

Forum:[Hack Forums](#)

Thread: [Raspberry Pi as OpenVPN Server](#)

Proxies.tv - November 7, 2020, 6:00 pm

Shell script to set up Raspberry Pi as a VPN server using the free, open-source OpenVPN software. Includes templates of the necessary configuration files for easy editing prior to installation, as well as a script for easily generating client .ovpn profiles after setting up the server.

The master branch of this script installs and configures OpenVPN on Raspbian Jessie, and should be used if you are running Jessie or Jessie Lite. If you would like to set up OpenVPN on Raspbian Wheezy, use the Wheezy branch.

Prerequisites:

To follow this guide and use the script to setup OpenVPN, you will need to have a Raspberry Pi Model B or later with an ethernet port, an SD or microSD card (depending on the model) with Raspbian installed, a power adapter appropriate to the power needs of your model, and an ethernet cable to connect your Pi to your router or gateway. It is recommended that you use a fresh image of Raspbian Jessie Lite or Wheezy from <https://raspberrypi.org/downloads>, but if you don't, be sure to make a backup image of your existing installation before proceeding. You will also need to setup your Pi with a static IP address (see either source 1 or 2 at the bottom of this Readme) and have your router forward port 1194 (varies by model & manufacturer; consult your router manufacturer's documentation to do this). You should also find your Pi's local IP address on your network and the public IP address of your network and write them down before beginning. Enabling SSH on your Pi is also highly recommended, so that you can run a very compact headless server without a monitor or keyboard and be able to access it even more conveniently (This is also covered by source 2) . And last but not least, you will need to be logged in under the default user pi, so be sure to change pi's user password from the default.

Server-Side Setup

You can download the OpenVPN setup script directly through the terminal or SSH using Git. If you don't already have it, update your APT repositories and install it:

```
Code sudo apt-get update
```

```
sudo apt-get upgrade
```

```
sudo apt-get install git
```

Then download the latest setup script via the command line with:

```
Code git clone git://github.com/StarshipEngineer/OpenVPN-Setup
```

Execute the script with:

```
Code cd OpenVPN-Setup
```

```
sudo chmod +x openvpnsetup.sh
```

```
sudo ./openvpnsetup.sh
```

The script will show you a menu of options. If this is your first time running the script, choose option 01, which will install OpenVPN and configure your system. If you prefer bypassing the menu and executing scripts directly from the command line, you can instead install simply by making the script install.sh executable and running it with sudo.

The script will first update your APT repositories, upgrade packages, and install OpenVPN, which will take some time. It will then ask you to input your Raspberry Pi's local IP address on your network and the public IP address of your network, and then to choose which encryption method you wish the guts of your server to use, 1024-bit or 2048-bit. 2048-bit is more secure, but will take much longer to set up. If you're unsure or don't have a convincing reason for 2048, just choose 1024.

After this, the script will go back to the command line as it builds the server's own certificate authority. If you wish to enter identifying information for the CA, replace the default values in the file `ca_info.txt` (CO for country, ST for state/province/territory, ORG for organization, etc.) before executing the setup script; however, this is not required, and you may leave the `ca_info.txt` file as-is. After this, the script will prompt you in the command line for input in similar identifying information fields as it generates your server certificate. Enter whatever you like, or if you do not desire to fill them out, skip them by pressing enter; make sure to skip the challenge field and leave it blank. After these fields, you will be asked whether you want to sign the certificate; you must press 'y'. You'll also be asked if you want to commit - press 'y' again.

Finally, the script will take some time to build the server's Diffie-Hellman key exchange. If you chose 1024-bit encryption, this will just take a few minutes, but if you chose 2048-bit, it will take much longer (anywhere from 40 minutes to several hours on a Model B+). The script will also make some changes to your system to allow it to forward internet traffic and allow VPN connections through the Pi's firewall. When the script informs you that it has finished configuring OpenVPN, reboot the system to apply the changes, and the VPN server-side setup will be complete!

Making Client Profiles:

After the server-side setup is finished and the machine rebooted, you may use the MakeOVPN script to generate the `.ovpn` profiles you will import on each of your client machines. To generate your first client profile, execute the `openvpnsetup` script once again and choose option 02 in the menu, or else make sure the script `MakeOVPN.sh` is executable and run it.

You will be prompted to enter a name for your client. Pick anything you like and hit 'enter'. You will be asked to enter a pass phrase for the client key; make sure it's one you'll remember. You'll then be prompted for input in more identification fields, which you can again ignore if you like; make sure you again leave the challenge field blank. The script will then ask if you want to sign the client certificate and commit; press 'y' for both. You'll then be asked to enter the pass phrase you just chose in order to encrypt the client key, and immediately after to choose another pass phrase for the encrypted key - if you're normal, just use the same one. After this, the script will assemble the client `.ovpn` file and place it in the directory 'ovpns' within your home directory.

To generate additional client `.ovpn` profiles at any time for other devices you'd like to connect to the VPN, `cd` into OpenVPN-Setup and execute the setup script, choose menu option 02, and repeat the above steps for each client.

Importing `.ovpn` Profiles on Client Machines

To move a client `.ovpn` profile to Windows, use a program like WinSCP or Cyberduck. Note that you may need administrator permission to move files to some folders on your Windows machine, so if you have trouble transferring the profile to a particular folder with your chosen file transfer program, try moving it to your desktop. To move a profile to Android, you can either retrieve it on PC and then move it to your device via USB, or you can use an app like Turbo FTP & SFTP client to retrieve it directly from your Android device.

To import the profile to OpenVPN on Windows, download the OpenVPN GUI from the community

downloads section of openvpn.net, install it, and place the profile in the 'config' folder of your OpenVPN directory, i.e., in 'C:\Program Files\OpenVPN\config'. To import the profile on Android, install the OpenVPN Connect app, select 'Import' from the drop-down menu in the upper right corner of the main screen, choose the directory on your device where you stored the .ovpn file, and select the file.

After importing, connect to the VPN server on Windows by running the OpenVPN GUI with administrator permissions, right-clicking on the icon in the system tray, and clicking 'Connect', or on Android by selecting the profile under 'OpenVPN Profile' and pressing 'Connect'. You'll be asked to enter the pass phrase you chose. Do so, and you're in! Enjoy your ~\$50 USD private VPN.

Removing OpenVPN:

If at any point you wish to remove OpenVPN from your Pi and revert it to a pre-installation state, such as if you want to undo a failed installation to try again or you want to remove OpenVPN without installing a fresh Raspbian image, just cd into OpenVPN-Setup, execute the setup script, and choose option 03, or make sure remove.sh is executable and run it with sudo.