**VPNs and Tor**

Placing a VPN on a local router to access Tor

**Pros**

* If machine is compromised by malware, it still couldn’t get the real IP address of the machine as any traffic sent out of the machine would still go through the network routers VPN first
* All traffic goes through the encrypted tunnel
* All devices on networked are routed through encrypted tunnel

**Cons**

* All devices on network are sent through the same tunnel/circuit (transparent proxy) so there is no streamline isolation
* Can leak if connection is dropped so needs to be configure in a way to deal with a drop
  + firewall

**Wi-fi Hotspots / Portable Routers**

* A portable router can be used as a Wi-Fi hotspot that is routed through Tor, that you can connect to
  + Machine 🡪 Hotspot (Tor) 🡪 Router (Internet)
* Connect to mobile hotspot using an ethernet for the securest connection
* Is good for connecting to unsecure networks like hotels
  + Protection from local hackers with local encryption

**Gateway VMs**

Whonix

* To use the whonix gateway socksport on any application, open the settings in the app and enter the proxy settings in the application i.e., the SOCKS host ip and the port (relay info)

PfSense