IPSEC

- Az IPSec protokoll a TCP/IP architektúra hálózati rétegének szabványosított (RFC 2401, 2402, 2406, 2408, 2409) biztonsági protokollja. Ez azt jelenti, hogy az IP és minden fölötte található protokoll (TCP, UDP, ICMP, stb.) számára védelmet biztosít.
- Két alprotokollja van, az **AH (Authentication Header)** és az **ESP (Encapsulated Security Payload).** Az AH és az ESP protokollok kombinálhatók az IP csomagok teljeskörű védelme érdekében.
- Az IPSec protokollhoz tartoznak még az ISAKMP (Internet Security Association and Key Management Protocol) és az IKE (Internet Key Exchange) protokollok. Mindkettő kulcscserével kapcsolatos feladatokat lát el.

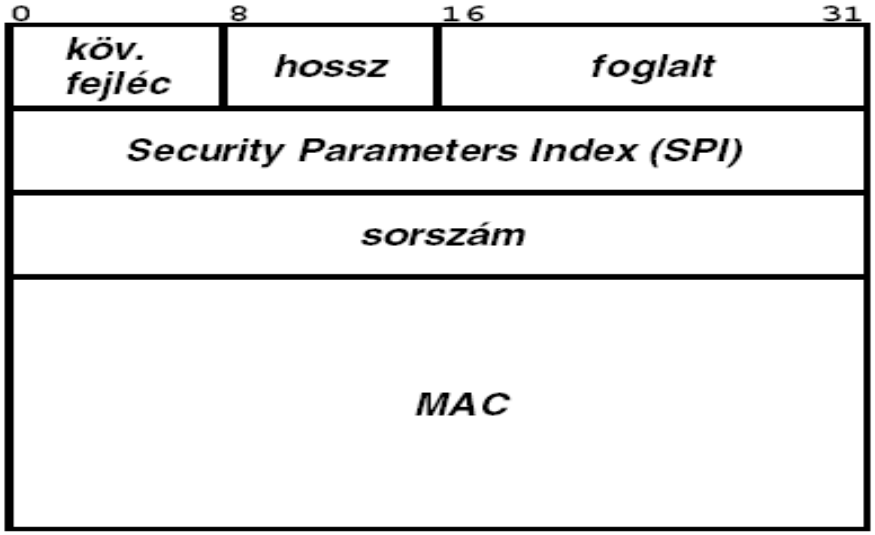
AH protokoll

Az AH protokoll

- integritásvédelmet,
- eredethitelesítést
- visszajátszás elleni védelmet

biztosít az IP csomagok számára.

AH fejléc



Az **integritásvédelmet és az eredethitelesítést** úgy éri el, hogy az IP fejléc és az azt követő felsőbb szintű protokoll fejléce közé beszúr egy AH fejlécet, mely egy, a teljes IP csomagra számolt üzenethitelesítő kódot (**MAC**) tartalmaz.

A **visszajátszások detektálásának** érdekében, az IP csomagokat sorszámozza.

Az AH fejlécben található MAC érték a sorszámot is védi.

AH fejléc

- *következő fejléc (next header):* Ez a mező az AH fejlécet követő fejléc típusát adja meg, azaz az IP csomag tartalmára utal.
- *hossz (length):* Ez a mező az AH fejléc 32 bites szavakban mért hosszára utal.
- *Security Parameter Index (SPI):* Ez egy azonosító, mellyel a küldő azt jelzi a vevő számára, hogy milyen módon és mely kulcsokat használva kell az AH fejlécet feldolgozni. Az AH protokoll feltételezi, hogy a küldő és a vevő korábban már megegyezett az alkalmazható algoritmusokban és kulcsokban, tipikusan az ISAKMP/IKE protokollokat használva.
- *sorszám (sequence number):* Ez a mező az aktuális IP csomag sorszámát tartalmazza.

