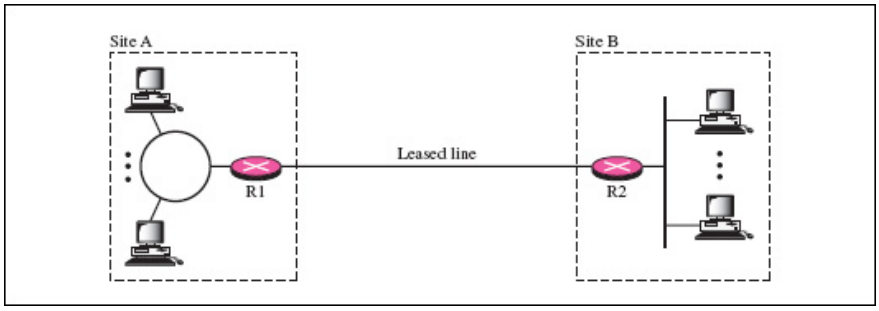
Learn about Virtual Private Network - VPN and Tunneling

When it is necessary to deploy a system to ensure safety, stability and flexibility to meet the requirements of businesses and organizations, one of the most selected and applied options is: Private Network , Hybrid Network and Virtual Private Network.

When it is necessary to deploy a system to ensure safety, stability and flexibility to meet the requirements of businesses and organizations, one of the most selected and applied options is: Private Network , Hybrid Network and Virtual Private Network . In the following article, we will learn about each system, discuss specific Virtual Private Network, VPN tunneling techniques, different VPN modes, how to configure and set up a model. Complete VPN image.

1.Private Network:

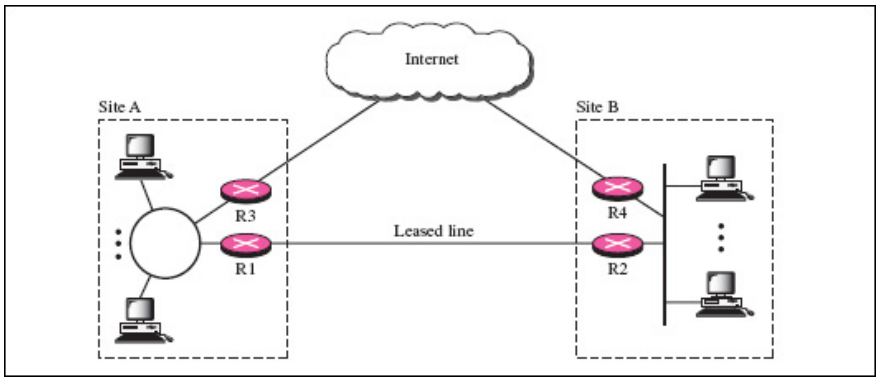
This is a separate type of **LAN** system that uses IP addresses to share data between connected nodes. In this type of model, applications and data ports (used to manage connection protocols) are specifically designed to increase security. **Private Network** is suitable for offices, companies with all computers, network devices in the same place, and if Private Network is deployed in many different locations, the administration department will have to buy more transmission lines. **Dedicate** , to ensure the data transmission process is smooth during operation:



2.Hybrid Network:

This model is a little different from **Private Network** , designed specifically for the company's headquarters, the main office and the ability to access and process data on a large scale. **Hybrid Network** system combines all technical features of **Private** and **Public network** to communicate with the external environment, but still ensures the security of the business. In terms of functionality, **Hybrid** Network will navigate all links, share data via **Private Network,** while the rest of the system, along with data sending, importing or processing information will Go through the **Public Network path.** Like **Private Network** , the process of deploying this system model

requires users to have a fixed line - **Dedicate** to ensure the communication and monitoring process as well as manage the amount of information inside is stable. to:

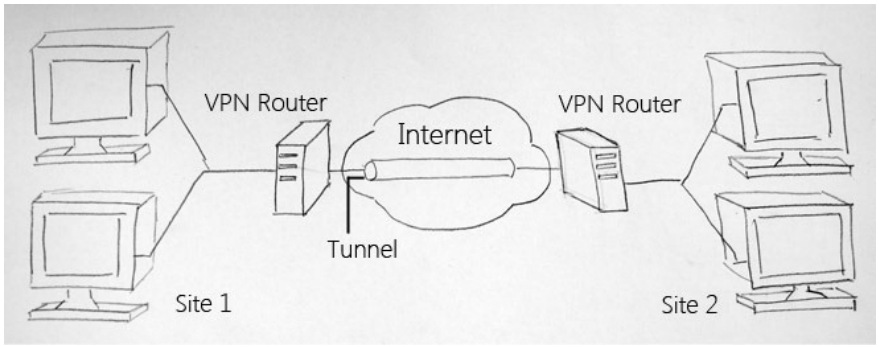


3. Why businesses use VPN:

In terms of technical nature, **Private Network** can ensure the safety of data sent and received, as well as the transmission speed. This simple network system model requires only one fixed line to send and receive the information that has been checked, but after deploying **Private Network** , we must apply **Public Network** to communicate with external environment. And this is also the cause, leading to the development of **Hybrid Network,** with many advantages combined from **Private** and **Public Network** . However, **Hybrid Network** will use 2 fixed lines for separate **Public** and **Private** connections. For example, if an organization has 4 different branches, it will require a secure connection to the network, besides access to the **WAN** system. And to solve this problem, many businesses have chosen and used Virtual Private Network.

4. Virtual Private Network - VPN :

As mentioned above, **Private** and **Hybrid** network systems are quite expensive and have separate lines to connect to **nodes** . **VPN** technology has helped users to cut a lot of initial costs as well as incurred compared to **Public** and **Private Network systems,** while allowing businesses and organizations to use **WAN** communication to connect to the system. public and private respectively. The reason why is called virtual system - because this model does not require physical equipment to secure data transmission. **VPN** technology uses many different information encryption modes to prevent unauthorized intrusion from hackers, malicious programs or common system attack methods, specifically using **VPN** Tunneling techniques to ensure the level of data security, easily compatible with many other technical systems:



Operation mechanism of VPN:

In fact, the way VPN works is quite simple, not much different from the usual server - client models. The server will be primarily responsible for storing and sharing data after encryption, monitoring and providing gateway systems to communicate and confirm client accounts during the connection process, while the VPN client is also compatible. As the client of the LAN system, will send requests - requests to the server to receive information about shared data, initiate connection to other clients in the same VPN system and handle data security process. via application provided.

VPN Tunneling:

This is the most fundamental difference of VPN compared to normal LAN. You can imagine this is a kind of tunnel in the Internet cloud through which requests to send and receive data work.

Tunnel concept has helped us to better understand the operational model of **VPN** network. When users initiate connection or send data via VPN, Tunneling protocol will be used by **VPN** network (eg **PPTP, L2TP, IPSec .**) will 'pack' all this information into 1 package. Other, then encrypt them and proceed to send them through the **tunnel** . At the end of the receiving address, the **tunneling** corresponding operation protocols will decode these packages, then filter the original content, check the origin of the packet as well as the information and data already other classified.

Tunneling Compulsory and Voluntary:

The **Tunneling** classification is based on the origin of the connection. And through that, there are 2 main types: **Compulsory** and **Voluntary Tunneling.**

- **Compulsory Tunneling is** usually initialized by the **Network Access Server** without requesting information from the user. Besides, **VPN clients** are not allowed to access information on **VPN servers** , since they are not responsible for controlling newly created connections. **Compulsory Tunneling** will work immediately between server and VPN client, taking the main function in confirming the legality of client account with VPN server.

- **Voluntary Tunneling** is different, is created, monitored and managed by users. Unlike **Compulsory Tunneling** - usually managed by service providers, this model requires users to directly initiate connection with **ISP** units by running the clien VPN application. We can use many different **VPN** client software to create highly secure tunnels for each private VPN server. When the VPN client program establishes a connection, it will proceed to determine the VPN server or user-specified. **Voluntary Tunneling** does not require too much, except installing additional tunneling protocols on the user's system.

5. Different types and techniques of VPN:

- **PPTP (Point-to-Point Tunneling Protocol) VPN** is the simplest **VPN** technology, using Internet connection provided by ISP to create security tunnel between client and server or client and client. **PPTP** is a **VPN-** based application, you probably know that Windows has built-in PPTP functionality, and all that is needed to connect to the VPN system is just a VPN support software. client. Although PPTP does not have a number of security mechanisms to secure the flow of information and data (**Point to Point Protocol** takes care of this with **PPTP**),

Windows, basically, has carried out validation and encryption with **PPTP** to previously encoded packages. The advantage of this model is that it does not require additional external support hardware to deploy, and the client system can use the software provided to connect to the VPN server. However, the disadvantage of this type of system is based on **Point to Point** protocol to increase the security of data packets, so before these packages start to "pass" the tunnel, they can still compromised from external sources.

