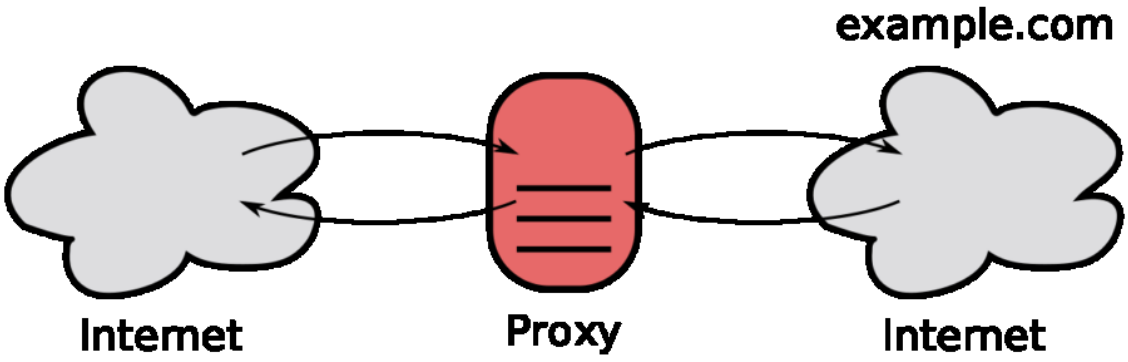
Which Is Better: TOR over VPN Or VPN over TOR?



Introduction

There has always been a lack of clarity in relation to the privacy and anonymity offered by VPNs and Tor.

People have different opinions on the ways to mix them together. Do a VPN and Tor work together? Should I use both a VPN and Tor? Or do they both contradict each other? What benefits are provided by mixing a VPN with Tor?

This article seeks to address these questions and the persistent discourses circulating on the web.

Tor Provides Strong Anonymity

Tor has always been considered providing stronger anonymity. Why? Because your data first arrives at the network through a random node around the world. It then makes a minimum of two hops, ultimately passing through a random exit node to its last destination.

In ideal circumstances, the information ought to be encrypted which hinders the exit node from reading it.

When Tor is contrasted with a VPN, Tor's strength shines since no sole node in this path receives the whole picture of your activities. An entry node can merely see your location. Significantly, the entry node is unable to see who you are communicating with. Nonetheless, the exit node can see who you are communicating with and not your location.

The relay established in the middle forbids the exit node from discovering what the entry node was. This is important to know since an adversary may end up operating both nodes (the entry and exit) that you use.

Tor may be considered slow. People who volunteer to run nodes are not obliged to make the entire process fast and efficient since the Tor network is unable to pay them for running these nodes.

The risks associated with making a payment to the volunteers is never a good idea due to privacy concerns. The same applies to users who would like to enhance the Tor connection speeds by paying the Tor network since it could reveal the entry/exit nodes they use.

The Privacy Benefit Of A VPN

VPNs differ from Tor in that it makes a peculiar compromise. VPNs achieve blazing speeds and usually only route traffic through one hop, commonly in a heavy-duty data center.

To retain stability and the blazing speeds offered by the VPN, the customers have to pay for the services.

The main concern that users of VPNs and Tor share are that users cannot see what is happening inside the servers they are connecting to. For instance, the user can't see if the VPN server is retaining logs or injecting malware.

The problem with someone using a VPN is that there is a high risk that the user can be identified from their VPN login details and the way they pay for the services.

A VPN provider that cooperates with law enforcement agencies can obtain details that are more detrimental to a user's privacy than one arising from using a Tor node.

Therefore, it is important to read reviews written by users of a VPN user to determine whether a VPN provider is malicious. Pay particular attention to VPN users who have been booted off for violating a VPN provider's terms of service or copyright laws.

Debate: Should You Combine A VPN With Tor Or Not?

The main assumption is that more hops indicate greater privacy. This is not always true. When a VPN provider implements a single node that is permanent, they are increasing the possibility of entirely compromising the anonymity that Tor famously grants.

Keep in mind that a VPN can be seen as making the circumstances worse for users as the VPN inevitably introduces a permanent entry guard or a permanent exit node which is dependant on the order the user connects using VPN and Tor together.

1. Using TOR over VPN

User (You) > VPN > Tor > Internet

If you decide to go with this setup, you would firstly connect to the VPN server, then launch the Tor Browser. The VPN encrypted traffic would transmit to the TOR network through a couple TOR hops prior to reaching its final destination which is the Internet.

