

Forum:[Hack Forums](#)

Thread: [\[GUIDE\] The Fundamentals of Web Privacy and Anonymity](#)

Elysium - January 26, 2019, 8:04 pm

Introduction

I have noticed that there are a lot of people mistaking the differences between proxies, socks, VPN, VPS, RDP, and a few others. I'm sure there are also some people who would be interested in learning more regarding the different services available to aide in web anonymity so I have taken the time to compile a list of the main services available, how they work, and a short list of some of the providers available.

Contents

- PROXIES
- VPN
- SOCKS
- VPS/VDS
- RDP
- Self-Contained Networks

PROXIES

An HTTP proxy is similar to SOCKS, and may be used for the same purpose when clients are behind a firewall and are prevented from making outgoing TCP connections to servers outside the firewall. However, unlike the SOCKS server, an HTTP proxy does understand and interpret the network traffic that passes between the client and downstream server, namely the HTTP protocol. Because of this the HTTP proxy can ONLY be used to handle HTTP traffic, but it can be very smart about how it does it. In particular, it can recognize often repeated requests and cache the replies to improve performance. Many ISPs use HTTP proxies regardless of how the browser is configured because they simply route all traffic on port 80 through the proxy server.

Web

To put it in simple terms, web proxies are websites that allow users to log in other web pages from its own site. These proxies can download the website requested by the user on his behalf and offer the content to them without demanding any direct user connection to the end website. This explains why a web proxy functions similar to an internet proxy. Web proxies can also function on a shared IP address and allow target websites to identify that a web proxy is being used.

SOCKS

Socket Secure (SOCKS) is an Internet protocol that transfers network packets between a client and server through a proxy server. SOCKS5 additionally provides authentication so only authorized users may access a server.

HTTP/HTTPS

HTTP is an acronym for Hypertext Transfer Protocol across Secure Socket Layer. It is a request protocol opted to facilitate reliable communications and transactions. HTTPS is an extension to HTTP which is used for secure communication

FTP

The FTP proxy allows controlling the FTP traffic. When an FTP client uploads or downloads files to/from a server the proxy identifies the traffic as FTP, allowing the appliance to control file transfers either using TCP optimization or Caching

VPN

A VPN (Virtual Private Network) is a service that lets you access the web safely and privately by routing your connection through a server and hiding your online actions.

PPTP

The Point-to-Point Tunneling Protocol (PPTP) is an older method of VPN encryption designed by Microsoft, which goes all the way back to Windows 95. It is still popular today, despite a known susceptibility to the ASLEAP dictionary attack tool dating back to 2004 that pretty much rendered it obsolete (or should have). So why is it still popular? That's mainly because PPTP is integrated into Windows, as well as Linux and macOS. PPTP enables the encrypted tunnel between the PC and VPN server using TCP port 1723 and General Routing Encapsulation (GRE). Despite the advantages of simple setup, and fast speeds, this protocol is spoiled by major security concerns which date back as far as 1998. In short, PPTP is best avoided for modern users.

L2TP/IPSec

L2TP is the Layer Two Tunneling Protocol, an extension of PPTP, which combines the latter with L2F (Layer 2 Forwarding Protocol) that was designed by Cisco. L2TP does not have integrated encryption, so this gets added via IPSec (Internet Protocol Security).

Unlike PPTP which uses a 128-bit key, L2TP/IPSec has a 256-bit key, and this is considered complex enough for top-secret communications. L2TP is a more recent protocol, and has been supported in Windows since XP, as well as macOS 10.3 or better, and mobile operating systems.

L2TP requires more overhead for the more complicated 256-bit encryption and double encapsulation. It can also be more difficult to set up and configure. It is generally felt to be secure, although more recent NSA leaks would suggest that L2TP is vulnerable to attacks when the encryption is using pre-shared keys.

SSTP

The Secure Socket Tunneling Protocol (SSTP) is directly owned and controlled by Microsoft. That explains its other name – Microsoft Secure Socket Tunneling Protocol (MS-SSTP) – so unsurprisingly, it follows that this is only available on Windows.

The name is derived from the traffic being routed through the Secure Sockets Layer (SSL) protocol, which uses TCP port 443, and makes it pass through firewalls and proxy servers, so it is much less likely to be blocked. As it is not open source, SSTP is one of the most secure of these VPN protocols.

