OpenVPN client

You can easily connect your Batocera to a VPN, as we ship OpenVPN with the distribution. However, it requires some manual configuration, and the steps involved will most probably be depending on your VPN provider.

In this example here, I will be connecting a Batocera 5.27 client to a NordVPN server, and adapt it to PIA when possible. The method here can be adapted to other VPN providers quite easily, please feel free to share your experience on the forum of Discord channel.

OpenVPN configuration

- Create a new folder for your OpenVPN configuration with `mkdir /userdata/system/openvpn`
- If your VPN provider offers you pre-configured openVPN configuration files download them in that directory.

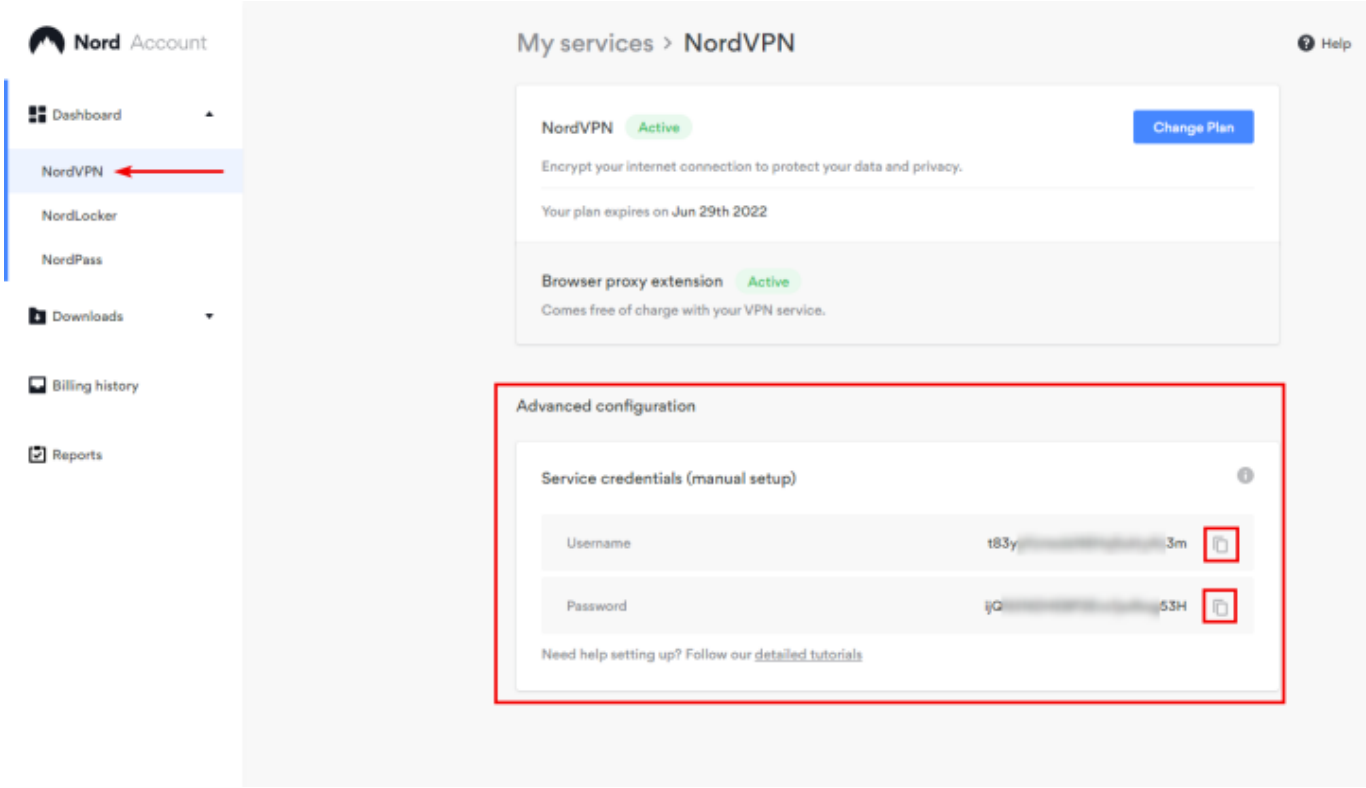
With NordVPN, I can get access to those files with:

```
cd /userdata/system/openvpn
wget https://downloads.nordcdn.com/configs/archives/servers/ovpn.zip
unzip ovpn.zip
rm ovpn.zip
```

With PIA:

```
cd /userdata/system/openvpn
wget https://www.privateinternetaccess.com/openvpn/openvpn.zip
unzip openvpn.zip
rm openvpn.zip
```

- Then, you need to create a new authentication file `/userdata/system/openvpn/auth.txt` that contains only two lines: first line is your login, second line is your password. No space, no tab, no empty line, just those two lines with login and password provided by your VPN server vendor. If you use PIA, you need to have a username starting with `p` (like `p1234567`, not just the numbers). In the case of NordVPN, you can get them from the dashboard.



- Select the VPN server you want to connect to, and find the associated openVPN configuration file. For example here, I want to connect to a VPN hosted in France, and will select the configuration file `/userdata/openvpn/ovpn_udp/fr661.nordvpn.com.udp.ovpn`. Edit this file, find the line that states `auth-user-pass` and append your authentication credentials file path to it:

```
auth-user-pass /userdata/system/openvpn/auth.txt
```

- Save the file... and now your VPN configuration is done! To connect to the VPN, just launch the command line:

```
openvpn /userdata/system/openvpn/ovpn_udp/fr661.nordvpn.com.udp.ovpn
```

Similarly with PIA:

```
openvpn /userdata/system/openvpn/us_silicon_valley.ovpn
```

Automatically launch the VPN when Batocera boots

It is possible to turn on the VPN with Batocera's boot sequence via the use of scripting.

