Are VPNs Anonymous?

Summary

A VPN (Virtual Private Network) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

For security, the private network connection may be established using an encrypted layered tunneling protocol, and users may be required to pass various authentication methods to gain access to the VPN [1]. Nowadays, OpenVPN is the best protocol available. There are other protocols, like PPTP, L2TP/IPSec, but we are not going to take them into account due to their security concerns.

Most VPN providers officially claim that they do not keep traffic logs, however it's always important to check the company's privacy policy and location of their headquarters (in terms of jurisdiction).

Where can we install VPNs?

VPNs are supported in many OS. Some of them are Windows, Mac OS X, iOS, Android, and Linux (Ubuntu) and Chrome book. They also work on mobile devices, like Android, IPhone and IPad.

Some routers also support VPNs. Find some of the firmwares that support VPNs below.

Firmware package	Cost	Developer
DD-WRT	Free	NewMedia-NET GmbH
Gargoyle	Free	Eric Bishop
OpenWrt	Free	Community driven development
OPNsense	Free	Deciso BV
Tomato	Free	Keith Moyer

Are they anonymous?

While most VPN providers claim they do not keep logs, it is true that most companies keep basic connection logs(User IP address and VPN timestamp). It is very important to check the companies privacy policy and the location of their headquarters (in terms of jurisdiction).

It is also important to take into account the encryption standard used. Many VPN clients allow you to choose different standards. While the securer standards may slow down the internet connection, they will make sure your data is safer.

Typically, your ISP (Internet Service Provider) would have to pay special attention to your activity in order to determine whether you are using a VPN or not. However, if well protected, they won't be able to learn the nature of your activity. They are only able to see you are connected to a certain endpoint and the bandwidth you are using. If they want to learn more about you, they

may request logs to your VPN provider (they probably need a court order to do that). See more information on this topics below.

Different levels of logging

Companies may have different logging levels. These are the three main categories:

1. **Usage (browsing) logs** – These logs basically include online activity: browsing history, connection times, IP addresses, metadata, etc. From a privacy standpoint, you should avoid any VPN that collects usage data. Most of the VPN services that are collecting usage logs are free VPN apps, which are basically spyware. The data they collect is then sold to third parties, thereby monitoring the "free VPN" service.
2. **Connection logs** – Connection logs typically include dates, times, connection data, and sometimes IP addresses. Typically this data is used for optimizing the VPN network and potentially dealing with user problems or terms of use issues (torrenting, illegal activities, etc.).
3. **No logs** – No logs simply means the VPN service is not keeping any logs whatsoever. Having a truly no logs policy can be difficult to implement while at the same time enforcing restrictions, such as device connections or bandwidth. This is especially the case when VPNs need to enforce restrictions such as bandwidth or the number of devices being used per subscription.

While basic connection logs are not necessarily a problem, there is an increasing number of VPNs that keep connection logs, while falsely claiming to be a "no logs" service. Examples of this are Betternet, PureVPN, Windscribe, and TunnelBear. That is why it is very important to be aware of our VPN provider's privacy policy and the jurisdiction of their headquarters [7].

Data encryption

Essentially, data encryption provides users with a secure VPN tunnel whereby data is protected. However, there are different levels of encryption as well. By default OpenVPN includes AES-128 [8], SHA1 [9], and RSA-2048 [10], while maximum encryption includes AES-256 [8], SHA256 [11], and RSA-4096 [10]. An encryption key tells your computer how to decrypt or encrypt data.

Data authentication is part of the encryption process and refers to the message authentication algorithm with which user data is authenticated. This is used to protect users from active security attacks.

Appendix

Communication protocol

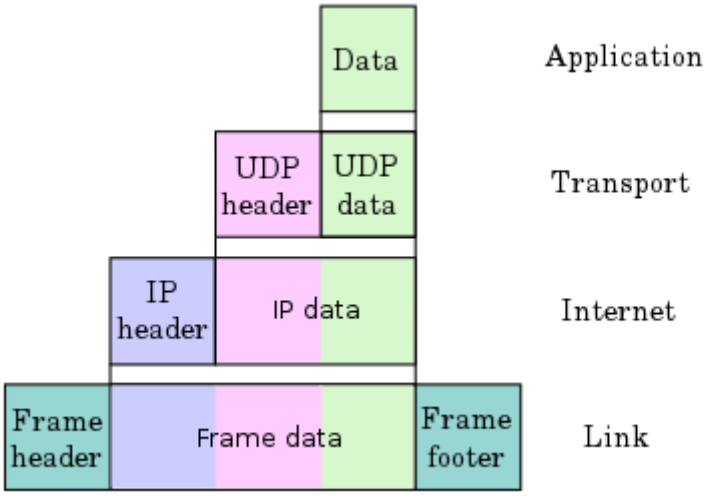
A communication protocol is a system of rules that allow two or more entities of a communications system to transmit information via any kind of variation of a physical quantity. The protocol defines the rules, syntax, semantics and synchronization of communication and possible error recovery methods. Protocols may be implemented by hardware, software, or a combination of both [3].

