How to set up OpenVPN Client on HH5a with OpenWrt

The instructions are fairly generic and should work with all other makes and models of OpenWrt routers.

Document revision history:

```
v1.3c (3 Feb 2024)      - Minor revisions.
v1.2p (15 Dec 2023)     - Keepsolid/VPNunlimited .ovpn parsing bug in 19.07 & 21.02?
v1.2n (23 Apr 2022)     - Minor updates for OpenWrt 22.03.
v1.2m (10 Oct 2021)     - Fix for OpenWrt 21.02 LuCI not loading.
v1.2ck (19 Aug 2021)    - Updated for OpenWrt 21.02.
v1.2j (3 Apr 2021)      - Add check for 'tun' in .ovpn file.
v1.2e (30 Oct 2019)     - Add DNS servers to LAN interface.
v1.2 (5 Sep 2019)       - Refreshed for OpenWrt 19.07 only.

v1.1 (21 Aug 2018)      - For LEDE 17.01 and OpenWrt 18.06.
v0.1 (29 Nov 2017)      - Created by 'bill'.
```

Contents

1. Introduction (updated Dec 2023)

This is a supplement to the 'OpenWrt/LEDE Installation Guide for the BT Home Hub 5A'. It describes how to install and configure the OpenVPN client for use with 3rd party VPN service providers. The instructions are fairly generic and should work with all other makes and models of OpenWrt routers.

This tutorial uses just LuCI. A file transfer utility such as WinSCP (Windows file transfer utility) may be required.

Update (Dec 2023): This tutorial has been refreshed to use ProtonVPN. They appear to offer free access to 3 countries at time of writing. Simply set up an account. Their free plan do not permit torrenting.

Speed test results using www.speedtest.net, speedof.me, BT wholesale, and Thinkbroadband speed testers in the UK for a number of routers I have personally tested over **ethernet** connection with my current VPN provider (Not ProtonVPN btw) to their closest and fastest server (using AES-256-CBC cipher).

Device	OpenWrt	SoC	Openvpn speed
BT Home Hub 5A	19.07.7	500 MHz MIPS VRX268	9 Mbps *
TP-Link Archer C50 v4	r10242 - Jun'19	580 MHz MIPS MT7628A	12 Mbps *
TP-Link Archer A6/C6 v3	22.03.0-rc4	880 MHz MIPS MT7621DAT	19 Mbps *
Xiaomi 4A Gigabit	22.03.0-rc4	880 MHz MIPS MT7621A	19 Mbps *
Linksys EA6350 v3	19.07.10	710 MHz ARM IPQ4018	25 Mbps *
TP-Link Archer VR2600 v1	21.02.1	1.4 GHz ARM IPQ8064	62 Mbps *
Dell Wyse 3040 (Realtek nic) + HH5a managed switch	22.03.4 22.03.4	1.44 GHz x86 Atom x5-z8350, AES-NI	135 Mbps **
Intel computer + RTL8169 PCI nic + HH5a managed switch	22.03.4 22.03.4	2.9 GHz x86 Core i5-3475s, AES-NI	244-294 Mbps
Intel computer (Intel nic) + HH5a managed switch	22.03.4 22.03.4	2.9 GHz x86 Core i5-3475s 2.7 GHz x86 Core i5-3340m 3.4 GHz x86 Core i5-8250u, AES-NI	440-482 Mbps
Intel computer (RTL8111 nic) + HH5a managed switch	22.03.4 22.03.4	2.8 GHz x86 Core i5-8400, AES-NI	450-500 Mbps

(* = Speeds via **wireless** will be **lower** than above quoted ethernet speeds)
(** = Monitor must be connected when OpenWrt starts to prevent performance degredation)

See also: https://OpenWrt.org/docs/guide-user/services/vpn/openvpn/performance

As can be seen from table above, most budget routers cannot reach 20 Mbps when connecting to VPN service providers.

Used routers using Qualcomm IPQ8064/65 tend to offer much faster speeds between 60 and 75 Mbps. The TP-Link C2600/VR2600(v) are difficult to flash. In the UK, the Netgear D7800 modem-router is worth considering, and is usually less expensive than the Netgear R7800 which has a faster 1.7 GHz cores.

Asus also offer routers with OpenVPN client/server functionality out of the box. eg. The **RT-AC86u** (1.8 GHz ARM) running stock AsusWrt can achieve openvpn speeds of **75 Mbps**. There is also 'custom' AsusWrt firmware from 'Merlin' which can achieve **170 Mbps** according to this PIA blog when hardware accelerated AES encryption is enabled.

https://www.privateinternetaccess.com/blog/2018/08/hardware-acceleration-is-here-for-routers-using-openvpn/

GL-inet offer their new GL-AX1800 AX router (1.2 GHz IPQ6000) running a custom version of OpenWrt, and they claim it is capable of upto **115** Mbps OpenVPN speeds with stock firmware, although google searches have reported speeds topping out at 70 Mbps – this may or may not depend on the cipher being used.

A **Raspberry Pi 4** with a AX88179 USB3 gigabit ethernet adapter can supposedly achieve 100 Mbps. A **NanoPi R4S** is alleged to be capable of 220 Mbps. The new **Raspberry Pi 5** boasts huge improvements in hardware performance and OpenWrt is expected soon – it is not known at this time whether the embedded AES-NI will be supported by OpenWrt.

For fastest OpenVPN speeds use a device where there is support for hardware accelerated AES-NI encryption (crypto engine) from OpenWrt/DDWRT etc.

I have also tested Openvpn client on x86 (64bit) 22.03.4 squashfs installed on Intel based devices. The AES-NI is supported by most Intel processors on OpenWrt. All devices booting from a usb2 flash drive. A VLAN trunk on the single ethernet cable into a HH5a (22.03.4) used as a managed switch to provide the separate WAN and LAN ethernet ports. ISP speed test returns 518 Mbps. Best OpenVPN speed test returns **500 Mbps**.

In general, I found OpenVPN client works very well on HH5a. I've had one unit with LEDE 17.01.4 running 24/7 for over a year connected to my VPN provider, and only times I had to reboot it had nothing to do with the VPN service. I upgraded it to OpenWrt 19.07.3 and it continued to be reliable for a further 10+ months of use before upgrading to faster Xiaomi 4A Giga and Linksys EA6350 v3 devices.

9 Mbps ethernet speeds is likely to be too slow for downloading files with HH5a, but is adequate for normal web browsing and HD video streaming.

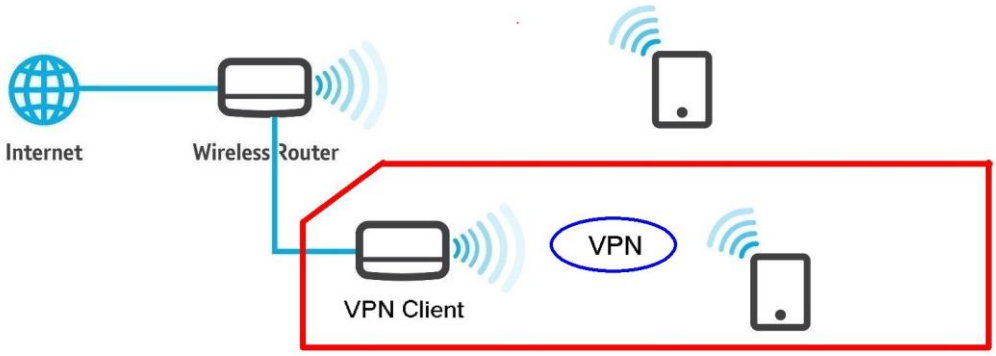
You can choose which devices use the VPN and which devices don't use the VPN to connect to the internet. There are two options in OpenWrt. One is called **'Policy based Routing'**, and the other is '**VPN Bypass'**. Both are beyond the scope of this document.

Also, due to the lack of processing power, it is not recommended to use a HH5a simultaneously as the main router and as a VPN client.

I've tested Wireguard on HH5a running 19.07.4 and speed tests and file downloads returned 40 mbps (speeds will be lower with later versions of OpenWrt) on my former 55 mbps FTTC connection at the time. This is considerably faster than the <9 mbps when using openvpn. I personally don't use Wireguard because I find it is unreliable with my current VPN provider. Also, it is not easy to change servers quickly because there is no GUI for managing multiple Wireguard connections, particularly if you use more than one VPN provider.

2. Installing the OpenVPN Client

2.1 Downloading the OpenVPN client package



Unless you are particularly paranoid about privacy, it is likely you only wish certain devices to use a VPN, whereas the majority of other devices will continue to connect to the regular internet service, particularly devices which are geolocation sensitive, such as smart TVs. Also, the maximum openvpn speed through HH5a is about 9 mbps and so it is unlikely the HH5a would be used as the sole internet wired router for broadband connections significantly greater than 10 mbps. This tutorial shows HH5a wired to existing internet facing router.

To install OpenVPN client, a working internet connection is required. The red WAN port on the HH5A will be be enabled for this purpose, so it can be connected to an existing router for internet access.

Example configuration:

```
Main ISP router LAN IP address            192.168.1.1
HH5a VPN client LAN IP address            192.168.111.1
HH5a VPN client static WAN IP address     192.168.1.209 (or use DHCP)
LEDE 17.01.2 stable or later.
```

It is recommended to factory reset the HH5a.

Power on the HH5a and wait a few minutes. Press and hold the Reset button on the back of the HH5A for at least 10 seconds. Release the button when the main power light starts blinking rapidly in red colour. When the colour changes to a constant green colour, the factory reset is complete.

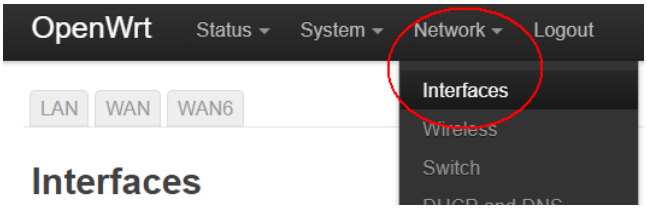
Alternatively, navigate to **LuCI -> System -> Backup/Flash Firmware** menu. Click on **Perform Reset** button.

Edit default LAN IP address

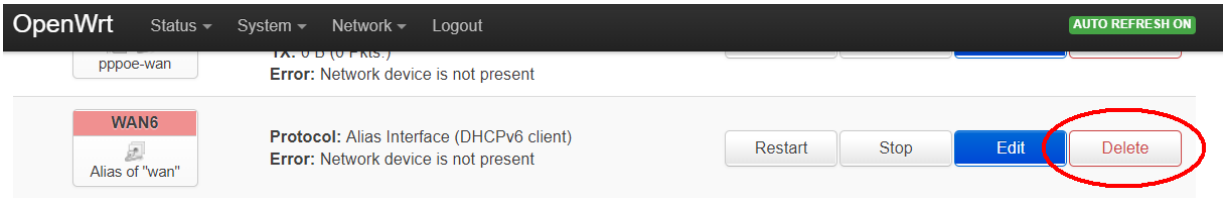
Connect a computer to one of the yellow LAN sockets on the HH5a with an Ethernet cable, and use a web browser and go to 192.168.1.1 and log into LUCI web admin.

Do **not** connect anything to the red WAN port at this time.

In LuCI and go to `Network -> Interfaces`.



IPv6 is beyond the scope of this document, so you may wish to delete the `WAN6` interface.



Press '`Save & Apply`' button at the bottom of the page.

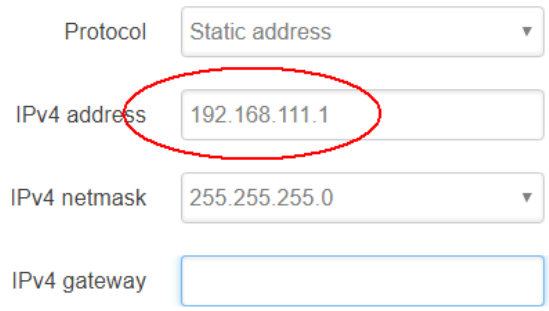
Navigate to `Network -> Interfaces -> LAN`.

Click on '`Edit`' button.

IMPORTANT:

If necessary, change the LAN IP address of the HH5a to use a different subnet (eg. `192.168.111.x`). Do **NOT** use the same subnet, such as `192.168.1.x`, on both WAN and LAN interfaces.

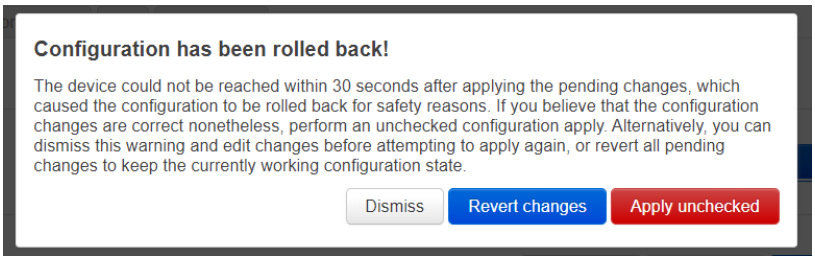
This example shows `192.168.111.1` assigned to the LAN interface of the HH5A.



Press '`Save`' button.

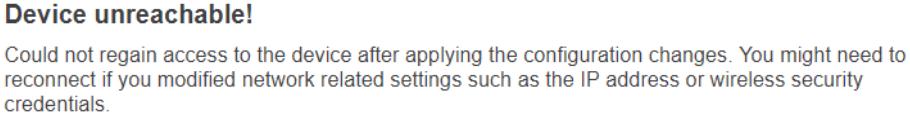
Press '`Save & Apply`' button at bottom of the page.

The following prompt will appear after 30 seconds.



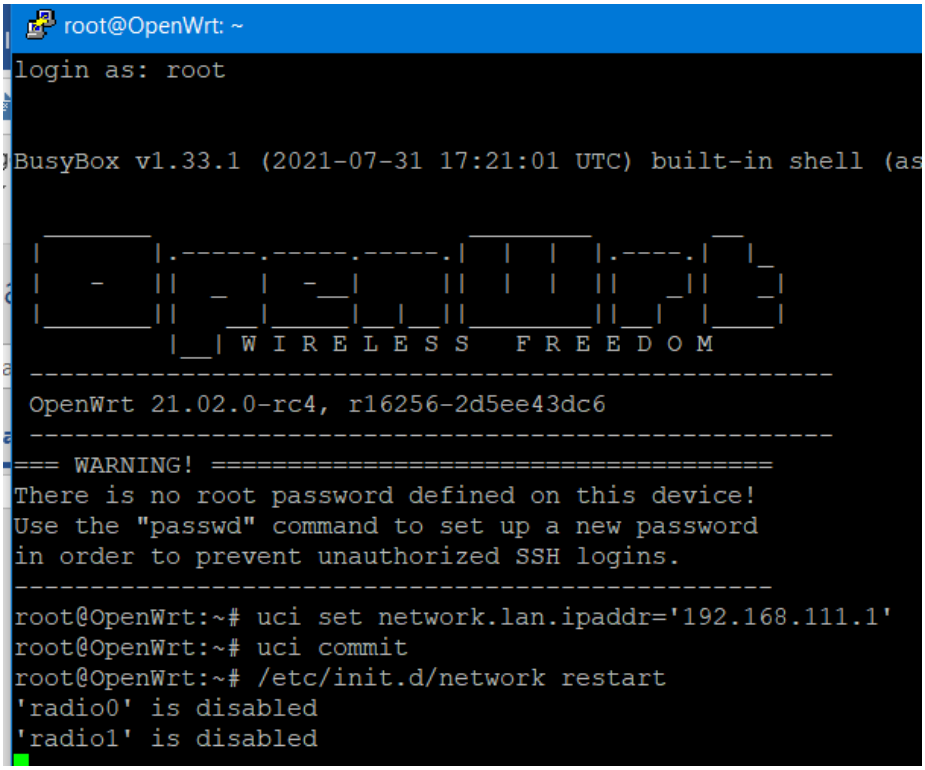
Simply click on the `Apply unchecked` button to continue.

After another 30 seconds has elapsed, the following message is likely to appear, to confirm the IP address has successfully changed.



