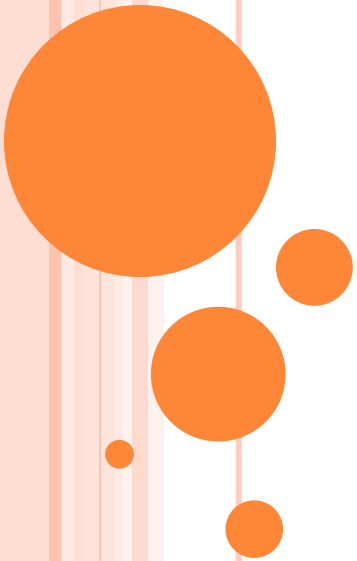
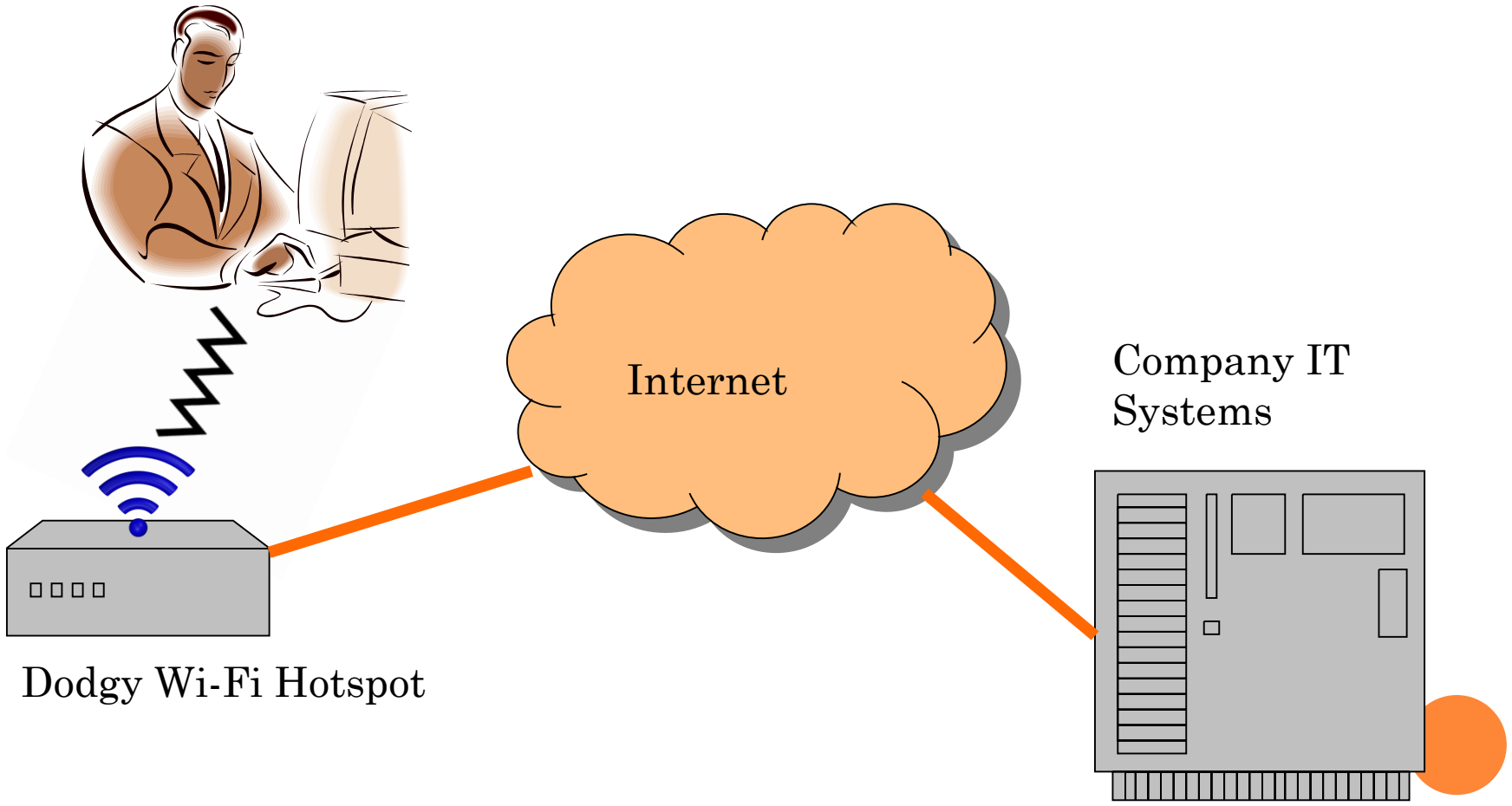


