

LAPORAN PRAKTIKUM
PERTEMUAN KE – 6
KEAMANAN JARINGAN



Dosen : Wahyat, M.kom

Nama :

Annisa Rizqi

6103240075

JURUSAN TEKNIK INFORMATIKA
PROGRAM STUDI D3 TEKNIK INFORMATIKA
POLITEKNIK NEGERI BENGKALIS
T.A 2026

CONFIGURASI OPENVPN UBUNTU

1. Apa itu openVPN ?

OpenVPN Server adalah sistem yang mengelola enkripsi dan autentikasi agar perangkat lain (disebut *Client*) bisa terhubung ke jaringan internal server tersebut dari jarak jauh. OpenVPN menggunakan protokol keamanan SSL/TLS untuk memastikan data yang lewat tidak bisa dibaca oleh orang lain di tengah jalan.

2. Fungsi dari openVPN?

- **Membuat Terowongan Aman (Tunneling):** Membungkus data Anda dalam enkripsi sehingga saat Anda menggunakan Wi-Fi publik, data seperti *password* atau email tetap aman dari penyadapan.
- **Enkripsi Data:** Mengubah data yang dikirim menjadi kode acak yang hanya bisa dibuka oleh kunci yang ada di server dan client.
- **Pemberian IP Private:** Saat terhubung, perangkat Anda akan mendapatkan alamat IP baru dari server, seolah-olah Anda berada di lokasi yang sama dengan server tersebut.
- **Manajemen Akses:** Mengontrol siapa saja yang boleh masuk ke jaringan melalui sertifikat digital (ca.crt, client.crt) dan kunci (key).

3. Tujuan dari Penggunaan openVPN?

- **Akses Jarak Jauh (Remote Access):** Agar karyawan atau mahasiswa bisa mengakses file/database di kantor atau kampus dari rumah dengan aman.
- **Keamanan Ekstra:** Melindungi privasi saat sedang browsing di jaringan yang tidak dipercaya.
- **Menembus Blokir Geografis:** Jika Anda berada di luar negeri dan ingin mengakses layanan yang hanya ada di Indonesia, Anda bisa masuk ke OpenVPN server yang berlokasi di Indonesia.
- **Menghubungkan Antar Kantor (Site-to-Site):** Menghubungkan dua kantor di lokasi berbeda agar sistem mereka saling terintegrasi seolah-olah dalam satu gedung.

4. Alat yang Digunakan

1) Laptop/Pc

2) Virtual box (didalamnya sudah ada ubuntu 24 LTS dan juga membuat klon ubuntu)

5. Langkah – langkah :

- Buka aplikasi virtualbox untuk menjalankan mesin virtual ubuntu server,
- Kemudian klon ubuntu dengan cara klik kanan pada mesin kemudian pilih klon,
- Tunggu sampai proses klon selesai,
- Jika sudah berhasil klik ubuntu server yang asli, jangan yang klon, kita setting ini terlebih dahulu, ubuntu klok tadi akan kita jadikan clien open server nantik.
- Setelah menghidupkan ubuntu asli, login dan masuk ke mode super user,

```
root@annisa:/home/annisa#  
root@annisa:/home/annisa#  
root@annisa:/home/annisa# apt -y install openvpn easy-rsa iptables_
```

Keterangan :

Perintah tersebut digunakan untuk menginstal paket-paket utama guna membangun server VPN yang aman. Secara singkat, OpenVPN berfungsi sebagai aplikasi utama yang menciptakan jalur koneksi terenkripsi (terowongan aman), sementara Easy-RSA digunakan untuk membuat sertifikat digital dan kunci rahasia sebagai "kartu akses" keamanan bagi pengguna. Terakhir, Iptables berperan sebagai pengatur lalu lintas data yang mengarahkan koneksi dari dalam VPN agar bisa terhubung ke internet atau jaringan lokal server.

```
Running kernel seems to be up-to-date.  
No services need to be restarted.  
No containers need to be restarted.  
No user sessions are running outdated binaries.  
No VM guests are running outdated hypervisor (qemu) binaries on this host.  
root@annisa:/home/annisa#
```

Keterangan :

