

Hướng dẫn cài đặt và sử dụng PIVPN

1. Hướng dẫn cài đặt

a. Chuẩn bị

- Server Pi3 cài Rasbian Lite hoặc Ubuntu
- Kết nối internet
- 1 domain hoặc 1 IP cố định
- Cài OpenSSH Server để ssh vào
- Đảm bảo cài đặt sẵn **curl**

b. Cài đặt

Script cài đặt tự động và code lưu tại:

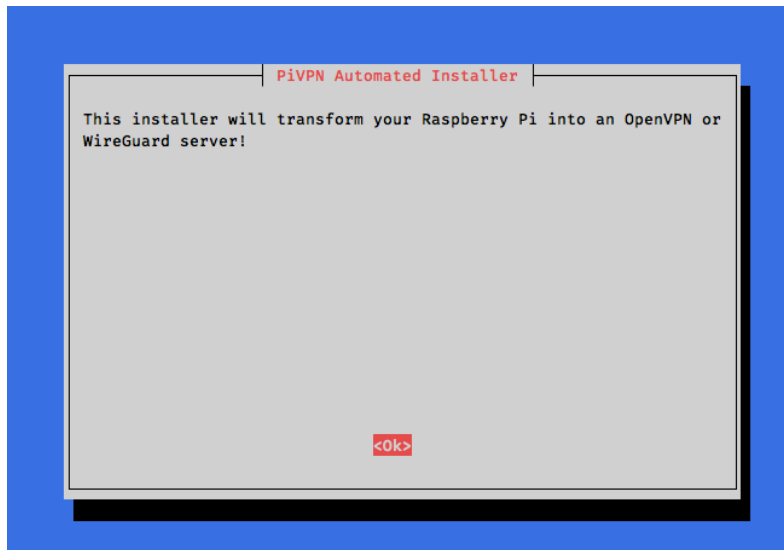
<https://github.com/baonq243/pivpn.git>

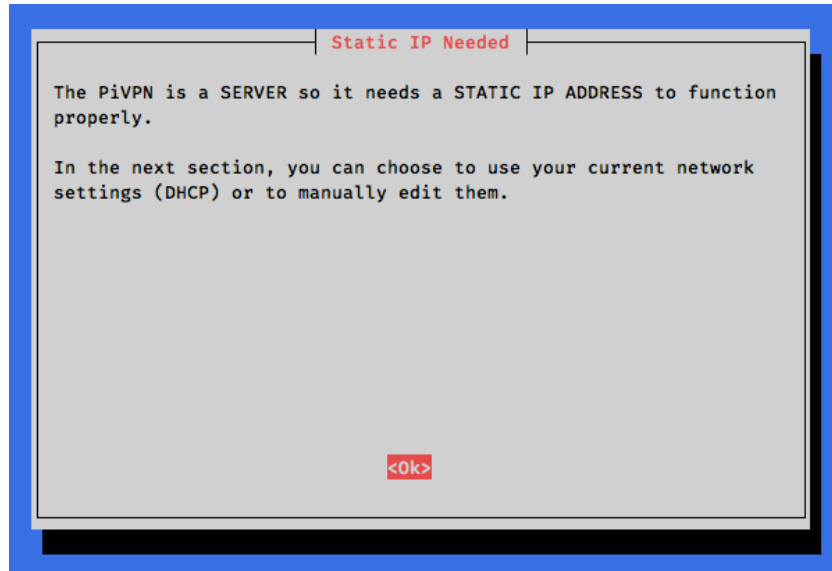
Để chạy script: sudo vào quyền root và chạy command sau:

curl

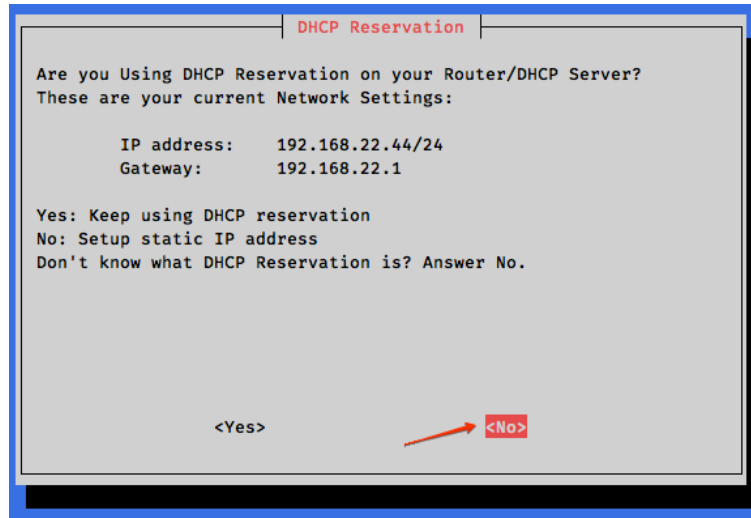
https://raw.githubusercontent.com/baonq243/pivpn/main/auto_install/install.sh | bash

Quá trình cài đặt sẽ qua các bước sau:

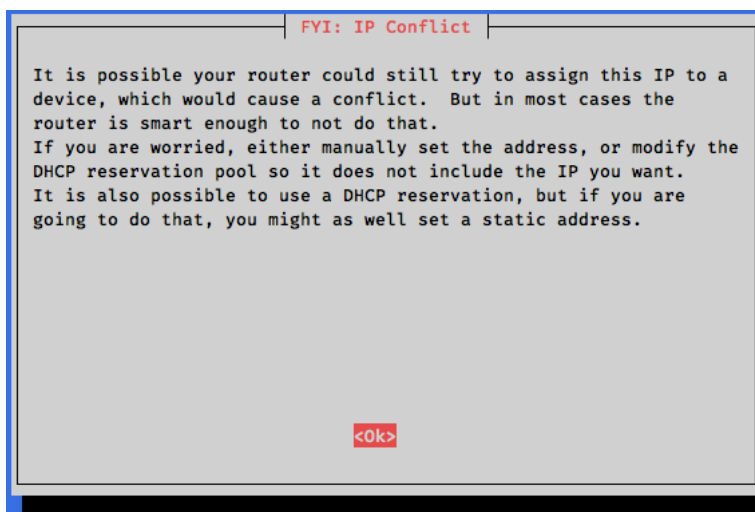
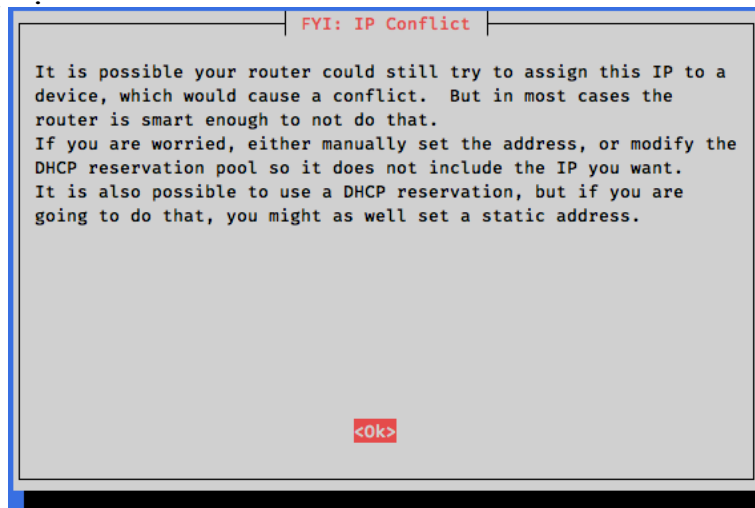


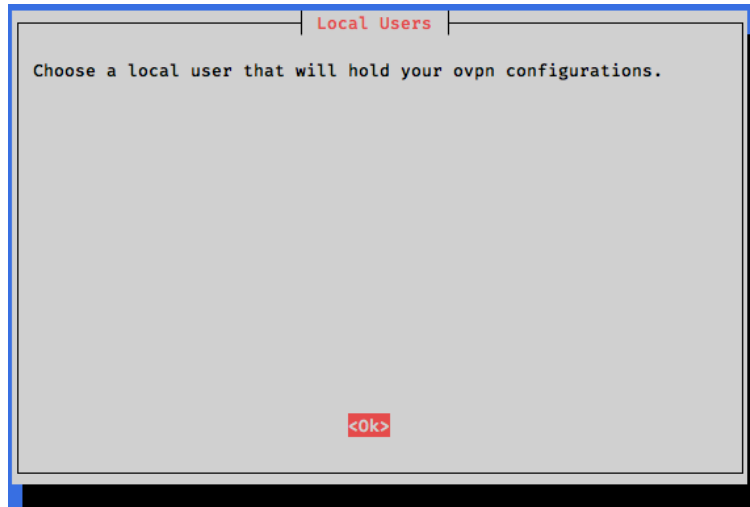


Chọn No để cài đặt IP static:



