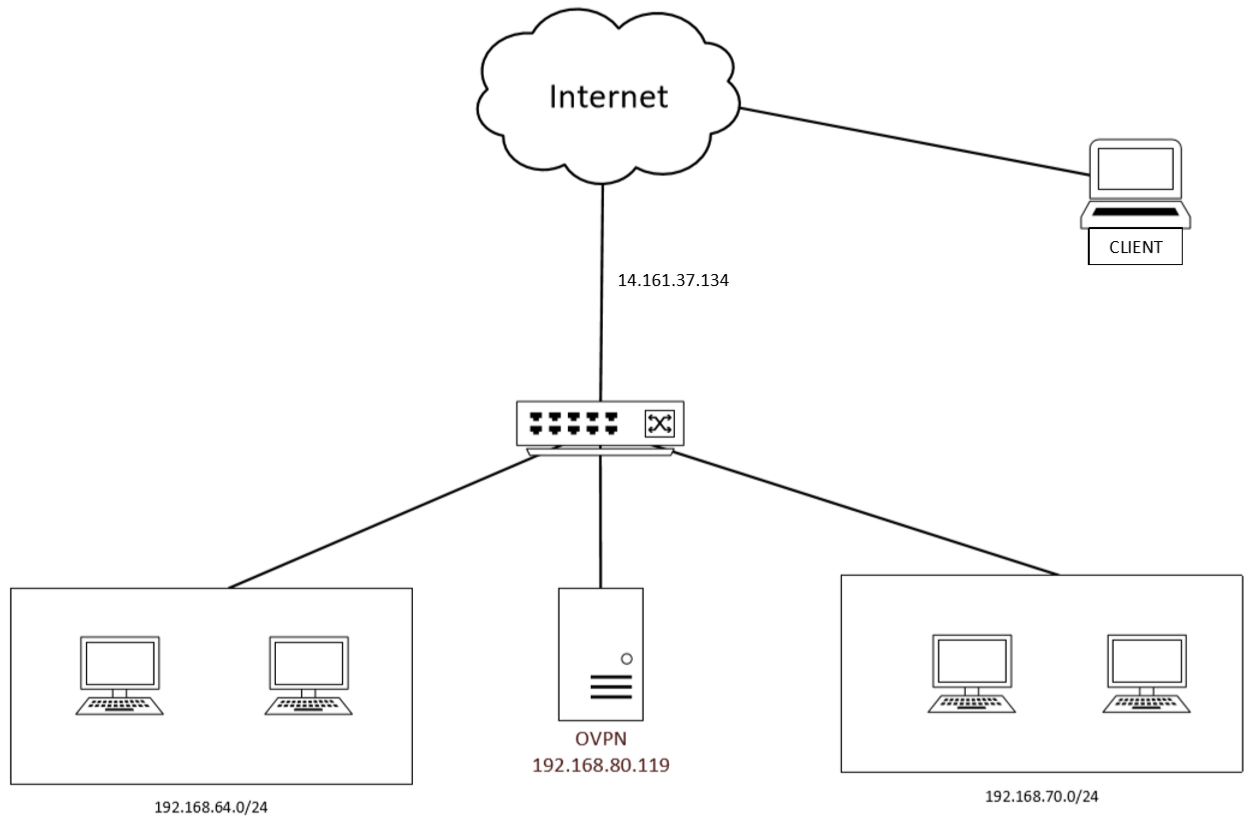
**Hướng dẫn cấu hình Open VPN trên Ubuntu 18.04 (Free OVPN)**

1. **Chuẩn bị.**

* 1 máy ảo chạy hệ điều hành Ubuntu 18.04 (đã bật SSH).
* File Script tự động cài đặt (có thể lấy trên Github).
* Phần mềm Putty để ssh vào server (máy ảo).
* Phần mềm WinSCP để edit và lấy file từ trong server.
* Phần mềm Open VPN Connect để cài vào máy Client



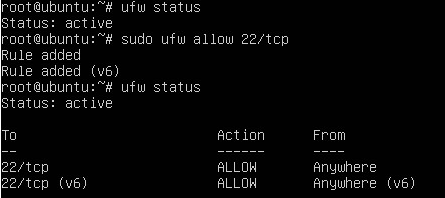
1. **Mô hình thử nghiệm**



\* Lưu ý: IP 14.141.37.134 là ip public đã note sẵn port UDP của Open VPN.

