**Nesting and Chaining**

**VPN 🡪 Tor 🡪 Internet**

* VPN will be able to see your traffic and real IP
* ISP will be able to see your VPN IP
* Tor guard relay will also be able to see your VPN IP
* VPN will know Tor guard relay IP
* Dst will be able to see Tor exit relay IP and that you’re using Tor

**Tor 🡪 VPN 🡪 Internet**

* ISP will see Tor traffic
* Tor guard will see real IP address
* Tor exit relay will see VPN IP
* VPN will see Tor relays IP
* Dst will know your VPN IP
* Dst will not know you are using Tor

**SSH/VPN/JonDoNym as first hop**

Strengths

* Avoid Tor censorship, when a country of website doesn’t allow it
* If you trust your VPN/SSH more than ISP from protecting you from a Tor deanonymisation attack like a correlation or sybil attack
* Any exploit used on the Tor client to anonymise your real IP, should be protected against
  + Injecting code to force you to send out UDP into the normal internet, because Tor doesn’t support it
  + When this happens, the traffic will still be encrypted by your SSH or VPN and real IP won’t be exposed, just that of the server
* Access to hidden services with Tor being last hop
* Can do two hops i.e., SSH and VPN meaning if the VPN connection drops or if the VPN gets compromised then it never knew your real IP, only the SSH servers

Weaknesses

* If tunnel connection drops, then your real IP will be viewable
* Website traffic fingerprinting might be able to discover that you’re using Tor
* Non-SSL or non-encrypted traffic has no protection from the exit relay (if it’s a bad actor)
  + VPN or SSL as last hop does protect from traffic analysis
* A nested setup could make you more suspicious with high anonymity needs

**Can even wrap your SSH or VPN tunnel in TLS using Stunnel to hide that you’re using SSH/VPN and mimic normal HTTPS traffic**

**Tor as first hop**

Strengths

* Can get around Tor censorship
* Won’t show dst that you’re using Tor
* Tor will hide your real IP from the SSH/VPN and they will only see the Tor exit node IP
* Can pretend to be from a specific location
* Probably most anonymous option if no money trail from VPN service

Weakness

* E2e timing/correlation attacks
  + If the VPN or SSH gets compromised, as it’s a fixed point in a chain, then over a period of time, correlation and timing attacks can be done to deanonymise
* Dst can see your traffic
* VPN or SSH can also see your traffic
  + TLS should be used to mitigate both of those^
  + You are only as anonymous as you are to the VPN/SSH and dst
* ISP and country can see you are using Tor
* Tor only supports TCP
  + OpenVPN is slower
  + Tunnelling is more difficult to set up
* Might not be able to use Tor
* Tor browser might not be able to use this method
  + Need to harden own browser
* No stream isolation as the same Tor circuit will be used for everything when using a Tor client first