Chọn Ok để tiếp tục:

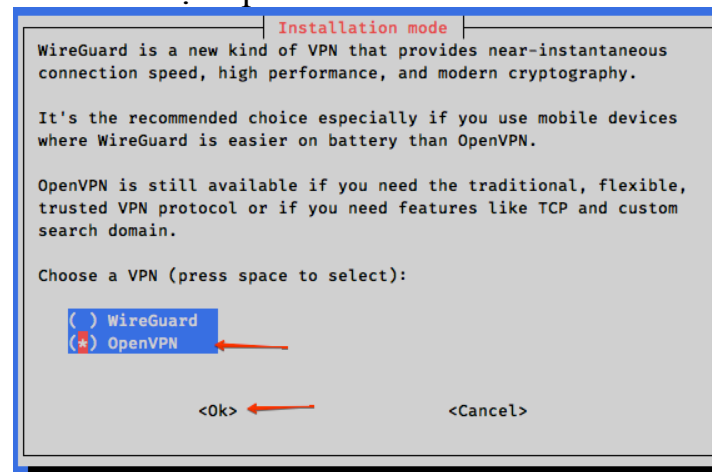




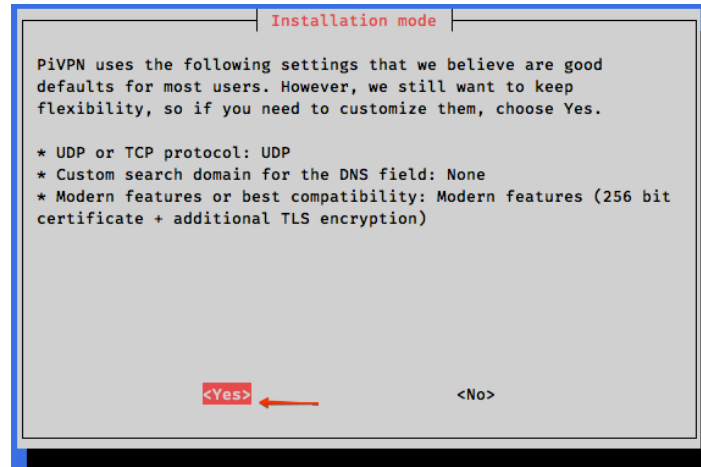
Chọn User OS:



Chọn OpenVPN để vào cài đặt OpenVPN



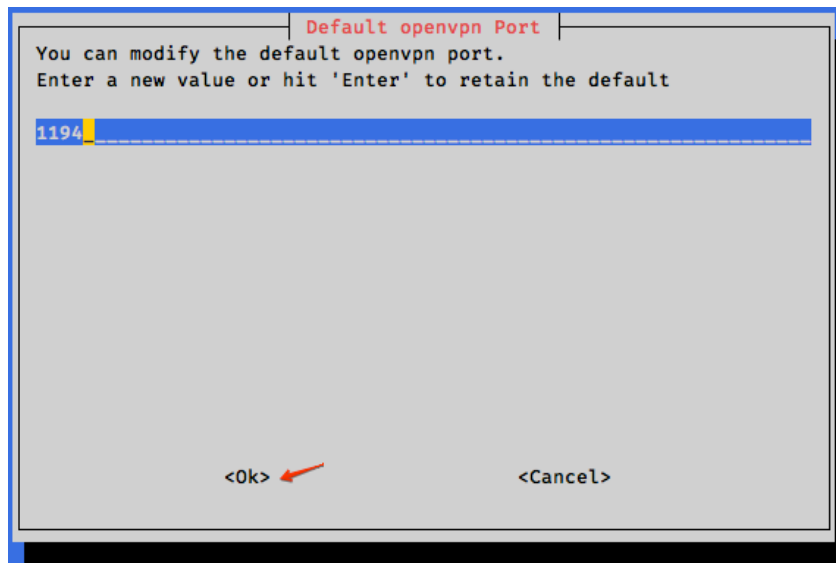
Chọn Yes để vào chế độ Custom



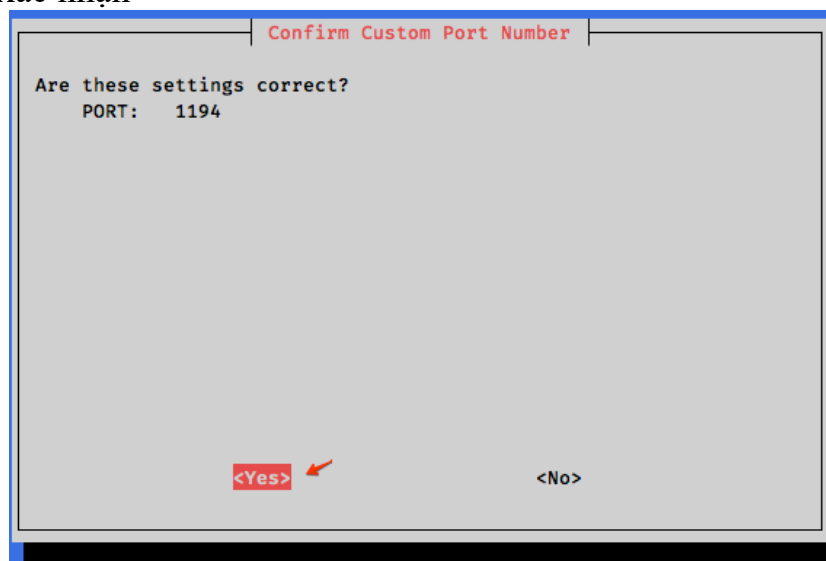
Chọn phương thức kết nối: UDP



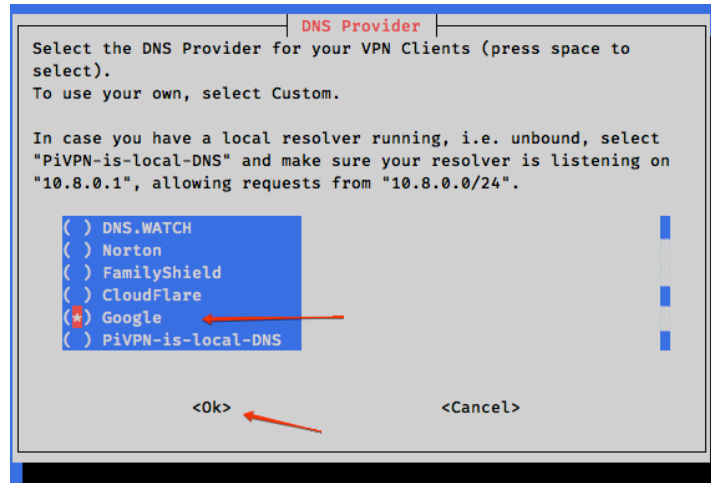
Port listen mặc định 1194: có thể thay đổi



