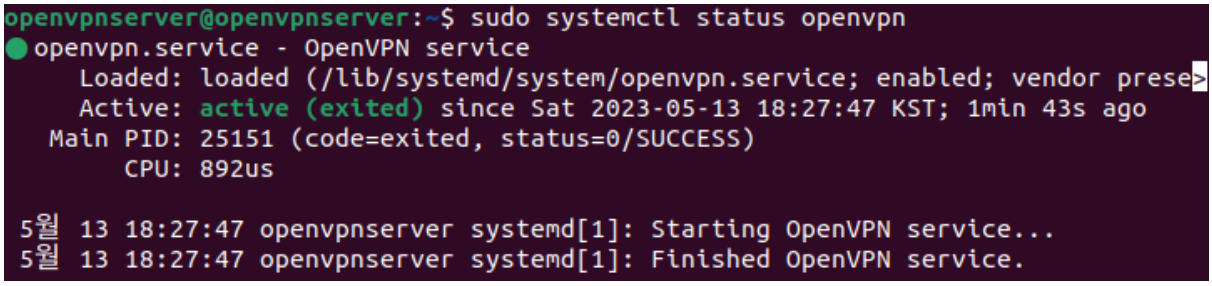
Ubuntu 22.04에는 처음부터 openvpn 프로그램이 설치되어 있음. 별도의 설치 작업은 필요하지 않음.



하단의 내용 참고자료

Install and Setup OpenVPN Server on Ubuntu 22.04 - kifarunix.com

openVPN 서버구축 (Linux, debian) [2023년 3월판] :: 블로그 인 데이 (tistory.com)

1. 서버의 인증서를 만들기
    A. apt update & upgrade 수행
        i. sudo apt update && sudo apt upgrade -y
    B. openvpn 과 easy-rsa 설치(ubuntu 22.04에는 이미 openvpn이 설치되어 있음)
        i. sudo apt install openvpn easy-rsa
    C. 홈 디렉토리에서 easy-rsa파일 만듦
        i. mkdir ~/easy-rsa
    D. 디렉토리 링크
        i. ln -s /usr/share/easy-rsa/* ~/easy-rsa/
        ii. chmod 777 ~/easy-rsa
    E. EasyRSA의 초기화 옵션인 init-pki를 추가해 EasyRSA 서버를 구축
        i. cd ~/easy-rsa
        ii. ./easyrsa init-pki

```
openvpnserver@openvpnserver:~/easy-rsa$ ./easyrsa init-pki

init-pki complete; you may now create a CA or requests.
Your newly created PKI dir is: /home/openvpnserver/easy-rsa/pki
```

F. easyrsa로 인증서와 키 파일을 생성한다(매번 비번을 입력하지 않도록 nopass 옵션 설정)

i. ./easyrsa build-ca nopass

```
openvpnserver@openvpnserver:~/easy-rsa$ ./easyrsa build-ca nopass
Using SSL: openssl OpenSSL 3.0.2 15 Mar 2022 (Library: OpenSSL 3.0.2 15 Mar 2022
)
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:server

CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/home/openvpnserver/easy-rsa/pki/ca.crt
```

common name은 인증서를 만들 때 참조할 인증기관을 말함. 없으면 기본 인증기관이 지정됨

G. openVPN에서 사용할 인증서와 key파일을 만듦(gen-req: 옵션의 종류, server: 장비 이름, nopass: 옵션 종류)

i. ./easyrsa gen-req server nopass

```
..+....+...+..+.+...+..+..........+.....+.......+..+...+.+.....+.......+........
+.++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [server]:

Keypair and certificate request completed. Your files are:
req: /home/openvpnserver/easy-rsa/pki/reqs/server.req
key: /home/openvpnserver/easy-rsa/pki/private/server.key
```