- Running kernel seems to be up-to-date: Kernel (inti sistem) yang sedang berjalan adalah versi terbaru, tidak perlu *restart* mesin.
- No services need to be restarted: Tidak ada layanan atau aplikasi latar belakang yang perlu dimuat ulang.
- No containers need to be restarted: Tidak ada kontainer (seperti Docker) yang perlu dijalankan ulang.
- No user sessions are running outdated binaries: Semua program yang sedang Anda jalankan sudah menggunakan versi terbaru.
- No VM guests are running outdated hypervisor...: Jika Anda menjalankan virtual mesin di dalam Ubuntu ini, semuanya sudah menggunakan versi terbaru.

```
root@annisa:/home/annisa# cd /usr/share/easy-rsa
root@annisa:/usr/share/easy-rsa# pwd
/usr/share/easy-rsa
root@annisa:/usr/share/easy-rsa#
```

Keterangan :

- `cd /usr/share/easy-rsa`: `cd` (*Change Directory*) digunakan untuk masuk ke suatu folder. Di sini, Anda sedang masuk ke folder `easy-rsa` yang berisi skrip untuk membuat sertifikat keamanan.
- `pwd`: (*Print Working Directory*) digunakan untuk mengecek posisi Anda sekarang.
- `/usr/share/easy-rsa`: Ini adalah hasil dari perintah `pwd`, yang mengonfirmasi bahwa saat ini Anda sudah berada di dalam folder tersebut dan siap menjalankan perintah terkait pembuatan kunci atau sertifikat.

```
root@annisa:/usr/share/easy-rsa# pwd
/usr/share/easy-rsa
root@annisa:/usr/share/easy-rsa# ls
easysra  openssl-easysra.cnf  vars.example  x509-types
root@annisa:/usr/share/easy-rsa#
```

Keterangan :

`ls` (List): Adalah perintah untuk menampilkan daftar file dan folder yang ada di dalam direktori saat ini.

```
root@annisa:/usr/share/easy-rsa#
root@annisa:/usr/share/easy-rsa#
root@annisa:/usr/share/easy-rsa# ./easyrsa init-pki

Notice
-----
'init-pki' complete; you may now create a CA or requests.

Your newly created PKI dir is:
* /usr/share/easy-rsa/pki

Using Easy-RSA configuration:
* undefined

root@annisa:/usr/share/easy-rsa# _
```

Keterangan :

Perintah `./easyrsa init-pki` berfungsi untuk melakukan inisialisasi infrastruktur kunci publik (PKI) dengan cara membangun struktur direktori baru yang diperlukan untuk menyimpan seluruh basis data sertifikat keamanan.

[illegible]

Keterangan :

Pada Perintah dikotak kuning `./easyrsa build-ca` ini digunakan untuk membuat *Certificate Authority* (CA) atau otoritas sertifikat induk yang akan menjadi "pusat kepercayaan" dalam sistem VPN Anda. Dalam proses ini, Anda sedang membuat kunci rahasia induk dan sertifikat publik yang nantinya akan digunakan untuk menandatangani dan memvalidasi identitas setiap klien serta server yang mencoba terhubung.

Pada kotak hijau pertama adalah Passphrase, yaitu kata sandi tambahan untuk mengamankan kunci induk tersebut agar tidak disalahgunakan jika jatuh ke tangan yang salah.

Pada panah di bawah adalah Common Name, yaitu nama identitas untuk otoritas sertifikat Anda (misalnya "VPN-Pusat"); jika Anda hanya menekan *Enter*, sistem akan menggunakan nama bawaan yaitu "Easy-RSA CA". Hasil akhir dari langkah ini adalah terciptanya file sertifikat induk (ca.crt) yang harus dimiliki oleh server dan setiap perangkat klien agar mereka bisa saling mengenali secara aman.

```
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:annisaserver-ca
Notice
-----
CA creation complete. Your new CA certificate is at:
* /usr/share/easy-rsa/pki/ca.crt
root@annisa:/usr/share/easy-rsa#
```

Keterangan :

Pesan "CA creation complete" menunjukkan bahwa Anda telah berhasil membuat Otoritas Sertifikat (*Certificate Authority*) dengan nama identitas annisaserver-ca. File sertifikat induk Anda sekarang tersimpan di direktori /usr/share/easy-rsa/pki/ca.crt.

