HTTPS VPN Twin Server Quick Start Guide

Rev A
March, 2019

Table of Content

List of Figures

1. Introduction

The HTTPS VPN Twin server solution is an innovative solution to add a VPN server in a private network over which you don't have administrative control, but to which you have physical access, or to add a VPN server in a private network that does not have public IP at all.

Both VPN devices provide WiFi hotspot. Therefore, any smart devices can use the VPN tunnel without a need to install VPN client software.

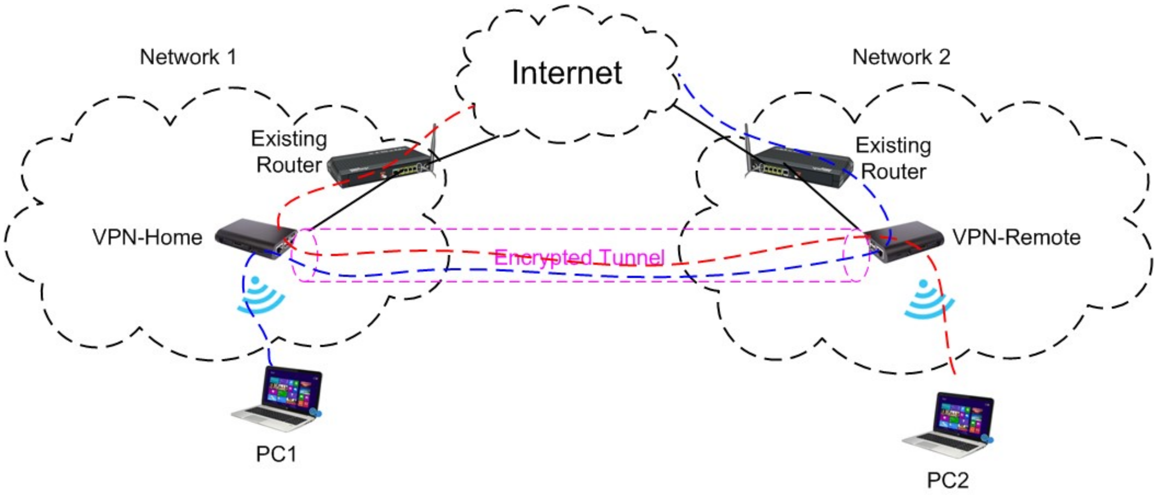


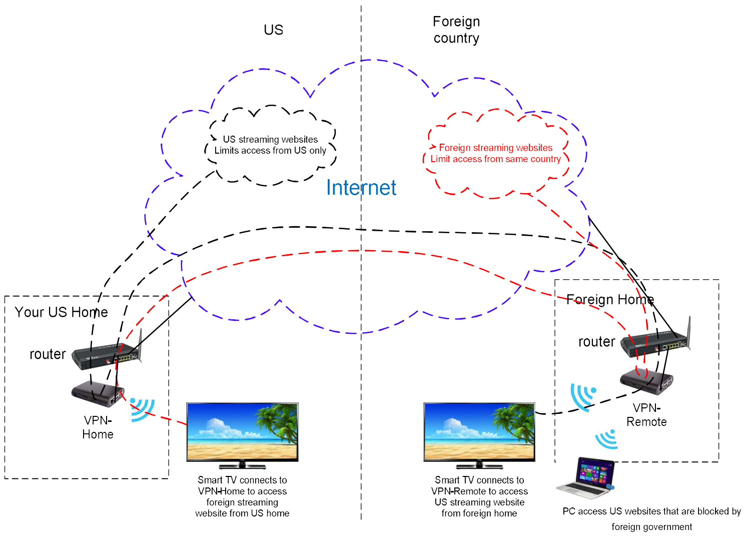
Figure 1 VPN Twin Server Working Model

How It Works

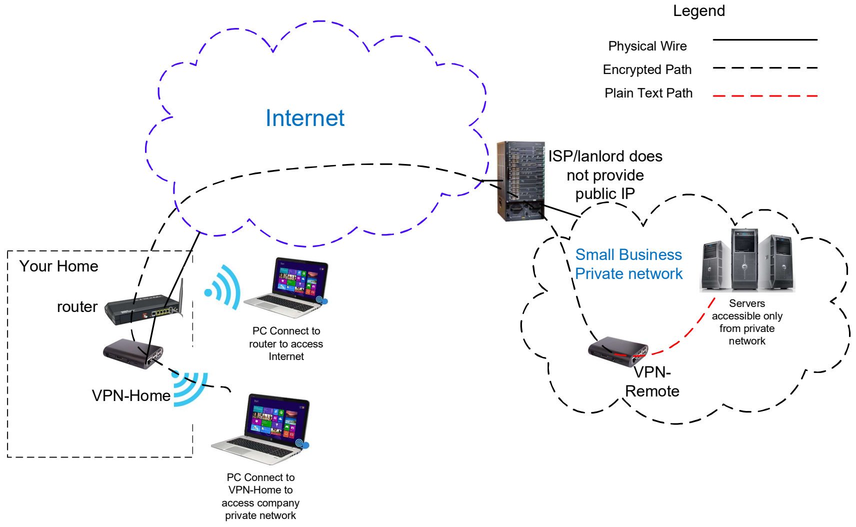
- Plug in the "VPN-Home" device in an existing router that has public IP.
- Configure the public IP of "VPN-Home" in "VPN-Remote" device.
- Plug in "VPN-Remote" device anywhere you want.
- An encrypted tunnel is created between "VPN-Home" and "VPN-Remote". Devices connected to "VPN-Home" WiFi can access the private network where "VPN-Remote" is. And device connected to "VPN-Remote" WiFi can access the home network. (Figure 1)

Typical Use Cases

- Video streaming geo-restricted websites from your home country while you are in US.


US
Foreign country
US streaming websites Limits access from US only
Foreign streaming websites Limit access from same country
Internet
Your US Home
router
VPN-Home
Smart TV connects to VPN-Home to access foreign streaming website from US home
Smart TV connects to VPN-Remote to access US streaming website from foreign home
Foreign Home
router
VPN-Remote
PC access US websites that are blocked by foreign government

- Add a VPN server in a network that does not have a public IP.


