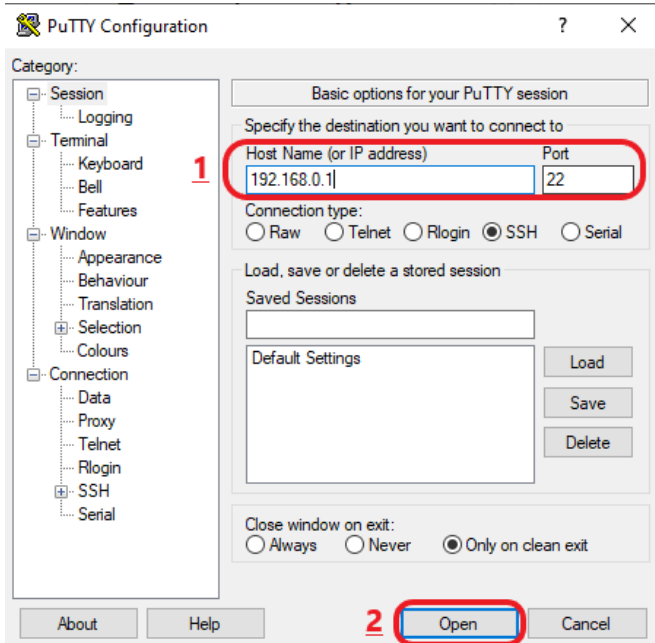


# OpenWRT – OpenVPN Client setup - PureVPN

This is an advanced tutorial on how to connect a router with OpenWRT firmware to PureVPN.

1. First, you need a router with OpenWRT firmware (tested with version 19.07) and an enabled OpenVPN client. The router will accept SSH connection open it with [PuTTY](#) . The OpenVPN package isn't included in the firmware image by default, so you need to install it:

Install PuTTY and access router IP in my case 192.168.0.1



## Use login and password of router



Run the following commands to install OpenVPN

**opkg update**

```
opkg install openvpn-openssl
```

```
opkg install ip-full
```

You can additionally install the LuCI component of the OpenVPN configuration, but this is optional:

## opkg install luci-app-openvpn

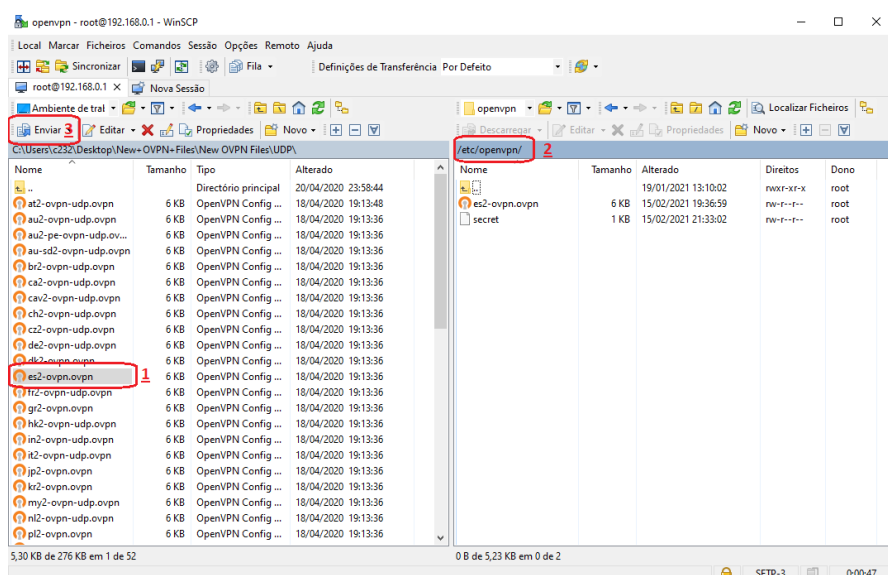
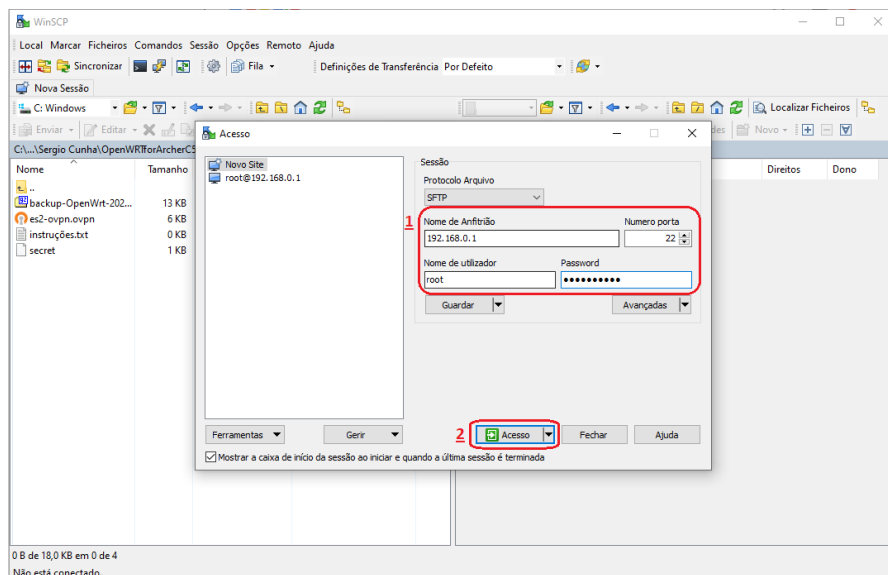
- Next, you will need to download the configuration files. I suggest using configuration files, which can be found [here](#). After downloading the file “**New + OVPN + Files.zip**”, unzip files to a know location and search for UDP folder witch contains ovpn files per server. I will use as an example Spanish server with the file “**es2-ovpn.ovpn**”.

