

StoreVPN Protocols

StoreVPN supports a wide variety of VPN connection types to make our service accessible to everyone. Learn more about the VPN protocols we offer below.

[GET STOREVPN](#) (button goes to packages page)

What VPN Connection Types Does StoreVPN Offer?

WireGuard®

WireGuard is a new protocol designed as an easier, faster, and more secure option than its predecessors. This general-purpose protocol is ideal for running on a diverse range of platforms and devices with easy implementation. Using state-of-the-art cryptography, WireGuard is far more secure than other available protocols. WireGuard is also noted for providing faster speeds than OpenVPN and is also significantly less complex than IPsec. WireGuard also improves the battery life of mobile devices due to its stateless nature.

IKEv2 (Internet Key Exchange Protocol Version 2)

IKEv2 is a modern protocol that uses IPsec. With this protocol, we support MOBIKE, allowing your mobile devices to switch between cellular and Wi-Fi networks without interrupting your VPN connection. As our protocol of choice at StoreVPN, IKEv2 is secure and fast.

OpenVPN

OpenVPN is widely adopted industry standard SSL VPN. Since OpenVPN is SSL-based, the traffic looks very similar to a secure website in your browser. StoreVPN supports TCP and UDP connection types on multiple ports, as well as OpenVPN Scramble. See below for more information on these three VPN connection types.

Available for:

- TCP (Transmission Control Protocol)

TCP, especially using port 443, most closely resembles encrypted web traffic. While TCP may lead to slower VPN speeds on high latency networks, such as Wi-Fi hotspots at hotels or coffee shops, it does protect against packet loss. StoreVPN offers OpenVPN TCP connections on multiple ports to help ensure maximum compatibility with routers.

- [UDP \(User Datagram Protocol\)](#)

UDP connections are often faster than TCP-based OpenVPN connections due to UDP having less overhead than TCP. Please be aware that some routers may block UDP ports and there is a small chance for packet loss.

- [Scramble](#)

Scramble is a patch on top of OpenVPN. This patch helps to further mask the OpenVPN protocol, making it harder to detect as VPN traffic. Both UDP and TCP connection types are available for use with OpenVPN Scramble. StoreVPN offers OpenVPN UDP connections on multiple ports to help ensure maximum compatibility with routers.

IPSec (IP Security)

This is the older, less secure form of IPSec, sometimes called Cisco IPSec. It has been replaced by IKEv2. For legacy reasons, we still support IPSec.

Firewall Considerations

IPSec/IKEv2

Some routers have an IPSec passthrough option, which will need to be enabled if there is one. This is usually the default. IPSec and IKEv2 also need UDP ports 500 and 4500 to not be blocked.

OpenVPN

StoreVPN allows several ports for OpenVPN, both UDP and TCP. If you are having trouble connecting, TCP 443 or UDP 53 may help.

WireGuard

WireGuard uses ports in the 50,000 to 60,000 range depending on the server. Since these are considered ephemeral ports, many firewalls will already allow access for these port numbers.

Which VPN Protocol Should I Use?

Choosing the right VPN protocol will depend on your needs and the type of device you're using. For Windows, macOS, and iOS, we would recommend using IKEv2 for the best speeds with the best encryption. However, if you're on Android, or have issues with IKEv2, OpenVPN may be a good alternative. For the best mix of speed and security, we recommend using WireGuard, as this is a general-purpose protocol that is supported for Windows, macOS, iOS, and Android.