Legend
Physical Wire
Encrypted Path
Plain Text Path
Internet
ISP/lanlord does not provide public IP
Small Business Private network
Servers accessible only from private network
VPN-Remote
Your Home
router
VPN-Home
PC Connect to router to access Internet
PC Connect to VPN-Home to access company private network

For questions, comments, supports or customizing solution, please contact us by email.
vpn.everyone@gmail.com

2. Plug VPN Device in Router

1) Connect VPN-Home to wireless router by Ethernet cable
2) Connect USB cable to power up VPN-Home (Figure 2)

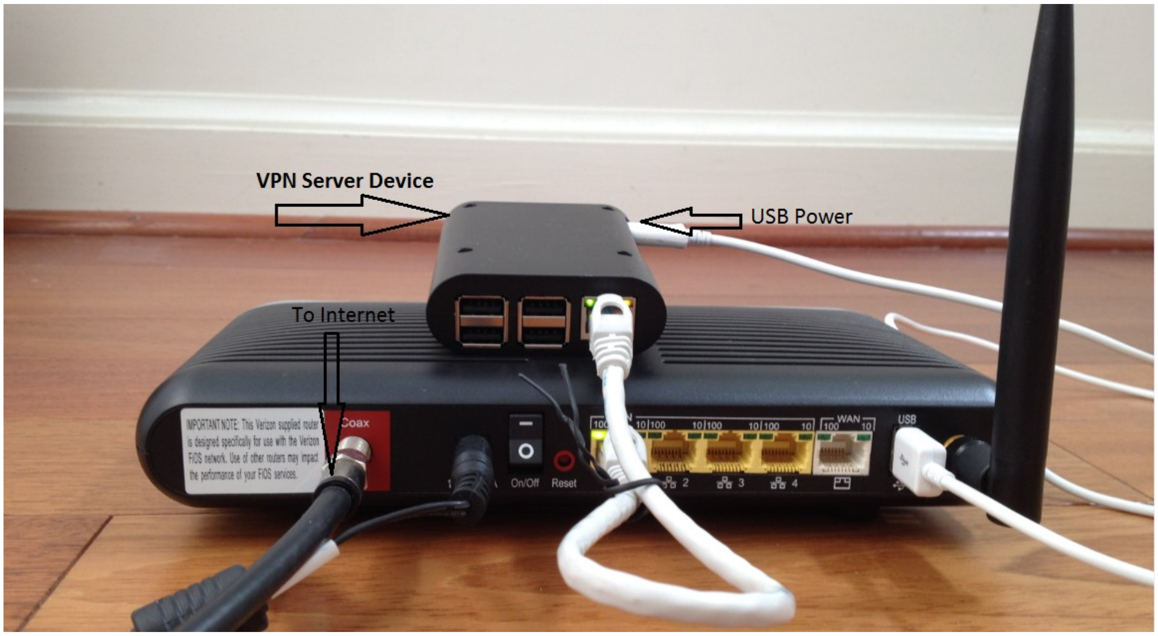


Figure 2 Connect VPN Device to Wireless Router

NOTE:

The figure above is for ***wiring*** illustration purpose**.** Do NOT put VPN server on top (or close to the grill) of your router. Otherwise, the heat generated by your router may drive VPN server to overheat.

Note 1: Ethernet cable is an optional accessory.

Note 2: USB data sync cable is an optional accessory. Please re-use your USB cable for your old Android phones. Nowadays, every household has one or more retired Android phones, therefore USB cables. To save environment, we don't ship USB cables.

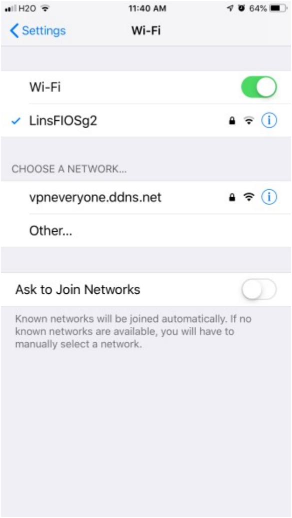
Note 3: The software only runs on the MicroSD card shipped.

Note 4: VPN-Home needs to reside on a network that has public IP. Check your wireless router for the WAN IP. If it's in format of *100.x.x.x, 10.x.x.x, 172.x.x.x or 192.168.x.x,* then your ISP does **not** give you public IP. That means VPN-Home won't work here.

3. Access VPN Device Configuration Web UI

3.1. Access Web UI by WiFi hotspot

VPN-Twin devices come with WiFi hotspot. Go to your iPhone WiFi setting screen. If you see "*vpneveryone.ddns.net*" in your network list, tap it to connect. The default password is *00000000*



Wi-Fi: on

✓ LinsFIOSg2

CHOOSE A NETWORK...

vpneveryone.ddns.net

Other...

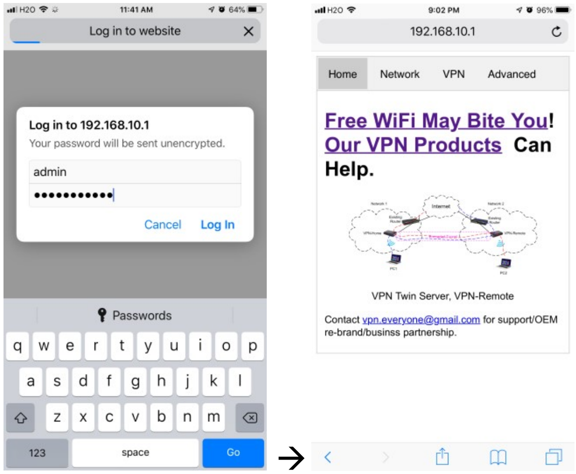
Ask to Join Networks: off

Known networks will be joined automatically. If no known networks are available, you will have to manually select a network.

Figure 3 Find vpneveryone.ddns.net WiFi hotspot

Note: The hotspot may complain about incorrect password. It may take up to 3 times to connect the WiFi hotspot. That is by design to avoid hacker guessing WiFi password.

After your iPhone successfully connects to "*vpneveryone.ddns.net*" WiFi hotspot, start web browser to access http://192.168.10.1 web page. Use "*admin*" & "*vpneveryone*" without quote sign as username and password to login to VPN server web UI.



Log in to 192.168.10.1

Your password will be sent unencrypted.

admin

••••••••••••

Free WiFi May Bite You! Our VPN Products Can Help.

