VIRTUAL PRIVATE NETWORK

By:

Himani D.	19030121027
Jui Kahate	19030121044
Priya Gupta	19030121068

Course: Network Security Essentials

What is VPN?

Virtual Private Network (VPN) is used to encrypt your data and add a layer of privacy to protect your identity

Mechanism of employing encryption, authentication and integrity protection: can use a public network (such as the internet) as if it is a private network (such as physical network created and controlled by you)

Combines the advantages of a public network (cheap and easily available) with those of a private network (secure and reliable)

VPN can connect distant networks of an organisation, or it can be used to allow travelling users to remotely access a private network over the internet.

Simulate a private network over a public network, such as the Internet.

When we use a VPN, it is like our connection is routed to the internet via a secure tunnel to a server in another location; sometimes in a different city, sometimes in a different country.

Types of VPN

Remote Access

Enables users who are working remotely to securely access and use applications and data that reside in the corporate data center and headquarters, encrypting all traffic the users send and receive.

Creating a tunnel between an organization's network and a remote user that is "virtually private," even though the user may be in a public location.

Site-to-Site Access

Network to network connection: encrypted link.

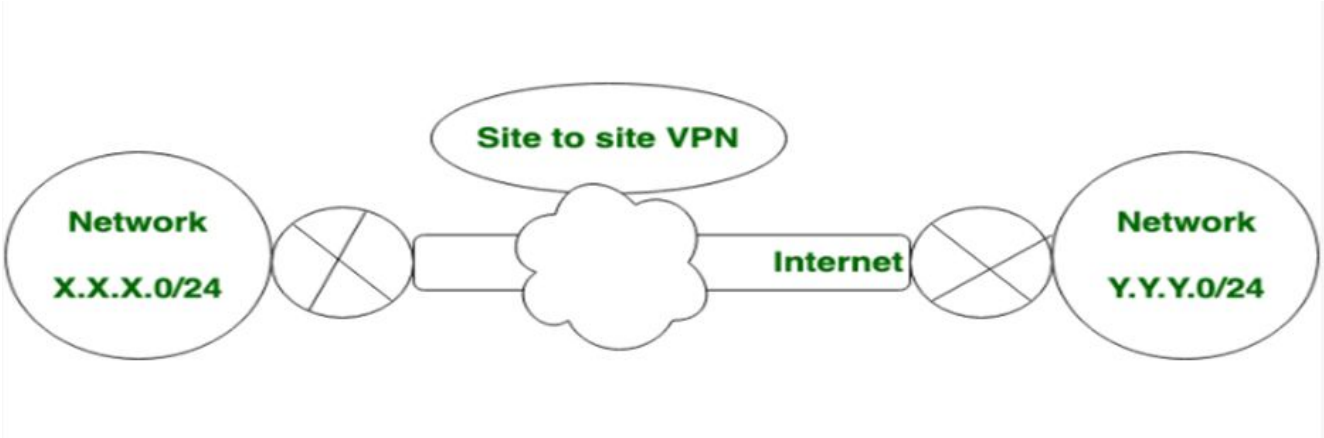
Commonly used in the large companies to connect with the network of the branch offices in different locations

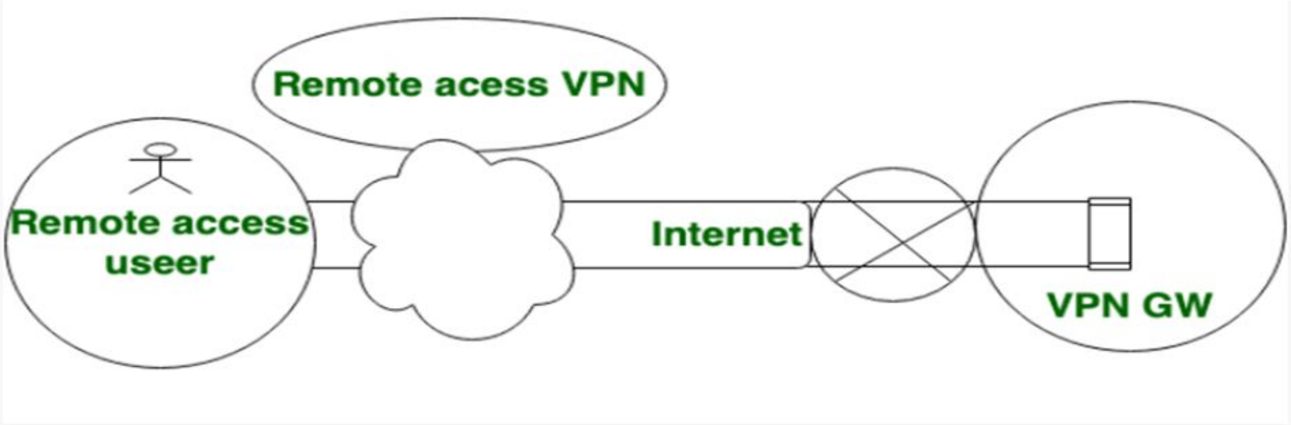
Create an imaginary bridge between the networks different locations.

