Field Security Basics
VPNs and not-so-hotspots

YARDELL PERKINS
YARDELL@PERKITECH.COM
PERKITECH.COM

Presentation Outline

- Our Current relationship with public hotspots
- Review of some provider's ToS'
- Brief discussion of WiFi dangers
- How VPN's work and how to pick a provider
- How to use a VPN Service
- Portable Hotspots

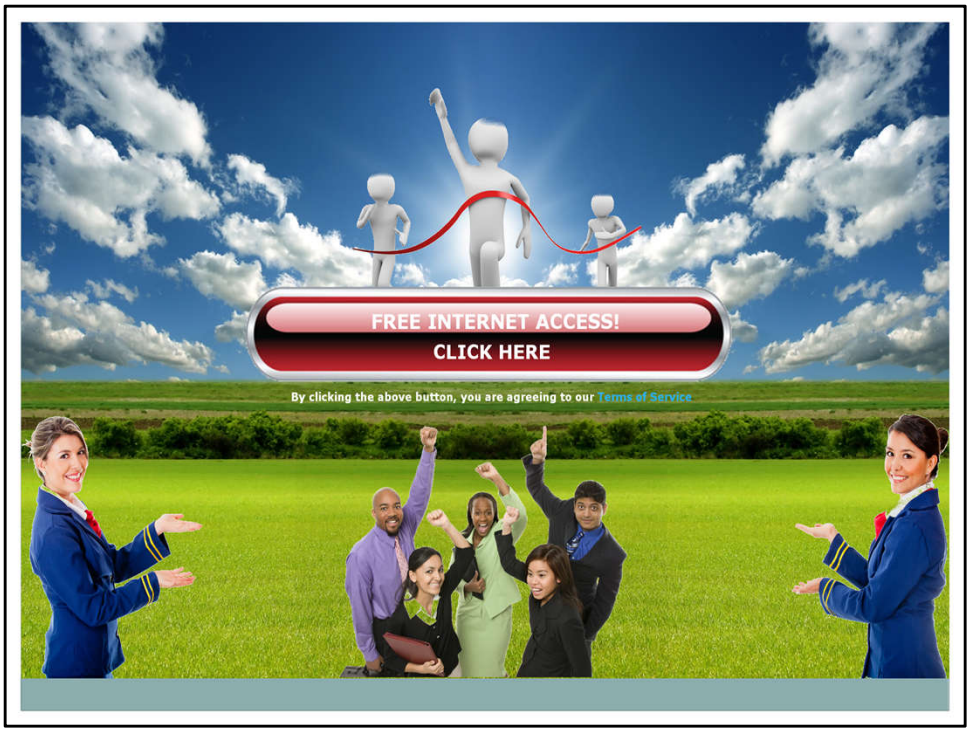
Wait a sec…."Who Is This Git?"

- Yardell (@yardper)
- Perkitech (perkitech.com)
- 10yrs Computer Repair
- 2+ yrs Systems Adm
- 2+ yrs Web Dev & Design

A Little About Telecommuting…

- Our work is very easy to decentralize
  - Little needed in the way of furniture, hardware, personnel
- Our "offices" can be anywhere, even "home"
  - Regular work-at-home, *among the non-self-employed population*, has grown by 103% since 2005.[1]
  - 3.7 million employees now work from home at least part time.[1]
- At some point, we migrate to some "public" workspace
  - Coffeeshop or coworking space
  - Main Benefit: Shared motivation of others

