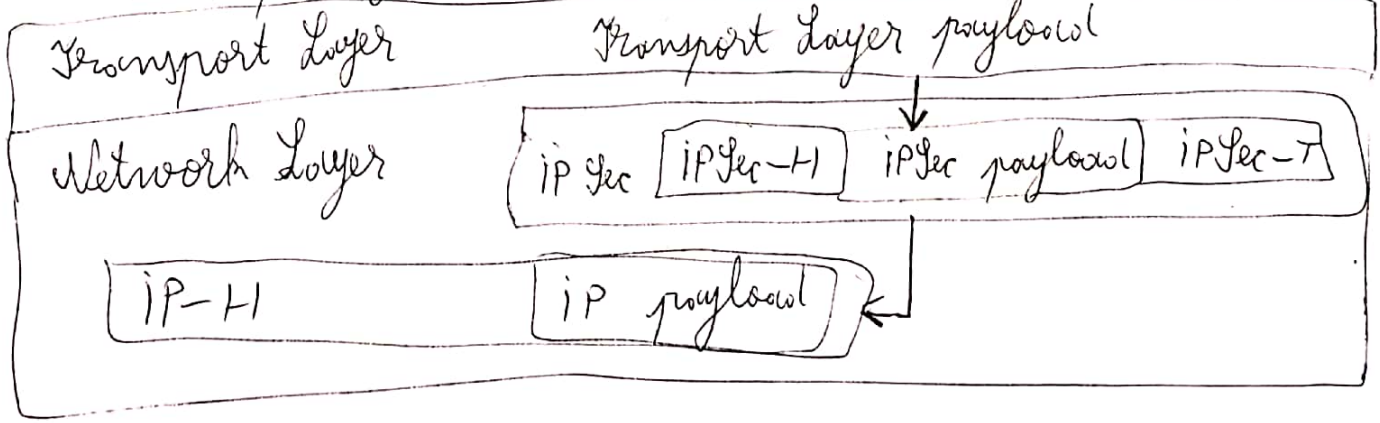
C12

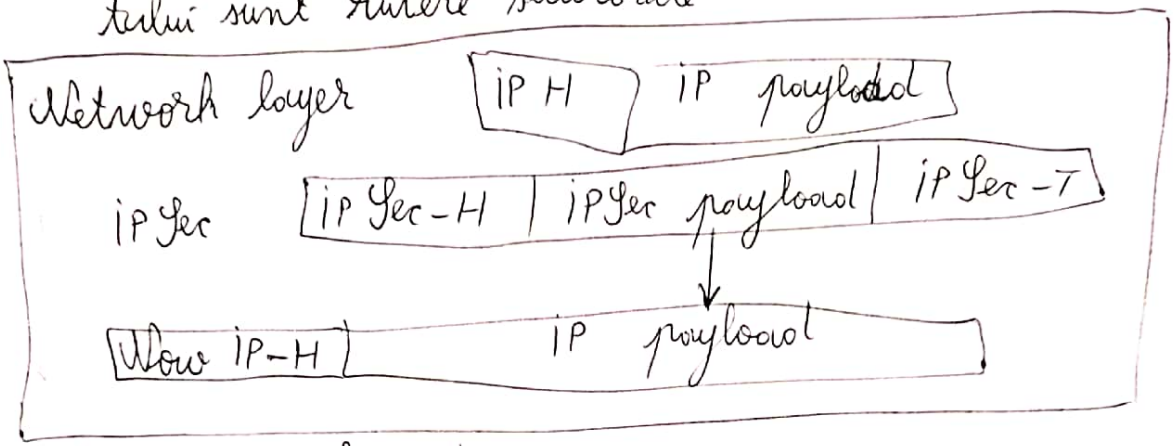
Securitatea în internet (I)

① Securitatea IP

- dezvoltarea de mecanisme de securitate specifice pt. diferite domenii de aplicații: e-mail, client/server sau acces web
- Pb. de securitate:
  - interzicerea legăturilor cu site-urile potențial nesigure
  - criptarea pachetelor emise și autentificarea pachetelor primite.
- Securitatea la nivelul IP cuprinde 3 zone funcționale:
  - autentificarea
  - confidențialitatea
  - managementul cheilor criptografice.
- Moduri de utilizare a IP Security:
  1. Modul transport:
     - asigură protecție numai pt. informațiile primitor de la protocoalele de nivel imediat superior IP (TCP, UDP, etc.)
     - este folosit pt. comunicarea a 2 calculatoare gazdă
     - nu protejează antetul IP, care este adăugat ulterior