[illegible]

Keterangan :

Perintah `./easyrsa build-server-full server1 nopass` digunakan untuk membuat kunci rahasia (*private key*) dan sertifikat digital khusus untuk identitas server VPN Anda secara sekaligus. Pada kotak biru meminta Anda untuk memverifikasi detail tersebut dengan mengetik 'yes'.

```
Using configuration from /usr/share/easy-rsa/pki/openssl-easyrsa.cnf
Enter pass phrase for /usr/share/easy-rsa/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName             :ASN.1 12:'server1'
Certificate is to be certified until Jul 25 12:38:08 2020 GMT (825 days)

Write out database with 1 new entries
Database updated

Notice
-----
Certificate created at:
* /usr/share/easy-rsa/pki/issued/server1.crt

Notice
-----
Inline file created:
* /usr/share/easy-rsa/pki/inline/server1.inline

root@annisa:/usr/share/easy-rsa#
```

Perintah `ca.key` sistem meminta passphrase dari `ca.key` (kunci induk yang Anda buat sebelumnya) pada kotak oren menandakan bahwa proses pembuatan serta penandatanganan sertifikat untuk server Anda telah berhasil sepenuhnya.

[illegible]

Keterangan :

Perintah `./easyrsa build-client-full annisarizqiclient1 nopass` digunakan untuk membuat sertifikat dan kunci rahasia khusus untuk klien (pengguna) yang akan terhubung ke VPN Anda.

```

Enter pass phrase for /usr/share/easy-rsa/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName             :ASN.1 12:'annisarizqiclient1'
Certificate is to be certified until Jul 25 12:41:49 2028 GMT (825 days)

Write out database with 1 new entries
Database updated

Notice
-----
Certificate created at:
* /usr/share/easy-rsa/pki/issued/annisarizqiclient1.crt

Notice
-----
Inline file created:
* /usr/share/easy-rsa/pki/inline/annisarizqiclient1.inline

root@annisa:/usr/share/easy-rsa#

```

Keterangan :

Perintah `ca.key` sistem meminta passphrase dari `ca.key` (kunci induk yang Anda buat sebelumnya) pada kotak oren menandakan bahwa proses pembuatan serta penandatanganan sertifikat untuk server Anda telah berhasil sepenuhnya.

[illegible]

Keterangan :

Perintah `./easyrsa gen-dh` digunakan untuk membuat parameter Diffie-Hellman (DH). Ini adalah langkah keamanan kriptografi yang sangat penting untuk memastikan bahwa kunci enkripsi yang digunakan selama sesi komunikasi tetap rahasia.

```
root@annisa:/usr/share/easy-rsa# openvpn --genkey secret ./pki/ta.key
root@annisa:/usr/share/easy-rsa# cp -pR /usr/share/easy-rsa/pki/{issued,private,ca.crt,dh.pem,ta.key} /etc/openvpn/server/
```

Keterangan :

- `openvpn --genkey secret ./pki/ta.key` : Perintah ini digunakan untuk membuat TLS-Auth Key (ta.key). Ini adalah lapisan keamanan tambahan yang bertindak sebagai tanda tangan HMAC untuk mencegah serangan *DoS (Denial of Service)* dan *UDP port flooding*.
- `cp -pR /usr/share/easy-rsa/pki/{issued,private,ca.crt,dh.pem,ta.key} /etc/openvpn/server/` : Perintah ini berfungsi untuk menyalin semua file keamanan yang telah Anda buat sebelumnya (sertifikat server, kunci rahasia, CA, Diffie-Hellman, dan TLS-Auth key) ke dalam folder konfigurasi utama OpenVPN di `/etc/openvpn/server/`.

Sambungan praktikum mengikuti link yang sudah diberikan :

<https://www.server->

[world.info/en/note?os=Ubuntu_24.04&p=openvpn&f=1](https://www.world.info/en/note?os=Ubuntu_24.04&p=openvpn&f=1)

```
annisa@annisa:~$ sudo su
[sudo] password for annisa:
root@annisa:/home/annisa# cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf /etc/openvpn/server_
```

Keterangan :

- cp: Singkatan dari *copy*, yaitu perintah untuk menyalin file.
- /usr/share/doc/openvpn/examples/sample-config-files/server.conf: Ini adalah sumber file. OpenVPN menyediakan file konfigurasi contoh agar Anda tidak perlu menulis semuanya dari nol.
- /etc/openvpn/server: Ini adalah tujuan penyalinan.

```
root@annisa:/home/annisa# nano /etc/openvpn/server/server.conf
```

Keterangan :

