HTTP-VPN Server & Client for Site-to-Site Quick Start Guide

Rev B
January, 2019

By: vpneveryone.ddns.net

Table of Content

Table of Figures

1. Introduction

Setting up VPN site-to-site is made easy with this pair of HTTPS-VPN server & client for dummy. You don't need to know anything about VPN. All you need to configure is username, password, etc. in this pair of VPN devices.

In some cases, IPsec VPN could be blocked by firewall that you don't have control, this HTTPS flavor VPN is a great alternative to IPsec site-to-site VPN deployment. E.g. Some customers are using Verizon MiFi as their office uplink to internet and they found Version MiFi blocks IPsec. This HTTPS site-to-site VPN is a great rescue to such situation.

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

2. Connect VPN Server to Wireless Router

1) Connect VPN server to wireless router LAN port by Ethernet cable
2) Connect USB cable to power up VPN server (Figure 1)

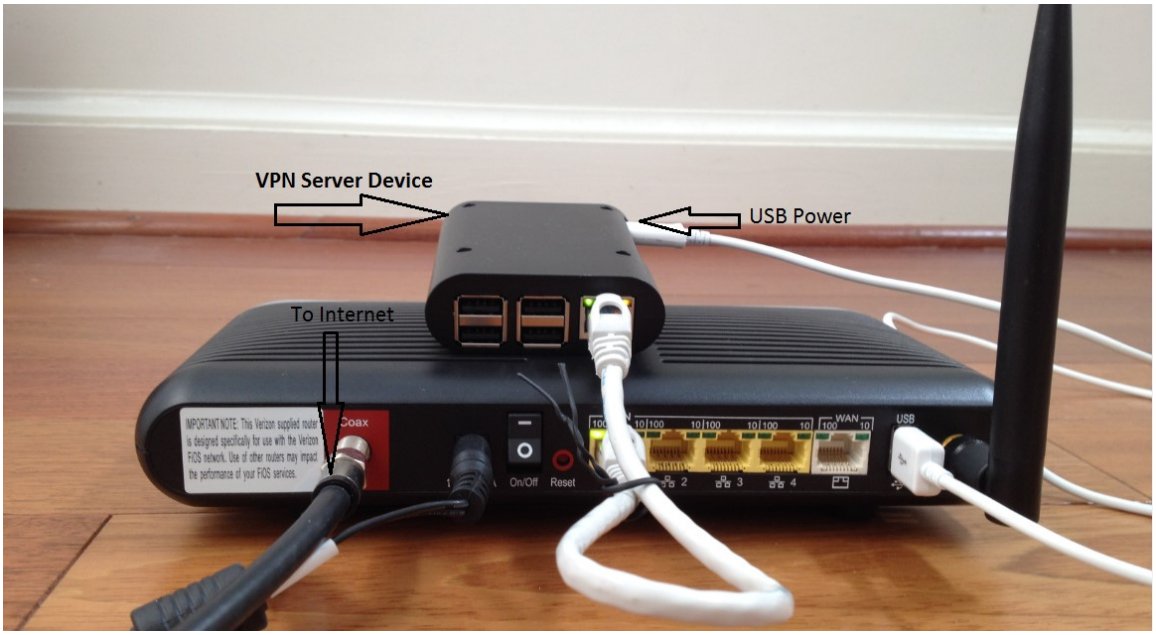

Figure 1 Connect VPN Server to Wireless Router

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.

3. Access VPN Server Configuration Web UI

3.1. Access Web UI by Built-in WiFi Hotspot

Your VPN device may be equipped with a short-range 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*

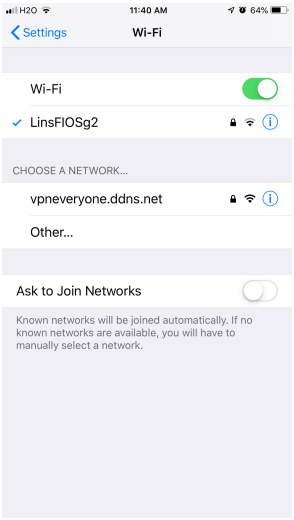

Figure 2 Find vpneveryone.ddns.net WiFi hotspot

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.

