VPN

Types of VPN	**1. Remote Access VPN** Remote access VPN allows a user to connect to a private network and access its services and resources remotely. The connection between the user and the private network happens through the Internet and the connection is secure and private. **2. Site - to - Site VPN** A site-to-site VPN allows offices in multiple locations to establish secure connections with each other over a public network such as the Internet. Site-to-site VPN is different from remote-access VPN as it eliminates the need for each computer to run VPN client software as if it were on a remote-access VPN.
Types of VPN protocols	**1. IPSec** Internet Protocol Security or IPSec is used to secure Internet communication across an IP network. IPSec secures Internet Protocol communication by authenticating the session and encrypts each data packet during the connection. **IPSec operates in two modes**, Transport mode and Tunneling mode, to protect data transfer between two different networks. The transport mode encrypts the message in the data packet and the tunneling mode encrypts the entire data packet. IPSec can also be used with other security protocols to enhance the security system. **2. L2TP** L2TP or Layer 2 Tunneling Protocol is a tunneling protocol that is usually combined with another VPN security protocol like IPSec to create a highly secure VPN connection. L2TP creates a tunnel between two L2TP connection points and IPSec protocol encrypts the data and handles secure communication between the tunnel. L2TP is a VPN protocol that doesn't offer any encryption or protection from the traffic that passes through the connection. For this reason, it's usually paired with IPSec, which is an encryption protocol. **3. PPTP** PPTP or Point-to-Point Tunneling Protocol creates a tunnel and encapsulates the data packet. It uses a Point-to-Point Protocol (PPP) to encrypt the data between the connection. **4. Secure Sockets Layer (SSL) and Transport Layer Security (TLS)** SSL (Secure Sockets Layer) and TLS (Transport Layer Security) create a VPN connection where the web browser acts as the client and user access is restricted to specific applications instead of entire network. **5. OpenVPN** OpenVPN is an open source VPN that is useful for creating Point-to-Point and Site-to-Site connections. It uses a custom security protocol based on SSL and TLS protocol. **6. Secure Shell (SSH)** Secure Shell or SSH creates the VPN tunnel through which the data transfer happens and also ensures that the tunnel is encrypted. SSH connections are created by a SSH client and data is transferred from a local port on to the remote server through the encrypted tunnel.

	7. IKEv2/IPSec IKEv2 is based upon IPSec. IKEv2/IPSec is a solid fast and secure VPN protocol.
VPN and describe IPsec VPN	Virtual Private Network (VPN) creates a secure network connection over a public network such as the internet. IPsec VPN means VPN over IP Security allows two or more users to communicate in a secure manner by authenticating and encrypting each IP packet of a communication session.
SSL VPN? How it is different from IPsec VPN?	SSL VPN provides remote access connectivity from almost any internet enabled location without any special client software at a remote site. You only need a standard web browser and its native SSL encryption. IPsec is a dedicated point-to-point fixed VPN connection where SSL VPNs provides anywhere connectivity without any configuration or special software at remote site.
VPN vs Proxy Server	Virtual Private Network (VPN) creates a secure network connection over a public network such as the internet. A proxy is a server that sits in between your computer and the internet. It will hide your IP address, so the website you're accessing will see the IP address of the proxy server, and not your real IP address. This makes it seem as if your online activities are originating somewhere else.