**Nesting Tor Setup**

**User 🡪 VPN 🡪 Tor 🡪 Internet**

Must use with a VPN that has leak protection on (external DNS resolution) and a kill switch in the host

Second connection with Tor using a VM guest

If the VPN drops, Tor cannot get out because of kill switch

* Could also use whonix for the VPN and Tor
* Look on whonix website for guidelines

**User 🡪 SSH 🡪 Tor 🡪 Internet**

Ssh -vvv -D 8080 [root@demo.stationx.net](mailto:root@demo.stationx.net)

* Set up a dynamic SOCKS proxy to forward the Tor traffic through

Sudo netstat -tupan │grep 8080

* This will show your current destination i.e., root@demo.stationx.net , IP and listening port

Then you open Tor

* Settings 🡪 configure 🡪 no for blocking 🡪 yes for proxy 🡪 put in IP and port (127.0.0.1 and 8080)
* Tor connection should be live

Another netstat should confirm the Tor traffic going through the ssh on 8080

Kill the signal and attempt to search with Tor

* If the Tor connection wont establish, then that’s confirmation that your browser is set up

**Multi-hop initial SSH**

Ssh -t -t -v -L 8080:localhost:9932 [root@demo.stationx.net](mailto:root@demo.stationx.net) ssh -t -D 9932 [root@demo2.stationx.net](mailto:root@demo2.stationx.net)

* Creating listening port on demo1 8080 to forward through to 9932 on demo2
* Creating SOCKS proxy on 9932 on demo2

Can also be done in whonix gateway by editing the torrc file

* Sudo nano /etc/tor/torrc
* Socks5Proxy 127.0.0.1:8080

If the proxy was set up from the whonix gateway then the cmd Is Socks5Proxy 127.0.0.1:1080

**Transproxy**

Tor will be normally configured to use a SOCKS proxy found in its settings

Normally with hops, VPN 🡪 Tor will make VPN the first hop and then move on to Tor

* What we actually want is to send our VPN through Tor (gateway/router)
* When using a transproxy, all traffic in all apps will be torified and you don’t need those SOCKS proxy settings in the browser

Read the Tor page on transproxy leaks to make sure it’s set up properly and that you can block leaks

* Corridor prevents leaking

In order to do this, the Torrc file will need to be configured

* Portal
* Whonix
* Hardware router
* Pfsence
* OpenWRT
* DD-WRT

User🡪Tor🡪SSH🡪Internet

Ssh -D 8080 [root@demo.stationx.net](mailto:root@demo.stationx.net)

* Creates an SSH tunnel to demo1 via 8080 thro0ugh Tor

Set up proxy settings in Tor (no proxy)

User🡪Tor🡪VPN🡪Internet

Assuming you’re going through a transproxy like Whonix gateway

In the VPN client, disable UDP

May also need to change gateway port from/to 443

**Whonix**

Many applications use Tor SOCKS port instead of the gateways transproxy – better for stream isolation

However, if we set up a VPN/SSH on the whonix workstation, all apps that are configured to use the SOCKS port will not tunnel through VPN/SSH but will just go through Tor

* This is because VPN/SSH will not affect local connections to gateway
* If we want the specially configured apps that go via SOCKS to use the VPN/SSH as final hop, then you need to reconfigure apps to not use the SOCKS proxy
  + This will remove stream isolation

In the Tor browser:

* No proxy (browser specifically won’t be going through the SOCKS proxy anymore)
* Ensure the app doesn’t go through the SOCKS and bypass what we want it to go through]
* This breaks Tor browser tab isolation as well, worsens browser fingerprints, consider using more than one browser or multiple workstations per identity/activity

Sudo apt-get install openssh-client

Sudo ssh -D 8080 [root@demo.stationx.net](mailto:root@demo.stationx.net)

Sudo apt-get install network-manager-kde

Sudo apt-get update &&apt-get install openvpn

Sudo openvpn –client –dev tun –auth-user-pass –remote demo.stationx.net 1194 –ca CA.pem –proto tcp

* Final command enables VPN connection to the demo server via port 1194

Loads of resources and info on the whonix page