Komunikacijski protokoli in omrežna varnost

Varnostni elementi

IPSec

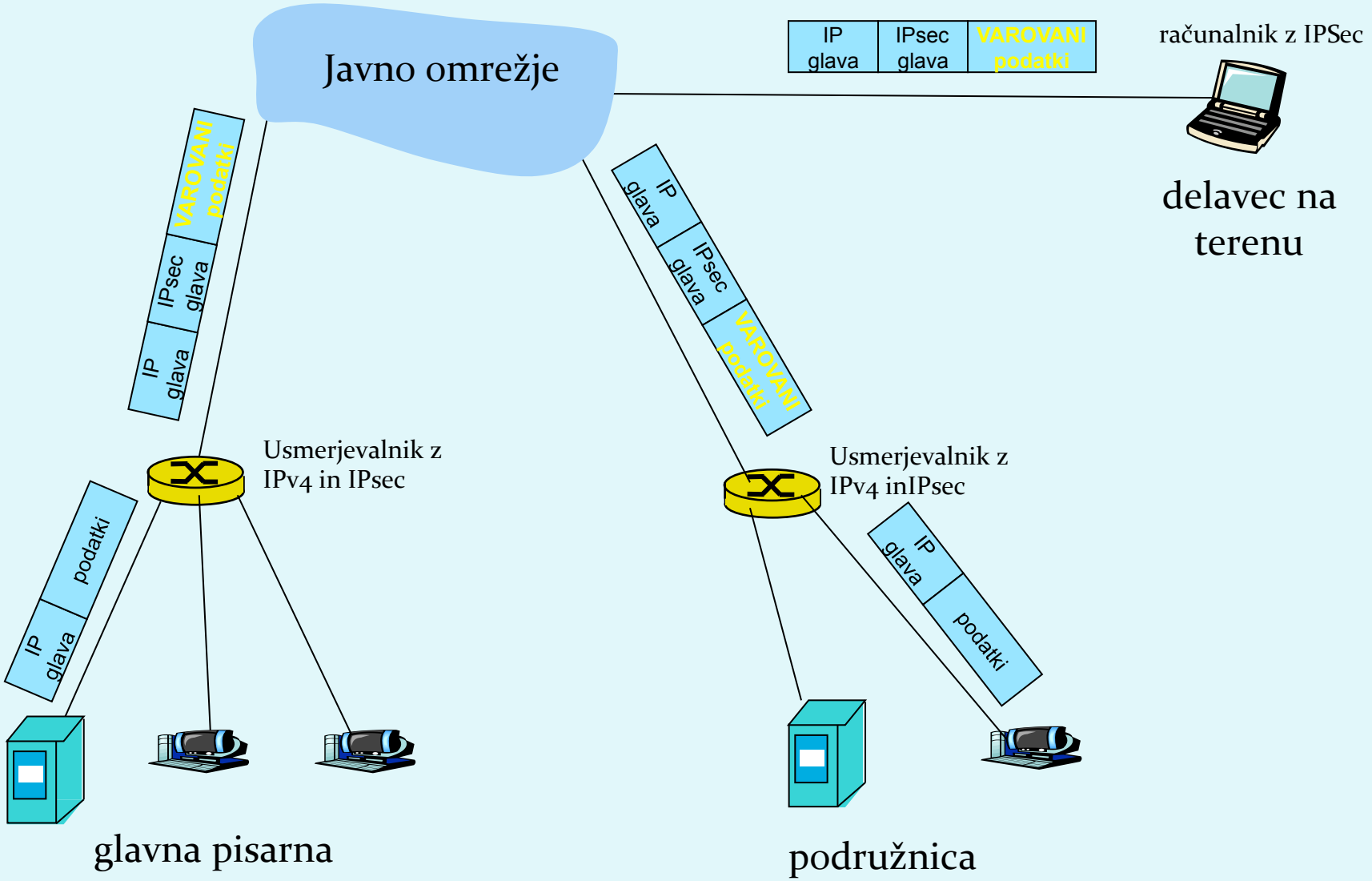
- IP security protocol (varnost na omrežni plasti)
- uporaba za varovanje povezav med dvema entitetama, uporaba za VPN (navidezna zasebna omrežja)!
- varnost na omrežni plasti:
  - zakrivanje vseh vrst podatkov (TCP segment, UDP segment, ICMP sporočilo, OSPF sporočilo itd.)
  - zagotavljanje avtentikacije izvora
  - integriteta podatkov pred spreminjanjem
  - zaščita pred ponovitvijo komunikacije
- RFC 2411: pregled mehanizmov in delovanja IPSec