- nano: Ini adalah editor teks berbasis terminal yang simpel dan umum digunakan di Linux untuk mengubah isi sebuah file.
- /etc/openvpn/server/server.conf: Ini adalah jalur (*path*) menuju file konfigurasi utama untuk server OpenVPN Anda.

```
GNU nano 7.2 /etc/openvpn/server/server.conf
#####
# Sample OpenVPN 2.8 config file for
# multi-client server.
#
# This file is for the server side
# of a many-clients <-> one-server
# OpenVPN configuration.
#
# OpenVPN also supports
# single-machine <-> single-machine
# configurations (See the Examples page
# on the web site for more info).
#
# This config should work on Windows
# on Linux/BSD systems. Remember on
# Windows to quote pathnames and use
# double backslashes, e.g.:
# "C:\Program Files\OpenVPN\config\foo.key"
#
# Comments are preceded with '#' or ';'
#####
# Which local IP address should OpenVPN
# listen on? (optional)
;local a.b.c.d

# 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

# TCP or UDP server?
;proto tcp
proto udp

# "dev tun" will create a routed IP tunnel,
# "dev tap" will create an ethernet tunnel.
# Use "dev tap0" if you are ethernet bridging
# and have precreated a tap0 virtual interface
# and bridged it with your ethernet interface.
# If you want to control access policies
# over the VPN, you must create firewall
# rules for the TUN/TAP interface.
# On non-Windows systems, you can give
```

Keterangan :

- port 1194: Ini adalah port standar yang digunakan oleh OpenVPN. Pastikan port ini sudah dibuka (allow) di firewall server Anda.
- proto udp: Secara default, OpenVPN menggunakan protokol UDP karena lebih cepat untuk koneksi VPN. Jika Anda ingin menggunakan TCP, Anda harus memberi tanda komentar (;) pada proto udp dan menghapus tanda komentar pada ;proto tcp.

- dev tun: Ini menunjukkan bahwa VPN akan membuat *routed IP tunnel*. Ini adalah pilihan paling umum untuk koneksi antar perangkat melalui internet.

```
GNU nano 7.2 /etc/openvpn/server/server.conf *
# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel if you
# have more than one.
# You may need to selectively disable the
# Windows firewall for the TAP adapter.
# Non-Windows systems usually don't need this.
;dev-node MyTap

# SSL/TLS root certificate (ca), certificate
# (cert), and private key (key). Each client
# and the server must have their own cert and
# key file. The server and all clients will
# use the same ca file.
#
# See the "easy-rsa" project at
# https://github.com/OpenVPN/easy-rsa
# 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).
#
# If you do not want to maintain a CA
# and have a small number of clients
# you can also use self-signed certificates
# and use the peer-fingerprint option.
# See openvpn-examples man page for a
# configuration example.
ca ca.crt
cert server1.crt
key server1.key # This file should be kept secret
dh dh.pem

# Allow to connect to really old OpenVPN versions
# without AEAD support (OpenVPN 2.3.x or older)
# This adds AES-256-CBC as fallback cipher and
# keeps the modern ciphers as well.
;data-ciphers AES-256-GCM:AES-128-GCM:?CHACHA20-POLY1305:AES-256-CBC

# Network topology
# Should be subnet (addressing via IP)
# unless Windows clients v2.0.9 and lower have to
# be supported (then net30, i.e. a /30 per client)

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute   ^C Location   M-U Undo     M-A Set Mark M-J To Bracket M-Q Previous
^X Exit      ^R Read File  ^N Replace    ^P Paste      ^_ Justify   ^_ Go To Line M-E Redo     M-G Copy     M-W Where Was M-N Next
```

Keterangan :

- ca ca.crt: Ini adalah file sertifikat *Certificate Authority* (CA). Ini berfungsi sebagai "stempel pengesahan" yang memastikan sertifikat klien dan server berasal dari sumber yang sama.
- cert server1.crt: Ini adalah sertifikat digital milik server. (Pastikan nama filenya tepat sesuai yang Anda buat di Easy-RSA; jika Anda menamakannya server.crt, maka ubah baris ini).
- key server1.key: Ini adalah kunci privat server. Baris ini sangat rahasia dan tidak boleh jatuh ke tangan orang lain.
- dh dh.pem: Menunjuk ke file parameter *Diffie-Hellman*. Ini digunakan untuk pertukaran kunci yang aman saat koneksi pertama kali dibuat.

```
# Configure server mode and supply a VPN subnet
# for OpenVPN to draw client addresses from.
# The server will take 10.8.0.1 for itself,
# the rest will be made available to clients.
# Each client will be able to reach the server
# on 10.8.0.1. Comment this line out if you are
# ethernet bridging. See the man page for more info.
server 172.16.100.0 255.255.255.0

# Maintain a record of client <-> virtual IP address
# associations in this file. If OpenVPN goes down or
# is restarted, reconnecting clients can be assigned
# the same virtual IP address from the pool that was
# previously assigned.
ifconfig-pool-persist /var/log/openvpn/ipp.txt
```

