**IPSec (Internet Protocol Security)**

**Che cos’è?**

È un insieme di protocolli e standard di sicurezza che lavora nel livello di rete. Fornisce i seguenti tipi di protezioni:

* **Confidenzialità:** crittografia dei dati trasmessi.
* **Integrità:** garantisce che i dati non siano stati alterati durante la trasmissione.
* **Autenticazione:** controllo dell’identità degli interlocutori.
* **Anti-replay:** prevenzione dalla ripetizione di pacchetti precedentemente inviati.
* **Protezione analisi traffico:** una terza parte non può sapere cosa e quanto è stato trasmesso, però riesce a vedere quanti pacchetti vengono scambiati.
* **Controllo di accesso:** solamente chi è autorizzato riesce ad accedere alla risorsa.

**Come funziona?**

L’IPsec ha due passaggi:

**Primo:**

**1.1** I due host scelgono l’algoritmo di cifratura (DES, triple DES, …)

**1.2** Scelta dell’algoritmo per verificare l’integrità del messaggio (MD5, SHA-1, …)

**1.3** Scelta di come verranno autenticate le connessioni (condivisione di chiave segreta, certificato di chiave pubblica, …)

**Secondo:**

**2.1** Se verrà utilizzato il protocollo Authentication Header (AH).

**2.2** Se verrà utilizzato il protocollo Encapsulating Security Payload (ESP).

**2.3** Quale algoritmo di crittografia verrà utilizzato per ESP

**2.4** Quale algoritmo di crittografia verrà utilizzato per AH

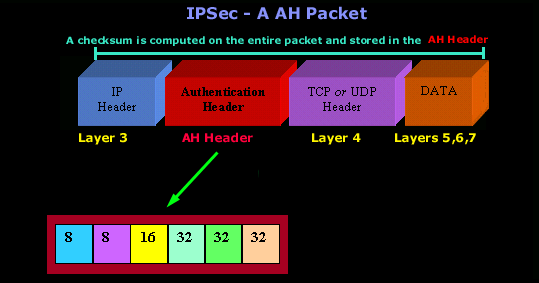
Si deve tener conto che AH e ESP possono essere usati entrambi o uno solo.

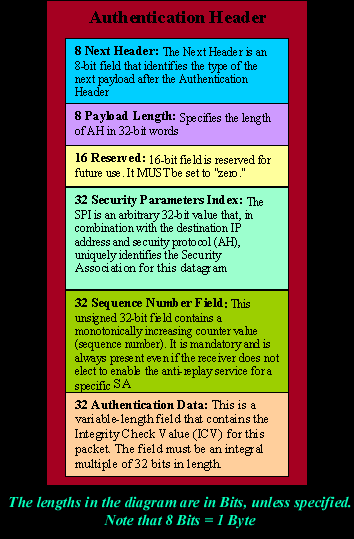
**Authentication Header (AH):**

**Fornisce** **autenticazione (indirizzi IP)** e **integrità (funzioni hash)**.

Le informazioni nell'AH vengono aggiunte nel pacchetto generato dal mittente, tra il livello di rete e di trasporto. AH firma digitalmente l'intero contenuto di ciascun pacchetto. Questa firma offre 3 vantaggi:

* **Protegge dagli attacchi di replay:** si evita il caso in cui un hacker riesce a catturare pacchetti, modificarli e quindi inviarli a destinazione.
* **Protezione contro la manomissione:** la firma indica che non è possibile modificare alcuna parte di un pacchetto senza essere rilevata.
* **Protezione contro lo spoofing:** controllo dell’autenticità degli interlocutori.

****

****

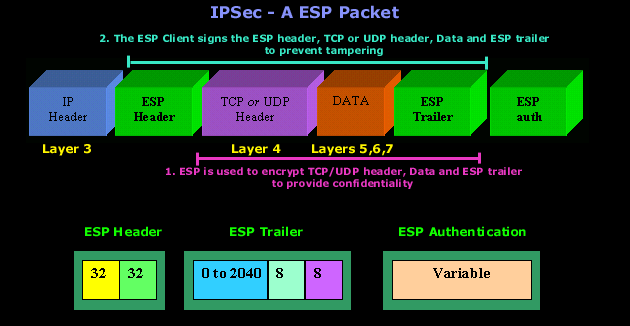
* **Next header:** identifica il tipo del prossimo header dopo AH
* **Payload length:** indica la lunghezza del payload
* **Reserved:** riservato per utilizzi futuri e di solito è impostato a 0
* **Security Parameter Index:** contiene informazioni come gli algoritmi di crittografia e di autenticazione da utilizzare
* **Sequence number field:** è un valore incrementato per ogni pacchetto che viene inviato con lo stesso SPI. Serve a proteggere contro gli attacchi di replay
* **Authentication data:** contiene i **dati** di **autenticazione** (MAC). che vengono utilizzati per **verificare** **l'autenticità** e **l'integrità** dei dati del pacchetto. Il **MAC** viene **calcolato** utilizzando **algoritmi** di **autenticazione** come **HMAC** (Hash-based Message Authentication Code) che **utilizzano** **chiavi** **condivise** tra le entità di comunicazione

