Sigurnost u Internetu

Virtualne privatne mreže

Creative Commons





- **slobodno smijete:**
  - **dijeliti** — umnožavati, distribuirati i javnosti priopćavati djelo
  - **remiksirati** — prerađivati djelo
- **pod sljedećim uvjetima:**
  - **imenovanje**. Morate priznati i označiti autorstvo djela na način kako je specificirao autor ili davatelj licence (ali ne način koji bi sugerirao da Vi ili Vaše korištenje njegova djela imate njegovu izravnu podršku).
  - **nekomercijalno**. Ovo djelo ne smijete koristiti u komercijalne svrhe.
  - **dijeli pod istim uvjetima**. Ako ovo djelo izmijenite, preoblikujete ili stvarate koristeći ga, preradu možete distribuirati samo pod licencom koja je ista ili slična ovoj.

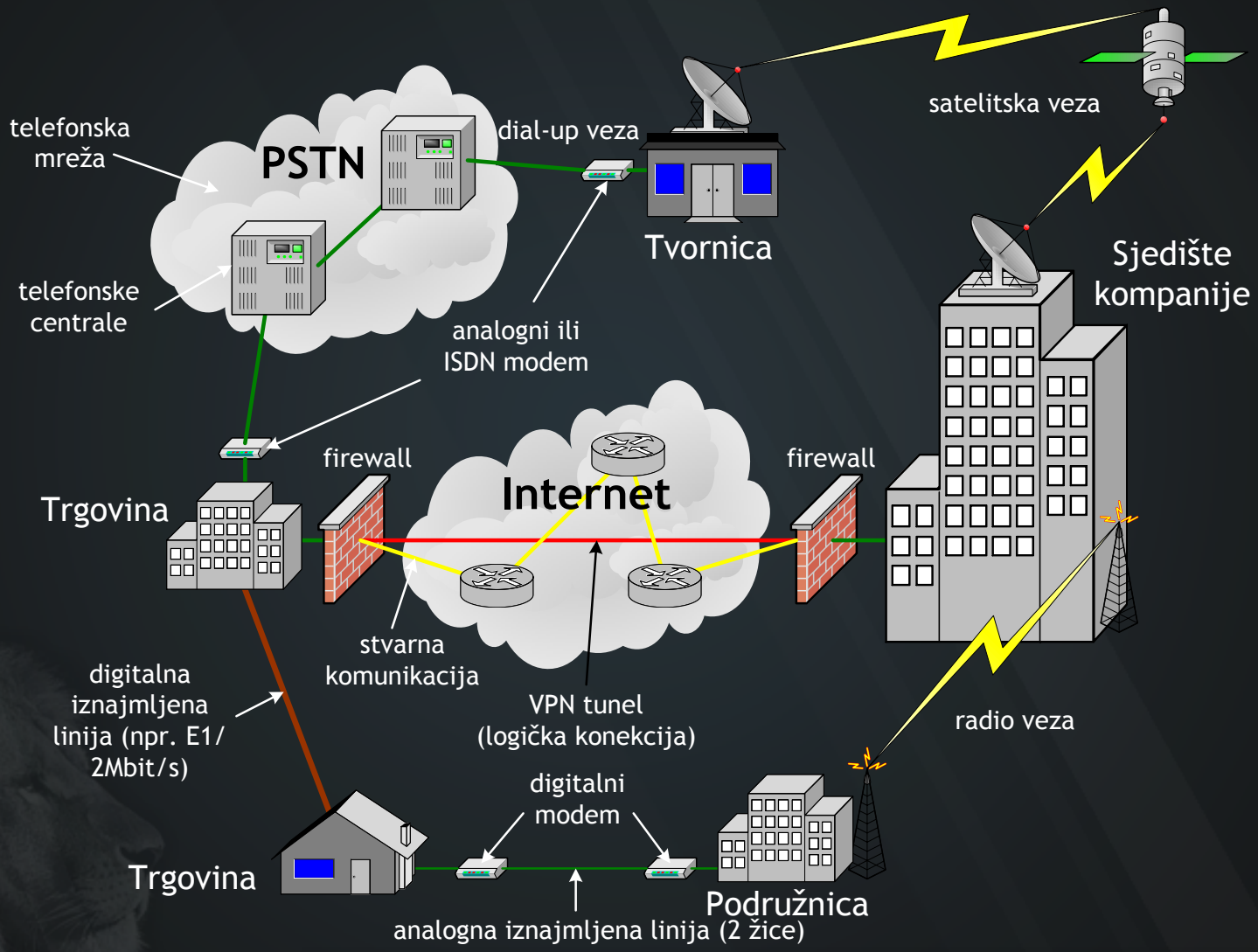
U slučaju daljnjeg korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom na ovu internetsku stranicu. Od svakog od gornjih uvjeta moguće je odstupiti, ako dobijete dopuštenje nositelja autorskog prava. Ništa u ovoj licenci ne narušava ili ograničava autorova moralna prava.

Tekst licencije preuzet je s http://creativecommons.org/.

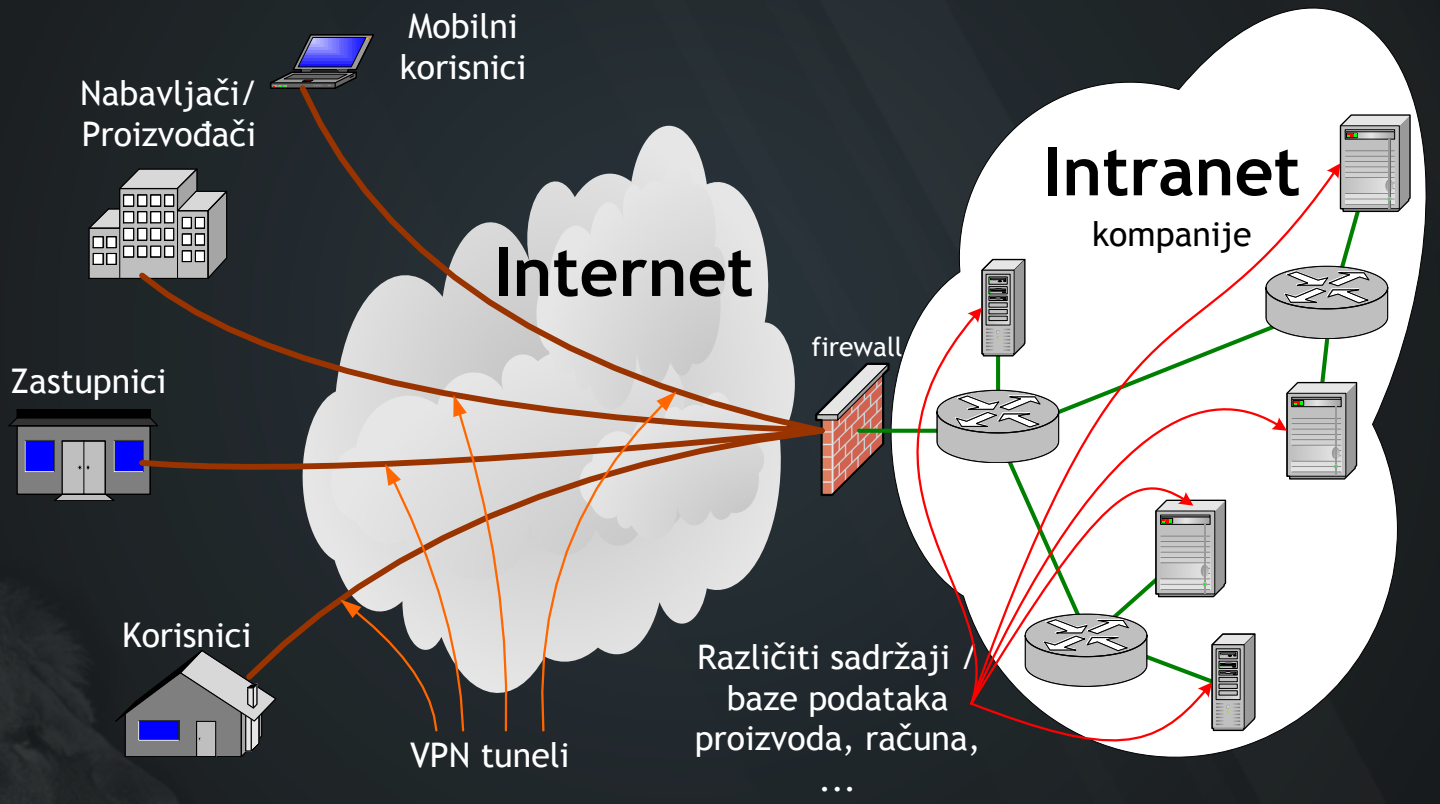
Internet/Intranet/Extranet

- Internet - javna mreža
- Intranet
  - privatna mreža (unutar kompanije, institucije)
    - korisnici unutar institucije
  - tehnologija ista kao i kod Internet-a
  - obično se koriste privatne IP adrese, no mogu se koristiti i javne
    - pod uvjetom da IP paketi nikada ne budu poslani na Internet
  - različite lokacije kompanije se povezuju preko WAN ili VPN veza
- Extranet
  - proširenje pojma Intranet
  - korisnici i izvan kompanije/institucije
    - dobavljači, proizvođači, partneri, korisnici
  - sigurnost i privatnost