If you are unable to change the LAN IP address using LuCI (An issue I've frequently seen since this annoying Rollback feature was introduced), it can be changed by SSH into the router, and executing the following commands:

```
uci set network.lan.ipaddr='192.168.111.1'
uci commit
/etc/init.d/network restart
```



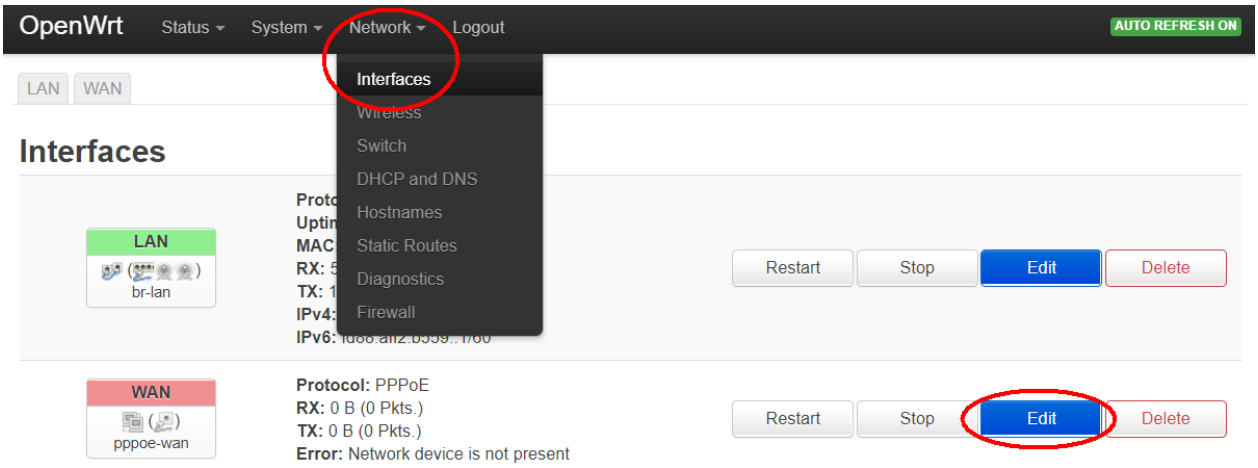
You may need to unplug the Ethernet cable between the PC and the HH5a a couple of times to encourage the PC to drop its former 192.168.1.x IP address, and acquire a new 192.168.111.x IP address.

Now point a web browser to 192.168.111.1 and log into LuCI.

The next step is to edit the `WAN interface` settings.

Navigate to `Network -> Interfaces -> WAN`.

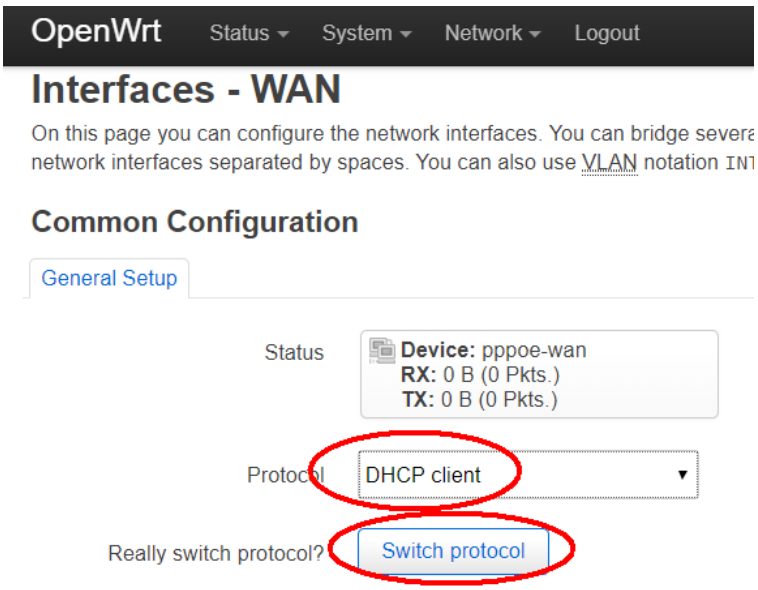
For the '`WAN`' interface, click '`Edit`'.


OpenWrt
Status
System
Network
Logout
AUTO REFRESH ON
Interfaces
Wireless
Switch
DHCP and DNS
Hostnames
Static Routes
Diagnostics
Firewall
LAN
WAN
Interfaces
LAN
br-lan
Restart
Stop
Edit
Delete
WAN
pppoe-wan
Protocol: PPPoE
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)
Error: Network device is not present
Restart
Stop
Edit
Delete

The default protocol for most routers is 'DHCP client'. However, as the HH5a is a modem-router, its default is 'PPPoE'.

For the HH5a, change the Protocol from 'PPPoE' to 'DHCP client '.

Click on 'Switch Protocol' button

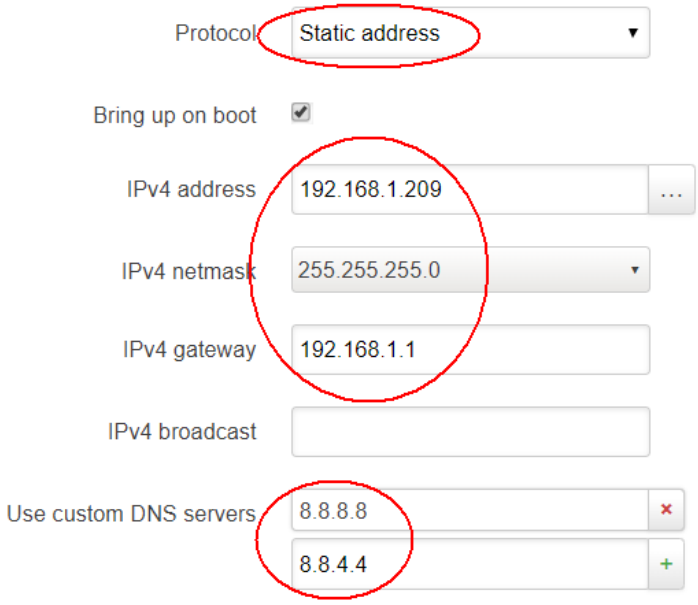


Press 'Save' button.

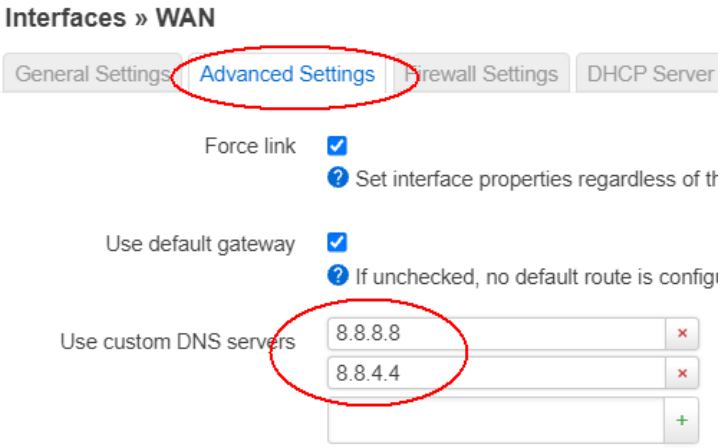
Press 'Save & Apply' button at the bottom of the page.

Alternatively, if you are confident with managing your IP addresses, you may wish to use 'Static address', but you will have to complete the remaining fields. For this example, the main ISP facing router has IP address 192.168.1.1, and 192.168.1.209 is unlikely to be in use, so has been chosen for the HH5a WAN interface. 8.8.8.8 is Google's DNS server.

IPv4 address:	192.168.1.209	
IPv4 gateway:	192.168.1.1	(same as LAN IP address of ISP facing router)
DNS server:	8.8.8.8 and 8.8.4.4	



If you are using OpenWrt 21.02, the 'custom DNS servers' boxes has moved to 'Advanced Settings' tab:



Press '`Save`' button.

Press '`Save & Apply`' button at the bottom of the page.

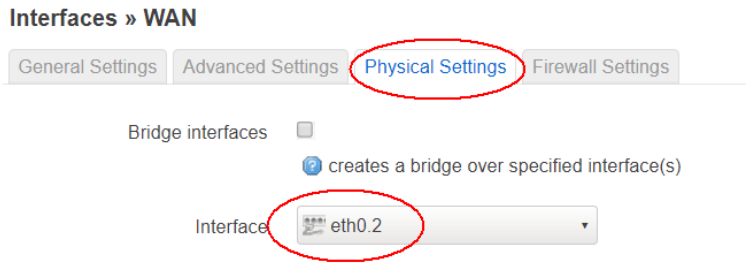
Modem-router Owners Only:

This is specific to routers which possess a Lantiq based DSL modem, such as the HH5a. For all other cable routers, you can review and skip past the following steps.

For OpenWrt 19.07 or earlier:

Go to `Network -> Interfaces`, and for the '`WAN`' interface, click '`Edit`'.

Under '`Physical Settings`', choose '`eth0.2`'

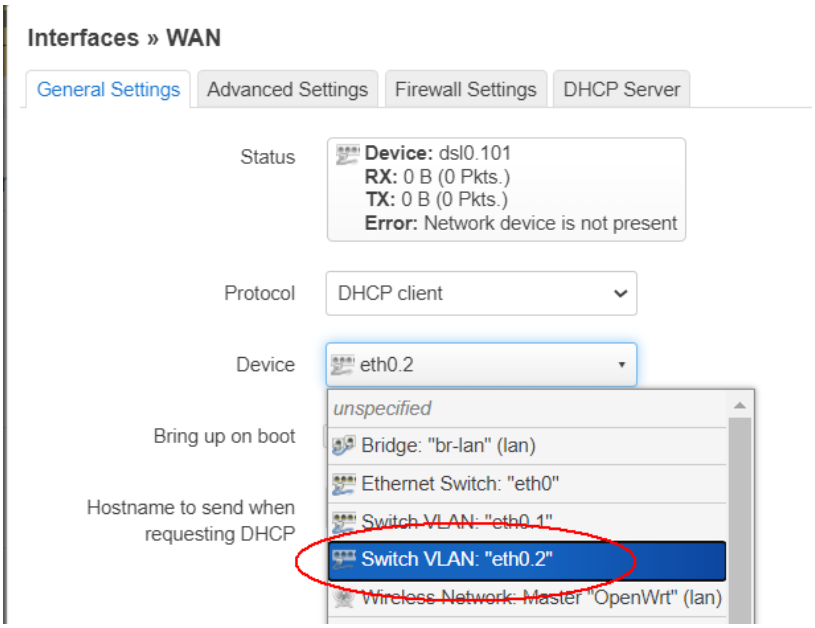


Press 'Save' button.

Press 'Save & Apply' button at the bottom of the page.

For OpenWrt 21.02, there is no 'Physical Settings' tab.

Select 'eth0.2' in Device list box as shown below.

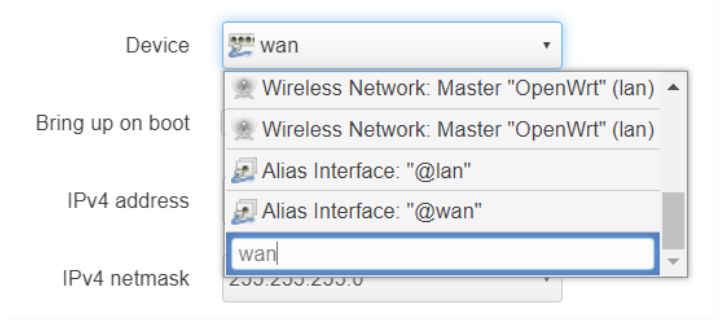


Press 'Save' button.

Press 'Save & Apply' button at the bottom of the page.

NEW For OpenWrt 22.03, there is no 'Physical Settings' tab.

Manually type in 'wan' in Device list box as shown below.



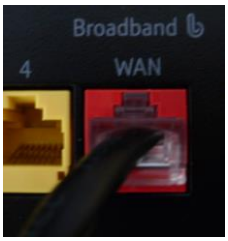
Do NOT use the Alias interface @wan, it will not work.

Press ‘Save’ button.

Press ‘Save & Apply’ button at the bottom of the page.

All router owners:

The next step is to download and install the OpenVPN package.

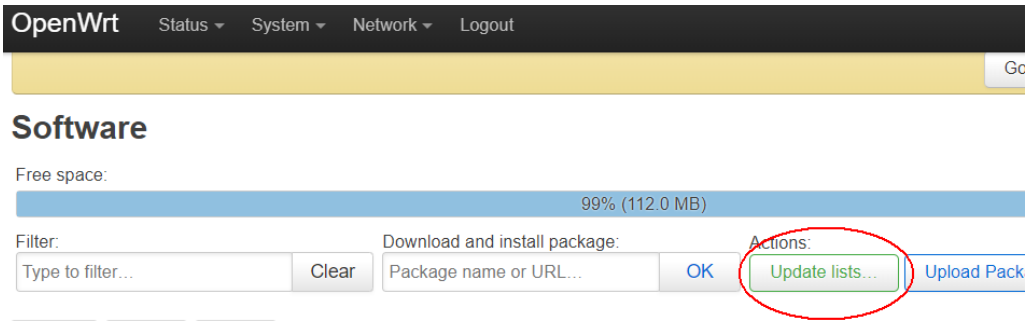


Connect an Ethernet cable from the red ethernet WAN port of the HH5a to a vacant LAN socket on your internet wired router.

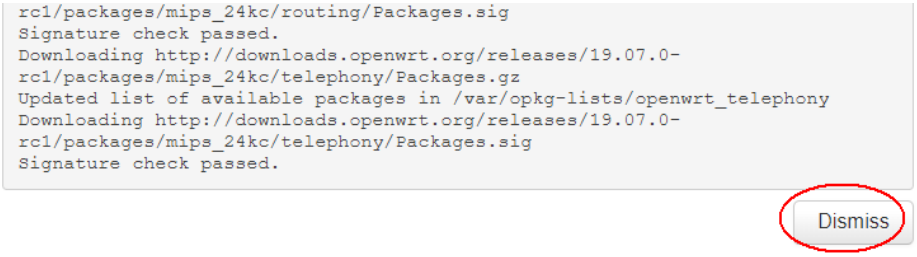
Check your PC has internet access with your web browser through the HH5a.

Navigate to `System -> Software`

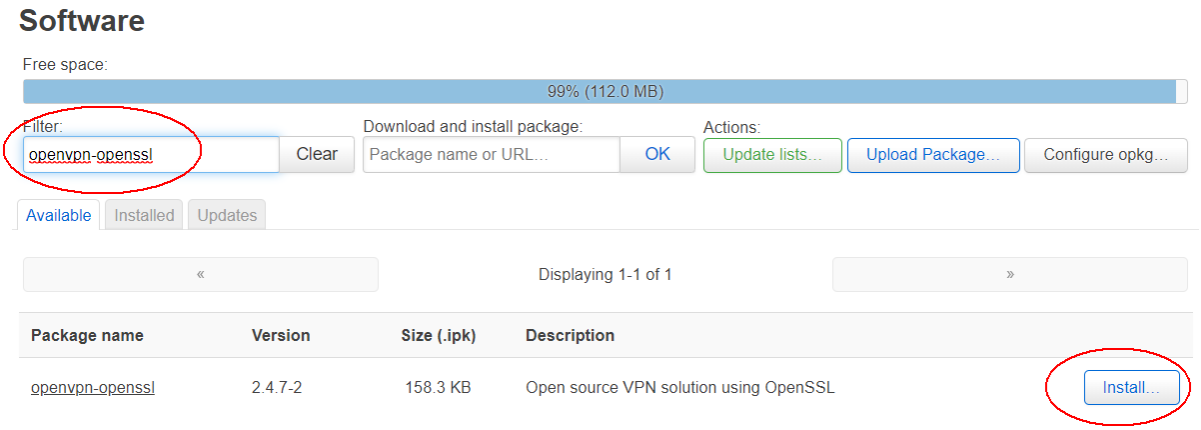
Click on '`Update lists…`' button.



A popup window shows the list of packages being updated. Press the `Dismiss` button.

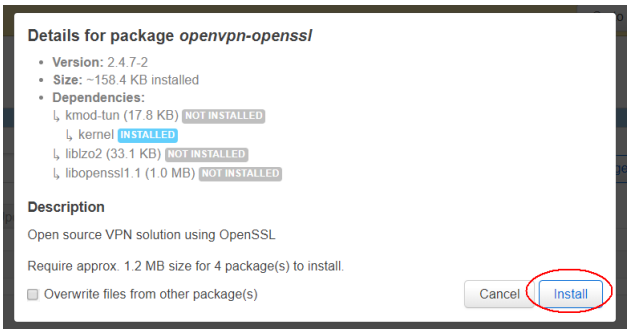


Now enter '`openvpn-openssl`' into the Filter box.



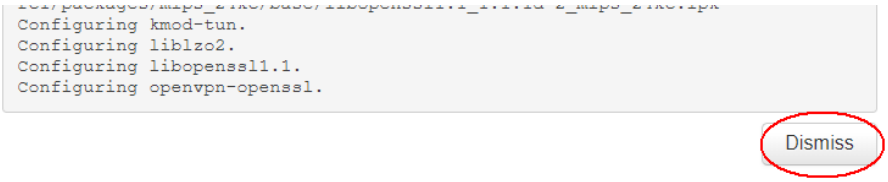
Press the `Install` button shown above.

A popup window will appear. Press the `Install` button to continue as shown below.