ESP protokoll

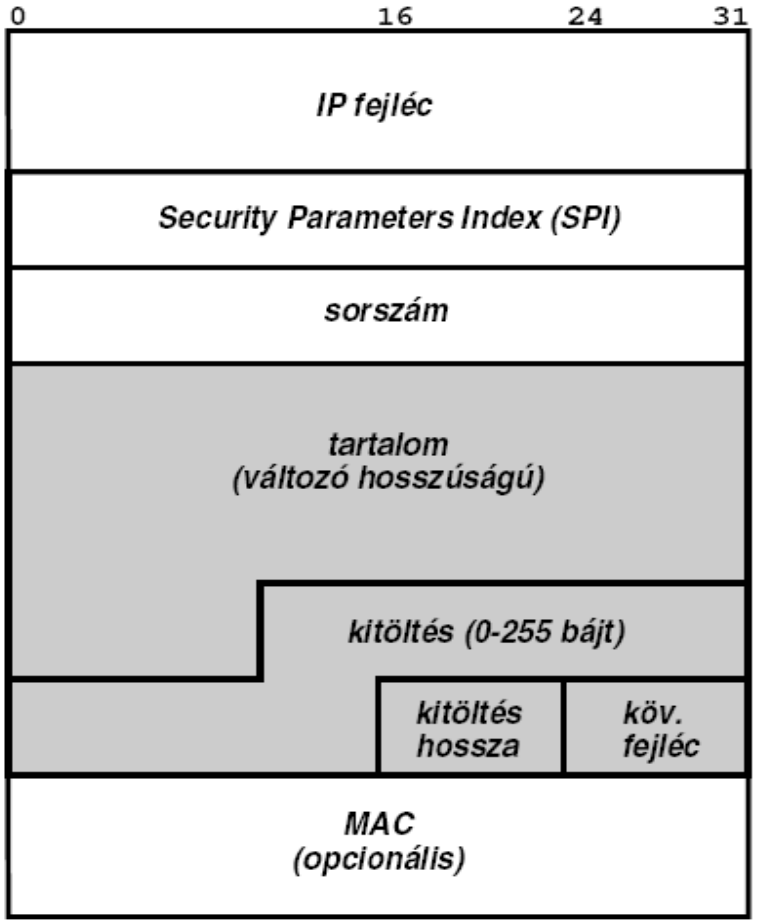
Az ESP protokoll feladata az

- IP csomag tartalmának rejtése,
- a tartalom integritásának védelme (opcionális)

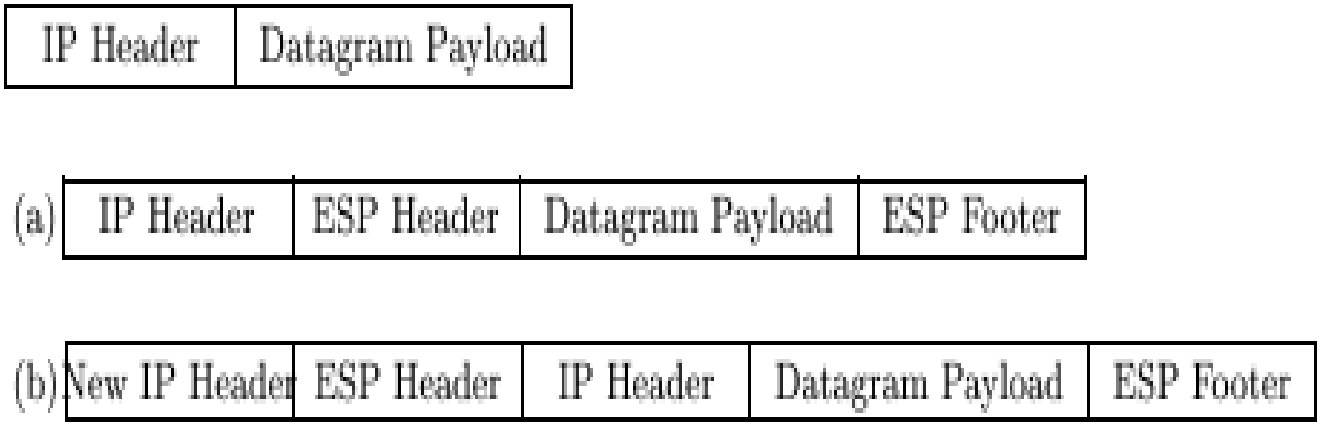
Az előbbit az IP csomag tartalmának rejtjelezésével oldja meg a protokoll, az utóbbit pedig úgy, hogy az ESP fejlécre és a csomag tartalmára számít MAC kódot és azt a csomaghoz csatolja.

Az AH-val ellentétben az ESP MAC nem védi az IP fejléc mezőit.

ESP-vel védett csomag felépítése



IPSEC üzemmódok



Mind az AH, mind az ESP protokollt két üzemmódban lehet használni. Ezeket **szállítási (transport)** és **alagút (tunnel)** módoknak nevezzük.
Szállítási módban (a) az AH vagy az ESP fejléc a csomag eredeti IP fejléce és a felsőbb szintű protokoll (például TCP, UDP) fejléce közé kerül.
Alagút módban (b) azonban az eredeti IP csomagot teljes egészében beágyazzuk egy másik IP csomagba (IP tunneling), és az AH vagy az ESP fejléc az új, és az eredeti IP fejléc közé kerül.

Alkalmazás

Az alagút móddal létrehozhatunk virtuális magánhálózatokat (Virtual Private Network , VPN), ahol két, tűzfallal védett belső hálózatot az interneten keresztül, IPSec-et használva biztonságosan összekötünk. *N*1 belső hálózaton található *H*1 gép egy IP csomagot küld az *N*2 belső hálózaton található *H*2 gépnek. Mikor az IP csomag eléri a *G*1 tűzfalat, a tűzfal az egészet beágyazza egy *G*2-nek szóló IP csomagba, és azt IPSec védelemmel ellátva küldi tovább. Így a csomag biztonságban jut át az interneten a *G*2 tűzfalhoz. *G*2 elvégzi az IPSec feldolgozást (dekódolja a csomagot, ellenőrzi a MAC kódot stb.), majd a csomagban található eredeti IP csomagot (most már nyíltan) továbbküldi az eredeti címzettnek.