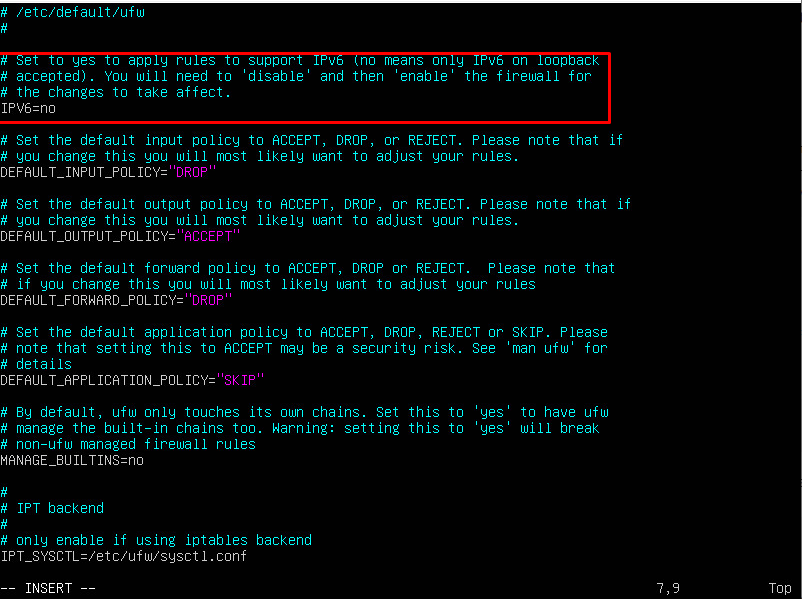
1. **Cài đặt.**
   1. **Bật ufw trên server Ubuntu và allow port 22 (SSH)**

# sudo ufw allow 22/tcp



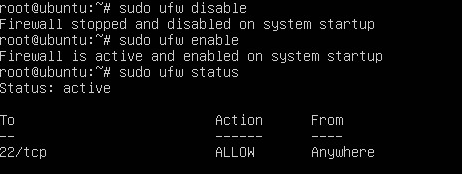
* Tắt chế độ IPv6 trên ufw

# sudo vi /etc/default/ufw



( sửa dòng IPV6=yes thành IPV6=no )

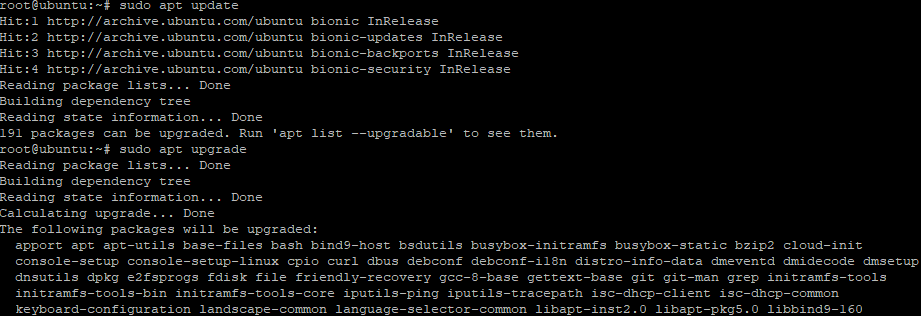
* Reload lại ufw và kiểm tra kết quả

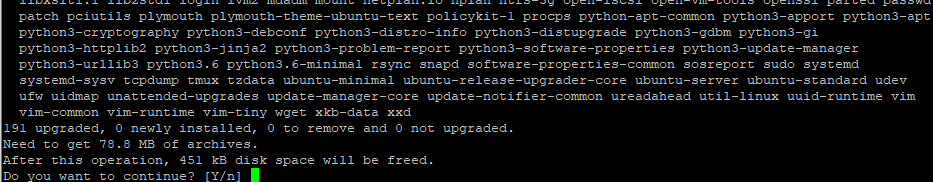


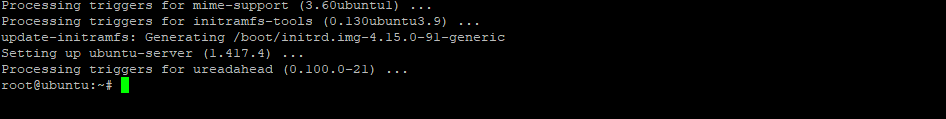
* 1. **Cài đặt Open VPN**
* Update Ubuntu

