Common terms used in the VPN world

If you're just starting out using a VPN, you may find many specific terms used here. Something might be new to you, but we will cover the most common VPN terminology in this article, so you get a better view.

Client/server. This terminology describes how network communications work. To make it simple – the client is always requesting information, and the server provides the requested information. If you connect to the US Dallas server, your Surfshark app is the client (asking for information), and the server in Dallas provides you with the requested information.

DNS. You may find this term used pretty often. You may not have noticed, but you are using various DNS servers every day. Basically, the DNS server translates the domain name (facebook.com) to an IP address (69.63.176.13). It's like a phone book where all names (website domains) and numbers (IP addresses) are stored.

DNS leaks. If your VPN is misconfigured or something interferes with a VPN connection, you may experience a DNS leak that exposes your real location to your visited websites.

Encryption. Encryption is a way to encode information. At PureVPN, encryption encodes (encrypts) all information that your device sends or receives. If the information is encrypted, it becomes unreadable for everyone else except you.

IP leak. If a VPN is not configured correctly, your real IP address might slip out.

IPv4. It's the original design of the internet protocol address. Due to the exponential growth of internet users, IPv4 is no longer sustainable, since it only allows a total of 4 billion IP addresses.

IPv6. Due to the lack of IP addresses that IPv4 can provide, IPv6 was introduced. It's the modern version of the original IPv4.

ISP. Internet service provider, a.k.a. ISP, is an organization that provides you with an internet connection.

Leaks. If your IP address, DNS address, or WebRTC addresses are still visible after connecting to a VPN, that's called a leak. Here you can check if you have leaks.

Logs. In general, there are two kinds of logs: Usage logs that include visited websites, and connection logs that contain connection times, data usage, users' real IP address, and an IP address assigned by a VPN. Some VPN providers keep no logs of your VPN activity, except information needed for billing and troubleshooting. PureVPN is one of them.

P2P. That stands for a peer-to-peer network that connects individual users to a system where they can share files (torrents) and other resources with each other directly.

Ping (latency). The ping method is useful for checking if the server is accessible and how long it takes to respond. To put it simply – by pinging the server (website name or IP address), you send a request to it and wait for an answer. If you receive a response that means that the server is available. Usually, the faster server responds, the smoother internet connection you will have.

Protocol. It’s a set of rules that determines how your information will be divided into pieces and sent from/to your device.

For example, the OpenVPN (UDP) protocol divides your information into tiny packs of bytes and send it to the server in random order. OpenVPN (TCP) will also split all the data into pieces, but it assigns a number to each pack of information and sends it in a strict order. Changing the protocol on your PureVPN app might improve the connection speed and stability.**WebRTC.** WebRTC stands for Web-Real Time Communication. As the name suggests, this technology allows for real-time communication between browsers without requiring an intermediate server (after the connection has been already established)