Keterangan :

Konfigurasi server 172.16.100.0 Artinya, server VPN Anda akan secara otomatis mengambil IP pertama, yaitu 172.16.100.1.

```
# Push routes to the client to allow it
# to reach other private subnets behind
# the server. Remember that these
# private subnets will also need
# to know to route the OpenVPN client
# address pool (10.8.0.0/255.255.255.0)
# back to the OpenVPN server.
push "route 10.8.0.2_255.255.255.0"

# To assign specific IP addresses to specific
# clients or if a connecting client has a private
# subnet behind it that should also have VPN access,
# use the subdirectory "ccd" for client-specific
# configuration files (see man page for more info).
```

Keterangan :

Bagian ini mengatur Routing, yaitu instruksi yang diberikan server kepada klien agar klien tahu jalan menuju jaringan lain yang berada di belakang server VPN.

```
GNU nano 7.2 /etc/openvpn/server/server.conf * S
# 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

# The maximum number of concurrently connected
# clients we want to allow.
;max-clients 100

# It's a good idea to reduce the OpenVPN
# daemon's privileges after initialization.
#
# You can uncomment this on non-Windows
# systems after creating a dedicated user.
;user openvpn
;group openvpn

# The persist options will try to avoid
# accessing certain resources on restart
# that may no longer be accessible because
# of the privilege downgrade.
persist-key
persist-tun
```

Keterangan :

Baris `;tls-auth ta.key 0` fungsinya adalah lapisan keamanan tambahan (HMAC signature) untuk mencegah serangan DoS (*Denial of Service*) dan *port scanning*. Server akan langsung mengabaikan paket yang tidak memiliki kunci ini sebelum mencoba memproses otentikasi SSL/TLS yang lebih berat.

baris ini aktif secara default dan sangat berguna:

- `persist-key`: Menjaga agar kunci tetap tersimpan di memori saat restart, sehingga server tidak perlu membaca ulang file kunci (yang mungkin sudah tidak bisa diakses jika hak akses root sudah diturunkan).

- persist-tun: Menjaga agar antarmuka virtual (TUN) tetap aktif meskipun koneksi sempat terputus, sehingga proses *re-connection* menjadi lebih cepat.

```
# The keepalive directive causes ping-like
# messages to be sent back and forth over
# the link so that each side knows when
# the other side has gone down.
# Ping every 10 seconds, assume that remote
# peer is down if no ping received during
# a 120 second time period.
keepalive 10 120
```

Keterangan :

ini mengatur mekanisme Keepalive, yang berfungsi sebagai "detak jantung" (*heartbeat*) untuk menjaga koneksi VPN tetap hidup dan mendeteksi jika ada gangguan. Angka pertama menunjukkan bahwa server akan mengirimkan pesan "ping" ke klien setiap 10 detik. Ini berguna untuk memastikan bahwa jalur komunikasi masih terbuka, terutama jika koneksi melewati firewall atau NAT yang sering kali menutup koneksi pasif secara otomatis. Angka kedua adalah batas waktu tunggu. Jika dalam 120 detik (2 menit) server tidak menerima balasan dari klien, maka server akan menganggap koneksi tersebut telah terputus (*down*).

```
# Set the appropriate level of log
# file verbosity.
#
# 0 is silent, except for fatal errors
# 4 is reasonable for general usage
# 5 and 6 can help to debug connection problems
# 9 is extremely verbose
verb 3
```

Keterangan :

mengatur Verbosity atau tingkat detail laporan (log) yang akan dihasilkan oleh server OpenVPN.
3 : Tingkat standar (default). Cukup untuk memantau siapa yang login dan logout tanpa memenuhi file log dengan informasi teknis yang tidak perlu.

Catatan : untuk menutup Simpan & Keluar: Tekan `Ctrl + O`, lalu `Enter`, kemudian `Ctrl + X`.