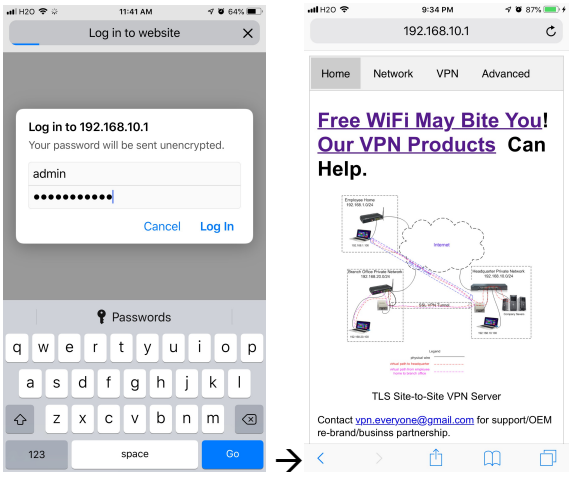

Figure 3 Access VPN Server Web UI by Built-in WiFi Hotspot

Note: The WiFi hotspot from VPN server is for convenience for out-of-box configuration. It is never meant to replace your regular WiFi at home. After you finish configuring your VPN settings, you may disable hotspot to avoid WiFi interference to your regular WiFi. You can always configure VPN server by VPN server IP directly. See below.

3.2. Access Web UI by http://Router IP:1234

If your VPN server is not equipped with WiFi hotspot or you are out of range, your iPhone can connect to your own wireless router where VPN server is attached. Then use your router IP with port 1234 to access VPN server web GUI.

Assume that your wireless router IP address 192.168.2.1. Open the Safari web browser, use http://192.168.2.1:1234 to access the web page on VPN device.

Figure 4 Access VPN Server Web UI by Router IP:1234

3.3. Access Web UI by VPN Server IP

Some router models don't support internal port forwarding. In this case, http://routerip:1234 will not work. You will have to login to your router to find out what IP address is allocated to the VPN server (e.g. 192.168.2.101). Then use that IP address (http://192.168.2.101) to access VPN device web page.

Figure 5 Access VPN Server Web UI by VPN server IP

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

4. Simple Configuration on Your Router

Main Office

- Connect VPN server to main office network by Ethernet cable.
- On your router's "***Advanced Routing Rule***" (or equivalent) section, add two static routes like below,
    a. "***To the branch office network, go via this VPN server device***".
    b. "***To network 10.1.1.0/24, go via this VPN server device***"

Note: 10.1.1.0/24 network is the virtual IP network used among VPN server & client device and any PC on-the-go.

!!!TIPs!!! VPN server use DHCP to get its IP address. It is highly recommended that you configure your DHCP server to reserve a fixed IP for VPN server. Otherwise, each time VPN server IP changes, you have to reconfigure the static route to branch office.

!!!Note!!! If have more than one branch office to connect, for each branch office network, you need to add one static route on your router to go via this VPN server.

Branch Office

- Connect VPN client device to your branch office network by Ethernet cable.
- On your router's "***Advanced Routing Rule***" (or equivalent) section, add two static routes like below,
    a. "***To the main office network, go via this VPN client device***".
    b. "***To the other branch office network, go via this VPN client device***".
    c. "***To network 10.1.1.0/24, go via this VPN client device***"

Note: 10.1.1.0/24 network is the virtual IP network used among VPN server & client device and any PC on-the-go.

!!!TIPs!!! VPN client uses DHCP to get its IP address. It is highly recommended that you configure your DHCP server to reserve a fixed IP for VPN client device. Otherwise, each time VPN client IP changes, you have to reconfigure router to update the static route to main office.

!!!Note!!! item b is for case that you have more than one branch office connected to main office, for each network (other than this office), you need to add one static route on your router to go via this VPN client.

5. HTTPS-VPN Device Configuration

Overall, the configuration on device side is extremely simple. Configure one combo of ***username*** & ***password*** & ***network address*** & ***network mask*** for each branch office from web UI.

