PI-VPN - The Easy VPN

By Aaron Grothe

Introduction

If anybody has any questions or comments at any time please let me know.

If I start to mumble please let me know as well :-)

PI-VPN

Command to Run

```
curl -L https://install.pivpn.io | bash
```

Thank you. Any Questions???

Maybe a bit more Detail

Since we've got a few minutes left we'll go into a bit more detail on the talk.

My Network Config
Basics of installing/configuring Raspberry Pi/Pi VPN

We'll be doing a test install using a Vultr VPS account throughout the talk as well so we'll be able to refer to it throughout the demo. At the end of the demo we'll flip to using it and see how it works

Why your own VPN?

- You control it - I can point you to StackSocial and there will be a ton of cheap VPNs on it, but you don't control them
  - Today's trusted VPN can get bought by somebody else tomorrow and the policies can change
  - Or there may just be a bug
- Theoretically you can run your own VPN for almost no cost, except electricity for the Raspberry PI

Why your own VPN?

- You can get access to your home network assets in a reasonably secure manner
- All your traffic is routed through the VPN, enabling you to do things like run Netflix at work if you want to
- Chance to learn/experiment - Pi-VPN is ideal for this
- Financial Times study finds half of the most popular VPN apps linked to China - https://www.ft.com/content/e5567d8a-ee65-11e8-89c8-d36339d835c0

My Home Network

Important Points

- Netgear Router - R7000 / running stock Netgear firmware currently. Am probably going to reinstall DD-WRT sometime - 192.168.0.254
- Raspberry PI/VPN - 192.168.0.249
- Current External IP Address: 70.187.14.105

Miscellaneous other machines/hardware/lightbulbs on my home network

Mom & Dad's Network

Important Points

- ASUS - (RT-ACRH13) / running stock Asus firmware currently. Am probably going to reinstall DD-WRT sometime - 192.168.0.254
- Server / Runs DNSMASQ for my home network - 192.168.0.1
- Raspberry PI/VPN - 192.168.0.249
- Current External IP Address: 70.187.14.105

Miscellaneous other machines/hardware/lightbulbs on their home network

Steps to Setting up your VPN

1. Configuring a Raspberry PI
2. Install PI VPN on Raspberry PI
3. Setting up Dynamic DNS (DDNS)
4. Making Router Modifications
5. Generating Client Certs
6. Playing around with PI VPN
7. Some other VPN options

Configuring a Raspberry Pi

About any Raspberry PI will do. Recommend Raspberry PI 3+ since it seems to work pretty well.

As for distros suggest raspbian-lite, don't need the full version of Raspbian.

PI-VPN works on most Debian based distributions. We'll be using regular Debian for our demo in Vultr.

Raspberry PI Models

My personal Pi-VPN is running on a Raspberry Pi Model 3b+ until recently this was the top of the line. Now the Raspberry PI 4 is available.

Raspberry PI 4 has full gig ethernet while the ethernet on the Model 3s was limited to 300 Mbit/s ethernet.

I only have 150Mbs on my home network so a Model 3B works fine for me.

Raspberry PI Zeros will top out at less than 100Mbs.

Raspberry PI Config

- Recommend a Raspberry PI 3 or 4, unless you have another one just lying around the house.
- Don’t forget to touch an empty SSH file on the sd card so SSH will be enabled by default
- Run config to resize Raspbian to use full MicroSD Card
- Command to find a Raspberry PI on your network
  - sudo nmap -sP 192.168.1.0/24 | awk '/^Nmap/{ip=$NF}/B8:27:EB/{print ip}'
- Use a quality MicroSD card, saves you a lot of grief over time
- Use a decent USB Power Supply trying to eek by with a crappy one is a false economy

```
sudo map -sP 192.168.1.0/24 | awk '/^Nmap/{ip=$NF}/B8:27:EB/{print
```

Installing PI-VPN

Stable (Recommended)

```
# curl -L https://install.pivpn.io | bash
```

Test (unstable) Branch install

```
# curl -L https://test.pivpn.io | TESTING= bash
```

Last time I ran Test was before Wireguard made it into the stable release.