Encrypts traffic at one end and sends it to the other site over the Internet where it is decrypted and routed on to its destination.

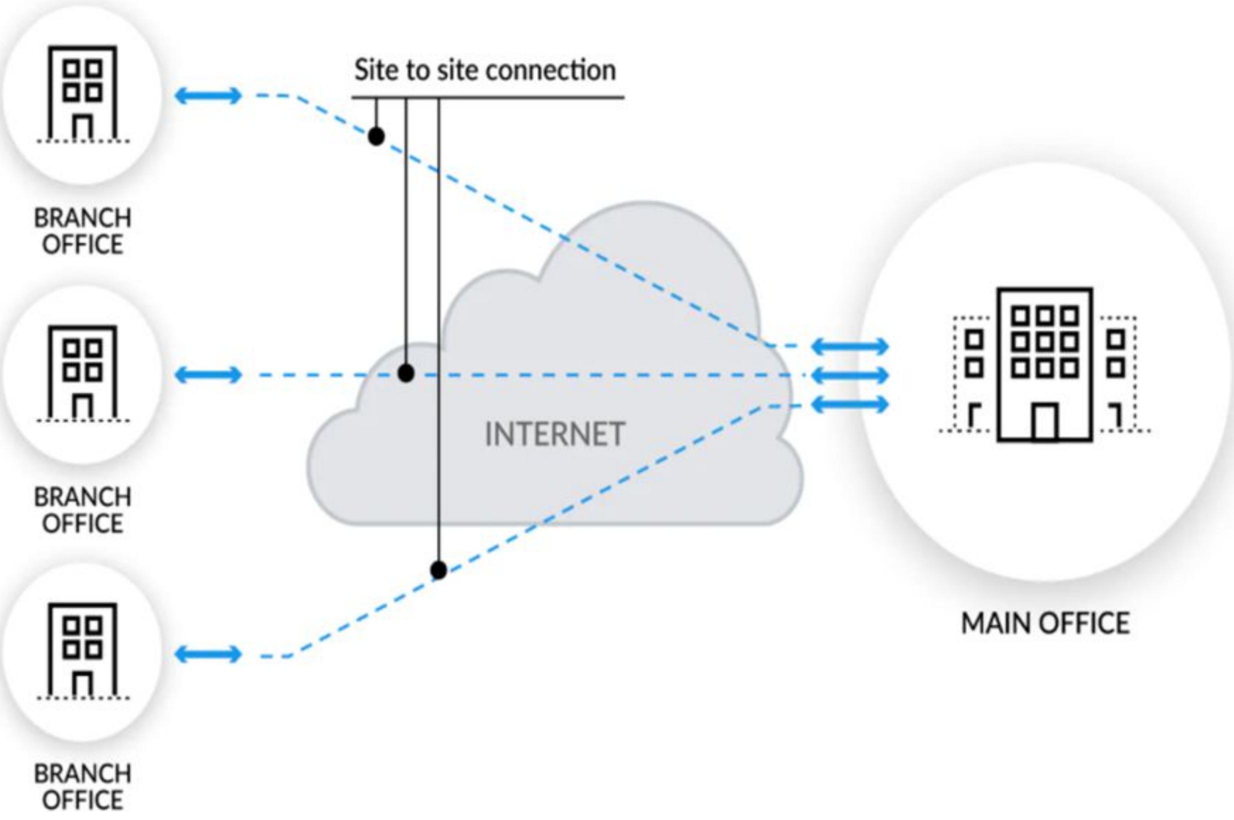
Intranet: Several offices of the same company are connected using Site-to-Site VPN.

Extranet: connect to the office of another company, it is called as Extranet based VPN.