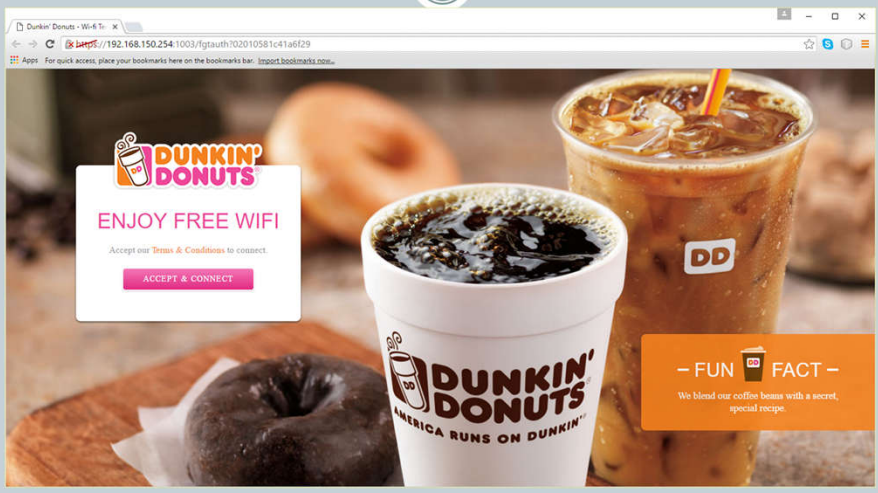
Your “Previous” Routine…


FREE INTERNET ACCESS!
CLICK HERE
By clicking the above button, you are agreeing to our Terms of Service

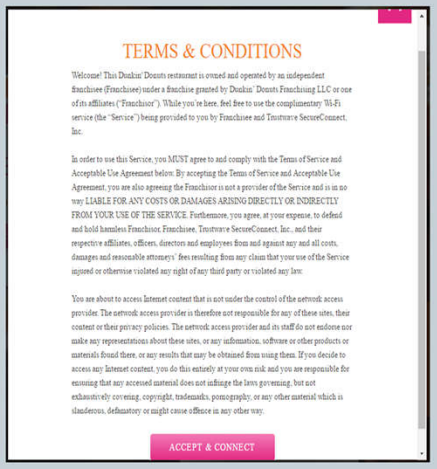
Spots I Researched

- Three Major Franchises
  - Starbucks
  - Dunkin Donuts
  - McDonalds
- "Follow In My Footsteps"
  - Odds are you will run into one of the first two
  - Duck in and see their ToS for yourself
  - Go somewhere else, boutique spot, more likely think to check their own (if they have one)

Dunkin Donuts “Happy” Splash



Dunkin Donuts ToS



TERMS & CONDITIONS

Welcome! This Dunkin' Donuts restaurant is owned and operated by an independent franchisee (Franchisee) under a franchise granted by Dunkin' Donuts Franchising LLC or one of its affiliates ("Franchisor"). While you're here, feel free to use the complimentary Wi-Fi service (the "Service") being provided to you by Franchisee and Trustwave SecureConnect, Inc.

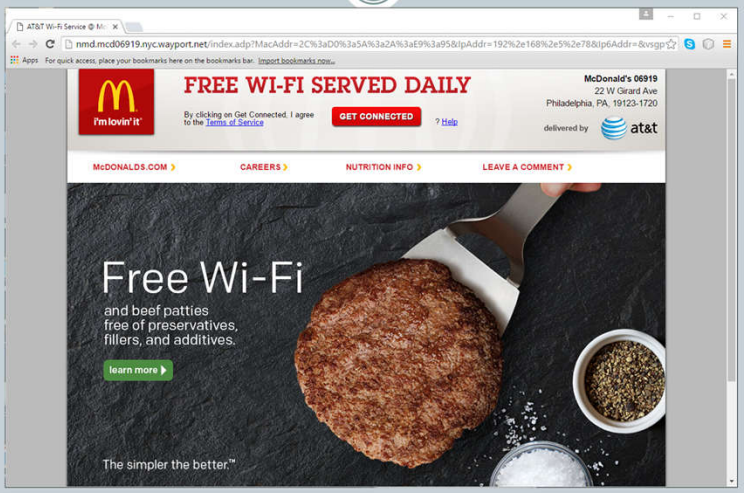
In order to use this Service, you MUST agree to and comply with the Terms of Service and Acceptable Use Agreement below. By accepting the Terms of Service and Acceptable Use Agreement, you are also agreeing the Franchisor is not a provider of the Service and is in no way LIABLE FOR ANY COSTS OR DAMAGES ARISING DIRECTLY OR INDIRECTLY FROM YOUR USE OF THE SERVICE. Furthermore, you agree, at your expense, to defend and hold harmless Franchisor, Franchisee, Trustwave SecureConnect, Inc., and their respective affiliates, officers, directors and employees from and against any and all costs, damages and reasonable attorneys' fees resulting from any claim that your use of the Service injured or otherwise violated any right of any third party or violated any law.