Advantages (PROS) of Tor Over VPN

- Anyone can set up Tor Over VPN easily since you just connect and connect. No need for technical skills.
- The VPN provider will not be able to see your traffic content and origin. The VPN provider can merely see that you are connecting to Tor nodes.
- Your Internet Service Provider cannot see that you are using Tor. Instead, they see that you are using a VPN which is more favored than seeing a Tor connection. Thus, they

would be less suspicious of you for using a VPN than Tor. Your Tor usage is concealed by the VPN.

- The Tor entry node will see the exit IP Address of the VPN server you are currently connected to. Therefore, the Tor entry node does not see your real IP address.
- Fast performance.
- You can still access the hidden services of Tor and the hidden websites that have the .onion suffix.
- Tor over VPN with end-to-end encryption is exceptionally strong as illustrated from leaked classified government documents. This setup poses a massive problem for even the most powerful adversaries such as the NSA.

Disadvantages (CONS) of Tor Over VPN

- The VPN server can see your real IP address which means the VPN provider (Employee) can also see it.
- If you are sending or receiving unencrypted traffic, you are vulnerable to malicious Tor exit nodes.
- You don't put your trust on the VPN provider. The VPN server can only see traffic that is encrypted by Tor and to the last destination and from numerous Tor guards. So the question is: Who do you trust more? Your Internet Service Provider or VPN Provider?
- There is a possibility that your Tor traffic becomes exposed to your Internet Service Provider if your VPN connection suddenly drops. This can be countered by choosing a VPN provider that offers a kill switch and its own DNS servers.
- If you don't utilize end-to-end-encryption then you are placing a tremendous amount of trust on the Tor exit node operators. It is bothersome to know that an exit node can actually be malicious and turn on you.

2. Using VPN Over TOR

User (You) > Tor > VPN > Internet

With this setup, your traffic becomes encrypted by the VPN as you leave TOR nodes. Ultimately, you connect to the websites you are visiting.

Advantages (PROS) of VPN Over Tor

- More privacy from the VPN provider since the VPN server cannot see your real IP address which means the VPN provider (Employee) can't see it. If you paid anonymously via a method like Bitcoins then establishing this setup makes more sense especially if you don't trust the VPN Provider.

- Your Internet Service Provider cannot see whether you are connected to a VPN. Instead, they can only see using Tor.
- You may access Tor from every application transparently. This provides the benefit of not needing to setup and configure any applications manually.
- A viable option for users who don't place their trust on the VPN provider.
- Allows you to choose the VPN server location which is useful for spoofing your geo-location.
- You can choose to connect to websites that restrict Tor exit node IP addresses. For example, if a Fortune 50 company uses Cloudflare's Enterprise plan, their site's use of the Cloudflare Enterprise blacklisting feature pertaining Tor exit node IP addresses can be bypassed more easily.

Disadvantages (CONS) of VPN Over Tor

- Slow, poor performance.
- If you did not pay anonymously via a method like Bitcoins, then there is little reason to establish this setup.
- Can only access hidden websites with .onion suffix from browsers that are properly configured to connect directly to Tor.
- There are very few VPN providers who allow this setup.
- Your VPN provider can still find out who you are via close scrutiny of financial records despite being only being to identify your IP address as that of the Tor exit node. This can be countered by paying anonymously. For example, Bitcoins are effective for this purpose.
- The Tor network does not approve of this setup since they believe that the VPN server is capable of establishing a profile of all of your activities and that over time that can be extremely detrimental to the user.
- Very susceptible to end-to-end timing attacks which are employed to deanonymize VPN and Tor users by associating the times they were connected to such anonymity services.

Should I use both a VPN and Tor?

If the typical internet user has nothing to hide then using only a VPN will suffice. But since all of your information and traffic online can reveal everything about you as a person then combining both suddenly becomes extremely plausible. It's definitely worthwhile to think about.

When you combine the usage of a VPN and Tor, it becomes increasingly difficult for everyone including the most powerful adversaries like the NSA

to find you. For the adversaries with the most resources and capabilities, they probably will find you if they really want to. But, using both Tor and VPN can make their jobs a lot more difficult and complicated than it needs to be.

I personally recommend using VPN through Tor since there is no reason to believe that any VPN provider won't turn on you one day in order to protect themselves. That possibility alone isn't worth risking in my honest opinion.

The choice is ultimately yours to decide.

Source: https://www.sunnyhoi.com/which-is-better-tor-over-vpn-or-vpn-over-tor/