Navidezna zasebna omrežja (VPN)

- *Virtual Private Network*

- podjetja, ki so na različnih geografskih lokacijah, si lahko želijo visoke varnosti pri komunikaciji. Rešitvi:
  1. gradnja ZASEBNEGA omrežja: podjetje zgradi lastno omrežje, popolnoma ločeno od preostalega Interneta (draga postavitev in vzdrževanje - potrebni usmerjevalniki, povezave, infrastruktura!)
  2. podjetje vzpostavi NAVIDEZNO ZASEBNO omrežje (VPN) z infrastrukturo javnega omrežja:
     - podatki znotraj lokalnih (zasebnih) delov omrežja se prenašajo tradicionalno (IP),
     - podatki, ki potujejo preko javnih delov omrežja se prenašajo zaščiteno (IPSec)

VPN: primer

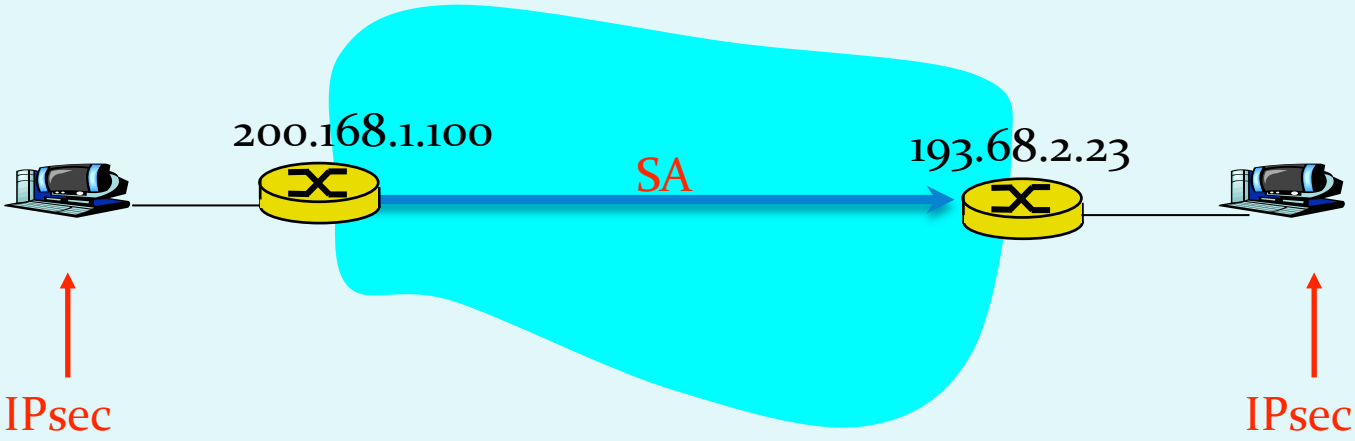

Javno omrežje
IP glava
IPsec glava
VAROVANI podatki
računalnik z IPSec
delavec na terenu
VAROVANI podatki
IPsec glava
IP glava
IP glava
podatki
Usmerjevalnik z IPv4 in IPsec
IP glava
IPsec glava
VAROVANI podatki
Usmerjevalnik z IPv4 inIPsec
IP glava
podatki
glavna pisarna
podružnica

Implementacija IPsec

- mehanizem IPSec ponuja dva protokola varovanja:
  - AH - *Authentication Header*
    - zagotavlja avtentikacijo izvora in integriteto podatkov
  - *ESP - Encapsulation Security Payload*
    - zagotavlja avtentikacijo izvora, integriteto podatkov IN zaupnost podatkov
- za vsako smer IPSec komunikacije je potrebno vzpostaviti SA (Security Association)
  - primer: glavna pisarna in podružnica uporabljata dvosmerno komunikacijo. Ravno tako glavna pisarna uporablja dvosmerno komunikacijo z n delavci na terenu. Koliko SA je potrebno vzpostaviti?

$$2 + 2n$$

Vzpostavitev SA



- Usmerjevalnik ima bazo SAD (*Security Association Database*), kjer hrani podatke o SA:
  - 32 bitni ID SA, imenovan SPI (Security Parameter Index)
  - izvorni in ponorni IP SA
  - vrsta enkripcije (npr. 3DES) in ključ
  - vrsta preverjanja integritete (npr. HMAC/MD5)
  - ključ za avtentikacijo

