Raw data

|  |  |
| --- | --- |
| Tor is free software and an opennetwork that helps you defend against traffic analysis,a form of network surveillance thatthreatens personal freedom and privacy, confidential businessactivities and relationships, and state security.  data packets on the Tor network take a random pathway through several relays that cover your tracks so no observer at any single point can tell where the data came from or where it's going.  No individual relay ever knows the complete path that a data packet has taken. The client negotiates a separate set of encryption keys for each hop along the circuit to ensure that each hop can't trace these connections as they pass through.  Tor can't solve all anonymity problems. It focuses only on protecting the transport of data. You need to use protocol-specific support software if you don't want the sites you visit to see your identifying information.  Tor does not provide protection against end-to-end timing attacks  Source: https://www.torproject.org/about/overview.html.en#overview | A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption.  Applications running across a VPN may therefore benefit from the functionality, security, and management of the private network.  To ensure security, data would travel through secure tunnels and VPN users would use authentication methods – including passwords, tokens and other unique identification methods – to gain access to the VPN. In addition, Internet users may secure their transactions with a VPN, to circumvent geo-restrictions and censorship, or to connect to proxy servers to protect personal identity and location to stay anonymous on the Internet.  some Internet sites block access to known VPN technology to prevent the circumvention of their geo-restrictions  Traditional VPNs are characterized by a point-to-point topology, and they do not tend to support or connect [broadcast domains](https://en.wikipedia.org/wiki/Broadcast_domain" \o "Broadcast domain)  A VPN connection depends on the VPN provider and the ISP. If either fails, the connection fails.  Source:  https://en.wikipedia.org/wiki/Virtual\_private\_network#Networking\_limitations |

1st version

|  |  |
| --- | --- |
| Tor is free software and an open network that helps its user defend against traffic analysis and protect their privacy. Data packets on the Tor network take a random pathway through several relays that cover user’s tracks so no observer at any single point can tell where the data came from or where it is going. No individual relay ever knows the complete path that a data packet has taken. Additionally, the client negotiates a separate set of encryption keys for each hop along the circuit to ensure that each hop can not trace these connections as they pass through. Tor can not solve all anonymity problems. It focuses only on protecting the transport of data. For instance, Tor users need to use protocol-specific support software if they do not want the sites they visit to see their identifying information. Another limitation of Tor is that it does not provide protection against end-to-end timing attacks. | A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption. Applications running across a VPN may therefore benefit from the functionality, security, and management of the private network. To ensure security, VPN data travels through secure tunnels and users would use authentication methods to gain access to the VPN. Internet users may also secure their transactions with a VPN, to circumvent geo-restrictions and censorship, or to connect to proxy servers to protect personal identity and location to stay anonymous on the Internet. Some Internet sites block access to known VPN technology to prevent the circumvention of their geo-restrictions. A VPN connection depends on the VPN provider and the ISP; if either fails, the connection fails. Traditional VPNs are characterized by a point-to-point topology, and they do not tend to support or connect broadcast domains. |

2nd version

Tor and VPN are two remote access methods that aim to defend against traffic analysis, protect user privacy and circumvent geo-restrictions and censorship. They help users to stay anonymous on the Internet to protect their privacy. Although Tor and VPN are similar in essence, both provide their security services using different approaches. In Tor, data packets travel through several relays such that no single observer can determine where the data came from or where it is going to. Additionally, Tor clients negotiate separate encryption keys for each hop on the path to prevent hops from tracing connections as packets pass through. Whereas VPN is a point-to-point connection that can be established by virtual tunnelling protocols, dedicated connections or traffic encryption. Internet users may secure their activities with a VPN to bypass geo-restrictions or censorship. Both Tor and VPN can not solve all anonymity issues over the Internet. Tor only protects the transport of data and requires users to use protocol-specific support software to protect their personal identity. This leaves Tor open to many attacks such as end –to-end timing attacks. Similarly, VPN has limitations that puts the user under the mercy of VPN provider and the ISP. For instance, many websites block access to common VPN technology. Another drawback of VPN is that it can not be used in broadcast domains which limits its use in any non point-to-point environment.