A virtual private network (VPN) is a technology that creates an encrypted connection over a less secure network. The benefit of using a secure VPN is it ensures the appropriate level of security to the connected systems when the underlying network infrastructure alone cannot provide it. The justification for using VPN access instead of a private network usually boils down to cost and feasibility: It is either not feasible to have a private network -- e.g., for a traveling sales rep -- or it is too costly to do so. The most common types of VPNs are remote-access VPNs and site-to-site VPNs.

A remote-access VPN uses a public telecommunication infrastructure like the internet to provide remote users secure access to their organization's network. This is especially important when employees are using a public Wi-Fi hotspot or other avenues to use the internet and connect into their corporate network. A VPN client on the remote user's computer or mobile device connects to a VPN gateway on the organization's network. The gateway typically requires the device to authenticate its identity. Then, it creates a network link back to the device that allows it to reach internal network resources -- e.g., file servers, printers and intranets -- as though it was on that network locally.

A remote-access VPN usually relies on either IPsec or Secure Sockets Layer (SSL) to secure the connection, although SSL VPNs are often focused on supplying secure access to a single application, rather than to the entire internal network. Some VPNs provide Layer 2 access to the target network; these require a tunneling protocol like PPTP or L2TP running across the base IPsec connection.

A site-to-site VPN uses a gateway device to connect the entire network in one location to the network in another -- usually a small branch connecting to a data center. End-node devices in the remote location do not need VPN clients because the gateway handles the connection. Most site-to-site VPNs connecting over the internet use IPsec. It is also common to use carrier MPLS clouds, rather than the public internet, as the transport for site-to-site VPNs. Here, too, it is possible to have either Layer 3 connectivity (MPLS IP VPN) or

Layer 2 (Virtual Private LAN Service, or VPLS) running across the base transport.

VPNs can also be defined between specific computers, typically servers in separate data centers, when security requirements for their exchanges exceed what the enterprise network can deliver. Increasingly, enterprises also use VPN connections in either remote-access mode or site-to-site mode to connect -- or connect to -- resources in a public infrastructure-as-a-service environment. Newer hybrid-access scenarios put the VPN gateway itself in the cloud, with a secure link from the cloud service provider into the internal network.

Parsing VPN gateways.