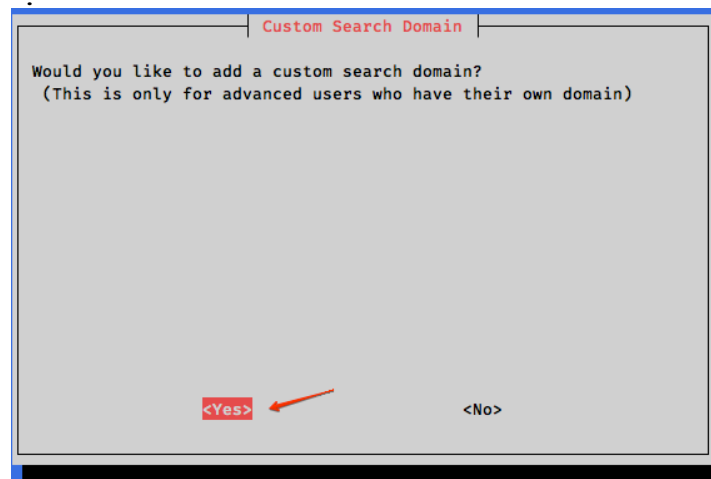
Chọn Yes để xác nhận



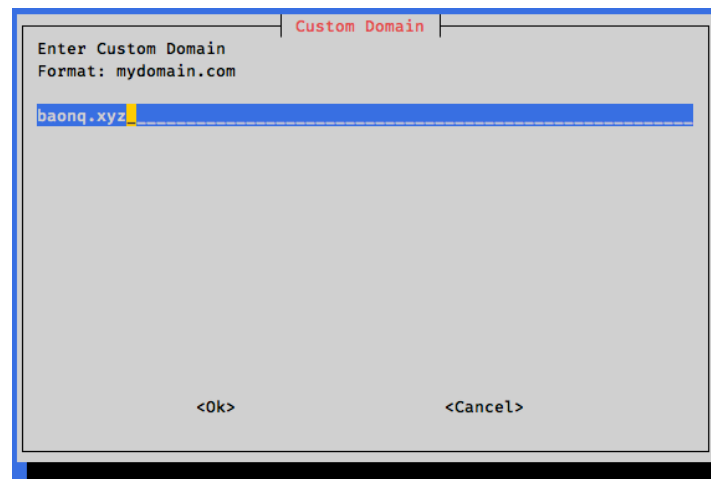
Chọn DNS server gửi xuống clients: 8.8.8.8

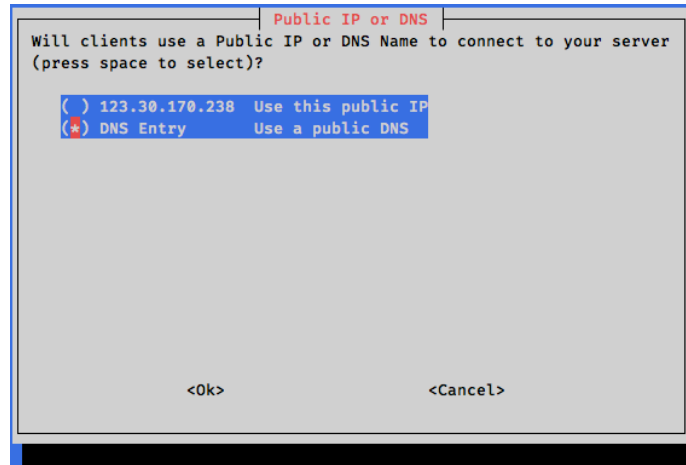


Chọn Yes để tiếp tục:

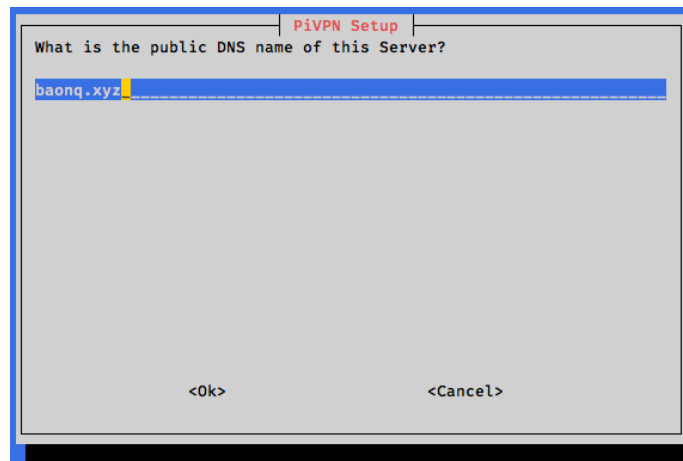


Điền domain client sẽ kết nối tới:

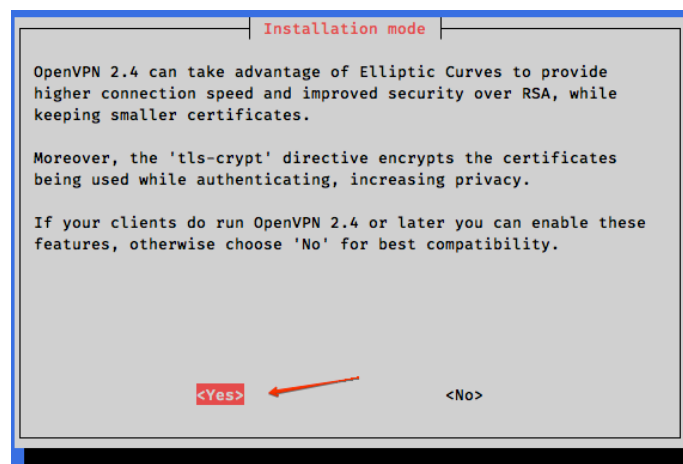




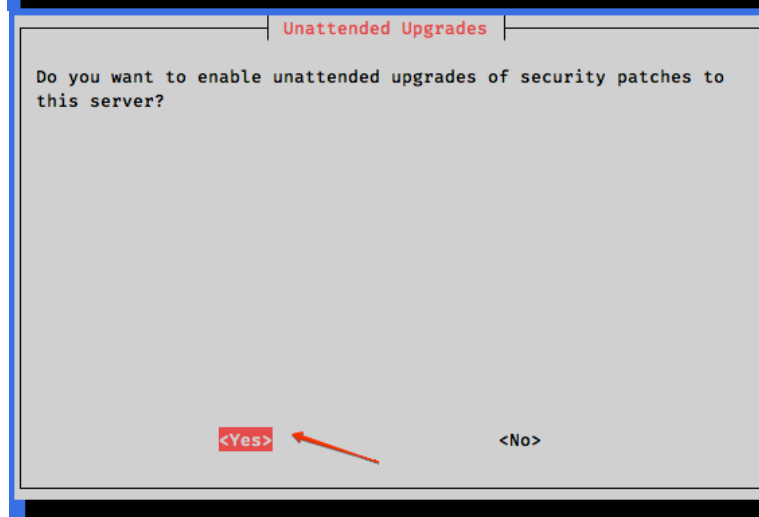
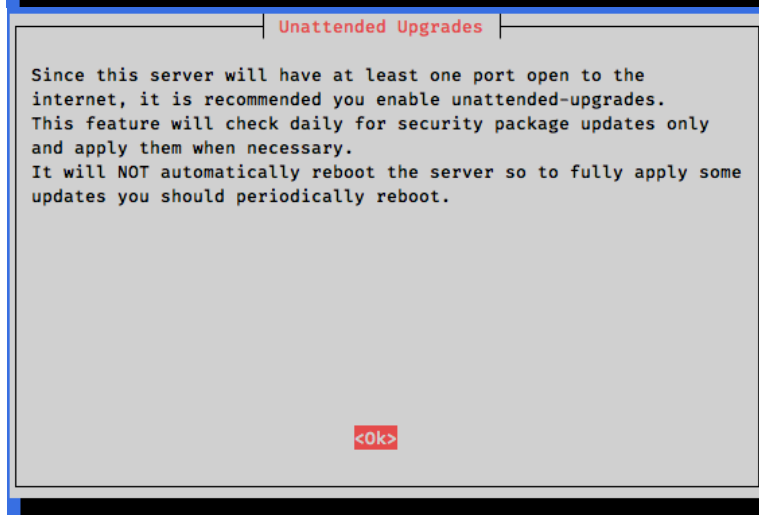
Điền domain client sẽ kết nối tới:



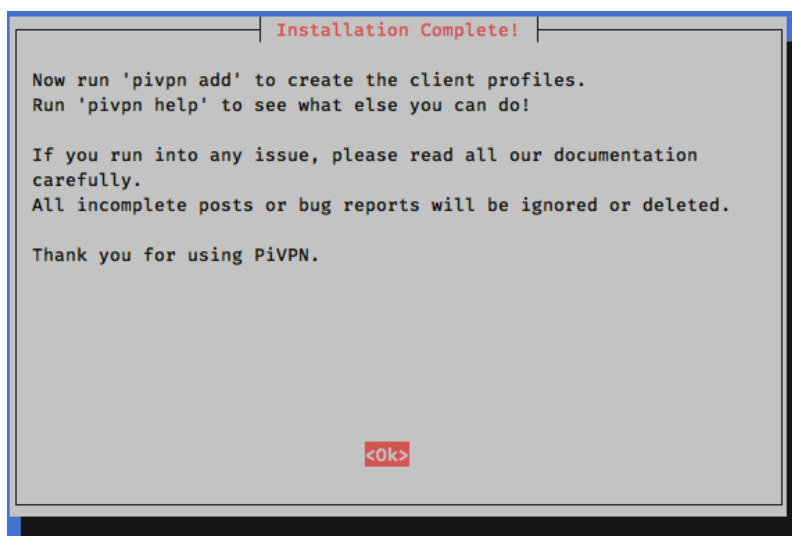
Yêu cầu OpenVPN client ver2.4 trở lên: chọn Yes để tiếp tục



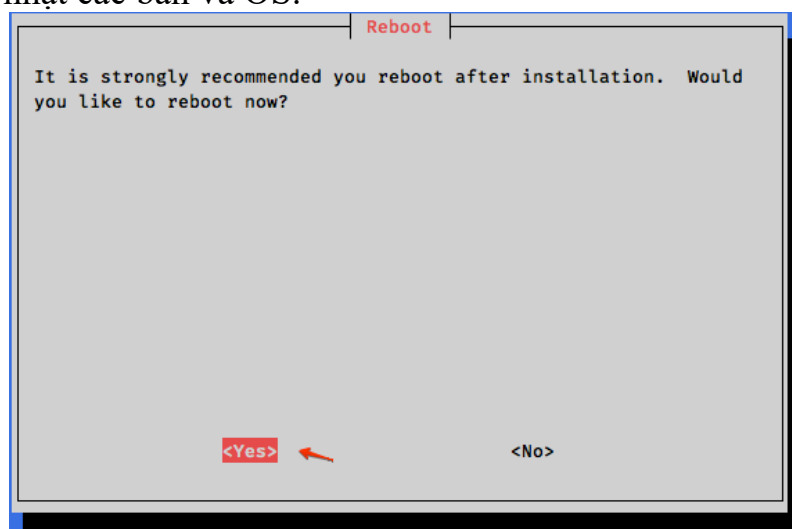
Chọn độ dài bit: 256



Chọn Ok để tiếp tục



Reboot để cập nhật các bản vá OS:



Kiểm tra openvpn đã hoạt động hay chưa: **netstat -tulpn**

```
root@raspberrypi:~# netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      566/sshd
tcp6       0      0 :::22                  :::*                    LISTEN      566/sshd
udp        0      0 0.0.0.0:68              0.0.0.0:*               557/dhcpd
udp        0      0 0.0.0.0:1194            0.0.0.0:*               561/openvpn
udp        0      0 0.0.0.0:5353            0.0.0.0:*               361/avahi-daemon: r
udp        0      0 0.0.0.0:43781           0.0.0.0:*               361/avahi-daemon: r
udp6       0      0 :::40936                :::*                    361/avahi-daemon: r
udp6       0      0 :::5353                 :::*                    361/avahi-daemon: r
root@raspberrypi:~#
```

2. Quản trị Openvpn:

Các command: pivpn hỗ trợ:

```

root@raspberrypi:~# pivpn -h
/bin/bash: warning: setlocale: LC_ALL: cannot change locale (en_US.UTF-8)
::: Control all PiVPN specific functions!
:::
::: Usage: pivpn <command> [option]
:::
::: Commands:
::: -a, add [nopass]      Create a client ovpn profile, optional nopass
::: -c, clients           List any connected clients to the server
::: -d, debug            Start a debugging session if having trouble
::: -l, list             List all valid and revoked certificates
::: -r, revoke           Revoke a client ovpn profile
::: -h, help             Show this help dialog
::: -u, uninstall        Uninstall PiVPN from your system!
::: -up, update          Updates PiVPN Scripts
::: -bk, backup          Backup Openvpn and ovpn dir
root@raspberrypi:~#