Add the following file to `/userdata/system`:

custom.sh

```
#!/bin/bash

if test "$1" != "start"
```

```
then
  exit 0
fi
openvpn /userdata/system/openvpn/<replace_me>.ovpn &
```

where <replace_me> is your VPN.

Tips and tricks

- You can verify that you are correctly connected to the VPN by checking your public IP address before and after openvpn is started by using the command `curl ipinfo.io` or `curl ifconfig.me`
- If you want to start up your VPN connection every time Batocera boots, you can add the command openvpn `/userdata/system/openvpn/ovpn_udp/fr661.nordvpn.com.udp.ovpn &` to the local custom startup script `/userdata/system/custom.sh` – this will be the very last process fired up in the boot sequence

Troubleshooting

It's not working!

First thing is to just check that your script is running in the first place. This is easy, just put something like:

```
test line >> /userdata/system/testoutput.txt
```

in the script and then search for `/userdata/system/testoutput.txt` on next boot.

The script is running but the VPN is still not working!

It could be that it's a problem with the VPN itself launching from the script. Even if the command works in SSH, running it from a script could be an entirely different story. In order to see the error code outputs from what the command would be doing (for example from openvpn):

custom.sh

```
#!/bin/bash

if test "$1" != "start"
then
  exit 0
fi
```

```
(openvpn /userdata/system/openvpn/<replace me>.ovpn &) 2>&1 | tee -a
/var/log/vpn.log
```

Adapt the <replace me> to your VPN of course.

My VPN works fine on my PC but not on my Raspberry Pi/other SBC!

The ARM build of Batocera does not include the necessary /dev/net directory and node structure that OpenVPN relies on by default. This can be added in with the script like so:

custom.sh

```
#!/bin/bash

if test "$1" != "start"
then
  exit 0
fi

if [ ! -d /dev/net ]; then
  mkdir -p /dev/net
  mknod /dev/net/tun c 10 200
  chmod 600 /dev/net/tun
fi

openvpn /userdata/system/openvpn/<replace_me>.ovpn &
```

Adapt the <replace me> to your VPN of course.

Tailscale VPN configuration

While not packaged with Batocera by default, the Tailscale VPN service (which is essentially a fancy wrapper for Wireguard and has a free tier) can be added and functions on both the x86 and ARM-based versions of Batocera. This can provide you with benefits including Netplay with Retroarch cores and multiplayer on PPSSPP standalone without needing port forwarding, as well as the ability to SSH or SCP into your device from another network. There are some extra steps if you are on an ARM-based single-board computer, but it is confirmed working on Batocera versions as early as V31 and tested with both 32-bit and 64-bit boards (the Odroid N2L and the Odroid XU4). You should have an account made with Tailscale ahead of trying this.

- Download a Tailscale build from the static binaries section (if using an SBC, grab the one that matches your CPU architecture. ARM for the tested XU4 and ARM64 for the N2L): https://pkgs.tailscale.com/stable/#static
- On your Batocera computer, create the directory /userdata/tailscale and move tailscale, tailscaled and the systemd folder inside your respective static build tarball to that folder. On a

Windows computer, you can use 7-Zip to unpack the .tgz file twice, then sent it to Batocera with WinSCP.
- Create a file called “custom.sh” in /userdata/system (can also be done with WinSCP). Add the following to /userdata/system/custom.sh

custom.sh

```
#!/bin/bash

if test "$1" != "start"
then
  exit 0
fi
/userdata/tailscale/tailscaled -state /userdata/tailscale/state >
/userdata/tailscale/tailscaled.log 2>&1 &/userdata/tailscale/tailscale
up
```

- **IF YOU ARE USING AN ARM SBC:** You need to use WinSCP or another program with this function to check that the tailscale and tailscaled files in /userdata/tailscale have the execute permission. Go to that directory and right click on both files, then click “Properties.” Make sure to check the checkboxes for “Owner” and “Group” marked “X,” then hit OK.
- SSH to your Batocera computer with PuTTY or another program, or access Batocera's local terminal. Run this command after logging in as root:

```
/userdata/tailscale/tailscaled -state /userdata/tailscale/state >
/userdata/tailscale/tailscaled.log 2>&1 &/userdata/tailscale/tailscale up
```

- Tailscale will present you with a web link in the terminal, which you need to type into a separate PC's browser. From there, you'll log into Tailscale's web UI and connect the device.
- In the Tailscale web UI, click the “…” to the right of your newly-connected Batocera device and click “disable key expiry” so you never have to do this again!
- You should see the “Connected” status in the Tailscale web UI any time you turn on your Batocera computer now. Running the command “ip a” in terminal should show the word “tailscale” somewhere in the networking readout.

To add your friends to the same Tailscale network for multiplayer (who can be running non-Batocera versions of PPSSPP like Android for that use case), you can go through this process yourself and authenticate their devices by logging in as yourself, or you can invite them to join your Tailnet. Note that the free version of Tailscale only allows you to add two other people to your network, but if you sign in as yourself on all the devices, you can get as many as 100.