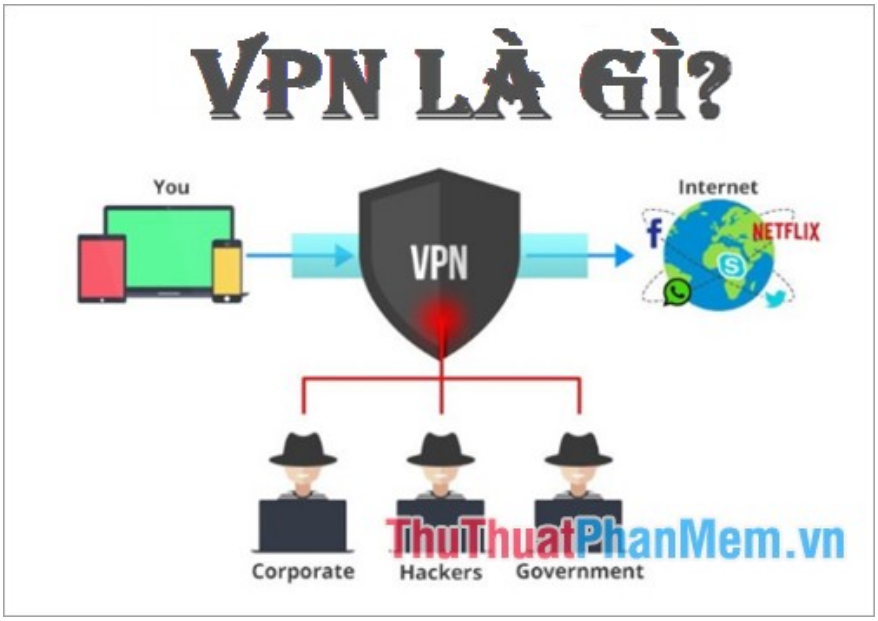
What is a VPN

The concept of VPN you are still quite vague, do not understand exactly what VPN is? What are the benefits of using VPN? What types of VPN connections are there? Which free VPN software is most used? How to use VPN on a computer ...? The following article will answer

Currently, spyware, monitoring and monitoring during the use of the Internet is increasing or many sites are blocked by geographic area you do not access. So many people are already interested in using VPN services. But the concept of VPN you are still quite vague, do not understand exactly what VPN is? What are the benefits of using VPN? What types of VPN connections are there? Which free VPN software is most used? How to use VPN on a computer .?

The following article will answer all your questions about VPN in the easiest way to understand.



VPN concept

VPN stands for **Virtual Private Network** (virtual private network) allows you to create connections to other network links securely over the Internet.

Basically, each VPN is a separate network that uses a common infrastructure (Internet) to connect with sites (individual networks) or multiple remote users. Instead of using a physical connection each VPN uses virtual connections established over the Internet from the company's private network to remote branches or employees.

To be able to send and receive data through the public network while ensuring safety and security, the VPN provides mechanisms to encrypt data on the transmission line into a secure tunnel between the sender. and destination. To create such a secure pipe, the data must be encrypted, providing only the first packet to be able to reach the destination through the public network quickly.

The benefits of VPN

1. Lower cost than private networks.
2. Flexibility in connection
3. Increased security: must have access to view data.
4. Encrypt your data: VPNs are hard to break, but not impossible, encrypting your information will be very useful because if someone breaks your connection, your information will not be compromised. damage because it is encrypted.
5. Support for the most common network protocols available today is TCP / IP.
6. IP address security: the information sent on the VPN is encrypted, so the addresses within the private network are concealed and only use addresses outside the Internet.

