# **OMREŽNA VARNOST**

**VARNOSTNI ELEMENTI**

1. **Peter Zmeda je slišal, da obstaja nek podporni protokol, ki se imenuje IKE in da je povezan z varnostnimi protokoli na internetu.**
2. **Opišite scenarij, kjer se protokol uporablja.**

Uporablja se v primeru, ko je treba izmenjati ključ z katerim se bo kriptirala komunikacija (skupna skrivnost)

1. **Opišite delovanje protokola.**

**FAZA 1:** Vzpostavitev dvosmernega **IKE SA**

* V IKE SA se vzpostavi ključ za varovanje nadaljnje komunikacije glede izmenjave ključev
* **Dva načina:**
  + **Aggressive mode:** Krajši, vendar **razkrije identiteto odjemalcev**
  + **Main mode:** Daljši, vendar **skrije identiteto**

**FAZA 2:** IKE generira ključe za druge storitve, kot je npr. IPsec. Vzpostavi se torej IPsec SA

* **Edini način: Quick mode**

1. **Recimo, da protokol ne bi obstajal, kaj bi to pomenilo? Bi se osnovna dejavnost, ki jo IKE podpira, ne mogla izvajati? Bi jo bilo težje izvajati?**

To bi pomenilo, da si prek mreže dva odjemalca nebi mogla izmenjati ključev in vzpostaviti SA. Osnovna dejavnost bi se še vedno lahko izvajalo ampak bi se moralo izvajati ročno, kar pa je zamudno.

1. **Peter je doma postavil lokalno omrežje z nekaj računalniki. Za prehod v internet je pred temi računalniki postavil še en računalnik, na katerem poganja Linux distribucijo OpenWRT. Na treh notranjih računalnikih mu tečejo openssh strežniki. Sedaj bi rad do teh računalnikov dostopal s širnega interneta.**
2. **Kaj mora postoriti na prehodnem računalniku, da bo lahko dostopal do notranjih računalnikov? Predlagajte vsaj dve rešitvi.**

* Lahko se SSH-ja (poveze) na enega izmed računalnikov na katerih teče SSH server
* Lahko vzpostavi VPN in konfigurira routing, da bodo računalniki znali komunicirati

1. **Če na vseh treh računalnikih ssh posluša na istih vratih, ali lahko sploh dostopa do vseh treh?**

Odvisno od tega kako je konfigurirano omrežje.. Če so na routerju pravilno nastavljene preusmeritve potem bo to delalo brez problema, saj so računalniki v NAT omrežju in se porti preslikajo.. Znotraj omrežja pa ima vsak računalnik drugačen naslov.

1. **Kakšno vlogo igra prehodni računalnik – mostiček, usmerjevalnik, požarna pregrada ali aplikacijski prehod? Utemeljite odgovor**

* **Igra vlogo aplikacijskega prehoda**: saj mora pravilno posredovati promet na pravi računalnik v notranjem omrežju in vsaka aplikacija mora imeti svoj aplikacijski prehod

1. **Varovanje prometa se lahko dogaja na različnih plasteh. Zapišite vse plasti in kako se lahko na vsaki od teh plasti izvaja varovanja prometa (navedite tudi imena protokolov za posamezno plast).**

* **Fizična plast:** Varovanje infrastrukture, preprečevanje prisluškovanja itd.
* **Povezavna plast: IEEE 802.1X** Nadzoruje kdo se lahko priključi v mrežo in kdo ne
* **Omrežna plast: IPsec** izvaja se zakrivanje vseh vrst podatkov, avtentikacija izvora, integriteta podatkov, zaščita pred ponovitvijo
* **Transportna plast: SSL** zagotavlja zaupnost, integriteto in avtentikacijo
* **Aplikacijska plast: Aplikacijski prehodi** filtrira promet glede na izbiro uporabnikov, ki lahko uporabljajo določeno storitev

**4. IPsec protokol lahko deluje v prenosnem (transport) ali tunelskem (tunnel) načinu. Opišite, kako izgleda pretvarajanje paketov v tunelskem načinu na poti od izvora do ponora, pri čemer nas zanima samo avtentikacija paketa. Bodite pazljivi pri opisu glav posameznih paketov.**

V tunelskem načinu se paket kriptira vključno z glavo paketa. Doda se **ESP rep** nato se vse skupaj zakriptira in doda se **ESP glava (rezultat je enchilada).** Doda se polje **ESP auth**, ki je izračunana zgoščena vrednost cele »enchilada«. Z to vrednostjo nato preverimo integriteto in avtorizacijo paketa (algoritem in ključ določa SA). Nato se izdela še nova IP glava in paket se pošlje.