Intranet - primjer



Extranet - primjer



Udaljeni pristup Intranetu

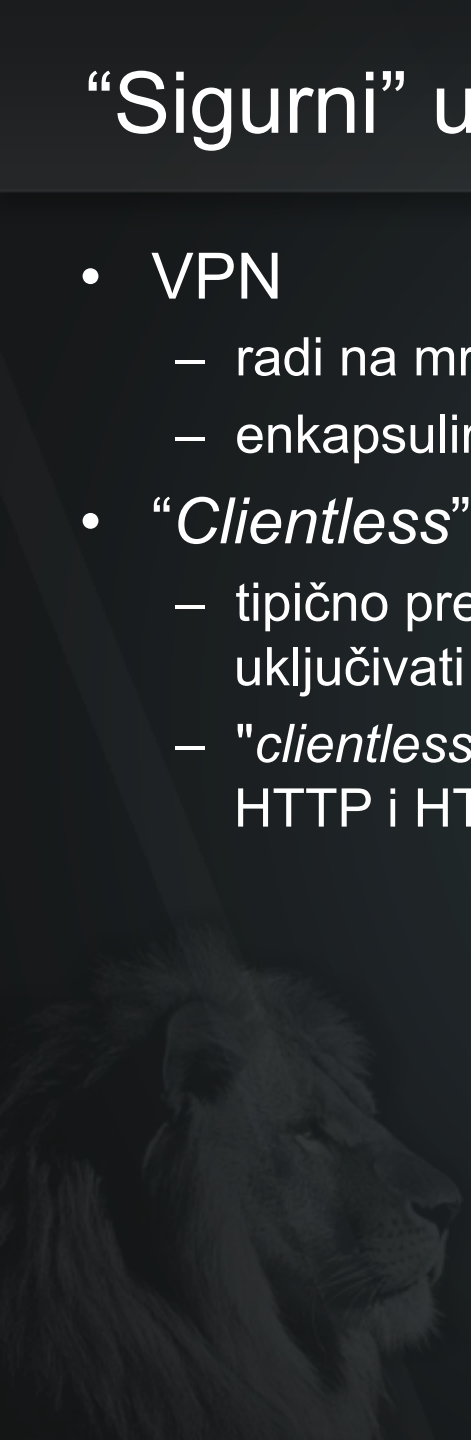
- zahtjevi:
  - privatnost – integritet podataka
    - korištenje enkripcijskih mehanizama na strani klijenta i servera:
      - protokol za sigurnu razmjenu kriptografskih ključeva (na primjer IKE, SSL),
      - algoritmi za enkripciju i
      - metode provjere integriteta podataka.
  - umrežavanje
    - podrška za korištenje IP protokola i mrežne infrastrukture:
      - mogućnost rada iza vatrozida, uz prisutne NAT (Network Address Translation) uređaje i *proxy* poslužitelje,
      - korištenje dinamički dodijeljenih IP adresa.
  - upravljivost
  - kontrola pristupa

Udaljeni pristup Intranetu

- (zahtjevi:)
  - upravljivost
    - korištenje različitih načina autentifikacije (na primjer korištenje digitalnih certifikata X.509, standardnih lozinki operacijskog sustava i slično)
    - korištenje direktorija (LDAP, RADIUS, Active Directory) za pohranjivanje i održavanje informacija o korisnicima.
  - kontrola pristupa
    - mogućnost administriranja nivoa pristupa:
      - enkripcijske tehnike mogu osigurati privatnost i integritet podataka ali one ne pridjeljuju prava pristupa korisnicima
      - ako korisnik može uspostaviti VPN tunel (bez obzira na korištenu tehnologiju) to ne znači da smije imati pristup svim resursima mreže.

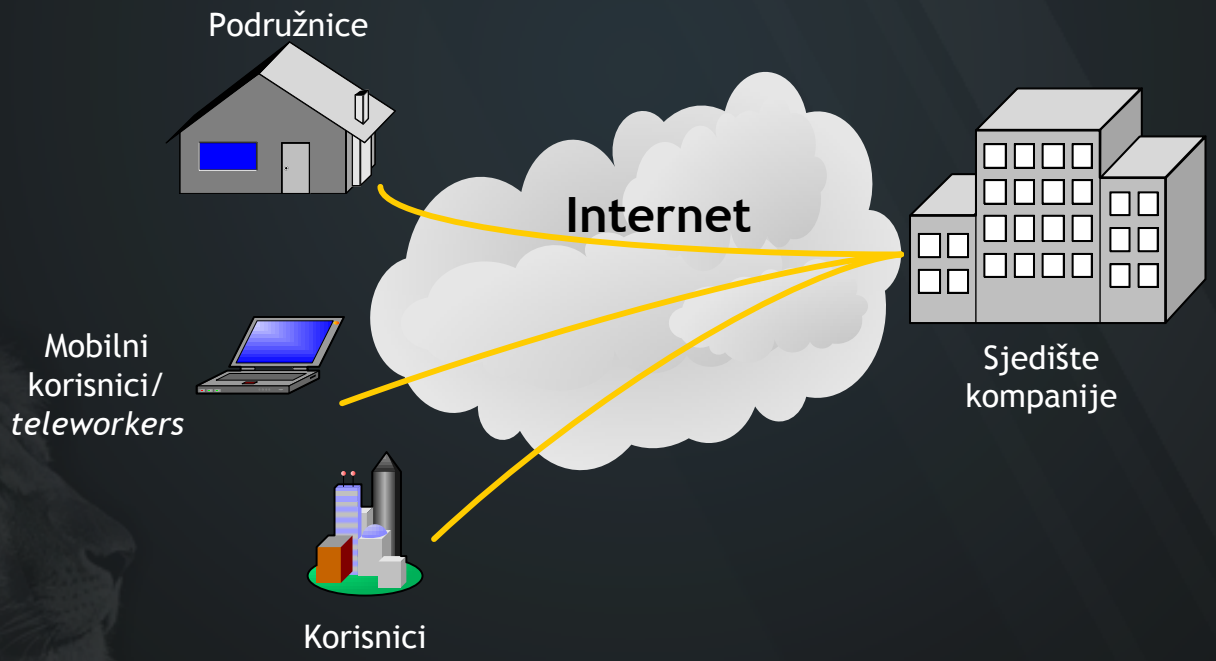
“Sigurni” udaljeni pristup intranetu

- VPN
  - radi na mrežnom sloju, nezavisan o aplikaciji,
  - enkapsulira originalne IP pakete unutar svog vlastitog paketa
- “*Clientless*” VPN
  - tipično predstavlja VPN temeljen na korištenju HTTPS ali može uključivati i aplikacije koje koriste SSL,
  - "*clientless*" jer računalo već ima Web preglednik koji podržava HTTP i HTTPS



Virtualne privatne mreže

- komunikacijske veze ostvarene preko jeftinije dijeljene infrastrukture
  - na primjer Interneta
  - ista (sigurnosna) politika i performanse kao i privatne mreže realizirane preko infrastrukture WAN

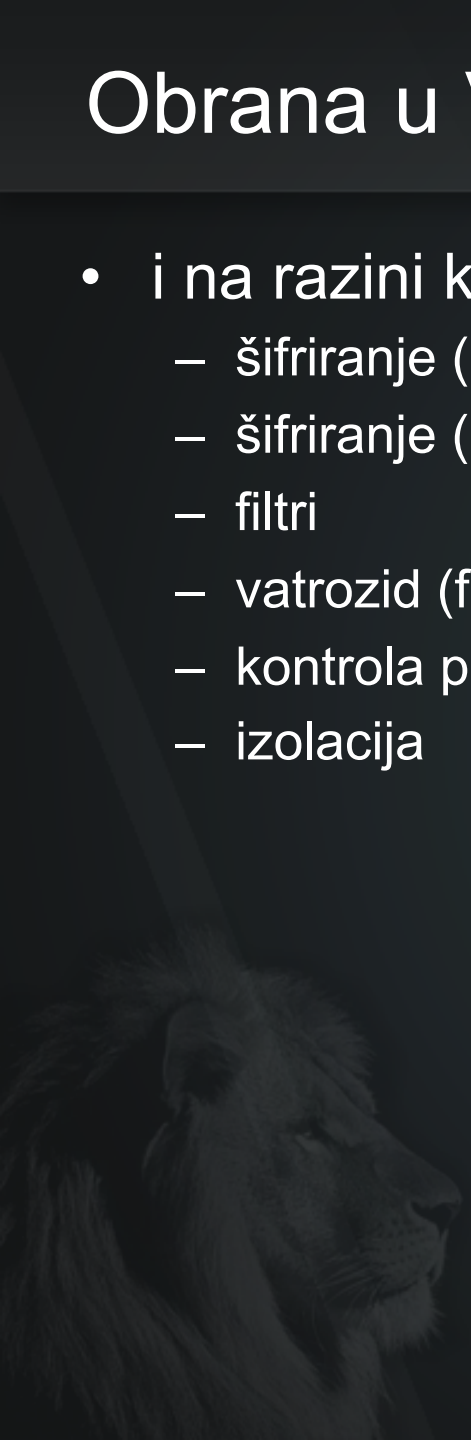


Prijetnje u VPN-ovima

- pitanja:
  - neovlašteni pristup prometu VPN-a
  - izmjena sadržaja prometa VPN-a
  - ubacivanje neovlaštenog prometa u VPN (*spoofing*)
  - brisanje i uništavanje prometa VPN-a
  - napadi uskraćivanjem usluge (DoS)
  - napadi na infrastrukturu mreže preko programske podrške za upravljanje mrežom
  - izmjene konfiguracije VPN-a
  - napadi na protokole VPN-a
- Internet služi samo kao transport

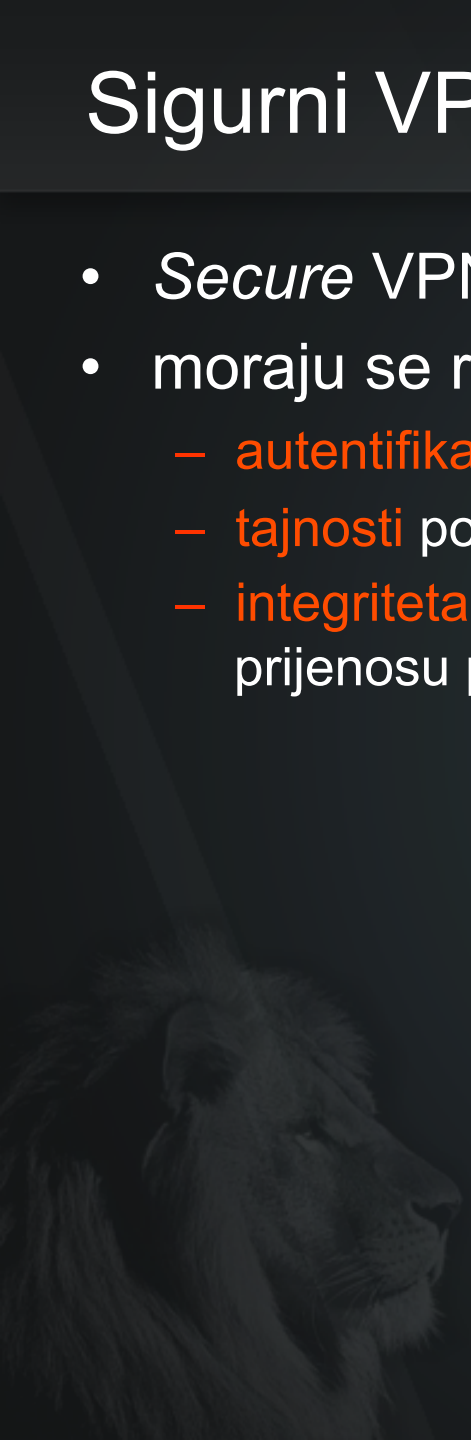
Obrana u VPN-ovima

- i na razini korisnika i na razini davatelja usluge VPN-a:
  - šifriranje (kriptozaštita) paketa
  - šifriranje (kriptozaštita) kontrolnog prometa
  - filtri
  - vatrozid (firewall)
  - kontrola pristupa
  - izolacija



