VPN theory - What is a virtual private network?

For those who are new to school, who have just stepped into the field of Information Technology - IT, until working people ... they must have heard of VPN many times, or virtual private network, virtual private network. ... So what is VPN really? Let's TipsMake.com discuss the definition of VPN, how to apply the model, this system in work.

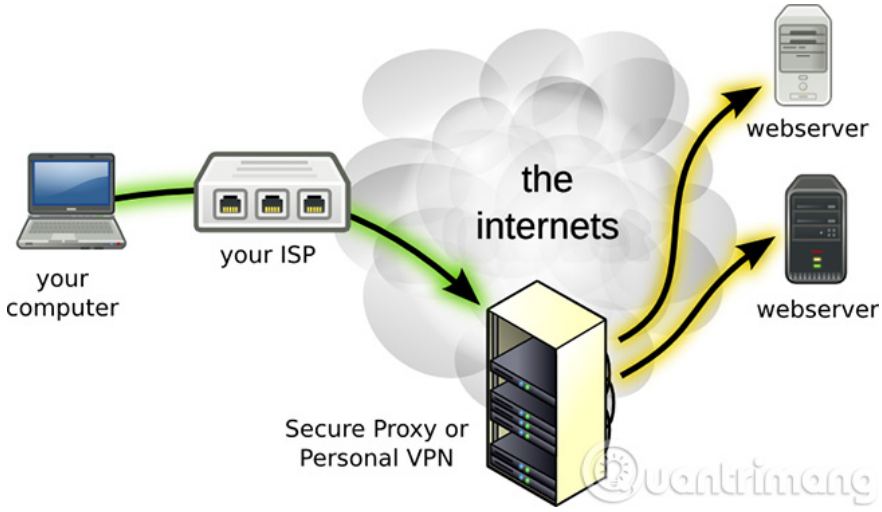
For those who are new to school, who have just stepped into the field of Information Technology - IT, until working people . they must have heard of VPN many times, or virtual private network, virtual private network. . So what is VPN really? Let's TipsMake.com discuss the definition of VPN, how to apply the model, this system in work.

Learn about VPN

1. 1. What is VPN?
2. 2. Common protocols in VPN
    1. Learn about VPN protocols
    2. Weak protocols
    3. These protocols have better security
    4. So which protocol should I choose?
3. 3. Advantages and disadvantages of VPN

1. What is VPN?

VPN is a virtual private network, Virtual Private Network, is a network technology that makes a secure network connection when joining a public network such as the Internet or a private network owned by a service provider. Large corporations, educational institutions and government agencies use VPN technology to allow remote users to securely connect to their own private network.



A VPN system can connect different sites, based on region, geographical area . similar to the **Wide Area Network (WAN)** . In addition, VPN is also used to "diffuse", expanding Intranet models to transmit better information and data. For example, schools still have to use VPNs to connect campuses (or between branches with headquarters) together.

If you want to connect to the VPN system, each account must be authenticated (must have a **Username** and **Password**). These account credentials are used to grant access through a **Personal Identification Number (PIN)** , which is usually valid for a certain period of time (30 seconds or 1 minute). .

When connecting a computer or another device such as a phone or tablet to a VPN, the computer works like it is on the same local network as the VPN. All traffic on the network is sent through a secure connection to the VPN. As a result, you can securely access your local network resources even when you're far away.

You can also use the Internet as if it were in the position of a VPN, which offers some benefits when using public WiFi or blocked web access, geographic limits.

When browsing with VPN, the computer will contact the site via an encrypted VPN connection. All requests, information, data exchanged between you and the website will be transmitted in a secure connection. If using a US VPN to access Netflix, Netflix will see your connection from the United States.