VPN Twin Server, VPN-Remote

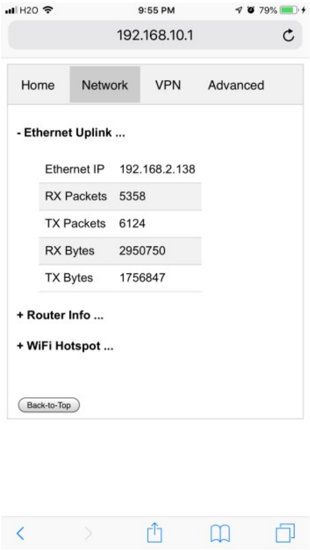
Contact vpn.everyone@gmail.com for support/OEM re-brand/businss partnership.

Figure 4 Access VPN Server Web UI by Built-in WiFi Hotspot

3.2. Access Web UI by VPN Server IP

WiFi hotspot password/network name cannot be changed via WiFi connection. To change WiFi hotspot setting on VPN-Twin devices, you will need to login to device by Ethernet IP.

To find out what IP address the VPN device Ethernet port gets, you can login to your router via WiFi hotspot first. Then click ***Network*** tab. You will see screen like below.



- Ethernet Uplink ...

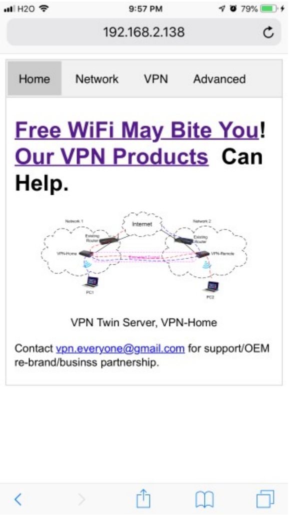
Ethernet IP	192.168.2.138
RX Packets	5358
TX Packets	6124
RX Bytes	2950750
TX Bytes	1756847

+ Router Info ...

+ WiFi Hotspot ...

Figure 5 VPN-Twin Device Ethernet IP

Then use that IP address (e.g. http://192.168.2.138) to access VPN device web page to change WiFi related setting.



Free WiFi May Bite You! Our VPN Products Can Help.

VPN Twin Server, VPN-Home

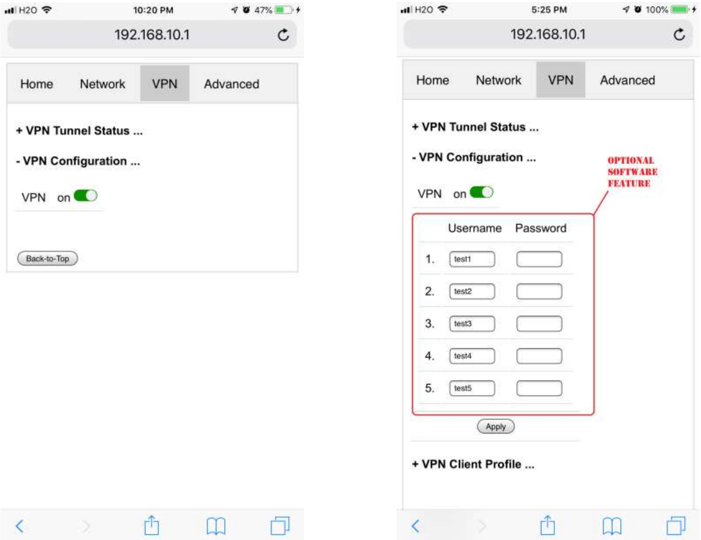
Contact vpn.everyone@gmail.com for support/OEM re-brand/businss partnership.

Figure 6 Access VPN Device Web UI by VPN server IP

4. Configure VPN-Home Device

VPN-Home device can be plug-n-play out of box. We recommend that you try factory default setting first. After you get familiar with the device, you can change settings to fit your needs.

If your purchase the "Road Warrior Feature" software option, you can set up 5 username & password pairs for VPN clients to access VPN-Home network or VPN-Remote network from anywhere on internet.



+ VPN Tunnel Status ...

- VPN Configuration ...

VPN on

+ VPN Tunnel Status ...

- VPN Configuration ...

VPN on

OPTIONAL SOFTWARE FEATURE

	Username	Password
1.	test1	
2.	test2	
3.	test3	
4.	test4	
5.	test5	

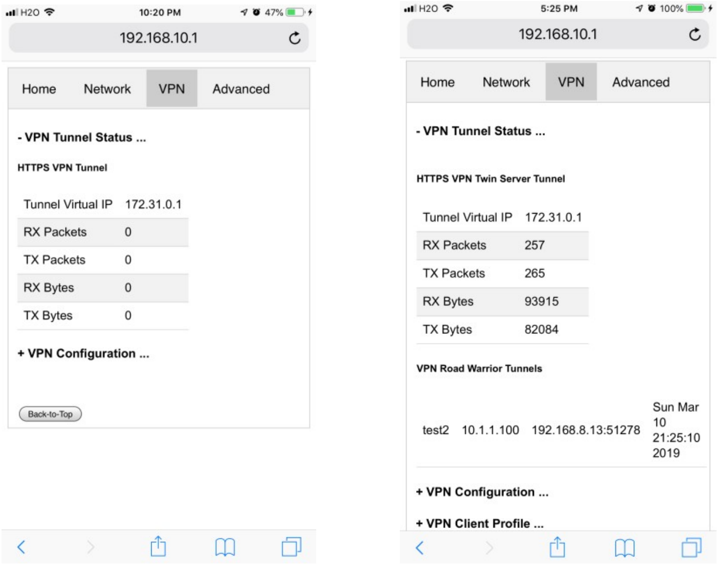
+ VPN Client Profile ...

Figure 7 Configure VPN-Home Device

- Connect to VPN-Home WiFi hotspot (default network: *vpneveryone.ddns.net* with password *00000000*)
- Click ***VPN*** tab
- Click ***+VPN Configuration …***
- ***[Option] Fill in 5 username & password pairs***
- Click ***Apply*** button
- That's it!

Note: VPN-Remote & VPN-Home are always sold in pair. The random & unique security keys are generated and programmed at manufacturing time. One VPN-Remote and only talk to the VPN-Home device shipped together.

If there is VPN-Remote device paired, you can see the VPN tunnel information by clicking ***+VPN Tunnel Status …***



- VPN Tunnel Status ...