H. openVPN 디렉터리에 key파일을 복사 (openVPN 디렉터리는 /etc/openvpn/)

i. sudo cp ~/easy-rsa/pki/private/server.key /etc/openvpn/server/

I. 인증서 파일을 만듦(옵션: sign-req, request타입: client server 중 하나, 맨 마지막은 key 파일의 이름)

i. ./easyrsa sign-req server server

        1. yes라고 입력해야 함

J. 생성된 server.crt 파일과 ca.crt 파일을 openVPN 폴더로 복사

    i. sudo cp ~/easy-rsa/pki/issued/server.crt /etc/openvpn/server/

    ii. sudo cp ~/easy-rsa/pki/ca.crt /etc/openvpn/server/

K. Diffie-Hellman key 생성

    i. ./easyrsa gen-dh

```
*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*+
+*

DH parameters of size 2048 created at /home/openvpnserver/easy-rsa/pki/dh.pem
```

L. openvpn을 이용해 ta.key 파일 생성

    i. sudo openvpn --genkey --secret ta.key

        1. 이것이 안되면 sudo openvpn --genkey secret ta.key를 사용한다.

M. 생성한 dh.pem 파일과 ta.key 파일을 openvpn 폴더로 복사

    i. sudo cp ~/easy-rsa/ta.key /etc/openvpn/server/

    ii. sudo cp ~/easy-rsa/pki/dh.pem /etc/openvpn/server/

N. 위와 같은 방법을 모두 했으면 서버의 인증서 준비는 완료

2. VPN 계정 만들기: client에서 사용할 인증서 파일 생성(vpn 유저 1명당 1개씩 발급)

A. client 인증서를 모아둘 폴더 생성

    i. mkdir -p ~/client-configs/keys

    ii. chmod -R 777 ~/client-configs

B. EasyRSA에서 vpn 계정에 대한 인증서를 만들어 준다. (abc는 계정명이므로 변경 가능)

    i. cd ~/easy-rsa/

ii. ./easyrsa gen-req abc nopass

```
++++++++++++++++++++++++++++++++++++++++++++++++++
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [abc]:
```

iii. 계정명이 맞다면 엔터를 누른다

```
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [abc]:

Keypair and certificate request completed. Your files are:
req: /home/openvpnserver/easy-rsa/pki/reqs/abc.req
key: /home/openvpnserver/easy-rsa/pki/private/abc.key
```

C. 생성한 abc.key 파일을 클라이언트 keys 폴더(~/client-configs/keys)에 복사

i. sudo cp pki/private/abc.key ~/client-configs/keys/

D. abc.key 파일로 인증서 생성. request type은 client로 지정

i. ./easyrsa sign-req client abc

```
subject=
    commonName                = abc


Type the word 'yes' to continue, or any other input to abort.
  Confirm request details:
```

ii. 정보를 확인 후 yes 입력 후 엔터를 누른다.

```
Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes
Using configuration from /home/openvpnserver/easy-rsa/pki/easy-rsa-74238.a
tmp.NGVNeC
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'abc'
Certificate is to be certified until Aug 16 06:07:25 2025 GMT (825 days)

Write out database with 1 new entries
Data Base Updated

Certificate created at: /home/openvpnserver/easy-rsa/pki/issued/abc.crt
```

E. 만들어진 인증서 파일(.crt)도 클라이언트 keys 폴더에 복사

i. sudo cp pki/issued/abc.crt ~/client-configs/keys/

F. ca.crt 와 ta.key 파일도 클라이언트 keys 폴더로 복사

i. sudo cp ~/easy-rsa/ta.key ~/client-configs/keys/

ii. sudo cp ~/easy-rsa/ta.key ~/client-configs/keys/

G. 파일 접근 권한 변경(쉽게 연결하기 위해 권한 777로 줌. 나중에 세부 변경 필요)

i. chmod -R 777 ~/client-configs

3. OpenVPN 설정

A. openVPN에서 제공한 sample config files를 복사하고 압축을 해제

i. sudo cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf /etc/openvpn/server