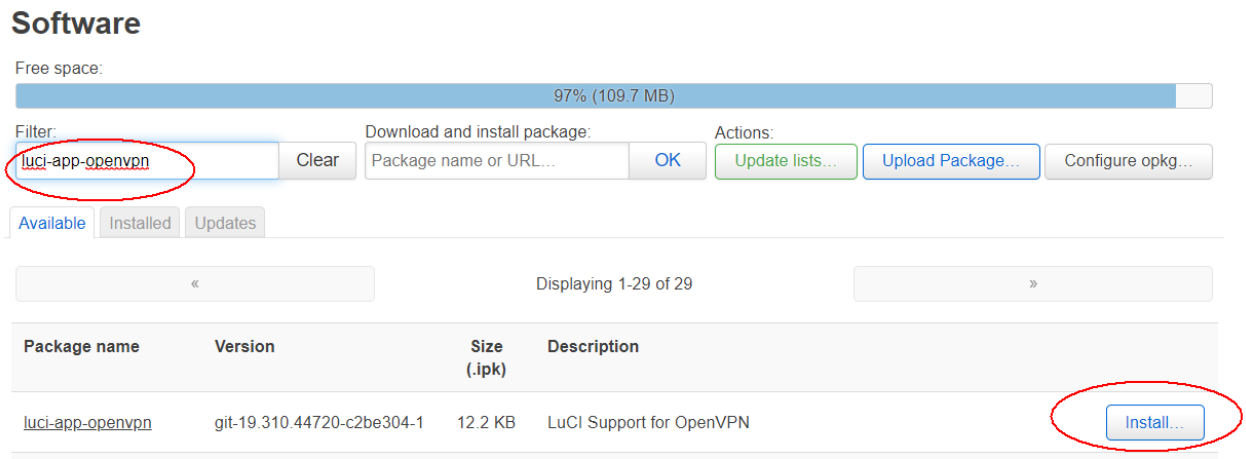


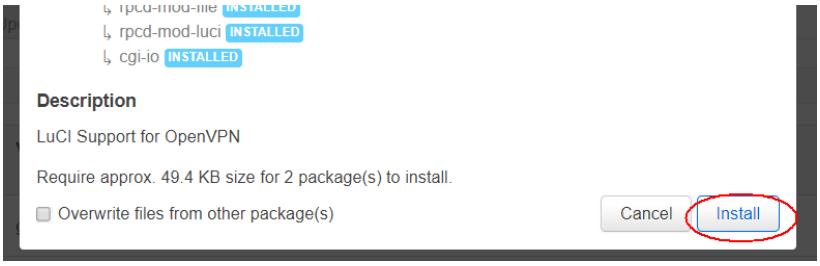
A window showing the progress for downloading and installing the `openvpn-openssl` package.

When complete, press the Dismiss button.

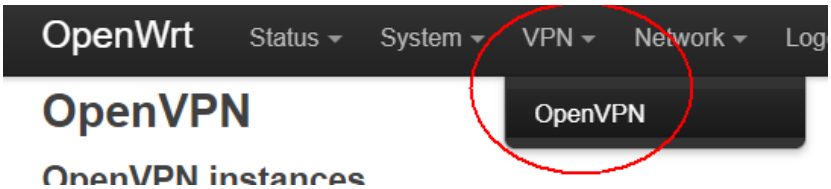


Now repeat above steps for ‘`luci-app-openvpn`’ package and install it.





Select another menu option such as `Network -> Interfaces` and eventually the 'VPN' menu should appear as shown below.



(Added. Bug in 19.07.3) If the 'VPN' menu fails to appear, you may have to navigate LuCI to `Logout`. When you log in again, the 'VPN' menu should be visible.

2.2 Configuring the OpenVPN Client for OpenWrt 19

Creating tun0 interface

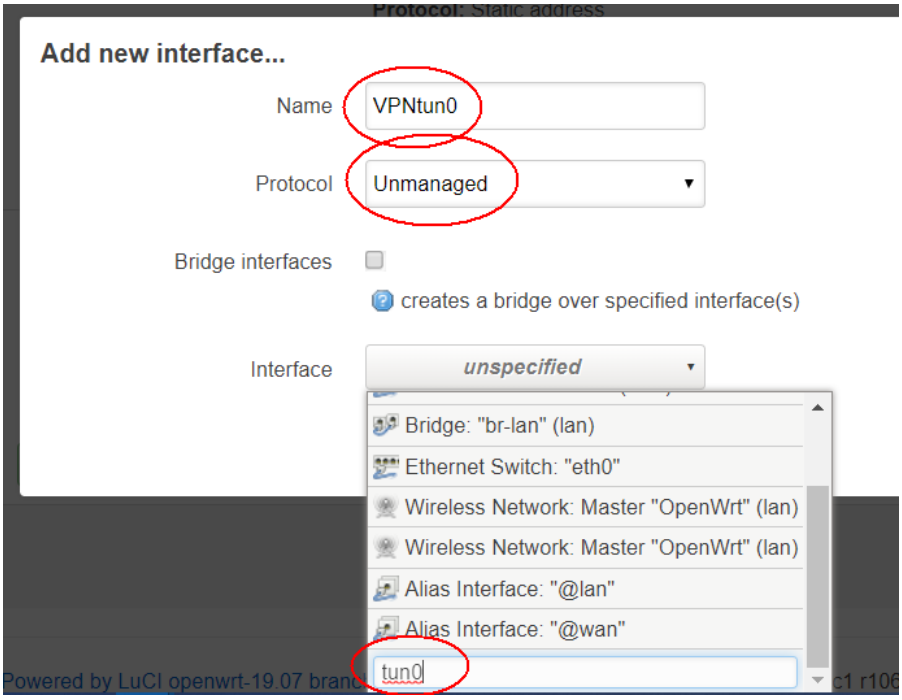
In LuCI, go to the `Network -> Interfaces` menu.

Click on the `'Add new interface'` button.

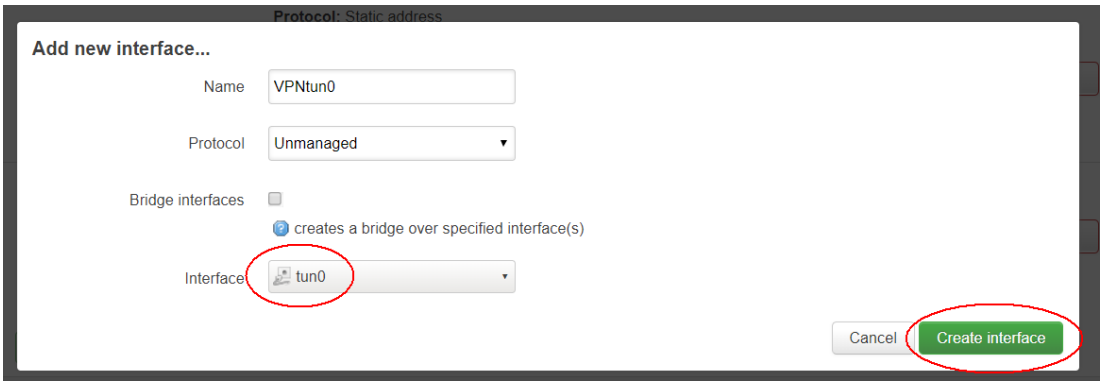
Specify a name of your choice for the interface. eg. `VPNtun0`

Choose '`Unmanaged`' for the Protocol.

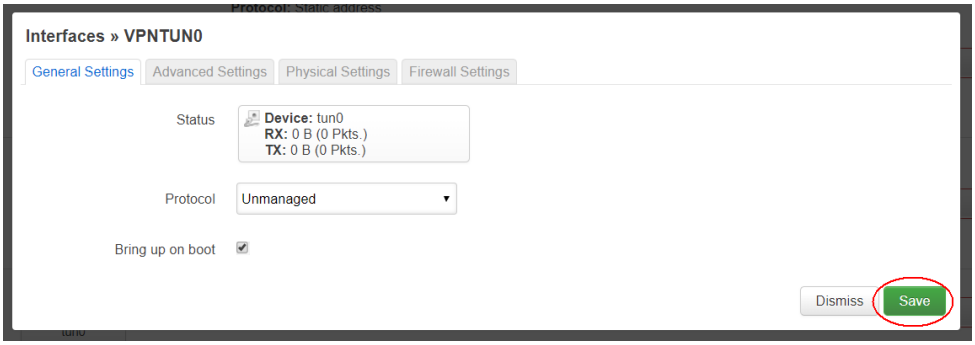
Enter '`tun0`' for Custom Interface.



Press the `Enter` key after carefully typing in `tun0`



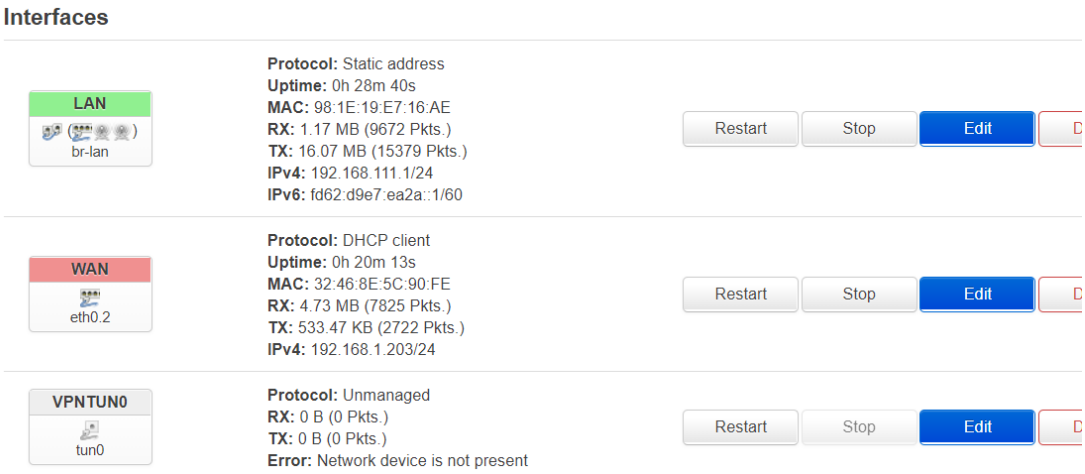
Press the '`Create Interface`' button.



Then press ‘`Save`’ button.

Then press ‘`Save & Apply`’ button at bottom of the page.

The page will refresh and return to the `Network -> Interfaces` menu.



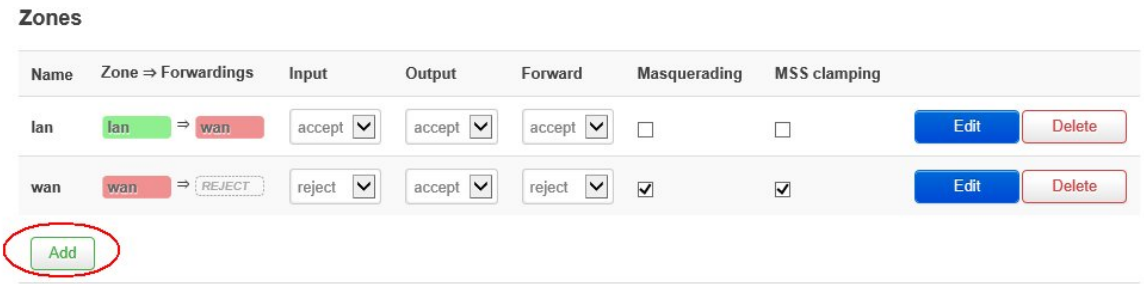
Creating VPN zone

The procedure below differs from the current OpenWrt wiki page. The following is based on the old wiki page setup method before it was rewritten from 2018 onwards. The advantage of this older method, is the ability to turn ‘Kill switch’ ON and OFF as required.

In LuCI, go to `Network -> Firewall` menu.

Scroll to the bottom of the page.

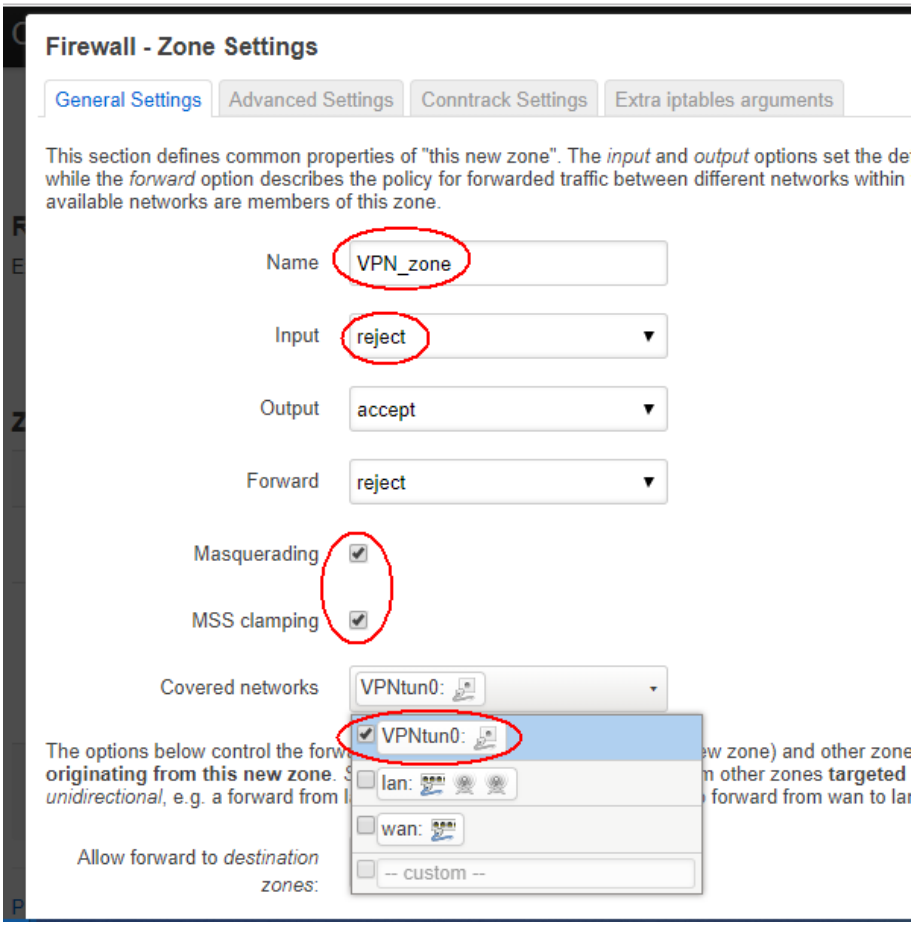
Now click on the Add button as shown below:



Specify a name of your choice for the new VPN firewall zone. eg. `VPN_zone`

Edit the five parameters as shown below for:

Name:	`VPN_zone`
Input:	`Reject`
Masquerading:	`tick`
MSS Clamping:	`tick`
Covered Networks:	`VPN_tun0`



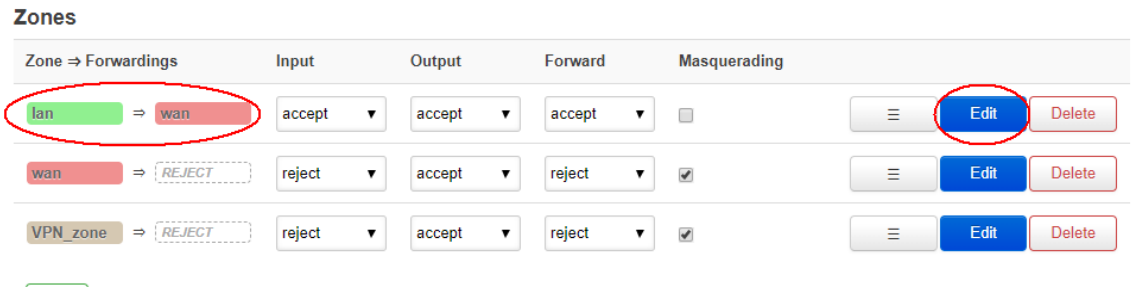
Press '`Save`' button.

Press 'Save & Apply' button at the bottom of the page.

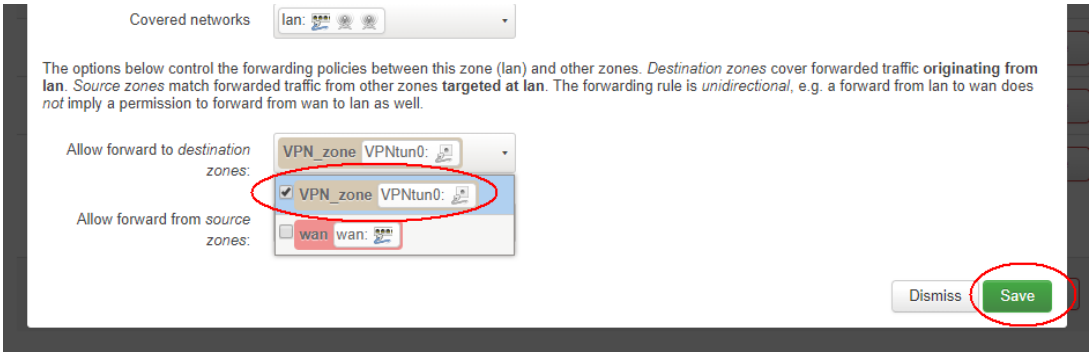
Return to Network -> Firewall menu.

Scroll down the page until you find the Zones section.

Click on 'Edit' button for the 'lan' zone as shown below.