Site to site VPN
Network
X.X.X.0/24
Internet
Network
Y.Y.Y.0/24


Remote acess VPN
Remote access
useer
Internet
VPN GW

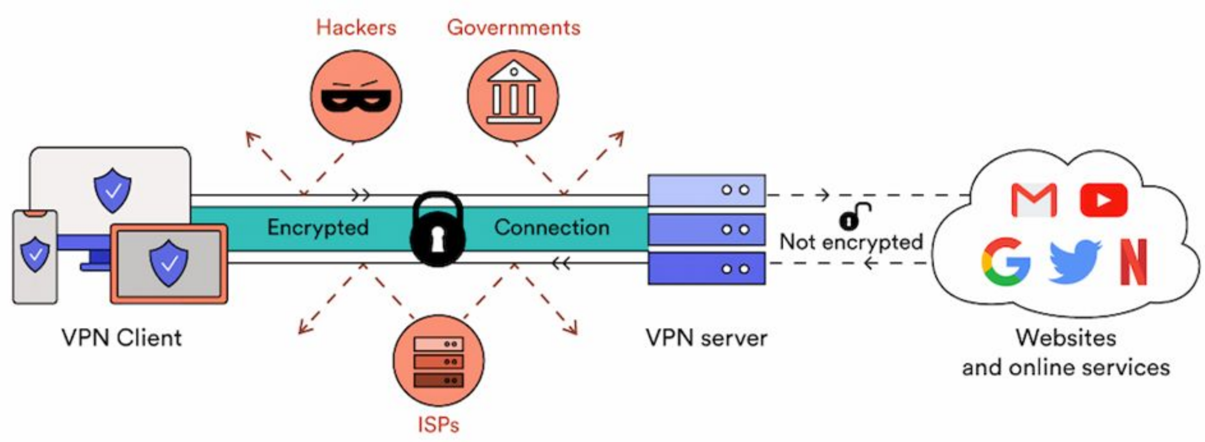
Site to Site VPN



VPN Protocols

1. **PPTP (Point to point tunnelling protocol)**
    a. Mainly supports the VPN connectivity between a single user and a LAN, rather than between 2 LANs generates a tunnel and confines the data packet. Point-to-Point Protocol (PPP) is used to encrypt the data between the connection.
2. **L2TP (Layer 2 tunnelling protocol) / IPSec (Internet Protocol Security)**
    a. Is an improvement over PPTP.
    b. L2TP is a tunneling protocol that is often combined with another VPN security protocol like IPSec to establish a highly secure VPN connection
3. **SSL (Secure Sockets Layer) and TLS (Transport Layer Security)**
4. **OpenVPN**

How does VPN work?



VPN Tunnel helps in data encapsulation. It protects your data from hackers, governments and ISPs.

It ensures the end-to-end encryption to provide high security to internet connection.

Effectiveness of tunnels depends upon type of tunneling protocol used by the VPN provider.

VPN creates a secure tunnel between your device and VPN server.

The request is encrypted using encryption ciphers to hide browsing activity details from other individuals and is sent to the VPN server through the tunnel.

When the request reaches the server, it is decrypted and passed over the Internet.

All the websites and services your accessing, will get VPN server's IP. Your actual IP and location will be remain hidden.

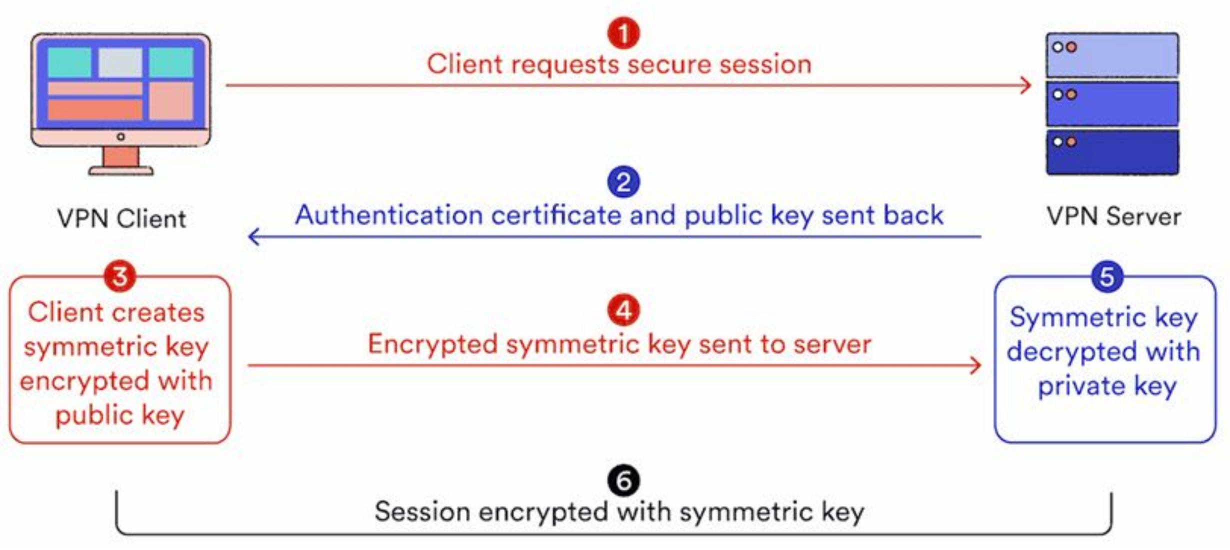
You can unblock restricted content as per country laws which you have connected through VPN server.

