1. Pertama install package openvpn, “apt install openvpn -y”
2. Lalu ubah value ipv4_forward menjadi 1 “nano /etc/sysctl.conf”

```
  GNU nano 3.2                    /etc/sysctl.conf                    Modified

#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#

#kernel.domainname = example.com

# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3

###############################################################3
# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

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

# Uncomment the next line to enable packet forwarding for IPv6
#  Enabling this option disables Stateless Address Autoconfiguration
#  based on Router Advertisements for this host
```

3. Selanjutnya copy folder easy-rsa ke /etc/openvpn, “cp -r /usr/share/easy-rsa /etc/openvpn”

```
root@alphacntauri:~# cp -r /usr/share/easy-rsa /etc/open
opensc/  openvpn/
root@alphacntauri:~# cp -r /usr/share/easy-rsa /etc/open
opensc/  openvpn/
root@alphacntauri:~# cp -r /usr/share/easy-rsa /etc/openvpn/
root@alphacntauri:~# _
```

4. Move vars.example ke vars “mv vars.example vars” dan buka file varsnya dengan command “nano vars”

```
root@alphacntauri:~# cd /etc/openvpn/easy-rsa/
root@alphacntauri:/etc/openvpn/easy-rsa# mv vars.example vars
root@alphacntauri:/etc/openvpn/easy-rsa#
```

Gambar 4.1: Ubah nama file

```
  GNU nano 3.2                                   vars                                   Modified


# Default CN:
# This is best left alone. Interactively you will set this manually, and BATCH
# callers are expected to set this themselves.

#set_var EASYRSA_REQ_CN         "ChangeMe"

# Cryptographic digest to use.
# Do not change this default unless you understand the security implications.
# Valid choices include: md5, sha1, sha256, sha224, sha384, sha512

#set_var EASYRSA_DIGEST         "sha256"

# Batch mode. Leave this disabled unless you intend to call Easy-RSA explicitly
# in batch mode without any user input, confirmation on dangerous operations,
# or most output. Setting this to any non-blank string enables batch mode.

#set_var EASYRSA_BATCH          ""

export KEY_COUNTRY="JAPAN"
export KEY_PROVINCE="CA"
export KEY_CITY="Hiroshima"
export KEY_ORG="Ryan"
export KEY_EMAIL="admin@smk13400.co.id"
export KEY_OU="OpenVPN"
```

Gambar 4.2: Edit vars

5. Lalu initialize PKI dengan command “./easyrsa init-pki”

```
root@alphacntauri:/etc/openvpn/easy-rsa# ./easyrsa init-pki

Note: using Easy-RSA configuration from: ./vars

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

root@alphacntauri:/etc/openvpn/easy-rsa#
```

Gambar 5: Init PKI

6. Next build CA no password “./easyrsa build-ca nopass”

```
root@alphacntauri:/etc/openvpn/easy-rsa# ./easyrsa build-ca nopass

Note: using Easy-RSA configuration from: ./vars

Using SSL: openssl OpenSSL 1.1.1n  15 Mar 2022 (Library: OpenSSL 1.1.1d  10 Sep 2019)
Generating RSA private key, 2048 bit long modulus (2 primes)
......+++++
...............+++++
e is 65537 (0x010001)
Can't load /etc/openvpn/easy-rsa/pki/.rnd into RNG
139634316706944:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/ran
d/randfile.c:98:Filename=/etc/openvpn/easy-rsa/pki/.rnd
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:
/etc/openvpn/easy-rsa/pki/ca.crt

root@alphacntauri:/etc/openvpn/easy-rsa#
```

7. Generate server key no password “./easyrsa gen-req server nopass”

```
root@alphacntauri:/etc/openvpn/easy-rsa# ./easyrsa gen-req server nopass

Note: using Easy-RSA configuration from: ./vars

Using SSL: openssl OpenSSL 1.1.1n  15 Mar 2022 (Library: OpenSSL 1.1.1d  10 Sep 2019)
Generating a RSA private key
...........+++++
.....................................................+++++
writing new private key to '/etc/openvpn/easy-rsa/pki/private/server.key.WHUsbzehrE'
-----
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: /etc/openvpn/easy-rsa/pki/reqs/server.req
key: /etc/openvpn/easy-rsa/pki/private/server.key

root@alphacntauri:/etc/openvpn/easy-rsa# _
```

8. Setelah itu baru kita generate sign certificate “./easyrsa sign-req server server”

```
root@alphacntauri:/etc/openvpn/easy-rsa# ./easyrsa sign-req server server

Note: using Easy-RSA configuration from: ./vars

Using SSL: openssl OpenSSL 1.1.1n  15 Mar 2022 (Library: OpenSSL 1.1.1d  10 Sep 2019)


You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a server certificate for 1080 days:

subject=
    commonName                = server


Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes
Using configuration from /etc/openvpn/easy-rsa/pki/safessl-easyrsa.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'server'
Certificate is to be certified until Sep 26 15:09:38 2025 GMT (1080 days)

Write out database with 1 new entries
Data Base Updated

Certificate created at: /etc/openvpn/easy-rsa/pki/issued/server.crt

root@alphacntauri:/etc/openvpn/easy-rsa# _
```