Although it sounds pretty simple, but in fact VPN is used to do a lot of things:

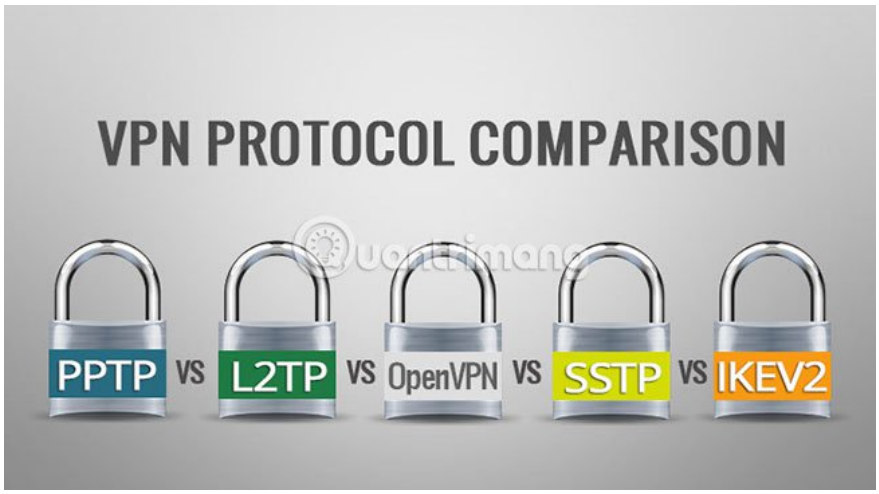
1. **Access to corporate networks when away:** VPNs are often used by business people to access their business networks, including all resources on the local network, while traveling on the go. travel, . Resources in the intranet do not need to be in direct contact with the Internet, thereby increasing security.
2. **Access your home network, though not at home:** You can set up your own VPN to access when you're not at home. This will allow remote Windows access via the Internet, using files shared on the local network, playing games on the computer via the Internet just like being on the same LAN.
3. **Anonymous Browsing:** If you are using public WiFi, browsing the web on non-https websites, then the safety of the exchange data in the network will be exposed. If you want to hide your browsing activity for more secure data, you should connect to VPN. All information transmitted over the network will now be encrypted.
4. **Access to websites that are restricted from geography,** bypass Internet censorship, bypass firewalls, .

5. **Downloading files:** Downloading BitTorrent on VPN will help speed up downloading files. This is also useful for traffic that your ISP may interfere with.

2. Common protocols in VPN

VPN products often have convenience, efficiency and security are varied. If security is a top concern, an organization needs to pay attention to the protocols supported by the VPN service. Some widely used protocols have concerns that are of concern, while others provide the most advanced security. The best protocols today are OpenVPN and IKEv2.

Learn about VPN protocols



The nature of the VPN protocol is a set of protocols. There are a number of functions that every VPN must solve:

- **Tunnelling** (data transfer technology across multiple networks with different protocols) - The basic function of VPN is to distribute packets from one point to another without exposing them to anyone on the line. . To do this, VPN packages all data in a format that both the client and server understand. The sender of the data places it in the format of tunnels and extractors to obtain information.

- **Encryption** : Tuning does not provide protection. Anyone can extract data. Data also needs to be encrypted on the line. The recipient will know how to decode the data from a certain sender.

- **Authentication** . For security, VPN must verify the identity of any client trying to communicate with it. The client needs to confirm that it has reached the intended server.

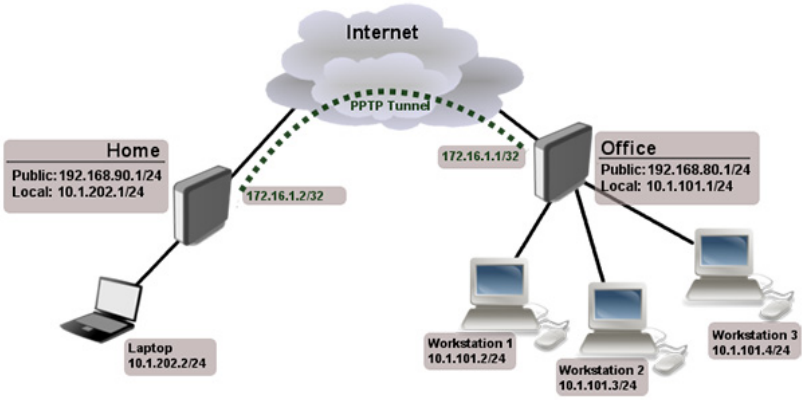
- **Session management** : Once the user is authenticated, the VPN needs to maintain the session so that the client can continue to "communicate" with it for a period of time.