VPN Handshakes

VPN Handshake is initial connection between your device and VPN server.

This connection helps to share encryption key between client & server. This key is used to encrypt and decrypt data at any side of tunnel during the entire browsing session.

Client creates and publishes the symmetric key encrypted with public key and sent encrypted symmetric key to server, here the symmetric key is decrypted with private key and the session is established between client-server which is encrypted with symmetric key.



VPN Client
1
Client requests secure session
VPN Server
2
Authentication certificate and public key sent back
3
Client creates symmetric key encrypted with public key
4
Encrypted symmetric key sent to server
5
Symmetric key decrypted with private key
6
Session encrypted with symmetric key

Mostly RSA algorithm is used for encryption purpose. Security depends on length of key so RSA-2048 and higher are considered to be secure but it may result in slower connection.

Security Issues

Logging Policies – Most of the VPNs claims to have zero-log policies. But some of provider keeps connection and usage logs. Usage logs track activities you do while using VPN.

Data Leaks – When VPN provider didn't configure their connections well there are chances of data leaks through tunnel such as IP address, network traffic. It can also happen because of browser related issues.

Collection and sale of personal data – Some free VPN services collects your personal data sell these to third-party organization whoever pays a good price.

Privacy Policies – We should read privacy policies to understand what they log and weather they share your data with third parties or advertisers.

Malware Infections – While install VPN client or pirated software malware is injected into your device and if you grant permission to access your data it may collect personal data, record your calls, steal your important credentials, as well.

Use of Protocols – There are protocols such as PPTP they are fast but can be compromised easily instead more stronger and safer protocols should be used.

Poorly-Configured Encryption – If providers have implemented weak encryption techniques then other individuals may decrypt your connection and manage to take control over your web traffic.

Advantages

1. **It hides online identity.**
    a. VPN hides the IP address of the computer and also encrypt the tunnel between the client and the server.
2. **It help the clients to bypass geo-blocks.**
    a. Geo-blocks are the issues that are generated when websites are restricted in a particular area. However, with help of VPN services, the client can access those websites irrespective of the area.
3. **It is a secure service for online connections.**
    a. Since the IP address of the system is hidden so a VPN can prevent web browsers and others to access connection .Therefore, the information that clients receives or sends is anonymous and secure.
4. **It prevents data throttling**
    a. Data throttling occurs when your internet service provider has restrained your service . Using VPN service it can be prevented.

Disadvantages

1. **Slow internet connection.**
    a. VPN usually reroutes and encrypts the internet connection which results in slightly low internet speed.
2. **Specific blockades of VPN services**
    a. Some government discourage the use of a VPN as it is improper for the citizens.
3. **Unaware of the encryption strength provided by the VPN.**
    a. Sometimes, the clients does not receive what they are promised by the service provider.
4. **Free VPNs**
    a. Free VPNs maybe does not provide the same security and privacy strength as the paid ones.

Examples

Client- based VPN

1. **Cisco’s AnyConnect:**
   a. It is a unified security endpoint agent that delivers multiple security services such as remote access, web security features and roaming protection to protect the enterprise.
   b. It provides the visibility and the control to identify who and which devices are accessing the extended enterprise.
2. **Pulse (formerly Juniper)**
   a. Junos Pulse is a program that allows off-campus users to access the libraries' online resources.
3. **Windows , MAC and mobile operating system have built-in VPN services.**

Use Cases

1. **Access Online Bank Account from oversea:**
   a. Some banks restrict using bank account in other countries.Therefore using VPN services and connecting to a VPN server will be helpful..
2. **AnyDesk:**
   a. VPN via AnyDesk provides a private network between two clients.Access is limited to remote device.
3. **Block Malware.**