SSTP is more modern than the previously discussed protocols, and it's available in Windows Vista SP1 and later. SSTP was designed for remote client access, and does not generally support site-to-site VPN tunnels.

OpenVPN TCP

All of this built-in redundancy means OpenVPN TCP is considered a highly reliable protocol, with all data being delivered. The downside of this is that all of the sends, confirmations, and resends, require a larger amount of overhead, which drags the network speed down. OpenVPN TCP is an ideal protocol for higher security where latency is not the priority, such as general web surfing and emails. OpenVPN is a popular security protocol created by James Yonan. Unlike the previous proprietary VPN protocols, OpenVPN is open source and published under a GNU General Public

License. This gives the community access to the source code so that any security flaws are identified and dealt with, rather than allowing potential flaws and backdoors to exist in the code. SSL/TLS is used for pre-shared key exchange, adding to the security. The encryption utilized for OpenVPN is also open source, as it uses OpenSSL which supports up to 256-bit encryption.

OpenVPN comes in two main flavors: OpenVPN TCP and OpenVPN UDP. Not all VPN providers give you a choice between these two OpenVPN protocols, but some certainly do – although they may offer little guidance on what's different between them, and which you should choose. We're explaining the TCP variant here, and UDP in the next section.

OpenVPN TCP is based on TCP (unsurprisingly), the Transmission Control Protocol, which combined with the Internet Protocol (IP) creates a set of rules for how computers exchange data back and forth. TCP is a protocol that is connection oriented, and it creates and keeps this connection going while applications perform the exchange of their data. TCP is the most used connection protocol on the internet. One of its advantages is that it's a 'stateful protocol' in that it has integrated error correction. This means that with each packet of data transmitted, a confirmation of the packet's arrival is needed before the next one is sent – and if no confirmation is received the current packet gets resent.

OpenVPN UDP

The alternative protocol to OpenVPN TCP is OpenVPN UDP. UDP stands for User Datagram Protocol, which is another communications protocol for transmitting data between a client and the internet. Unlike OpenVPN TCP, which is designed to maximize reliability of data transmission, OpenVPN UDP is targeted at low-latency transmission of data, without the emphasis on the guaranteed delivery of data (so therefore reliability is sacrificed). UDP just transmits the packets of data without all the redundancy and checks, so it has less overheads, and therefore lower latency. These characteristics make OpenVPN UDP well suited for audio and video streaming tasks, and indeed gaming.

SOCKS

SOCKet Secure (SOCKS) is an Internet protocol that routes network packets between a client and server through a proxy server. A SOCKS server is a general purpose proxy server that establishes a TCP connection to another server on behalf of a client, then routes all the traffic back and forth between the client and the server. It works for any kind of network protocol on any port. SOCKS Version 5 adds additional support for security and UDP. The SOCKS server does not interpret the network traffic between client and server in any way, and is often used because clients are behind a firewall and are not permitted to establish TCP connections to servers outside the firewall unless they do it through the SOCKS server. Most web browsers for example can be configured to talk to a web server via a SOCKS server. Because the client must first make a connection to the SOCKS server and tell it the host it wants to connect to, the client must be "SOCKS enabled." On Windows, it is possible to "shim" the TCP stack so that all client software is SOCKS enabled. SOCKS5 additionally provides authentication so only authorized users may access a server. Practically, a SOCKS server proxies TCP connections to an arbitrary IP address, and provides a means for UDP packets to be forwarded. SOCKS performs at Layer 5 of the OSI model (the session layer, an intermediate layer between the presentation layer and the transport layer).

SOCKS4

SOCKS4 is the first widely adopted version of the protocol. It suffers from a couple of problems which have been remedied in SOCKS4A and SOCKS5, namely:

It requires clients to know the IP address (e.g. 123.123.123.123) of the servers they want to connect to. This means, in most cases, that they must be able to resolve domain names.

There is no authentication. A client only requires a user-name to be able to access SOCKS4 services.

SOCKS4A is a simple extension to SOCKS4 which solves the former problem, but not the latter.

SOCKS4A

SOCKS4a extends the SOCKS4 protocol to allow a client to specify a destination domain name rather than an IP address; this is useful when the client itself cannot resolve the destination host's domain name to an IP address.

