Install OpenVPN Server on Debian

Before starting, it is a good idea to update your system’s packages to the latest version.

Run the following command to update and upgrade your system’s packages:

apt-get update -y

apt-get upgrade -y

Once your system is up-to-date, you can proceed to the next step.

**Step 1 – Enable IP Forwarding**

Next, you will need to enable IP forwarding in your system. IP forwarding allows your operating system to accept the incoming network packets and forward it to the other network if the destination is on another network.

To enable the IP forwarding, edit the file /etc/sysctl.conf:

nano /etc/sysctl.conf

Add the following line:

net.ipv4.ip\_forward = 1

Save the file when you are finished. Then, run the following command to apply the changes:

sysctl -p

**Step 2 – Install OpenVPN Server**

By default, the OpenVPN package is available in the Debian 10 default repository. You can install it with the following command:

apt-get install openvpn -y

Once the installation has been completed, you will also need to copy the easy-rsa directory for managing SSL certificates.

Run the following command to copy easy-rsa directory from /usr/share directory to /etc/openvpn directory.

cp -r /usr/share/easy-rsa /etc/openvpn/

**Step 3 – Setup Certificate Authority**

Easy RSA uses a set of scripts to generate keys and certificates. First, you will need to configure the Certificate Authority on your system.

To do so, change the directory to /etc/openvpn/easy-rsa and create a new Easy RSA’s configuration file:

cd /etc/openvpn/easy-rsa

nano vars

Add the following lines including your country, city, and preferred email address:

set\_var EASYRSA "$PWD"

set\_var EASYRSA\_PKI "$EASYRSA/pki"

set\_var EASYRSA\_DN "cn\_only"

set\_var EASYRSA\_REQ\_COUNTRY "INDIA"

set\_var EASYRSA\_REQ\_PROVINCE "Gujrat"

set\_var EASYRSA\_REQ\_CITY "Ahmedabad"

set\_var EASYRSA\_REQ\_ORG "Tecadmin CERTIFICATE AUTHORITY"

set\_var EASYRSA\_REQ\_EMAIL "admin@tecadmin.net"

set\_var EASYRSA\_REQ\_OU "Tecadmin EASY CA"

set\_var EASYRSA\_KEY\_SIZE 2048

set\_var EASYRSA\_ALGO rsa

set\_var EASYRSA\_CA\_EXPIRE 7500

set\_var EASYRSA\_CERT\_EXPIRE 365

set\_var EASYRSA\_NS\_SUPPORT "no"

set\_var EASYRSA\_NS\_COMMENT "Tecadmin CERTIFICATE AUTHORITY"

set\_var EASYRSA\_EXT\_DIR "$EASYRSA/x509-types"

set\_var EASYRSA\_SSL\_CONF "$EASYRSA/openssl-easyrsa.cnf"

set\_var EASYRSA\_DIGEST "sha256"

Save the file when you are finished.

Next, run the following command to initiate the PKI directory.

./easyrsa init-pki

Output:

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

Next, build the CA certificates with the following command:

./easyrsa build-ca

You should get the following output:

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

Using SSL: openssl OpenSSL 1.1.1c FIPS 28 May 2019

Enter New CA Key Passphrase:

Re-Enter New CA Key Passphrase:

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

140218549745472:error:2406F079:random number generator:RAND\_load\_file:Cannot open file:crypto/rand/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]:

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

The above command will generate two files named ca.key and ca.crt. These certificates will be used to sign your server and clients’ certificates.

**Step 4 – Generate Server Certificate Files**

Next, you will need to generate a keypair and certificate request for your server.