In general, VPN protocols consider tunneling, authentication and session management as a package. Weaknesses in any function are potential security holes in the protocol. Encryption is a specialty, it is also very difficult, so instead of trying to create something new, VPNs often use a combination of reliable encryption protocols. Here are the common VPN protocols and their weak strengths.

Weak protocols

Point-To-Point Tunneling Protocol (PPTP)

The oldest protocol still in use is PPTP (Point-to-Point Tunneling Protocol).PPTP was first used in 1995. PPTP does not specify encryption protocols but may use some protocols such as powerful MPPE-128.The lack of strong protocol standardization is a risk, since it can only use the strongest encryption standard that both sides support.If one side only supports the weaker standard, the connection must use weaker encryption than the user expects.



However, the real problem with PPTP is the authentication process. PPTP uses MS-CHAP protocol, can be easily cracked in the current period. An attacker can log in and impersonate an authorized user.

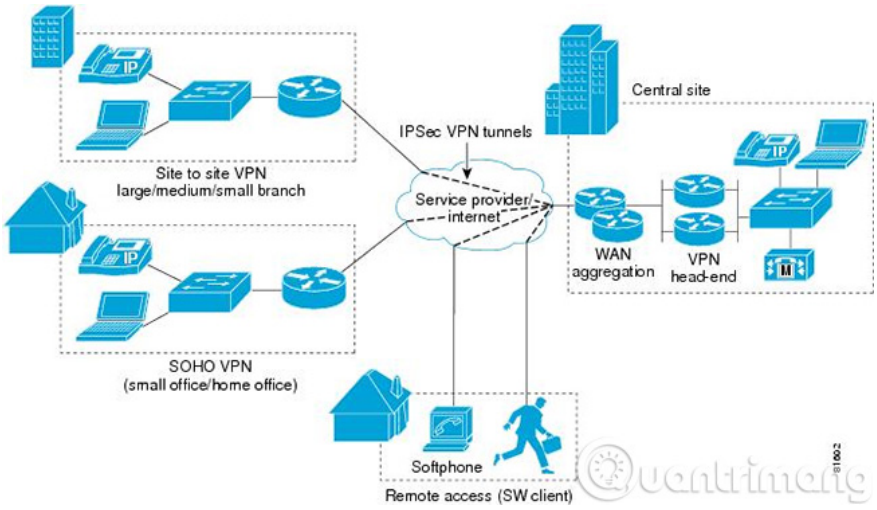
IP security (IPSec)

Used to secure communications, data streams in the **Internet** environment (external VPN environment). This is the key point, the amount of traffic through IPSec is used mainly by **Transport modes** , or **tunnels** (or tunnel - this concept is often used in Proxy, SOCKS) to **CODE** data in VPN.

1. What is a proxy?
2. What is SOCKS?

The difference between these modes is:

1. **Transport mode is** only responsible for encrypting data inside packets (or even knowing under the payload word). While the **Tunnel** encrypts the entire data package.