Installing PI-VPN

Let's walk through the basics for the install. For this we'll be running in our vultr instance

1. First off it does basic checks against system
2. If running on a Raspberry PI asks you about setting a static IP
3. Choose a user to own the PI VPN install
4. Select Wireguard or OpenVPN, you probably want Wireguard
5. Select port and if OpenVPN choose protocol (UDP/TCP)

Installing PI-VPN

6. Select DNS provider
7. Public IP or DNS
8. If OpenVPN select key length
9. Unattended Security Updates
10. Reboot

#1. Basic Checks

Runs apt-update against system to make sure everything is up to date. Also installs relevant packages

#2. Static or DHCP

Raspbian by default will come up with DHCP. You can setup your DHCP to permanently assign the same IP address lease to the Raspberry PI or go with a Static IP address.

I go with a static IP (192.168.0.249) address for my VPN, making sure that IP is not handed out by the DNSMasq running on my server.

#3. Choose a user to own PI-VPN files

This will be where all the config files and backups are stored. On a Pi unless you setup an additional user this will be the pi user.

#4. Select Wireguard or Open VPN

Differences between Wireguard and OpenVPN

- Wireguard is faster/lighter weight and very popular right now
- Wireguard has been accepted into the Linux Kernel and will be in more versions of Linux in the near future
- Wireguard being newer is still being evaluated for security
- Wireguard has a much smaller code base
- OpenVPN runs over TCP and UDP, Wireguard is UDP only
- Wireguard client is very simple to use on Android/Apple phones

Unless you have a compelling reason to use OpenVPN I

#5. Select Port/Protocol for VPN

Again will probably just pick the defaults

Default Port for Wireguard is 51820

Default Port for OpenVPN is 1194
Default Protocol for OpenVPN is UDP

Recommend taking defaults unless you have a reason for changing them.

#6. Select DNS Provider

This allows you to select the DNS Provider.

I usually select Custom. I put my local dns first and then put the google DNS of 8.8.8.8 afterwards this allows me to hit resources that have local DHCP reservations, more easily

#7. Public IP or DNS

#7.   along with configuring the Firewall to forward ports are usually the two things that cause the most stress for people setting up their own VPN.

Most internet companies will periodically change your IP address. The way around this is to use something called Dynamic DNS. This updates your IP address when it changes from the cable company.

If your router supports Dynamic DNS this is probably the best way to handle it since the router knows when the external IP is updated.