HTTPS VPN Tunnel

Tunnel Virtual IP	172.31.0.1
RX Packets	0
TX Packets	0
RX Bytes	0
TX Bytes	0

+ VPN Configuration ...

- VPN Tunnel Status ...

HTTPS VPN Twin Server Tunnel

Tunnel Virtual IP	172.31.0.1
RX Packets	257
TX Packets	265
RX Bytes	93915
TX Bytes	82084

VPN Road Warrior Tunnels

test2	10.1.1.100	192.168.8.13:51278	Sun Mar 10 21:25:10 2019

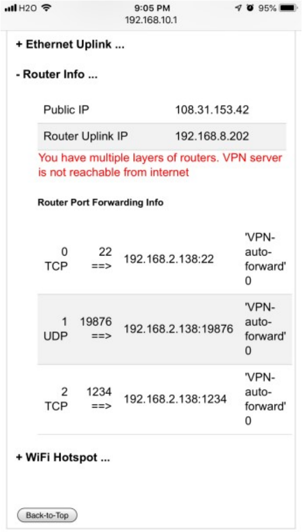
+ VPN Configuration ...

+ VPN Client Profile ...

Figure 8. VPN Tunnel Status UI on VPN-Home Device

Figure 8 above shows HTTPS VPN tunnel between VPN-Home and VPN-Remote devices. If your purchase includes "Road Warrior Feature", it shows the active road warrior VPN client list, too.

Note: The screenshot in Figure 8 is captured based on test lab. In real deployment, you should see a public IP instead of private IP in 192.168.x.x format.



+ Ethernet Uplink ...

- Router Info ...

Public IP	108.31.153.42
Router Uplink IP	192.168.8.202

You have multiple layers of routers. VPN server is not reachable from internet

Router Port Forwarding Info

0 TCP	22 ==>	192.168.2.138:22	'VPN-auto-forward' 0
1 UDP	19876 ==>	192.168.2.138:19876	'VPN-auto-forward' 0
2 TCP	1234 ==>	192.168.2.138:1234	'VPN-auto-forward' 0

+ WiFi Hotspot ...

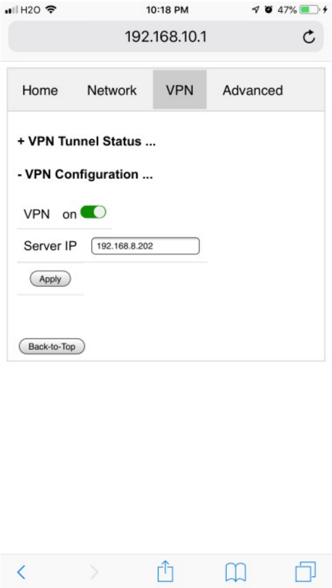
Figure 9. Find VPN-Home Device Public IP

- Click ***Network*** tab
- Click ***+Router Info …***
- Write down the ***Public IP*** value on screen. You will need it to configure VPN-Remote Device.

Note: Figure 9 screenshot is based on our test lab. In your real deployment, the ***Public IP*** should match ***Router Uplink IP***. Otherwise, VPN-Home device is not reachable from internet. Then VPN-Remote device won't be able to connect to VPN-Home device.

5. Configure VPN-Remote Device

Configuring VPN-Remote device is pretty much the same as configuring VPN-Home device except that you need to turn VPN on and put public IP of VPN-Home device in.



VPN on

Server IP 192.168.8.202

Figure 10 Configure VPN-Remote Device

- Connect to VPN-Home WiFi hotspot (default network: *vpneveryone.ddns.net* with password *00000000*)
- Click ***VPN*** tab
- Click ***+VPN Configuration …***
- Click the switch next to ***off*** to turn VPN on
- Input the public IP of VPN-Home device in ***Server IP*** (refer to Figure 9)
- Click ***Apply*** button

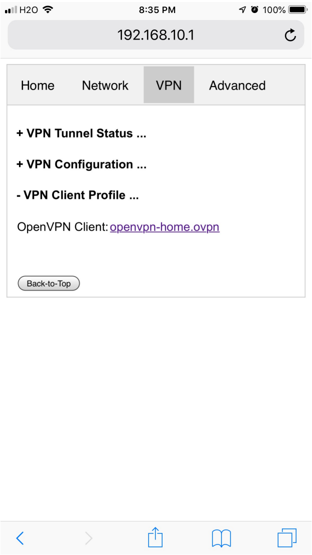
6. Configure OpenVPN Clients

If you bought "Road Warrior Feature" software option when you order, you can use OpenVPN client to connect to VPN-Home device. This section shows you how to configure OpenVPN clients. It is super easy. In one sentence, import in your device, the OpenVpn configuration file generated by VPN-Home device.

6.1. Configure TLS VPN Client on Windows 7/10 PC

The commercial of-the-shelf free **OpenVPN client** can be used to create TLS VPN tunnel to TLS VPN server. Google "openvpn download" to find the software and install it on your PC.

VPN-Home device prepares the OpenVPN configuration file. You can download it from web UI page. Click ***VPN*** tab. Then click ***+VPN Client Profile …***



+ VPN Tunnel Status ...

+ VPN Configuration ...

- VPN Client Profile ...

OpenVPN Client: openvpn-home.ovpn

Figure 11 OpenVPN Client Configuration Prepared by VPN Server

Right click openvpn-home.ovpn link and save it at OpenVPN configuration directory ***C:\Program Files\OpenVPN\config\.***

Note 1: C:\Program Files\OpenVPN\config\ may need administrator privilege to save file.
Note 2: This openvpn-home.ovpn file is good for OpenVPN clients of all platforms (Windows, iOS, Android, MacBook)