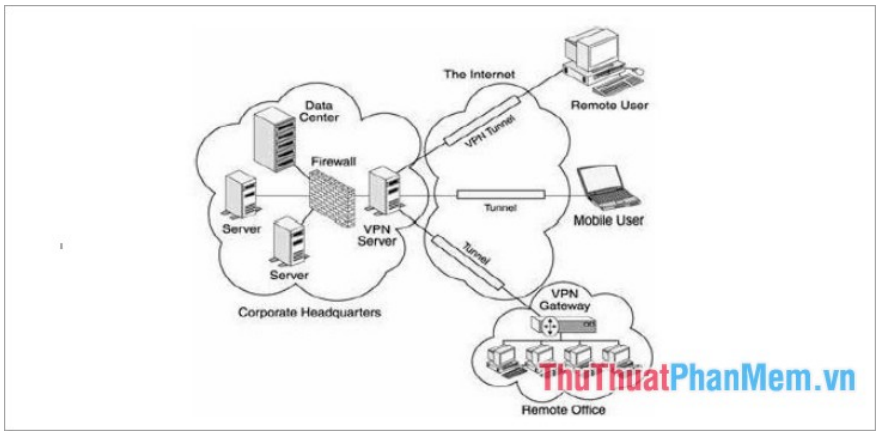
Types of VPN connections

VPN technology is classified into two basic types: **Remote Access VPN** and **Site-to-Site.**

1. Remote Access VPN - Remote access

Remote Access VPN allows users to connect to a private network and access services and resources remotely. Connection between user and private network will occur via Internet and secure, private connection.

Remote Access VPN is useful for business users as well as home users.



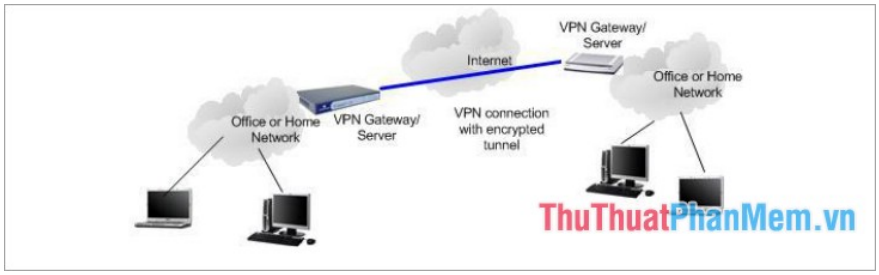
A company employee, while traveling, uses a VPN to connect to his or her own corporate network and remotely access files and resources on the private network.

Home users or private users of a VPN primarily use the VPN service to bypass regional restrictions on the Internet and access blocked websites.

Internet security conscious users also use VPN services to enhance Internet security and security.

2. Site-to-Site

Site-to-Site VPN is primarily used in businesses, **site-to-site** creates a virtual bridge between networks at remote offices and connects them via the Internet and maintains secure communications. and privacy between networks.



When multiple offices of the same company are connected using the Site-to-Site VPN type, it is called an **Intranet-** based VPN (local VPN). When companies use a **site-to-site** VPN to connect to another company's office, it is called an **Extranet-** based VPN (extended VPN).

VPN protocols

The above two types of VPNs are based on different VPN security protocols. Each VPN protocol offers different features and security levels.

1. Internet Protocol Security (IPSec)

Internet Protocol Security (IPSec) is the protocol used to ensure Internet communication over IP networks. IPSec holds Internet Protocol by authenticating the session and encrypting each data packet during connection.

IPSec operates in two modes: **Trandsport mode** and **Tunneling mode** , to protect data transmission between two different networks. The transport method encrypts the message in the packet and tunnel mode encrypts the entire packet.

IPSec can also be used with other security protocols to enhance security systems.

2. Layer 2 Tunneling Protocol (L2TP)

Layer 2 Tunneling Protocol is a **tunneling protocol** often combined with another VPN security protocol such as **IPSec** to create a highly secure VPN connection. **L2TP** creates a tunnel between two **L2TP** connection points and **IPSec** protocol that encrypts data and handles secure communication between the tunnel.

3. Point-to-Point Tunneling Protocol (PPTP)

Protocol **Point-to-Point Tunneling Protocol** creates a tunnel and encapsulate packets. It uses the **Point-to-Point (PPP)** protocol to encrypt data between connections. **PPTP** is one of the most widely used VPN protocols and has been in use since Windows 95. In addition to Windows, **PPTP is** also supported on Mac and Linux.

4. Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

Secure Sockets Layer (SSL) and **Transport Layer Security (TLS)** create a VPN connection, where web browsers act as client and user access restricted to specific applications instead of the entire network.

Protocols **SSL** and **TLS** are often used by the online shopping sites and service providers. Web browsers switch to **SSL** easily and virtually no action is required from users, as web browsers are integrated with **SSL** and **TLS** . **SSL** connections have https at the beginning of the **URL** instead of http.

5. Open VPN

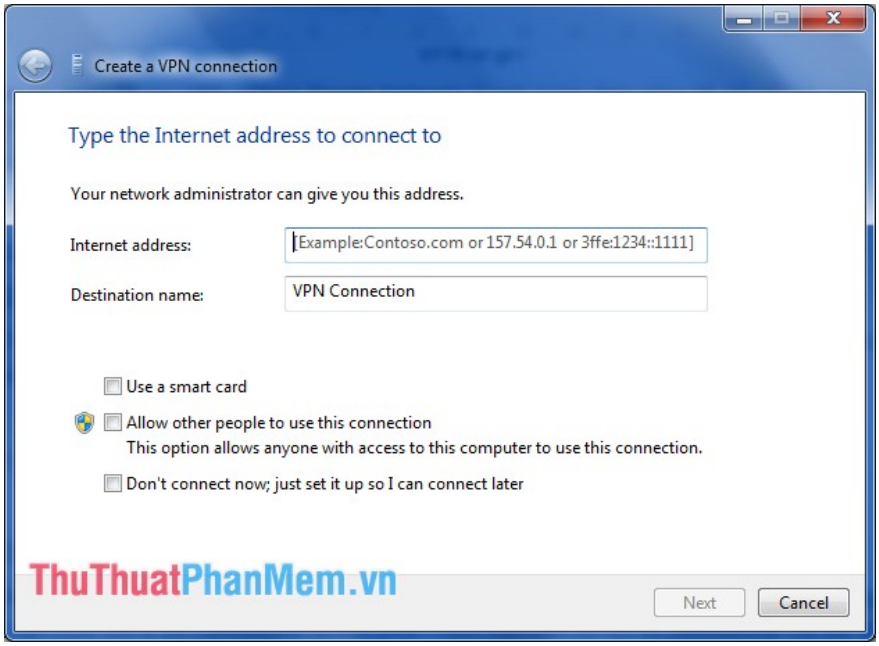
OpenVPN is an open source VPN useful for making point-to-point and site-to-site connections. It uses a custom security protocol based on **SSL** and **TLS protocols** .

6. Secure Shell (SSH)

Secure Shell (SSH) creates a VPN tunnel through which data transfer will occur and ensures that the tunnel is encrypted. **SSH** connections are created by an **SSH** client and data is transferred from a local port to the remote server via encrypted tunnel.

How to use a VPN

On Windows operating system, press the **Windows** key **(** Start **Menu**), and enter the keyword VPN into the search box. Then choose **Set up a virtual private network (VPN) connection** . Here you can create vpn at the **Create a VPN connection interface.**



Free VPN options

If you're just starting to use a VPN to use public wifi access or geographically blocked websites, **TunnelBear** is a software you should use. **TunnelBear** installs with just a few clicks, and you do not need to configure VPN in Windows. **TunnelBear** offers 500MB / month with the free version, if you use more then you can upgrade to the paid version.

You can download **TunnelBear** software here: https://www.tunnelbear.com/

In addition, you can also refer to and use the software **SurfEasy** or **StrongVPN.**

Download **SurfEasy** software here: https://www.surfeasy.com/lang/fr/

Download the **StrongVPN** software here: https://strongvpn.com/

Hopefully, with the article provided to you, you will understand what VPN is? And you will easily choose a VPN software to use. Good luck!

You finished reading the article "**What is a VPN**" 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.