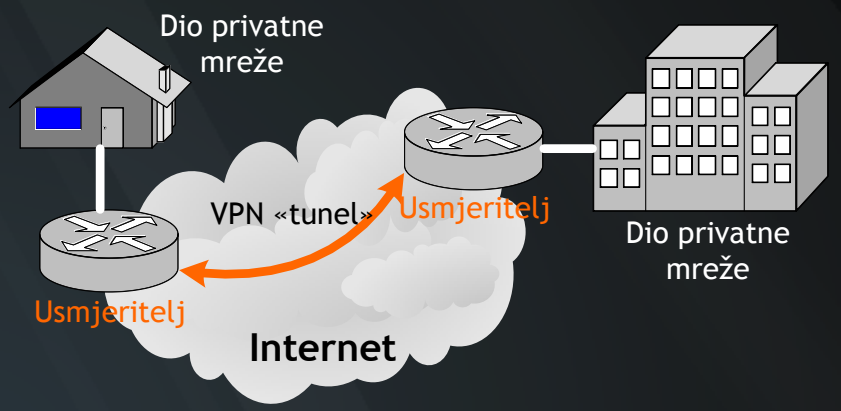
Sigurni VPN

- *Secure* VPN
- moraju se riješiti pitanja:
  - autentifikacije entiteta (korisnika, računala)
  - tajnosti podataka – zaštita od neovlaštenog pristupa podacima
  - integriteta podataka – zaštita od neovlaštene izmjene podataka u prijenosu preko javne IP mreže (Internet)

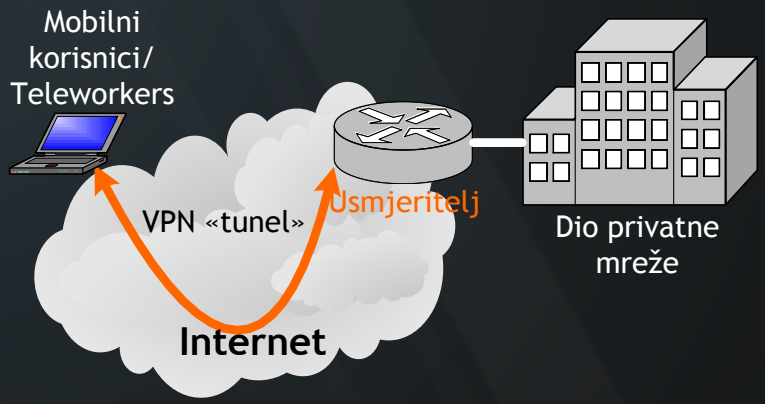


Vrste VPN-a

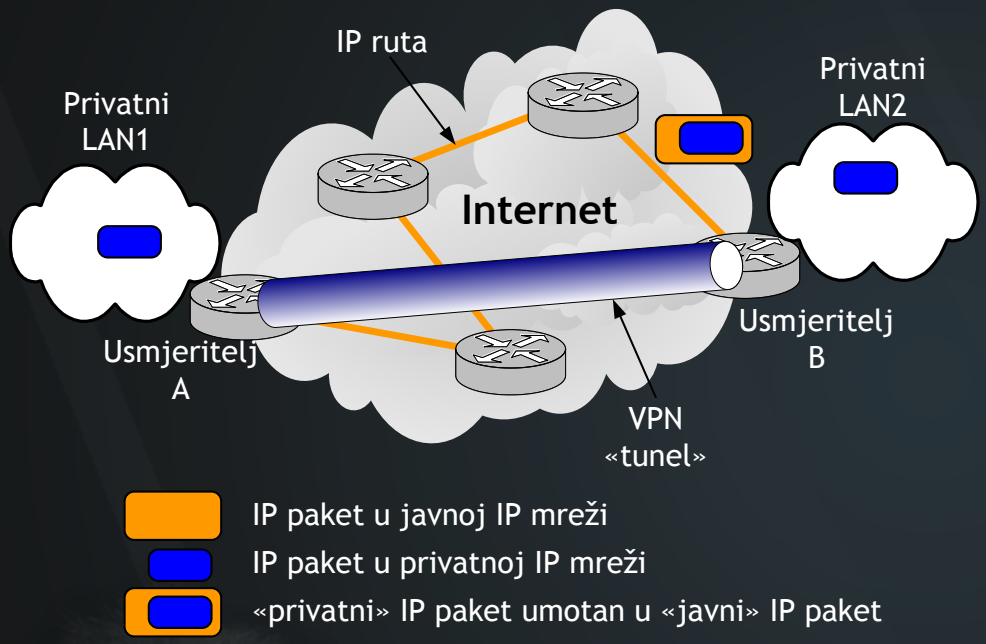
- od točke do točke (*Site-to-site*)
  - između dva mrežna entiteta (na primjer usmjeritelja)
  - privatne i zaštićene mreže iza oba entiteta



- udaljeni pristup (*Remote Access*)
  - između uređaja i usmjeritelja
  - na udaljenoj lokaciji ne nalazi se zaštićena mreža



Tuneliranje u VPN-ovima

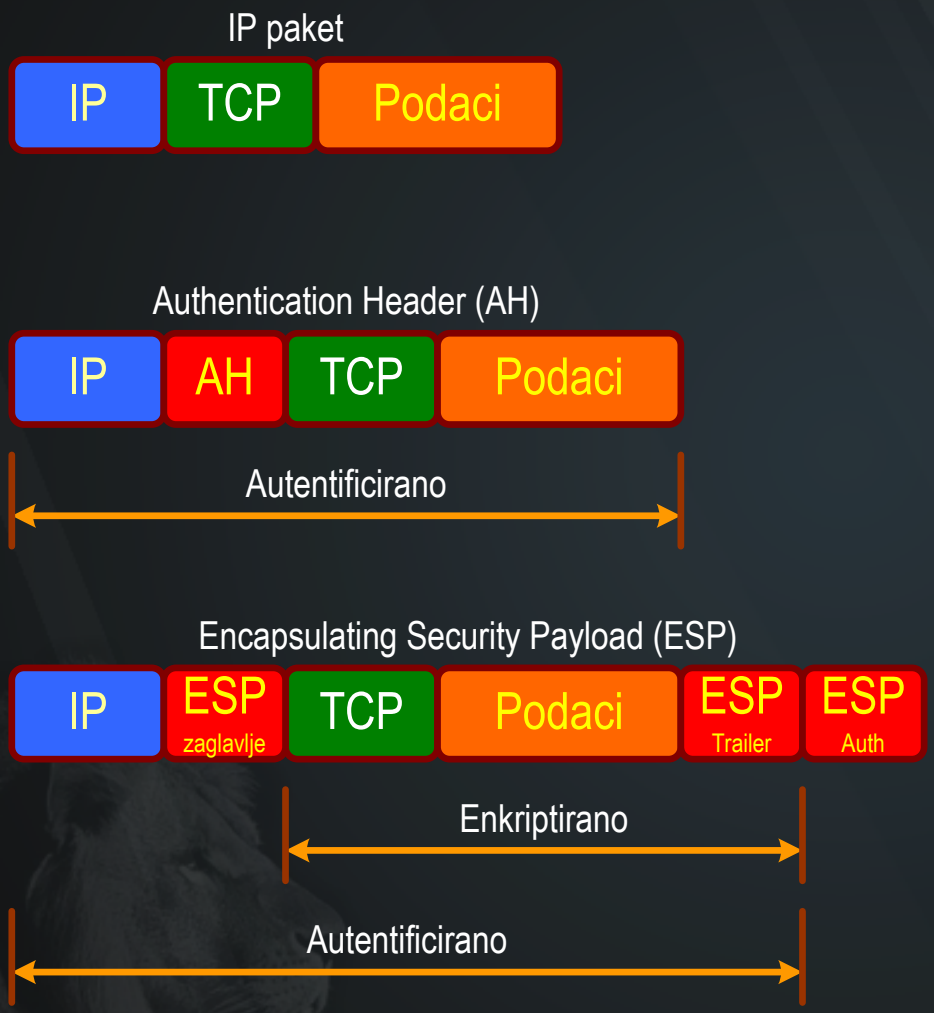


- privatna i javna mreža koriste različito IP adresiranje
- tunel: “privatni” IP paketi “umataju” se u “javne” IP pakete (šifriranje “privatnog” IP paketa)
- tehnologije tuneliranja:
  - L2TP – Layer 2 Tunneling Protocol (Cisco)
  - PPTP – Point-to-Point Tunneling Protocol (Microsoft)
  - IPSec – IP Security
    - IETF standard
- tuneliranje se koristi s nekom tehnologijom za autentifikaciju
  - RADIUS

IPsec

- ideja: poboljšana sigurnost za IPv4 i IPv6
- rješenje na mrežnom (IP) sloju, osigurava sigurnosne usluge sloju IP i svim višim slojevima
- uspostavljanje i upravljanje sigurnim komunikacijama između mrežnih entiteta; omogućava šifriranje i autentifikaciju
- Internet Standard (RFC),
- primjene: virtualna privatna mreža, sigurni pristup udaljenom računalu, elektronička trgovina, ...
- temelji se na:
  - sigurnosnim protokolima
  - kriptografskim algoritmima za šifriranje i algoritmima za vjerodostojnost
  - uporabi procedura i protokola za upravljanje kriptografskim ključevima

IPsec: AH i ESP

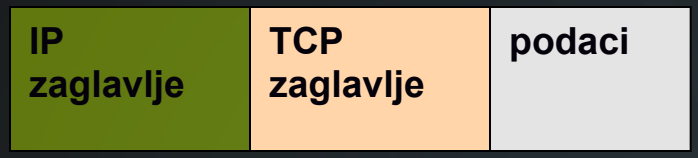


Sigurnosni protokoli

- Authentication Header (**AH**)
  - osigurava autentičnost izvora podataka i integritet niza IP datagrama
  - onemogućuje i napade izvedene ponovljenim slanjem snimljenog prometa
  - primjena: kada ne treba povjerljivost
- Encapsulating Security Payload (**ESP**)
  - prvenstveno osigurava povjerljivost komunikacije
  - koliko je povjerljivost "jaka" ovisi o izboru algoritma šifriranja
  - dodatna mogućnost je primjena autentifikacijskog algoritma uz algoritam šifriranja, koja dodaje autentičnost i zaštitu od napada pomoću ranije snimljenog prometa
    - napomena: u tom slučaju zaglavlje IP datagrama "izvan" ESP zaglavlja nije autentificirano