You are about to access Internet content that is not under the control of the network access provider. The network access provider is therefore not responsible for any of these sites, their content or their privacy policies. The network access provider and its staff do not endorse nor make any representations about these sites, or any information, software or other products or materials found there, or any results that may be obtained from using them. If you decide to access any Internet content, you do this entirely at your own risk and you are responsible for ensuring that any accessed material does not infringe the laws governing, but not exhaustively covering, copyright, trademarks, pornography, or any other material which is slanderous, defamatory or might cause offence in any other way.

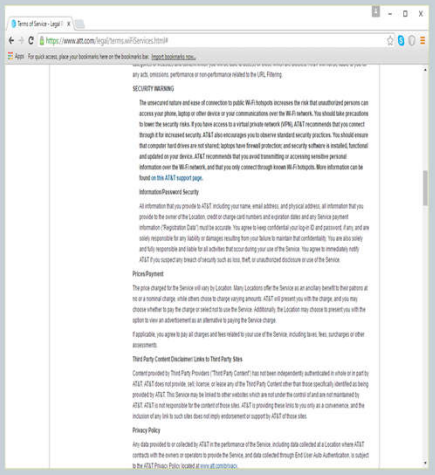
ACCEPT & CONNECT

- Most Concise
  - Fits into a single sub window
- Can easily skim
- Gist of their ToS
  - Don't be a web jerk
  - Anything goes wrong, its on you

McDonalds “Happy” Splash



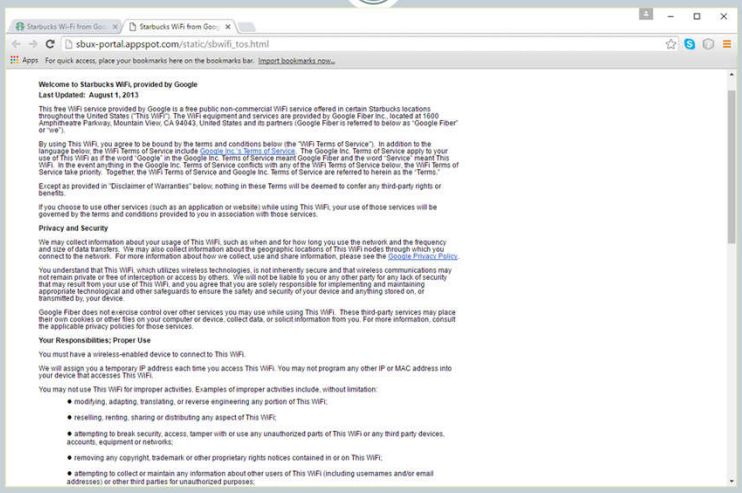
McDonalds ToS



- Typical ToS Length / Legalese
- "Security Warning"
  - Public WiFi's are generally unsecure
  - Suggest making use of a VPN service while on their network
- Data Collections
  - Collect metrics info
  - Nothing personal without notifying you, and with consent

