VPN Twin Server Quick Start Guide

Rev C
January, 2019

Table of Content

List of Figures

1. Introduction

The 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.
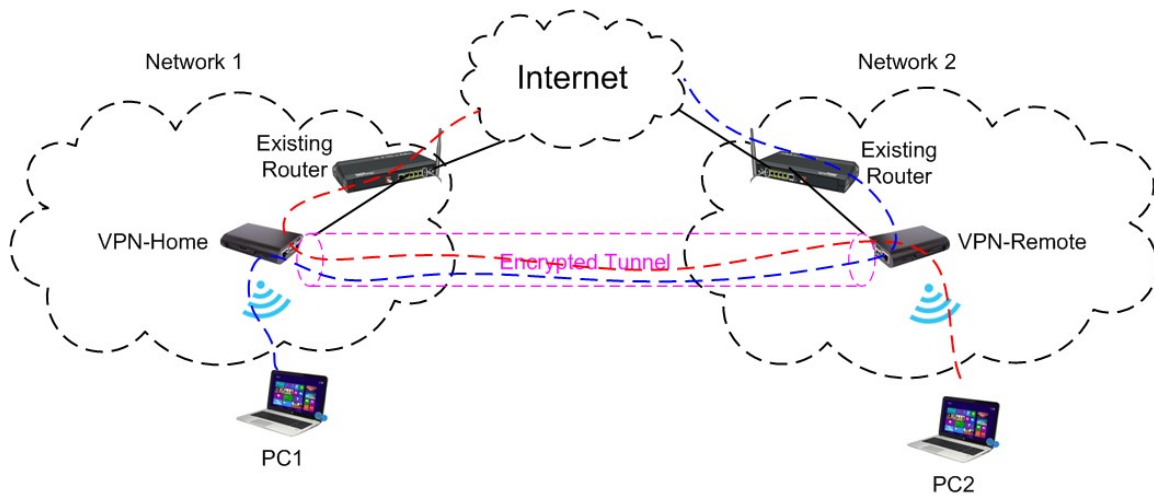
Figure 1 VPN Twin Server Working Model

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". PC connected to "VPN-Home" WiFi can access the private network where "VPN-Remote" is. And PC connected to "VPN-Remote" WiFi can access the home network. (Figure 1)

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)
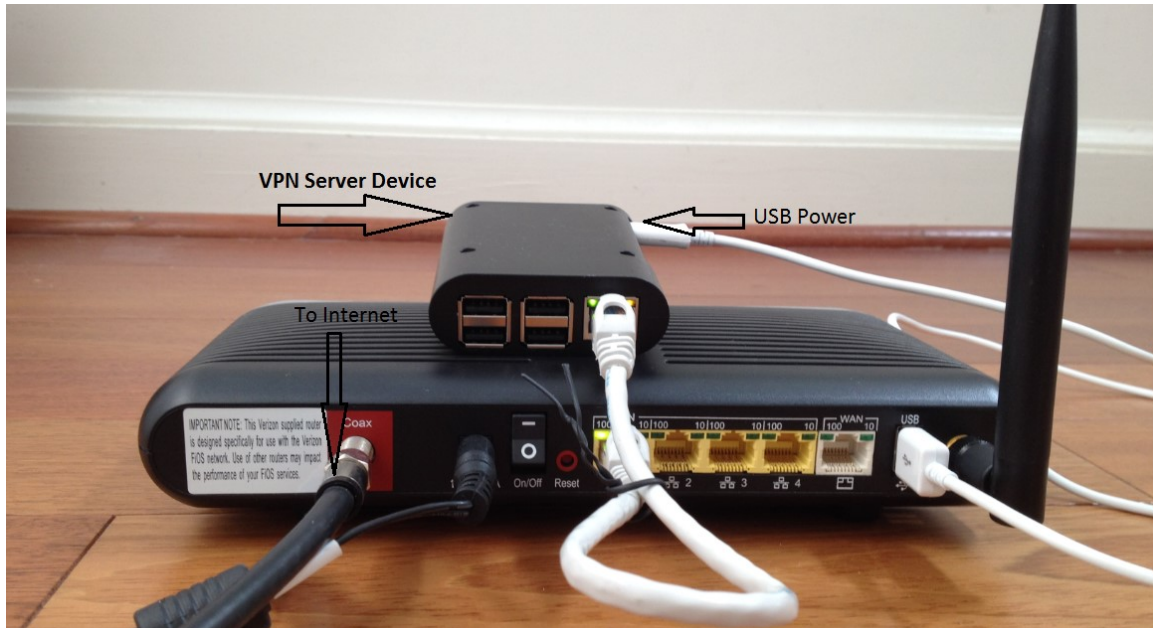

Figure 2 Connect VPN Device to Wireless Router

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.

Most wireless routers come with a USB interface. This USB interface on your wireless router can provide enough power for the VPN-Home/Remote. Connect VPN device to your router by USB data sync cable (Figure 2).