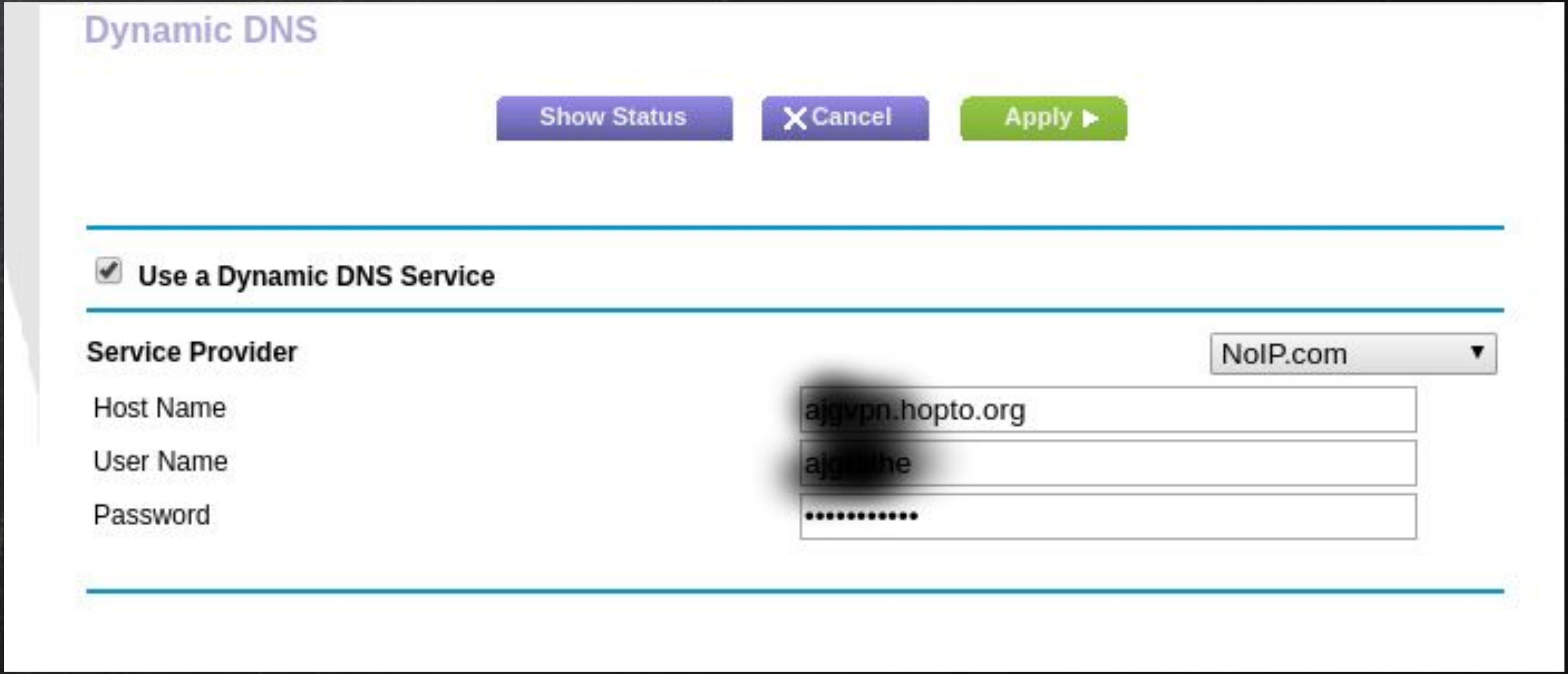
#7. Public IP or DNS

Another option is to run a client on your PI that will periodically check the external IP address and if needed update the DDNS entry. The client will be provided by the DDNS service you use.

There are quite a few DDNS services out there. I recommend noip.com since they have a free tier. A lot of other groups have gotten rid of their free tiers over time.

Noip.com forces you to login to their service every 30 days to renew your lease or you can pay them $25.00 a year and have it hang around.

#7. Public IP or DNS



Dynamic DNS

☑ Use a Dynamic DNS Service

Service Provider: NoIP.com ▾

Host Name: [redacted].hopto.org

User Name: [redacted]he

Password: ••••••••••••

#8. If OpenVPN Select Key Length

You’ll be given Several options for key length. I usually take the recommended length. You can choose more paranoid lengths, but they are slower than the recommended option.

#9. Unattended Upgrades

This will automatically install security updates from the distro vendor. You should always turn this on.

Keep in mind this won't reboot your system to finish installing the patches so you should on a periodical basis reboot the system so any partially installed patches are finished being installed.

#10. Reboot the System

Reboot the system so everything is in a clean state.

Completed Part 1

That completes Part 1. You now have a Pi setup to be a VPN. However you still can’t use it yet.   For that we have to setup a port forwarding rule.

This will direct traffic from the internet that hits your local router to hit the Raspberry Pi.