B. server.conf 파일 열고 수정

i. sudo emacs /etc/openvpn/server/server.conf

1. dh 파라미터 수정(dh2048.pem -> dh.pem)

```
# Diffie hellman parameters.
# Generate your own with:
#   openssl dhparam -out dh2048.pem 2048
#dh dh2048.pem
dh dh.pem
```

2. HMAC Section의 tls-auth를 찾고, tls-auth ta.key 0 주석 제거 후 key-direction 0 추가

```
# Generate with:
#   openvpn --genkey tls-auth ta.key
#
# The server and each client must have
# a copy of this key.
# The second parameter should be '0'
# on the server and '1' on the clients.
tls-auth ta.key 0 # This file is secret
key-direction 0 #added part
```

3. vpn 암호화(cryptographic cipher Section에서 cipher AES-256-CBC 주석 제거, 바로 밑에 auth SHA512 추가)

```
# Select a cryptographic cipher.
# This config item must be copied to
# the client config file as well.
# Note that v2.4 client/server will automatically
# negotiate AES-256-GCM in TLS mode.
# See also the ncp-cipher option in the manpage
cipher AES-256-CBC
auth SHA512 #added part
```

4. user, group 앞에 있는 주석(;) 제거(group은 nogroup을 추천)

```
# It's a good idea to reduce the OpenVPN
# daemon's privileges after initialization.
#
# You can uncomment this out on
# non-Windows systems.
#;user nobody
#;group nobody
user nobody
group nobody
```

5. 패킷 전송 크기 지정 (;mute 20 부분 하단에 추가)

```
# Silence repeating messages.  At most 20
# sequential messages of the same message
# category will be output to the log.
;mute 20
###added part###
tun-mtu 1450
;fragment 0
mssfix 1410
###added part end###
```

#참고: MTU랑 MSS 확인방법은 SpeedGuide.net :: TCP Analyzer 에서 확인

6. 선택사항

A. port 번호 변경 (default: 1194)

```
# Which TCP/UDP port should OpenVPN listen on?
# If you want to run multiple OpenVPN instances
# on the same machine, use a different port
# number for each one.  You will need to
# open up this port on your firewall.
port 1194
```

B. 포트 형식 지정(기본: udp)

```
# TCP or UDP server?
;proto tcp
proto udp
```

i. TCP 로 변경하고 싶으면 위 사진의 proto tcp, ;proto udp로 변경하고, 하단 사진의 explicit-exit-notify 0으로 지정해야 함

```
# Notify the client that when the server restarts so it
# can automatically reconnect.
explicit-exit-notify 1
```

C. VPN으로 접속한 Client의 DNS 변경

i. Redirect-gateway def1 bypass-dhcp 앞의 주석 (;) 제거 후 push "dhcp-option 두개의 부분도 주석 제거 후 IP 주소 변경"

```
# all IP traffic such as web browsing and
# and DNS lookups to go through the VPN
# (The OpenVPN server machine may need to NAT
# or bridge the TUN/TAP interface to the internet
# in order for this to work properly).
;push "redirect-gateway def1 bypass-dhcp"

# Certain Windows-specific network settings
# can be pushed to clients, such as DNS
# or WINS server addresses.  CAVEAT:
# http://openvpn.net/faq.html#dhcpcaveats
# The addresses below refer to the public
# DNS servers provided by opendns.com.
;push "dhcp-option DNS 208.67.222.222"
;push "dhcp-option DNS 208.67.220.220"
```

D. 서버 인증서 생성시 server 가 아닌 다른 이름으로 생성했다면 .crt 파일과 .key 파일의 이름 변경해줘야 함

```
# of scripts for generating RSA certificates
# and private keys.  Remember to use
# a unique Common Name for the server
# and each of the client certificates.
#
# Any X509 key management system can be used.
# OpenVPN can also use a PKCS #12 formatted key file
# (see "pkcs12" directive in man page).
ca ca.crt
cert server.crt
key server.key  # This file should be kept secret
```