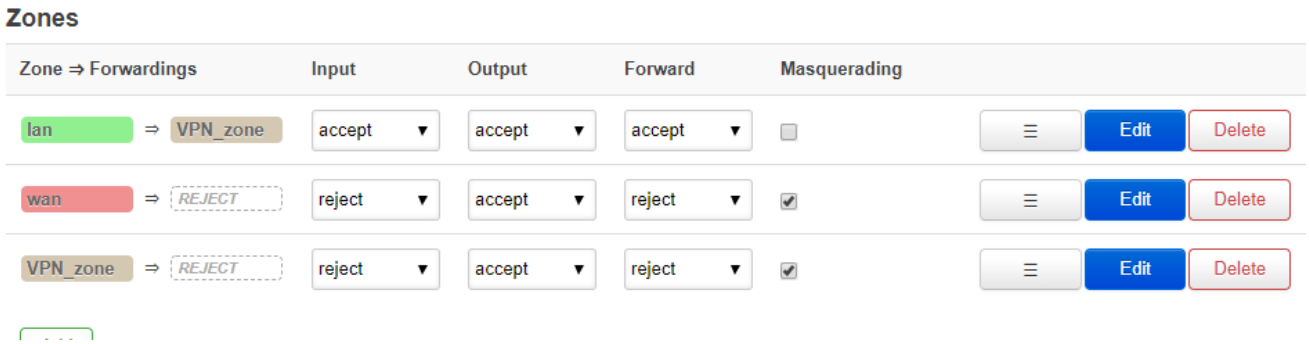
Scroll to the bottom of the page and change the 'Allow forward to destination zones' from 'wan' to the newly created 'VPN_zone' as shown below.



Press the 'Save' button.

Press the 'Save & Apply' button at the bottom of the page.

Important: Check the three zones: `lan, wan, VPN_zone` match **ALL** of the settings shown below:



Editing OpenVPN configuration

Update (Dec 2023): ProtonVPN offer free accounts to their USA, Netherlands and Japan servers. (The free accounts do not permit torrenting)

Download the relevant OpenVPN configuration files from your chosen VPN service provider. See section 4. The free VPN service provider, ProtonVPN, is used in this example.

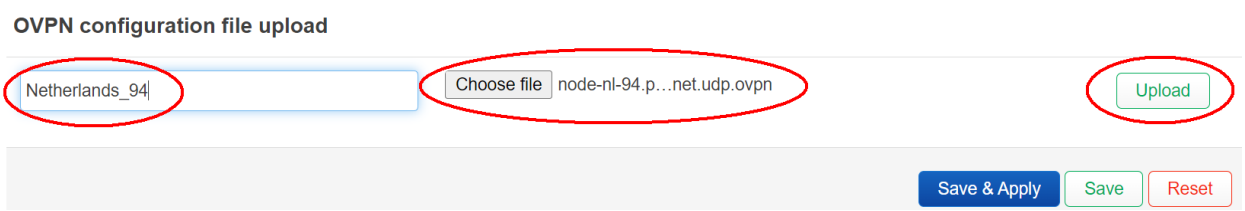
In LuCI, go to `VPN -> OpenVPN` menu.

Scroll down to the `OVPN configuration file upload` section as shown below.

Enter a name for the VPN instance. eg. `Netherlands_94`

For best performance it is recommended to use the `.ovpn` files for `UDP` connections. They will contain `udp` in the filename.

Choose the `.ovpn` file you wish to use.



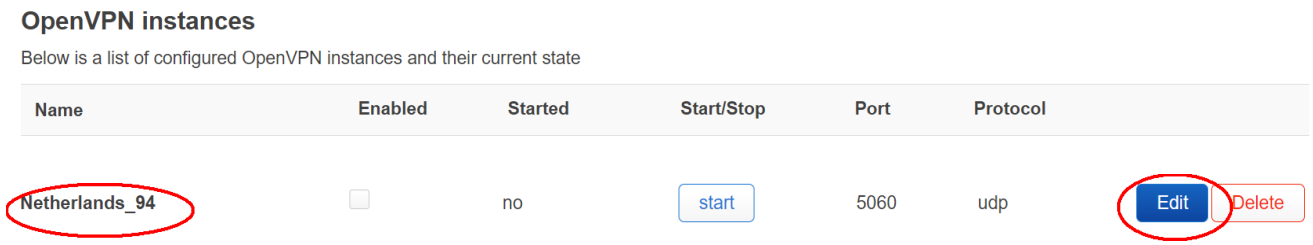
Press the `Upload` button.

~~Press the 'Save & Apply' button.~~

The ovpn file will be uploaded to the folder `/etc/openvpn` on the router and renamed. The new filename is derived from the name of the 'VPN instance'. eg.

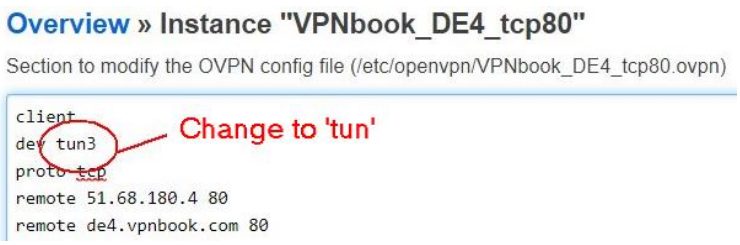
`/etc/openvpn/Netherlands_94.ovpn`

The new VPN instance will appear in the list as shown below.



Click on the '`Edit`' button to reveal the contents of the `.ovpn` file.

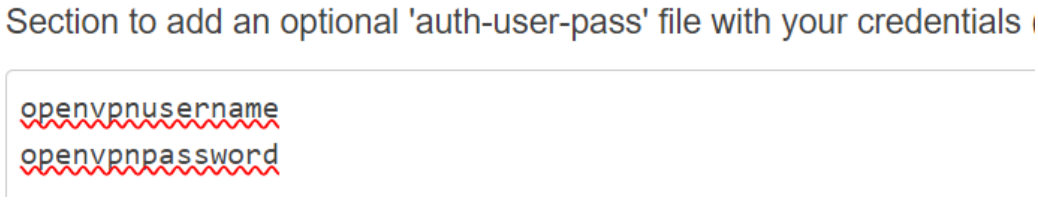
(NEW) Where necessary, you may need to edit the file to read '`tun`' as in example below.



Scroll down the page and look for a line containing `'auth-user-pass'` as shown below. This indicates a separate file containing the username and password (ie. Credentials) to log into the VPN service is required.

If you cannot see `'auth-user-pass'` line, it may mean your VPN provider does not require one.

If an `auth-user-pass` file is required, scroll to the bottom of the page and enter a valid username (eg. `openvpnusername`) and password (eg. `openvpnpassword`) on separate lines as shown below.



This will be saved to a filename derived from the name of the 'VPN instance'. In this example, the filename will be:

`/etc/openvpn/Netherlands_94.auth)`

Locate and edit the '`auth-user-pass`' line in the `.ovpn` file to add the full path of the above file as shown below.

Tip: simply copy & paste the highlighted blue text shown below.

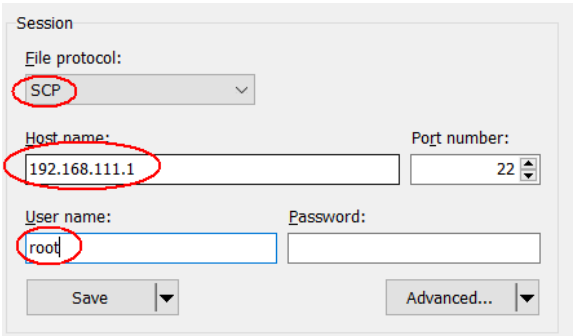
Press `Save` button.

Uploading additional configuration files

If your VPN service provider has supplied any additional configuration files, such as separate certificates or static keys which are not contained within the `.ovpn` file, these must be uploaded to the `/etc/openvpn` folder on the router. You will also need to edit the `.ovpn` file contents to include the full path to these files. Windows users can use WinSCP to upload these files to the router. For example:

```
ca /etc/openvpn/ca.crt
cert /etc/openvpn/server.crt
key /etc/openvpn/server.key
dh /etc/openvpn/dh1024.pem
```

Start WinSCP and log into the HH5A at 192.168.111.1.

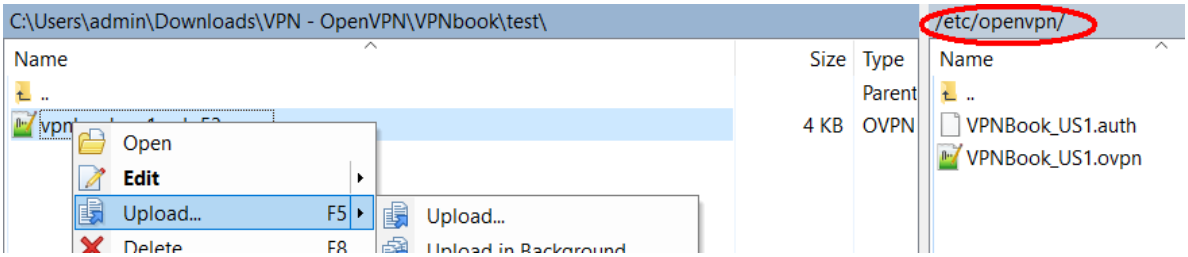


In the left hand pane of WinSCP, navigate to the folder which contains any additional certificates or static key files which your VPN provider has supplied.

In the right hand pane of WinSCP, navigate to the `/etc/openvpn` folder.

Upload the files to the on the HH5A by right-clicking on a file in the left hand pane, and choose ‘Upload’.

In this tutorial, ProtonVPN does not provide any ‘extra’ certificate or key files so there is nothing extra to upload. You can see there is already an `VPNBook_US1.ovpn` file which was uploaded earlier, and the credentials (username & password) `VPNBook_US1.auth` file.

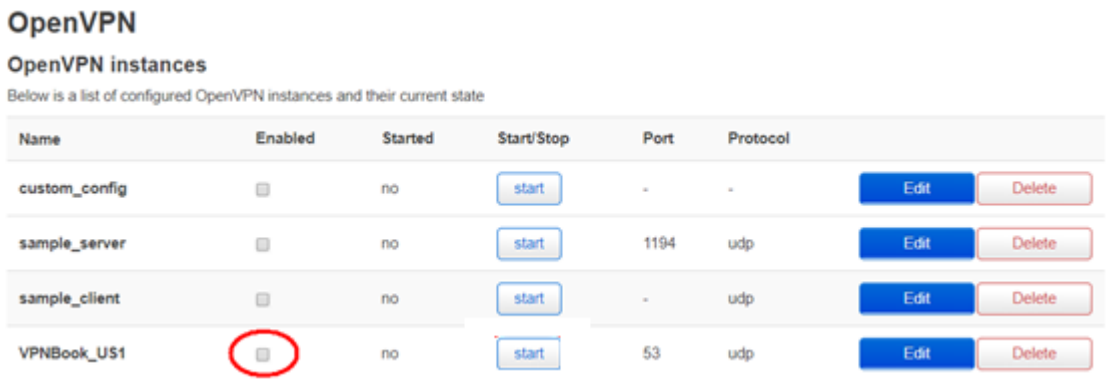


How to start VPN client

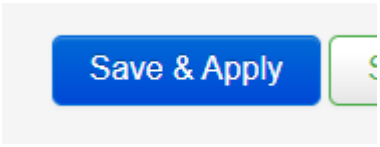
In LuCI, go to the `VPN -> OpenVPN` menu.

Note that simply pressing the `'Start'` button **does not** start the VPN instance.

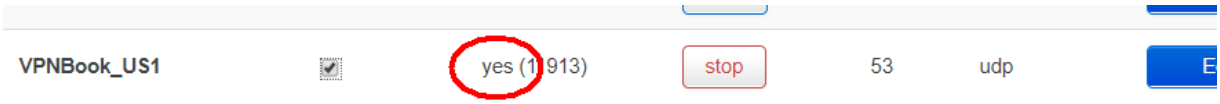
Tick the '`Enabled`' check box as shown below.



Then press `Save & Apply` button to initiate the VPN connection.



If the VPN instance starts, you should see the status change from '`No`' to '`Yes`' as shown below:



The `Start/Stop` button will function correctly while the `Enabled` check box is ticked.

You may need to shut down and restart the HH5A if nothing happens.

If the VPN instance fails to start, there is likely to be a problem with the configuration. If required by the VPN provider, check the credentials and the path has been appended to the '`auth-user-pass`' line in the `.ovpn` file.

Go to `Status -> System Log` menu to examine the system log. Look for lines beginning 'daemon.notice.openvpn'.

Look specifically for **'Initialization Sequence Completed'** as shown in the image below. The message is an indication of a successful VPN connection.

```
Fri Sep  6 09:31:21 2019 daemon.notice openvpn(VPNBook_US1)[12541]: Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
Fri Sep  6 09:31:21 2019 daemon.notice openvpn(VPNBook_US1)[12541]: TUN/TAP device tun0 opened
Fri Sep  6 09:31:21 2019 daemon.notice openvpn(VPNBook_US1)[12541]: TUN/TAP TX queue length set to 100
Fri Sep  6 09:31:21 2019 daemon.notice openvpn(VPNBook_US1)[12541]: /sbin/ifconfig tun0 10.8.0.70 pointopoint 10.8.0.69 mtu 1500
Fri Sep  6 09:31:21 2019 daemon.notice netifd: Interface 'VPNBook' is enabled
Fri Sep  6 09:31:21 2019 daemon.notice netifd: Network device 'tun0' link is up
Fri Sep  6 09:31:21 2019 daemon.notice netifd: Interface 'VPNBook' has link connectivity
Fri Sep  6 09:31:21 2019 daemon.notice netifd: Interface 'VPNBook' is setting up now
Fri Sep  6 09:31:21 2019 daemon.notice netifd: Interface 'VPNBook' is now up
Fri Sep  6 09:31:21 2019 user.notice firewall: Reloading firewall due to ifup of VPNBook (tun0)
Fri Sep  6 09:31:23 2019 daemon.notice openvpn(VPNBook_US1)[12541]: /sbin/route add -net 198.7.62.204 netmask 255.255.255.255 gw 192.168.1.254
Fri Sep  6 09:31:23 2019 daemon.notice openvpn(VPNBook_US1)[12541]: /sbin/route add -net 0.0.0.0 netmask 128.0.0.0 gw 10.8.0.69
Fri Sep  6 09:31:23 2019 daemon.notice openvpn(VPNBook_US1)[12541]: /sbin/route add -net 128.0.0.0 netmask 128.0.0.0 gw 10.8.0.69
Fri Sep  6 09:31:23 2019 daemon.notice openvpn(VPNBook_US1)[12541]: /sbin/route add -net 10.8.0.1 netmask 255.255.255.255 gw 10.8.0.69
Fri Sep  6 09:31:23 2019 daemon.notice openvpn(VPNBook_US1)[12541]: Initialization Sequence Completed
```

If you do not see **'Initialization Sequence Completed'**, then it indicates there is a problem with the VPN connection. The router may be misconfigured, or there is a problem with the VPN provider.

Go to `Network -> Interfaces` menu, and the `tun0` interface should look like the following image.

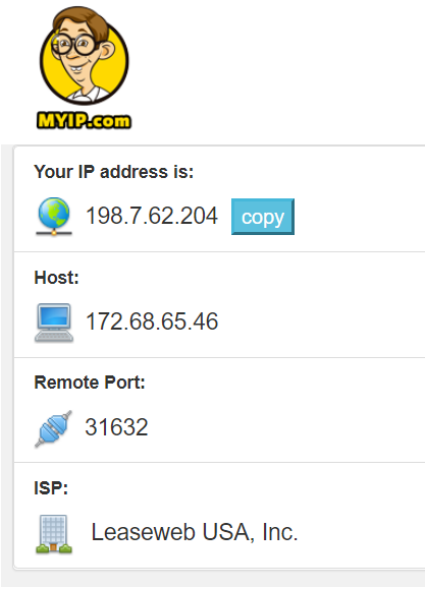
Protocol: Unmanaged
Uptime: 0h 2m 27s
RX: 7.40 MB (7897 Pkts.)
TX: 1.03 MB (6718 Pkts.)

Testing VPN tunnel

Then check the PC is able to access the internet with a web browser through the VPN service.

You can verify your public IP address has changed to the one provided by your VPN service provider:

- myip.com
- whatismyipaddress.com



If you are unable to bring up any web page, there is probably a DNS resolver issue. OpenWrt uses the DNS servers known to the WAN interface, and these may be unreachable via the VPN tunnel.

Ping a known website by its IP address to verify whether there is internet connectivity, but note that some VPN providers such as VPNbook may block use of ICMP Ping.

```
C:\Users\admin>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=14ms TTL=55
Reply from 8.8.8.8: bytes=32 time=15ms TTL=55
Reply from 8.8.8.8: bytes=32 time=15ms TTL=55
Reply from 8.8.8.8: bytes=32 time=15ms TTL=55

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 15ms, Average = 14ms
```

Proceed to section 2.3 to set up the DNS resolvers.

Remember to complete the steps in section 3 to resolve a number of known bugs with the HH5a.

2.3 DNS Resolvers and Leak Protection

The HH5a will be using the default DNS servers defined by the WAN interface connection. This will usually be your ISP's DNS servers, or your local DNS server. This is likely to be 'undesirable' from a privacy point of view or may be blocked by your ISP when using the VPN tunnel.