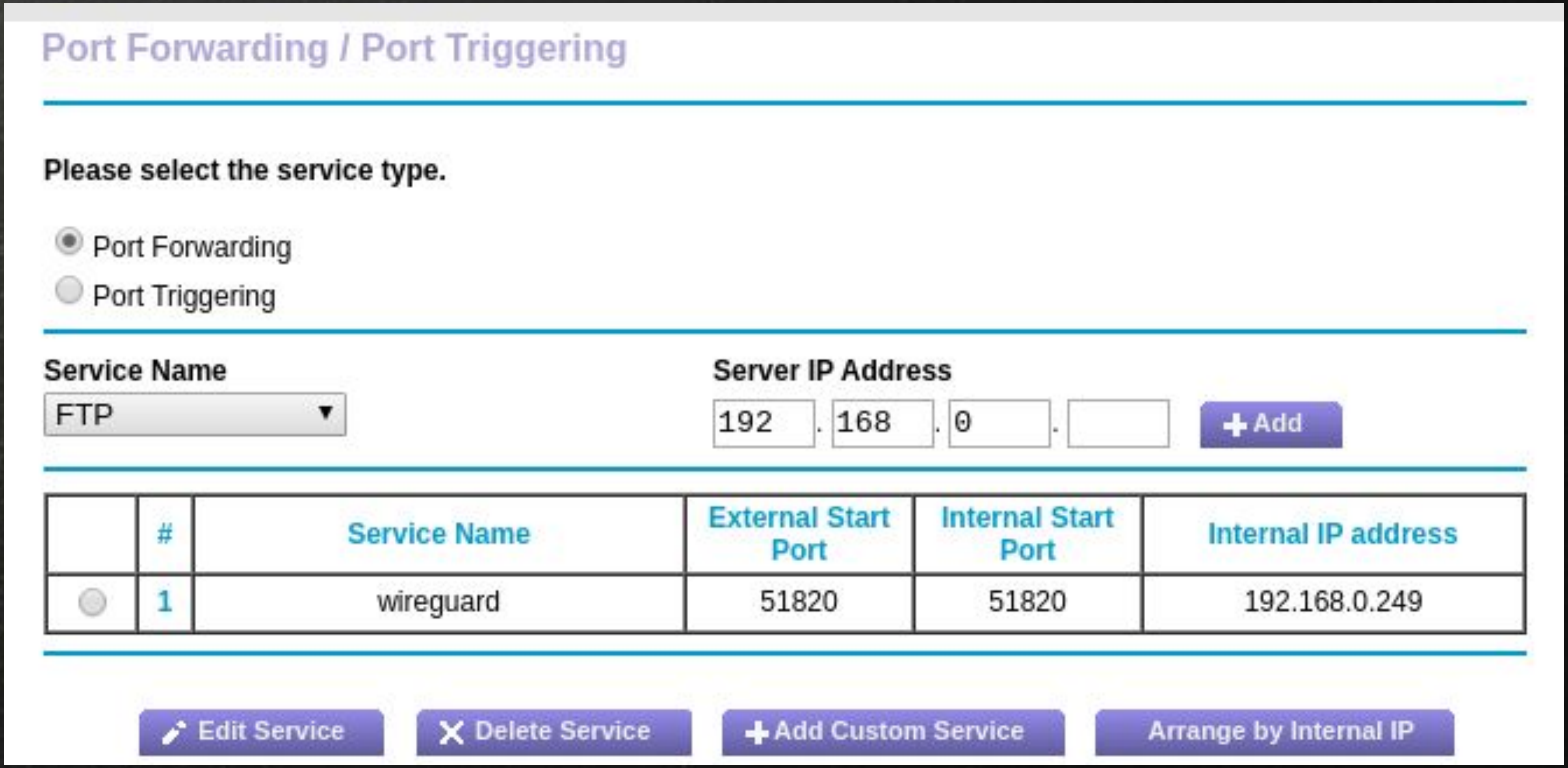
Port Forwarding Rule

For this you'll need to configure your router to forward the relevant port/protocol for the VPN

For Wireguard - Port 51820 and UDP
For OpenVPN - Port 1194 and either UDP or TCP

Internal IP address for Raspberry PI

What it Looks like in my Router



Port Forwarding / Port Triggering

Please select the service type.

● Port Forwarding
○ Port Triggering

Service Name: FTP ▾

Server IP Address: 192 . 168 . 0 .

	#	Service Name	External Start Port	Internal Start Port	Internal IP address
○	1	wireguard	51820	51820	192.168.0.249

Completed Part 2

So now we have configured VPN and have made the relevant changes to our Router to allow communication from the internet.

Next Step is to setup a client

Setting up a Client

For the first part of this will simply setup an android phone using the wireguard client from the Google Play Store

Need to run pivpn on Pi

First we'll list all the options available via pivpn

```
# pivpn
```

-a add a client lets do that one

```
# pivpn -a
```

Creating client config for test

```
pi@vpn:~/noip-2.1.9-1 $ pivpn -a
Enter a Name for the Client: test
::: Client Keys generated
::: Client config generated
::: Updated server config
::: WireGuard restarted
=============================================================
===============
::: Done! test.conf successfully created!
::: test.conf was copied to /home/pi/configs for easy
transfer.
::: Please use this profile only on one device and create
additional
::: profiles for other devices. You can also use pivpn -qr
```

We'll confirm that the Client is configured on the server

```
pi@vpn:~/noip-2.1.9-1 $ pivpn -c
```