1. From windows start menu, find “OpenVPN GUI” icon. Right click it and click “Run as administrator”. (Figure 12).

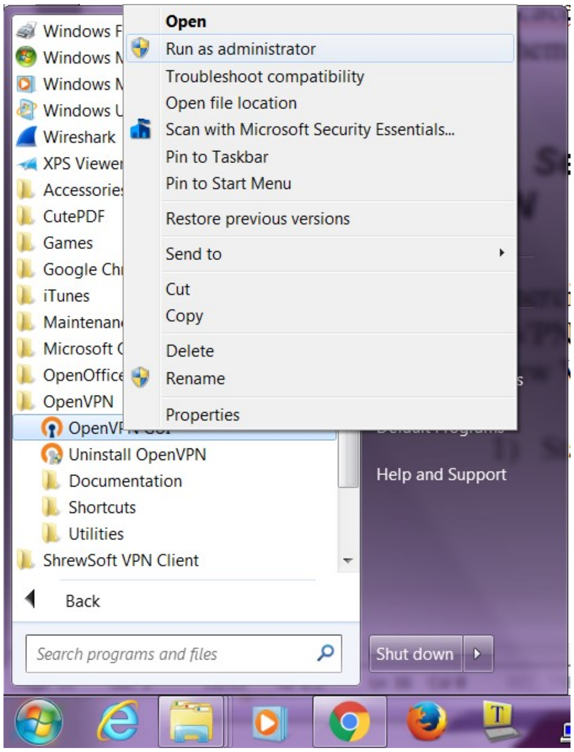


Figure 12 Run OpenVPN GUI as administrator

2. There will be an icon that looks like a lock at bottom right corner of screen. (Figure 13)

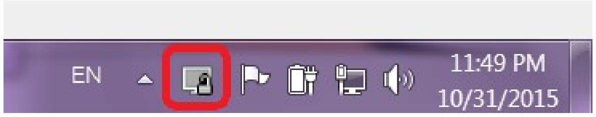


Figure 13 OpenVPN Icon in Task Bar

3. Right click on this lock-like icon and click "connect" on the menu. You will be asked for user name and password. Use one of the users you created on VPN server.

   The factory default user is "**test1**" with password "**vpneveryone**" (without quote sign)

   In a short moment, OpenVPN successfully creates VPN tunnel and assign the PC a virtual IP.

   Now all your internet access will be through this OpenVPN tunnel.

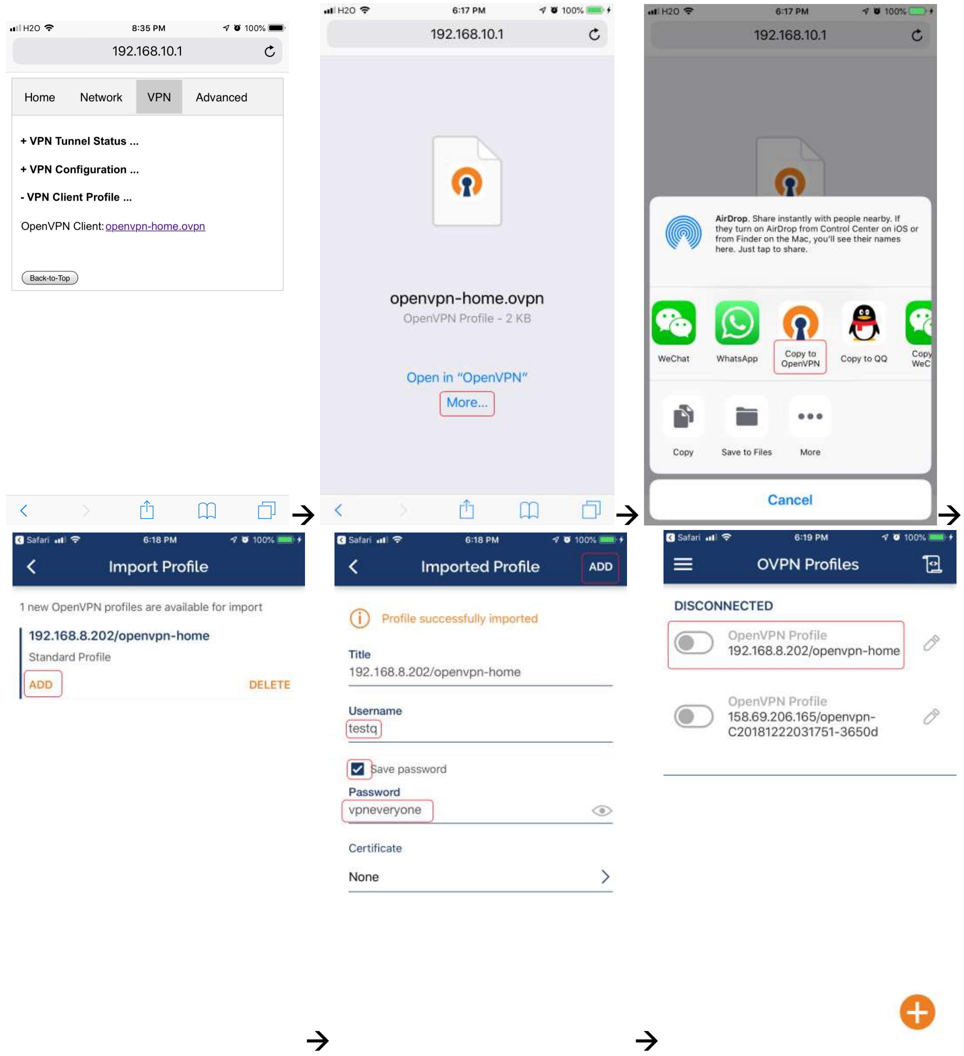
6.2. Configure TLS VPN Client on iOS

First you need to install OpenVPN app on your iPhone/iPad.

After that, use your iPhone/iPad to access VPN server web UI.

- Tap ***VPN*** tab.

- Then tap ***+VPN Client Profile ….***
- Then tap openvpn-home.ovpn link.
- Then follow red marks in the screenshots below



+ VPN Tunnel Status ...

+ VPN Configuration ...

- VPN Client Profile ...

OpenVPN Client: openvpn-home.ovpn

openvpn-home.ovpn

OpenVPN Profile - 2 KB

AirDrop. Share instantly with people nearby. If they turn on AirDrop from Control Center on iOS or from Finder on the Mac, you'll see their names here. Just tap to share.

