OpenVPN client on Linux

Contents

Introduction

OpenVPN is an open-source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities.

This article provides a guide on how to configure an OpenVPN Tunnel connection between an OpenVPN client on a Linux PC/Laptop and any OpenVPN server using TLS certificates as the authentication method. The examples in this article are created from a **Ubuntu 16.04** distribution perspective, although they should apply to most newer **Debian** and even some other distributions as well. For a Windows guide, click **here**.

Configuration overview and prerequisites

Before we begin, let's overview the configuration that we are attempting to achieve and the prerequisites that make it possible.

Prerequisites:

- A PC or Laptop running on Debian Linux
- An active Internet connection

Configuration scheme:

The scheme itself is very simple - an OpenVPN client connects to an OpenVPN server. The client is configured on a PC or Laptop using a Debian Linux distribution OS, while the server is undefined in this example, i.e., we will be focusing mainly on the client configuration method, since the server could belong to any OpenVPN service provider.

Installation and configuration

If you have familiarized yourself with the configuration scheme and have everything in order, we can start configuring the OpenVPN client using instructions provided in this section.

- Install OpenVPN service on your computer. To do so, open up a Terminal and execute the following commands:

```
sudo apt-get update
sudo apt-get install openvpn
```

- Create or obtain an OpenVPN client configuration file. If you are using a third party OpenVPN server, the client configuration file and TLS certificates should be provided by that party. If that is the case, we suggest you skip this part and move on to the next step of the guide.
  If you're using your own server and need to create a configuration file, you can either find one online or just download our configuration file from **here** and use it as a template. If you don't have TLS certificates, you can
  Open the configuration file with any text editor. Enter the OpenVPN options relevant to your configuration. Then copy the contents of the certificates into that file. Below is an example of what the file looks like:

- Copy the configuration file to **/etc/openvpn/** and rename if to **client.conf**. To do so, simply open up a Terminal in the location where your configuration file is present and execute this command:

```
cp example.ovpn /etc/openvpn/client.conf
```

- Enable the autostart of the OpenVPN service:

```
sudo systemctl enable openvpn@client.service
```

- Start the client:

```
sudo service openvpn@client start
```

- At this point all you need to do is wait a few seconds for the connection to complete. To check the status of the connection, use this command:

```
sudo service openvpn@client status
```

- An OpenVPN interface should also appear. To check it, execute this command:

```
ifconfig
```

The entry for the interface should look something like this:

```
tun_c_ovpn   Link encap:UNSPEC  HWaddr
00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
             inet addr:10.0.0.6  P-t-P:10.0.0.5  Mask:255.255.255.255
             inet6 addr: fe80::df8c:ec55:e5b8:ab27/64 Scope:Link
             UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
             RX packets:0 errors:0 dropped:0 overruns:0 frame:0
             TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:100
             RX bytes:0 (0.0 B)  TX bytes:288 (288.0 B)
```

- Additional testing for the connection may be required depending on the server's configuration and the overall intent of your OpenVPN connection. For instance, if you were supposed get access to server's private network or other clients' private networks, you can open a Terminal and try pinging private IP addresses of the devices in the networks in question. Or if the server was intended to be used as a proxy, your computer's Public IP address should be the same as the server's. To check your public IP address, visit **this website**.

Different configurations

The configuration we discussed in earlier sections is very basic. Some options used in client configurations depend on the server's configuration, some are only specific to the client. If you're using a third party OpenVPN service, the configuration files (and necessary certificates) are almost always provided by that party, so if that is the case we suggest simply using their configuration file.

If you are configuring the server yourself you will also need to create the client config file yourself. You can use the one provided in this guide as a base, but keep in mind that you'll have set the options specific to your own configuration yourself. OpenVPNs supports a lot of different options and can be customized almost endlessly. A complete list of OpenVPN options can be found in the **OpenVPN manual** (external link).

See also

- Other OpenVPN related articles from our wiki:
  - OpenVPN Manual section - OpenVPN section of the router's manual
  - OpenVPN configuration examples - basic OpenVPN configuration scenarios with detailed examples
  - OpenVPN traffic split - a detailed example on how to configure different default gateways for devices in the router's LAN
- OpenVPN client on Windows

External links

- http://www.whatsmyip.org/ - a website where you can check your Public IP address
- https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage - OpenVPN manual