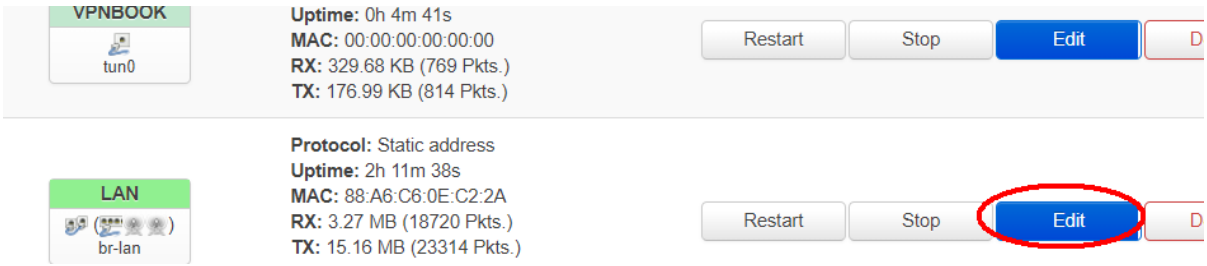
Most VPN service providers offer their own internal DNS servers for additional privacy.

Unlike DDWRT or Tomato OpenVPN client implementations, there isn't a simple toggle setting to enable OpenVPN users on OpenWrt to choose to use the internal DNS servers provided by their VPN service provider.

If you know the IP addresses of your VPN provider's DNS servers, complete the following additional instructions. Otherwise, consider using OpenDNS or Google DNS servers.

Using LuCI, go to `Network -> Interfaces`

For `LAN` interface, click on `Edit` button



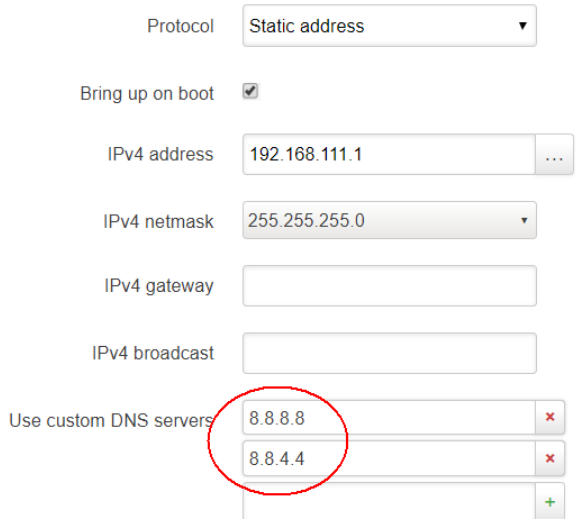
If your VPN provider does not offer their own DNS servers, you may wish to use:

Google servers: `8.8.8.8` and `8.8.4.4`

OpenDNS servers: `208.67.222.222` and `208.67.220.220`

Cloudflare DNS servers: `1.1.1.1` and `1.0.0.1`

Edit the 'Use custom DNS servers' boxes as in example shown below.

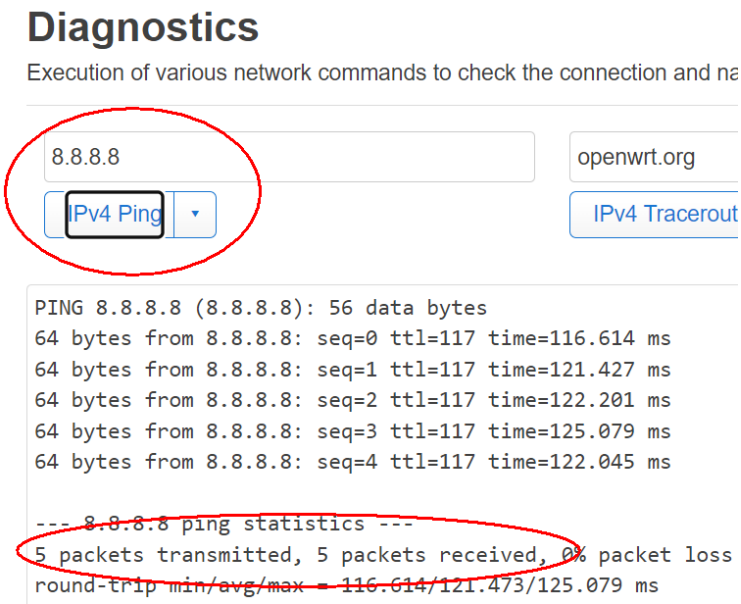


Press 'Save' button.

Press 'Save & Apply' button at bottom of the page.

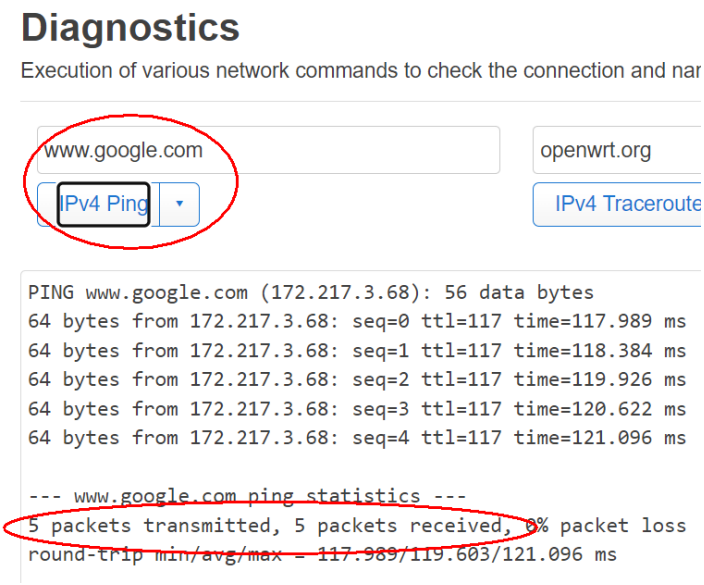
Using LuCI, go to Network -> Diagnostics

Now to ping a known host such as Google's DNS server 8.8.8.8



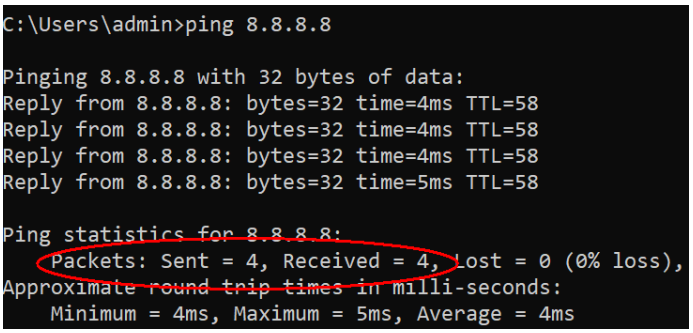
If the results returns "0 packets received", there is likely to be a problem with the configuration (unless the VPN provider blocks use of ping command). Check the VPN instance is started and/or has not stopped prematurely. Review the contents of settings for the VPN instance, username & password, and firewall zone settings.

Ping a known host such as `www.google.com`

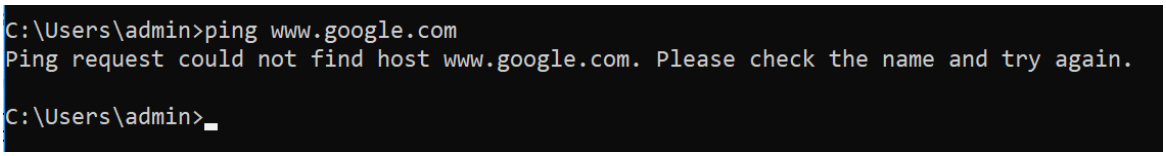


If the results returns "`0 packets received`", there is likely to be a problem with the DNS servers you have specified. (unless the VPN provider blocks use of ping command)

Using the computer connected to the LAN port, check it has internet access. Try pinging known IP address and host.



If the results returns "`0 packets received`", there is likely to be a problem with the firewall on the OpenWrt router. In LuCI, go to `Network -> Firewall` Review the `Zones` settings for the `Lan`.



If you see the above error message, there is likely to be a problem with the DNS settings.

If you explicitly wish your connected wired and wireless devices to directly access the DNS servers, you can complete the following optional procedure:

Click on `DHCP Server` tab.

Click on `Advanced Settings` tab.

In the box 'DHCP-Options', enter you new DNS servers, prefixed with '6,' and if there is more than one server, separated by comma, ','.

eg. for Google servers 8.8.8.8 and 8.8.4.4, the line would be:

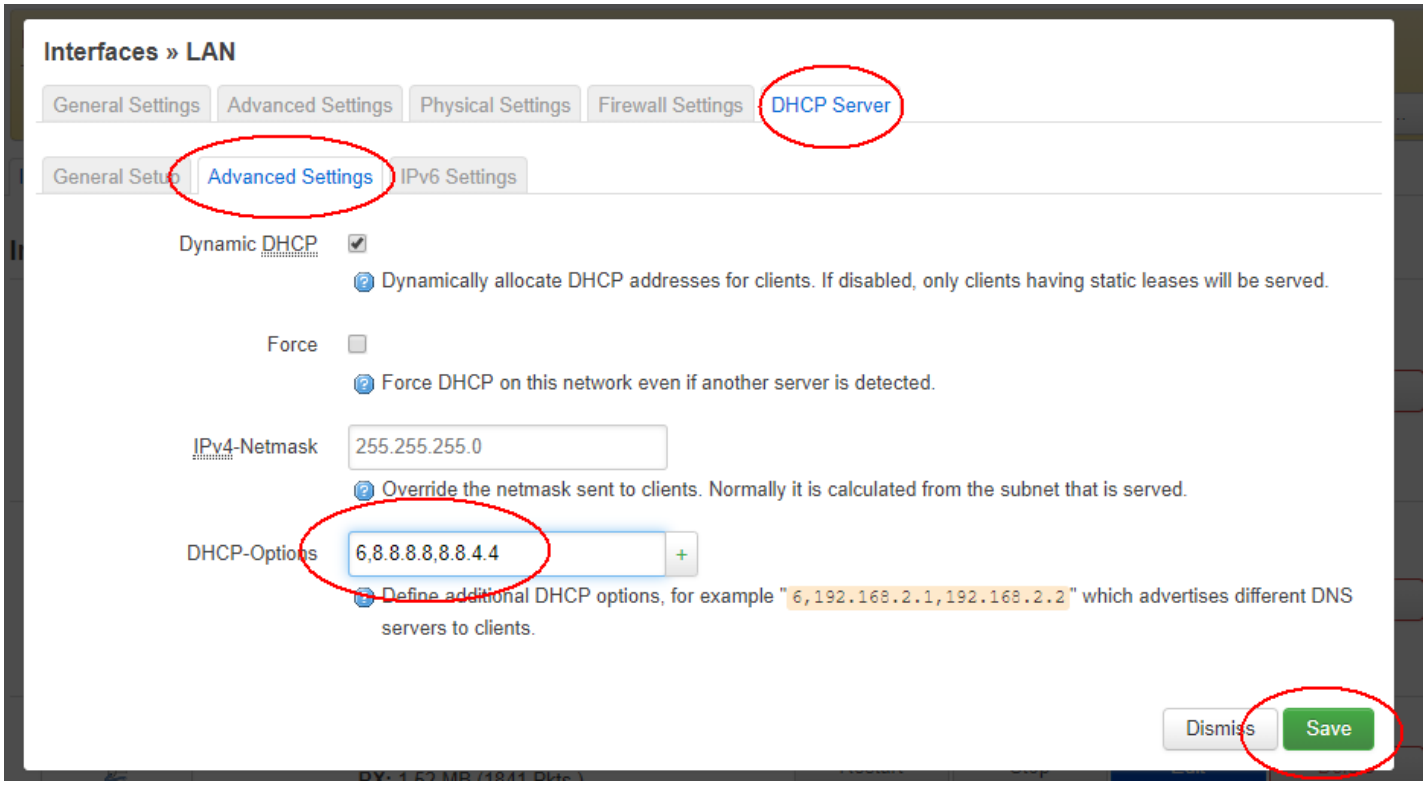
```
6,8.8.8.8,8.8.4.4
```

for OpenDNS servers 208.67.222.222 and 208.67.220.220, the line would be:

```
6, 208.67.222.222, 208.67.220.220
```

for recently launched Cloudflare DNS servers 1.1.1.1 and 1.0.0.1, the line would be:

```
6,1.1.1.1,1.0.0.1
```



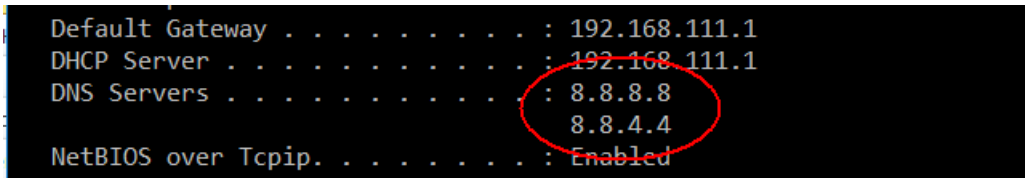
Press 'Save' button.

Press 'Save & Apply' button at the bottom of the page.

Disconnect and reconnect the PC from the HH5a to force it to acquire new DHCP supplied settings.

In Windows, open a `cmd` window and enter the command `ipconfig /all`

The new DNS servers should be visible



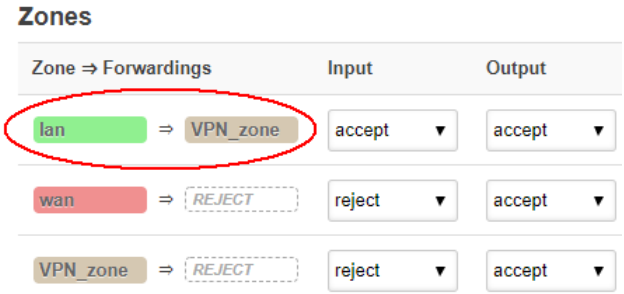
You can test for DNS leaks using this useful website:

https://dnsleaktest.com/

2.4 Kill switch

By completing the instructions described earlier in this guide, a 'Kill switch' has been added.

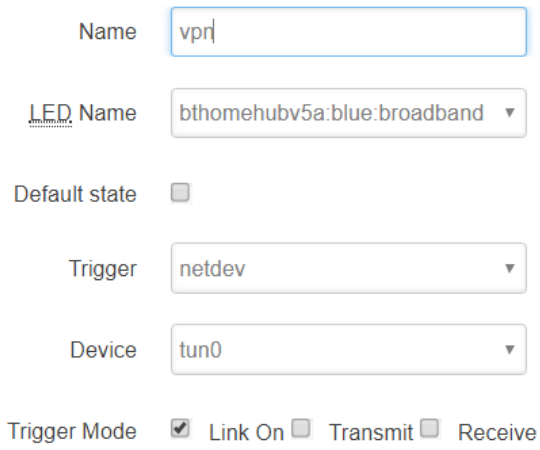
When inspecting the Firewall Zones, it can be observed all LAN traffic is directed towards the VPN firewall zone only. ie. if the VPN connection should fail, `LAN` traffic will not be directed to the `WAN` interface.



2.5 LED configuration

Go to `System -> LED Configuration` menu. You may wish to edit the existing LED configuration for 'Internet' as shown below. The 'b' (broadband) indicator will light up while the HH5a is connected to the VPN service provider.

Edit the settings by renaming the original '`dsl`' LED configuration as shown below:



2.6 System Log spammed by odhcp messages

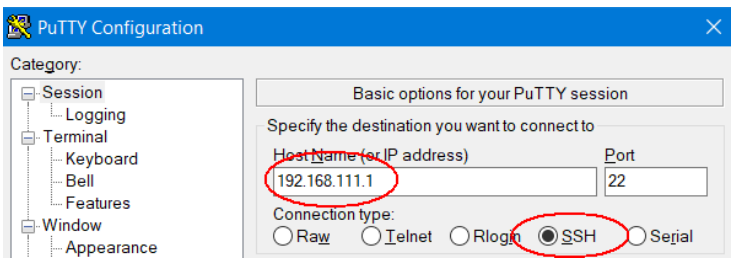
If you discover the System Log is being repeatedly spammed with `odhcpd` messages as in example below:

```
Wed Oct 18 22:58:53 2017 daemon.info odhcpd[643]: Using a RA lifetime of 0 seconds on br-lan
Wed Oct 18 23:05:34 2017 daemon.info odhcpd[643]: Using a RA lifetime of 0 seconds on br-lan
Wed Oct 18 23:11:58 2017 daemon.info odhcpd[643]: Using a RA lifetime of 0 seconds on br-lan
Wed Oct 18 23:17:07 2017 daemon.info odhcpd[643]: Using a RA lifetime of 0 seconds on br-lan
Wed Oct 18 23:19:07 2017 daemon.info odhcpd[643]: Using a RA lifetime of 0 seconds on br-lan
Wed Oct 18 23:19:12 2017 daemon.info odhcpd[643]: Using a RA lifetime of 0 seconds on br-lan
Wed Oct 18 23:20:20 2017 daemon.info odhcpd[643]: Using a RA lifetime of 0 seconds on br-lan
```

Here is the explanation for the above example.