Tunneling protocol

A tunneling protocol is a communication protocol that allows for the movement of data from one network to another. Because tunneling involves repackaging the traffic data into a different form, perhaps with encryption as standard, it can hide the nature of the traffic that is run through a tunnel [2].

Encapsulation

In computer networking, encapsulation is a method of designing modular communication protocols in which logically separate functions in the network are abstracted from their underlying structures by inclusion or information hiding within higher level objects [4].



Encryption

In cryptography, encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Only authorized parties can decipher a ciphertext back to plaintext and access the original information [5].

OpenVPN

OpenVPN is open-source software (there is a commercial version and a free edition) that implements virtual private network (VPN) techniques to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange. It is capable of traversing network address translators (NATs) and firewalls.

OpenVPN allows peers to authenticate each other using pre-shared secret keys, certificates or username/password (this part requires third party modules). When used in a multi client-server configuration, it allows the server to release an authentication certificate for every client, using signatures and certificate authority. It uses the OpenSSL encryption library extensively, as well as the TLS protocol, and contains many security and control features.

OpenVPN uses the OpenSSL library to provide encryption of both the data and control channels. It lets OpenSSL do all the encryption and authentication work, allowing OpenVPN to use all the ciphers available in the OpenSSL package. It can also use HMAC packet authentication feature to add an additional layer of security. Mbed TLS is available starting from version 2.3 [6].

Security Attacks

Security attacks [12] can be divided in two groups: active and passive attacks:

- **Active attacks** - An Active attack attempts to alter system resources or effect their operations. Active attack involve some modification of the data stream or creation of false statement
- **Passive attacks** - A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of

eavesdropping on or monitoring of transmission. The goal of the opponent is to obtain information is being transmitted.

Encryption Key

Encryption keys are used to encrypt data. The most common forms of encryption are symmetric-key encryption and public-key encryption [13].

- **Symmetric-key encryption** - All users share the same key, enabling everyone with the key to encrypt and decrypt data.
- **Public-key encryption** - Each user has a public-private key pair. One user has a private key to encrypt data while another user has the corresponding public key to decrypt that data.

References

1. https://en.wikipedia.org/wiki/Virtual_private_network "Wikipedia - Virtual Private Network" 10/08/2020
2. https://en.wikipedia.org/wiki/Tunneling_protocol "Wikipedia - Tunneling protocol" 10/08/2020
3. https://en.wikipedia.org/wiki/Encapsulation_(networking) "Wikipedia - Encapsulation" 10/08/2020
4. https://en.wikipedia.org/wiki/Communications_protocol "Wikipedia - Communications Protocol" 10/08/2020
5. https://en.wikipedia.org/wiki/Encryption "Wikipedia - Encryption" 10/08/2020
6. https://en.wikipedia.org/wiki/OpenVPN "Wikipedia - OpenVPN" 11/08/2020
7. https://www.bestvpnz.com/vpn-101-everything-you-need-to-know-about-virtual-private-networks/ "About VPNs" 11/08/2020
8. https://pixelprivacy.com/vpn/no-log-vpn/ "Logless VPNs" 11/08/2020
9. https://en.wikipedia.org/wiki/Advanced_Encryption_Standard "AES Encryption Standard" 13/08/2020
10. https://en.wikipedia.org/wiki/SHA-1 "SHA-1 Encryption Standard" 13/08/2020
11. https://en.wikipedia.org/wiki/SHA-2 "SHA-2 Encryption Standard" 13/08/2020
12. https://en.wikipedia.org/wiki/RSA_(cryptosystem) "RSA Encryption Standard" 13/08/2020
13. https://www.geeksforgeeks.org/active-and-passive-attacks-in-information-security/ "Active and Passive Security Attacks" 13/08/2020
14. https://support.microsoft.com/en-us/help/246071/description-of-symmetric-and-asymmetric-encryption "Encryption Keys" 13/08/2020