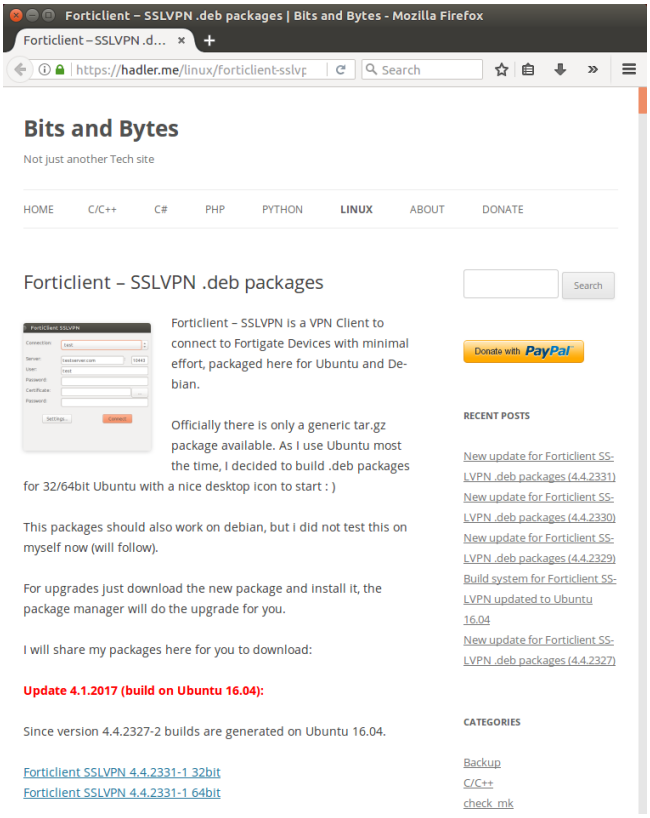
Linux: How to access Plymouth University VPN

These instructions have been tested on Ubuntu 16.10 and Kubuntu 16.10. They use the proprietary Bits and Bytes client but there are open-source alternatives (see at the end of this article).



Step 1: Obtain a FortiNet client

Download the client from Bits and Bytes:

<https://hadler.me/linux/forticlient-sslvpn-deb-packages/>

For most PU desktops and laptops you will need the 64-bit version:

<forticlient-sslvpn_4.4.2331-1_amd64.deb>

This was built for Ubuntu 16.04 but it also works on Ubuntu 16.10 (and is the kind of package that is unlikely to date much unless FortiNet do something unexpected).

Save the file somewhere on you computer. I saved it in /home/rod/Software so use that example to show the next steps.

Step 2: Install the client

If you use Nautilus or Dolphin as file manager, open it and go to the directory (folder) where you saved that file. Right click and select ‘Open with → Qapt Package Installer’ (or Synaptic, or Software Install, or whatever package manager you prefer). Follow the instructions to install in the usual way. You will of course need to give your password.

Alternatively you can do the same using a terminal (Konsole or similar) . First, go to the directory where you stored the file. Using the above example, type:

cd /home/rod/Software

(*Obviously* you will need to adjust the bit after '/home/...' to suit you own case.) To install the software type:

sudo apt install forticlient-sslvpn_4.4.2331-1_amd64.deb

If you downloaded a different file (e.g. because you wanted a 32-bit client) you will have to adjust the file-name to match. As usual you will be asked for your password. You will not see anything as you type it in, but having done so press'Enter' and messages reporting progress with the installation will appear. When the thing is done the command prompt (something like: rod@rod:~$) will reappear.