Using a raspberry pi as a vpn server

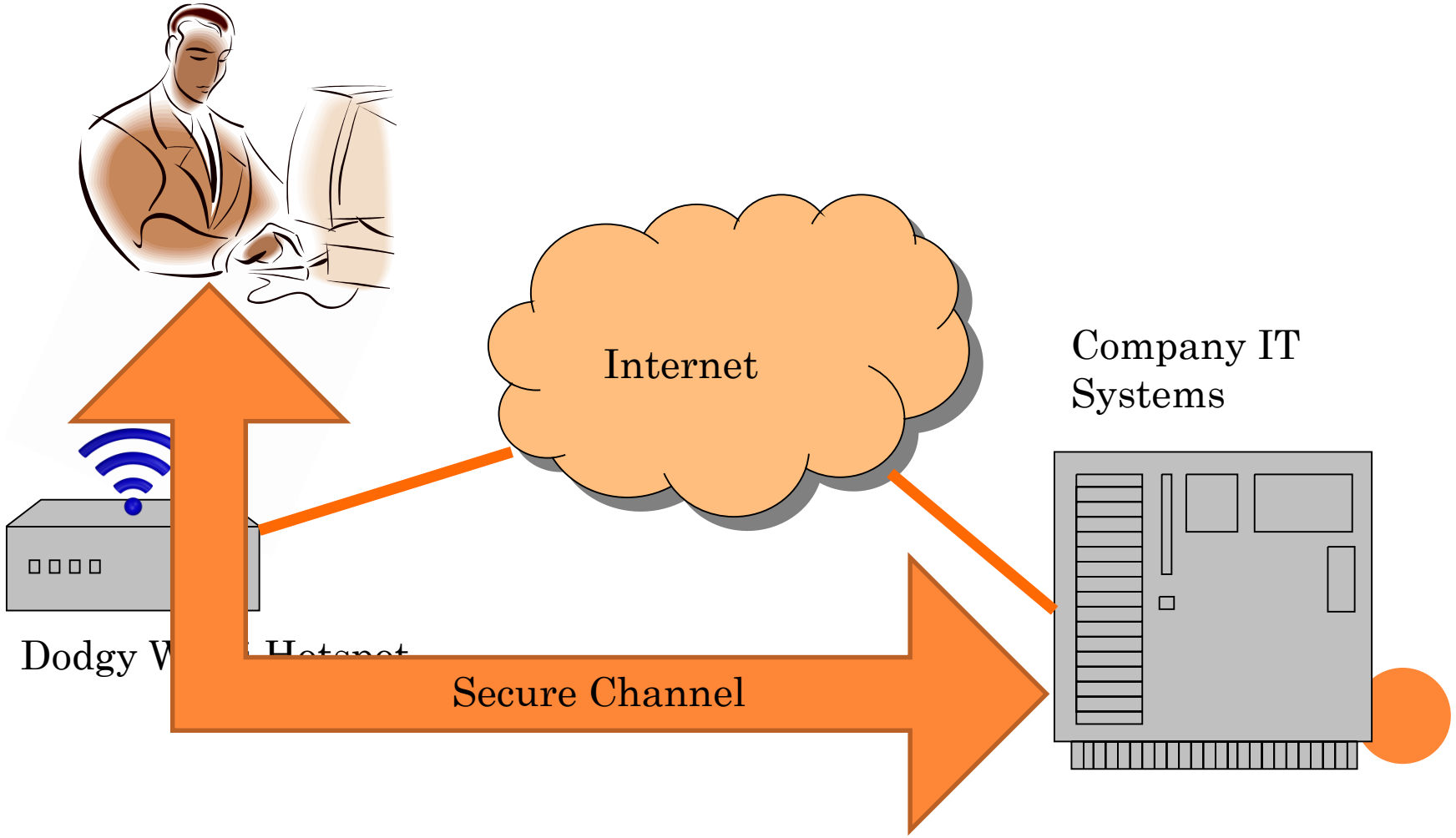
What is a VPN?