Run the following command to generate the server key named tecadmin-server:

./easyrsa gen-req tecadmin-server nopass

You should get the following output:

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

Using SSL: openssl OpenSSL 1.1.1c FIPS 28 May 2019

Generating a RSA private key

...........................+++++

...............................................................................................................................................................................................................................................................................................+++++

writing new private key to '/etc/openvpn/easy-rsa/pki/private/tecadmin-server.key.kOlBTwtY6a'

-----

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) [tecadmin-server]:

Keypair and certificate request completed. Your files are:

req: /etc/openvpn/easy-rsa/pki/reqs/tecadmin-server.req

key: /etc/openvpn/easy-rsa/pki/private/tecadmin-server.key

**Step 5 – Sign the Server Key Using CA**

Next, you will need to sign the tecadmin-server key using your CA certificate:

Run the following command to sign the server key:

./easyrsa sign-req server tecadmin-server

You should get the following output:

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

Using SSL: openssl OpenSSL 1.1.1c FIPS 28 May 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 365 days:

subject=

commonName = tecadmin-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

Enter pass phrase for /etc/openvpn/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:'tecadmin-server'

Certificate is to be certified until Feb 16 05:00:50 2021 GMT (365 days)

Write out database with 1 new entries

Data Base Updated

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

Next, verify the generated certificate file with the following command:

openssl verify -CAfile pki/ca.crt pki/issued/tecadmin-server.crt

If everything is fine, you should get the following output:

pki/issued/tecadmin-server.crt: OK

Next, run the following command to generate a strong Diffie-Hellman key to use for the key exchange:

./easyrsa gen-dh

You should get the following output:

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

Using SSL: openssl OpenSSL 1.1.1c FIPS 28 May 2019

Generating DH parameters, 2048 bit long safe prime, generator 2

This is going to take a long time

....+................................+........................................+.....++\*++\*++\*++\*

DH parameters of size 2048 created at /etc/openvpn/easy-rsa/pki/dh.pem

After creating all certificate files, copy them to the /etc/openvpn/server/ directory:

cp pki/ca.crt /etc/openvpn/server/

cp pki/dh.pem /etc/openvpn/server/

cp pki/private/tecadmin-server.key /etc/openvpn/server/

cp pki/issued/tecadmin-server.crt /etc/openvpn/server/

**Step 6 – Generate Client Certificate and Key File**

Next, you will need to generate the key and certificate file for the client.

First, run the following command to build the client key file:

./easyrsa gen-req client nopass

You should see the following output:

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

Using SSL: openssl OpenSSL 1.1.1c FIPS 28 May 2019

Generating a RSA private key

......................................................+++++

...+++++

writing new private key to '/etc/openvpn/easy-rsa/pki/private/client.key.e38GUtzHie'

-----

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

Next, sign the client key using your CA certificate:

./easyrsa sign-req client client

You should get the following output:

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

Using SSL: openssl OpenSSL 1.1.1c FIPS 28 May 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 365 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

Enter pass phrase for /etc/openvpn/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:'client'

Certificate is to be certified until Feb 16 05:11:19 2021 GMT (365 days)

Write out database with 1 new entries

Data Base Updated

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

Next, copy all client certificate and key file to the /etc/openvpn/client/ directory:

cp pki/ca.crt /etc/openvpn/client/

cp pki/issued/client.crt /etc/openvpn/client/

cp pki/private/client.key /etc/openvpn/client/

**Step 7 – Configure OpenVPN Server**

Next, create a new OpenVPN configuration file inside /etc/openvpn/ directory:

nano /etc/openvpn/server.conf

Add the following lines:

port 1194

proto udp

dev tun

ca /etc/openvpn/server/ca.crt

cert /etc/openvpn/server/tecadmin-server.crt

key /etc/openvpn/server/tecadmin-server.key

dh /etc/openvpn/server/dh.pem

server 10.8.0.0 255.255.255.0

push "redirect-gateway def1"

push "dhcp-option DNS 208.67.222.222"

push "dhcp-option DNS 208.67.220.220"

duplicate-cn

cipher AES-256-CBC

tls-version-min 1.2

tls-cipher TLS-DHE-RSA-WITH-AES-256-GCM-SHA384:TLS-DHE-RSA-WITH-AES-256-CBC-SHA256:TLS-DHE-RSA-WITH-AES-128-GCM-SHA256:TLS-DHE-RSA-WITH-AES-128-CBC-SHA256

auth SHA512

auth-nocache

keepalive 20 60

persist-key

persist-tun

compress lz4

daemon

user nobody

group nogroup

log-append /var/log/openvpn.log

verb 3

Save the file when you are finished.