Načini rada (vrijedi za AH i za ESP protokol)

- izvorni IP datagram

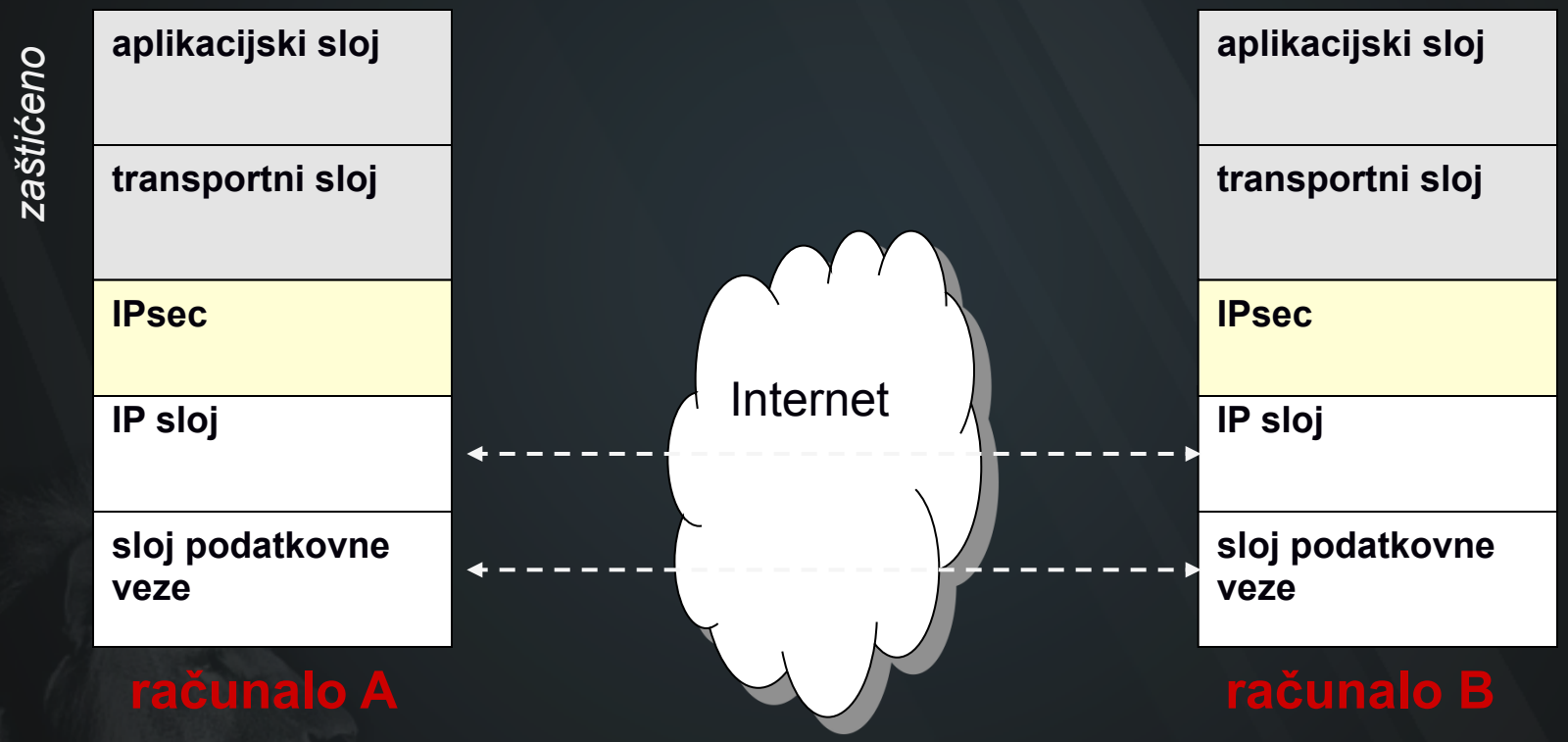


- **transportni način:** štiti podatke protokola viših slojeva (od transp. na više)

- **tunelirani način:** primjena SA na tunel; štiti cijeli izvorni IP paket

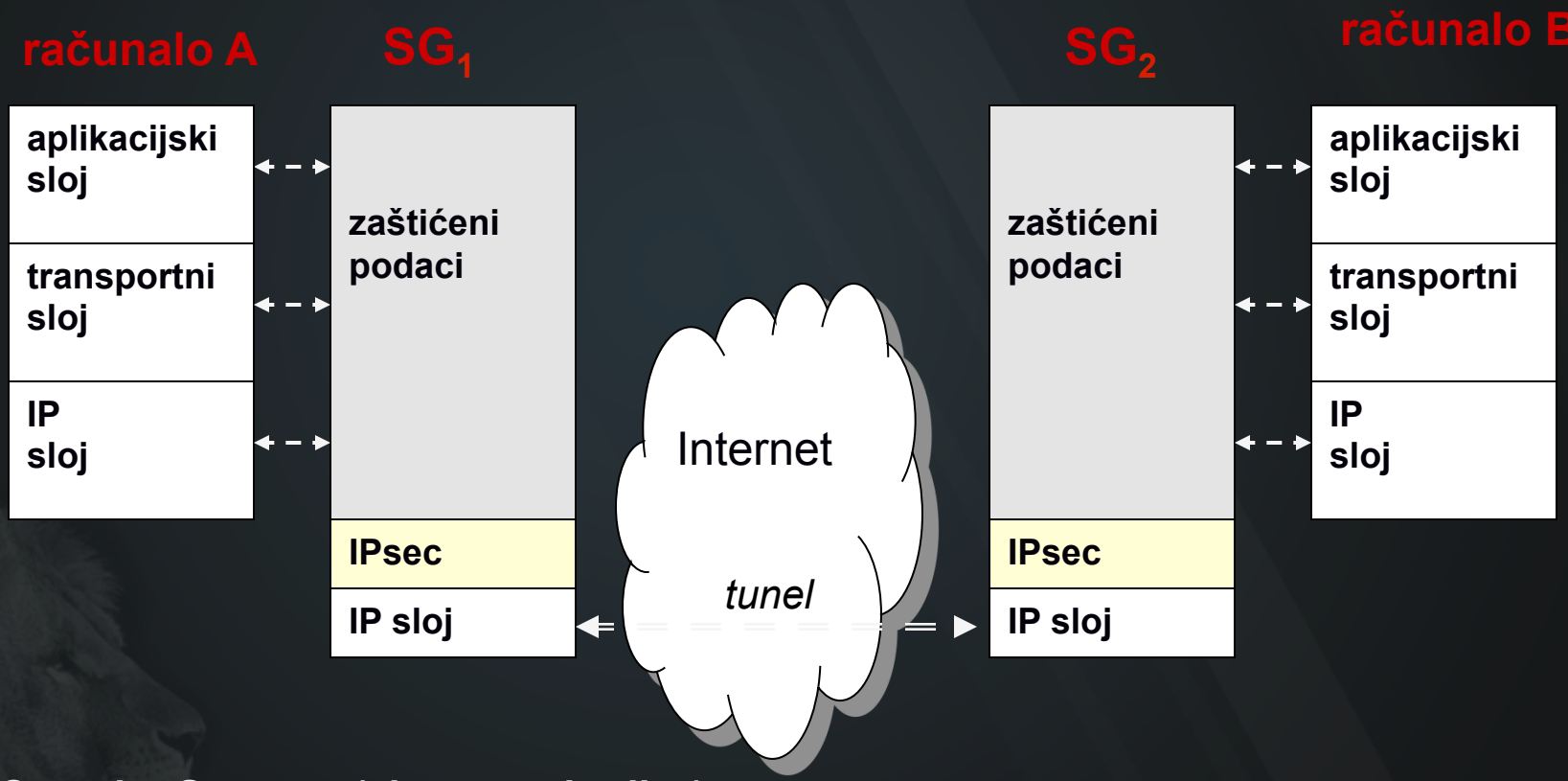
Transportni način

- krajnje točke: krajnje računalo – krajnje računalo



Tunelirani način

- krajnje točke: krajnje računalo – mrežni uređaj (A-SG_2) ili između dva mrežna uređaja (SG_1-SG_2)

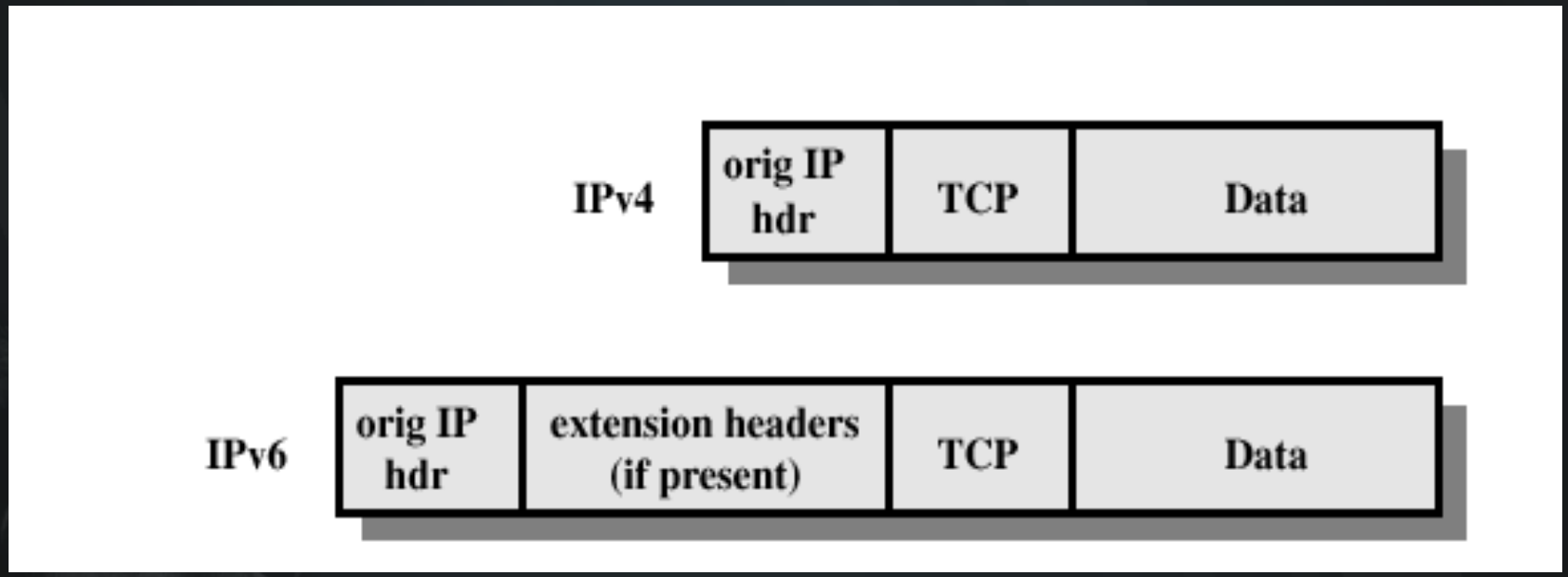


SG = Security Gateway (sigurnosni prilaz)