# sudo apt update

# sudo apt upgrade

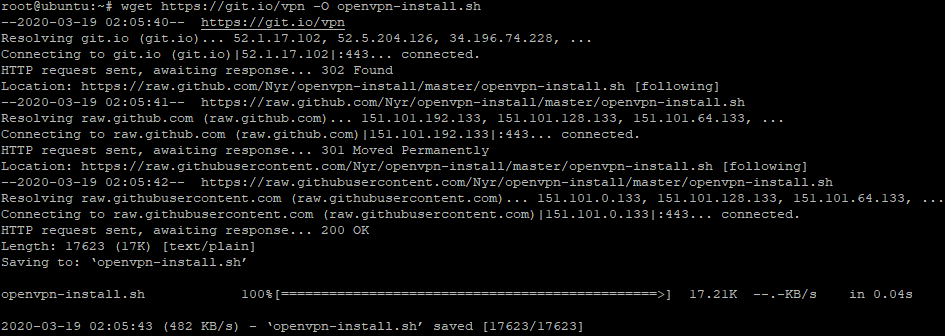






* Get file script từ Github để cài Open VPN

# wget https://git.io/vpn -O openvpn-install.sh



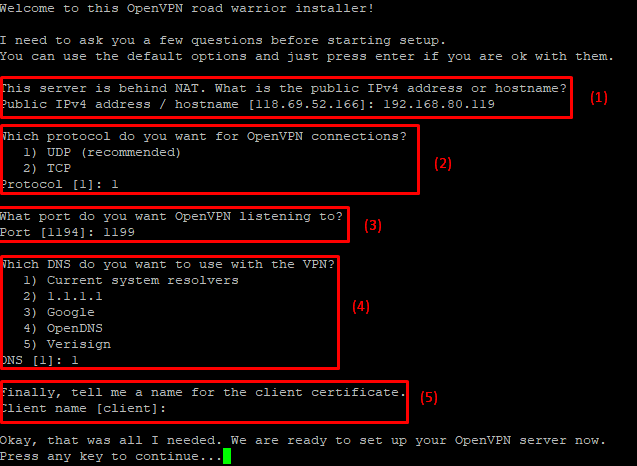
* Cấp quyền cho file Script (tên file Script: openvpn-install.sh)

# chmod +x openvpn-install.sh

* Chạy file Scrip

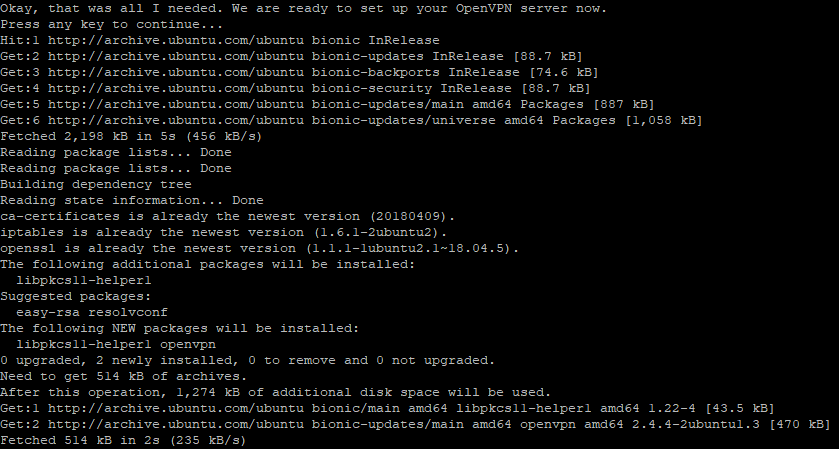
# sudo ./openvpn-install.sh

* Khi chạy file script thì ta sẽ cấp 1 số thông tin để tiến hành cài đặt

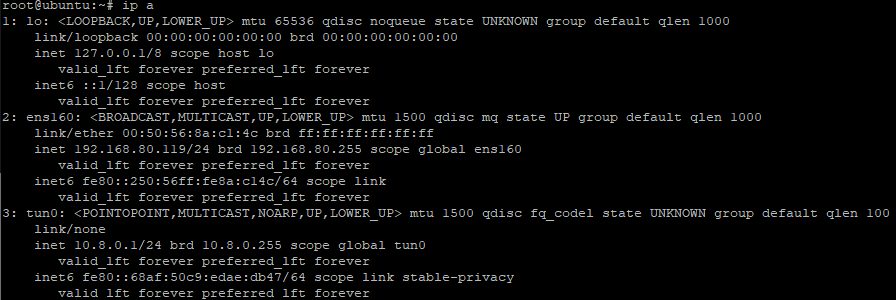


1. Nhập IP của Server, nếu server sử dụng IP Public thì nhập vào IP Public, nếu server sử dụng IP Privare thì nhập vào IP Prevate (ở đây sử dụng ip private 192.168.80.119).
2. Chọn Protocol cho Open VPN (ở đây chọn UDP cho bảo mật).
3. Chọn port cho Open VPN, mac75 định là 1194 (ở đây sử dụng port 1199)
4. Chọn DNS cho VPN.
5. Khởi tạo 1 user đầu tiên cho hệ thống.