VPN Server Setting

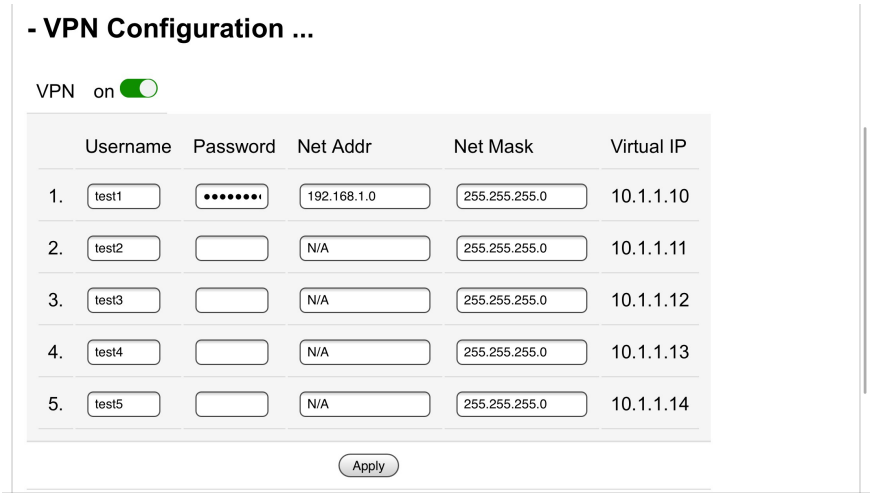

Figure 6 HTTPS VPN Site-to-Site Server Configuration

- Login to VPN server device web UI

- Click ***VPN*** tab
- Click ***+VPN Configuration …***
- Fill in 5 groups of ***username***, ***password***, ***network address***, ***network mask***
- Click ***Apply*** button

Note: You can put ***N/A*** words in network address field. That means, this ***username*** & ***password*** will be used as an PC VPN client (vs. a branch office network)
That's it! So easy!

VPN Client Setting

VPN client setting is pretty much the same as VPN server. VPN client needs to configure public IP of VPN server.

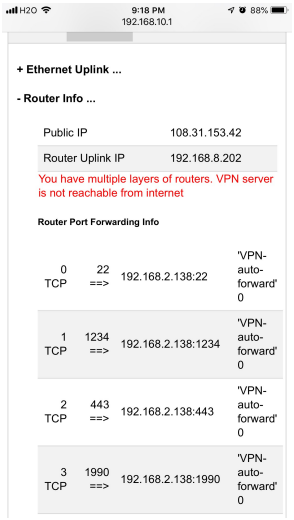

Figure 7 VPN Server Public IP

If you don't know what your VPN server public IP is, go to VPN server web UI. Click ***Network*** tab, then click ***+ Router Info …,*** you will see the public IP.

Note: Figure 7 is captured based on our lab test environment. In actual deployment, ***Public IP*** should match ***Router Uplink IP***. Otherwise,VPN server is not reachable from internet.

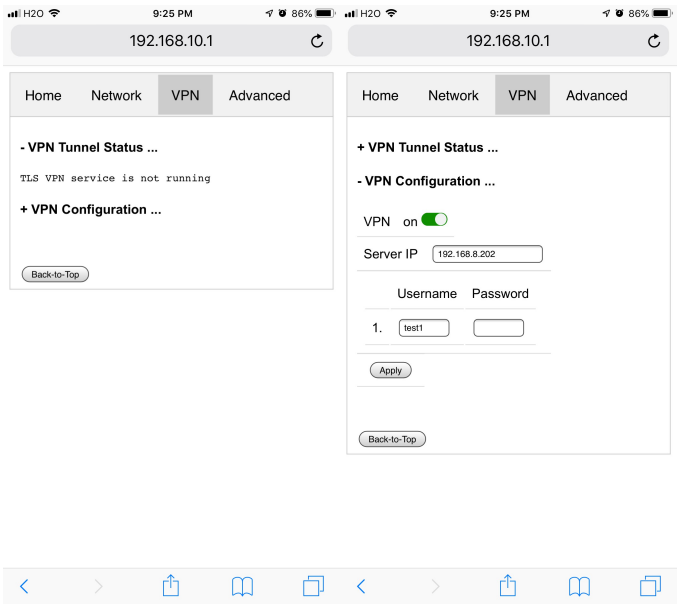

Figure 8 IPsec Site-to-Site VPN Client Configuration

- Login to VPN client device web UI
- Click ***VPN*** tab
- Click ***+VPN Configuration …***
- Click the ***on/off*** switch to turn on VPN
- Fill in VPN ***Server IP*** (public IP)
- Fill in ***Username & Password.*** They must be one of the 5 users configured on VPN server side.
- Click ***Apply*** button

