# How to configure a SSTP VPN in Debian/Ubuntu

## Install the CA certificate

You have to install the certificate of the Certification Authority to authenticate your host in the VPN server. To achieve this goal execute the following lines in your terminal:

```
sudo cp your_certificate.crt /usr/local/share/ca-certificates/your_certificate.pem
sudo update-ca-certificates
```

## Installation of the sstp-client

Add the following PPA (Personal Package Archive) for Debian/Ubuntu (install the add-apt-repository application if you don't have it with `sudo apt-get install software-properties-common`)

```
sudo add-apt-repository ppa:eivnaes/network-manager-sstp
```

and install the SSTP client

```
sudo apt-get install sstp-client
```

OPTIONAL: if your use the Network Manager utility you can also install the plugin for SSTP VPN as

```
sudo apt-get install network-manager-sstp
```

OPTIONAL2: if you use GNOME or Unity too, you can install the themed version of the plugin

```
sudo apt-get install network-manager-sstp-gnome
```

## Setting your credentials

There are two ways to perform this step. You can follow the terminal native Linux path (recommended) or use the Network Manager plugin. In the second way you only have to fill in the form with the corresponding configuration passed by your network admin. So we will cover the first way here, witch is indeed more funny.

Edit the `/etc/ppp/chap-secrets` file and append the username and password you need to authenticate behind the VPN server

```
echo "your_username connection 'your_password' *" | sudo tee -a /etc/ppp/chap-secrets
```

## Connection

You should write something like this to configure a new VPN connection in a new file named `/etc/ppp/peers/connection`:

```
remotename      connection
linkname        connection
ipparam         connection
pty             "sstpc --ipparam connection --nolaunchpppd your.vpn.server"
name            username
plugin          sstp-pppd-plugin.so
sstp-sock       /var/run/sstpc/sstpc-connection
usepeerdns
refuse-eap
noauth
defaultroute
debug
file /etc/ppp/options.pptp
```

Play with these parameters to your taste according to the configuration provided by your network administrator. Do not forget to change the DNS of the VPN server at the end of the pty entry.

## Network route

It is possible that your host does not link the network packages sent from your local network, attached to the eth0 device, to the VPN network, which is attached to the ppp0 device. In that case, you must create a route between them using the route command:

```
sudo route add -net 172.16.2.0/24 dev ppp0
```

However, this is a temporary fix. If you want to make the change permanent (once you have checked it works) you are going to create a file `/etc/ppp/ip-up.d/0route` with this content

```
#!/bin/bash
NET=`echo $4 | cut -d . -f 1,2,3`
route add -net $NET.0/24 dev $1
```

## Connect

Every time you want to connect to your new VPN just use the following command

```
sudo pon connection
```

## Testing

Check that your connection is working by pinging a host IP inside the VPN, like 172.16.2.11

```
ping 172.16.2.11
```

In order to get the IP of your host inside the VPN (assigned with DHCP) you can use

```
ip addr show | grep ppp0
```

If something goes wrong check at the system log for errors thrown by the pppd daemon

```
sudo tail -f /var/log/syslog | grep pppd
```

## Fallback

If everyone else fails, then try this command to create a new temporary connection

```
sudo sstpc --save-server-route --user your_username --password your_password
your.vpn.server noauth
```