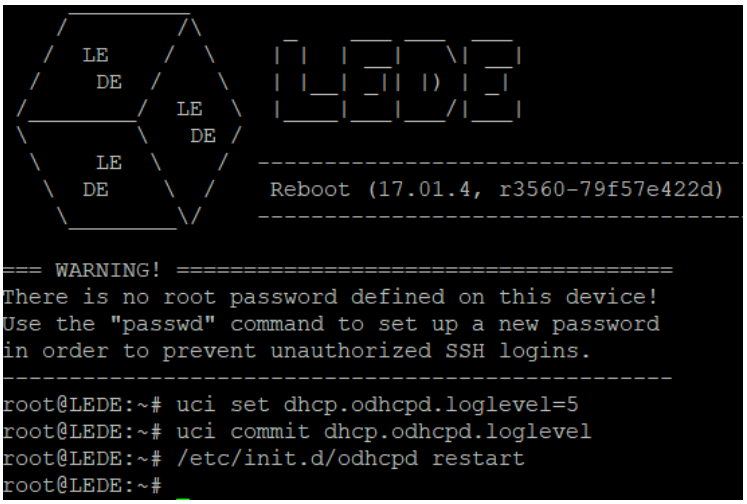
> https://bugs.OpenWrt.org/index.php?do=details&task_id=1274
>
> "As such the frequency and contents of the trace is completely normal; the trace is there for trouble shooting purposes (which is often required if people complain about IPv6 connectivity issues) but if you want to suppress the trace you can set the loglevel uci parameter to 0 in the `dhcp odhcpd uci` section."

To change the `loglevel`, open a SSH session using PuTTY to the HH5a.



Changing the `loglevel` from default of 6 to 5 will suppress `info` messages from `odhcpd`. (The `loglevel` of 4 can suppress `info` and `notice` messages) Execute the following three commands by copying each line and pasting into PuTTY:

```
uci set dhcp.odhcpd.loglevel=5
uci commit dhcp.odhcpd.loglevel
/etc/init.d/odhcpd restart
```



The above UCI commands will add a `loglevel` line to the `/etc/config/dhcp` file.

```
config odhcpd 'odhcpd'
   option maindhcp '0'
   option leasefile '/tmp/hosts/odhcpd'
   option leasetrigger '/usr/sbin/odhcpd-update'
   option loglevel '5'
```

If you see these similar messages with later versions of OpenWrt:

```
Thu Oct 10 08:20:13 2019 daemon.notice odhcpd[1016]: Sending a RA on lan
Thu Oct 10 08:29:13 2019 daemon.notice odhcpd[1016]: Sending a RA on lan
Thu Oct 10 08:36:34 2019 daemon.notice odhcpd[1016]: Sending a RA on lan
Thu Oct 10 08:43:46 2019 daemon.notice odhcpd[1016]: Sending a RA on lan
Thu Oct 10 08:47:15 2019 daemon.notice odhcpd[1016]: Sending a RA on lan
Thu Oct 10 08:51:42 2019 daemon.notice odhcpd[1016]: Sending a RA on lan
Thu Oct 10 08:55:25 2019 daemon.notice odhcpd[1016]: Sending a RA on lan
Thu Oct 10 09:01:34 2019 daemon.notice odhcpd[1016]: Sending a RA on lan
```

Changing the `loglevel` from default of 6 to 4 will suppress `notice` messages from `odhcpd`. (The `loglevel` of 4 can suppress `info` and `notice` messages) Execute the following three commands by copying each line and pasting into PuTTY:

```
uci set dhcp.odhcpd.loglevel=4
uci commit dhcp.odhcpd.loglevel
/etc/init.d/odhcpd restart
```

2.7 OpenWrt 19.07 information

OpenWrt 19.07 currently includes OpenVPN client 2.4.7. This v1.2 guide has been refreshed for OpenWrt 19.07 only. If you are looking for instructions for LEDE 17.01 or OpenWrt 18.06, please download the older v1.1 guide.

There have also been changes to LuCI since the early availability of OpenWrt 19.07-snapshots. This guide has been refreshed based on OpenWrt 19.07.0-rc1 stable release.

There are some issues which I have witnessed when testing OpenWrt with my VPN provider:

- When attempting to change the `LAN` IP address, the `auto rollback` prompt does not appear if both `WAN` and `LAN` IP addresses are on the same subnet (eg. 192.168.1.x). To resolve the problem, change the `LAN` IP address first BEFORE allowing any IP address to be assigned to the `WAN` interface. Section 2.1 has been revised following this discovery.

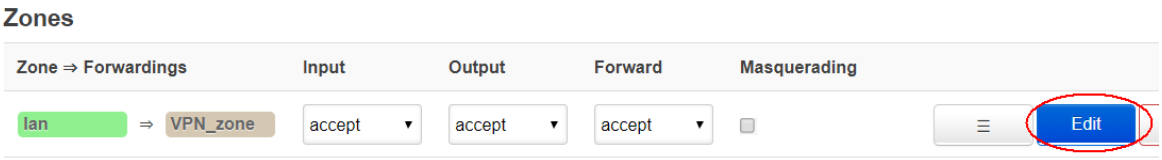
New to OpenWrt 19.07, is the ability to upload and edit the `.ovpn` configuration file saved directly to the `/etc/config/openvpn` folder using LuCI. However, you may still have to use WinSCP or other tool to upload/edit any other files provided by the VPN service provider.

2.8 How to upgrade OpenWrt

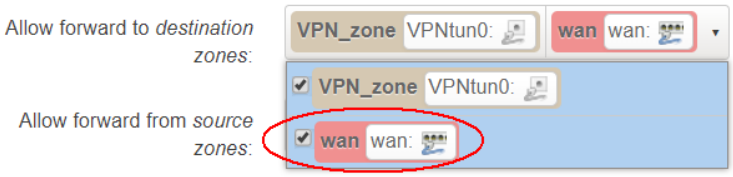
2.8.1 Upgrading to 19.07.x

If you already possess a HH5a with LEDE 17.01 or OpenWrt 18.06 configured with working OpenVPN client as described in previous versions of this document, and wish to upgrade to OpenWrt 19.07, then I recommend the following summarised procedure for the HH5a. It involves temporarily disabling the VPN and re-instating normal internet access through the router.

Navigate to LuCI `> Network > Firewall` Click on `Edit` button for the `lan` zone.



Add the `wan` zone as shown below to the '`Allow forward to destination zones`'. This removes the 'Kill Switch' when the VPN is not active.

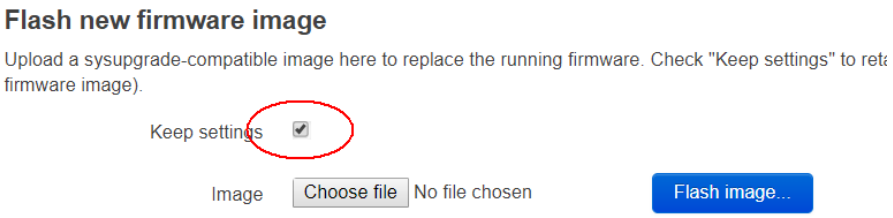


Navigate to LuCI > `VPN > OpenVPN`. Untick box for the active VPN instance. Then press '`Save & Apply`' button. The '`stop`' button should change to '`start`' as shown below. You may need to restart the router.

Use a web browser and confirm the router is connected to your ISP. eg. visit `myip.com`

Download the latest OpenWrt firmware, and navigate to LuCI > `System > Backup/Flash firmware`.

Ensure 'Keep settings' is enabled as shown below, and flash the new firmware to the router.

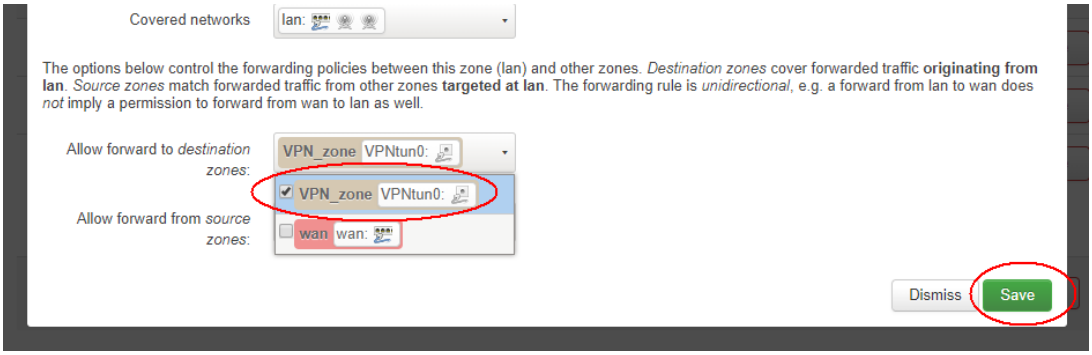


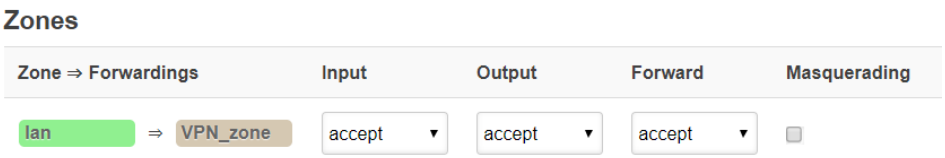
After the new firmware is installed, navigate to LuCI > `System > Software`. Click on `Update lists…` button.

Install the '`openvpn-openssl`' and '`luci-app-openvpn`' packages (as described in section 2.1)

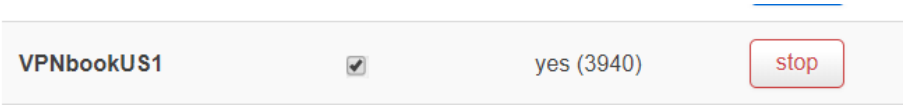
Remove the `wan` from the `lan` firewall zone to reinstate the 'Kill switch'.

(Added) For '`Allow forward to destination zones`' uncheck '`wan`' to the newly created '`VPN_zone`' as shown below.



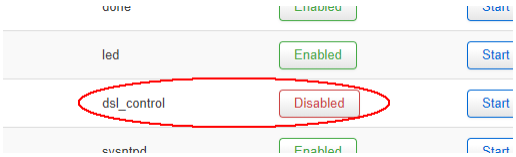


Enable the VPN by ticking the check box and pressing '`Save & Apply`' button. You may need to press the '`Start`' button too.



Use a web browser and go to `myip.com` to confirm VPN is active.

For HH5A, remember to disable `dsl_control` as described in section 3.1



2.8.2 Upgrading to 21.02.x (LuCI bug)

The procedure described in section 2.8.1 has always worked for 18.06 and 19.07 for a number of different model routers I own which have very basic openvpn client configuration.

For HH5a, upgrading from 19.07 to 21.02 is not much different to previous versions of OpenWrt while keeping settings. **Warning:** for other devices which have been migrated to the new DSA architecture, it is NOT possible to keep settings when upgrading to 21.02.

If you discover LuCI fails to load after upgrading to 21.02.0 and keeping existing settings, you may have to make 2 changes, if clearing the browser cache, and opening LuCI using incognito window in Chrome, or InPrivate window in Edge browser etc. fails to resolve the problem.

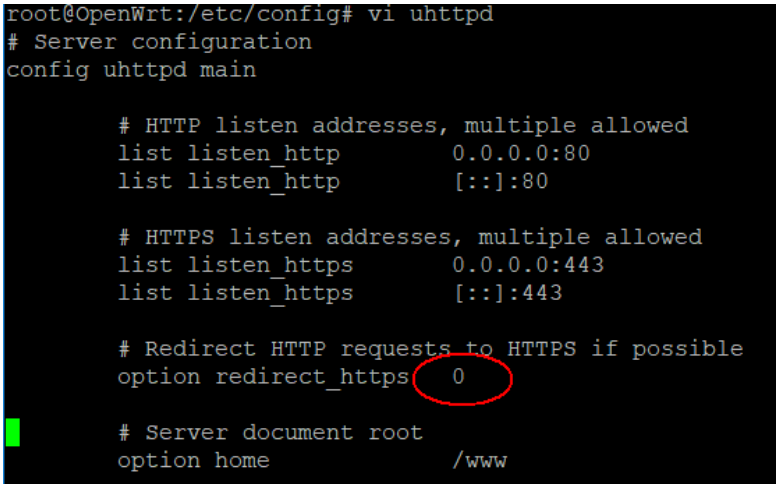
Use VI or WinSCP, locate and edit the file `/etc/config/uhttpd`

Locate the following line:

```
option redirect_https       1
```

Change line to read:

```
option redirect_https       0
```



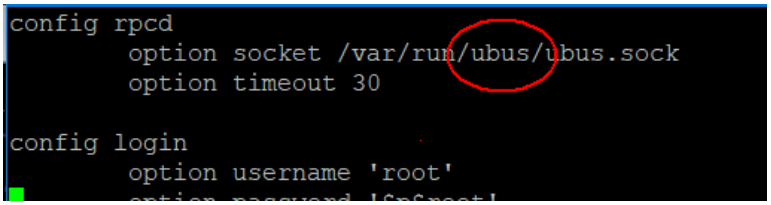
Use VI or WinSCP, locate and edit the file `/etc/config/rpcd`

Locate the following line:

```
option socket /var/run/ubus.sock
```

Change the line to read:

```
option socket /var/run/ubus/ubus.sock
```



Reboot the HH5a and LuCI should appear.

2.8.3 Upgrading to 22.03.x or 23.05.x

It is NOT possible to directly upgrade and keep configuration settings from versions of OpenWrt prior to 22.03.

OpenWrt 22.03 for HH5a moves from using legacy Switch architecture to new DSA.

Similarly, upgrading from 22.03 to 23.05 did not retain settings for some devices I tested. It may be because 23.05 introduces new Firewall 4.

When you install OpenWrt 22.03/23.05 sysupgrade.bin using LuCI, you MUST untick the 'Keep Settings' check box. You may also need to tick the 'Force Upgrade' checkbox to continue. After installation, go to 192.168.1.1 and set up the HH5a from scratch for basic internet access.

After installing the packages `openvpn-openssl` and `luci-app-openvpn`

You can then use Windows tools such as WinSCP to restore the following openvpn files and folders.

Configuration file:	`/etc/config/openvpn`
Contents of the folder:	`/etc/openvpn/`

2.9 Simple VPN and non-VPN access with HH5A, up to 21.02

(Sep 2021): Note this procedure does NOT work with devices which use DSA, such as HH5a with very latest development snapshots or OpenWrt 22.03.

This may be a ‘simpler’ alternative to using ‘VPN Bypass’ and ‘Policy Based Routing (PBR)’ offered by OpenWrt.

There may be a situation where you wish to configure the wifi on the HH5A so you can choose between whether a wifi device uses the VPN, or not. For example, you may wish devices which are connected to 2.4 GHz wifi or LAN interface to use VPN, but devices connected to 5 GHz wifi are NOT to use VPN.

Normally, I would recommend you simply connect your wifi device to your existing wifi network if you do not require VPN.

Please note the proposed solution only works because the WAN port of the HH5A is wired to the LAN port of the main ISP facing router.

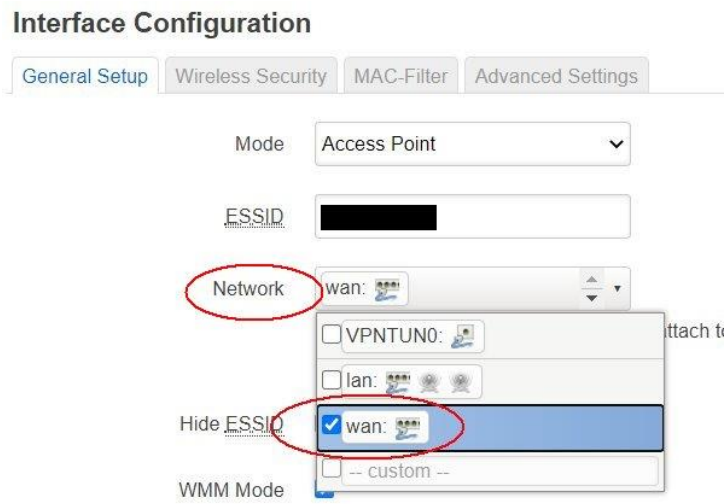
> If your openvpn client router **is connected direct to your internet service provider**, this proposed solution **must NOT be attempted and it will NOT work!**

By bridging a wifi interface to the WAN port on the HH5A, your wifi devices will connect to the LAN interface of your existing ISP facing router, which will serve a DHCP IP address to your device, to enable it to connect to the internet.

In LuCI, navigate to **Network > Wireless**

Click 'Edit' for the wireless interface which will **not** be used for VPN.

Change the `Network` setting from `LAN` to `WAN`.