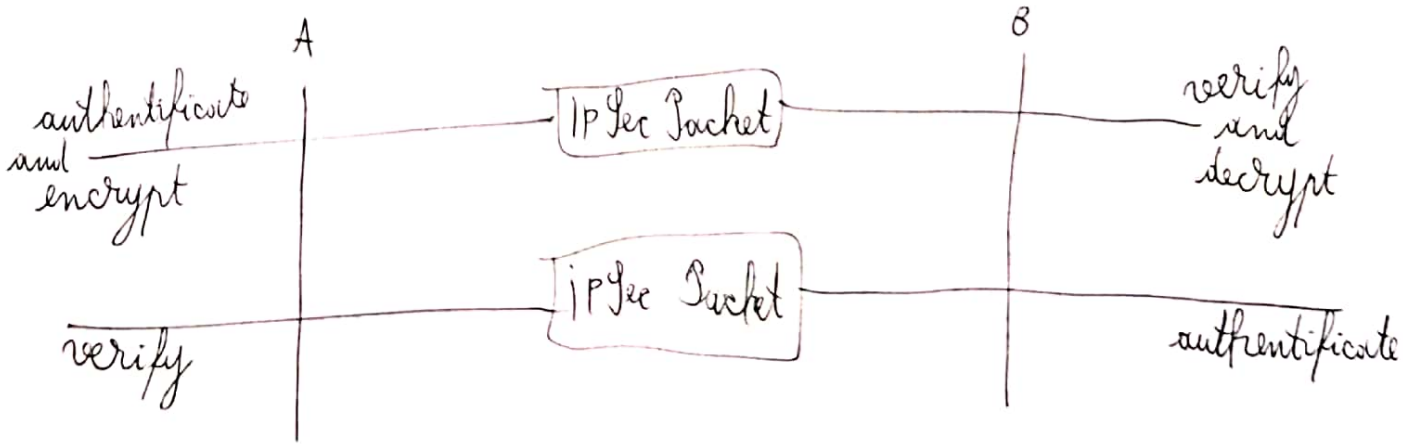


2. Modul tunel:
- asigură protecție pt. întregul pachet IP.
- ia pachetul IP, aplică IPSec.
- este utilizat atunci când sursa și/sau destinația pachetului sunt rutere securizate



② Arhitectura IP Security
→ Specifice pt. IPSec avem următoarele grupuri:
- arhitecturii
- protocolul ESP (Encapsulating Security Payload)
- protocolul AH (Authentification Header)
- alg de criptare și autentificare.
- managementul cheilor
- domeniul de interpretare

→ Asocieri de securitate: IP este un protocol fără conexiune, asocierea parametrii de securitate pot fi stabiliți într-una din urm. modalități:
1. individual pt. fiecare pachet IP.
2. înainte de a se începe transmiterea pachetelor IP propriu-zise (variantă ineficientă)
3. incluși în primul pachet IP (IPSec). Gazda destinație îi salvează pt. a-i utiliza și pt. celelalte pachete.



C12

→ O asociere de securitate este definită în mod unic prin:
- indexul parametrilor de securitate (SPI).
- adresa de destinație IP.
- identificatorul protocolului de securitate.
- nr. de secvențe.
- nr. de depășire.
- fereastra anti-replay.
- informații AH.
- informații ESP.
- timp de viață.
- modul de IPSec.
- MTU (Maximum Transmission Unit).

③ Baza de date a SA (SPD - Security Policy Database).
- fiecare poartă are nevoie de informații legate atât de intrare, cât și de ieșire.
- o implementare a IPSec care definește parametrii asociați cu fiecare SA.
- se folosește protocolul IKE (Internet Key Exchange).

④ Selectori SA (set de valori definite de câmpuri ale formatului IP și de nivel superior protocolului IP; conțin o SA pt. tipul respectiv de trafic):
- adresele IP pt. sursă și destinație.
- protocolul de transport.
- denumirea protocolului IPSec (AH/ESP).
- adresele porturilor sursă sau destinație.

⑤ Protocolul Authentication Header (AH)
- Headerul AH asigură mecanismul pt. controlul integrității și autenticității pachetului ip. Acest control elimină posibilitatea modificării pachetelor în tranzit, fără ca modificările să fie detectate.
- AH este format din:
  - next header
  - payload length
  - reserved
  - security parameters index
  - sequence data
  - authentication data

⑥ ICV – Integrity Check Value → Câmpul Authentication Data din AH conține o valoare denumită ICV care este un cod de autentificare a mesajului (MAC) sau o versiune trunchiată a unui cod produs cu un algoritm MAC.

⑦ IPSec – Mecanismul anti-replay

– La stabilirea unei noi asocieri de securitate SA, sursa inițializează un contor de pachete cu valoarea 0. Acesta va fi incrementat cu fiecare pachet emis și valoarea lui va fi scrisă în câmpul nr. de secvență din AH.