Razrada načina rada i utjecaja AH i ESP

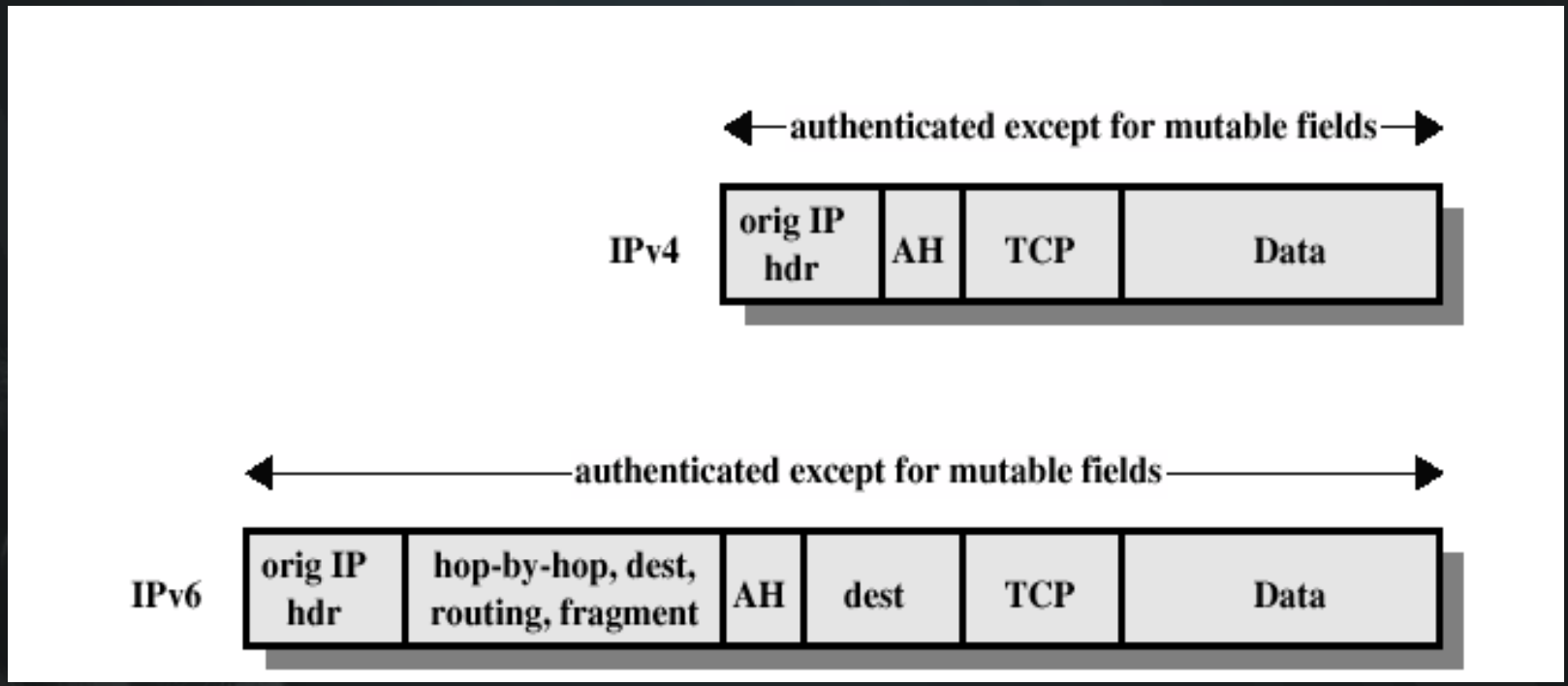
- u sljedećih osam slika proučit ćemo svojstva SA uz primjenu AH i ESP u **transportnom** i **tuneliranom** načina rada - što se osigurava i kako

- počinjemo od standardnog IP datagrama (IPv4 ili IPv6)



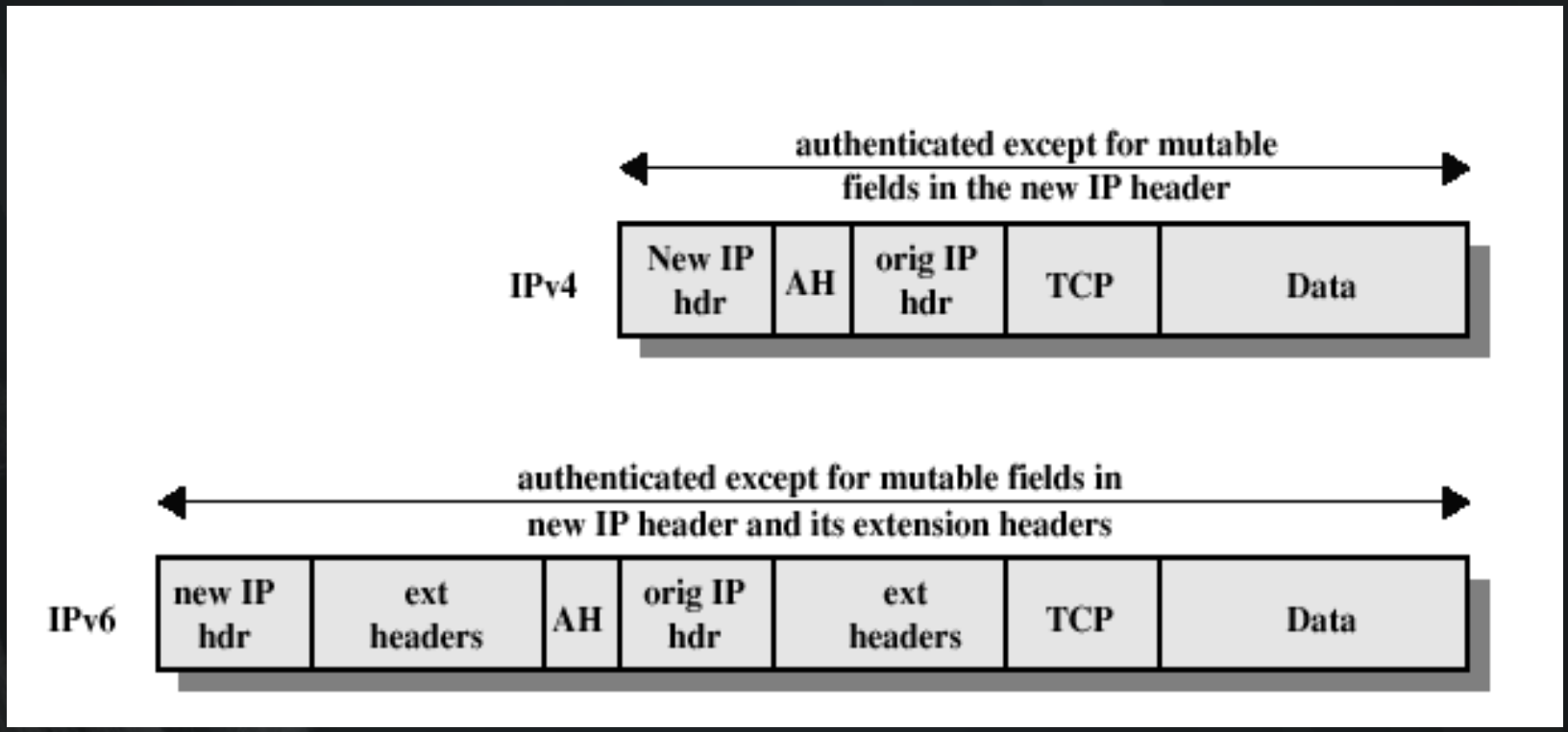
AH u transportnom načinu

- IPv4 - AH zaglavlje dolazi prije TCP zaglavlja i podataka
- IPv6 - AH zaglavlje dolazi poslije dijela dodatnih zaglavlja, a prije TCP zaglavlja i dodatnih zaglavlja namijenjenih odredištu
- SA osigurava vjerodostojnost svih polja osim onih koja se mijenjaju pri prolasku kroz mrežu (na pr. TTL)