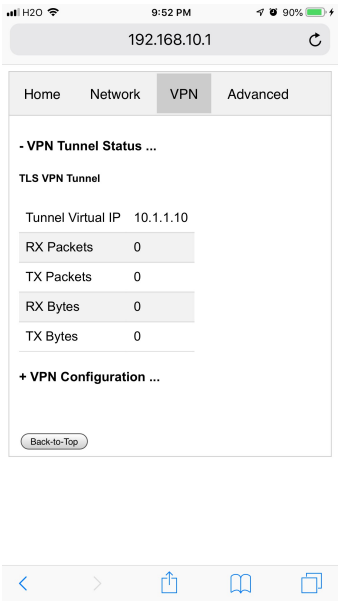

Figure 9 VPN Connection Status

Once VPN client is configured well, click ***+VPN Tunnel Status …***
You will see VPN tunnel is created successfully.

Tip: All hardware devices shipped are the same. They are inter-changeable. The difference is on software in the MicroSD card.

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

6. Configure OpenVPN Clients

The HTTPS-VPN server supports OpenVPN protocol, too. One of the 5 users is used for HTTPS-VPN site-to-site client device. You can use the rest 4 users for OpenVPN clients. 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 HTTPS-VPN server.

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

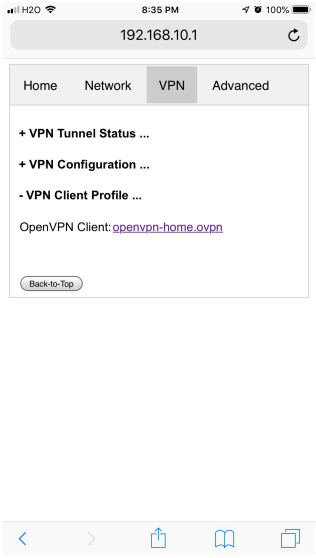

Figure 10 OpenVPN Client Configuration Prepared by VPN Server

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 11).