We will need to copy some files from the computer to the router, for that we need to activate SFTP on the router. To do this run SSH commands

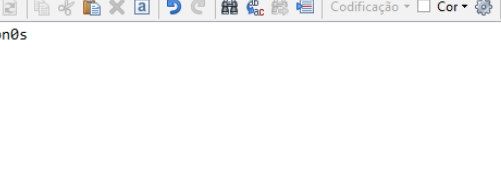
## opkg update

## opkg install openssh-sftp-server

After previous command copy the file " **es2-ovpn.ovpn** " using the [WinSCP](#) on Windows to the /etc/openvpn/ folder of the router's filesystem.



Right click on right side (router side) and select new -> File with name “secret” (without file extension), put the PureVPN user on the first line and on the second line put the password. (This data is available on the Account & Billing tab in the PureVPN Member area).

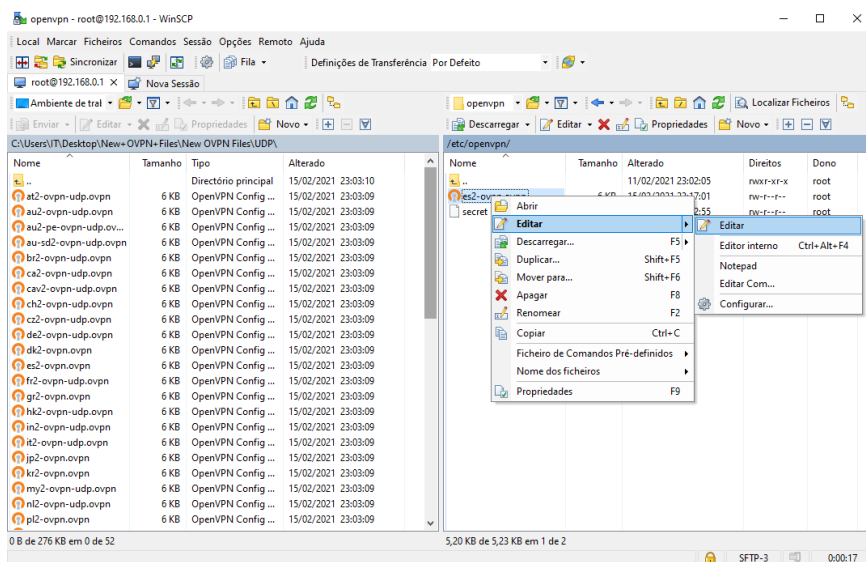


The screenshot shows a WinSCP terminal window. The title bar reads "/etc/openvpn/secret - root@192.168.0.1 - Editor - WinSCP". The menu bar includes File, Edit, View, Tools, Settings, and Help. The toolbar contains icons for file operations (new, open, save, copy, paste, delete, undo, redo), editing (find, replace), and window management (split, zoom, fullscreen). The status bar at the bottom indicates "Linha: 2/2" and "Codificação: 1252 (ANSI -)". The terminal content shows the command "purevpn0s" followed by "psw" on the next line.

```
/etc/openvpn/secret - root@192.168.0.1 - Editor - WinSCP
purevpn0s
psw
```

Save in the end.

Edit "es2-ovpn.ovpn" and put path to "secret" file, witch contain PureVPN credentials.

[illegible]

Save in the end.

3. Configuring OpenVPN (Continuing using SSH with PuTTY)

Specify the file name in /etc/config/openvpn. You can use uci:

```
uci set openvpn.purevpn=openvpn
uci set openvpn.purevpn.enabled='1'
uci set openvpn.purevpn.config='/etc/openvpn/es2-ovpn.ovpn'
uci commit openvpn
```

4. Create a new network interface

```
uci set network.purevpntun=interface
uci set network.purevpntun.proto='none'
uci set network.purevpntun.ifname='tun0'
uci commit network
```

5. Create a new firewall zone and add a forwarding rule from LAN to VPN:

```
uci add firewall zone
uci set firewall.@zone[-1].name='vpnfirewall'
uci set firewall.@zone[-1].input='REJECT'
uci set firewall.@zone[-1].output='ACCEPT'
uci set firewall.@zone[-1].forward='REJECT'
uci set firewall.@zone[-1].masq='1'
uci set firewall.@zone[-1].mtu_fix='1'
uci add_list firewall.@zone[-1].network='purevpntun'
uci add firewall forwarding
uci set firewall.@forwarding[-1].src='lan'
uci set firewall.@forwarding[-1].dest='vpnfirewall'
uci commit firewall
```

6. Now you need to configure the DNS servers. The simplest approach is to use Google DNS for the WAN interface of the router. Here's how to add Google DNS:

```
uci set network.wan.peerdns='0'
uci del network.wan.dns
uci add_list network.wan.dns='8.8.8.8'
uci add_list network.wan.dns='8.8.4.4'
uci commit
```