Starbuck's "Happy" Splash

Starbucks ToS

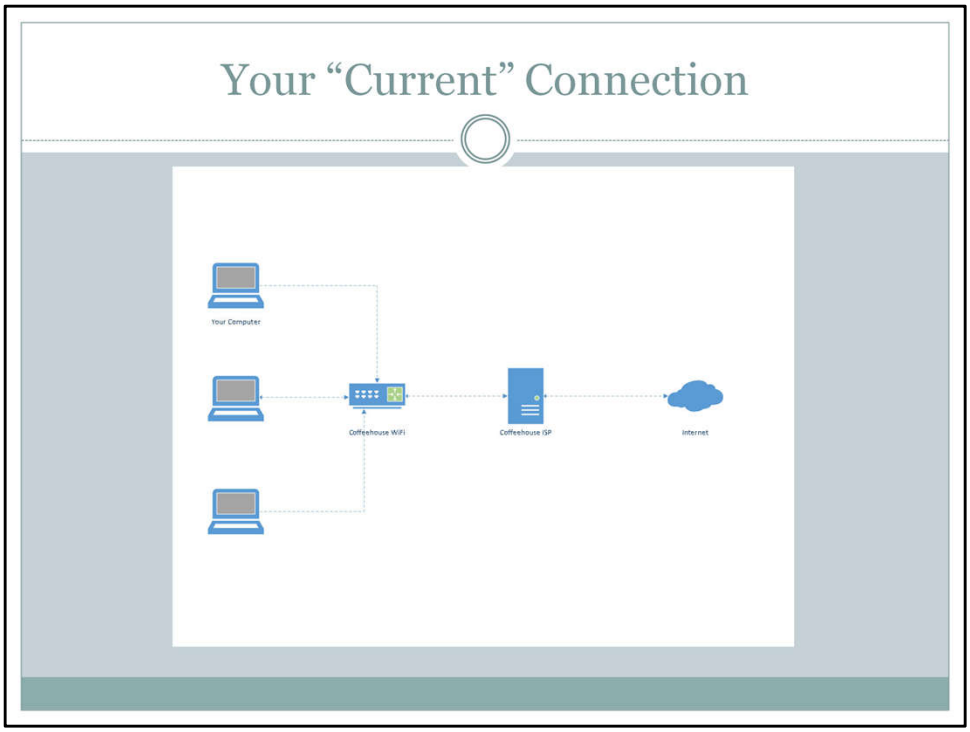


Starbucks ToS (Cont.)

- They will give you a temporary IP
  - You cannot program any other IP or MAC address into your device while using their network.
- This WiFi is not inherently secure and (any) wireless communications may not remain private or free of interception or access
- "We reserve the right to monitor, intercept, and disclose any transmission on or using our facilities, and to provide user information, or use records and other related information under certain circumstances
  - Lawful process, orders, subpoenas, warrants, Google, Persons
  - …"for Reasons"

"Nothing to hide, Why Hide Anything?"

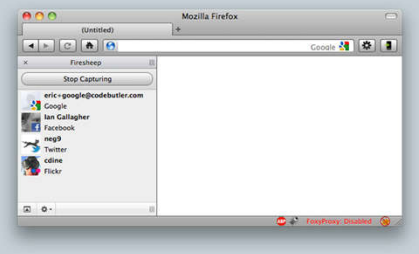
- Right to Privacy ≠ Obfuscation of an illicit act
- "Innocent UNTIL proven guilty
  - You're accused of something, typically the burden of proof is on the "Accuser"
  - If I say: "You stole a box from 3rd street at 5pm"…
    - I have to prove that you did
    - You don't necessarily have to prove that you didn't
  - The 2nd and 3rd thing you hear in an arrest
    - You have the right to remain silent
    - Anything you say may be used against you in a court of law

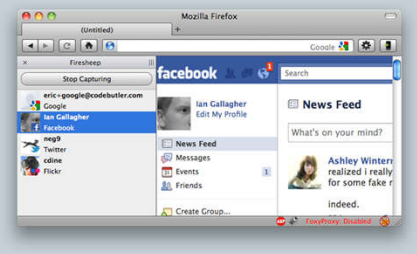

Your "Current" Connection
Your Computer
Coffeehouse WiFi
Coffeehouse ISP
Internet

“Firesheep”

- http://codebutler.com/firesheep
- Firefox Extension
  - Grab a user’s session cookie to a site to gain their login information
  - On a public network, those cookies are periodically passed through the air usually unencrypted.
  - Dated (2010) but nonetheless prime example

“Firesheep” (cont.)