\* Sau khi setup xong các thông số trên thì ấn nút bất kì để file Script bắt đầu cài đặt

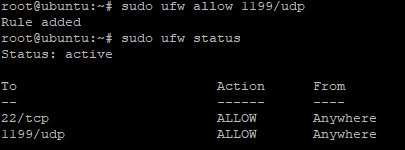


* Kiểm tra list card mạng thì sẽ thấy thêm 1 card tun0 tạo ra cho các user trong VPN



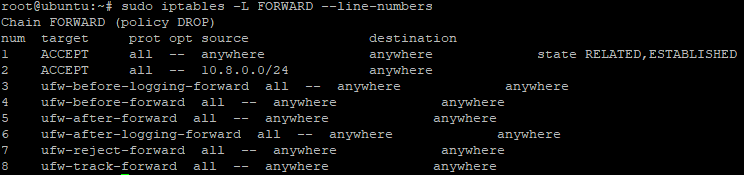
* Kiểm tra tạo policy cho phép port Open VPN trên ufw

# sudo ufw allow 1199/udp



* Kiểm tra policy trên iptables

# sudo iptables -L FORWARD --line-numbers

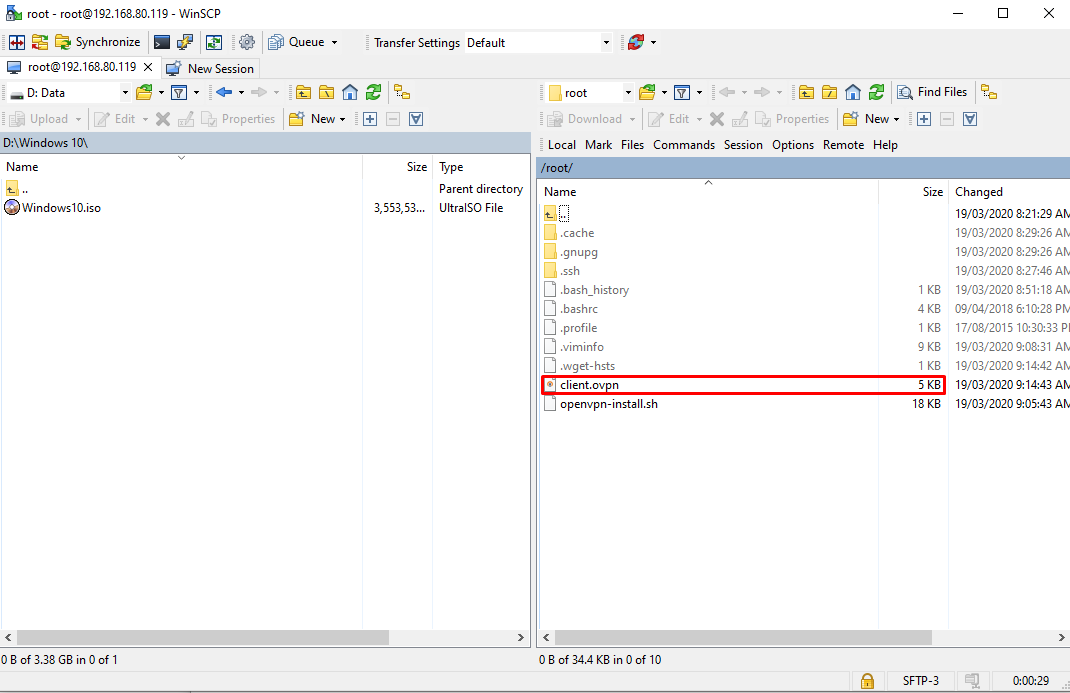


\* Ở policy số 1 có nghĩa là cho phép bất cứ kết nối nào được thành lập.

\* Ở policy số 2 có nghĩa là cho phép bất cứ ip nào trong lớp mạng 10.8.0.0/24 (range ip của card tun0).

