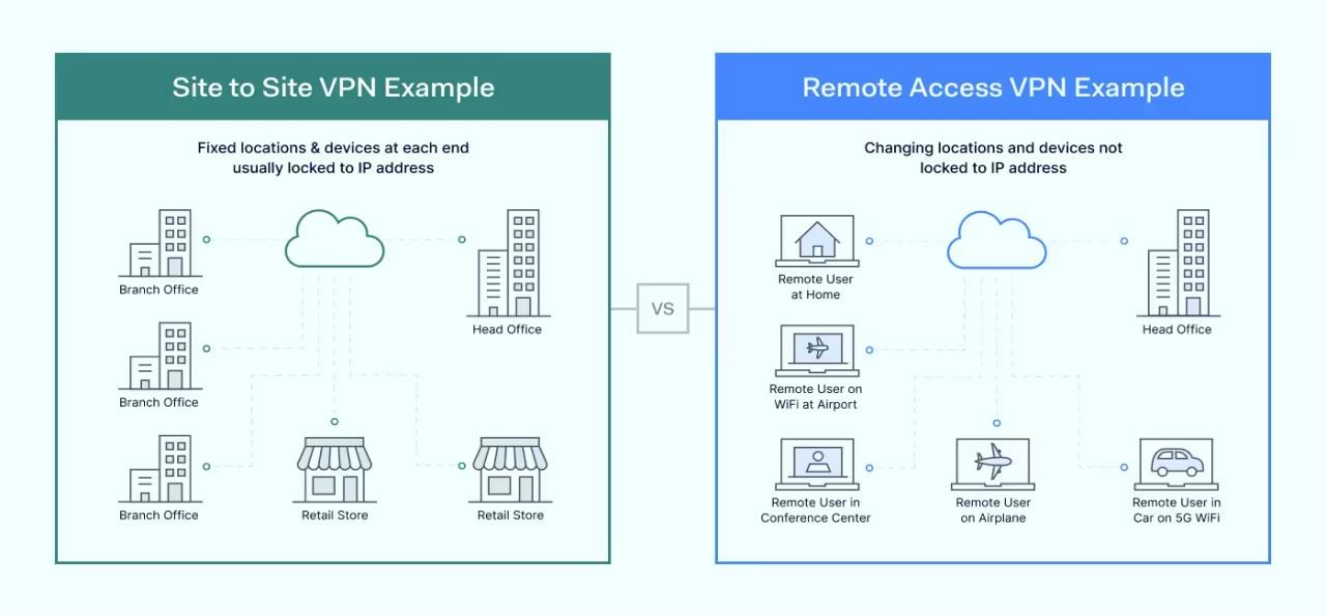
Types of Virtual Private Network (VPN) and its Protocols

VPN stands for Virtual Private Network (VPN), that allows a user to connect to a private network over the Internet securely and privately. VPN creates an encrypted connection that is called VPN tunnel, and all Internet traffic and communication is passed through this secure tunnel.

Virtual Private Network (VPN) is basically of 2 types:

1. Remote Access VPN

Remote Access VPN permits a user to connect to a private network and access all its services and resources remotely. The connection between the user and the private network occurs through the Internet and the connection is secure and private. Remote Access VPN is useful for home users and business users both. An employee of a company, while he/she is out of station, uses a VPN to connect to his/her company's private network and remotely access files and resources on the private network. Private users or home users of VPN, primarily use VPN services to bypass regional restrictions on the Internet and access blocked websites. Users aware of Internet security also use VPN services to enhance their Internet security and privacy.



2. Site to Site VPN

A Site-to-Site VPN is also called as Router-to-Router VPN and is commonly used in the large companies. Companies or organizations, with branch offices in different locations, use Site-to-site VPN to connect the network of one office location to the network at another office location.

- **Intranet based VPN:** When several offices of the same company are connected using Site-to-Site VPN type, it is called as Intranet based VPN.
- **Extranet based VPN:** When companies use Site-to-site VPN type to connect to the office of another company, it is called as Extranet based VPN.

- Remote access VPN connects individual users to a remote network, while site-to-site VPN connects two entire networks together.

3. Cloud VPN

A Cloud VPN is a virtual private network that allows users to securely connect to a cloud-based infrastructure or service. It uses the internet as the primary transport medium to connect the remote users to the cloud-based resources. Cloud VPNs are typically offered as a service by cloud providers such as Amazon Web Services (AWS) and Microsoft Azure. It uses the same encryption and security protocols as traditional VPNs, such as IPsec or SSL, to ensure that the data transmitted over the VPN is secure. Cloud VPNs are often used by organizations to securely connect their on-premises resources to cloud-based resources, such as cloud-based storage or software-as-a-service (SaaS) applications.

