

Forum:[Hack Forums](#)

Thread: [Ways to be Anonymous Online | Advanced Details & Protocols](#)

Deities - August 28, 2019, 6:27 pm

So you want to wear a mask online..

How to stay anonymous while using the internet!

The discussion of being anonymous online should not start with the idea of a proxy, Tor, or a VPN, but rather with the definition of what it means to be anonymous online. You can be anonymous while connecting to someones server, but it's a totally different ball park when anonymously raising your websites search engine status. All these tasks are solved in different ways and I want to share the basic workings of what it means to be anonymous online as a user.

Understand that there is a Social anonymity that deals with protecting and not exposing personal data about himself/herself on the web. Then there is technical anonymity where it deals with hiding the data associated with the used hardware, location, time, and user of the application.

This guide will mostly be dealing with the technical aspect of it all!

What Is A Proxy?

Globally, when we talk about proxy server, it means something that acts as an intermediary between the client and the server being accessed. In terms of ensuring anonymity, proxy servers can be: HTTP (web) proxy servers.

SOCKS proxy servers.

Unlike HTTP proxy servers, SOCKS transmits all information without adding anything from itself. The SOCKS protocol is at the session-level of the OSI model; which allows SOCKS to pass all traffic through itself, not just HTTP.

Separately, it is worth mentioning CGI-proxy. Also known as "anonymizers," which are essentially a web-server with a form where the client enters the address of the desired site. After that, the requested page opens, but the address of the CGI proxy is visible in the browser's address bar. A CGI proxy, like any web server, can use https to protect the communication channel between itself and the client.

Advantages of Proxy:

- They are cheap or even free.
- You can easily find tons of them.

Disadvantages of Proxy:

- You have to trust them.
- Need to filter HTTP headers for HTTP proxy.
- Encryption supported not on all layers.
- Proxy chains are ineffective.
- It requires you to configure a proxy for each application.

As we can see – proxy is cheap/free and easy to find and use; however, they have far more disadvantages in comparison to VPN or SSH tunnels.

What Is A VPN?

VPN or "Virtual Private Network" is a vital privacy, security, and anti-censorship tool which acts as a secure tunnel between your device and the internet. A VPN can help you protect your online traffic from snooping, interference, and censorship among other things.

Currently, commercial providers offer the following VPN protocols: PPTP – used most widely, fast, easy to configure, but is considered the "least protected" compared to the others.

L2TP + IPSec – L2TP provides transport, and IPSec which are responsible for encryption. This bundle has stronger encryption than PPTP, and it is resistant to PPTP vulnerabilities. Also, it ensures message integrity and proper party authentication.

OpenVPN – safe, open, and therefore, common. It allows you to bypass many locks or limitations but requires a separate software client.

SSTP – is as secure as OpenVPN and does not require a separate client.

Most commercial VPN providers offer a choice of two protocols: OpenVPN and PPTP. Less commonly, the proposed protocol L2TP + IPSec. And quite a few offer the protocol SSTP.

There are also services that provide "DoubleVPN," when, before you access the internet, traffic passes two different VPN servers in different countries, or even "QuadVPN," when four servers are used, which the user can select himself and place in any order.

VPN / SSH Pros:

- Quick and convenient; no need to separately configure applications.

VPN / SSH Cons:

- You have to trust the VPN or SSH server/provider.

What Is TOR?

The Tor project is a non-profit organization that conducts research and development into online privacy and anonymity. It is designed to stop people – including government agencies and corporations – learning your location or tracking your browsing habits.

Technically – Tor is a router system in which a client connects to the internet through a chain of nodes. As a rule, the chain consists of at least three nodes; each node knows the addresses of the client and the resource. Also, Tor encrypts messages separately for each node, and open traffic is

visible only to the exit node.

Advantages of TOR:

- High level of client anonymity

Disadvantages of TOR:

- Sending only http-traffic from start node to end node
- User often expects too much from TOR.
- Highly specific for a single task.

Staying anonymous online is becoming harder and harder, and it may become a headache to the main user. Having the proper knowledge and tools available when the need to be anonymous presents itself is important to staying safe. Feel free to add your own experiences with staying anonymous online!

Those dark KR MMO's requiring you to actually live in KR...[/color]

Crimin4L - August 31, 2019, 11:08 am

Definitely a good thread about internet security, very precise and informative.