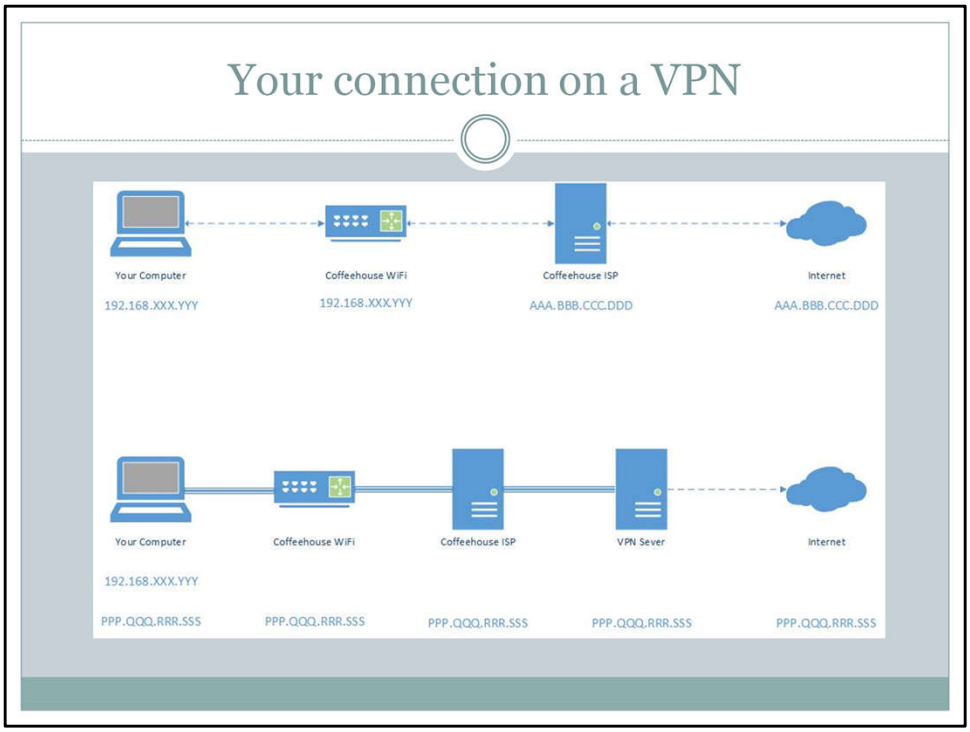
The "TL;DR"

Take some time to understand what you're signing ***onto*** when you sign ***into*** any public hotspots

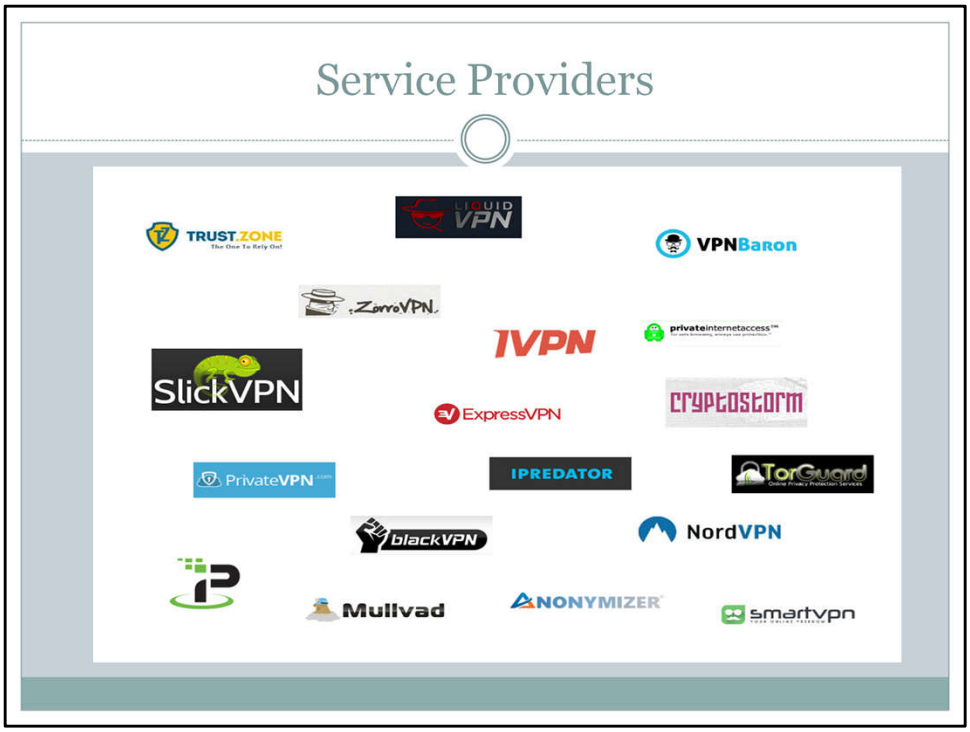
- Skim the ToS
- Screenshot and Save for Later
- If you can't find one, find another place to work