**Step 8 – Start OpenVPN Service**

OpenVPN is now installed and configured. You can now start the OpenVPN service and enable it to start after the system reboot using the following command:

systemctl start openvpn@server

systemctl enable openvpn@server

Run the following command to verify the status of OpenVPN service:

systemctl status openvpn@server

You should get the following output:

● openvpn@server.service - OpenVPN connection to server

Loaded: loaded (/lib/systemd/system/openvpn@.service; enabled; vendor preset: enabled)

Active: active (running) since Fri 2020-02-21 15:38:31 UTC; 4s ago

Docs: man:openvpn(8)

https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage

https://community.openvpn.net/openvpn/wiki/HOWTO

Main PID: 3044 (openvpn)

Status: "Initialization Sequence Completed"

Tasks: 1 (limit: 2359)

Memory: 1.3M

CGroup: /system.slice/system-openvpn.slice/openvpn@server.service

└─3044 /usr/sbin/openvpn --daemon ovpn-server --status /run/openvpn/server.status 10 --cd /etc/openvpn --config /etc/openvpn/server.

Feb 21 15:38:31 debian10 systemd[1]: Starting OpenVPN connection to server...

Feb 21 15:38:31 debian10 systemd[1]: Started OpenVPN connection to server.

Once the OpenVPN service started successfully, it will create a new network interface named tun0. You can check it with the following command:

ip a show tun0

You should get the new interface tun0 in the following output:

59: tun0: mtu 1500 qdisc pfifo\_fast state UNKNOWN group default qlen 100

link/none

inet 10.8.0.1 peer 10.8.0.2/32 scope global tun0

valid\_lft forever preferred\_lft forever

inet6 fe80::90:e3c0:5f1a:27f5/64 scope link stable-privacy

valid\_lft forever preferred\_lft forever

**Step 9 – Generate Client Configuration**

Next, create a new OpenVPN client configuration file named client.ovpn. You will require this file to connect your OpenVPN server from the client system.

nano /etc/openvpn/client/client.ovpn

Add the following lines:

client

dev tun

proto udp

remote vpn-server-ip 1194

ca ca.crt

cert client.crt

key client.key

cipher AES-256-CBC

auth SHA512

auth-nocache

tls-version-min 1.2

tls-cipher TLS-DHE-RSA-WITH-AES-256-GCM-SHA384:TLS-DHE-RSA-WITH-AES-256-CBC-SHA256:TLS-DHE-RSA-WITH-AES-128-GCM-SHA256:TLS-DHE-RSA-WITH-AES-128-CBC-SHA256

resolv-retry infinite

compress lz4

nobind

persist-key

persist-tun

mute-replay-warnings

verb 3

Save the file when you are finished.

**Step 10 – Configure Routing using UFW**

By default, the UFW firewall is not installed in Debian 10. You can install it with the following command:

apt-get install ufw -y

After installing the UFW firewall, you will need to add firewall rules to enable masquerading so that your VPN clients access to the Internet.

First, you will need to configure UFW to accept the forwarded packets. You can do it by editing the file /etc/default/ufw:

nano /etc/default/ufw

Change the following line:

DEFAULT\_FORWARD\_POLICY="ACCEPT"

Save and close the file. Then, open the /etc/ufw/before.rules file:

nano /etc/ufw/before.rules

Add the following lines at the end of the file:

\*nat

:POSTROUTING ACCEPT [0:0]

-A POSTROUTING -s 10.8.0.0/16 -o ens3 -j MASQUERADE

COMMIT

Save the file when you are finished.

Note: Replace ens3 with the name of your public network interface.

Next, allow the default OpenVPN port 1194 and OpenSSH with the following command:

ufw allow 1194/udp

ufw allow OpenSSH

Next, reload the UFW firewall using the following command:

ufw disable

ufw enable