

# Forum:[Hack Forums](#)

Thread: [\[Tor\] Using Stream Isolation \[Tor\]](#)

**Nakamoto** - October 12, 2014, 4:52 pm

Today I'm going to quickly cover stream isolation with Tor. I'll go over what it is and how to implement it for increased anonymity. I don't ever see anyone talk about this so I felt like I should at least go over it quickly for those who don't know what it is. Do note that these instructions only apply to GNU/Linux.

Stream isolation does exactly what it sounds like it does. It separates your traffic in order to inhibit the effectiveness of rogue exit nodes. Having only some of your traffic sniffed is far better than having all of your traffic sniffed.

By separating and isolating your traffic, you prevent rogue exit node operators from potentially making a connection in all of your traffic.

Something to keep in mind however is that doing this does not guarantee completely fresh circuits for every program. Sometimes you will only get new entry or middle relays, but the same exit relay as your other programs. This is still better however because your traffic will be originating from somewhere else in the network and making the connection will now become harder.

Implementing it is actually quite easy. All you need to do is add a line to your torrc configuration file for each program you plan on using through Tor. How do we do that? Easy.

Open up a terminal and enter in the following command

```
Code sudo nano /etc/tor/torrc
```

After entering your password, your torrc file will be opened as root. This is done so that you can actually save changes made to the file, otherwise you will receive "Permission Denied" errors.

Now scroll down until you see the following text.

```
Code ## Tor opens a socks proxy on port 9050 by default -- even if you don't
## configure one below. Set "SocksPort 0" if you plan to run Tor only
## as a relay, and not make any local application connections yourself.
#SocksPort 9050 # Default: Bind to localhost:9050 for local connections.
#SocksPort 192.168.0.1:9100 # Bind to this address:port too.
```

Below the last line in that block of text, add however many lines you need for each program that you want to run through Tor. Each line should look like this.

```
Code SocksPort 127.0.0.1:9051
SocksPort 127.0.0.1:9052
SocksPort 127.0.0.1:9053
etc.
```

For your own sake, you can choose to add a comment above each line detailing which port is for

which program.

Now just close out of Nano by hitting the following keys

Code CTRL + X - Exit the program

Y - Save your changes

Enter - confirm file to write to (don't type anything, just hit enter)

Alright, you're just about finished. Now that you've gotten your torrc file set up how you want it, all that's left to do is reload and restart the Tor daemon.

Code sudo service tor reload - Reloads the configuration file

sudo service tor restart - Restarts the daemon

Perhaps you only have to reload the service but I tend to restart it as well just for good measure.

Alright, thanks for reading. Pardon the lack of any detail in this one as I'm rather ill at the moment. If I'm feeling better I might fix this up a bit later on.

Thanks for reading and as always if you have any questions don't be afraid to ask. You can contact me through PM or Jabber. Please leave feedback as well if you have any.