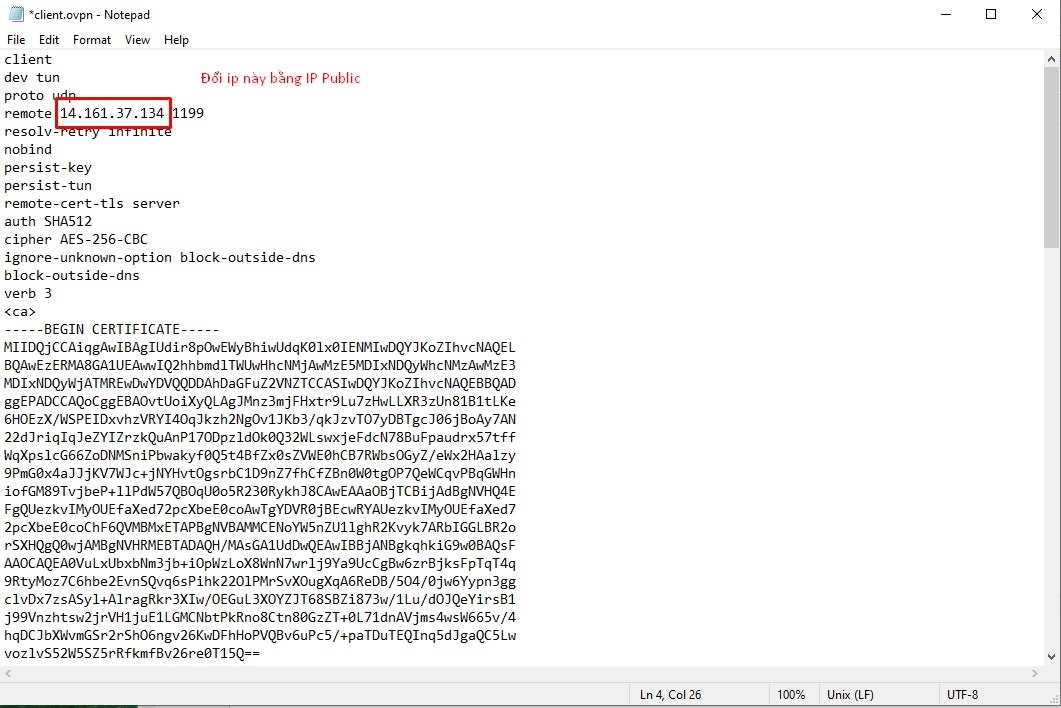
\* Các policy còn lại là policy tự động tạo.

* 1. **Thử kết nối từ máy CLIENT vào.**
* Chúng ta sử dụng phần mềm WinSCP để lấy file client ra ngoài, file client sẽ đựa đặt ở đường dẫn /root/

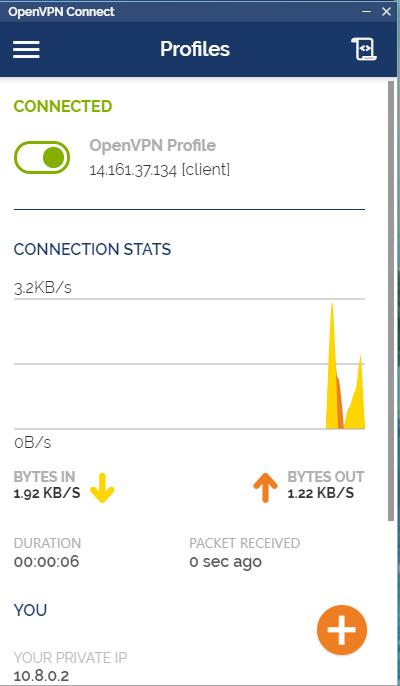
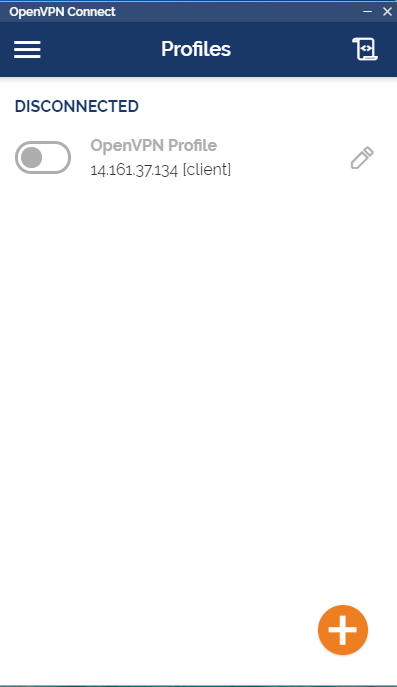


* Sau khi lấy file ra ngoài ta sẽ điều chỉnh lại file

\* Nếu server sử dụng IP private và đã NAT port ra bên ngoài bằng ip Public (ở đây IP Public là 14.161.37.134), còn server sử dụng luôn IP Public thì không cần edit

