```
$ sudo apt-get update
$ sudo apt-get install openvpn easy-rsa
```

The needed software is now on the server, ready to be configured.

Step 2: Set Up the CA Directory

OpenVPN is an TLS/SSL VPN. This means that it utilizes certificates in order to encrypt traffic between the server and clients. In order to issue trusted certificates, we will need to set up our own simple certificate authority (CA).

To begin, we can copy the `easy-rsa` template directory into our home directory with the `make-cadir` command:

```
$ make-cadir ~/openvpn-ca
```

Move into the newly created directory to begin configuring the CA:

```
$ cd ~/openvpn-ca
```

Step 3: Configure the CA Variables

To configure the values our CA will use, we need to edit the `vars` file within the directory. Open that file now in your text editor:

```
$ nano vars
```

Inside, you will find some variables that can be adjusted to determine how your certificates will be created. We only need to worry about a few of these.

Towards the bottom of the file, find the settings that set field defaults for new certificates. It should look something like this:

~/openvpn-ca/vars

```
. . .

export KEY_COUNTRY="US"
export KEY_PROVINCE="CA"
export KEY_CITY="SanFrancisco"
export KEY_ORG="Fort-Funston"
export KEY_EMAIL="me@myhost.mydomain"
export KEY_OU="MyOrganizationalUnit"

. . .
```

Edit the values in red to whatever you'd prefer, but do not leave them blank:

~/openvpn-ca/vars

```
. . .

export KEY_COUNTRY="US"
export KEY_PROVINCE="NY"
export KEY_CITY="New York City"
export KEY_ORG="DigitalOcean"
export KEY_EMAIL="admin@example.com"
export KEY_OU="Community"

. . .
```

While we are here, we will also edit the `KEY_NAME` value just below this section, which populates the subject field. To keep this simple, we'll call it `server` in this guide:

~/openvpn-ca/vars

```
export KEY_NAME="server"
```