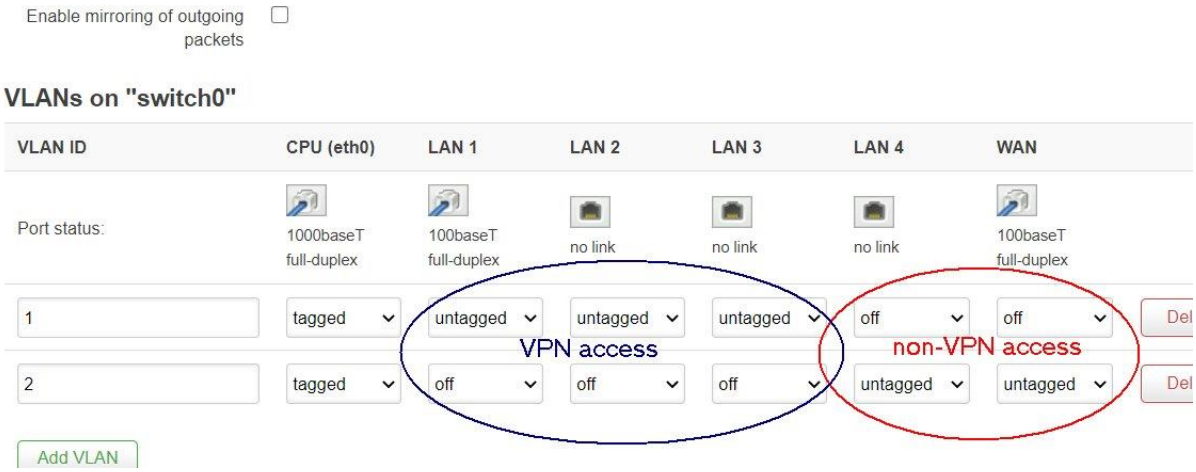
Save the settings.

Similarly, the HH5A OpenWrt client router is installed in another room, and wired to LAN interface of the main ISP facing router by a long ethernet cable. There may be a situation where you want to provide an extra ethernet connection but do not wish to install an ethernet switch or lay additional cables to the same room as the HH5A.

> If your openvpn client router **is connected direct to your internet service provider**, this proposed solution **must NOT be attempted and it will NOT work!**

The HH5A has four LAN ports. You can reconfigure one or more ethernet ports so they are bridged to the original WAN interface. In example below, I have bridged former `LAN 4` port to the `WAN` port.

Navigate to **LuCI -> Network -> Switch**



`LAN 4` port is connected to the ISP facing router's LAN. ie. Does NOT use the VPN.

Any ethernet device plugged into the `LAN 4` port will bypass the VPN and connect to the existing network for regular internet access.

2.10 Troubleshooting

2.10.1 Hub One (stock firmware) blocking VPN

A reader recently reported a problem connecting to three different party VPN providers, namely PureVPN, VPNbook and ProtonVPN.

Their main ISP facing router is a Plusnet Hub One running stock firmware (firmware 4.7.5.1.83.8.263) and connecting to Plusnet broadband service. They were trying to configure a HH5a with OpenWrt 19.07.5 and Openvpn client.

When trying to connect to VPNbook, the system log displayed the following messages which were repeated. There was no '`Initialisation Completed`' message.

daemon.notice openvpn(PureVPN)[15279]: TCP/UDP: Preserving recently used remote address: [AF_INET]5.254.77.10:53

daemon.notice openvpn(PureVPN)[15279]: UDP link local: (not bound)

daemon.notice openvpn(PureVPN)[15279]: UDP link remote: [AF_INET]5.254.77.10:53

daemon.err openvpn(PureVPN)[15279]: TLS Error: TLS key negotiation failed to occur within 60 seconds (check your network connectivity)

daemon.err openvpn(PureVPN)[15279]: TLS Error: TLS handshake failed

daemon.notice openvpn(PureVPN)[15279]: SIGUSR1[soft,tls-error] received, process restarting

After some trial and error, adding the IP address of the OpenWrt HH5a into the Hub One's DMZ resolved the problem for when using UDP. DMZ is not required for TCP connections.

There have been no other similar reports from other readers when using HH5a or Hub One with stock firmware.

2.10.2 AEAD Decrypt error: bad packet ID (may be a replay)

I was installing openwrt 22.03.5 on linksys EA6350 v3, and observed this error messages in the System log. They were appearing every few seconds when streaming video through the vpn connection.

> AEAD Decrypt error: bad packet ID (may be a replay): [#] -- see the man page entry for --no-replay and --replay-window for more info or silence this warning with --mute-replay-warnings

Using mssfix parameter within the .ovpn file did not resolve the issue.

This was caused by using a wireless bridge (all devices on same LAN subnet 192.168.10.x). The WAN ethernet port from the EA6350 v3 was connected to the bridge, and the bridge connects wirelessly to my home wifi.

I was able to reproduce the issue with two different wireless bridges. Old Belkin f7d4302 (Broadcom) running FreshTomato using 2.4 GHz, and Asus RT-AC57u (MT7621) running Padavan using 5 GHz.

When I hard wired the Linksys EA6350 v3 openwrt router to the home ethernet home LAN, the above error message did not appear.

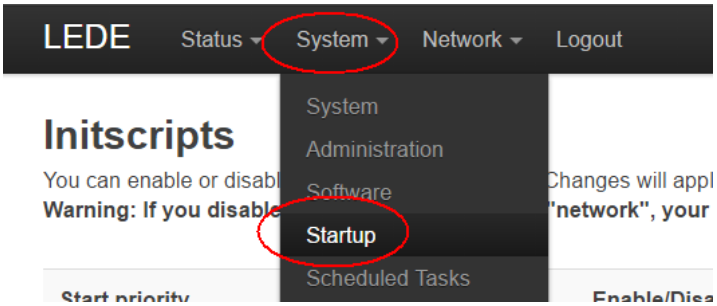
3. Bug fixes for Home Hub 5A

3.1 How to disable ‘dsl_control’ (DSL port)

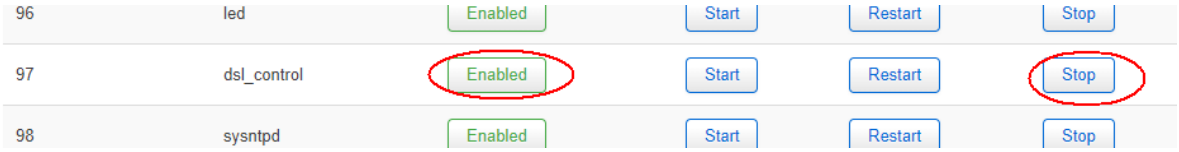
It appears when the DSL port is not being used, a bug in the VDSL app causes unexpected high load, and can eventually cause the HH5a to crash and reboot without warning. This usually occurs within an hour of starting the HH5A. This issue may also affect other modem routers with Lantiq SoC.

In the meantime, it is recommended to disable ‘`dsl_control`’ if the DSL port won’t be used.

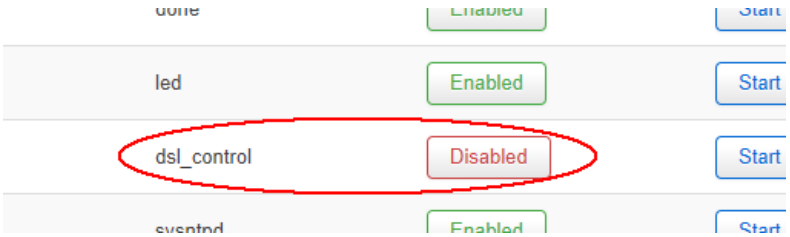
Start LUCI and navigate to `System -> Startup` menu



Scroll down until you find ‘`dsl_control`’. Then click on ‘`Enabled`’ and ‘`Stop`’ buttons.



Ensure that `Disabled` is displayed as shown below.



Optionally, shut down and restart the HH5a.

The DSL port is now disabled.

3.2 Random WAN port MAC address fix

If the HH5a is configured to use the red Ethernet WAN port, you may observe when using DHCP-client, the WAN port acquires a different IP address every time the hub is power-cycled. This is because the WAN port's MAC address has not been defined properly during boot up. A side effect is if the hub is attached to your LAN, it could use up the pool of DHCP IP addresses if the hub is rebooted very frequently. Fortunately, the WAN port's MAC address does not change during DHCP IP address renewal.

For up to OpenWrt 19

To resolve the issue, start LUCI and navigate to `Network -> Interfaces` menu.

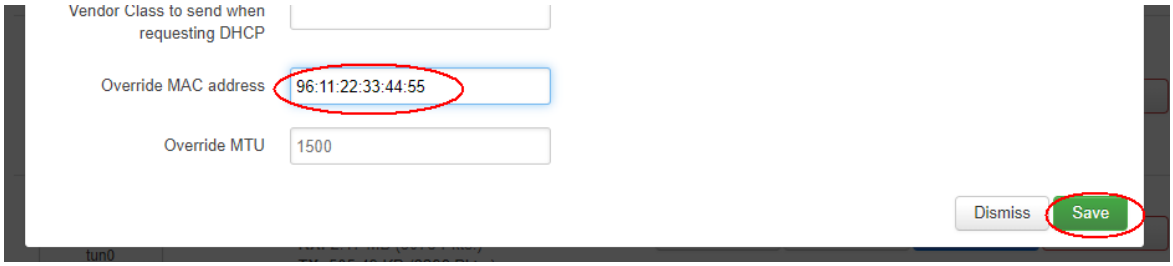
Notice the MAC addresses for the LAN and WAN interfaces are very different in above example.

Click on '`Edit`' and go the '`Advanced Settings`' tab.

Scroll down the page until you find the '`Override MAC Address`' field.

In the above example, the MAC address beginning `'96:6F'` changes every time the hub is power cycled.

Enter a new MAC address. Ensure any address you choose is NOT used elsewhere. You can choose to use the MAC address already shown in the above box such as the address beginning `'96:6F'` if you wish. Ensure the 2nd digit is always an even number, such as '6' in example below.



Press the '`Save`' button

Press the '`Save & Apply`' button at the bottom of the page.

OpenWrt – all versions

The above method is no longer available starting from OpenWrt 21.02, as part of eventual migration to DSA.

Fortunately, you can also fix the problem by editing the `'wan_dev'` section of the `/etc/config/network` configuration file.

For LEDE 17, search for '`ptm0`' as shown below.

For OpenWrt 18, 19 & 21, search for '`dsl0`'

For `dhcp-client` mode

```
config interface 'wan'
      option ifname 'eth0.2'
      option proto 'dhcp'
      option ipv6 'auto'
```

```
config device 'wan_dev'
      option name 'ptm0'          # requires to be changed to 'eth0.2'
      option macaddr 'xx:xx:xx:xx:xx:yy'
```

For LEDE 17, OpenWrt 18 and 19, the existing `'wan_dev'` should be amended to read:

```
config device 'wan_dev'
        option name 'eth0.2'
        option macaddr '78:65:59:ae:fc:51'
```

For OpenWrt 21.02, the `option name` should be changed from `dsl0` to `eth0.2`:

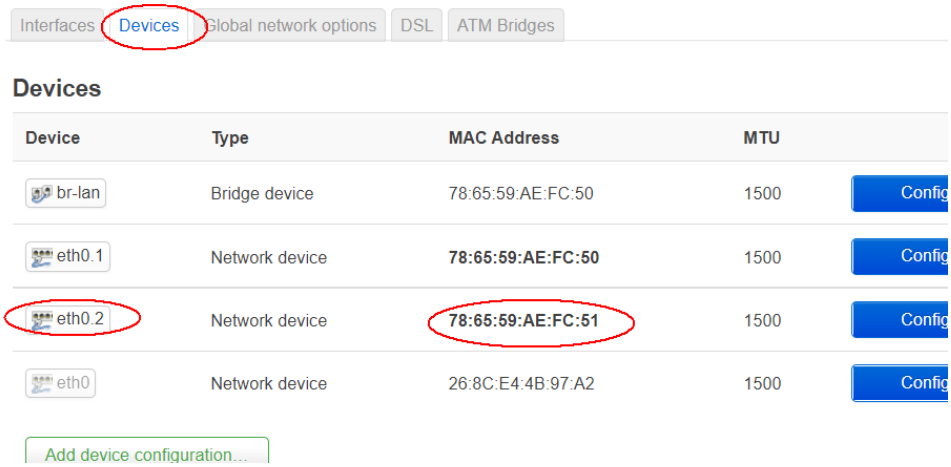
```
config device
        option name 'eth0.2'
        option macaddr '78:65:59:ae:fc:51'
```

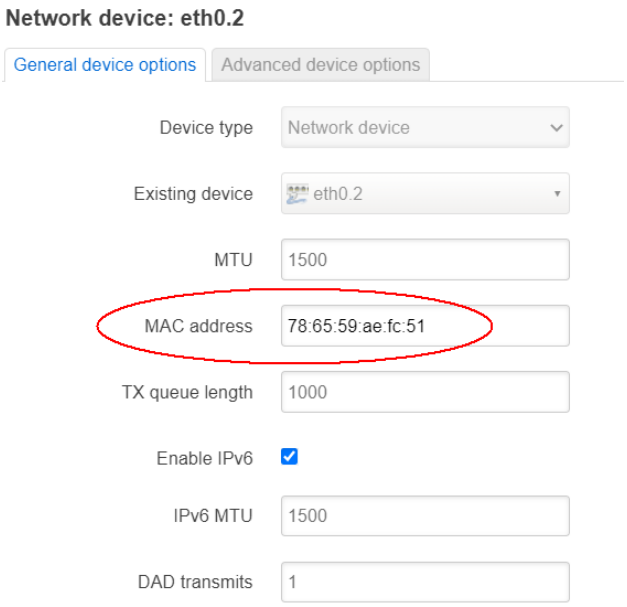
Enter a new MAC address. Ensure any address you choose is NOT in active use elsewhere.

Important: Ensure the 2nd digit is always an even number, such as '8' in above example images.

Note that if you choose to edit the '`option name`' to match what is shown in the `'wan'` section, the `'Override MAC address'` option in LuCI will no longer work in versions of OpenWrt up to 19.07.

For OpenWrt 21.02, navigate to **LuCI -> Network -> Interfaces -> Devices** tab. You can make further changes by clicking on 'Configure' button in future.



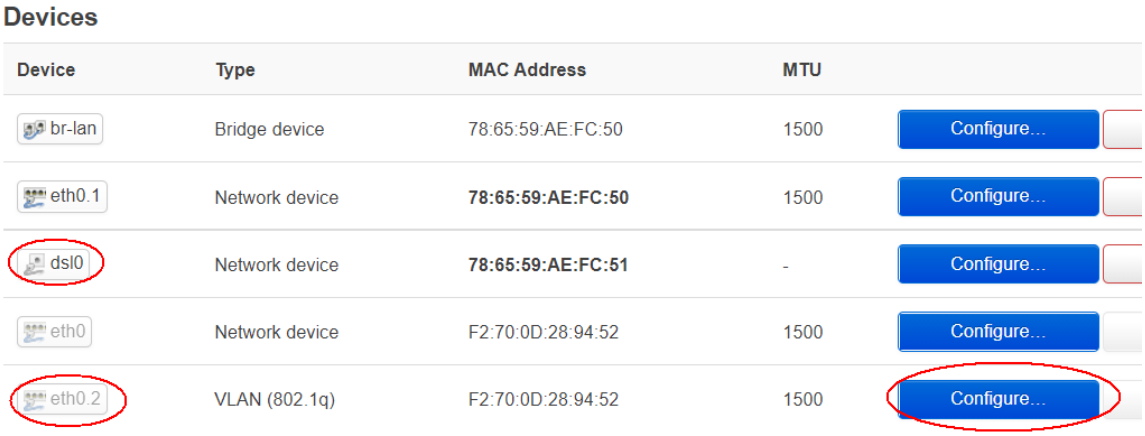


OpenWrt - 21.02

If you don't wish to use SSH and VI, this alternative method also appears to work but may leave your **/etc/config/network** file looking a bit more complicated

Navigate to **LuCI -> Network -> Interfaces -> Devices** tab

Locate the `'eth0.2'` entry and click **Configure** button.

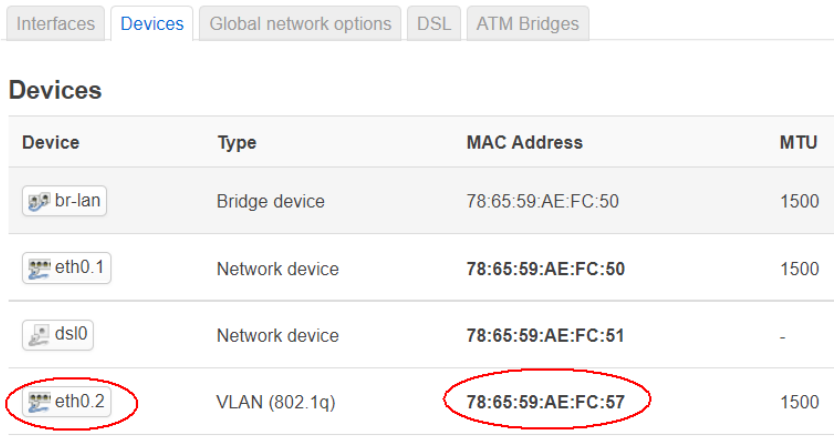


Edit the `MAC address` field as shown below:

Ensure any address you choose is NOT in active use elsewhere.