Dva načina komunikacije

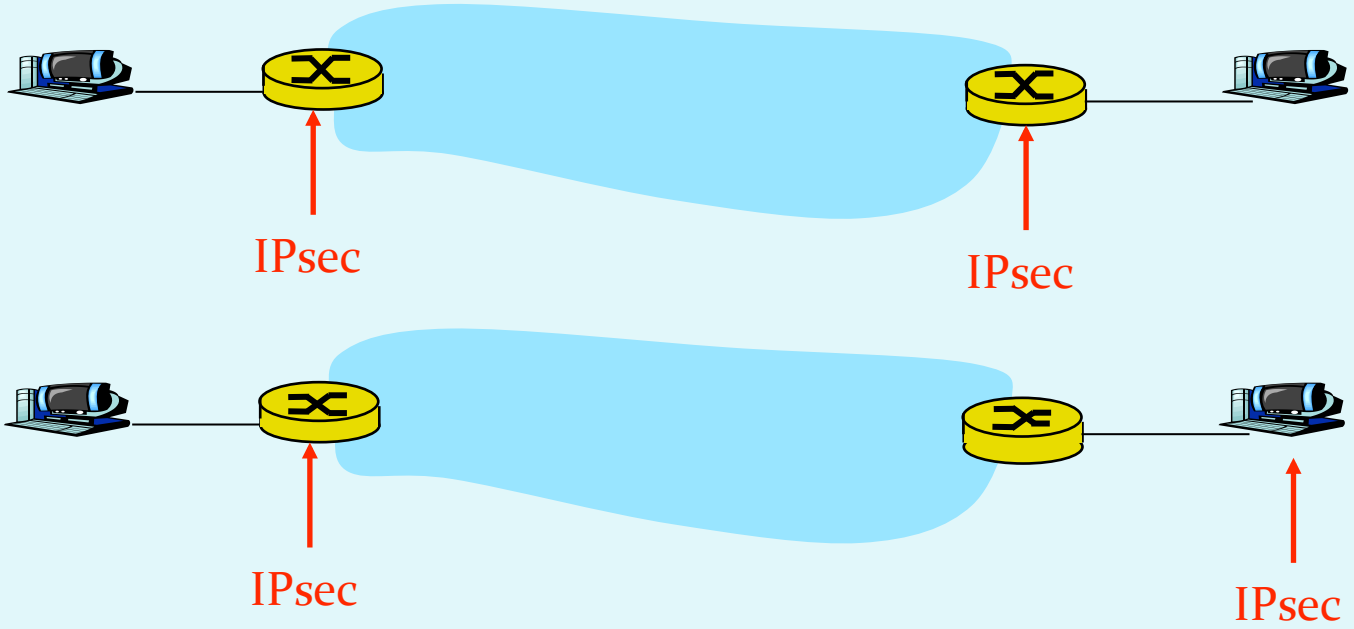
- *transport mode* - implementiran med končnimi odjemalci (vmesniki računalnikov), ščiti zgornje plasti protokola. Transparentno vmesnikom, kriptira samo podatke v paketu.
- *tunnel mode* - transparentno končnim odjemalcem, usmerjevalnik-usmerjevalnik ali usmerjevalnik-uporabnik. Kriptira podatke in glavo paketa.

Transport mode z AH	Transport mode z ESP
Tunnel mode z AH	Tunnel mode z ESP

IPsec Transport Mode

- IPsec datagram potuje med končnima sistemoma.
- Ščitimo zgornje plasti.

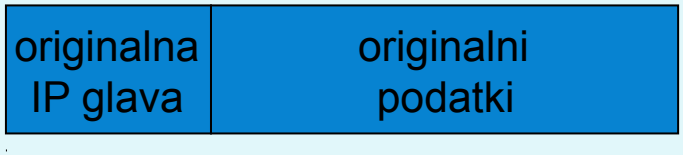
IPsec – tunneling mode



- IPsec se izvaja na končnih usmerjevalnikih
- za odjemalce ni nujno, da izvajajo IPsec