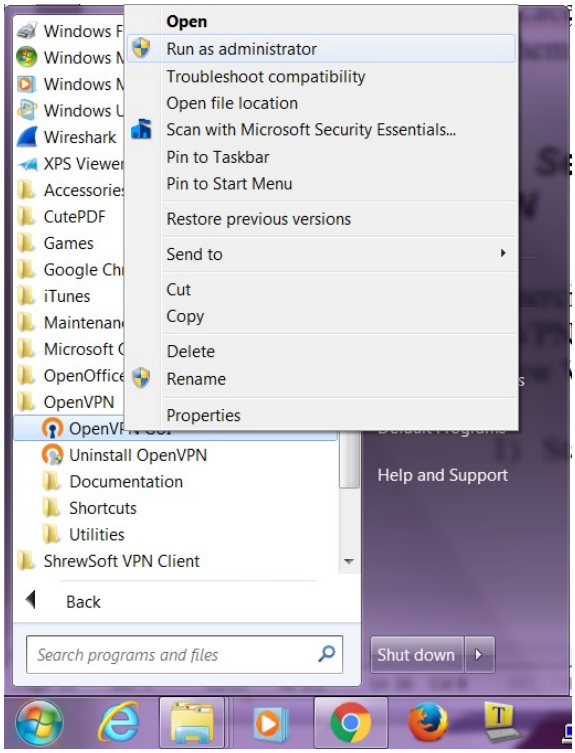

Figure 11 Run OpenVPN GUI as administrator

2. There will be an icon that looks like a lock at bottom right corner of screen. (Figure 12)

Figure 12 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

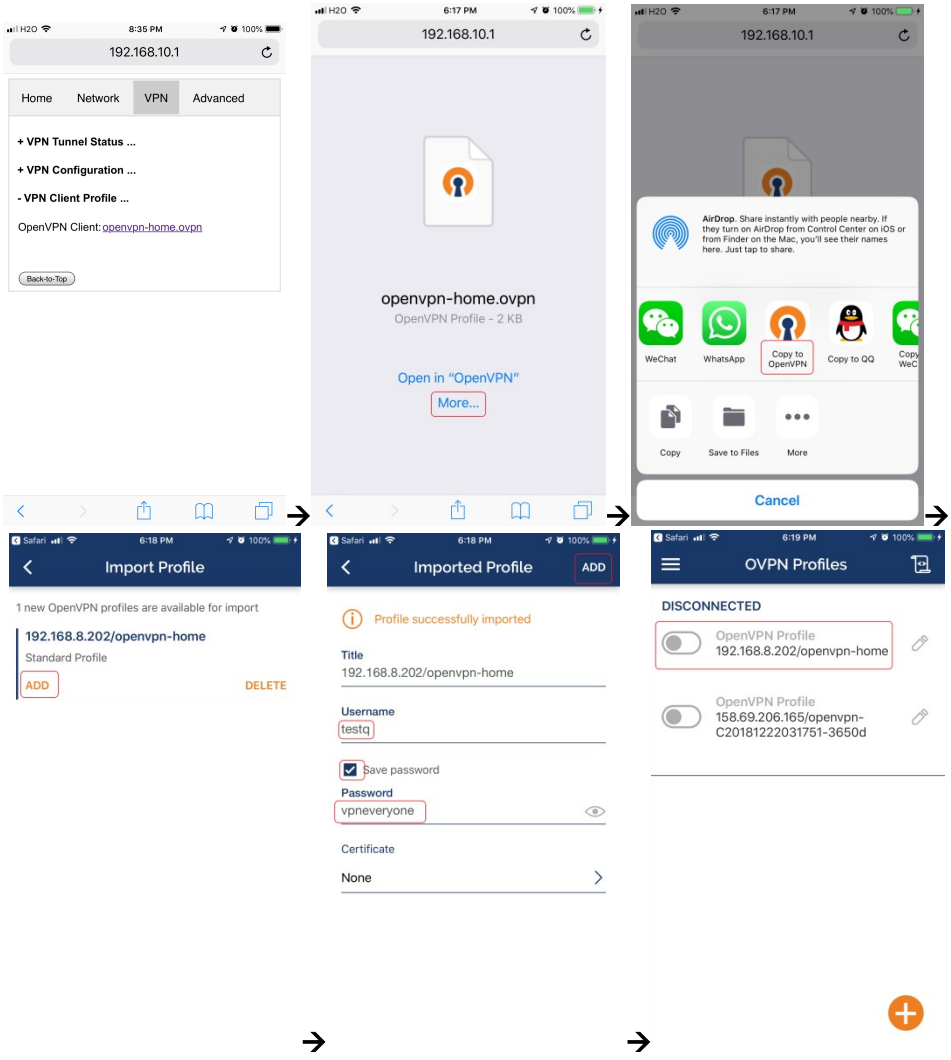

Figure 13 OpenVPN iPhone Client Screenshots

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