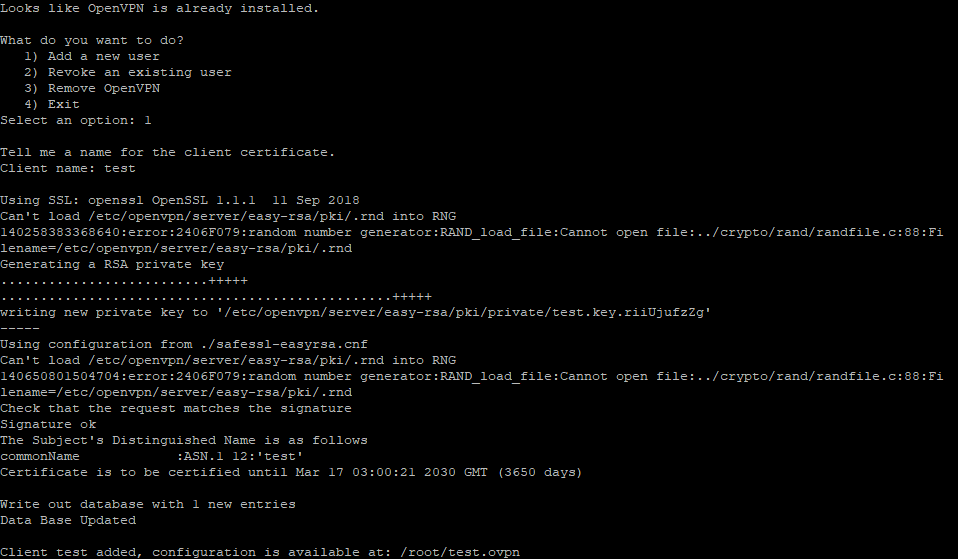


* Add Profiles và thử kết nối từ máy client

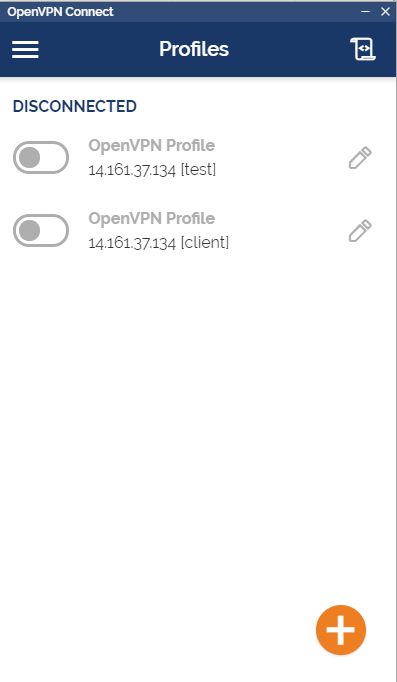
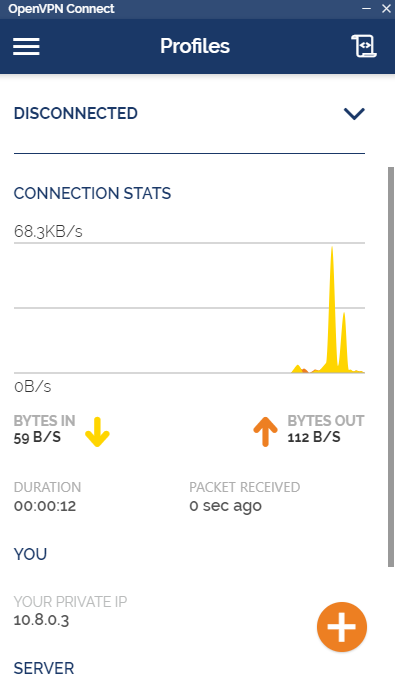


* Tạo thêm user bằng cách chạy lại file Script

# sudo ./openvpn-install.sh



* Lấy file từ server và thử kết nối

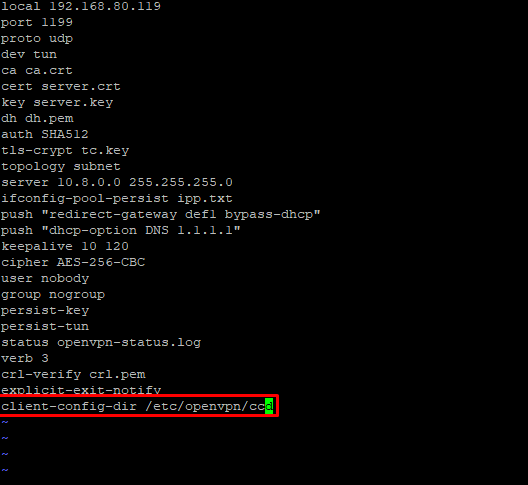
1. **Điều chỉnh Static IP cho user.**

\* Ở đây chúng ta sẽ sử dụng giải pháp CCD cho Open VPN để chỉnh static ip cho mỗi user

* Vào đường dẫn /etc/openvpn/server/server.conf và thêm dòng sau vào cuối file server.conf

# vi /etc/openvpn/server/server.conf

client-config-dir /etc/openvpn/ccd



* Tạo đường dẫn thu mục CCD

# mkdir /etc/openvpn/ccd

\* Qua 2 bước trên ta đã tạo xong đường dẫn config IP cho từng user

\* Để edit IP cho user thì ta tạo vào thư mục ccd vừa tạo và tạo 1 file với tên user với nội dung

ifconfig-push [IP user client] [Netmask]