Important: Ensure the 2nd digit is always an even number, such as '8' in the following example image.

Press the `'Save'` button.



Press the `'Save & Apply'` button.

Now reboot the HH5a for the changes to take effect.

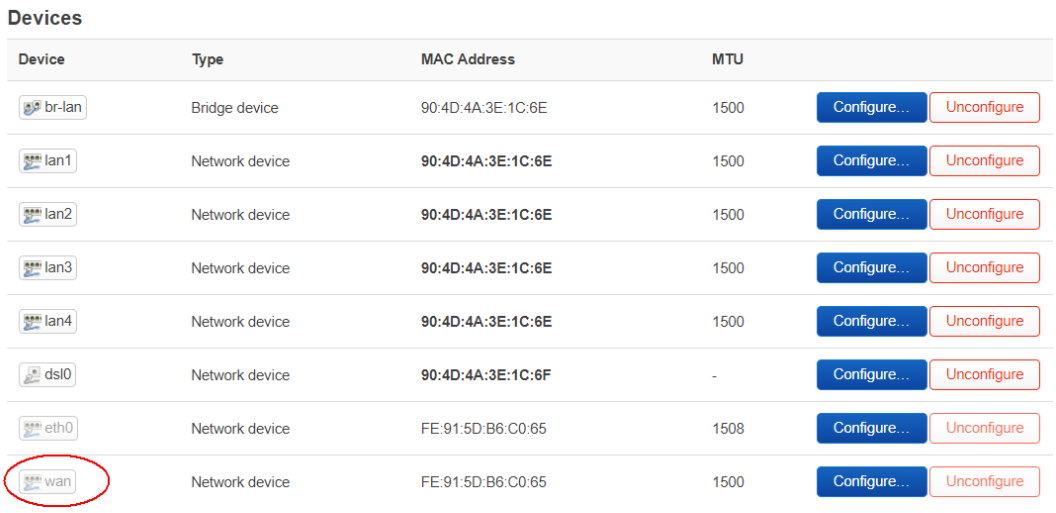
The /etc/config/network file will contain a new section:

```
config device
        option name 'eth0.2'
        option type '8021q'
        option ifname 'eth0'
        option vid '2'
        option macaddr '78:65:59:AE:FC:57'
```

OpenWrt - 22.03 or later

Navigate to **LuCI -> Network -> Interfaces -> Devices** tab

Locate the `'wan'` entry and click **Configure** button.

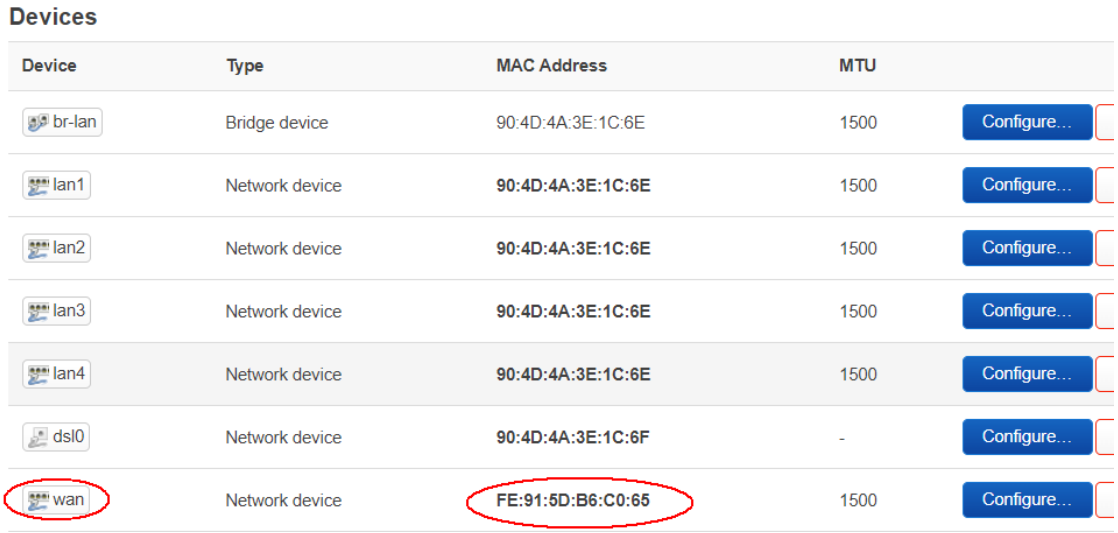


Edit the `MAC address` field as shown below:

Ensure any address you choose is NOT in active use elsewhere.

Important: Ensure the 2nd digit is always an even number, such as '8' in the following example image.

Press the `'Save'` button.



Press the `'Save & Apply'` button.

Now reboot the HH5a for the changes to take effect.

The /etc/config/network file will contain a new section:

```
config device
        option name 'wan'
        option macaddr 'FE:91:5D:B6:C0:65'
```

4. VPN service provider configuration files

The OpenVPN client configuration files can be found on the VPN service providers website.

Some providers choose to include the Certificate and static key within the OVPN file. However, others are known to supply them separately.

Place the ovpn, certificate and key files into the `/etc/openvpn` folder on HH5a.

• CyberGhost (Feb 2024)

Home page: www.cyberghostvpn.com

Required files:
```
.ovpn
ca.crt
client.crt
client.key
```

You may need to add the following into the imported `.ovpn` file if you encounter the IPv6 errors described in this thread: https://forum.openwrt.org/t/use-openvpn-of-cyberghost-on-openwrt/186529/14

```
verb 5

# to block IPv6 traffic necessary on newer clients
pull-filter ignore "route-ipv6"
pull-filter ignore "ifconfig-ipv6"
block-ipv6
```

• ExpressVPN (2018)

Home page: https://www.expressvpn.com

Downloads page: Available to registered users

Required files: `*.ovpn`

`Ensure the .ovpn file includes certificates and`

`keys, otherwise, you will have to specify paths to any additional files.`

Tested: Yes

- ## Hotspot Shield (2018)

Home page: https://www.hotspotshield.com

Downloads page:

Required files: `config.ovpn`

Tested: Yes

- ## IPVanish (2018)

Home page: www.ipvanish.com

Downloads page: www.ipvanish.com/software/configs/

Required files: `*.ovpn`
`ca.ipvanish.com.crt`

Tested: No

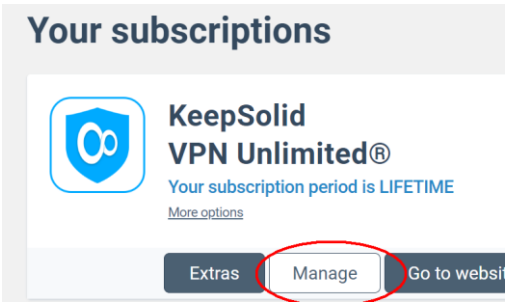
- ## Keepsolid/VPN Unlimited (Dec 2023)

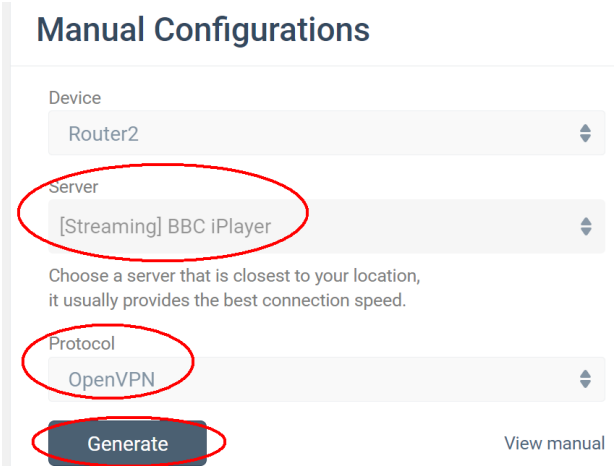
Home page: https://www.vpnunlimitedapp.com

Downloads page: https://my.keepsolid.com/products/vpn/

Log into account and generate unique `ovpn` file for the device.
Username & Password **are not required** when using the `ovpn` file.

Required files: `*.ovpn`





Tested: Yes.

Not the best for torrent users as they only have 3 dedicated torrent servers in Canada, France and Romania. Lifetime subscription (5 connections) has been offered for as little as US$18 from stacksocial.com with discount code in the past.

Update (15 Dec 2023): Openvpn suddenly stopped working on 19.07.10 and 21.02.2 routers. Upon investigation, it looked like new .ovpn files required. However, the new .ovpn files from Keepsolid simply would not work.

For 21.02: I had to open the downloaded .ovpn files in notepad++, copy and paste entire contents into notepad.exe in Windows. Use the new notepad compatible .ovpn file.

For 19.07: OpenWrt/Keepsolid don't support **allow-compression** or **comp-lzo** parameters respectively.

At time of writing, I have not yet ascertained why there is a problem parsing the new .ovpn files into openwrt. I have noted the <ca> section of the new .ovpn files contains two certificates.

The issue is resolved by upgrading to openWrt 22.03.5.

Wireguard protocol is now supported. (Note there are privacy concerns when using wireguard)
https://www.vpnunlimitedapp.com/help/manuals/open-wrt-wireguard-setup

Update (Aug 2021): I briefly tested wireguard client on 21.02-0-rc4 returning 32 mbps in speed tests. Too early to comment on wireguard server reliability/availability – connection is to 'unique' server IP address, and not to a DNS resolved host name.

To fix the time sync issue, this worked for me:
Go to LuCI > System > Startup > 'Local Startup' tab.

Add this dirty quick fix:

```
date -s "2030-01-01 00:00:00"
```

from: https://forum.OpenWrt.org/t/problematic-system/56435/36

Wireguard frequently stops working after a few days especially if the wireguard router is turned off for any length of time. It then requires new config to be generated and applied to the openwrt router to resolve the problem. This can be frustrating (This is not an issue when using openvpn)

- ## Mullvad (2019)

Home page:	https://www.mullvad.net
Downloads page:	https://www.mullvad.net/download/config/
Required files:	`*.ovpn` (Download the Android version)
Tested:	Yes.

No longer provide free 3 hour trials since April 2019.

Wireguard also supported:
https://mullvad.net/en/help/running-wireguard-router/

- ## NordVPN (2018)

Home page:	http://www.nordvpn.com
Downloads page:	https://nordvpn.com/api/files/zip
Required files:	`*.ovpn`

Tested: Yes

3 day free trial available.

Nord also supports wireguard:
https://support.nordvpn.com/Connectivity/Router/1047411192/OpenWrt-CI-setup-with-NordVPN.htm

- ## PIA (2018)

Home page: https://www.privateinternetaccess.com/

Downloads page:

https://helpdesk.privateinternetaccess.com/hc/en-us/articles/218984968-What-is-the-difference-between-the-OpenVPN-config-files-on-your-website-

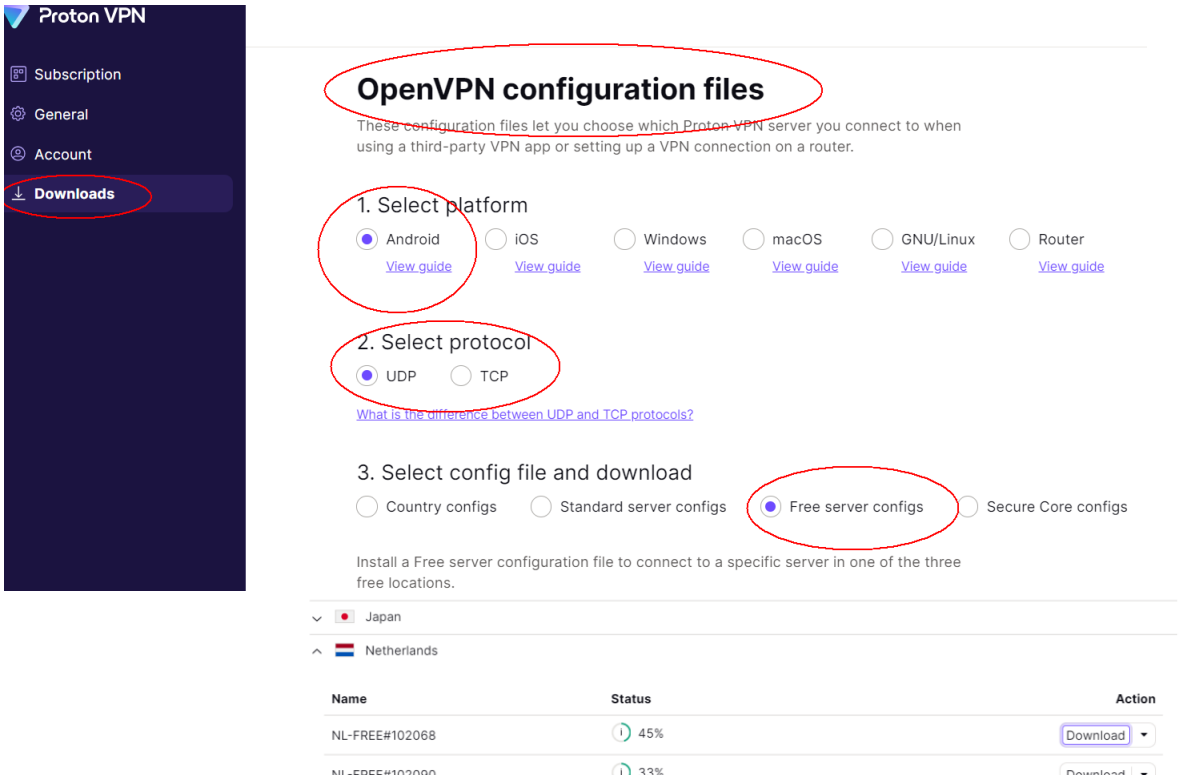
Required files:
```
*.ovpn
ca.rsa.2048.crt
ca.rsa.2048.pem
```

Tested: No

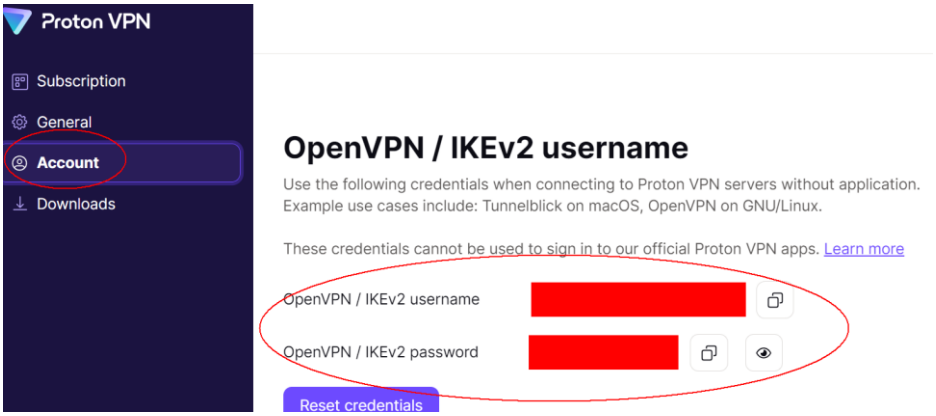
- ## ProtonVPN (Dec 2023)

Home page: https://protonvpn.com/

Required files: `*.ovpn`



OpenVPN username & password located here:



Tested: Offer free account to access their free USA, Netherland and Japan servers.

nb. openvpn username/password are not the same as Account username/password.

- ## PureVPN (2019)

Home page:	www.purevpn.com
Downloads page:	https://support.purevpn.com/openvpn-files
Required files:	`*.ovpn` `ca.crt` for v1 files only `Wdc.key` for v1 files only
Tested:	Yes

2021: PureVPN now offer two different versions of .ovpn files. The newer v2 files include the certificate and keys within the single file. The older v1 files require separate certificate and key files to be uploaded to the router and .ovpn file edited to point path of these uploaded files.

- ## Surfshark (2018)

Home page:	www.surfshark.com
Downloads page:	https://account.surfshark.com/setup/manual
Required files:	`*.ovpn`
Tested:	Yes.

- ## VPNbook (2018)

Home page:	www.vpnbook.com
Downloads page:	www.vpnbook.com/freevpn
Required files:	`*.ovpn`
Tested:	Yes. Username & Password changes every 2 weeks.

I don't consider this to be a be a safe or secure VPN provider so use with caution.

Update (Jan 2022): VPNbook has proven to be unreliable lately. Consider using ProtonVPN instead.

- ## Zoog VPN (2019)

Home page:	https://zoogvpn.com/
Downloads page:	https://zoogvpn.com/vpn-setup/android
	Log into zoogvpn website to retrieve opvn files.
Required files:	`*.ovpn (Download the Android version)`
Tested:	Yes. Username & Password is same as required to log into zoogvpn account.

Free accounts offer 2GB per month usage allowance and access to UK, NL, US free servers. The free servers use 128 bit instead of 256 bit cipher. Appears to work when briefly tested.