1 new OpenVPN profiles are available for import

192.168.8.202/openvpn-home

Standard Profile

Profile successfully imported

Title: 192.168.8.202/openvpn-home

Username: testq

☑ Save password

Password: vpneveryone

Certificate: None

DISCONNECTED

OpenVPN Profile
192.168.8.202/openvpn-home

OpenVPN Profile
158.69.206.165/openvpn-C20181222031751-3650d

Figure 14 OpenVPN iPhone Client Screenshots

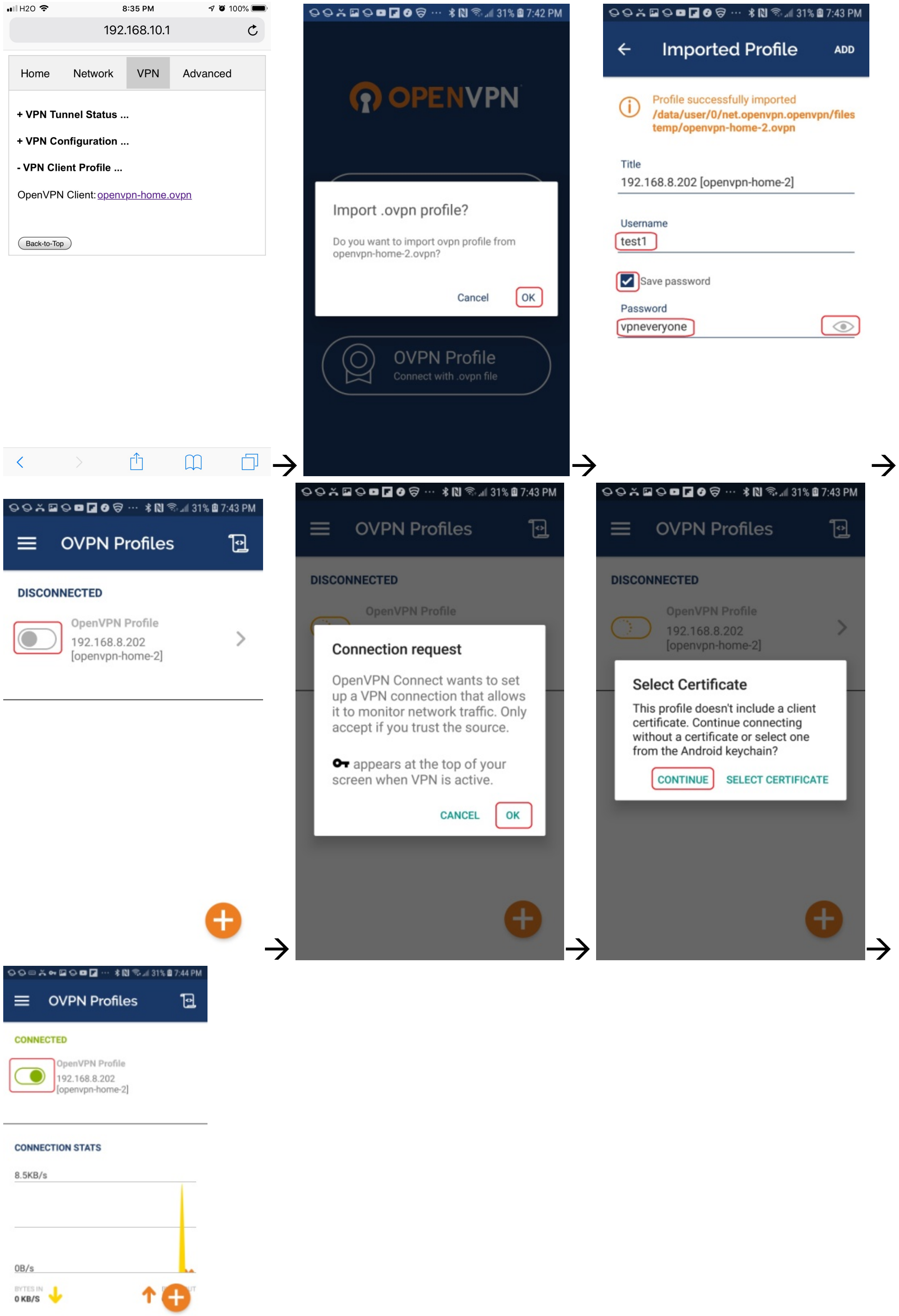
Note: Use the right username & password you set on HTTP server.

6.3. Configure TLS VPN Client on Android

It is pretty much the same as TLS VPN client setup in iOS.

First you need to install OpenVPN on Android phone/tablet.
After that, use your Android device to access VPN server web UI.

- Tap ***VPN*** tab.
- Then tap ***+VPN Client Profile ….***
- Then tap openvpn-home.ovpn link.
- Then follow red marks in the screenshots below



OpenVPN Client: openvpn-home.ovpn

Import .ovpn profile?

Do you want to import ovpn profile from openvpn-home-2.ovpn?

Profile successfully imported /data/user/0/net.openvpn.openvpn/files temp/openvpn-home-2.ovpn

Title: 192.168.8.202 [openvpn-home-2]

Username: test1

☑ Save password

Password: vpneveryone

OpenVPN Profile 192.168.8.202 [openvpn-home-2]

Connection request

OpenVPN Connect wants to set up a VPN connection that allows it to monitor network traffic. Only accept if you trust the source.

appears at the top of your screen when VPN is active.

Select Certificate

This profile doesn't include a client certificate. Continue connecting without a certificate or select one from the Android keychain?

Figure 15 Android OpenVPN Client Setup Screenshots

6.4. Configure TLS VPN Client on MacBook

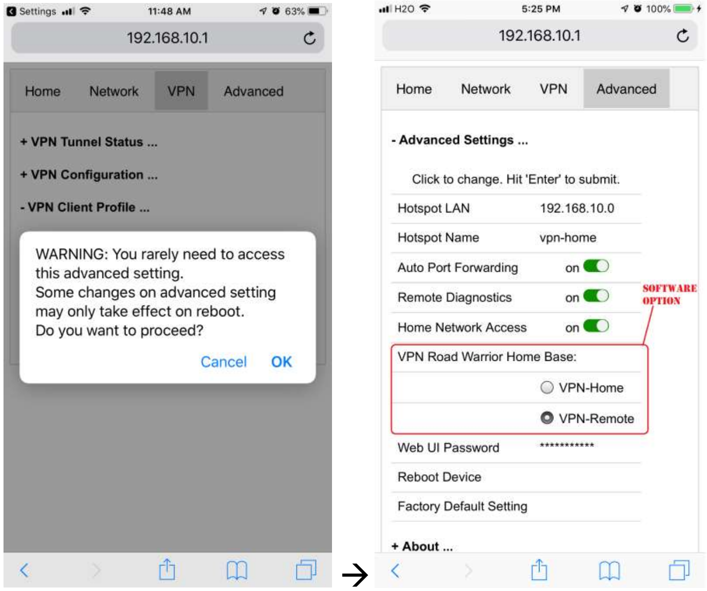
Download the Tunnelblick disk image file (a ".dmg" file) from https://tunnelblick.net

Tunnelblick is the popular OpenVPN client.
After installing tunnelblick, run it.
Download openvpn-home.ovpn prepared by VPN server device
Drag openvpn-home.ovpn to tunnelblick app. That’s it!

