VPN

A virtual private network (VPN) allows a company to securely extend its private intranet over the existing framework of a public network, such as the Internet. With VPN, a company can control network traffic while providing important security features such as authentication and data privacy.

VPN runs on the network layer of the TCP/IP layered communications stack model. Specifically, VPN uses the IP Security Architecture (IPSec) open framework. IPSec provides base security functions for the Internet, as well as furnishes flexible building blocks from which you can create robust, secure virtual private networks.

VPN also supports Layer 2 Tunnel Protocol (L2TP) VPN solutions. L2TP connections, which are also called virtual lines, provide cost-effective access for remote users by allowing a corporate network server to manage the IP addresses assigned to its remote users. Further, L2TP connections provide secure access to your system or network when you protect them with IPSec.

Types Of VPN:

1. Remote access
   A remote access VPN securely connects a device outside the corporate office. These devices are known as endpoints and may be laptops, tablets, or smartphones. Advances in VPN technology have allowed security checks to be conducted on endpoints to make sure they meet a certain posture before connecting. Think of remote access as computer to network.

2. Site-to-site
   A site-to-site VPN connects the corporate office to branch offices over the Internet. Site-to-site VPNs are used when distance makes it impractical to have direct network connections between these offices. Dedicated equipment is used to establish and maintain a connection. Think of site-to-site access as network to network.