2025/09/26 07:09 1/3 OpenVPN

OpenVPN

Follow one of the excellent guides from DigitalOcean (see Links below). Follow all the steps to the detail and everything will work, below are modifications I made for my personal requirements. Make sure you run commands as regular user and only elevate to root when told to do so.

Prerequisites

- 1. Make sure you followed Initial Server Setup with Debian 9 before you setup the VPN Server
- 2. Establish a non-root administrative user with sudo privileges
- 3. Install UFW Firewall and make sure the correct interface is set up in /etc/ufw/before.rules
- 4. I separated the Certificate Authority Server (*CA Server*) and the *VPN Server* as recommended in the walk-through. I use 2 different *VPN Servers* in 2 locations with the same credentials, the *CA Server* is located on a virtual machine and switched off when not used. (bco: OpenVPN)
- 5. Install EasyRSA

Migrating server

If you resinstall OpenVPN on a new machine with existing client configurations do the following:

- 1. Copy /etc/openvpn/ from the old server and copy to the new server
- 2. Follow Adjusting the Server Networking Configuration (steps 5 and 6)
- 3. Check the VPN is running with

sudo systemctl status openvpn@server

Adding Clients

Setting up the environment (*VPN Server(s)* and *CA Server*) takes a while, the many steps are outlined clearly and in detail in the Original Article below in my Wiki or on the DigitalOcean website. In this paragraph I summarized the steps necessary to add clients to the VPN. Since both *VPN Servers* use the same credentials, the process is identical apart from using a different *base.conf* file which contains the server's IP address.

VPN Server

• Navigate to the EasyRSA directory on your *VPN Server* and run the easyrsa script with the genreq and nopass options, along with the common name for the client:

```
$ cd ~/EasyRSA-3.0.4/
$ ./easyrsa gen-req client1 nopass
```

• Press ENTER to confirm the common name. Then, copy the client1.key file to ~/client-

2025/09/26 07:09 2/3 OpenVPN

configs/keys/:

\$ cp ~/EasyRSA-3.0.4/pki/private/client1.key ~/client-configs/keys/

CA Server

• Log in to your *CA Server* and copy the client1.req file from the *VPN Server*:

```
$ rsync -avz -e "ssh -p <port>"
user@vpn.server.com:EasyRSA-3.0.4/pki/reqs/client1.req
~/EasyRSA-3.0.4/pki/reqs/.
```

 Navigate to the EasyRSA directory and sign the request, be sure to specify the client request type:

```
$ ./easyrsa sign-req client client1
```

At the prompt, enter **yes** to confirm that you intend to sign the certificate request and that it came from a trusted source. This will create a client certificate file named client1.crt.

Copy the signed client1.crt file back to the VPN Server:

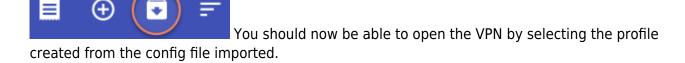
```
$ rsync -avz -e "ssh -p <port>" ~/EasyRSA-3.0.4/pki/issued/client1.crt
user@vpn.server.com:client-configs/keys/
```

VPN Server

• Log in to your *VPN Server* then navigate to ~/client-configs and run the 'make config' script:

```
$ cd ~/client-configs
$ sudo ./make_config.sh client1
```

- This will create a file named *client1.ovpn* in your ~/client-configs/files directory. Transfer this file to the device you plan to use as the client.
- Install the *OpenVPN Client* for Windows, Android, or other platforms.
- On Android, open the app and select the import icon top right to import the config file.



Links

- How To Set Up an OpenVPN Server on Debian 11
- How To Set Up an OpenVPN Server on Debian 10
- How To Set Up an OpenVPN Server on Debian 9

2025/09/26 07:09 3/3 OpenVPN

- Easy-RSA 3
- Github Easy-RSA
- OpenVPN HowTo

• Problem connecting to local resources from a laptop

From:

https://wiki.condrau.com/ - Bernard's Wiki

Permanent link:

https://wiki.condrau.com/deb9:openvpn

Last update: 2025/09/22 15:08

