Have fun with I2P, the 2018 edition

Masayuki Hatta Follow
Oct 14, 2018 · 4 min read

An easy, concise, and up-to-date introduction to the I2P anonymous network.

"man in formal suit standing while holding white balloon" by Andrew Worley on Unsplash

What's I2P?

I2P (Invisible Internet Project) is…well, you can read an introduction on the official site:

> *I2P is an anonymous network, exposing a simple layer that applications can use to anonymously and securely send messages to each other. The network itself is strictly message based (a la IP), but there is a library available to allow reliable streaming communication*

> *on top of it (a la TCP). All communication is end to end encrypted (in total there are four layers of encryption used when sending a message), and even the end points ("destinations") are cryptographic identifiers (essentially a pair of public keys).*

Difficult? There is an even lengthier Wikipedia entry.

Simply put, I2P is something like Tor. You may call it Tor's distant cousin. Like Tor, you can visit or operate (special) websites without being known your identity. You can use I2P for protecting your privacy, without fearing tracking or censorship. Remember, privacy IS freedom. I2P can help you keeping it.

In this article, I would like to show you how to use I2P *now*. There are lots of information on I2P out there, but unfortunately some of (well, maybe most of) them are severely outdated. I intend to fill this gap.

Installing I2P

Installing I2P is quite easy now. The Download page of the official I2P website lists pre-built installer packages for Windows, MacOS, GNU/Linux, and Android. The Android version of I2P can be obtained from Google Play or F-Droid, too. There is also a Docker image. In addition, many GNU/Linux distros have I2P packages nowadays. Debian/Ubuntu packages are maintained by yours truly.

After installation, you can run I2P. On Windows, you can find "Start I2P" somewhere in Start Menu. On Debian/Ubuntu, you can run I2P on the command line:

```
$ i2prouter start
```

(Note that you should run it by a non-root account)

Then, visit http://localhost:7657 with your web browser. You will be greeted by the I2P router console.

Configure bandwidth for speeding up

To use I2P comfortably, you have to share some of your internet bandwidth. The default is 48 KBps, which is too conservative and too slow.

From the I2P router console, you can change bandwidth configuration. Find “Configure Bandwidth” in the “Applications And Configuration” section.

The optimal bandwidth depends on your situation. You can check your internet provider’s specification or speedtest. Maybe 10–20% of the whole bandwidth should be good?

Using the remote I2P via SSH port fowarding

I2P is a decentralized, peer-to-peer network. So your I2P local instance (“router”) needs some time to be “integrated” into the global I2P network. The longer you run I2P, the better I2P’s performance becomes. If possible, you should run I2P 24 hours a day, 7 days a week.

However, if you are using mobile computers, it might be difficult. If you have a VPS or such, you may run I2P remotely, then use SSH port-forwarding. After setting up SSH access to the remote server, run the following on your local machine:

```
$ ssh -fTNL 4444:127.0.0.1:4444 -L 7657:127.0.0.1:7657 -L
7658:127.0.0.1:7658 -L 6668:127.0.0.1:6668 yourlogin@remoteipaddress
```

Replace “yourlogin” with your login name on the remote server and “remoteipaddress” with IP address of the remote server.

In this way, you can still visit http://localhost:7657, but actually connect with the remote server’s port 7657. If you want to know about the other ports, see Ports Used by I2P.

Using Firefox and FoxyProxy with I2P

There are many “eepsites” inside the I2P network. They are essentially websites, but have pseudo Top-Level Domain “.i2p” and only accessible via I2P.

To browse eepsites, you have to configure proxy setting of your web browser. Find browser's proxy setting page, then set "HTTP Proxy" and "SSL Proxy" to "127.0.0.1" port "4444".

However, if you set proxy globally for all web accesses, you will access non-I2P, usual internet (often called "clearnet") websites through "outproxy" sites on the I2P network. Outproxies are extremely slow, thus not recommended. So, what you may want to do is:

- Use I2P proxy setting for accessing *.i2p
- Use default (non-)proxy setting for accessing clearnet sites (*.com, *.org, etc.)

This can be achieved by using Mozilla Firefox and its addon called FoxyProxy. FoxyProxy can change proxy settings on the fly, according to the pre-set rules. You can import this config file to FoxyProxy 6.x (current version) for use with I2P.

I2P Browser Bundle?

When you use the regular web browser, by default it leaks lots of personal information which can be used for tracking and identifying you. If you want to know how much information you leak, try EFF's Panopticlick.

Because of this, The Tor Project released excellent Tor Browser Bundle. TBB is actually a carefully configured version of Mozilla Firefox & Co. to protect your anonymity without any hassles.

There has been several attempts to build "I2P Browser Bundle", but for now, it would be easier to piggyback on Tor Browser Bundle. Simply install TBB, then install and set up FoxyProxy (and I2P, of course) as explained above.

Conclusion

Now you must be able to access eepsites via I2P. Let me introduce to you 3 eepsites as starting points.

- Legwork.i2p (a search engine for the I2P network, run by me)
- I2PWiki (Lots of how-to information on I2P's other services)

- I2P Support Forum (there is also the clearnet version)

Welcome.

Privacy I2p Tor Internet Freedom