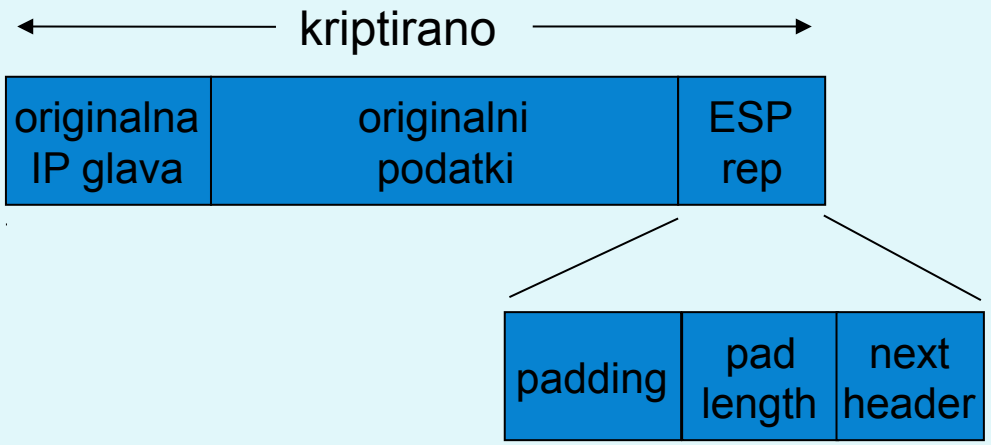
IPsec datagram: tunnel mode in ESP

- Poglejmo si, kako deluje najbolj pogosto uporabljen IPSec način
- Originalni podatki:



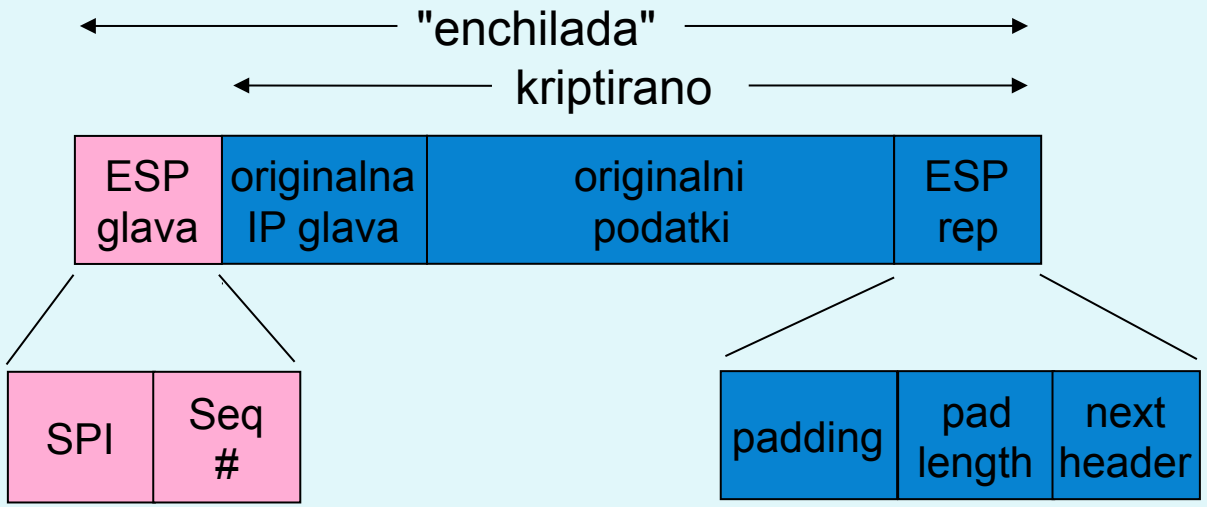
IPsec datagram: tunnel mode in ESP

- na konec datagrama se doda ESP glava (zapolnitev je potrebna za bločno kodiranje, next header je protokol, vsebovan v podatkih)
- rezultat se kriptira (algoritem in ključ določa SA!)