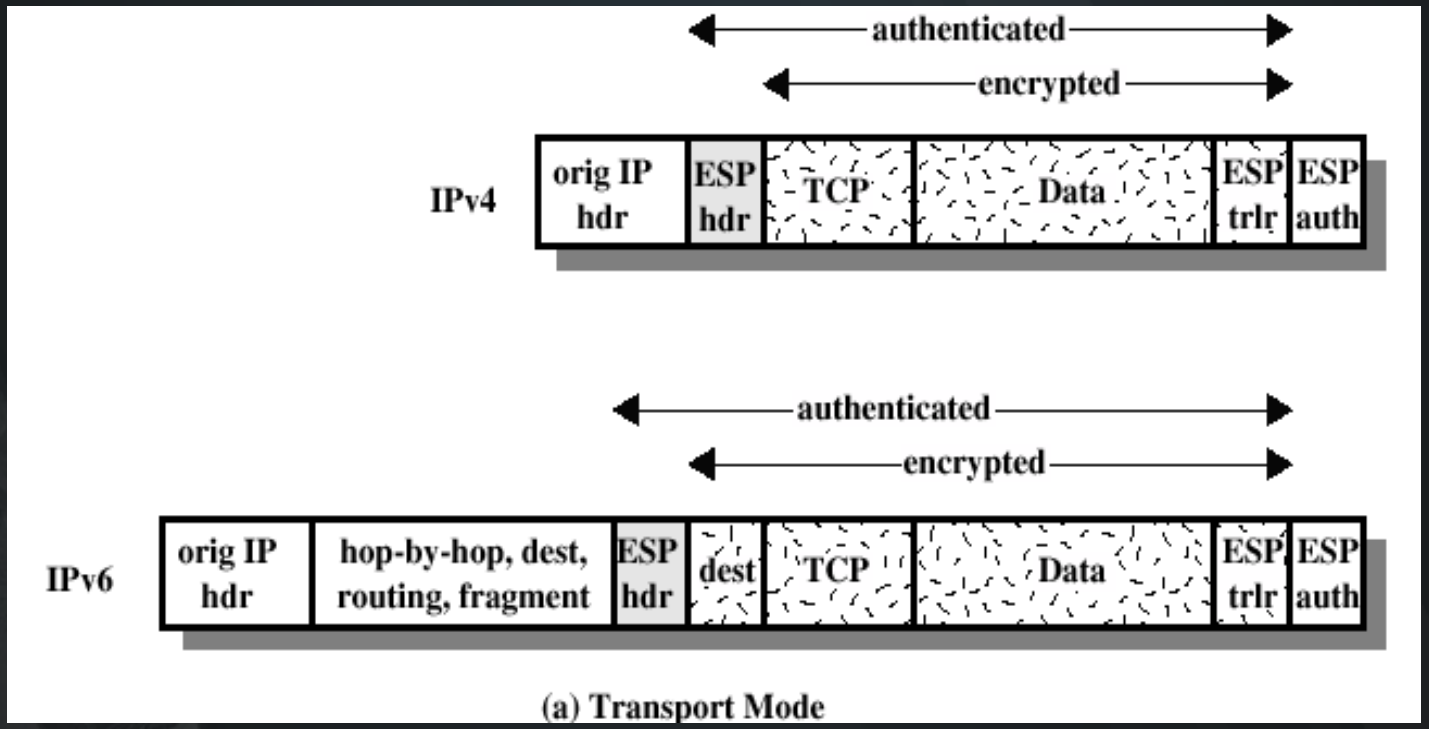
AH u tuneliranom načinu

- IPv4 i IPv6 - datagram se ovija novim datagramom
- osigurana vjerodostojnost svih polja, osim onih koja se mijenjaju pri prolasku kroz mrežu



ESP (s AH opcijom) u transportnom načinu

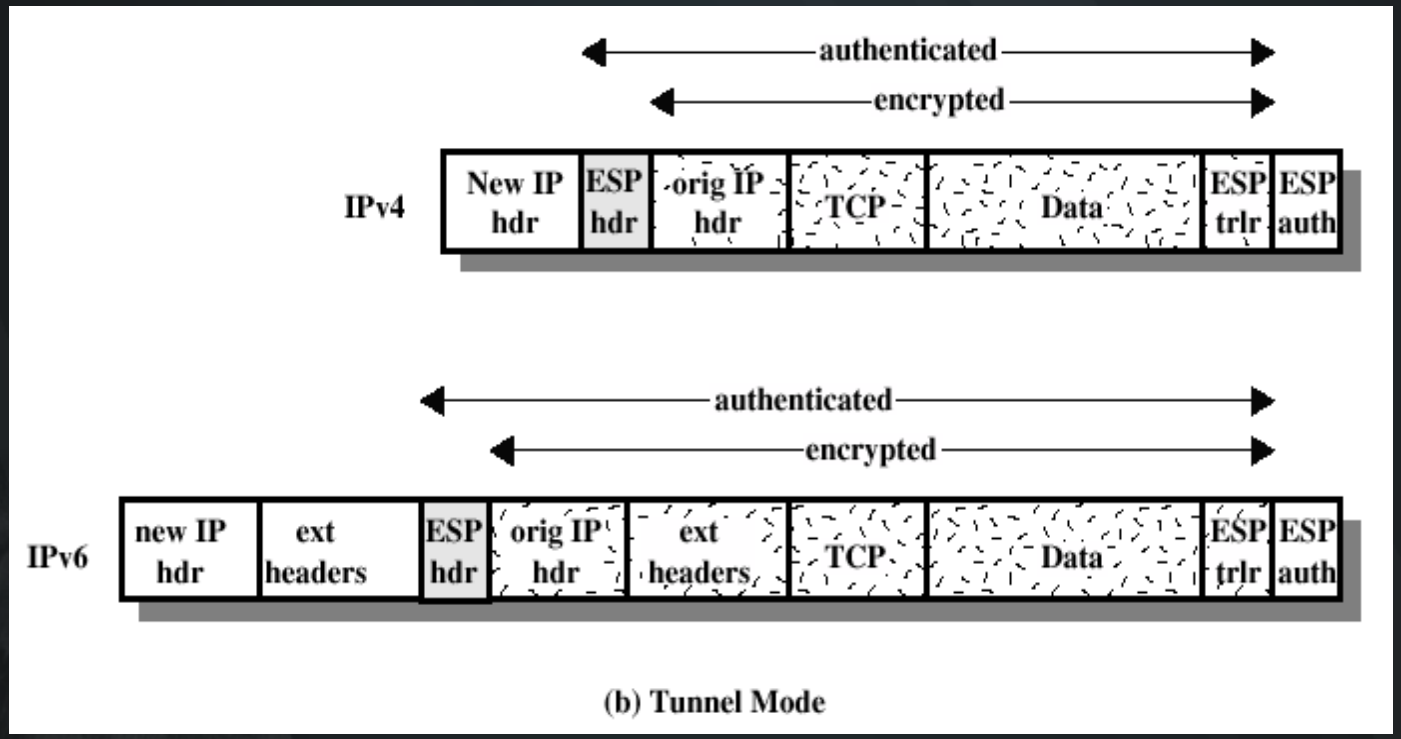
- IPv4: ESP paket obavija i šifrira TCP zaglavlje i podatke, a podaci za provjeru vjerodostojnosti (AH opcija, izborno) slijede na kraju
- IPv6: ESP paket obavija i šifrira TCP zaglavlje i podatke i dodatna zaglavlja namijenjena odredištu



(a) Transport Mode

ESP (s AH opcijom) u tuneliranom načinu

- IPv4 i IPv6: datagram se ovija novim datagramom; osigurana povjerljivost cijelog originalnog IP datagrama

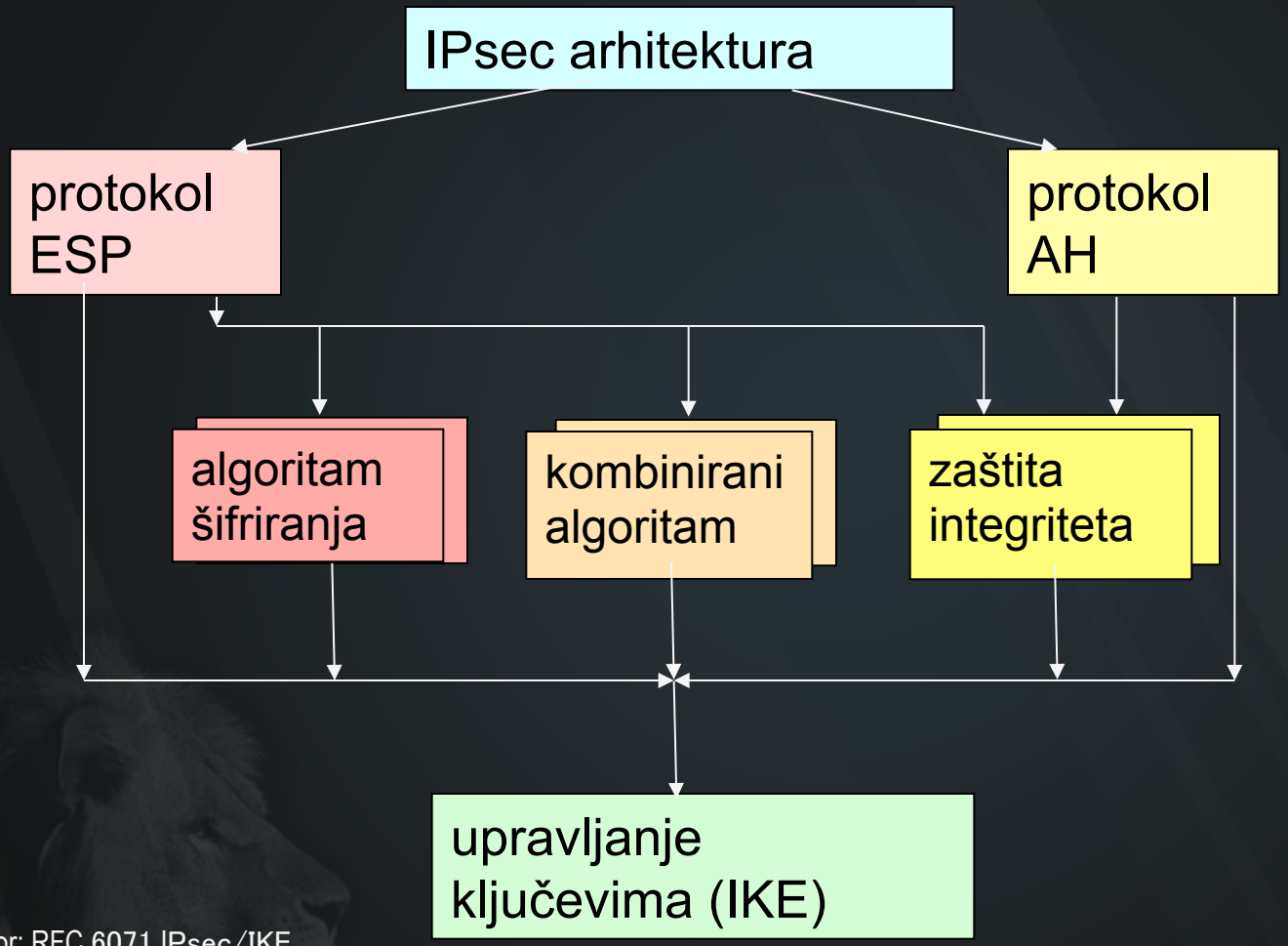


(b) Tunnel Mode

Pregled svojstava sigurnosne asocijacije

	Sigurnosna asocijacija u **transportnom** načinu	Sigurnosna asocijacija u **tuneliranom** načinu
AH	osigurava vjerodostojnost IP tereta i dijela IP zaglavlja osigurava vjerodostojnost dodatnih zaglavlja IPv6	osigurava vjerodostojnost cijelog "unutarnjeg" IP paketa i djelomično "vanjskog" IP zaglavlja
ESP (samo šifriranje)	šifrira teret IP datagrama šifrira IPv6 dodatna zaglavlja	šifrira "unutarnji" IP paket
ESP (šifriranje i vjerodostoj-nost)	šifrira teret IP datagrama šifrira IPv6 dodatna zaglavlja osigurava vjerodostojnost IP tereta, ali ne i samog IP zaglavlja	šifrira "unutarnji" IP paket osigurava vjerodostojnost cijelog "unutarnjeg" IP paketa

