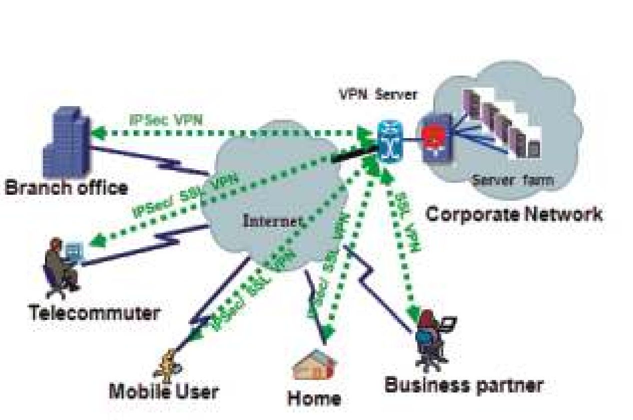
SSL VPN: A Technology Overview

In the world of distributed computing, corporate applications are hosted in data centers located in multiple locations and are accessed by many users from various locations. To provide secure access to such network resources, technocrats have designed Secure Socket Layer Virtual Private Network (SSL VPN), a remote access technology to connect private networks over Internet - with strong encryption features, multiple authentication and connectivity options for mass deployments.

Arpita Burman
Principal Systems Analyst
arpita.burman@nic.in

A virtual private network (VPN) has been traditionally used to connect branch offices to the corporate office over Internet as an alternative to expensive WAN connections. Now it is also being used by individual users to access sensitive data, to increase mobility and online transactions. VPN creates a virtual "tunnel" connecting two endpoints by encrypting end to end communication and protecting the data from unauthorized access or interception. There are many VPN technologies such as IPSec, PPTP, L2TP and MPLS which are deployed to meet this requirement. IPSec and L2TP VPN are used for connecting Remote/ branch offices to corporate network over Internet and provide consistent network access similar to LAN. Telecommuters and mobile users, who require seamless access to corporate network for regular work, usually use IPSec VPN or Client based SSL VPN. Clientless SSL VPN connection is provided to business partners, suppliers, public dealing executives, who require partial access to internal applications involving financial transactions, customer details etc from multiple locations such as reservation counters, KIOSKS, Cyber Café, Public Utility centres.

IP Security (IPSec) VPN is very popular VPN technology which is being used for both Site to Site and Remote Access. IPSec VPN can encrypt any IP traffic including Video with multiple encryption algorithms and authentication options. Though IPSec VPN is an accepted industry standard for remote access, there are some interoperability issues which make it difficult for mass deployment. IPSec VPN binds the user to a particular machine/laptop where the VPN client S/W is installed. Secondly VPN clients of one vendor usually conflicts with other vendors. Also VPN clients behind Proxy servers face difficulty in establishing IPSec VPN connection as some Proxy Servers do not support IPSec or block the ports required for IPSec communication.



Virtual Private Network Architecture

Secure Socket Layer (SSL) VPN is an emerging VPN technology which allows users to connect to the enterprise network from anywhere anytime over Internet using any standard web browser. It supports access to all applications like Http, HTTPS, FTP, SSH, RDP over secure SSL tunnel. SSL VPN does not require any client software to be installed thus allowing VPN connection even from less trusted network as Cyber café and KIOSKS.

This article intends to give general overview of SSL VPN Technology, architecture, functions and features.

SSL protocol

SSL protocol was designed by Netscape Corporation to protect only traffic generated by Web browser. This protocol aims to encrypt entire communication between client's browser and Web server. SSL VPN uses this concept to create a secure tunnel using SSL protocol between the client and SSL Server and then relays the web traffic to the actual servers.

SSL functions in between the Application Layer and Transport layer using TCP port 443. SSL receives data from application layer, authenticate, signs and encrypts before sending to the transport layer.

Any SSL session has two main phases.

- **SSL Session Negotiation:** It starts when the SSL client initiates a https connection to the SSL server. The SSL Server responds by presenting its SSL certificate issued by a trusted Certificate Authority. The User accepts the Certificate and presents its own Digital certificate if demanded by the server. Then the server and client exchange their security parameters (Cipher suite) to negotiate on a master key. This master key is used to generate session keys which are used for data encryption. SSL supports multiple encryption algorithms and are deployed as per the organizations' security policies. It uses asymmetric cryptographic algorithms to secure the exchange of the session keys.
- **SSL connection:** Once the negotiation phase is completed, the session key generated from the master key is used to encrypt, Hash the data and transport the data. It uses symmetric cryptography for data encryption / decryption.

Periodically the session keys are exchanged between the client and server using the pre negotiated master key. The security parameters negotiated in a SSL session and are effective until the session is terminated. Whereas for any new connection, new session key is used for data encryption between the client and server.

