Roll Your Own VPN???

July 17, 2019 - CSF NEbraskaCERT

by Aaron Grothe

Who am I?

Information Security Professional

Member of the Board of Directors for NEbraskaCERT since 2004

Linked In Profile:

https://www.linkedin.com/in/aaron-grothe-1b89271/

Couple of Things

- If you have a question during my presentation, please feel free to ask anytime. You don't need to wait until the end
- If I start to mumble or am speaking way too fast please let me know. I do that sometimes

Goals

Goals for Today are as follows

- Talk a bit about VPNs
- How to make smarter VPN decisions
- Talk about rolling out your own VPN
  - How hard is it?
  - Is it worth it?
  - How secure is it?

Why your Own VPN?

Study finds half of the most popular VPN apps linked to China

https://www.ft.com/content/e5567d8a-ee65-11e8-89c8-d36339d835c0

App include TurboVPN, VPN Proxy Master, VPN 360 and Snap VPN.

Total number of downloads on iphone and android devices more than 100 million times.

Some of the user terms of agreement even mention they'll share your data in Terms of Service

VeePN - An Example VPN

- One of the VPNs that are available in a lifetime option from StackSocial - https://stacksocial.com/collections/exclusive-lifetime-vpn-protection

VeePN Summary

- Based in Panama - Good country wrt to Privacy
- Many servers (2500+) in many countries (42+)
- Keeps "minimal session logs" amount of web traffic for each session and session dates
- Policies are of course subject to change

Other VPNs

- Quality of a VPN varies a great deal from company to company. Some are designed for privacy and some are designed for marketing
- VPN companies policies are regularly changed because of acquisitions, mergers, new management and so on
- Recommend you research quite a bit before you trust a VPN. Some of them such as NordVPN have pretty good reputations
- Personally I've probably played with over 10 different commercial VPNs over the last few years. Last one I used was RawVPN.

What Do you Want from your VPN?

- To protect your data from being snooped on in the Coffee Shop
  - Have to mention wifi pineapple, wifi pumpkin here
- To hide what sites/data you are accessing from your device
- To remove ads/trackers from sites that you are accessing
- To route data over TOR transparently
- To be able to watch Netflix UK?

What I'm looking for from a VPN

- To protect the data coming off my device from to the internet

Three Options I've Tried

Outline by Jigsaw
Streisand
Algo VPN

Also in the past have played with options like setting up my own openvpn and running stunnel and so on. Usually dropped doing these after a period of time.

Typical Install of Your Own VPN

1. You use your desktop machine to install software VPN
2. Generate an access token to your Hosting Provider
3. Run install software that will then create a NEW droplet/instance/vm, etc
4. Software on your desktop continues to drive the install
5. Install VPN software on client machines
6. Distribute keys to machines using VPN
7. VPN!!!

Typical Install of VPN (Cont'd)

- There are a lot of other options during the install
- Most of the software have multiple options
  - install on a machine that is already configured, nice if you've already got a VM running
  - Generate install scripts so you can recreate the install
  - Configure options

My Outline Deployment

Setup a Vultr account in London, UK initially

- Wanted to see about the netflix testing
- Installation on Linux pretty easy
  - Downloaded appImage on Linux and fired it up
  - Fire up your cloud host
  - Run a bash command to pull latest version of software
    - Creates a couple of docker containers
    - Put the API key into your locally running outline manager
    - Generate a key and send to your device
    - Install outline app on your device
    - Install key on your device

My Outline Deployment (Cont'd)

- Total time to get up and running about 30 minutes
- Total cost - $5/month
- Notice I decided not to use the default installer because I wanted to see what options were available
- Has good support for doing server setup from Mac/Linux and Windows

Outline Results

- Results from what is my ip : show the VPN's address
- Netflix Test
  - Shows UK shows (Star Trek Discovery)
  - Unable to stream shows, netflix blocks off Hosting providers by default
- Updates
  - For android/iphone devices handled by itunes/google play store
  - For systems handled by watchtower
- Mom & Dad test
  - Could my Mom & Dad install it? With some help and a good chunk of reading I believe so, but they'd really complain about it. Odd of success 90%

Streisand (Install)

Success is rarely total. Failure on the other hand :-(

Has a lot of options: Tor, OpenVPN, Wireguard, many, many others.

Initally tried to setup on my vultr account. Made a lot of mistakes on it.