Should see our configuration file for the client

Installing cert on Phone

Easiest way to do that is to generate a QR Code

```
# pi -qr
```

And select relevant client certification

Will display Client Cert, now just need to use the App to load the relevant cert

Installing on Phone

File containing all relevant info is also available in ~configs/xxx.conf file. You can enter that as well by hand but QR codes are faster, easier and less error prone.

```
[Interface]
PrivateKey =
CMGxkzVDT/EnRuld0z18OmqY+SObiqf20QfFFCY4fkg=
Address = 10.6.0.4/24
DNS = 192.168.0.1, 1.1.1.1
```

Testing on Phone

Lets list the clients on the pi

Hit a website or two on the phone

Update the client info again

```
% pivpn -c
```

Should see relevant information

Installing the client Software on Systems

Hit wireguard.com for installation instructions

Example for Debian

```
echo "deb http://deb.debian.org/debian/ unstable main" > /etc/apt/sources.list.d/unstable.list
printf 'Package: *\nPin: release a=unstable\nPin-Priority: 90\n' > /etc/apt/preferences.d/limit-unstable
apt update
apt install wireguard
```

Quick Notes

Copy relevant conf file from ~pi/configs over to linux system

```
# scp pivpn@remotesystem:configs/configfile /etc/wireguard/configs/wg0.conf
# wg-quick up wg0 - to start it up to test
```

To set wireguard to start automatically

```
# systemctl enable wg-quick@wg0
```

Quick Notes: Continued

The quality of tools for configuring Wireguard is still coming along on Linux.

Pretty soon it will probably just be a part of the network manager and the setup won't require any command line configuration.

Right now it is still a bit of a PITA.

Performance Hit

Straight up you're going to take a performance hit. This is part of using a VPN.

Tests done with Speed of Me (Android Phone)

Performance Hit

Straight up you're going to take a performance hit. This is part of using a VPN.

Tests done with Speed of Me (Cloudbook)

Typically lose about 25% of my network performance

Go from 176.76 (Mbps) download to 123.41 (Mbps) for network

Over 4g network performance hit seems to be closer to about 50-75% at my house. I also have crappy 4g at my house and the overhead of encryption is more overall.

Is it worth it?

Quite simply for the peace of mind it gives me I think it is well worth it to have PI-VPN running on my home network.

Also think the ability to create a temporary VPN out on a VPS for work/travel/conferences is quite nice.

Give it a try. I think you'll be impressed by how well it works.

Things to Consider

Update your VPN software every now and then.

```
# pivpn -u
```

Reboot it every now and then to keep it up to date

Pivpn.io has a pretty good community. Some enhancements I'd like to see. The ability to run both OpenVPN and Wireguard are under consideration.

Possibly a micro-k8s implementation with a watchtower type upgrade approach might be kind of interesting.

Alternatives

I did a talk about rolling your own VPN at NEbraskaCERT last year - https://www.nebraskacert.org/csf/CSF-Jul2019.pdf

In it I discussed the following

Outline by Jigsaw
Streisand
Algo VPN

Outline by Alphabet

Has some nice components - is docker based so it separates the VPN part from the base O/S, updates are pretty robust

Has a good gui for both client/server and the installation tools work pretty well. As well as apps in the Play Store/Apple Store.

Every now and then would quit working on my phone and I gave up on it.

Alphabet says it isn't a VPN, but suggests may be worthwhile for journalists.

Streisand

Is worthwhile to give it a spin. I never got it to install successfully in my several attempts with it. Could be me.

Has a lot of tinfoil hat worthy capabilities - Create certs and then clean up all traces of them on your system. Make sure you're using very paranoid settings and so on.

Has a good user community. Uses OpenVPN and wireguard, worth looking at for ideas that might be interesting to incorporate into PI-VPN

Algo VPN

Supports Wireguard so you can use same apps on your phone/tablet

Upgrades are a bit interesting. They suggest deploying a new instance for changes. No official releases, is based upon git clone/pulls

Summary - Q & A

If you have a spare Raspberry PI and want to have it do something useful I highly recommend turning it into a VPN. PI-VPN makes it pretty darn easy. Makes me feel safer on my phone/pc when I'm connected to untrusted Wifi.

You can learn a lot of stuff along the way.

Thanks for Listening.

Links

PiVPN - https://www.pivpn.io

Wireguard - https://www.wireguard.com