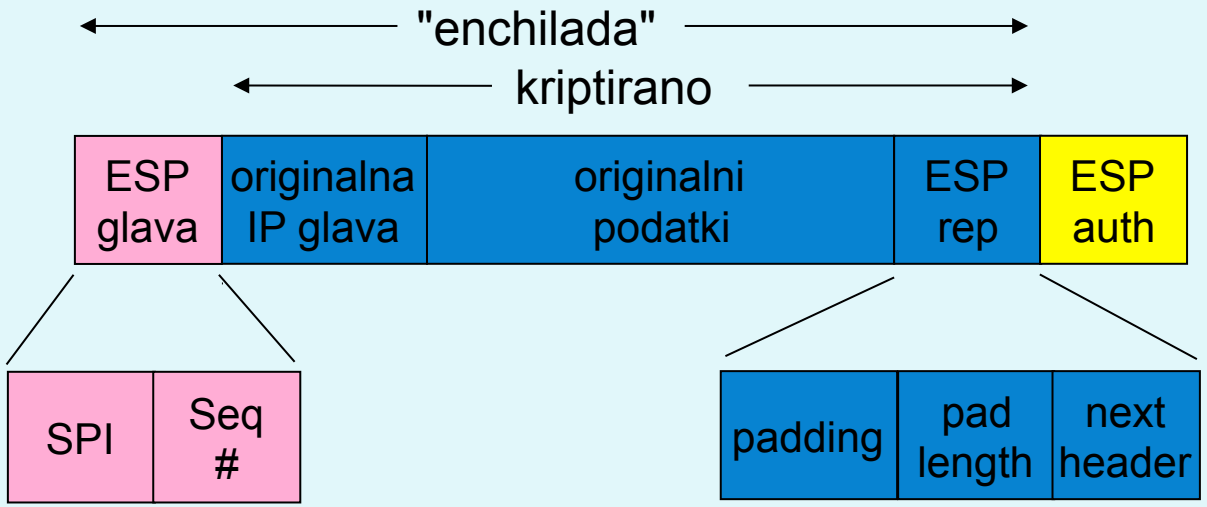
IPsec datagram: tunnel mode in ESP

- doda se ESP glava: rezultat je "*enchilada*" (SPI - indeks SA, ki se ga uporabi za določanje nastavitev, Seq# - zaščita proti ponovitvi komunikacije)