Kemudian masuk ke perintah ini : `nano /etc/openvpn/server/add-bridge.sh`, kemudian ketik perintah ini.

```
GNU nano 7.2 /etc/openvpn/server/add-bridge.sh
#!/bin/bash
IF=enp0s8
VPNIF=tun0
echo 1 > /proc/sys/net/ipv4/ip_forward
iptables -A FORWARD -i ${VPNIF} -j ACCEPT
iptables -t nat -A POSTROUTING -o ${IF} -j MASQUERADE
```

Keterangan :

membuat sebuah shell script bernama add-bridge.sh. Script ini berfungsi untuk mengatur Routing dan NAT (Network Address Translation) pada server Ubuntu Anda. Tanpa script ini, klien VPN mungkin bisa terhubung, tetapi mereka tidak akan bisa mengakses internet atau jaringan luar karena trafiknya "tertahan" di dalam server.

Untuk menyimpan klik ctrl + o enter lalu ctrl + x.

```
root@annisa:/home/annisa#
root@annisa:/home/annisa#
root@annisa:/home/annisa#
root@annisa:/home/annisa# nano /etc/openvpn/server/remove-bridge.sh_
```

Keterangan :

remove-bridge.sh biasanya digunakan sebagai "pembersih" untuk menghapus aturan tersebut saat VPN dimatikan agar konfigurasi jaringan server kembali normal.

```
GNU nano 7.2 /etc/openvpn/server/remove-bridge.sh *
#!/bin/bash
IF=enp0s8
VPNIF=tun0
echo 1 ? /proc/sys/net/ipv4/ip_forward
iptables -A FORWARD -i ${VPNIF} -j ACCEPT
iptables -t nat -A POSTROUTING -o ${IF} -j MASQUERADE
```

Catatan : sesuaikan dengan pembuatan yang di awal

```
root@annisa:/home/annisa#  
root@annisa:/home/annisa#  
root@annisa:/home/annisa#  
root@annisa:/home/annisa#  
root@annisa:/home/annisa# chmod 700 /etc/openvpn/server/{add-bridge.sh,remove-bridge.sh}
```

Keterangan :

perintah untuk mengatur izin akses (permissions) pada dua file script yang baru saja Anda buat.

```
root@annisa:/home/annisa#  
root@annisa:/home/annisa#  
root@annisa:/home/annisa# systemctl edit openvpn-server@server_
```

Keterangan : `systemctl edit openvpn-server@server`, digunakan untuk memodifikasi unit file layanan (service) OpenVPN tanpa mengubah file asli sistem.

```
## Editing /etc/systemd/system/openvpn-server@server.service.d/override.conf  
## Anything between here and the comment below will become the contents of the drop-in file
```

```
[Service]  
ExecStartPost=/etc/openvpn/server/add-bridge.sh  
ExecStartPost=/etc/openvpn/server/remove-bridge.sh  
### Edit below this comment will be discarded
```

```
## /usr/lib/systemd/system/openvpn-server@.service  
# [Unit]  
# Description=OpenVPN service for %I  
# After=network-online.target  
# Wants=network-online.target  
# Documentation=man:openvpn(8)  
# Documentation=https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/  
# Documentation=https://community.openvpn.net/openvpn/wiki/HOWTO  
#  
# [Service]  
# Type=notify  
# PrivateTmp=true  
# WorkingDirectory=/etc/openvpn/Server  
# ExecStart=/usr/sbin/openvpn --status %t/openvpn-server/status-%i.log --status-version 2 --suppress-timestamps --config %i.conf  
# CapabilityBoundingSet=CAP_IPC_LOCK CAP_NET_ADMIN CAP_NET_BIND_SERVICE CAP_NET_RAW CAP_SETGID CAP_SETUID CAP_SETPCAP CAP_SYS_CHROOT CAP_DAC_OVERRIDE CAP_AUDIT_WRITE  
# LimitNPROC=10  
# DeviceAllow=/dev/null rw  
# DeviceAllow=/dev/net/tun rw  
# ProtectSystem=true  
# ProtectHome=true  
# KillMode=process  
# RestartSec=5s  
# Restart=on-failure  
#  
# [Install]  
# WantedBy=multi-user.target
```

Keterangan : setelah mengedit ini klik `ctrl + o` enter lalu `ctrl + x`.

```
root@annisa:/home/annisa#  
root@annisa:/home/annisa#  
root@annisa:/home/annisa# systemctl enable --now openvpn-server@server  
root@annisa:/home/annisa#
```

Keterangan :

- **enable:** Mengatur agar layanan OpenVPN otomatis menyala setiap kali komputer/server Anda dihidupkan (*booting*). Anda tidak perlu menyalakannya secara manual lagi di masa depan.
- **--now:** Langsung menyalakan layanan tersebut saat ini juga.