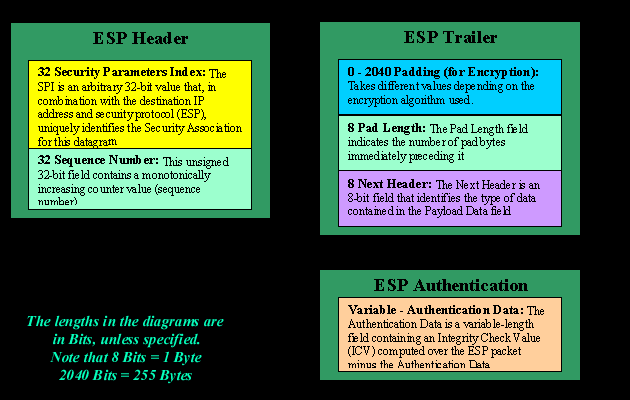
**Encapsulating Security Payload (ESP)**

AH protegge i dati dalle manomissioni, invece **ESP** viene usato per **crittografare (confidenzialità)** l’intero **payload** di un **pacchetto** **IPSec**.

ESP da solo **fornisce** **autenticazione**, **confidenzialità** e **integrità**. Ottiene questo risultato aggiungendo **3** **componenti** **separati**:

* **ESP header:** fornisce l’integrità del payload.
* **ESP trailer:** fornisce la confidenzialità.
* **ESP authentication block:** garantisce autenticazione e protezione contro attacchi replay.

****

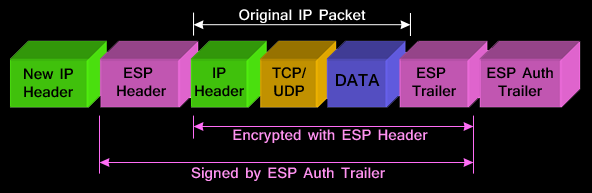


**Le due modalità IPSec:**

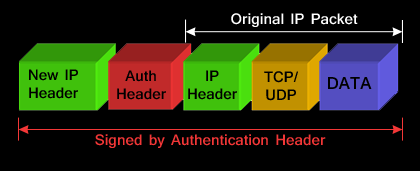
**Modalità tunnel:**

**IPSec** **avvolge** il **pacchetto** **originale** (non solo il payload), lo **crittografa**, aggiunge una **nuova** **intestazione** **IP** e lo invia all'altro lato del tunnel VPN. Questa modalità viene utilizzata per crittografare il traffico tra gateway IPSec sicuri.

Modalità tunnel IPSec con intestazione **ESP**:



Modalità tunnel IPSec con intestazione **AH**:

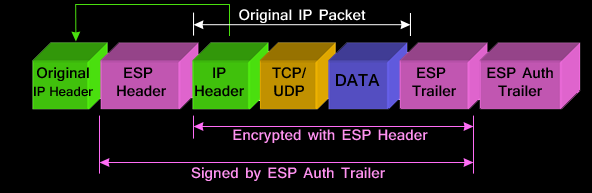


Viene utilizzato spesso nei gateway a gateway e host-to-gateway

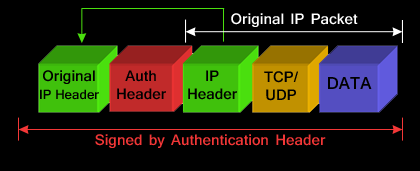
**Modalità trasporto:**

Viene utilizzata per le comunicazioni end-to-end e **crittografa** **solo** il **payload** mentre l'intestazione **IP** **originale** **non viene toccata.**

Modalità di trasporto IPSec con intestazione **ESP**:



Modalità di trasporto IPSec con intestazione **AH**:



Viene utilizzato spesso nel host-to-host

C’è un problema ed è quando un pacchetto subisce il NAT, l'indirizzo IP sorgente viene modificato, rendendo l'hash nel campo di intestazione AH non valido. Di conseguenza, il pacchetto viene considerato corrotto o manipolato.

**IKE (Internet Key Exchange)**

Fornisce un modo per **gestire** lo **scambio di chiavi**, autenticare i peer e concordare una policy di comunicazione sicura. Caratteristiche:

* IKE **utilizza** un **protocollo** chiamato **ISAKMP** per negoziare i parametri IPSec tra due peer.
* ISAKMP comunica sulla **porta** **UDP** **500**.

**GRE (Generic Routing Encapsulation)**

**Che cos’è?**

È un protocollo di tunnelling per **consentire** la **trasmissione** di **dati** **attraverso** una **rete** che potrebbe **non supportare** direttamente il tipo di **pacchetto originale.** **L’implementazione** dell’**IPSec** garantisce una **maggiore** **sicurezza**.

È preferibile usare GRE IPSec perché questo consente ai pacchetti multicast di attraversare il tunnel.

