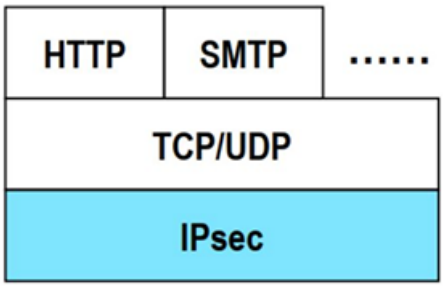
IPsec:
Opera a livello 3 dello stack, quindi offre sicurezza ai protocolli di livello 4.



Network layer security

Di solito la protezione è “per-host” per il fatto che sono meccanismi di sicurezza a livello IP.
In TLS si usa lo stesso protocollo per la gestione delle chiavi e i protocolli di sicurezza, mentre in IPsec ci sono due specifiche diverse.

Security associations:
Si possono avere:

- Tra due host
- Tra host e gateway
- Tra due gateway

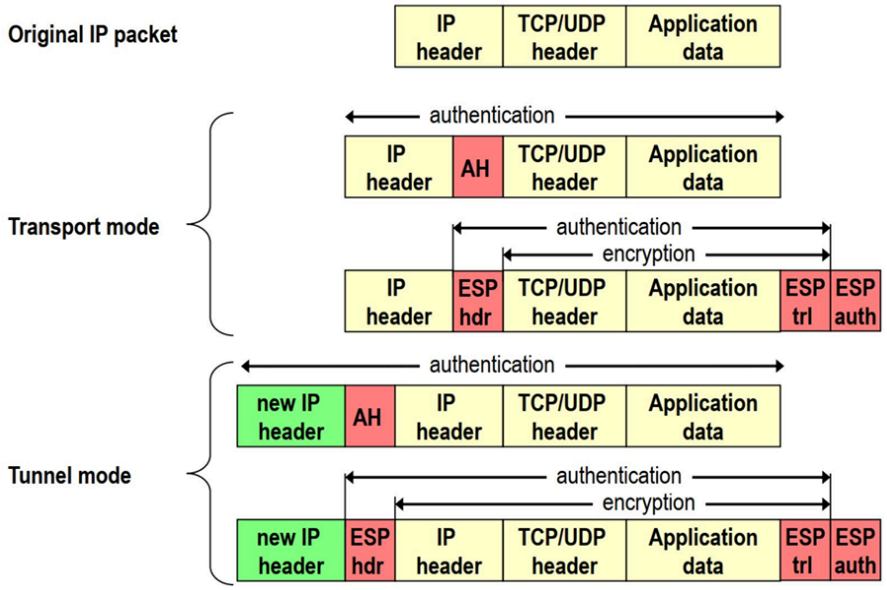
Definisco il materiale crittografico per cifrare i pacchetti.
Le SAs sono monodirezionali. Intuitivamente si usano le SAs monodirezionali quando non c’è il concetto di connessione.
SPI→ è l’identificatore di una SA (con l’indirizzo IP)
SAD→ SAs database. Contiene il materiale crittografico per ogni SA.

La gestione delle chiavi può essere manuale o automatica.
Manuale→ vengono fornite le chiavi statiche. Si usa solo in piccoli scenari.
Automatica→ più gestibile (IKEv2). Le SAs vengono create on-demand.

IPsec è un insieme di protocolli.
Due tipologie di funzionamento:

- AH→ fornisce autenticazione e integrità
- ESP→ fornisce autenticazione e/o cifratura, ma non integrità

L’integrità dell’header IP esterno non ha bisogno di essere controllata.



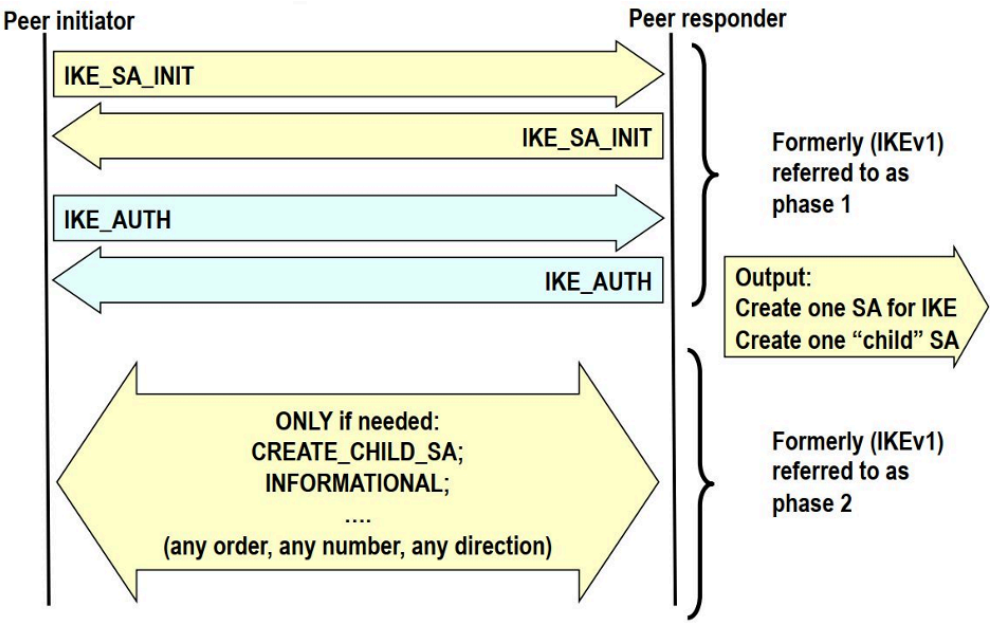
Transport e tunnel mode:
In **tunnel mode** aggiungiamo un header IP esterno, incapsuliamo il pacchetto.
L'header interno e cifrato e autenticato, nel caso di ESP mode, quindi non c'è bisogno di fare questi controlli sull'header esterno.
Si usa quando vogliamo instradare i pacchetti fuori dalla nostra rete realizzando delle VPN.

In **transport mode** si usa SOLO per connessioni end to end. I gateway usano il transport mode solo per le connessioni che iniziano e finiscono nei gateways, in pratica non possono instradare in modo sicuro pacchetti di altri dispositivi.

Security policies:
Si possono definire policies in base al tipo di pacchetto.
Le security policies sono mantenute nel security policy DB (SPD).
Le security policies sono delle regole di tipo "match-action".Il match può essere in base a:Indirizzo IP sorgente o destinazione, protocollo IP e porte sorgente/destinazione L4.
Le possibili azioni sono: bypass, discard e protect (applicare IPsec AH o ESP).

Operazioni di IPsec:
Pacchetti in uscita: si guarda se qualche policy matcha nel SPD, se c'è match passano il pacchetto al SAD. Se si trova la SA statica si applica, altrimenti se ne richiede una: inizia il processo d negoziazione.
Pacchetti in ingresso: si estrae la SPI e IP sorgente e destinazione dal pacchetto, si processa il pacchetto e si interroga il SPD.

IKEv2:
IKEv2 stabilisce e mantiene le SAs.



Solitamente c’è un “initiator”, poi IPsec stabilisce entrambe le SAs.
Si ha una SA, poi si creano le SAs figlie per le sottoreti e per le diverse configurazioni di rete che si hanno dietro i security gateways.

Le SAs sono utilizzate per i messaggi di controllo (no AH/ESP), le SAs figlie stabilite dinamicamente per i messaggi sul piano data (con uso di AH/ESP), ad esempio per definire tunnel su diverse sottoreti..