- **SSH (Secure Shell) Tunneling** uses secure shell protocols to create separate tunnels to transfer data from one point to another. The biggest advantage of using tunneling on **SSH** is that it is easy to 'bypass' the bypass Internet **firewall** system. Typically, organizations (who need to force employees to use a fixed **proxy server** to access **websites** and private documents) use the **SSH** protocol to navigate the entire traffic from the **dedicate server** . There is a slight difference from **SSL-** based **VPN** , where **HTTPS protocol** starts taking effect on applications, management systems, web browsers . to secure data transmission between devices. Outside to the established VPN network, only two **HTTPS protocols** are required to initiate the connection between the two endpoints.

Developed by IETF, **IPSec** is primarily responsible for securing IP connectivity between the endpoint of the system and **VPN** tunnels. Data packets 'going through' IPSec will be encrypted by **AES, DES or 3DES** . Besides, it also provides additional data compression function and account confirmation for different network layers. **IPsec** VPN technique uses instead of transport **tunnel** mode. Before sending data, the system will proceed to 'pack' the IP package into a new IP package, then assign an additional IP header layer, accompanied by **ESP** - Encapsulated Security Payload header to improve security. In addition to **ESP** , this model also uses **AH** - Authentication Header as a support protocol to apply the security layer to the original information and data.

Microsoft has partnered with **Cisco** and developed an alternative protocol for PPTP, **L2TP** - Layer to Tunneling Protocol to integrate more data. However, it should be noted that **L2TP** , like **PPTP,** does not provide additional information encryption mechanisms based on **PPP** - Point to Point Protocol to encode different data layers. L2TP tunneling will add **L2TP header** data to the original **payload** layer, then move to the last point in the **UDP** diagram. Besides the **Point to Point** protocol, security and account authentication can be done by applying **IPSec** in the network layer.

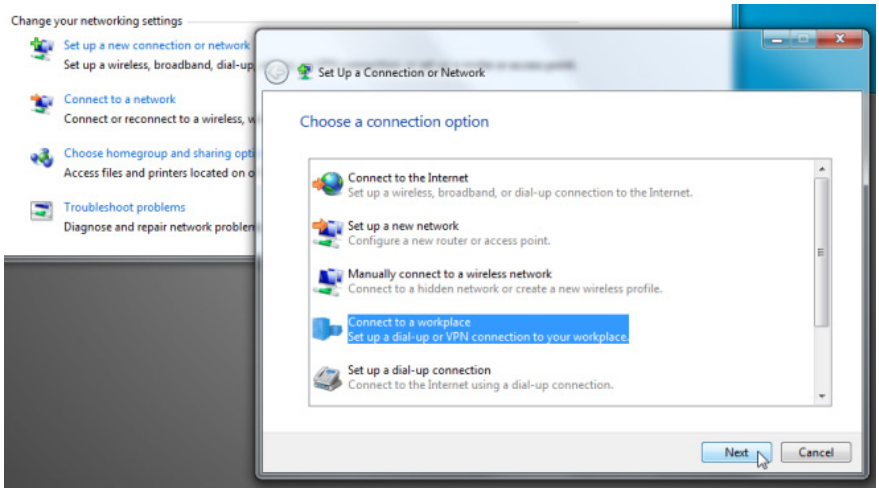
6. Set up and use VPN:

In fact, there are many ways to create and set up **VPN** systems for customers, clients and company branches in different parts of the world, so they can be easily shared. Personal information, providing gateway to communicate with external networks.

Connect to remote VPN network (Office VPN):

Like previous Windows operating systems, Windows 7 already has a basic way to connect to a **VPN** server. If the user intends to connect to the office, **PPTP / L2TP VPN** network, you can use the **VPN** client program to start at the connection.

