**Whonix**

**Uses TOR network and is based on Debian GNU Linux**

Implements security through isolation

* Specifically uses principle of isolation for privacy and anonymity

**What does Whonix do**

* Hide ISP assigned IP
* Prevent ISP spying
* Prevent websites and Malware ID’ing you
* Circumvent censorship

**It’s broken into 2 VMs**

* One is the **gateway**
  + Solely runs TOR and acts as a gateway to the internet for the Workstation
* The other is the **Workstation**
  + On a completely isolated network, only connections through TOR are possible
  + DNS leaks are impossible and even users with root privileges cannot find the hosts ISP assigned IP address

“sudo route” shows the route of the internet traffic

* Workstation traffic should be running through gateways ipaddr

Whonixcheck

* Updates, news, version, patches and packages

Timesync

* Needs to be synced to correct time but does it in a special way as syncing with host can create an attack vector

Torrc

* Tor configurator

Different workstation per alias to prevent correlation attacks

Whonix is best used when physically isolated

Whonix.org shows apps that you may want to install

* All downloads are done through the TOR gateway with no chance of leaks

With any OS where tor isn’t happening on a gateway, newly installed apps could leak

* Therefore it isn’t recommended to download apps on Tails because the Torification happens internally

Keep a master copy of Whonix workstation

* Don’t use it directly for any activity
* Only for snapshots of a clean state, freshly updated version
* Don’t make any edits or changes

**Weaknesses**

* Its obvious to an observer that youre using TOR when using whonix
* Doesn’t encryot documents by default
* Doesn’t clear metadata out of documents
* Doesn’t encrypt subject or other headers of emails
* Doesn’t separate contextual identities
  + Not advisable to use the same whonix workstation for multiple aliases
* No protection from bias attacks or firmware root kits or hardware compromises like keylogger or rangemaster, VGA cable retroreflector etc.

Not an amnesiac system

* Unlike tails, its not an amnesiac live cd
* Will leave local traces on the hard drive that you installed Whonix
* Any files will still exist after powering off unless securely wiped
* No special measures to limit what’s written to the disk
  + Back up files, messaging files, temporary files, usr created files, browser history

Could use snapshots and revert to a clean VM when finished session

Fully encrypt host operating system to mitigate local forensic examination

* If this is your main concern though, Whonix is not the correct option
* Recommended for protection against protocol level leaks and ISP snooping