9. Barulah build DH (Diffie-Hellman) key nya “./easyrsa gen-dh”

```
root@alphacntauri:/etc/openvpn/easy-rsa# ./easyrsa gen-dh

Note: using Easy-RSA configuration from: ./vars

Using SSL: openssl OpenSSL 1.1.1n  15 Mar 2022 (Library: OpenSSL 1.1.1d  10 Sep 2019)
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
..............................+.....................................................................
.........................................+.........................................+...............
....................................+.......................................+...+..............+.
.......................................................................................................
```

10. Lalu generate HMAC Keynya lewat command “openvpn –genkey –secret ryan.key” dan copy semua hasil generate ke “/etc/openvpn”

```
root@alphacntauri:/etc/openvpn/easy-rsa# openvpn --genkey --secret ryan.key
root@alphacntauri:/etc/openvpn/easy-rsa# cp ryan.key /etc/openvpn/
root@alphacntauri:/etc/openvpn/easy-rsa# cp pki/ca.crt /etc/openvpn/
root@alphacntauri:/etc/openvpn/easy-rsa# cp pki/private/server.key /etc/openvpn/
root@alphacntauri:/etc/openvpn/easy-rsa# cp pki/issued/server.crt /etc/openvpn/
root@alphacntauri:/etc/openvpn/easy-rsa# cp pki/dh.pem /etc/openvpn/
root@alphacntauri:/etc/openvpn/easy-rsa# _
```

11. Lalu buatlah untuk di sisi client “./easyrsa gen-req client nopass”

```
root@alphacntauri:/etc/openvpn/easy-rsa# ./easyrsa gen-req client nopass

Note: using Easy-RSA configuration from: ./vars

Using SSL: openssl OpenSSL 1.1.1n  15 Mar 2022 (Library: OpenSSL 1.1.1d  10 Sep 2019)
Generating a RSA private key
...................+++++
.................+++++
writing new private key to '/etc/openvpn/easy-rsa/pki/private/client.key.jXW0YhyDyt'
-----
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) [client]:

Keypair and certificate request completed. Your files are:
req: /etc/openvpn/easy-rsa/pki/reqs/client.req
key: /etc/openvpn/easy-rsa/pki/private/client.key

root@alphacntauri:/etc/openvpn/easy-rsa#
```

12. Setelah itu generate sign client dengan command “./easyrsa sign-req client client”

```
root@alphacntauri:/etc/openvpn/easy-rsa# ./easyrsa sign-req client client

Note: using Easy-RSA configuration from: ./vars

Using SSL: openssl OpenSSL 1.1.1n  15 Mar 2022 (Library: OpenSSL 1.1.1d  10 Sep 2019)


You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a client certificate for 1080 days:

subject=
    commonName                = client


Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes
Using configuration from /etc/openvpn/easy-rsa/pki/safessl-easyrsa.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'client'
Certificate is to be certified until Sep 26 15:18:05 2025 GMT (1080 days)

Write out database with 1 new entries
Data Base Updated

Certificate created at: /etc/openvpn/easy-rsa/pki/issued/client.crt

root@alphacntauri:/etc/openvpn/easy-rsa# _
```

13. Copy semua file generate client ke “/etc/openvpn/client”

```
root@alphacntauri:/etc/openvpn/easy-rsa# cp pki/ca.crt /etc/openvpn/client/
root@alphacntauri:/etc/openvpn/easy-rsa# cp pki/issued/client.crt /etc/openvpn/client/
root@alphacntauri:/etc/openvpn/easy-rsa# cp pki/private/client.key /etc/openvpn/client
root@alphacntauri:/etc/openvpn/easy-rsa# _
```

14. Next konfigurasi server.conf, “nano /etc/openvpn/server.conf”

```
  GNU nano 3.2                          server.conf                          Modified

port 1194
proto udp
dev tun
ca ca.crt
cert server.crt
key server.key
dh dh.pem
server 10.10.10.0 255.255.255.0
push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
keepalive 10 120
tls-auth ryan.key 0
cipher AES-256-CBC
user nobody
group nogroup
persist-key
persist-tun
status /var/log/openvpn/openvpn-status.log
log /var/log/openvpn/openvpn.log
log-append /var/log/openvpn/openvpn.log
verb 3
explicit-exit-notify 1
```