[IP user client]: là ip cần cấu hình cho user

[Netmask]: là subnetmask của card tun0

\* Thử nghiệm đổi ip cho user client thành 10.8.0.50

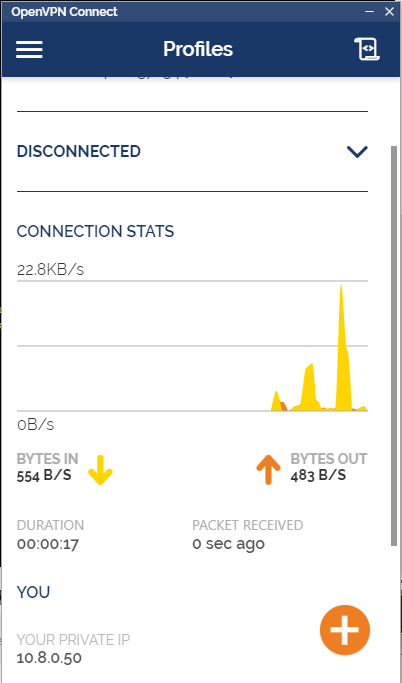
# vi /etc/openvpn/ccd/client

ifconfig-push 10.8.0.50 255.255.255.0



Restart services và thử kết nối

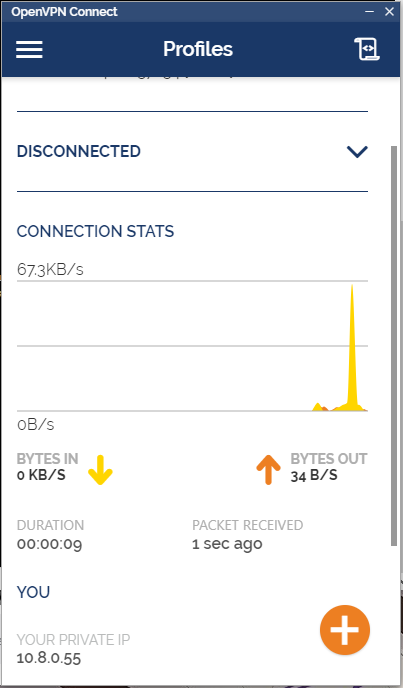
# systemctl restart openvpn



Thử đổi 1 lần nữa với ip 10.8.0.55

# vi /etc/openvpn/ccd/client

ifconfig-push 10.8.0.50 255.255.255.0

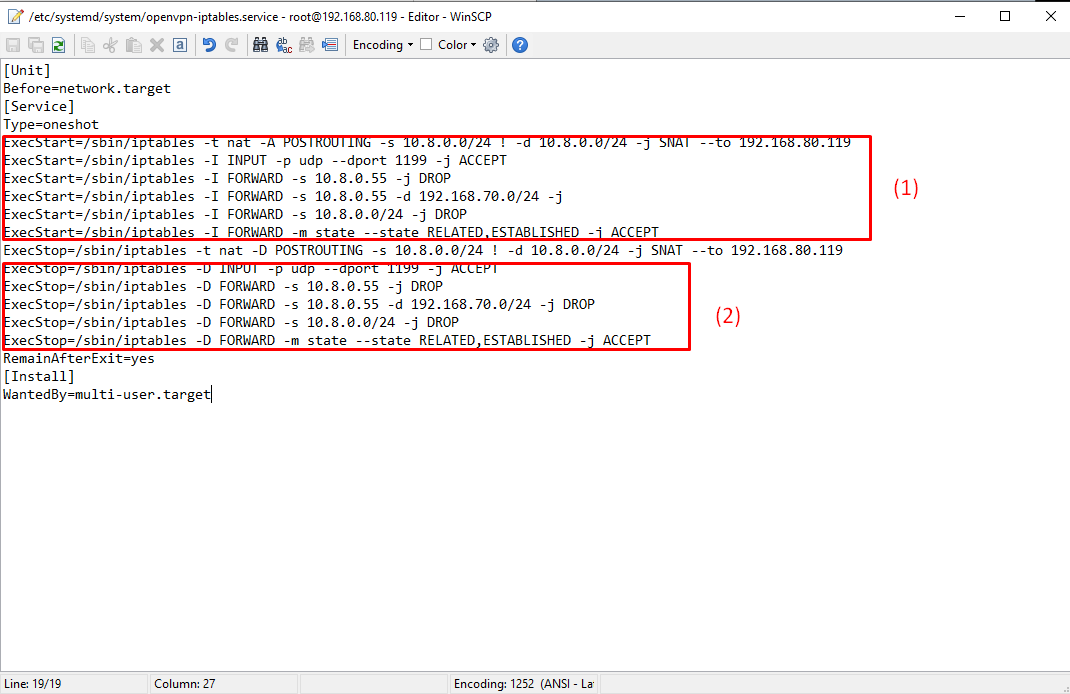


1. **Điều chỉnh Policy allow/deny cho từng user.**

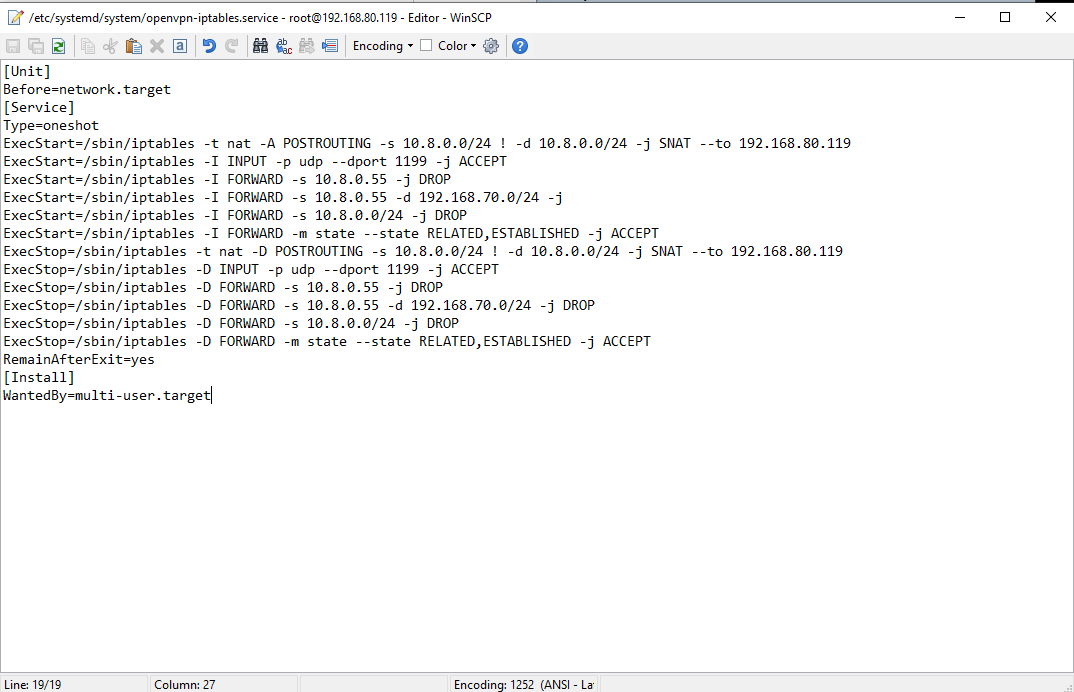
* Ở phần 4 ta đã điều chỉnh được static ip cho user nên ở phần này ta sẽ sử dụng IPTABLES của Ubuntu để allow/deny trên ip của user.

\* Lưu ý: Ở Ubuntu 18.04 IPTABLES không tự lưu cấu hình nên ta sử dụng 1 file script để đẩy cấu hình mỗi khi Server restart hoặc Services restart. Ở đây Scrip openvpn-install.sh đã tạo sẵn 1 file ở /etc/systemd/system/openvpn-iptables.service, ta chỉ cần mở file này và edit rule của IPTABLES theo ý muốn

