A **virtual private network** (**VPN**) is a private communications network often used within a company, or by several companies or organizations, to communicate confidentially over a publicly accessible network. VPN message traffic can be carried over a public networking infrastructure (e.g. the Internet) on top of standard protocols, or over a service provider's private network with a defined Service Level Agreement (SLA) between the VPN customer and the VPN service provider.

Secure VPN (SVPN) use cryptographic tunneling protocols to provide the necessary confidentiality (preventing snooping), sender authentication (preventing identity spoofing), and message integrity (preventing message alteration) to achieve the privacy intended. When properly chosen, **implemented, and used**, such techniques can provide secure communications over unsecured networks.

Secure VPN protocols include the following:

- IPsec (IP security) - commonly used over IPv4, and an obligatory part of IPv6.
- SSL used either for tunneling the entire network stack, such as in OpenVPN, or for securing what is essentially a web proxy. Although the latter is often called a "SSL VPN" by VPN vendors, it is not really a fully-fledged VPN. (See also TUN/TAP.)
- PPTP (point-to-point tunneling protocol), developed jointly by a number of companies, including Microsoft.
- L2TP (Layer 2 Tunnelling Protocol), including work by both Microsoft and Cisco.
- L2TPv3 (Layer 2 Tunnelling Protocol version 3).

source - {Virtual private network}. (2006, September 1). In *Wikipedia, The Free Encyclopedia*. Retrieved September 2, 2006, from http://en.wikipedia.org/wiki/Vpn

Hautspot encourages the use of VPN technologies to encrypt and secure the transmission of sensitive data between a hotspot or hotzone and the corporate enterprise. Hautspot allows the pass-through of major VPN strategies.

Back