- A VPN is a “Virtual Private Network”
- It is designed to secure the link from a device such as a phone or PC to a remote server.

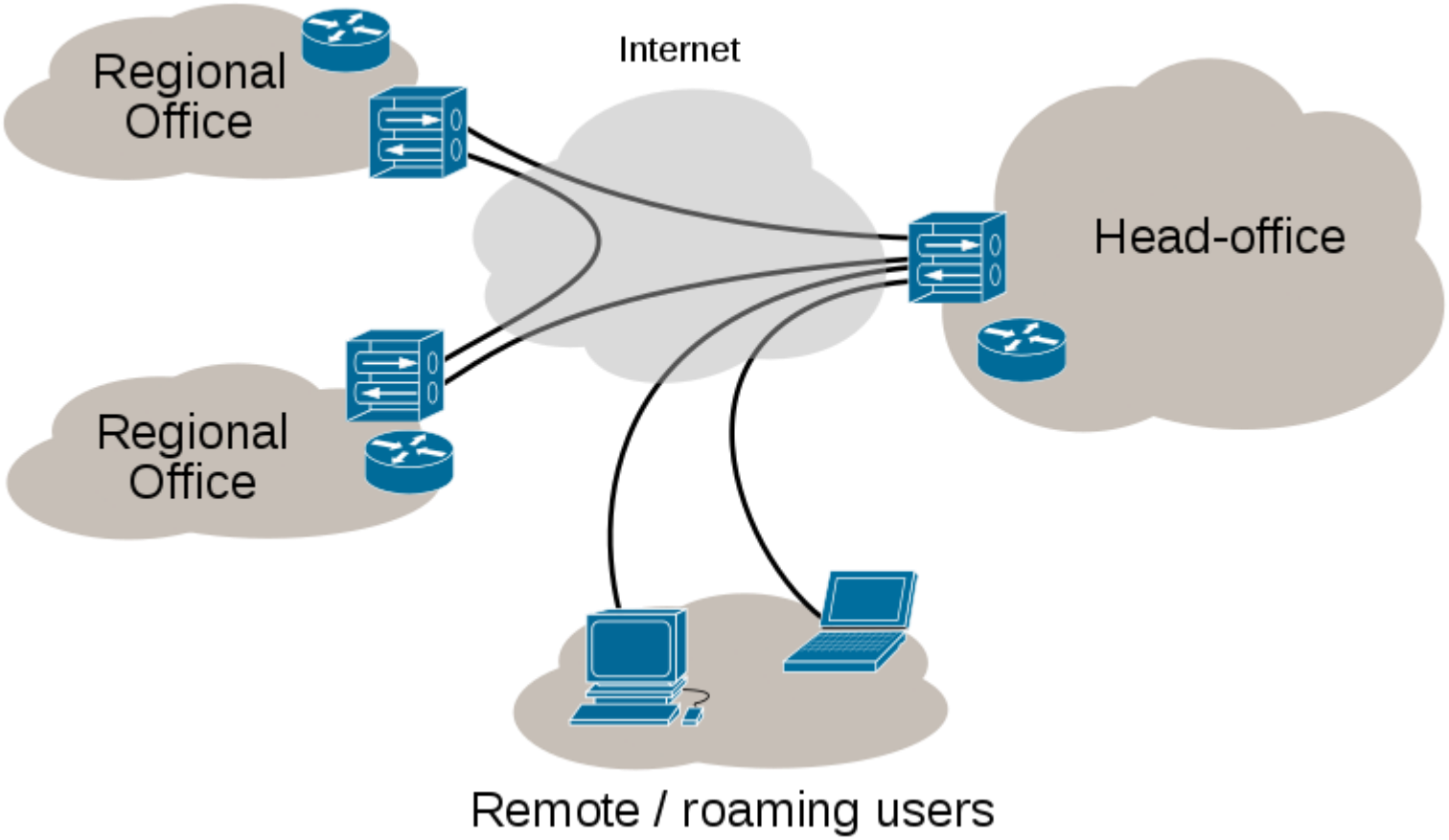
Corporate VPN Access