What is a “VPN”

- Wikipedia:
  - A private network that extends across a public one
  - https://en.wikipedia.org/wiki/Virtual_private_network


Your connection on a VPN
Your Computer
192.168.XXX.YYY
Coffeehouse WiFi
192.168.XXX.YYY
Coffeehouse ISP
AAA.BBB.CCC.DDD
Internet
AAA.BBB.CCC.DDD
Your Computer
192.168.XXX.YYY
PPP.QQQ.RRR.SSS
Coffeehouse WiFi
PPP.QQQ.RRR.SSS
Coffeehouse ISP
PPP.QQQ.RRR.SSS
VPN Sever
PPP.QQQ.RRR.SSS
Internet
PPP.QQQ.RRR.SSS

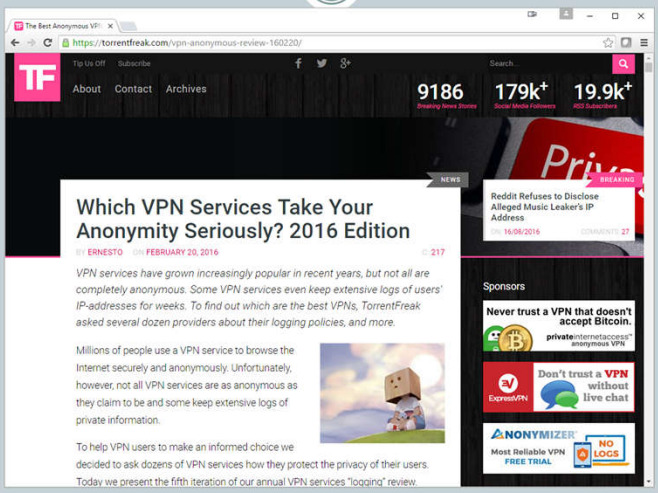
Service Providers



Some Things To Look For…

- Server Locations
  - 2-3 servers of geographic ***proximity*** to you
  - 1-2 servers of geographic ***significance*** to you
- Connection Security
  - IKEv2 – One of the stronger ones, but can be "heavy"
  - OpenVPN – All around ideal encryption protocol
  - SSTP – Meh
- Hardware / OS Support
  - You can use it on anything you'd likely use it on.
- Customer Support Access

TorrentFreak – Yearly VPN Services Article



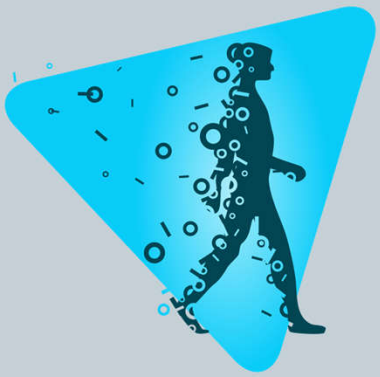
Article Suggestion…

- https://torrentfreak.com/vpn-anonymous-review-160220/Yearly Article
  - Feb – March
  - Home page - > “About” link
- Contacted Several of the major and minor VPN providers
- Asked twelve pointed questions about their offerings
  - What / Where / How of their services
  - Payment Options
  - Operating Jurisdictions