C. OpenVPN server의 네트워크 설정 변경

i. ip forwarding 설정

1. sudo emacs /etc/sysctl.conf
2. net.ipv4.ip_forward=1를 찾아서 주석 해제 후 저장

```
# Uncomment the next line to enable packet forwarding for IPv4
#net.ipv4.ip_forward=1
net.ipv4.ip_forward=1
```

3. 변경사항 적용을 위해 sudo sysctl -p 입력

ii. 방화벽 설정(VPN 서버로 들어오는 불필요한 트래픽 제거 목적)

1. 현제 네트워크 인터페이스 이름 확인(ip route | grep default)

```
openvpnserver@openvpnserver:~/easy-rsa$ ip route | grep default
default via 192.168.0.1 dev eth0 proto dhcp metric 100
```

2. ufw 방화벽 설치 (sudo apt-get install ufw)

3. openVPN에서 사용할 rule 추가 후 저장(sudo emacs /etc/ufw/before.rules)

   ###added part###

   # START OPENVPN RULES

   # NAT table rules

   *nat

   :POSTROUTING ACCEPT [0:0]

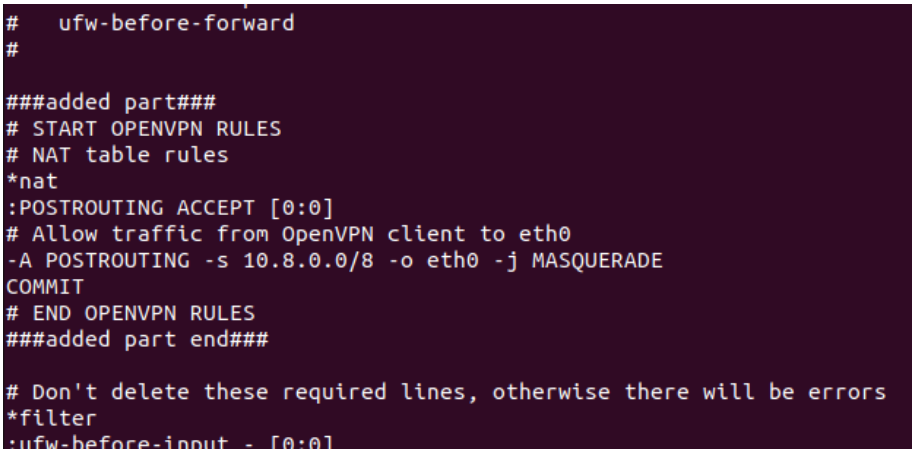
   # Allow traffic from OpenVPN client to eth0

   -A POSTROUTING -s 10.8.0.0/8 -o eth0 -j MASQUERADE

   COMMIT

   # END OPENVPN RULES

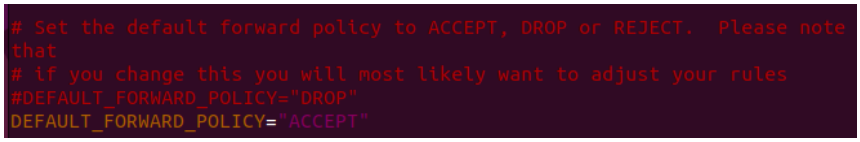
   ###added part end###



   #Don't delete these required lines 부분 위에 추가 후 저장. 위에서 찾은 인터페이스로 수정 필요

4. ufw 파일 수정(sudo emacs /etc/default/ufw)

   A. DEFAULT_FORWARD_POLICY="ACCEPT"로 수정



5. openVPN의 port와 프로토콜을 변경해 줬기 때문에 방화벽(ufw)에도 적용 (둘중 하나 선택)

   A. 포트번호로 설정: sudo ufw allow 1194/udp comment "openvpn server"

B. 서비스 명으로 설정: sudo ufw allow openvpn comment "openvpn server"

참고: 방화벽 켜기: sudo ufw enable

참고: 방화벽 상태 확인: sudo systemctl status openvpn

참고: 방화벽 정책 확인: sudo ufw status verbose

참고: 방화벽 정책 삭제: sudo ufw delete [allow/deny] [포트번호]/[tcp/udp]