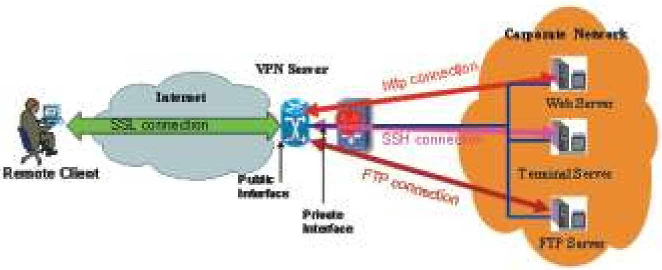
SSL VPN Architecture

Components of SSL VPN include SSL VPN Server / Gateway, VPN users, AAA servers and Network resources as application servers.

SSLVPN Server / Gateway

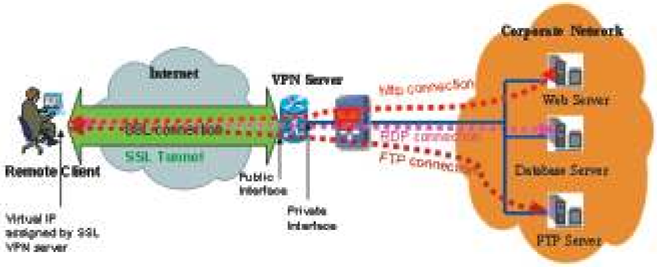
SSL VPN servers are usually hardware appliances like Firewall which have a Public Interface and multiple private interfaces. The SSL VPN client connects to the SSL VPN server's public interface using https protocol through any standard Web Browser such as Internet Explorer, Mozilla FireFox etc that supports SSL Version 3 and above. All internal application servers are connected to the private interfaces of the SSL appliance. Primarily there are two ways in which SSL VPN can be designed:

- **Web VPN (Clientless SSL) :** In this type of SSL VPN , users connect to SSLVPN server and after the SSL session is established, the server redirects the connection to a Web Portal which has multiple links to other internal Web Servers, FTP server, Terminal servers etc. All user requests are received by this portal and relayed to the respective internal servers and vice versa. A single SSL connection is established between client and SSL Server and connection to application is established between the SSL VPN Server and corresponding application server. However it doesn't support all applications which require client side scripting.



WebVPN (Clientless SSL VPN)

- **Client based SSL:** It allows users to connect non Web applications like Remote Desktop , Outlook Express, SSH Client, Database Server etc. After the SSL VPN connection is established, SSL client agent is automatically loaded and activated as plug-ins into the user's machine. The SSL client is assigned a Virtual IP address from the SSL VPN Server. SSL Client agent uses proprietary mechanism to encapsulate all non Web traffic of the client and transports through the SSL tunnel. Though some functionalities of IPSEC VPN are fulfilled in Client based SSL VPN, still it cannot support some VoIP/ Video Conferencing applications.



Client based SSL VPN

Additional features of SSL VPN

- **Authentication of SSL Client:** In general SSL connection does not require client authentication. However for implementing SSL VPN, authentication is essential to identify the users and enforcing group policies. SSL VPN supports flexible client authentication methods such as X.509 digital certificates, smart cards, username and password and two-factor authentication (e-Tokens). SSL VPN also supports authentication from external servers such as RADIUS, Active Directory, and Lightweight Directory Access Protocol (LDAP). This is required to integrate with existing authentication databases for centralized management, accounting and billing.

- **Application Translation:** The latest version of SSL VPN also performs as application translation which can convert information of non Web-enabled applications. This allows users to use a Web browser to access applications that do not have their own Web interfaces or require client software. For example, SSL Web VPN can be configured to upload files from FTP Servers without using FTP or SSH client at user end. The SSL VPN server translates this application into Web-based format and relays to the user.

- **Network Access:** Apart from tunneling Web applications, SSL VPN can also encapsulate all TCP/IP traffic and transport through the SSL Tunnel including the routing information. In full tunneling mode, it can transport all TCP/IP traffic generated from applications like Outlook Express, terminal services, file sharing in the client system to corporate network through the SSL tunnel. In Split tunneling mode, only traffic for internal applications are routed through the SSL tunnel and other Internet traffic is routed through normal network connection. To support this feature the remote client agent (SSL Client) is activated as plug-in in the client machine from the VPN server.

- **Access Control:** SSL VPN can control the access of remote users in granular level such as per-user, per-group and per-network through group polices. Group policies can be configured to allow users of certain group to access more resources, if they are coming from specific network i.e. branch offices and during office hour. However, the same user group is limited to few resources if they are not coming from specific network.

- **Endpoint security controls:** SSL VPN can validate the integrity of remote client by checking weather it has up-to-date patches and antivirus software, before permitting access to the client.

As mentioned SSL VPN is an emerging technology and vendors are regularly upgrading the features of their products. However the selection of VPN technologies depends on the user's requirement. Even though many functionalities of IPSec VPN are incorporated in Client based SSL VPN, it is not a substitute of IPSec. SSL VPN is a useful technology for mass deployment for semi trained users as customers, suppliers, temporary work force from un-trusted network.