15. Habis itu kita start dan kita liat status dari openvpnnya “systemctl start openvpn@server && systemctl status openvpn@server”

```
root@alphacntauri:/etc/openvpn# systemctl start openvpn@server && systemctl status openvpn@server
● openvpn@server.service - OpenVPN connection to server
   Loaded: loaded (/lib/systemd/system/openvpn@.service; disabled; vendor preset: enabled)
   Active: active (running) since Wed 2022-10-12 11:25:38 EDT; 63ms ago
     Docs: man:openvpn(8)
           https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage
           https://community.openvpn.net/openvpn/wiki/HOWTO
 Main PID: 2105 (openvpn)
   Status: "Pre-connection initialization successful"
    Tasks: 1 (limit: 1120)
   Memory: 1.1M
   CGroup: /system.slice/system-openvpn.slice/openvpn@server.service
           └─2105 /usr/sbin/openvpn --daemon ovpn-server --status /run/openvpn/server.status 10 --co

Oct 12 11:25:38 alphacntauri systemd[1]: Starting OpenVPN connection to server...
Oct 12 11:25:38 alphacntauri systemd[1]: Started OpenVPN connection to server.
lines 1-15/15 (END)
```

16. Lalu kita konfigurasi bagian client, pertama jangan lupa installasi terlebih dahulu dengan command “apt install openvpn -y”
17. Selanjutnya kita import cert nya ke clientnya dengan menggunaakn command “scp root@(ip_server):/etc/openvpn/client/* /etc/openvpn/”

```
root@chentaury:~# scp root@192.168.50.79:/etc/openvpn/client/* /etc/openvpn/
The authenticity of host '192.168.50.79 (192.168.50.79)' can't be established.
ECDSA key fingerprint is SHA256:fGCjhabF5m5hMLBOz4TcyWd9FvhepRoxrZNE77gGWyc.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.50.79' (ECDSA) to the list of known hosts.
root@192.168.50.79's password:
ca.crt                                                    100% 1184     1.3MB/s   00:00
client.crt                                                100% 4470     5.3MB/s   00:00
client.key                                                100% 1704     2.8MB/s   00:00
root@chentaury:~#
```

Gambar 17.1: Copy Cert

```
root@chentaury:/etc/openvpn# scp root@192.168.50.79:/etc/openvpn/ryan.key /etc/openvpn/
root@192.168.50.79's password:
ryan.key                                                  100%  636   382.5KB/s   00:00
root@chentaury:/etc/openvpn#
```

Gambar 17.2: Copy HMAC Key

18. Lalu konfigurasi client.conf dengan command “nano /etc/openvpn/client.conf”

```
  GNU nano 3.2                          client.conf                          Modified

client
dev tun
proto udp
remote 192.168.50.79 1194
resolv-retry infinite
nobind
user nobody
group nogroup
persist-key
persist-tun
ca ca.crt
cert client.crt
key client.key
remote-cert-tls server
tls-auth ryan.key 1_
cipher AES-256-CBC
verb 3
```

19. Lalu kita start openvpnnya dan lihat statusnya dengan command “systemctl start openvpn@client && systemctl status openvpn@client”

```
File Server   Web Server
root@chentaury:/etc/openvpn# systemctl start openvpn@client && systemctl status openvpn@client
● openvpn@client.service - OpenVPN connection to client
   Loaded: loaded (/lib/systemd/system/openvpn@.service; disabled; vendor preset: enabled)
   Active: active (running) since Wed 2022-10-12 11:39:06 EDT; 466ms ago
     Docs: man:openvpn(8)
           https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage
           https://community.openvpn.net/openvpn/wiki/HOWTO
 Main PID: 1825 (openvpn)
   Status: "Pre-connection initialization successful"
    Tasks: 1 (limit: 501)
   Memory: 1.1M
   CGroup: /system.slice/system-openvpn.slice/openvpn@client.service
           └─1825 /usr/sbin/openvpn --daemon ovpn-client --status /run/openvpn/client.status 10 --cd
```

20. Dan hasilnya seperti ini

```
root@alphacntauri:/etc/openvpn# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 10
00
    link/ether 00:0c:29:9a:9a:fc brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.79/25 brd 192.168.50.127 scope global dynamic ens33
       valid_lft 422sec preferred_lft 422sec
    inet6 fe80::20c:29ff:fe9a:9afc/64 scope link
       valid_lft forever preferred_lft forever
144: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group d
efault qlen 100
    link/none
    inet 10.10.10.1 peer 10.10.10.2/32 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::e6bc:5e27:5927:9bd1/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
root@alphacntauri:/etc/openvpn# _
```

Gambar 20.1: Server

```
root@chentaury:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 10
00
    link/ether 00:0c:29:24:7f:b7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.4/25 brd 192.168.50.127 scope global dynamic ens33
       valid_lft 574sec preferred_lft 574sec
    inet6 fe80::20c:29ff:fe24:7fb7/64 scope link
       valid_lft forever preferred_lft forever
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group def
ault qlen 100
    link/none
    inet 10.10.10.6 peer 10.10.10.5/32 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::9fec:50cd:2411:c04a/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
4: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:98:23:2e:bf brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
root@chentaury:~#
```

Gambar 20.2: Client