ESP Encapsulation Security Payload Protocol:

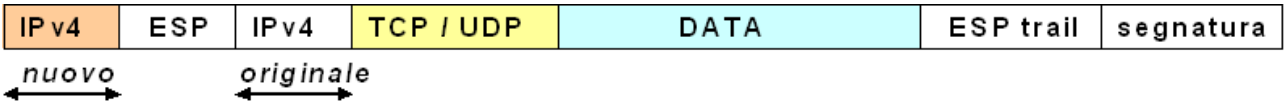
I servizi offerti da IPSEC sono disponibili alle entità IP con una modifica dei datagrammi IP.

Per usufruire del servizio di autenticazione occorre inserire all'interno del datagramma IP l'intestazione ESP **(valore campo protocol = 50).**

Le modalità di funzionamento possono essere:

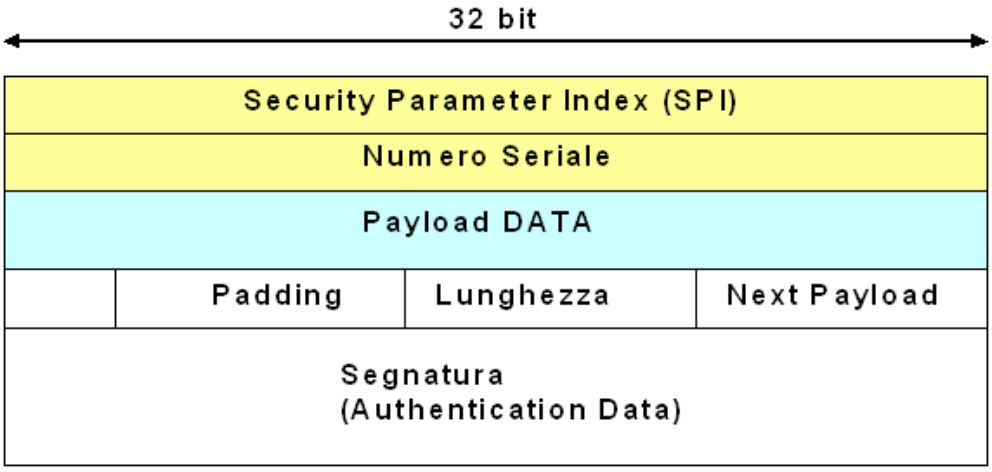
- **modalità trasporto:**

- **modalità tunnel:**



La modalità **trasporto** fornisce protezione per i protocolli di livello superiore rispetto ad IP; tale modalità viene utilizzata per implementare funzioni crittografiche fruibili direttamente dalle stazioni finali (end to end).

La modalità **tunnel** fornisce protezione all'intero datagramma IP; anche se questa modalità ha scopi end to end, viene usata molto anche per implementare funzioni crittografiche presso gli apparati di frontiera di una rete locale (router e firewall); la modalità tunnel è estremamente interessante per le realizzazioni VPN (Virtual Private Network)



Per garantire la riservatezza delle informazioni contenute in un datagramma IP, il progetto IPSEC utilizza ESP Protocol; esso si compone di un servizio per la confidenzialità delle informazioni (data) e di un servizio di autenticazione.

Il servizio di autenticazione per produrre la segnatura utilizza lo schema noto come HMAC (**Hash** Message Authentication Code).

- **SPI:** indica a quale SA (associazione) appartiene il datagramma IP
- **Numero Seriale:** indica la posizione del datagramma all'interno del flusso di messaggi scambiati entro una data associazione (2^{32} – 1 datagrammi IP validi)
- **algoritmi simmetrico:** DES, 3DES, IDEA, Blowfish, CAST, RC4

Il protocollo ESP non descrive come creare una nuova SA ma stabilisce solo le trasformazioni da apportare ad un datagramma IP per garantire riservatezza ed integrità.

Pur definendo un servizio di autenticazione indipendente è possibile rinunciare a tale servizio ed avvalersi di quello definito da Authentication Protocol; poiché ciascuna SA mantiene informazioni relative ad un singolo protocollo, se le entità IP decidono di avvalersi dei servizi di entrambi i protocolli devono essere impiegate due distinte SA.