4. Mobile VPN

Mobile VPN is a virtual private network that allows mobile users to securely connect to a private network, typically through a cellular network. It creates a secure and encrypted connection between the mobile device and the VPN server, protecting the data transmitted over the connection. Mobile VPNs can be used to access corporate resources, such as email or internal websites, while the user is away from the office. They can also be used to securely access public Wi-Fi networks, protecting the user's personal information from being intercepted. Mobile VPNs are available as standalone apps or can be integrated into mobile device management (MDM) solutions. These solutions are commonly used by organisations to secure their mobile workforce.

5. SSL VPN

SSL VPN (Secure Sockets Layer Virtual Private Network) is a type of VPN that uses the SSL protocol to secure the connection between the user and the VPN server. It allows remote users to securely access a private network by establishing an encrypted tunnel between the user's device and the VPN server. SSL VPNs are typically accessed through a web browser, rather than through a standalone client. This makes them easier to use and deploy, as they don't require additional software to be installed on the user's device. It can be used to access internal resources such as email, file servers, or databases. SSL VPNs are considered more secure than traditional IPsec VPNs

because they use the same encryption protocols as HTTPS, the secure version of HTTP used for online transactions.

6. PPTP (Point-to-Point Tunneling Protocol) VPN

PPTP (Point-to-Point Tunneling Protocol) is a type of VPN that uses a simple and fast method for implementing VPNs. It creates a secure connection between two computers by encapsulating the data packets being sent between them. PPTP is relatively easy to set up and doesn't require any additional software to be installed on the client's device. It can be used to access internal resources such as email, file servers, or databases. PPTP is one of the oldest VPN protocols and is supported on a wide range of operating systems. However, it is considered less secure than other VPN protocols such as L2TP or OpenVPN, as it uses a weaker encryption algorithm and has been known to have security vulnerabilities.

7. L2TP (Layer 2 Tunneling Protocol) VPN

L2TP (Layer 2 Tunneling Protocol) is a type of VPN that creates a secure connection by encapsulating data packets being sent between two computers. L2TP is an extension of PPTP, it adds more security to the VPN connection by using a combination of PPTP and L2F (Layer 2 Forwarding Protocol) and it uses stronger encryption algorithm than PPTP. L2TP is relatively easy to set up and doesn't require additional software to be installed on the client's device. It can be used to access internal resources such as email, file servers, or databases. It is supported on a wide range of operating systems, but it is considered less secure than other VPN protocols such as OpenVPN, as it still has some vulnerabilities that can be exploited.

8. OpenVPN

OpenVPN is an open-source software application that uses SSL and is highly configurable and secure. It creates a secure and encrypted connection between two computers by encapsulating the data packets being sent between them. OpenVPN can be used to access internal resources such as email, file servers, or databases. It is supported on a wide range of operating systems and devices, and can be easily configured to work with various network configurations and security settings. It is considered one of the most secure VPN protocols as it uses the industry standard SSL/TLS encryption protocols and it offers advanced features such as two-factor authentication and kill switch.

Types of Virtual Private Network (VPN) Protocols:

1. **Internet Protocol Security (IPSec):** Internet Protocol Security, known as IPSec, is used to secure Internet communication across an IP network. IPSec secures Internet Protocol communication by verifying the session and encrypts each data packet during the connection. IPSec runs in 2 modes:
    - (i) Transport mode
    - (ii) Tunneling mode
2. **Layer 2 Tunneling Protocol (L2TP):** L2TP or Layer 2 Tunneling Protocol is a tunneling protocol that is often combined with another VPN security protocol like IPSec to establish a highly secure VPN connection. L2TP generates a tunnel between two L2TP connection points and IPSec protocol encrypts the data and maintains secure communication between the tunnel.
3. **Point–to–Point Tunneling Protocol (PPTP):** PPTP or Point-to-Point Tunneling Protocol generates a tunnel and confines the data packet. Point-to-Point Protocol (PPP) is used to encrypt the data between the connection. PPTP is one of the most widely used VPN protocol and has been in use since the early release of Windows. PPTP is also used on Mac and Linux apart from Windows.
4. **SSL and TLS:** SSL (Secure Sockets Layer) and TLS (Transport Layer Security) generate a VPN connection where the web browser acts as the client and user access is prohibited to specific applications instead of entire network. Online shopping websites commonly uses SSL and TLS protocol. It is easy to switch to SSL by web browsers and with almost no action required from the user as web browsers come integrated with SSL and TLS. SSL connections have "https" in the initial of the URL instead of "http".
5. **Secure Shell (SSH):** Secure Shell or SSH generates the VPN tunnel through which the data transfer occurs and also ensures that the tunnel is encrypted. SSH connections are generated by a SSH client and data is transferred from a local port on to the remote server through the encrypted tunnel.
6. **SSTP (Secure Socket Tunneling Protocol):** A VPN protocol developed by Microsoft that uses SSL to secure the connection, but only available for Windows.
7. **IKEv2 (Internet Key Exchange version 2):** A VPN protocol that provides fast and secure connections, but not widely supported by VPN providers.
8. **OpenVPN:** An open-source VPN protocol that is highly configurable and secure, widely supported by VPN providers and considered one of the most secure VPN protocols.