7. Advanced Settings

Note: In very rare case that you will need to change advanced settings. If you are not very comfortable with computer networking, leave the setting as is.

After you login to the VPN server web UI, click ***Advanced*** tab to see the UI below. You can click ***OK*** to enter ***Advanced*** UI page.



+ VPN Tunnel Status ...
+ VPN Configuration ...
- VPN Client Profile ...

WARNING: You rarely need to access this advanced setting.
Some changes on advanced setting may only take effect on reboot.
Do you want to proceed?

- Advanced Settings ...

Click to change. Hit 'Enter' to submit.

Hotspot LAN	192.168.10.0
Hotspot Name	vpn-home
Auto Port Forwarding	on
Remote Diagnostics	on
Home Network Access	on
VPN Road Warrior Home Base:	
	○ VPN-Home
	● VPN-Remote
Web UI Password	***********
Reboot Device	
Factory Default Setting	

+ About ...

Figure 16 VPN Device Advanced Settings

Each item except for ***Web UI Password*** on this Advanced UI is independent and will take effect on change.

1) **Hotspot LAN**

   Only when the router LAN happens to be 192.168.10.0, will you need to change hotspot LAN network.
   To change it, click the IP ***192.168.10.0***. Then the ***10*** part becomes editable. Enter any value between 0~254 and hit enter to change.

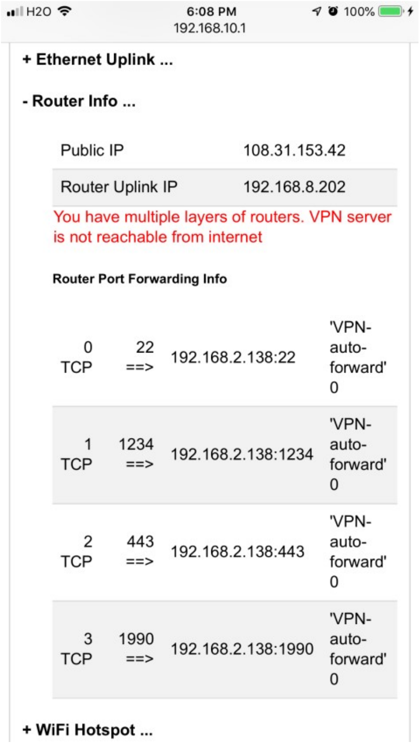
2) **Hotspot Name**

   The default hotspot network name “*vpneveryone.ddns.net*” should be unique enough identify itself. If you want to change it, click it. Then it becomes editable. Enter whatever name you like and hit enter to change.

3) Auto Port Forwarding

In order for VPN server to be reachable from internet, your router needs to forward a few ports to VPN server. This is done automatically by VPN server telling router to do port forwarding. You should never disable it.

If you have to disable this feature for whatever reason, you will have to manually set up your router to forward ports below to VPN server.



H2O 6:08 PM 100%
192.168.10.1

+ Ethernet Uplink ...

- Router Info ...

Public IP	108.31.153.42
Router Uplink IP	192.168.8.202

You have multiple layers of routers. VPN server is not reachable from internet

Router Port Forwarding Info

0 TCP	22 ==>	192.168.2.138:22	'VPN-auto-forward' 0
1 TCP	1234 ==>	192.168.2.138:1234	'VPN-auto-forward' 0
2 TCP	443 ==>	192.168.2.138:443	'VPN-auto-forward' 0
3 TCP	1990 ==>	192.168.2.138:1990	'VPN-auto-forward' 0

+ WiFi Hotspot ...

Figure 17 Router Port Forwarding Info

4) Remote Diagnostics

In case that you need remote help on troubleshooting VPN server, we may run diagnostics tools which use TCP port 22.

Disabling Remote Diagnostics only tell VPN server not to tell router to auto forward port 22 to VPN server.

5) Home Network Access

http://vpneveryone.ddns.net/reasons-for-vpn.html

One of the key use cases to VPN is to access home network. In some cases, you may not want VPN users to access home network at all. For example, you let your friends at oversea to use your VPN to access internet websites that are blocked by his country. You want your friends to access internet only, and disable his access to your home network.

In this case, you can turn off ***Home Network Access***.

6) **VPN Road Warrior Home Base**
If you bought "Road Warrior Feature" when you ordered this product, you see this option in ***Advanced*** setting.
By default, VPN Road Warrior Home Base is VPN-Home. It means, Your PC on internet with VPN client connected to VPN-Home device would appear to be in VPN-Home network. It can access VPN-Home network (subject to ***Home Network Access*** setting) and it appears to the websites it visits as if it is from VPN-Home network.
If you want to make VPN client appear to be in VPN-Remote network, simply click the radio button next to VPN-Remote.