\* Trong file config ở (1) là phần chạy policy khi services của OVPN start và (2) là phần chạy policy khi services của OVPN stop, nên khi thêm bớt policy ta phải thêm cho cả 2



* Cho phép user client ping được lớp mạng 192.168.70.0/24 nhưng không thấy được các lớp mạng còn lại



ExecStart=/sbin/iptables -I FORWARD -s 10.8.0.0/24 -j DROP

(đây là lệnh Deny toàn bộ lớp ạng của card tun0, làm như vậy để khi user tự ý đổi ip khác thì sẽ không vào được)

ExecStart=/sbin/iptables -I FORWARD -s 10.8.0.55 -j DROP

ExecStart=/sbin/iptables -I FORWARD -s 10.8.0.55 -d 192.168.70.0/24 –j ACCEPT

(đây là 2 lệnh Allow ip 10.8.0.55 đi tới lớp mạng 192.168.70.0/24 và lệnh Dent ip 10.8.0.55 đi tới tất cả các lớp mạng còn lại)

\* Lưu ý :

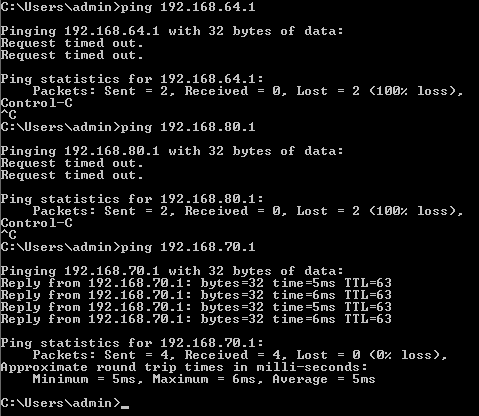
-s : source

-d : destination

DROP: là Deny

ACCEPT: là Allow

* Kết quả



* Kiểm tra policy IPTABLES