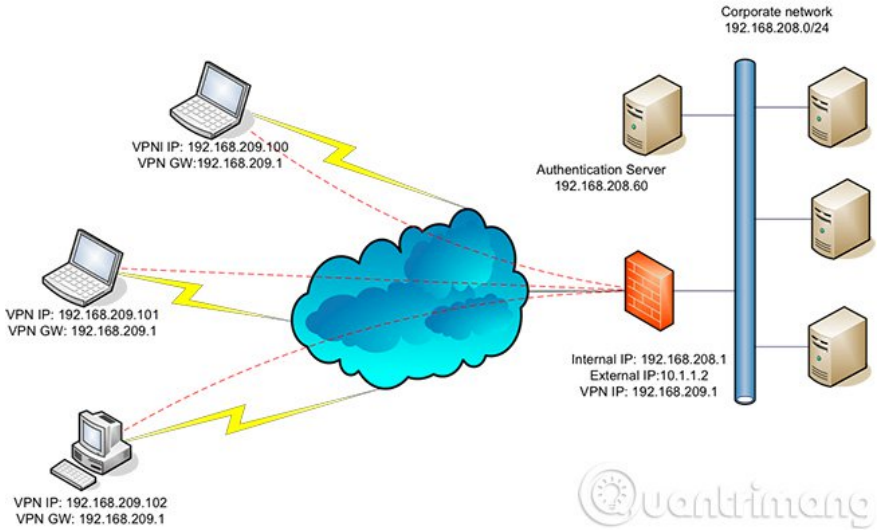
Therefore, IPSec is often referred to as **Security Overlay** , because IPSec uses security classes compared to other protocols.

L2TP

L2TP protocol usually works with IPSec encryption algorithm.It is significantly more powerful than PPTP but still makes users worry.The main vulnerability in L2TP / IPSec is the public key exchange method.Exchange key public Diffie-Hellman is a way for both parties to agree on the next encryption key and no one will know about this key.There is a method that can 'crack' this process, which requires quite a bit of computing power, but then it allows access to all communications on a certain VPN.

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

There is a section similar to IPSec, the above two protocols also use passwords to ensure safety between connections in the Internet environment.

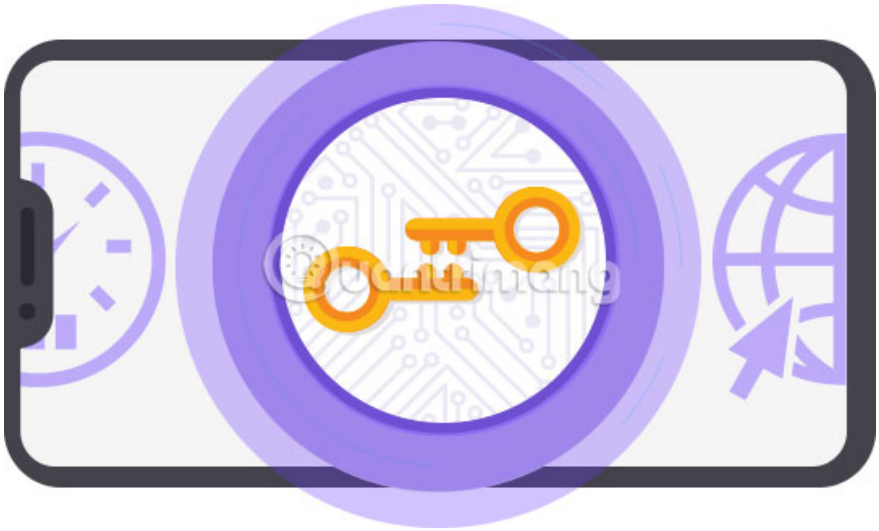


SSL VPN model

In addition, the above two protocols also use **Handshake** mode - related to the account authentication process between the client and server. In order for a connection to be considered successful, this authentication process uses **certificates** - the account authentication keys are stored on both the server and the client.

These protocols have better security

IKEv2 (Internet Key Exchange)



IKEv2 (Internet Key Exchange) is rated highly secure among the current protocols. IKEv2 uses IPSec tunning and has a variety of encryption protocol options. IKEv2 is used with AES-256 encryption so it is difficult to be cracked. IKEv2 uses powerful certificate-based authentication and can use the HMAC algorithm to verify the integrity of the transmitted data. IKEv2 supports fast communication and is particularly powerful in maintaining sessions, even when Internet connection is interrupted. Windows, MacOS, iOS and Android all support IKEv2. Some open source implementations are also available.