The client should set the first three bytes of DSTIP to NULL and the last byte to a non-zero value. (This corresponds to IP address 0.0.0.x, with x nonzero, an inadmissible destination address and thus should never occur if the client can resolve the domain name.) Following the NULL byte terminating USERID, the client must send the destination domain name and terminate it with another NULL byte. This is used for both "connect" and "bind" requests.

SOCKS5

The SOCKS5 protocol is defined in RFC 1928. It is an extension of the SOCKS4 protocol; it offers more choices for authentication and adds support for IPv6 and UDP, the latter of which can be used for DNS lookups. The initial handshake consists of the following:

Client connects and sends a greeting, which includes a list of authentication methods supported.

Server chooses one of the methods (or sends a failure response if none of them are acceptable).

Several messages may now pass between the client and the server, depending on the authentication method chosen.

Client sends a connection request similar to SOCKS4.

Server responds similar to SOCKS4.

Virtual Private Server / Virtual Dedicated Server (VPS / VDS)

VPS term stands for Virtual Private Server. The term is very popular among web hosting enthusiasts and providers. It basically means a virtual box or a virtual machine (VM). It could be used with or without a domain name. VPS is being created for hosting purposes. For example, you can host your website on a VPS. It's a virtualized box which gives users dedicated server resources, storage and bandwidth. The VPS runs its own copy of an operating system (OS). Customers may get root access to the operating system instance. VPS are typically being sold as a web hosting service.

Remote Desktop Protocol (RDP)

RDP is based on, and an extension of, the ITU T.120 family of protocols. RDP is a multiple-channel capable protocol that allows for separate virtual channels for carrying device communication and presentation data from the server, as well as encrypted client mouse and keyboard data. RDP provides an extensible base and supports up to 64,000 separate channels for data transmission and provisions for multipoint transmission.

On the server, RDP uses its own video driver to render display output by constructing the rendering information into network packets by using RDP protocol and sending them over the network to the client. On the client, RDP receives rendering data and interprets the packets into corresponding Microsoft Windows graphics device interface (GDI) API calls. For the input path, client mouse and keyboard events are redirected from the client to the server. On the server, RDP uses its own keyboard and mouse driver to receive these keyboard and mouse events.

In a Remote Desktop session, all environment variables—for example, variables determining color depth and wallpaper enabling and disabling—are determined by the RDP-Tcp connection settings. This applies to all functions and methods that set environment variables in the Remote Desktop

Web Connection Reference and the Remote Desktop Services WMI Provider interface.

Self-Contained Networks

Tor is free and open-source software for enabling anonymous communication. The name is derived from an acronym for the original software project name "The Onion Router". Tor directs Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult to trace Internet activity to the user: this includes "visits to Web sites, online posts, instant messages, and other communication forms". Tor's intended use is to protect the personal privacy of its users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities from being monitored.

The Invisible Internet Project (I2P) is a decentralized anonymizing network built using Java on similar principles to Tor, but which was designed from the ground up as a self-contained darknet. I2P is effectively an internet within an internet. Once connected you can send email, browse websites, use blogging and forum software, host websites, take advantage of decentralized file storage, engage in anonymous real-time chat, and much more. As noted, you can also surf the open web anonymously, but I2P is probably not the best tool for the job in this regard.

Freenet is free software which lets you anonymously share files, browse and publish "freesites" (web sites accessible only through Freenet) and chat on forums, without fear of censorship. Freenet is decentralised to make it less vulnerable to attack, and if used in "darknet" mode, where users only connect to their friends, is very difficult to detect. Communications by Freenet nodes are encrypted and are routed through other nodes to make it extremely difficult to determine who is requesting the information and what its content is. Users contribute to the network by giving bandwidth and a portion of their hard drive (called the "data store") for storing files. Files are automatically kept or deleted depending on how popular they are, with the least popular being discarded to make way for newer or more popular content. Files are encrypted, so generally the user cannot easily discover what is in his datastore, and hopefully can't be held accountable for it. Chat forums, websites, and search functionality, are all built on top of this distributed data store.