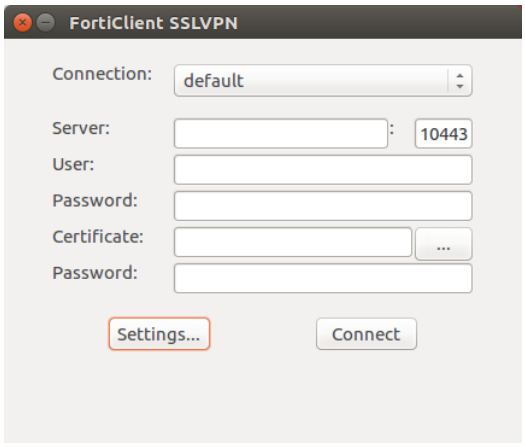
Step 3: Set up the client

On Ubuntu, you should now be able to click on the Ubuntu symbol and type 'forticlient' to find and run the application. Alternatively, from a terminal:

cd /opt/forticlient-sslvpn/64bit/
./forticlientsslvpn

The 32-bit client is installed into /opt/forticlient-sslvpn/32bit/

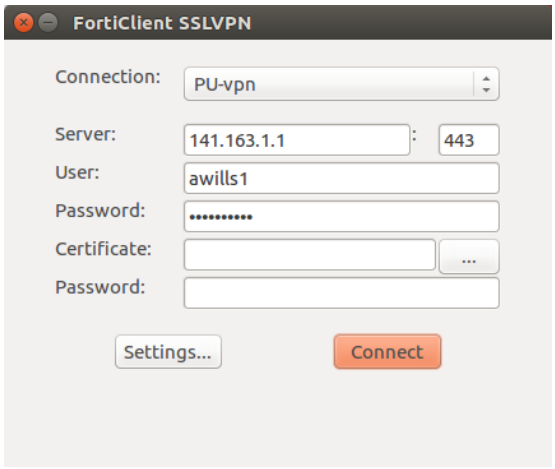
The client might greet you with a message: 'The certificate for the SSLVPN server is invalid'. Click on 'Continue'.



Click on 'Settings...'
If PU's is the only VPN that you use, you might as well select (click) 'Keep connection alive until manually stopped' and 'Start connection automatically'. Leave the rest of the Global Settings (top half of the menu) blank.

Under 'Connection Profile' click in the '+' then enter the following settings:
Connection: [Whatever you want to call it]
Server: 141.163.1.1.
Instead of 10443, which sometimes appears automatically, put into the second box on that line (after the ':') the correct port number: 443

User: [Your usual PU user-name, e.g. awills1]
Password: [Your usual current PU password]
The remaining fields, ‘Certificate:’ and (rather confusingly) the lower ‘Password:’ fields should be left blank.
Click ‘Create’, then click ‘Done’.



Step 4: Connect!
Back at the main (starting) menu, from the ‘Connection:’ drop-down box select the connection you just created. Click ‘Connect’. A Connection Status window appears, showing ‘Status: Tunnel running’ and the amount of bytes travelling to and fro.

Leave this window open (e.g. minimise it onto the taskbar) whilst you get on with whatever you wanted to use the VPN for.

To kill the connection (so that you can safely browse Facebook etc. again), don’t forget to click ‘Stop’.

Open-source alternative #1

For an open-source command line tool, you can build **openfortivpn** from source:

https://github.com/adrienverge/openfortivpn

following the instructions on that site. Basically, download (or git clone) the files, and then follow the installation instructions in README.md

After installation, alter the configuration file */etc/openfortivpn/config* with a text editor to look like this:

```
# config file for openfortivpn, see man openfortivpn(1)
host = 141.163.1.1
port = 443
username = awills1
password = your-password
trusted-cert = 77fc635c3240fa03ee3d1e2d0d1f25d81fbc760fffe9ca44a54de5037dd19623
```

Then you can run from the terminal:

sudo openfortivpn

Open-source alternative #2

If you want open-source **and** a graphic user interface, then this is possible but a bit of a faff. Use the link on PU's IT website to Roland's Blog

<http://rolandtapken.de/blog/2016-11/connect-fortigatevpn-openfortivpn>

and follow the instructions there. Frankly, if you can make this work, you probably don't need a GUI in the first place, but the option is there. Linux is choice :-)

Rod Sheaff
Andy Wills
2017-02-14