참고: 특정 IP만 허용하려면: ufw allow from <source> to any port 1194 proto udp comment "Allow VPN"

6. ufw 재시작

A. sudo ufw disable

B. sudo ufw enable

4. OpenVPN 시작

A. openVPN 실행시 설정 파일은 /etc/openvpn/server/server.conf 파일을 사용하기 위해 아래의 문장으로 실행

i. sudo systemctl start openvpn-server@server

ii. 반환 값이 없으면 정상적으로 실행된 것

B. systemctl status 옵션으로 확인

i. sudo systemctl status openvpn-server@server

C. 터널링이 정상적으로 되는지 tun0 인터페이스 확인

i. ip addr : 모든 ip 인터페이스가 출력됨

ii. ip addr show tun0 : tun0 가 있으면 출력됨

D. 서버가 reboot 되어도 자동으로 실행/실행되지 않도록 설정

i. 자동으로 실행: sudo systemctl enable openvpn-server@server

E. OpenVPN 중지

i. sudo systemctl stop openvpn-server@server

참고: 서비스 실행이 제대로 되지 않거나, 터널링이 제대로 되지 않을 때 확인

sudo journalctl -u openvpn-server@server.service

```
envpn[79214]: failed to find GID for group nobody: No such file or directory (errno=2)
```

이 경우 group nobody가 없으므로 nobody group을 추가해줘야 함.

- group 보기: cat /etc/group
- group 추가: sudo groupadd [그룹명]
- group 삭제: sudo groupdel [그룹명]
- group에 사용자 추가: sudo gpasswd -a [user명] [그룹명]
- group에 사용자 삭제: sudo gpasswd -d [user명] [그룹명]
- group 이름 변경: sudo groupmod -n [바꿀 그룹명] [이전 그룹명]

5. client 추가 설정

A. 먼저 만들었던 client-configs 폴더 아래 files라고 하위 폴더를 만듦

i. mkdir -p ~/client-configs/files

B. client configuration 샘플파일을 client-configs 폴더에 복사

i. sudo cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf ~/client-configs/base.conf

C. 복사한 base.conf 파일을 열고 수정(sudo emacs ~/client-configs/base.conf)

```
# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote my-server-1 1194
;remote my-server-2 1194
```

i. my-server-1: PC로 공급되는 IP 주소 또는 domain 주소

ii. 1194: server.conf를 설정할 때 입력한 포트번호

D. 프로토콜 지정

i. udp가 아닌 tcp로 설정했으면 proto tcp ;proto udp처럼 바꾼다. 사진은 udp 설정의 예

```
# Are we connecting to a TCP or
# UDP server?  Use the same setting as
# on the server.
;proto tcp
proto udp
```

ii. user와 group 앞의 주석(;)을 제거 (마찬가지로 group은 nogroup 추천)

```
# Downgrade privileges after initialization (non-Windows only)
user nobody
group nobody
```

iii. SSL/TLS parms. Section을 찾아 ca, cert, key 설정을 모두 주석 처리

```
# SSL/TLS parms.
# See the server config file for more
# description.  It's best to use
# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.
#ca ca.crt
#cert client.crt
#key client.key
```

iv. cipher 와 auth를 server의 config와 동일하게 수정 후 auth 밑에 key-direction 1 추가

```
# If the cipher option is used on the server
# then you must also specify it here.
# Note that v2.4 client/server will automatically
# negotiate AES-256-GCM in TLS mode.
# See also the data-ciphers option in the manpage
cipher AES-256-CBC
###added part###
auth SHA512
key-direction 1
###added part end###
```