Providers For more information on specific VPN providers please reference the thread listed below, written by [Pronouncer](#):

[== SECRECY == >>> AN INTRODUCTION TO VPN'S <<<](#)

VPN Options:

- [WhoamiVPN](#)
- [ProtonVPN](#)
- [.com/\]\[censored\]](#)
- [ExpressVPN](#)
- [AirVPN](#)
- [AZIREVPN](#)
- [blackVPN](#)
- [cryptostorm](#)
- [FrootVPN](#)
- [HIDEme](#)
- [IVPN](#)
- [MULLVAD](#)
- [OVPN](#)
- [Perfect-Privacy](#)
- [proxy.sh](#)

- [Trust.zone](#)
- [vpn.ht](#)
- [VPN AREA](#)
- [VPNTunnel](#)

Proxy Options:

- [Proxies24](#)
- [Hide](#)
- [FineProxy](#)

RDP Options:

- [BoomRDP](#)
- [99RDP](#)
- [AmInServe](#)
- [QHoster](#)
- [RouterHosting](#)

VPS Options:

- [SolVPS](#)
- [HOSTINGER](#)
- [orangewebsite](#)
- [Securedragon](#)
- [.com/\]\[censored\]](#)

Self-contained Networks:

- [TOR](#)
- [I2P](#)
- [The Freenet Project](#)

Other Options:

- [SADD.IO](#)

Cyber86 - January 26, 2019, 9:08 pm

Tor, you need to mention Tor, the free onion router that doesnt log.

Elysium - January 26, 2019, 9:23 pm

(Jan 26, 2019 10:08 PM)Cyber86 Wrote: [\[CITE\]](#) Tor, you need to mention Tor, the free onion router that doesnt log.

SADD.IO is one option that provides web based virtual desktops who route all connections through the tor network. You're right though, TOR would be a good addition. I'll add that shortly.

Cyber86 - January 26, 2019, 11:39 pm

(Jan 26, 2019 10:23 PM).Elysium. Wrote: [\[CITE\]](#) SADD.IO is one option that provides web based virtual desktops who route all connections through the tor network. You're right though, TOR would be a good addition. I'll add that shortly.

SADD.IO is pretty dank, just tried it.

Also for VPNs, I reccomend you list the ones on privacytools.io website.

WhoamI probably logs, N-o-r-d is honepot and Express Logs.

I suggest BlackVPN, Ipredator.se, or ProtonVPN

Elysium - January 27, 2019, 8:09 am

(Jan 27, 2019 12:39 AM)Cyber86 Wrote: [\[CITE\]](#) SADD.IO is pretty dank, just tried it.

Also for VPNs, I recommend you list the ones on [privacytools.io](https://www.privacytools.io) website. Whoami probably logs, N-o-r-d is honeypot and Express Logs.

I suggest BlackVPN, Ipredator.se, or ProtonVPN

WhoamiVPN is run by a member here on the forum. Per their site, they do not log. I have expanded the VPN list to include some listed on [provacytools.io](https://www.privacytools.io). Also Express is listed on [privacytools](https://www.privacytools.io) and per my research they don't keep any traffic logs.

Phantogram890 - January 28, 2019, 7:21 pm

This is a pretty well put together guide, thanks for sharing this for the community.

Elysium - February 10, 2019, 11:14 am

I have updated the providers list with few more options that accept bitcoin as payment for services.

yet_man_jack - June 23, 2019, 5:55 pm

Well Written guide. I didn't know fully how socks worked, thanks for that.

hendrawan - July 4, 2019, 6:01 am

Informasi yg cukup lengkap dan mudah dimengerti

iProtox - October 30, 2019, 1:32 pm

This is a very well written guide, thank you for your knowledge. Can anyone give insight on the best funnel to mix some of these protocols in order to achieve a multi-layered setup of security that gives the highest level of anonymity?

i.e Host OS (with high end firewall + hardware firewall) > VPN (kill switch enabled) > RDP or VPS > TOR?

ThatCoderX - October 30, 2019, 1:57 pm

At this moment I would not recommend having [censored] included in this. If you are un-aware, they have recently been amid controversy of a breach on one of their servers in 2018. Though they claim no data was accessed and that this was an isolated incident this is not something you want to see from a VPN company. Never mind the fact that they did not even disclose it to users. Otherwise good guide and introduction to network privacy.