- Used CentOS - Steisand seems to go a lot better with Ubuntu
- Used vultr for hosting initially, moved to Digital Ocean for second attempt
- Chose defaults which also appears to be a failure
- Tried bunch of options, times and eventually gave up

Streisand Install (Cont'd)

Closest successful attempt
Setup two nodes

- One setup to control installation
- Second created by steisand app during installation
  - Chose defaults throughout
  - Built multiple times eventually dropping down to Ubuntu 18.04, documentation "suggests" 16.04 so that could be part of it
- Ran into timeouts with gpg keyring access
- Interesting project

Streisand Results (Cont'd)

- Invested several hours into it
- Has a good user community behind it, many suggestions but not a lot of success for me
- Would probably just setup up own VPN system instead
- Several sites say it can be installed in 10 minutes, so maybe it is just me
- Odds of Mom & Dad succeeding in installing/configuring 10%, which is higher than I gave myself since I figured they'd read the instructions more carefully

Algo VPN Install

- Has some interesting options: Blocking Ads via DNS blackholes
- Install went pretty well
  - Took defaults for almost everything
  - Has a lot more configuration options than Outline
  - Typical install (client created instance in Digital Ocean and did all the installation)
  - Used wiredrop for the VPN option
    - Used the QR code .png file options to import key to Android device
  - Has deprecated some of the older protocols to increase security
    - Can still be optionally enabled

Algo VPN Install (Cont'd)

- Configured with 3 keys (Desktop, Phone, Laptop) - also the default names
- Added my Digital Ocean access key during the install and let the script take care of it
- Took about 30 minutes overall to install/configure and run
- Setup to use the WireGuard app
- Told it to put the droplet in London
  - Passed IP test
  - Also failed the Netflix test

Algo VPN Results (Cont'd)

- Still in heavy development
  - Upgrades are your responsibility
    - Client side is handled by App Stores
    - Server side, they suggest deploying a new instance for changes
    - There are no official releases currently. It is a git baby
- That being said, it installed for me from a Debian 10 (buster) instance without any major issues
- Odds of Mom & Dad success over 50% which is pretty good
- Odds of them using it/keeping it patched 0% :-(
- Was designed for corporate traveler so it matches up well with my requirements

True Roll Your Own

You can truly "Roll Your Own" VPN

- Create a Certificate Authority (CA) - OpenSSL and some GUI tools
- Wireguard, OpenVPN, Stunnel and other software options can be installed client and server
- Configuration, rollout and so on
- Total control and total responsibility
- Odds of Mom & Dad Success - -10% (Not Gonna Happen)

Questions to Ask

- Has the software been audited?
  - Outline - Yes by Radically Open Security and Cure53 - public reports are available
  - Stresisand/Algo - Not yet are open to it
- Have they had security issues?
  - Outline - early versions of Outline prior to 1.2 didn't encrypt all Windows traffic
  - Streisand - has had some issues with code (insufficent randomization of variables and some others)
  - Algo VPN - none that I'm aware of. Is a smaller project than both of the others.

Questions to Ask (Cont'd)

- How do I keep it up to date?
  - Outline (watchdog automated updates)
  - Streisand (looking for volunteers to help write solution)
  - Algo (deploy a new one you hoser)
- What clients does it support
  - Outline custom client (MacOS, Android, iOS, Windows, Linux)
  - Streisand has OpenVPN/Wireguard client support so will support about everything
  - Algo also has OpenVPN/Wireguard clients

Questions To Ask (Cont'd)

How much care do I need to provide?

- Outline autoupdates, pretty much takes care of self
- Algo/Streisand - have to periodically redeploy
  - Bringing over the configurations is a manual process currently so you'll have to figure it out. Both of them have documentation to help with this
- Algo/Streisand are both written in Python 2.7 so they'll have to be updated shortly to Python 3 (January 2020 - Python 2.x goes into maintenance mode)

Questions to Ask (Cont'd)

Who do you trust?

- Outline - Do you trust Jigsaw/Alphabet?
- Streisand/Algo VPN - both have small groups of contributors you're trusting not to backdoor your access key for your cloud service provider

Basic cleanup

- If you use the wizard for the install, remove the Personal Access Token to your Cloud account that you generated for the VPN install
- Change any passwords, etc after install

What I've installed

- I went with Outline
  - Manually installed via the curl | bash install
- Used Vultr to host VPN
  - Host in NJ - $3.50 month - $42/year
  - 10Gb disk space, 0.5gb ram, 500gb transfer monthly
  - Centos 7
    - Yum-cron for autoupdates

Initial Review of Outline

Works pretty well

- Performance hit isn't that noticeable
- Speed of me without Outline turned on
  - DL 46.48 Mbs / UL 2.25 Mbs
- Speed of me with Outline turned on
  - DL 37.25 Mbs / UL 2.63 Mbs
- Would be nice if there was a tool for doing the VPN automatically (No VPN at home, VPN everywhere else). There are some apps that support Geofencing so is doable, or by time.
- Still forget to turn on and off periodically. Pretty much just leave it on by default unless I have an issue.

Q & A

Any Questions?

Thanks for listening.

Links

Outline

https://getoutline.org/en/home

###

Streisand VPN

https://github.com/StreisandEffect/streisand

Links (Cont'd)

Algo VPN

https://github.com/trailofbits/algo

Install Yum-Cron for security updates

https://www.howtoforge.com/tutorial/how-to-setup-automatic-security-updates-on-centos-7/