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.
3. **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.

Basically, Site–to–site VPN create a imaginary bridge between the networks at geographically distant offices and connect them through the Internet and sustain a secure and private communication between the networks. In Site–to–site VPN one router acts as a VPN Client and another router as a VPN Server as it is based on Router–to–Router communication. When the

authentication is validated between the two routers only then the communication starts.

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:

2.
- (i) Transport mode
- (ii) Tunneling mode

The work of transport mode is to encrypt the message in the data packet and the tunneling mode encrypts the whole data packet. IPSec can also be used with other security protocols to improve the security system.

3. **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.

4. **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.

5. **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”.

6. **OpenVPN:**
   OpenVPN is an open source VPN that is commonly used for creating

Point–to–Point and Site–to–Site connections. It uses a traditional security protocol based on SSL and TLS protocol.

7.**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.