**Nested VPN Setup**

Direct VPN is set up on the Host OS (Router or Laptop)

Indirect VPN is set up on Guest OS (Laptop or VM)

Direct and indirect should always be joined in the same order

* Never allow VPN 2 to know your real IP

This stops either VPN1, VPN2 or DST from knowing both your real IP and the DST IP

Router is connected to indirect VPN 2 out to the internet

* ISP see’s that you are connected to a VPN but cannot read traffic
* VPN 2 (Indirect) provider can read traffic and see DST
* DST can see VPN 2s (Indirect) exit IP
* VPN 2 cannot see your real IP

Laptop is then powered on and connected via Direct VPN 1

* Never connect to VPN 2 (WIFI) without being connected to VPN 1 first, otherwise your real IP will be leaked to the indirect VPN
* Have a firewall on laptop that doesn’t allow connection to Wi-Fi without a VPN
* Also have a killswitch on the indirect VPN 1 so that a drop in connection doesn’t leak any information to VPN 2

Use pfsence or DD-WRT on the router, in a VM you can route the traffic through a pfsence internal network adapter for your direct VPN

This can work with a laptop and a VM aswell

* Direct VPN 1 is connected to on the Host OS
* The VM is then opened and connected to the Indirect VPN2
* Again, with firewalls and killswitches set up

Indirect must NEVER connect directly to real IP, only to VPN 1

Indirect must also be purchased anonymously

If there is any money trail or accidental connections, then anonymity is out the window and this is really only a **privacy service**

If encryption is necessary for the traffic so that neither VPN can see your traffic, an extra layer of TLS encryption is necessary