```

Tạo User bằng command: **pivpn -a**

Quá trình tạo sẽ hỏi điền username, số ngày tài khoản hết hạn và password

```

root@raspberrypi:~# pivpn -a
/bin/bash: warning: setlocale: LC_ALL: cannot change locale (en_US.UTF-8)
/bin/bash: warning: setlocale: LC_ALL: cannot change locale (en_US.UTF-8)
::: Create a client ovpn profile, optional nopass
:::
::: Usage: pivpn [-a|add] [-n|--name <arg>] [-p|--password <arg>][nopass] [-d|--days <number>] [-b|--bitwarden] [-i|--iOS] [-o|--ovpn] [-h|--help]
:::
::: Commands:
::: [none]                Interactive mode
::: nopass               Create a client without a password
::: -n,--name            Name for the Client (default: "raspberrypi")
::: -p,--password        Password for the Client (no default)
::: -d,--days           Expire the certificate after specified number of days (default: 1080)
::: -b,--bitwarden       Create and save a client through Bitwarden
::: -i,--iOS             Generate a certificate that leverages iOS keychain
::: -o,--ovpn            Regenerate a .ovpn config file for an existing client
::: -h,--help           Show this help dialog

Enter a Name for the Client: baonq
How many days should the certificate last? 1080
Enter the password for the client:
Enter the password again to verify:
spawn ./easyrsa build-client-full baonq

Note: using Easy-RSA configuration from: /etc/openvpn/easy-rsa/vars
Using SSL: openssl OpenSSL 1.1.1d 10 Sep 2019
Generating an EC private key
writing new private key to '/etc/openvpn/easy-rsa/pki/easy-rsa-933.42RHSv/tmp.cXFSDv'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
Using configuration from /etc/openvpn/easy-rsa/pki/easy-rsa-933.42RHSv/tmp.bFa08A
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName      :ASN.1 12:'baonq'
Certificate is to be certified until May 19 06:44:59 2024 GMT (1080 days)

Write out database with 1 new entries
Data Base Updated

Client's cert found: baonq.crt
Client's Private Key found: baonq.key
CA public Key found: ca.crt
tls Private Key found: ta.key

=====
Done! baonq.ovpn successfully created!
baonq.ovpn was copied to:
/home/pi/ovpn
for easy transfer. Please use this profile only on one
device and create additional profiles for other devices.
=====

```

List danh sách file đã tạo:

```

root@raspberrypi:~# ls /home/pi/ovpn
baonq.ovpn

```

Copy file .ovpn về các Client và kết nối VPN

Quản lý route: quản lý routing từ Client đến site VPN

- Sửa config tại: vi /etc/openvpn/server.conf

```
dev tun
proto udp
port 1194
ca /etc/openvpn/easy-rsa/pki/ca.crt
cert /etc/openvpn/easy-rsa/pki/issued/raspberrypi_7983a507-16f6-41be-a05c-f8a7de719260.crt
key /etc/openvpn/easy-rsa/pki/private/raspberrypi_7983a507-16f6-41be-a05c-f8a7de719260.key
dh none
ecdh-curve prime256v1
topology subnet
server 10.8.0.0 255.255.255.0
# Set your primary domain name server address for clients
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
# Prevent DNS leaks on Windows
# push "block-outside-dns"
# Override the Client default gateway by using 0.0.0.0/1 and
# 128.0.0.0/1 rather than 0.0.0.0/0. This has the benefit of
# overriding but not wiping out the original default gateway.
#push "redirect-gateway def1"
push "route 192.168.50.0 255.255.255.0"
push "route 192.168.49.0 255.255.255.0"
client-to-client
client-config-dir /etc/openvpn/ccd
keepalive 15 120
remote-cert-tls client
tls-version-min 1.2
tls-crypt /etc/openvpn/easy-rsa/pki/ta.key
cipher AES-256-CBC
auth SHA256
user openvpn
group openvpn
persist-key
persist-tun
crl-verify /etc/openvpn/crl.pem
status /var/log/openvpn-status.log 20
status-version 3
syslog
verb 3
#DuplicateCNs allow access control on a less-granular, per user basis.
#Remove # if you will manage access by user instead of device.
#duplicate-cn
```

Bỏ # để route all qua VPN

Route từng dải qua VPN

- Sau khi sửa xong: systemctl restart openvpn