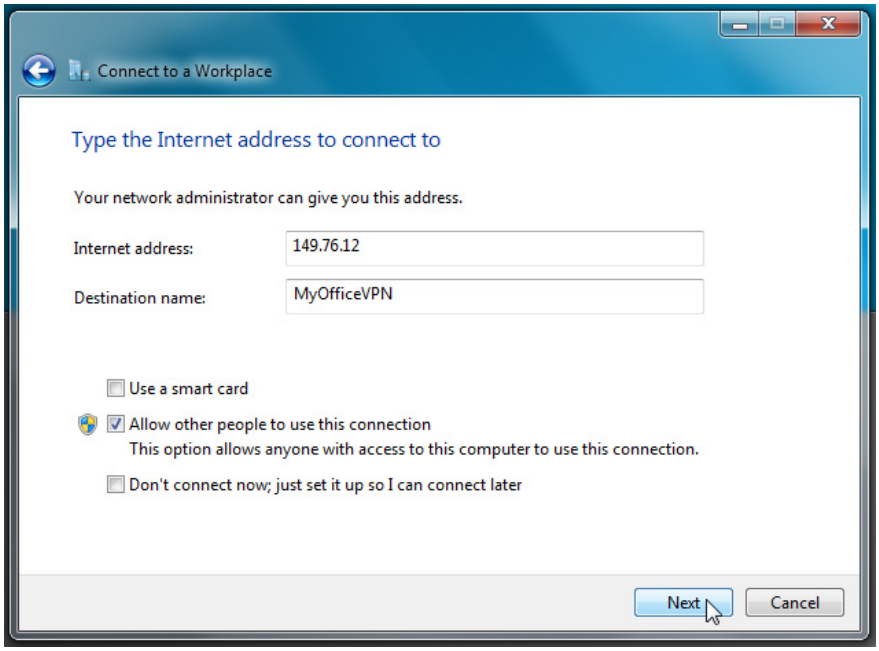
Before starting to proceed, please make sure that you have configured it, set up the device according to the instructions of the system administrator. Next, open the **Network & Sharing Center,** select the **Set up a new connection or network link** , the **Connection Wizard** window will **appear** , and select **Connect to a workplace** and **Next** :



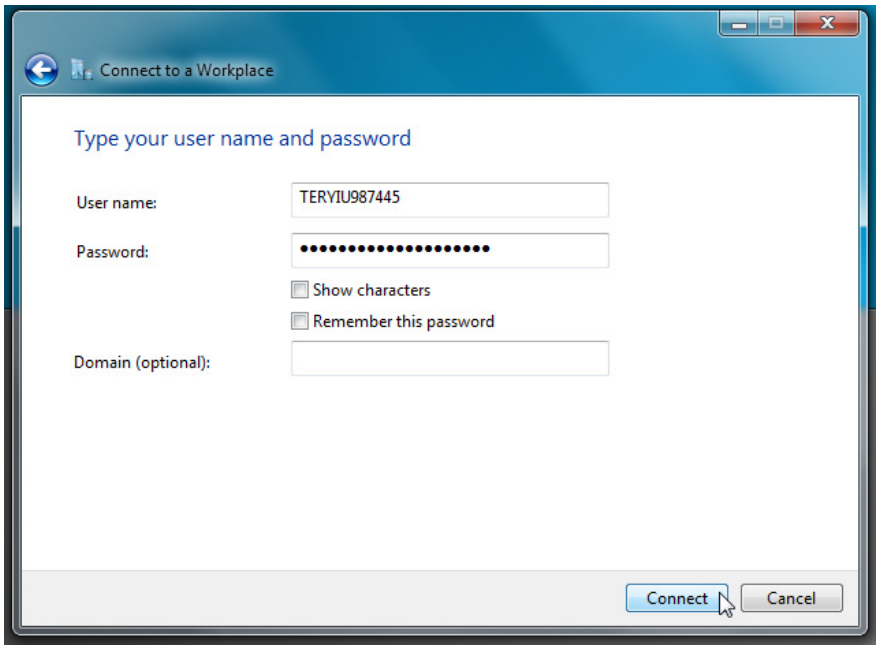
Next, select the connection type to use:

Here we choose Use my Internet connection (VPN)

At the following screen, you need to enter the corresponding information provided by Admin, namely IP address, domain, or via smart card device:



After clicking **Next** is the last step of this setup process, you need to enter the **Username** and **Password** provided by **Admin** :



Then, click **Connect** to begin the process of connecting to the **VPN** . When done, you can check the details of the IP address from the **Network and Sharing Center** or type **ipconfig** command in the **Command Prompt.**

With some of the above technical features, we can see that **Virtual Private Network** is one of the best solutions for securing personal or corporate data when it must be transmitted to many other locations. each other, easily meet the security and security needs of the model. Compared to other paid systems with similar functions, **VPN** technology deserves one of the hardest to beat in creating and managing data processing centers.

You finished reading the article "**Learn about Virtual Private Network - VPN and Tunneling**" 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.