Pregled IPsec dokumenata



sigurnosni protokoli

algoritmi za šifriranje i vjerodostojnost

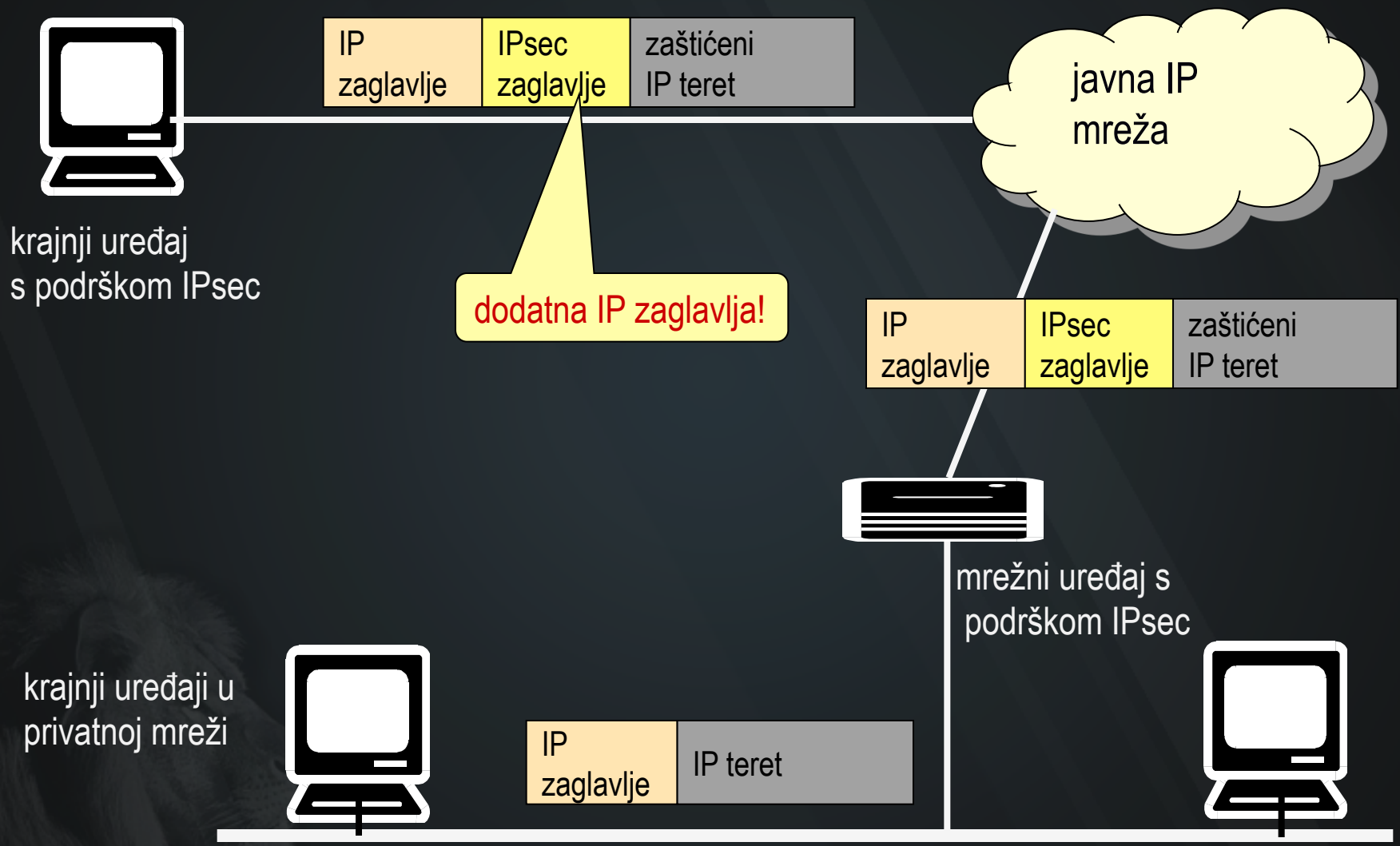
upravljanje ključevima

Izvor: RFC 6071 IPsec/IKE Document Roadmap

Pregled IPsec dokumenata (2)

- IPsec arhitektura, osnovni dokument
  - RFC 4301, "Security Architecture for the Internet Protocol"
- sigurnosni protokoli
  - AH (RFC 4302) i ESP (RFC 4303)
- algoritmi za šifriranje i algoritmi za vjerodostojnost
  - RFC 7321 - definira obavezne algoritme za AH i ESP
  - posebni RFC za svaki kriptografski algoritam (IPsec je neovisan o algoritmu!)
- automatsko upravljanje kriptografskim ključevima
  - "Internet Key Exchange (IKEv2) Protocol" (RFC 7296)
  - kriptografski algoritmu za uporabu u IKEv2 (RFC 4307)

Primjer: Sigurna komunikacija uz IPsec



Prednosti IPsec arhitekture

- IPsec je izveden ispod transportnog sloja
  - za potpunu funkcionalnost (ipak) potrebna prilagodba aplikacija i API-ja
  - može se izvesti u krajnjem korisnikovom računalu ili u mrežnom uređaju: vatrozidu (*firewall*) ili usmjeritelju
- ako je IPsec zaključen u vatrozidu ili usmjeritelju, uređaj osigurava granicu prema ostatku mreže
  - lokalni promet se ne opterećuje sigurnosnim mehanizmima
  - osiguran je siguran pristup s autentificiranog mrežnog sučelja iz vanjske mreže
  - omogućeno je sigurno povezivanje dislociranih mreža, npr. na raznim lokacijama iste tvrtke, preko nesigurnog javnog Interneta (primjena: virtualna privatna mreža)
- kod usmjeravanja, IPsec osigurava identitet usmjeritelja

Sigurnosne usluge IPsec arhitekture

- kontrola pristupa
  - “sigurnosna granica” između zaštićenih i nezaštićenih sučelja
- cjelovitost na razini datagrama
  - cjelovitost nekonekcijskog toka, npr. UDP prometa
- vjerodostojnost izvora datagrama
- zaštita protiv napada ponovnim slanjem snimljenog prometa
  - vrsta napada pri kojem se ponovnim slanjem snimljenih paketa (npr. prilikom prijave na sustav) pokušava neovlašteno ostvariti pristup ili neka radnja na sustavu
- povjerljivost (šifriranje prometa)
- ograničena povjerljivost prometnog toka
  - izvorišna i odredišna IP adresa su vidljive, ali se ne vidi izvor i odredište na transportnom sloju (port)

Pojam sigurnosne asocijacije (SA)

- sigurnosna asocijacija (*Security Association*, SA): *jednosmjerna "veza"* koja prometu koji se odvija preko nje pruža odabranu sigurnosnu uslugu
- svaka strana zasebno stvara SA, posebno za AH i ESP (ne oba u istoj SA)

- SA je definirana s tri parametra:
  - Security Parameter Index, SPI (lokalni identifikator sigurnosne asocijacije)
  - odredišna IP adresa (očitana iz standardnog zaglavlja IPv4 ili IPv6 datagrama)
  - identifikator sigurnosnog protokola (odabir: AH ili ESP)

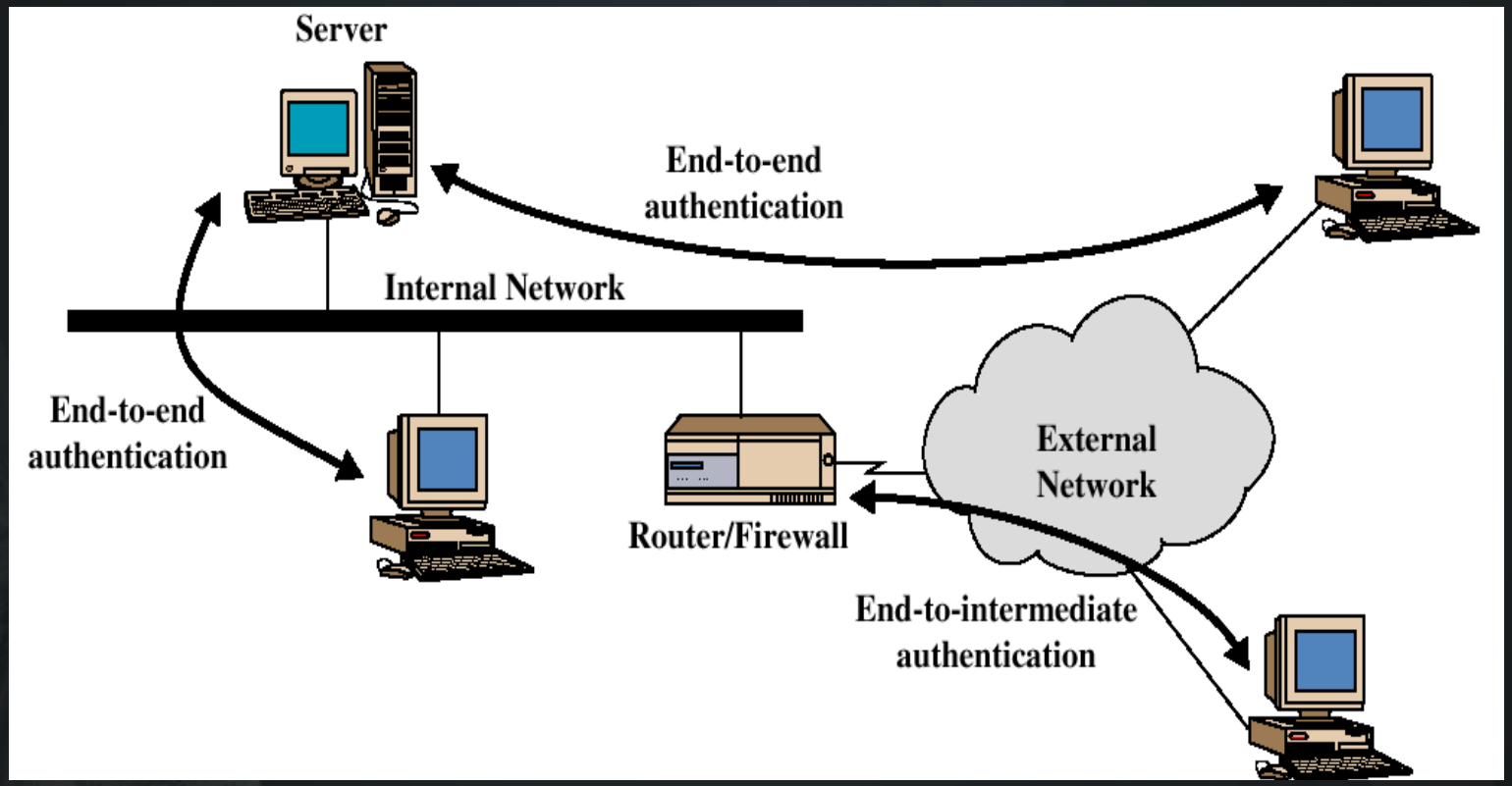
- dogovor dva "peer" sustav (iste razine) oko sigurnosne politike:
  - kako će podaci biti šifrirani (DES, 3DES)
  - hash (MD5 ili SHA)
  - kako će se entiteti autentificirati
  - dijeljeni ključevi sesije
  - koliko će asocijacija trajati (vrijeme života)
  - postoji baza podataka Security Association Database
    - svaki zapis povezan s Security Policy Database