More Pertinent Questions…

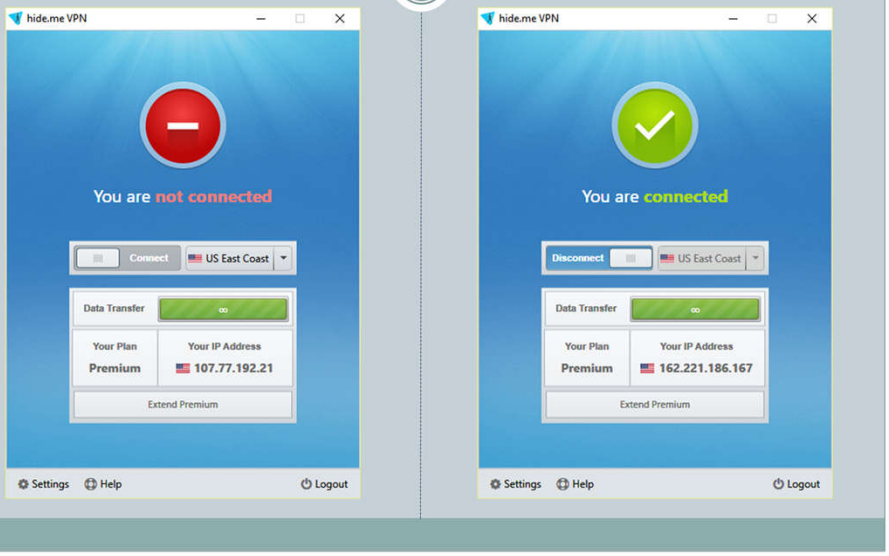
- What Countries are your servers located in?
  - Do you have physical control over your VPN servers and network or are they hosted by/accessible to a third party? ("Plus" if they do, not necessarily a "Minus" if they don't)
- What is the most secure VPN connection and encryption algorithm you would recommend to your users?
- Do you offer a custom VPN application to your users?
  - If so, for which platforms?

My Personal Pick: “Hide Me”

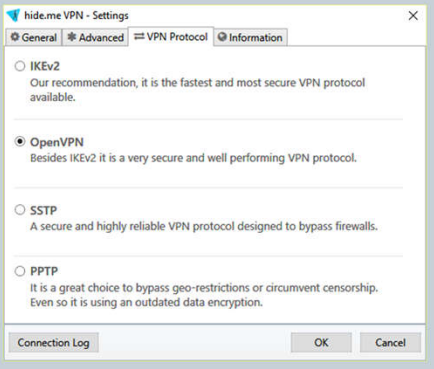


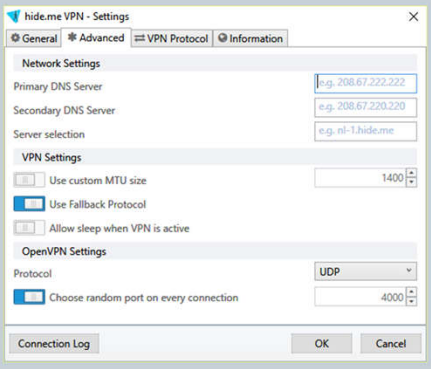
- https://hide.me/en/
- Metrics
  - Servers in 29 locations / 21 countries
    - Closely partnered with the server managers
  - Highest Encryption: IKEv2
  - Support all major hardware / software platforms

General Client Operation



App Advanced Settings





The “Extra” Mile – Personal Hotspots

- About the size/shape of a cellphone, if not smaller
- Connects through a cell network solely for data
  - Data pool separate from your cellphone data pool
- Current smartphones can do this…
  - May not be able to take calls or calls will break the connection

General Operation Notes

- Want the encryption at the "Last Mile"
  - Turn on JUST the laptop app (preferably) or just the phone app.
    - Don't need both
- Familiarize with your providers security options
  - Some sites will slow down or "complain" about a VPN connection
  - Lowering the encryption level

Thank You

- SLIDES/ASSETS WILL BE ON THE WEBSITE BY 8/21
- TINYURL: HTTP://TINYURL.COM/HBTY5CX
- QUESTIONS /COMMENTS
- YARDELL@PERKITECH.COM

- 1) Latest Telecommuting Statistics
  - http://globalworkplaceanalytics.com/telecommuting-statistics