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 meansVPN-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*
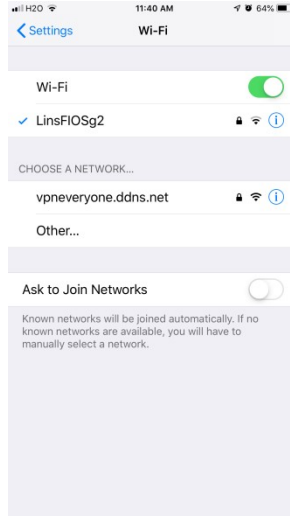

Figure 3 Find vpneveryone.ddns.net WiFi hotspot

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.
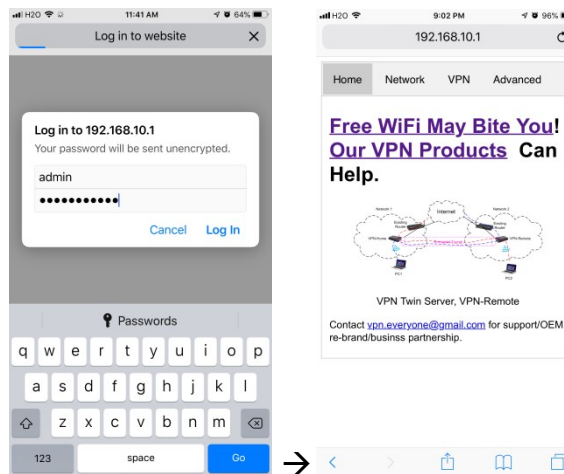

Figure 4 Access VPN Server Web UI by Built-in WiFi Hotspot

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.
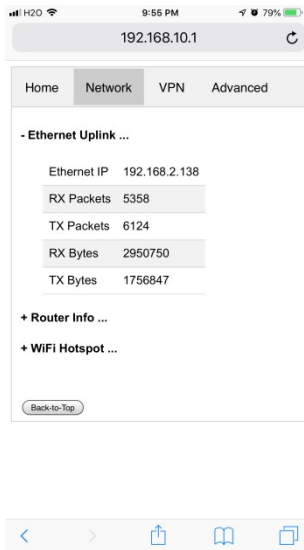

Figure 5 VPN-Twin Device Ethernet IP

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

Figure 6 Access VPN Device Web UI by VPN server IP

4. Configure VPN-Home Device

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 …*
- Set *Pre-shared key* (minimum 8 characters)
- Click *Apply* button
- That's it!

If there is VPN-Remote device paired, you can see the VPN tunnel information by clicking *+VPN Tunnel Status …*
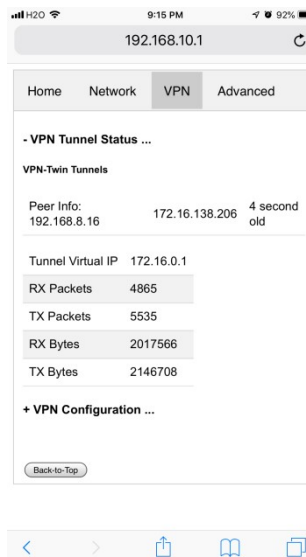
Figure 8. VPN Tunnel Status UI on VPN-Home Device

Figure 8 above shows Peer Info: one real IP(192.168.8.16) and one virtual IP (172.16.138.206) and status of the VPN tunnel (when is the last time traffic seen in tunnel).

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.
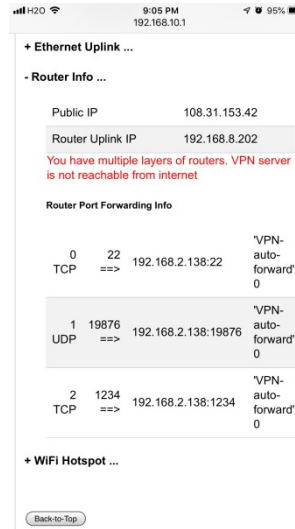
Figure 9. Find VPN-Home Device Public IP

- 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.
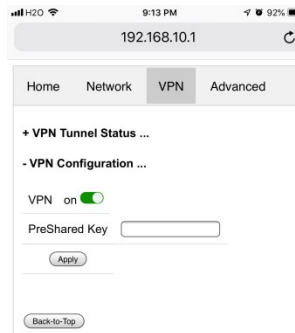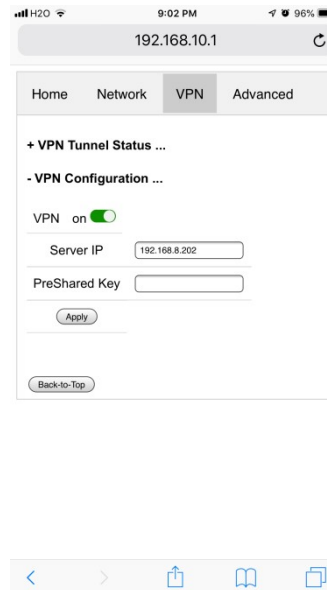