– La atingerea valorii $2^{32}-1$ sursa trb. să termine SA curentă și să negocieze o nouă SA, cu o nouă cheie

⑧ Formatele AH în mod transport și în mod tunel

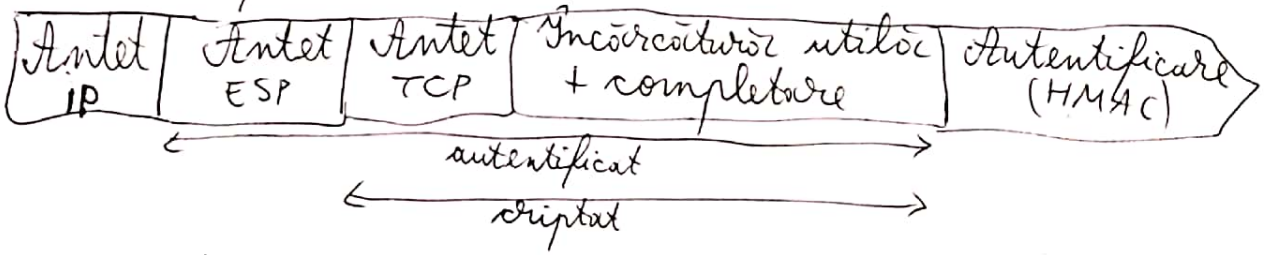
IP este inserat după header. — tot pachetul IP este autentica

⑨ Protocolul ESP (Encapsulating Security Payload)

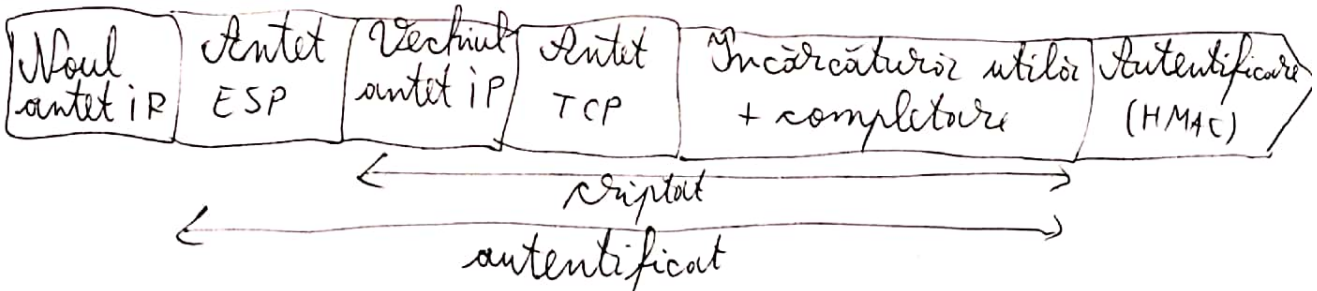
– asigură confidențialitatea conținutului mesajelor și, parțial, confidențialitatea traficului.

– este atât pe modul de transport, cât și pe autentificare. Realizează criptarea unității de date IP și a pachetului IP original.

– ESP transport:



– ESP tunel:



– Formatul unui pachet ESP conține:

- Security Parameter Index.
- Number Sequence

C12

- Payload Data
- Padding - Pad Length
- Next Header
- Authentication Data

(10) Alg. ESP constă în:
- un trailer ESP este adăugat datelor primite de la niv. superior
- sarcina utilă și trailer-ul sunt criptate.
- header-ul ESP este adăugat.
- header-ul ESP, sarcina utilă și trailer-ul ESP sunt folosite pt. a crea datele de autentificare.
- datele de autentificare sunt adăugate la sf. trailer-ului ESP.
- header-ul IP este adăugat după valoarea protocol (50)

(11) VPN - Rețea virtuală privată
- rețele private.
- intranet (rețea locală privată).
- extranet (resursele pot fi accesate de grupuri din afara organizației sub controlul administratorului de rețea).

Pt. realizarea confidențialității organizațiile pot folosi una dintre strategiile:
- rețele private.
- rețele hibride.
- rețele virtuale private.

(12) Tunelarea este o metodă de folosire a infrastructurii unei inter-rețele pt. transferul datelor dintr-o rețea peste o altă rețea. Calea logică pe care pachetele încapsulate o urmează în inter-rețea se numește tunel.
Tunelarea include întregul proces: încapsulare, transmitere și decapsulare a pachetelor. Tunelarea necesită 3 protocoale diferite:
- protocolul de transport.
- protocolul de încapsulare.
- protocolul pasager.

(13) VPN → folosește IPSec în mod tunel pt. a realiza autentificare, integritate și caracter privat. Fiecare datagramă IP destinată pt. utilizare privată în cadrul organizației este încapsulată într-o datagramă.