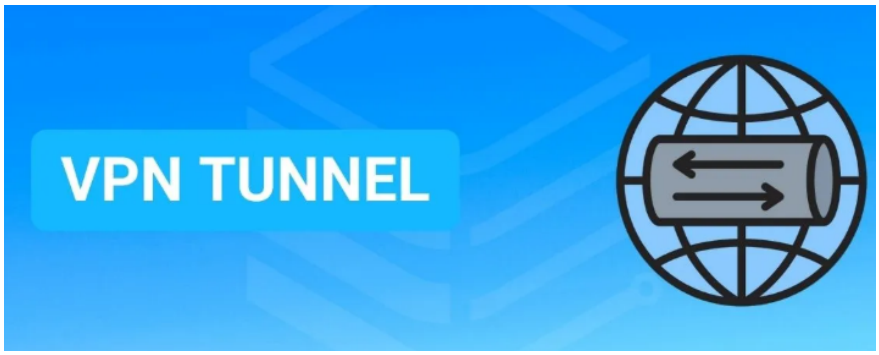
What is VPN Tunnel? How does it work?

VPN Tunnel is an encrypted connection between your device and the VPN server. Neither hackers nor Internet service providers can access your data without the password.

Normally, people often use VPN to break the firewall, access a website that is blocked by the network. And conversely, to encrypt and secure activities on the Internet, people will use VPN Tunnel? So what is VPN Tunnel and how do they work? Find out with ***TipsMake*** in the article below.

What is VPN Tunnel?

VPN Tunnel is an encrypted connection between your device and a VPN server. Neither hackers nor Internet service providers can access your data without the password. VPN Tunnel protects users from attacks and hides their activities on the Internet.



What is VPN Tunnel?

How does VPN Tunnel work?

VPN Tunnel works by using tunneling protocols to create a secure, encrypted connection between your device and a remote server. Internet traffic is then routed through this tunnel to protect your data from being intercepted or stolen, hiding your internet activity from hackers, trackers, and other third parties.

When you turn on a VPN, it establishes an encrypted connection between your device and the server, hiding your IP address and allowing you to send and receive data privately and securely.

Popular VPN Tunnel Protocols

WireGuard

WireGuard is a free, open source VPN protocol. Unlike older protocols, WireGuard offers fast connection speeds, efficient resource usage, and simple configuration. WireGuard uses advanced encryption techniques to create tunnels.

WireGuard is a popular VPN Tunnel protocol on mobile devices. WireGuard is constantly being improved by developers, so its performance and service quality are also increasing.

1. Security: High
2. Speed: Fast
3. Type: Full tunnel or split tunnel

OpenVPN

OpenVPN is a widely used open source VPN protocol known for its strong security and flexibility. It is currently considered one of the leading VPN Tunnel protocols because of its strong encryption, customization, and firewall bypass capabilities.

OpenVPN supports many computer operating systems such as Linux, Windows, MAC and mobile operating systems such as iOS, Android. In addition, OpenVPN also supports mobile operating systems such as FreeBSD, NetBSD, Solaris and OpenBSD.

1. Security: High
2. Speed: Medium
3. Type: Full tunnel or split tunnel

Secure Socket Tunneling Protocol (SSTP)

SSTP (Secure Socket Tunneling Protocol) is a highly secure VPN protocol developed by Microsoft. This protocol encapsulates data in an SSL/TLS encrypted tunnel and does not use fixed ports. Therefore, SSTP has strong firewall protection and bypass capabilities. SSTP can even bypass the Great Firewall of China, a firewall that many VPN protocols have not been able to bypass.

SSTP has low compatibility although this VPN Tunnel is supported on Windows operating system but if you want to use it on other devices then you still need a third party application.

1. Security: High
2. Speed: Medium
3. Type: Full tunnel

Layer 2 Tunneling Protocol (L2TP/IPsec)

L2TP/IPsec is a VPN Tunnel that combines two protocols: Layer 2 Tunneling Protocol and Internet Protocol Security to establish a secure VPN connection. L2TP creates a tunnel to transmit data while IPsec is responsible for encrypting and authenticating that data.

1. Security: Medium
2. Speed: Medium
3. Type: Full tunnel

Point-to-Point Tunneling Protocol (PPTP)

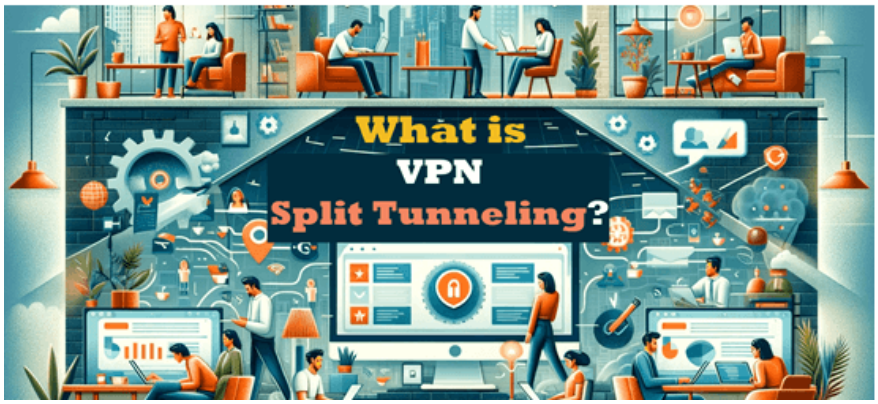
PPTP (Point-to-Point Tunneling Protocol) was one of the first VPN Tunnels and is not widely used today. In its heyday, PPTP was known for its extremely fast connection speeds and easy setup.

Although they have fast connection speeds, their encryption capabilities are weaker than some current VPN Tunnels. This means that hackers can easily access and steal user information while transmitting data.

1. Security: Low
2. Speed: Fast
3. Type: Full tunnel

What is VPN Split Tunneling?

VPN Split Tunneling is a feature that allows users to route some Internet traffic through the VPN while others go directly to the Internet, bypassing the VPN. VPN Split Tunneling splits traffic into two streams. One stream is encrypted and routed through the VPN Tunnel, while the other stream is unencrypted and connects directly to the Internet.



What is VPN Split Tunneling?

One of the advantages of VPN Split Tunnels is their performance. VPN Tunnels save bandwidth and improve speeds for unencrypted activities by specifying which traffic should go through the VPN.

However, VPN Split still has potential risks. Since some traffic is not encrypted, it can be threatened or attacked. Therefore, when using VPN Split Tunnel, users need to be careful to maintain security.

Benefits of using VPN Tunnel

VPN Tunnel is a secure connection between the device and the server, protecting traffic and activities when accessing the Internet. All data and activities are tightly encrypted, information theft is almost impossible. Users can browse the web without worrying about being hacked.

Can VPN Tunnel be hacked?

The answer is yes but this is very rare. However, you do not need to worry too much because you are just a normal user, hackers often target profitable targets.

Hacking a VPN Tunnel cannot be done by breaking the encryption, but by stealing the encryption key. There are many different ways to do this, but using a VPN will significantly reduce the risk of this happening.

Conclude

VPN Tunnel is a useful tool to protect your personal information and improve your Internet browsing experience. However, like any other technology, VPN is not completely free from risks. Hopefully this article has helped you better understand what VPN Tunnel is and how this technology works.

You finished reading the article "**What is VPN Tunnel? How does it work?**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
