IP security protocol, je varnostni protokol, ki omogoča varnost na omrežni plasti. Uporablja se za varovanje povezave med dvema entitetama in njunima entitetnima paroma. Definiran je v RFC 2411

> V praksi je dostikrat uporabljen, kot sestavni del VPN-jev (Virtual Private Network)

Protokol, kot tak je nadgradnja oz. zamenjava za IP protokol, saj poleg prenosa prometa zagotavlja tudi zakrivanje in celovitost. Poleg teh dveh dimenzij varnosti, ščiti tudi proti ponovitvijo komunikacije in zagotavlja avtentikacijo izvora komunikacije.

Varnostna protokola

IPsec implementira dva varnostna protokola: - **Authentication Header**, ki zagotavlja avtentikacijo izvora in celovitosti podatkov

- **Encapsulation Security Payload**, ki pa zagotavlja avtentikacijo izvora, celovitost *in* zaupnost podatkov

Načini komunikacije

IPsec lahko deluje v tveh načinih komunikacije: - **Tunnel mode**: Kjer deluje transparentno končnim odjemalcem, torej velja router-to-router ali pa router-to-user. Šifrira podatke in glavo paketa. TOREJ le od routerja... - **Transport mode**: Kjer je implementiran med končnimi odjemalci (vmesniki računalnikov), ščiti zgornje polasti protokola in je transparentem vmesnikom, šifrira samo podatke v paketu.

Tunnel način se uporablja, ko povezujemo network-to-network, transportni pa ko želimo neko peer-to-peer z odjemalcem

Tunnel mode z ESP

Preden originalni paket z IP glavo šifriramo, ji na rep dodamo ESP rep, ki vsebuje neko prazno solato, tako da pridobimo bitno poravnanost. Potem pa dodamo še prednji del ESP glave, ki vsebuje SPI SA-ja in sekvenčno številko paketa, tako **preprečimo napad z ponavljanjem**.

![[Pasted image 20230111201518.png]] Tako poskrbimo za šifriranje in dešifriranje, za celovitost pa dodamo še en del repa, ki je hash izvleček celotnega zavitka in šifriran z ključem oz. takim algoritmom, kot ga določa SA. ![[Pasted image 20230111202430.png]]

Nad vse to se pa doda nova IP glava, ki servira, kot IPsec glava. Tako ločimo originalni promet z novo glavo, kot dodatna lupina. ![[Pasted image 20230111202630.png]]