Qubes + Whonix I2P Guide - Simple Version - TorHunter

4-5 minutes : 12/14/2023

Prerequesites

- Qubes OS R4.1 or later with Whonix Gateway (GW) and Workstation (WS) installed (16 or later).

Step 1: A Qube is Born

The older I2P guide we made previously is somewhat confusing and very technically challenging especially for beginners. While we don't want to encourage beginners to rely on the inherent security of Qubes, we want them to learn and become more knowledgeable about how Qubes can and can't protect you. Please take some time and read the whonix.org/wiki/Documentation to learn more about online anonymity and privacy. To quickly get I2P up and running on Qubes, you can follow this simple guide.

First we need to create a new StandaloneVM that will keep all of our I2P information.

To create a new StandaloneVM:

- Open your Qube Manager and select "New Qube".
- Name your qube and set the colour.
- Set the type to StandaloneVM.
- Set the template to "whonix-ws-XX" where XX is your whonix version (16 or 17)
- Set the networking to "sys-whonix"
- Click OK

Launch the new Qube by going to the blue Qubes Start Menu and selecting Your Qube > Xfce Terminal. Update your qube:

```
sudo apt update && sudo apt upgrade -y && sudo apt autoremove -y
```

Step 2: I2PD, a better solution

In our personal experience, I2PD just works better than the Java implementation. However, the debian repositories available in Whonix Workstation ship broken I2PD packages and you will run into a segmentation fault. Let's install it by following the official I2PD readthedocs! With your new StandaloneVM qube open, run the following commands:

```
sudo apt install apt-transport-https
```

```
wget -q -O - https://repo.i2pd.xyz/.help/add_repo | sudo bash -s -
```

```
sudo apt update
sudo apt install i2pd
```

Now we have a working version of I2PD on our system!

Step 3: Configuration

There's so much you can change with I2PD's simple configuration files, they are even commented so you don't need

any documentation. Simply read the config file to learn more about it's possibilities! We need to disable a few things just to be safe:

```
sudo nano /etc/i2pd/tunnels.conf
```

This will open the tunnels configuration for I2PD, you will see the uncommented tunnel information for an IRC client. You can simply remove everything from this file or just comment the enabled tunnels and save.
You might also want to change some settings in:

```
sudo nano /etc/i2pd/i2pd.conf
```

Read through this file to better understand it's capabilities. After editing, you can enable I2PD on startup and start the service for use right now!

```
sudo systemctl enable i2pd
sudo systemctl restart i2pd
```

Step 4: Tor Browser

Since you are running I2P on the Whonix Workstation, you have to modify some Tor Browser settings in order to connect to the I2P http proxy. Go to the blue Qubes Start Menu and select Your Qube > Tor Browser (AnonDist). Once open, you should first edit your security settings by clicking the Shield icon in the top right corner. Set this setting to "Safest" for maximum security (this disables JavaScript which is still capable of deanonymization on I2P).

- Navigate to **about:config** in the address bar and proceed past the warning.
- Set the following settings:

```
extensions.torbutton.use_nontor_proxy => true
network.proxy.http = 127.0.0.1
network.proxy.http_port = 4444
network.proxy.no_proxies_on = 127.0.0.1
dom.security.https_first_pbm = false
dom.security.https_only_mode = false
dom.security.https_only_mode_pbm = false
```

Conclusion

You can now navigate to your I2P console at **127.0.0.1:7070**in the Tor Browser. Here you can see your Routers, Floodfills, and Tunnels. You may have to wait 10-20 minutes to gather enough tunnels to connect to eepSites.

Thanks for reading! If you have any additions, corrections, or questions, please leave them in the comments and we will answer them as soon as possible. Have a super day and stay vigilant!

Post navigation