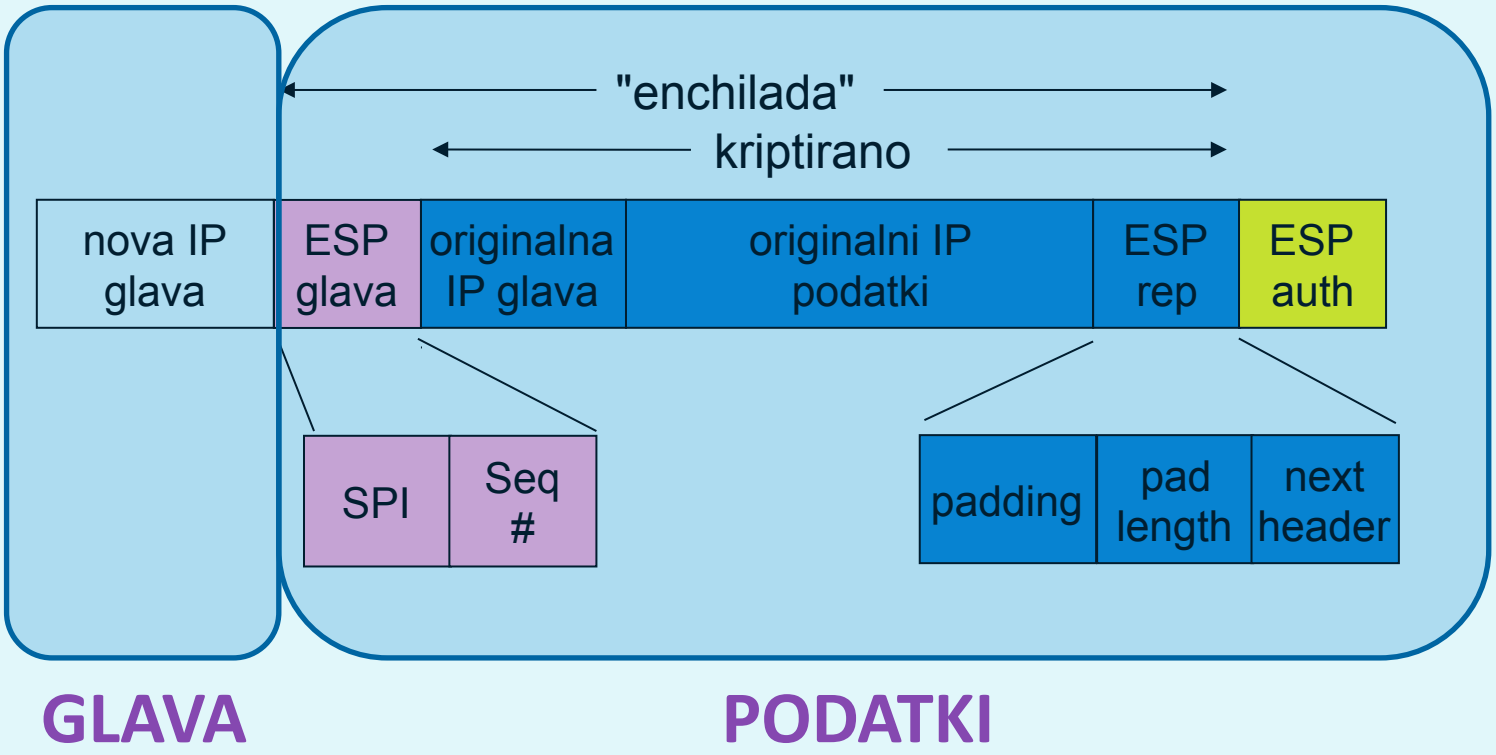
IPsec datagram: tunnel mode in ESP

- doda se polje ESP auth, ki je izračunana zgoščena vrednost cele "*enchilade*". Algoritem in ključ določa SA.



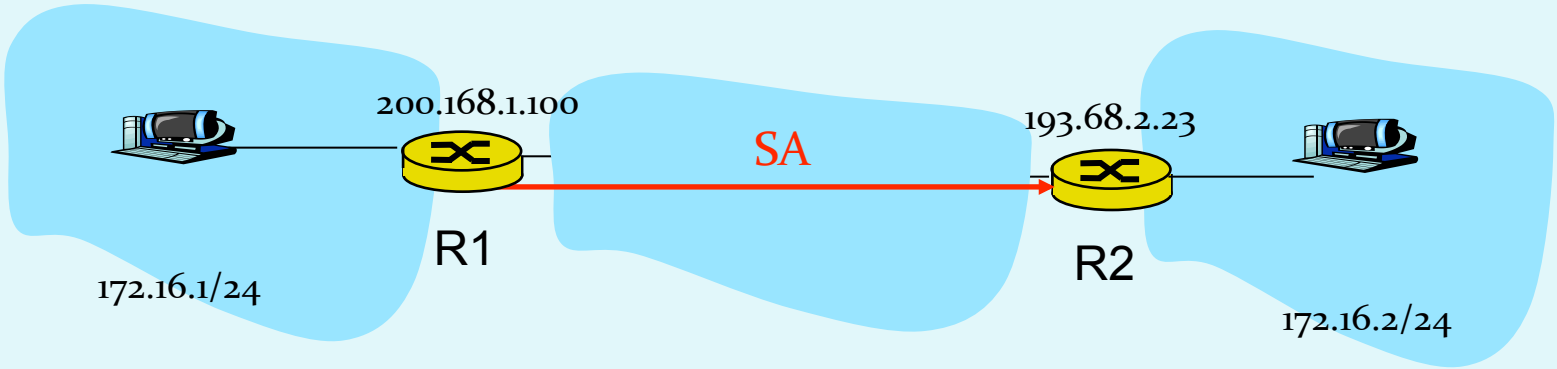
IPsec datagram: tunnel mode in ESP

- izdela se nova IP glava, ki se doda pred podatke
- oblikuje se nov IP paket, ki se klasično pošlje skozi omrežje



IPsec datagram: tunnel mode in ESP

- Kaj je v novi glavi paketa?
  - protokol = 50 (pomeni, da so podatki ESP)
  - IP pošiljatelja in prejemnika sta vozlišči, med katerima poteka IPsec (usmerjevalnika R1 in R2)
- Kaj naredi prejemnik (R2)?
  - iz SPI v glavi poišče podatke o SA, preveri MAC enchilade, preveri Seq#, odkodira enchilado, odstrani zapolnitev, ekstrahira podatke, posreduje ciljnemu računalniku



Kako izbrati datagrame za IPsec zaščito?

- To določa *Security Policy Database* (SPD): določa, ali naj se datagram ščiti glede na izvorni IP, ponorni IP in tip protokola
- Določa, kateri SA naj se uporabi

- SPD določa “KAJ” narediti z datagramom
- SAD določa "KAKO" to narediti!

Kakšno zaščito ponuja IPsec?

- Denimo, da je Janez naš *man-in-the-middle* med R1 in R2. Janez ne pozna ključev. Kaj lahko naredi?
  - Ali lahko vidi vsebino datagrama, izvor, ponor, protokol, port?
  - Ali lahko spremeni bite v paketu?
  - Ali lahko pošilja v imenu R1?
  - Ali lahko ponovi komunikacijo?