**Security Association:**

Per poter funzionare correttamente IPSEC prevede la trasformazione di IP da sistema connection-less a protocollo in grado di mantenere un insieme di informazioni di stato (SPD) tra entità coinvolte (chiavi condivise e sistemi crittografici).

Le informazioni di stato definiscono un'associazione unilaterale tra sorgente e destinazione individuata da tre parametri:

- **Security Parameter Index (SPI):** identifica l'associazione localmente alla sorgente
- **IP Destination Address:** indirizzo della postazione remota relativa alla associazione
- **Security Protocol Identifier:** indica la natura dei protocolli collegati all'associazione (AH o ESP).

L'insieme delle SA valide memorizzate presso una entità IP viene detta **Security Policy Database (SPD);** ogni volta che un pacchetto IP richiede di essere instradato da una entità IP, il processo IPSEC provvede a controllare se nel SPD esista una o più SA valide per la destinazione richiesta.

Il controllo delle entry del DB viene valutato sulla base di diversi fattori, tra cui:

- **Indirizzo IP destinazione**
- **Indirizzo IP sorgente**
- **Identificativo utente locale** che ha generato il pacchetto (non significativo nel caso di un gateway)
- **Livello di sicurezza** associato ai dati (Secret e Unclassified)
- **Livello di trasporto** (campo Protocol dell'intestazione IP)
- **Porta sorgente**
- **Porta destinazione**
- **Tipo di controllo** incapsulato in IP (compreso AH e ESP)
- Valore del **campo TOS** nell'intestazione IP.