Sigurnosne usluge za SA

- skup sigurnosnih usluga koje pruža SA ovisi o:
  - odabranom protokolu
    - Authentication Header - AH
    - Encapsulating Security Payload - ESP
  - načinu rada
    - tunelirani
    - transportni
  - krajnjim točkama SA
    - krajnji uređaj (npr. računalo)
    - mrežni uređaj (npr. usmjeritelj)
  - izboru dodatnih funkcija unutar protokola

Raspon osiguravanja vjerodostojnosti

- između krajnjih sudionika u komunikaciji (*end-to-end*)
- između krajnjeg sudionika i posrednika (*end-to-intermediate*)



Algoritmi za vjerodostojnost za AH

- različite izvedbe IPsec moraju imati najmanje jedan zajednički algoritam da bi bile kompatibilne
- RFC 4835 - popis dozvoljenih kriptografskih algoritma za protokole ESP i AH i stupanj zahtjevanosti njihove izvedbu

- Algoritmi uz AH (RFC 4835)

Zahtjev	Algoritam vjerodostojnosti (napomene)
MUST	HMAC-SHA1-96 [RFC2404]
SHOULD+	AES-XCBC-MAC-96 [RFC3566]
MAY	HMAC-MD5-96 [RFC2403] (slabosti otkrivene za MD-5 ne bi trebale utjecati na primjenu s HMAC)

Algoritmi šifriranja i vjerodostojnosti za ESP

- Algoritmi uz ESP (RFC 4835)

Zahtjev	Algoritam šifriranja (napomene)
MUST	NULL (bez ESP-a; ne smije biti NULL istovremeno kad i AH)
MUST-	TripleDES-CBC [RFC2451]
MUST	AES-CBC with 128-bit keys [RFC3602]
SHOULD	AES-CTR [RFC3686]
SHOULD NOT	DES-CBC [RFC2405] (upitna sigurnost zbog relativno kratkog ključa)

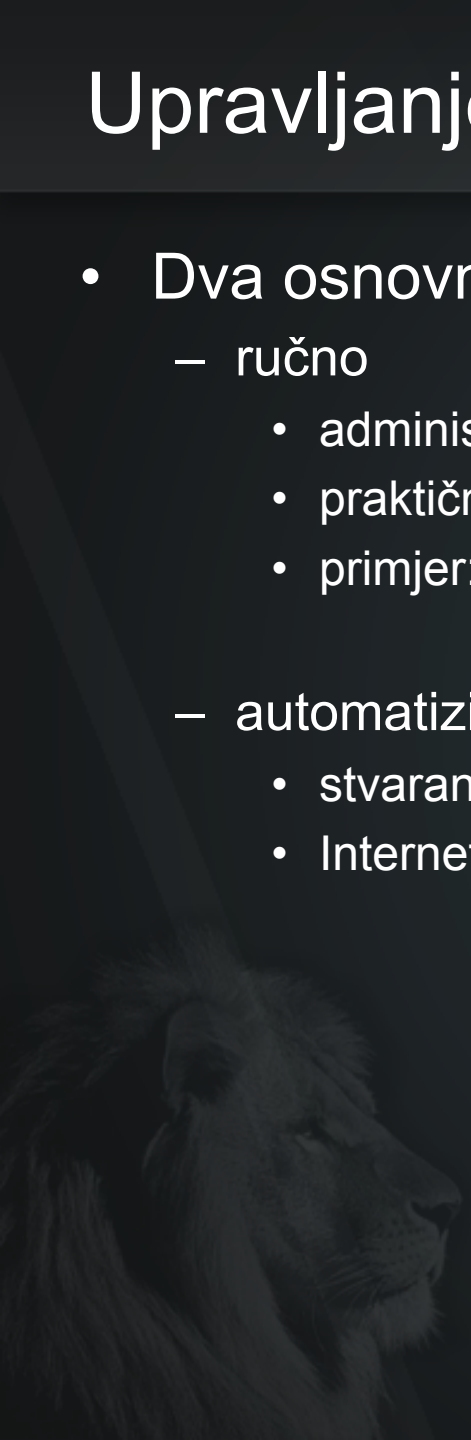
Zahtjev	Algoritam vjerodostojnosti (napomene)
MUST	HMAC-SHA1-96 [RFC2404]
MAY	NULL (bez AH; ne smije biti NULL istovremeno kad i ESP)
SHOULD+	AES-XCBC-MAC-96 [RFC3566]
MAY	HMAC-MD5-96 [RFC2403] (slabosti otkrivene za MD-5 ne bi trebale utjecati na primjenu s HMAC)

Veza sigurnosnih usluga i protokola

Sigurnosni protokol / Sigurnosna usluga	AH	ESP (samo šifriranje)	ESP (šifriranje i vjerodostojnost)
Kontrola pristupa	da	da	da
Cjelovitost na razini datagrama	da		da
Vjerodostojnost izvora podataka	da		da
Odbacivanje ponovljenih ranije snimljenih paketa	da	da	da
Povjerljvost		da	da
Ograničena povjerljivost prometnog toka		da	da

Upravljanje ključevima

- Dva osnovna načina:
  - ručno
    - administrator konfigurira svaki sustav
    - praktično samo za mala, relativno statična okruženja
    - primjer: VPN s malo odredišta
  - automatizirano
    - stvaranje ključeva na zahtjev
    - Internet Key Exchange Protocol (IKEv2) (RFC 7296)



Internet Key Exchange version 2 (IKEv2)

- IKEv2 je komponenta IPsec koja služi za uzajamnu autentifikaciju izvora i odredišta IP datagrama i uspostavljanje IKE sigurnosnih asocijacija
  - IKE SA sadrži zajedničku tajnu informaciju koja služi za uspostavu SA-ova za ESP i AH i skup kriptografskih protokola koje SA koristi za zaštitu prometa kojeg prenosi
  - IKE omogućuje pregovaranje o skupu protokola koje koristi SA nizom zahtjeva i odgovora

Izvedba IPsec - baze podataka

- općeniti model obrade prometa vezan za IPsec funkcionalnost koristi tri baze podataka:

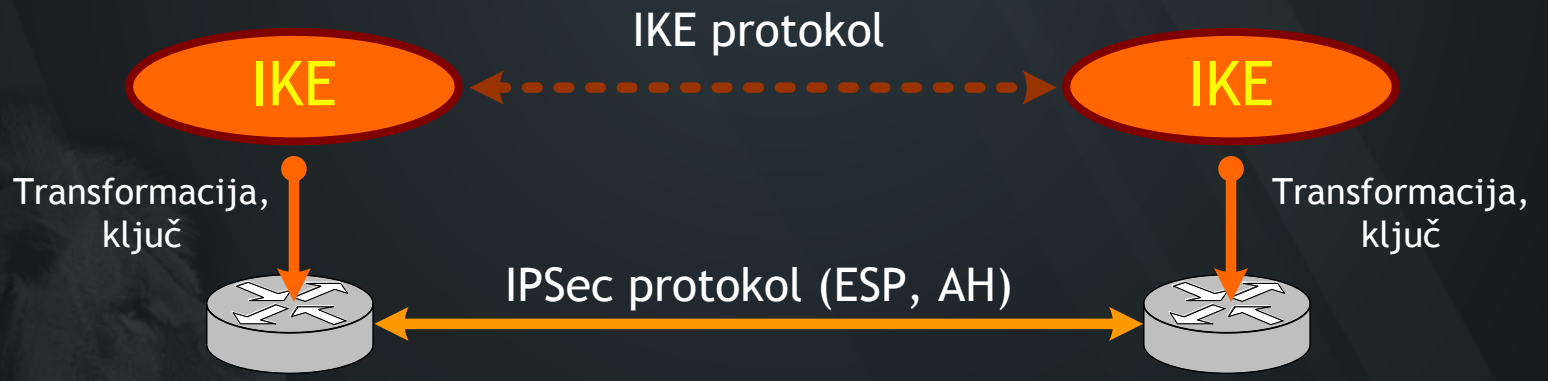
- Security Policy Database (SPD)
  - specificira politike koje određuju prirodu ulaznog ili izlaznog IP prometa u odnosu na krajnje računalo ili sigurnosni prilaz
- Security Association Database (SAD)
  - sadrži parametre za svaku uspostavljenu SA
- Peer Authorization Database (PAD)
  - veza protokola koji upravlja sa sigurnosnom asocijacijom (npr., IKE) i drugih dviju baza SPD i SAD

IPsec SA

- Vrste:
  - Uni-Directional (IPsec SA)
  - Bi-directional (IKE SA)

IPSec – Upravljanje ključevima

- Ključevi su bitni za enkripciju
  - Kako će biti korišteni (distribuirani, re-distribuirani)
- IKE – Internet Key Exchange protokoli
- Re-distribucija ključeva u odgovarajućim vremenskim intervalima



Prednosti i nedostaci IPsec

- prednosti:
  - osigurava se sav promet viših slojeva (TCP, UDP)
  - korisnici i aplikacije ne moraju se brinuti o sigurnosti
  - stvaraju se sigurni tuneli kroz nesigurne mreže (VPN)
  - osim samog sadržaja, skriva se i vrsta prometa
  - IPsec je standardni dio IPv6 specifikacije
- nedostaci:
  - ne autentificira se korisnik, već računalo
  - nema sigurnosti ako sam sistem nije siguran ili ako je već kompromitiran