Figure 10 Configure VPN-Remote Device

- 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)
- Set ***Pre-shared key*** (minimum 8 characters)
- Click ***Apply*** button

6. 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.
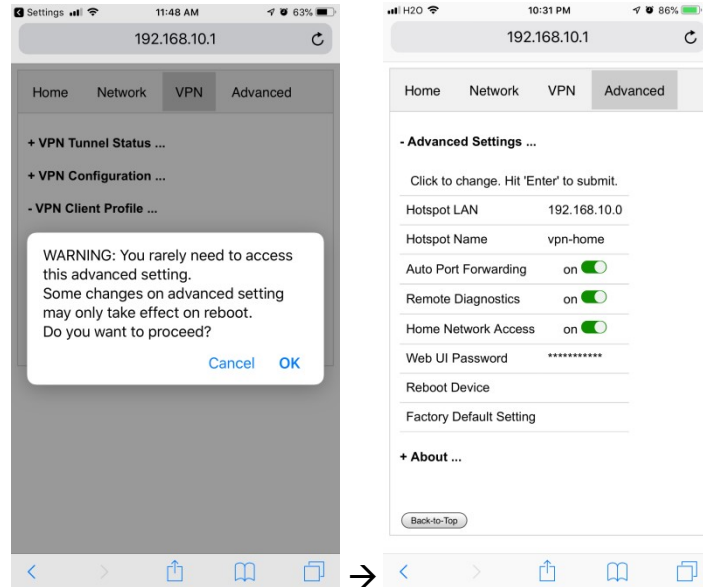
Figure 11 VPN Device Advanced Settings

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.
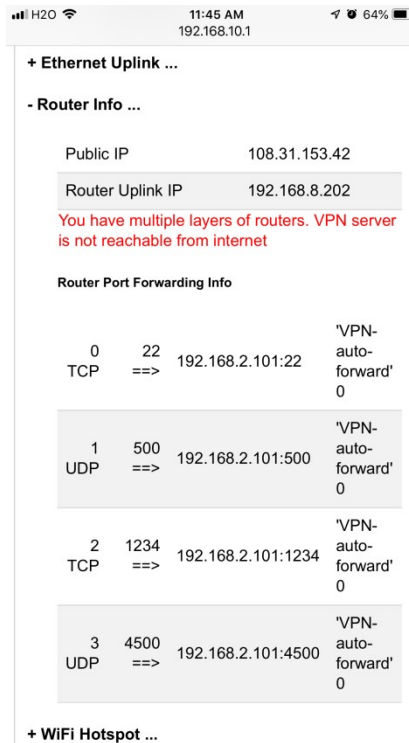
Figure 12 Router Port Forwarding Info

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.
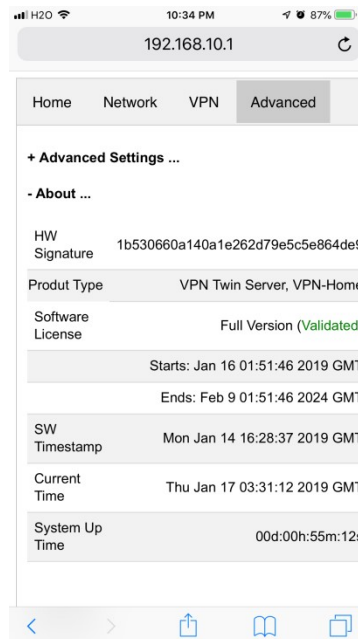
6.1.   About Product

Figure 13 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.

7. 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 14 below) will help you. If the **_Public IP_** does not match the **_Router Uplink IP_**, it means you have multiple-layer router problem.
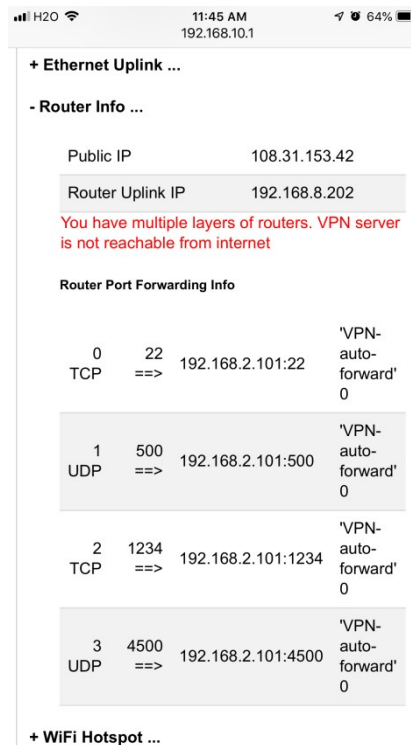

Figure 14 Router Info UI Page

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 14, you are good.

If you had disabled UPNP on your router, you need to enable it. Or manually forward ports like in Figure 14

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"