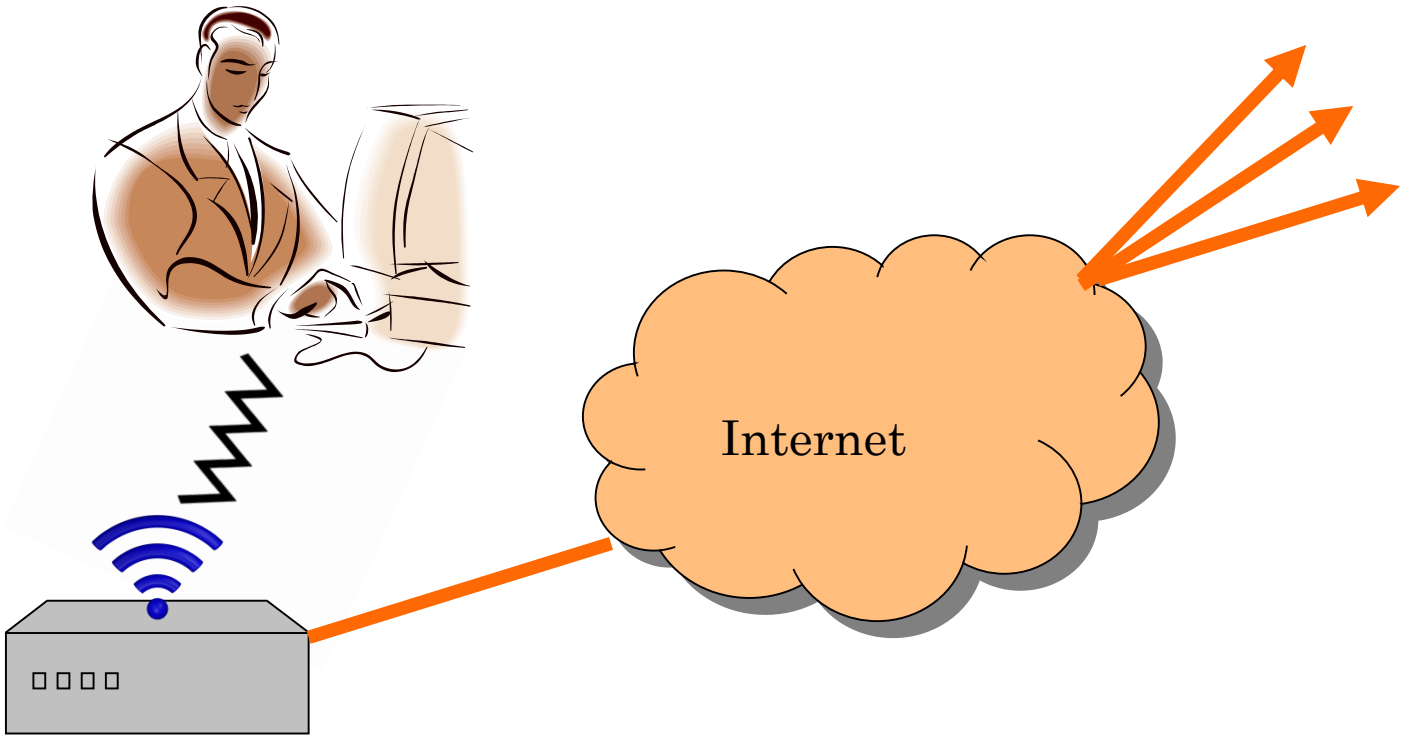
Corporate VPN Access



Corporate VPN

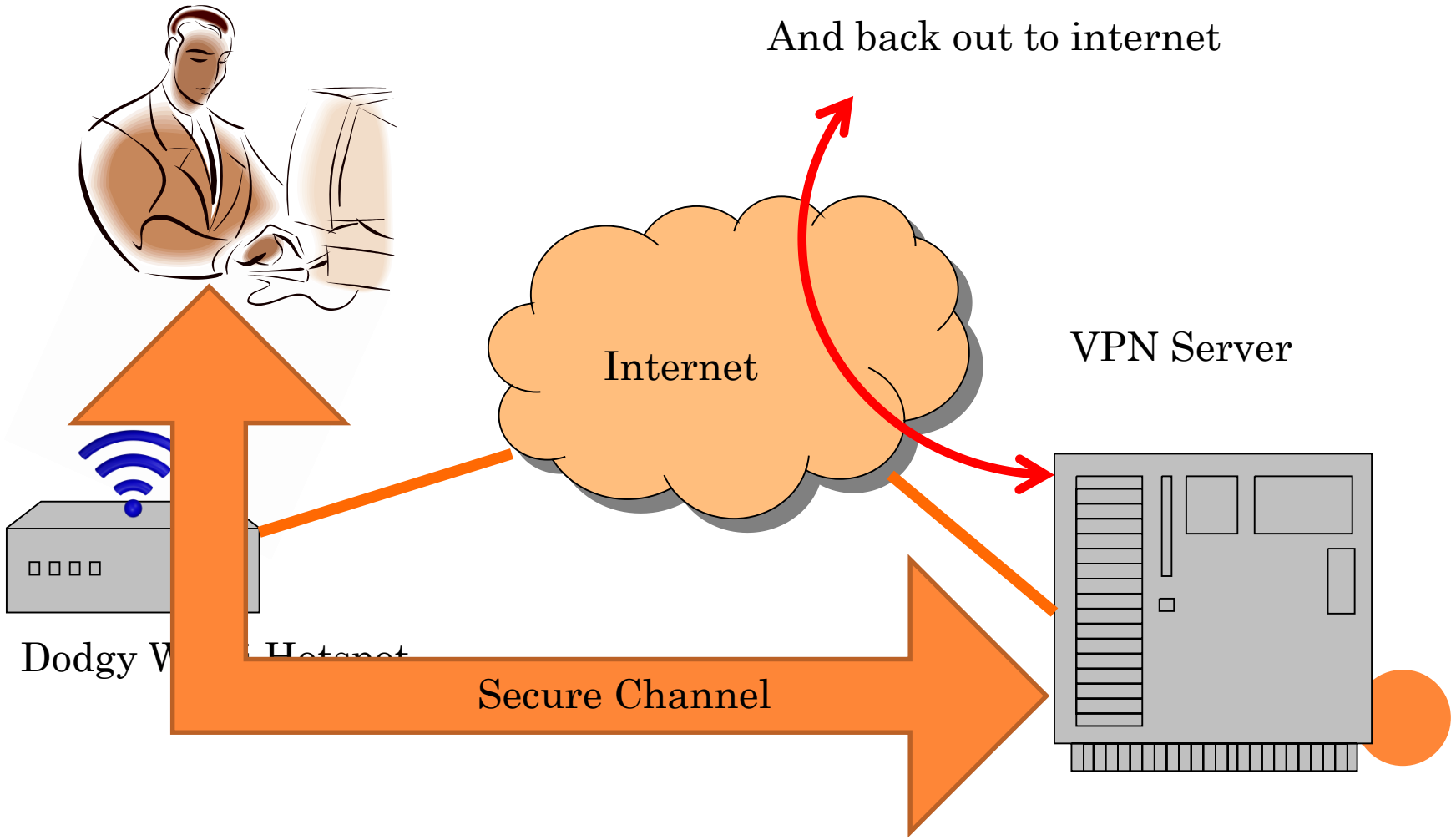


Consumer VPN



Dodgy Wi-Fi Hotspot

Consumer VPN



On the TV and social media recently

- Seen adverts like this?.....

https://www.bing.com/videos/search?q=youtube+nordvpn+advert&view=detail&mid=56A55C37C84871AD978856A55C37C84871AD9788&FORM=VIRE

Why use a VPN?