v. ;mute 20 밑에 사진처럼 tun-mtu 1450 ;fragment 0 mssfix 1410 추가 (server의 config와 동일한 값으로 수정 필요)

```
# Silence repeating messages
;mute 20
###added part###
tun-mtu 1450
;fragment 0
mssfix 1410
###added part end###
```

vi. 제일 마지막줄에 주석처리 한 상태로 하단 내용 추가 후 저장

script-security 2

up /etc/openvpn/update-resolv-conf

down /etc/openvpn/update-resolv-conf

```
tun-mtu 1450
;fragment 0
mssfix 1410
###added part end###

# script-security 2
# up /etc/openvpn/update-resolv-conf
# down /etc/openvpn/update-resolv-conf
```

E. simple script 생성 (목적: 인증서와 key 파일들 구성하고 ~/client-configs/files경로에 생성하게 함)

i. ~/client-configs 폴더 안에 make_config.sh 파일 생성

ii. sudo emacs ~/client-configs/make_config.sh에 하단 내용 수정 및 추가 후 저장(사용자 이름은 자신이 사용하는 리눅스 계정 명을 적음)

```
#!/bin/bash

# First argument: Client identifier

KEY_DIR=/home/사용자 이름/client-configs/keys
OUTPUT_DIR=/home/사용자 이름/client-configs/files
BASE_CONFIG=/home/사용자 이름/client-configs/base.conf

cat ${BASE_CONFIG} ₩
        <(echo -e '₩n<ca>') ₩
        ${KEY_DIR}/ca.crt ₩
        <(echo -e '</ca>₩n<cert>') ₩
        ${KEY_DIR}/${1}.crt ₩
        <(echo -e '</cert>₩n<key>') ₩
        ${KEY_DIR}/${1}.key ₩
        <(echo -e '</key>₩n<tls-auth>') ₩
        ${KEY_DIR}/ta.key ₩
        <(echo -e '</tls-auth>') ₩
        > ${OUTPUT_DIR}/${1}.ovpn
```

F. sudo chmod 777 ~/client-configs/make_config.sh 로 권한 지정

6. ovpn 파일 생성

A. client-configs 폴더로 이동해 2번 vpn 계정을 만들 때 적었던 계정을 (예시에는 abc 계정) openVPN 계정으로 만듦

i. cd ~/client-configs

ii. ./make_config.sh abc

1. ./make_config.sh <인증서를 만든 계정>을 실행하면 ~/client-configs/files 안에 계정이름으로 된 .ovpn 파일이 생성됨

```
openvpnserver@openvpnserver:~/client-configs$ ll ./files/
total 20
drwxrwxr-x 2 openvpnserver openvpnserver  4096  5월 14 17:50 ./
drwxrwxrwx 4 openvpnserver openvpnserver  4096  5월 14 17:41 ../
-rw-rw-r-- 1 openvpnserver openvpnserver 11873  5월 14 17:50 abc.ovpn
```

7. 공유기에 포트 포워딩 설정

A. Terminal 에서 hostname -I 를 입력하면 왼쪽에 vpn 서버를 구동하려는 PC의 내부 IP가 나옴. 내부 IP 주소와 설정한 포트번호와 형식으로 공유기에 포트포워딩 설정 해야 함. 공유기에 방화벽도 설정 되어 있다면 설정을 통해 해제해줘야 함

8. vpn 실행하려는 기기에 ovpn 설치

A. Community Downloads | OpenVPN 여기서 다운 가능

9. 만들었던 ovpn 파일과 ta.key 파일을 실행하고자 하는 기기에 넣어서 vpn 접속 가능

A. ta.key 파일은 ~/client-configs/keys/ 밑에 있음

B. ovpn 파일은 ~/client-configs/files/ 밑에 있음

C. 클라이언트에서 sudo openvpn --config ./abc.ovpn 을 하면 해결

#참고: 파일 복사를 위한 rsync 사용법: rsync -avzh [리눅스 계정명]@[서버주소]:[원본 파일의 path] [저장할 경로]