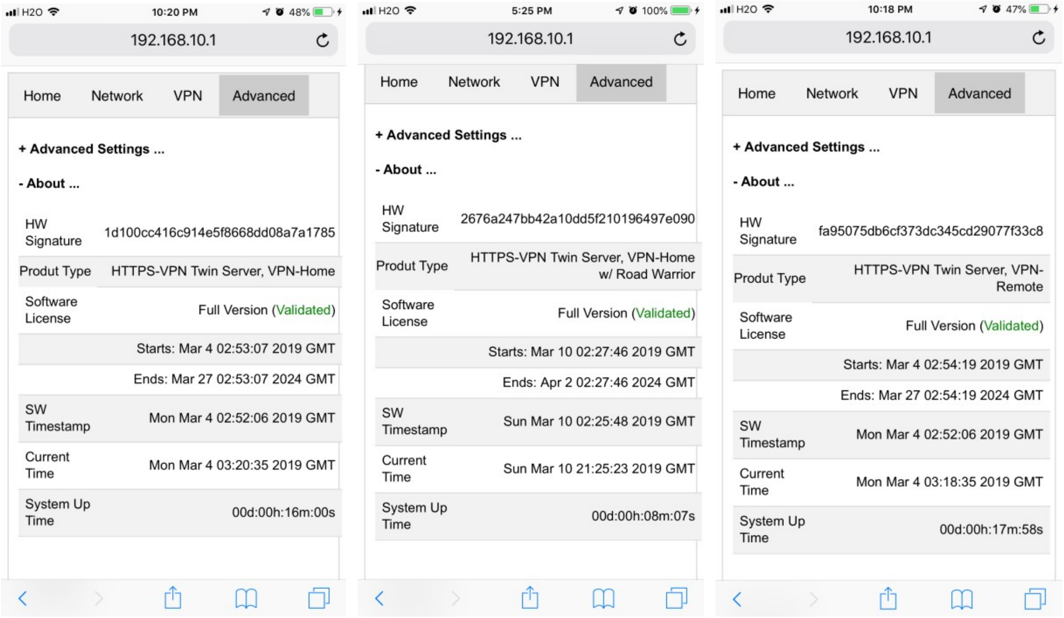
7) **Web UI Password**
By default, web UI password is vpneveryone
Although the VPN server web UI is not accessible from internet, you may not want everyone to know your VPN server UI password. You can change it. Click the ******. It will become editable. Enter your password and hit enter to change it.
Note: New UI password only take effect on next boot.

8) **Reboot Device**

In rare cases, you will need to reboot VPN server by web UI. If you are at home, power cycle VPN server device would be a better way to reboot it.

9) **Factory Default Setting**
Only when you think you don't know what you have done and everything fell apart, should you do a factory default setting.

7.1. About Product



+ Advanced Settings ...

- About ...

HW Signature	1d100cc416c914e5f8668dd08a7a1785
Produt Type	HTTPS-VPN Twin Server, VPN-Home
Software License	Full Version (Validated)
	Starts: Mar 4 02:53:07 2019 GMT
	Ends: Mar 27 02:53:07 2024 GMT
SW Timestamp	Mon Mar 4 02:52:06 2019 GMT
Current Time	Mon Mar 4 03:20:35 2019 GMT
System Up Time	00d:00h:16m:00s

+ Advanced Settings ...

- About ...

HW Signature	2676a247bb42a10dd5f210196497e090
Produt Type	HTTPS-VPN Twin Server, VPN-Home w/ Road Warrior
Software License	Full Version (Validated)
	Starts: Mar 10 02:27:46 2019 GMT
	Ends: Apr 2 02:27:46 2024 GMT
SW Timestamp	Sun Mar 10 02:25:48 2019 GMT
Current Time	Sun Mar 10 21:25:23 2019 GMT
System Up Time	00d:00h:08m:07s

+ Advanced Settings ...

- About ...

HW Signature	fa95075db6cf373dc345cd29077f33c8
Produt Type	HTTPS-VPN Twin Server, VPN-Remote
Software License	Full Version (Validated)
	Starts: Mar 4 02:54:19 2019 GMT
	Ends: Mar 27 02:54:19 2024 GMT
SW Timestamp	Mon Mar 4 02:52:06 2019 GMT
Current Time	Mon Mar 4 03:18:35 2019 GMT
System Up Time	00d:00h:17m:58s

Figure 18 Product Info

Each VPN device runs the software programmed in the MicroSD card included. The software is only licensed to run on this MicroSD card.
For full version product, the software is ***licensed for 5 years***.
For trial/free version software image, it is only licensed for 30 days (subject to change without notice).

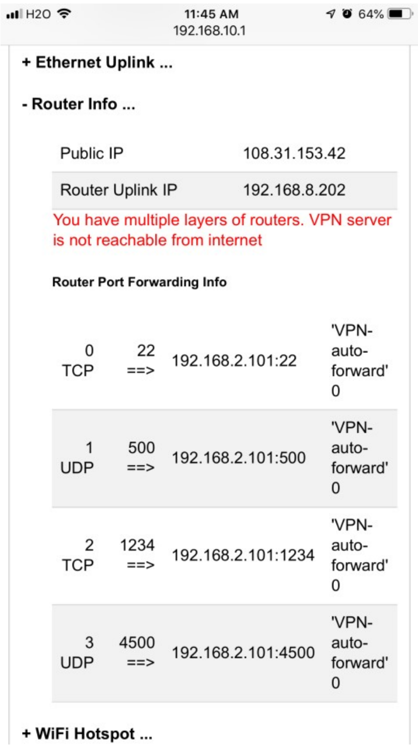
The **About** section in **Advanced** tab tells the license info. After software license expires, you still have access to web UI. But the VPN service is automatically shut down.

8. Quick Troubleshoot

1) Make sure you don't have multiple layers of routers cascaded.

   VPN server can only tell the router directly connected to auto forward ports. If you have multiple layers of router cascaded, the VPN server is not reachable from internet. Therefore, it will never work.

   The ***Router Info*** section on ***Network*** web UI page (Figure 19 below) will help you. If the ***Public IP*** does not match the ***Router Uplink IP***, it means you have multiple-layer router problem.



+ Ethernet Uplink ...

- Router Info ...

Public IP	108.31.153.42
Router Uplink IP	192.168.8.202

You have multiple layers of routers. VPN server is not reachable from internet

Router Port Forwarding Info

0 TCP	22 ==>	192.168.2.101:22	'VPN-auto-forward' 0
1 UDP	500 ==>	192.168.2.101:500	'VPN-auto-forward' 0
2 TCP	1234 ==>	192.168.2.101:1234	'VPN-auto-forward' 0
3 UDP	4500 ==>	192.168.2.101:4500	'VPN-auto-forward' 0

+ WiFi Hotspot ...

Figure 19 Router Info UI Page

2) Make sure router port forwarding works correctly

   99.99% of residential routers support UPNP and it is by default enabled. The auto port forwarding should work by default.
   If you see port forwarding info like Figure 19, you are good.

   If you had disabled UPNP on your router, you need to enable it. Or manually forward ports like in Figure 19

   If you router have ***UPNP secure version*** enabled, it may not work well with VPN server. Please disable security on UPNP and run regular version UPNP.

3) Please be noted that all keys/passwords/usernames are case sensitive. “Password” is not the same as “password”