- Most of these adverts are scaremongering
- There are occasions where it makes sense
  - Corporate PC network access
  - Using untrustworthy Wi-Fi hotspots
  - If you are paranoid

- I manage a couple of websites that, like the WARC website, do not use TLS
- But I manage them from my phone so a Wi-Fi hotspot can see the admin password in clear

EXAMPLE

- Let's log on to the WARC website…..

More VPN types than you can shake a stick at

- PPTP (Point-to-point Tunneling Protocol)
- L2TP (Layer 2 tunneling protocol) & IPsec
- SSTP
- SSL
- IKE V2
- MPLS (Multi-protocol Label Switching) VPN
- Hybrid VPN such as (combined SSL & IPsec)
- Wireguard

- And so the list goes on. OpenVPN is a form of hybrid VPN

OpenVPN

OpenVPN is an open-source commercial[10] software that implements virtual private network (VPN) techniques to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol[11] that utilizes SSL/TLS for key exchange. It is capable of traversing network address translators (NATs) and firewalls. It was written by James Yonan and is published under the GNU General Public License (GPL).

OpenVPN

- OpenVPN is used by commercial companies to offer consumer VPN services.
  - You pay them a fee
  - You download the client software
  - You use it to connect to their server
  - Your traffic is routed securely to their servers and routed back to the internet from their server
- Or you can put together your own server.
- The VPN protects against security risks on the link from your client to the server (for example Wi-Fi hotspots)

OpenVPN protocol

- Uses X.509 certificates to authenticate client & server
  - e.g. 2048 bit RSA with SHA-384
- Uses these certificates to establish a TLS link.
  - e.g. TLSv1.2/TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384
- This creates a secure channel between client and server
- Use this link to communicate a set of 4 keys (for example AES keys)
- Use the keys in two pairs, one for each direction. One key in each pair used to encrypt, one to MAC with HMAC
- Use these keys to encrypt & decrypt all comms
  - E.g. AES-256-GCM with HMAC-SHA1

What hardware is needed by the server?

- A Raspberry PI, power supply and network cable
- An SD card and a means to write to it. Can get away with 4 GBytes (just) but 8 is better
- A keyboard, mouse & display to build software

- Once built, just plug it into your home network and power it up. No need for keyboard & display.

- BBC Click produced a step by step guide
  - Which is fine once you correct the errors.
    - Ask me if you want a corrected version

Building the software

The main steps are as follows:

- Part 1 – the basics

1. Install Raspbian on the SD card
    1. You don't need the GUI – all can be done from a command line.
2. Sort out network addressing
    1. Static IP address for the pi
    2. Port forwarding on home router
    3. Dynamic DNS service for home broadband address, for example www.changeip.com
3. Enable SSH so you can log into the pi from another PC

Building the software - 2

- Install OpenVPN
- Generate keys and a server certificate
- Generate keys & certificates for each user
- Go get a drink whilst Diffie-Hellman key exchange keys are generated
- Implement Denial of Service attack protection
- Configure the server
- Configure DDClient to ensure DNS address for home router is kept up to date
- Generate per user config files (.ovpn files)

Client

- For phone, install openvpn client (for example, for Android, install OpenVPN Connect from play store)
- For PC, install community OpenVPN package (https://openvpn.net/community-downloads/)
- For both, import the .ovpn config file
- Try it out.

Other bits

- For good measure:
  - Make the pi reboot periodically (e.g. weekly)
  - Make the OpenVPN logs rotate (for example daily)

- Gotchas
  - A lot of Wi-Fi hotspots block ports such as that allocated to OpenVPN (UDP port 1194)
    - So use the port number of a common service such as 995 (POP3)
  - Using a subnet at home that is used by a WiFi hotspot such as 192.168.0.* can cause routing problems.
    - So put up with it or change your home network addressing