There is a lot of information and endless discussion about which VPN provider is best. Let’s take a look at a few popular VPN solutions today and then decide what you should choose.

OpenVPN

The OpenVPN tunneling protocol is an incredibly secure option for VPN connections, utilizing the Secure Socket Layer (SSL) encryption protocol and AES-256 encryption to ensure data shared via the Internet remains private. OpenVPN is widely regarded as the most secure VPN tunneling protocol, and it can provide faster connections than other protocols. Additionally, it’s often able to bypass most firewalls, making it a popular choice for users who require maximum privacy and security.

Pros:

- Strong security measures utilizing the best encryption algorithms available.
- Decent connection speeds, making it a viable option for streaming and other data-intensive tasks.
- Highly customizable settings to meet specific user needs.
- Regular updates to ensure optimal performance and security.
- Extensive testing and auditing to ensure the protocol’s reliability and safety.
- Compatibility with all major platforms, including Windows, macOS, iOS, and Android.
- The ability to bypass most firewalls.

Cons:

- Difficulty in setting up the protocol manually, especially for users with limited technical expertise.
- The need for third-party software to set up and configure the protocol, which may require additional time and effort.

L2TP/IPsec

The Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs). However, L2TP only uses encryption for its own control messages, using an optional pre-shared secret, and does not provide any encryption or confidentiality of content by itself. Instead, it creates a tunnel for Layer 2, which may be encrypted, and this tunnel can be passed over a Layer 3 encryption protocol like IPsec. Therefore, while L2TP provides a secure tunnel for data transmission, it relies on other encryption protocols to ensure full confidentiality and security of the transmitted content.

Pros:

- Decent connection speeds, making it a viable option for most everyday tasks.
- A good security package, providing a reliable level of security for data transmitted over the VPN.
- Ease of setup, with many VPN providers offering simple software solutions to get started quickly.
- Native support for L2TP on a wide range of platforms, including Windows, macOS, and mobile devices, making it a convenient option for users on these platforms.

Cons:

- Resource-intensive due to the double encapsulation process, which can affect connection speeds and system performance.
- Limited availability of ports (only 3 ports available), which may be easily blocked by firewalls.

IKEv2/IPSec

IKEv2 (Internet Key Exchange) is a VPN protocol jointly developed by Cisco and Microsoft, with a focus on mobility and compatibility with smartphones, tablets, and other mobile devices. One of the main advantages of IKEv2 is its ability to maintain a secure VPN connection seamlessly, even if your device switches between different network types, such as Wi-Fi or mobile data.

IKEv2 is often used in conjunction with the IPSec (Internet Protocol Security) protocol to provide even greater data encryption and authentication security. Together, these two protocols provide robust protection for data transmitted over the VPN, making IKEv2 a popular choice for users who prioritize security and mobility.

Pros:

- High connection speeds, making it one of the fastest VPN protocols available.
- Excellent stability, ensuring reliable connections even during network changes or disruptions.
- Ease of setup, with many VPN providers offering simple software solutions to get started quickly.
- Compatibility with many cryptographic algorithms, providing flexibility in terms of security and encryption options.

Cons:

- Can be easily blocked by some firewalls, which can limit its availability in certain network environments.
- It is supported by fewer platforms than other VPN protocols, which can make it less accessible for some users.

SSTP

SSTP (Secure Socket Tunneling Protocol) was developed by Microsoft and first introduced with Windows Vista. It’s a VPN protocol that’s widely regarded as the successor to PPTP and L2TP, and is included in later versions of Windows as well. SSTP provides strong security measures that are comparable to OpenVPN, and it’s also capable of bypassing many firewalls.

Overall, SSTP is a reliable and secure VPN protocol that’s particularly well-suited for users who are using a Windows-based system.

Pros:

- Good security measures with solid encryption algorithms, ensuring that data transmitted over the VPN is kept secure and confidential.
- Decent connection speeds, making it a viable option for most everyday tasks.
- The ability to bypass many firewalls.
- Intuitive design and easy integration with Windows-based systems, providing a seamless experience for users on these platforms.

Cons:

- Poorer performance on non-Windows operating systems.
- Difficult to set up on non-Windows devices, especially for users with limited technical expertise.