Version 1 of the protocol was introduced in 1998 and version 2 in 2005. IKEv2 is not one of the latest protocols, but is well maintained.

SSTP (Secure Socket Tunneling Protocol)

SSTP (Secure Socket Tunneling Protocol) is a Microsoft product, mainly supported on Windows. When used with AES and SSL encryption, SSTP provides good security, theoretically. Currently, no SSTP vulnerability has been found but it is possible that a weak point still exists.

A real problem with SSTP is limited support on non-Windows systems.

OpenVPN

OpenVPN is an open protocol suite that provides powerful security features and has become very popular. OpenVPN was first released in 2001 under the GPL license. OpenVPN is open source, so checking for vulnerabilities is guaranteed. OpenVPN encryption functions often use the OpenSSL library. OpenSSL supports multiple encryption algorithms, including AES.

There is no support for OpenVPN at the operating system level, but many packages include their own OpenVPN clients.

Getting the most security with a protocol requires administrators to handle it correctly. The OpenVPN community provides recommendations to enhance the security of OpenVPN.

SoftEther (Ethernet Software)

SoftEther (Software Ethernet) is a new name, first launched in 2014. Like OpenVPN, SoftEther also has open source. SoftEther supports the strongest encryption protocols, including AES-256 and RSA 4096-bit. SoftEther provides greater communication speed than most protocols, including OpenVPN, at a certain data rate. It does not support its own operating system but can be installed on many operating systems, including Windows, Mac, Android, iOS, Linux and Unix.

As a new protocol, SoftEther is not supported as much as some other protocols. SoftEther does not exist long enough as OpenVPN, so users do not have much time to check the weaknesses that may appear on this protocol. However, SoftEther is a strong candidate for anyone who needs top quality security.

So which protocol should I choose?

Question 'Which is the safest protocol?' It is difficult to give an answer. IKEv2, OpenVPN and SoftEther are all strong candidates. OpenVPN and SoftEther have the advantage of being open source. IKEv2 has open source implementations but also has proprietary implementations. IKEv2's main security advantage is its ease of installation, reducing the risk of configuration errors. SoftEther provides very good security, but users do not have much time to experience SoftEther as with the other two protocols, so it is possible that SoftEther still has problems that users have not discovered.

OpenVPN's code has been around for years for security experts to check. OpenVPN is widely used and supports the strongest encryption protocols. Making the final decision also needs to consider other factors, such as convenience and speed, or whether security issues are of greatest interest.

3. Advantages and disadvantages of VPN

The theory is that, when applied to reality, VPN will have advantages and disadvantages like. Please continue to discuss with TipsMake.com.

To build a private network, virtual private network, using a VPN is an inexpensive solution. We can imagine this, the Internet environment is the bridge, the main communication for data transmission, in terms of cost it is perfectly reasonable compared to paying to establish a separate connection line with high price. In addition, the use of software and hardware systems to support account authentication is not cheap. The comparison of the convenience that VPN brings with the cost to you to set up a system as you want, obviously VPN dominates.

But besides, there are obvious disadvantages such as:

VPN does not have the ability to manage**Quality of Service (QoS)**through the Internet environment, so data packets - Data packages are still at risk of being lost or risked.The management capabilities of VPN providers are limited, no one can expect what can happen to their customers, or in short, be hacked.

Refer to the following articles:

1. Theory - What is a proxy?
2. Instructions for setting up individual FTP Server with FileZilla
3. Instructions for setting up individual FTP Server with FileZilla

Hope the above article is useful to you!

You finished reading the article "**VPN theory - What is a virtual private network?**" 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.

© 2019 TipsMake.com