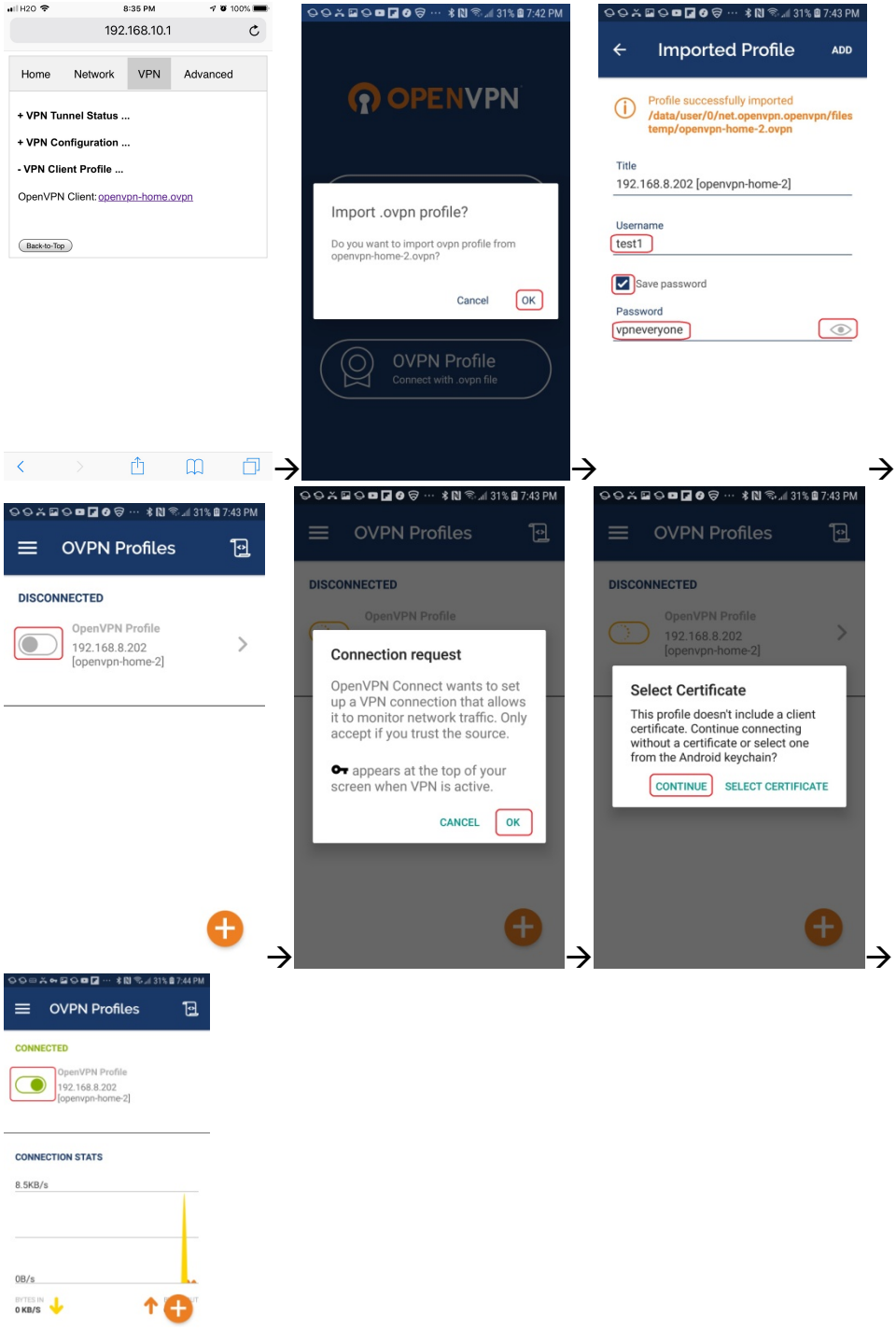

Figure 14 Android OpenVPN Client Setup Screenshots

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.

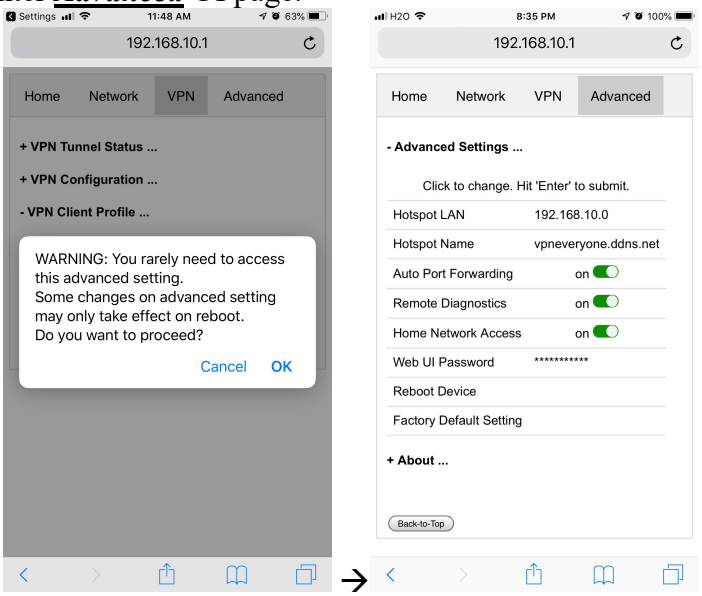

Figure 15 VPN Device Advanced Settings

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 set up your router to manually forward ports below to VPN server.

