Can I use TOR with the Private Internet Access service?

Travis - 2022-08-15 - Browsing / Internet

Yes! To use PIA with TOR, please make sure that you run the TOR Browser after you have connected to the PIA service.

Although in many ways both are very different, VPN's and the Tor anonymity network use encrypted proxy connections to hide users' identities. There are a few similarities and differences for example:

- VPN speeds are generally faster than the TOR Browser as messages pass through only one VPN server instead of 3 TOR nodes.
- With your PIA service, you will get more privacy rather than anonymity.
- Tor is much slower, is often blocked by websites, and is not suitable for P2P, but it does not require that you trust anybody, and is therefore much more genuinely anonymous.

The cool thing is that VPN and Tor can be used together to provide an extra layer of security and to mitigate some of the drawbacks of using either technology exclusively. The main downside of using both together is the combined speeds of both technologies can take a hit, making connecting in this way secure... however, it's quite slow.

Tor through your PIA Service
First, you will want to connect to your choice of server offered on your PIA application, then you can then access the Tor network before connecting to the internet. To do so, follow the steps below:

Your computer -> VPN -> TOR -> Internet

Due to the use of 3rd party unsupported hardware and/or operating systems, we cannot provide support for TOR to VPN setups. If you do decide to go this route, then the easiest way to set this up is by using either PORTAL, Whonix or TAILS for maximum security) while connected to a PIA server; this would mean that your public IP is that of the TOR exit node and not the IP provided to you by the VPN.

Below we have provided you with a list of pros and cons on using a VPN with a TOR Browser.

Pros:

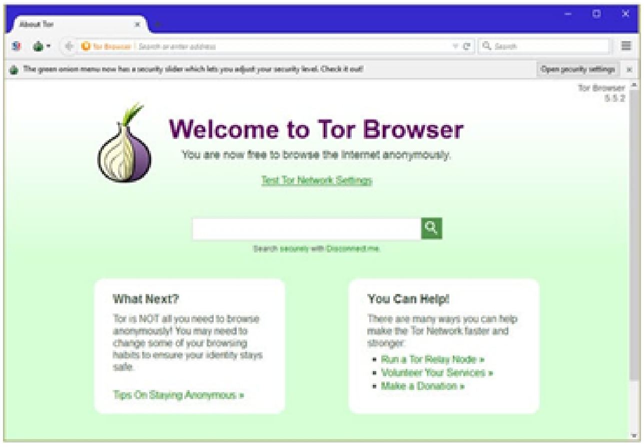
- Your ISP will not know that you are using Tor (although it can see that you are using a VPN)
- The Tor entry node will not see your real IP address, but the IP address of the PIA server. PIA being a no log VPN provider, means that your identity is safe and secure.
- Allows access to TOR hidden services (.onion websites).

Cons:

- No protection from malicious TOR exit nodes. Non-HTTPS traffic entering and leaving TOR exit nodes is unencrypted and could be monitored
- TOR exit nodes are often blocked
- You should note that using a TOR bridge such as Obfsproxy can also be effective at hiding TOR use from your ISP (although a determined ISP could, in theory, use deep packet inspection to detect TOR traffic).

  Important Note: Private Internet Access currently does not offer TOR through VPN via an OpenVPN configuration file.

However, do be aware that this is nowhere near as secure as using the TOR Browser, where TOR encryption is performed end-to-end from your desktop to the TOR servers. The TOR Browser has also been hardened against various threats in a way that your usual Browser almost certainly has not been.



The green onion menu now has a security slider which lets you adjust your security level. Check it out!

Welcome to Tor Browser

You are now free to browse the Internet anonymously.

Test Tor Network Settings

Search securely with Disconnect.me.

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

Tips On Staying Anonymous »

You Can Help!

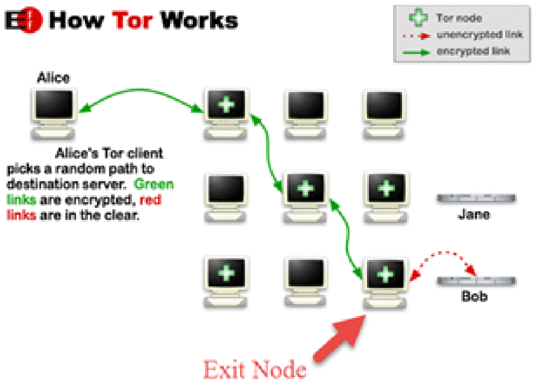
There are many ways you can help make the Tor Network faster and stronger:

- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

For maximum security when using TOR through a VPN you should always use the Tor browser.

Security Risk: Malicious exit nodes

When using TOR, the last node in the chain between your computer and the open internet is called an exit node. Traffic to or from the open internet (Bob in the diagram below) exits and enters this node unencrypted. Unless some additional form of encryption is used (such as HTTPS), this means that anyone running the exit node can spy on users' internet traffic.


How Tor Works
Tor node
unencrypted link
encrypted link
Alice
Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Bob
Exit Node

This is not usually a huge problem, as a user's identity is hidden by the 2 or more additional nodes that traffic passes through on its way to and from the exit node. However, if the unencrypted traffic contains personally identifiable information, this can be seen by the entity running the exit node.

Such nodes are referred to as malicious exit nodes and have also been known to redirect users to fake websites.

SSL connections are encrypted, so if you connect to an SSL secured website (HTTPS://), your data will be secure, even if it passes through a malicious exit node.

Security Risk: End-to-end timing attacks
This is a technique used to de-anonymize VPN and Tor users by correlating the time they were connected, to the timing of otherwise anonymous behavior on the internet.

An incident where a Harvard student (who made bomb threats to skip finals) got caught while using TOR is an excellent example of this form of de-anonymization attack in action. However, it is worth noting that the culprit was only caught because he connected to Tor through the Harvard campus WiFi network.

On a global scale, pulling off a successful e2e attack against a TOR user would be a monumental undertaking, but possibly not impossible for the likes of the NSA, who are suspected of running a high percentage of all the world public TOR exit nodes.

Tags
TOR