IPSec fornisce la più completa architettura per i tunnel VPN ed è ritenuto in assoluto il protocollo più sicuro. Può essere impiegato sia per connessioni LAN to LAN sia in modalità “accesso remoto” (con client dedicati oppure in combinazione con L2TP).

Durante la fase di negoziazione del tunnel i due *peer* negoziano dei metodi detti “Security Association (SA)”, i quali governano la crittografia, l’incapsulamento, la gestione delle chiavi, ect..... Durante l’instaurazione di un tunnel avvengono due distinte negoziazioni:

- Scambio delle chiavi crittografate (IKE SA)
- Apertura del tunnel IPSec

Il protocollo prevede che sia il *peer* che inizia la connessione (ossia il client remoto) a proporre le proprie SA, che il ricevente (il concentratore VPN) può accettare o rifiutare, eventualmente inviando delle controproposte. Il tunnel può essere stabilito solo ed unicamente se i *peer* individuano delle SA accettabili per entrambi.