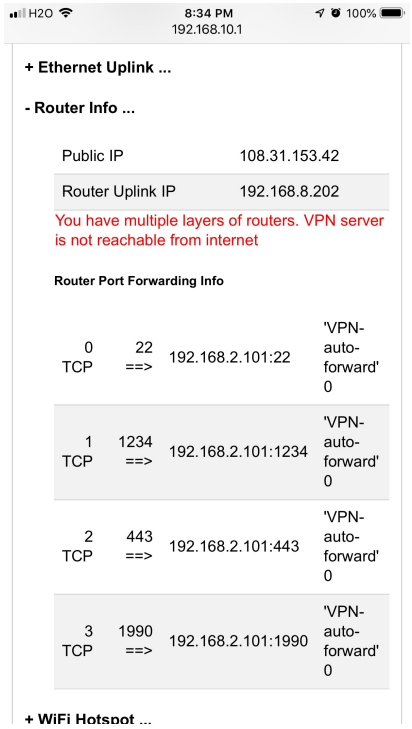

Figure 16 Router Port Forwarding Info

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) **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.

7) **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.

8) **Factory Default Setting**
Only when you think you don't know what you did and broke everything, should you do a factory default setting.

7.1. About Product

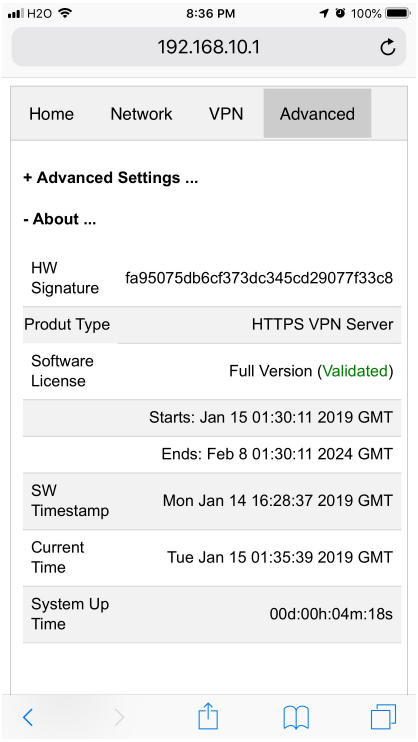

Figure 17 Product Info

Each VPN device runs the software programmed in the MicroSD card. The software is only licensed to run on the MicroSD card shipped.
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 router 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 18 below) will help you. If the ***Public IP*** does not match the ***Router Uplink IP***, it means you have multiple-layer router problem.

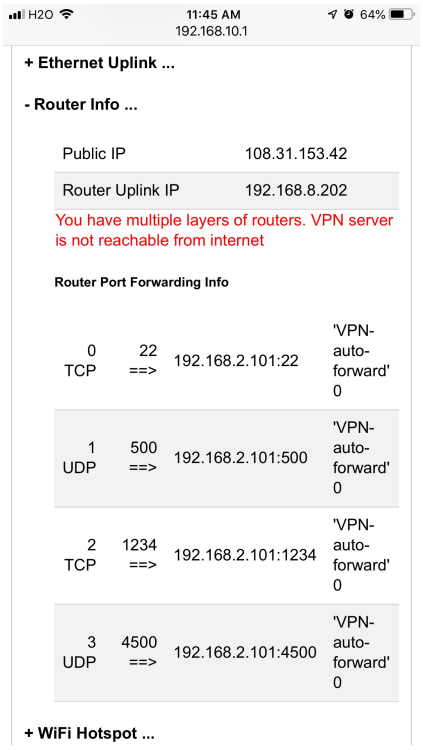

Figure 18 Router Info UI Page

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 18, you are good.

If you had disabled UPNP on your router, you need to enable it. Or manually forward ports like in Figure 18

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”