# **10.a** Ismertesse az IPSec protokoll célját, felépítését, működését, üzemmódjait és beállításának lépéseit!

# A VPN fogalma, rendeltetése, alaptípusai, funkciói, szolgáltatásai, topológiák

## VPN – Virtual Private Network

* **Virtuális:** A magánhálózat forgalma nyilvános hálózaton halad keresztül egy virtuális alagúton.
* **Védett:** Átmenő forgalom titkossága biztosított.

## Rendeltetése

* Biztonság növelése, Anonimitás
* Nem elérhető tartalomhoz jutás (adott országon belül például tiltva van)
* Adatvédelem

## Alaptípusai

* IPSec – Internet Protocol Security
* L2TP - Layer 2 Tunneling Protocol
* PPTP – Point-to-Point Tunneling Protocol
* SSL és TLS, OpenVPN, SSH – Secure Shell

## Topológiák

* **Site-to-Site VPN**
  + Két vagy több LAN kapcsolható össze.
  + Az állomások normál IP csomagokat küldenek, ami egy VPN gateway-en megy keresztül.
* **Client-to-Site VPN:**
  + Kliens-szerver kapcsolat, ahol kliens alkalmazás szükséges.
* **Client-to-Client VPN:**
  + Közvetlen kommunikáció két számítógép között, központi szerver nélkül.

# IPsec VPN komponensek (protokollok), alprotokollok, működés, előnyök, korlátok

## AH – Authentication Header

* Sértetlenséget, hitelesítést és visszajátszás elleni védelmet biztosít.
* Beszúr egy AH fejlécet, ami egy MAC-et tartalmaz.
* A visszajátszás detektálásának érdekében, az IP csomagokat sorszámozza.
* Az AH fejlécben található MAC érték a sorszámot is védi.

## ESP – Encapsulated Security Payload

* Feladata az IP csomag tartalmának rejtése és opcionálisan a tartalom integritásának védelme.
* IP csomag tartalmának rejtését rejtjelezéssel oldja meg.
* **Tartalom integritásának védelme:** ESP fejlécre és a csomag tartalmára számít MAC kódot és azt a csomaghoz csatolja.
* ESP MAC nem védi az IP fejléc mezőit.

## ISAKMP – Internet Security Association and Key Management Protocol

* Általános célú keretprotokoll, ami bármilyen konkrét kulcscsere protokoll üzeneteit képes szállítani.

## IKE – Internet Key Exchange

* IPSec hivatalos kulcscsere protokollja.
* A host-ok ebben a fázisban hitelesítik egymást shared secret vagy RSA kulcs segítségével.
* Felépítenek egy kétirányú ISAKMP SA-t.
* Az ISAKMP SA-t alkalmazva megvitatják az egyirányú IPSec SA-kat.

# Az IPsec protokollok paramétereinek konfigurálási megfontolásai és lépései

## Megfontolások

* **Titkosítási módszer:** DES, 3DES, AES, stb
* **Autentikációs módszer:** Például SHA, MD5, stb
* **Kulcsrotációs periódus:** Mennyi ideig használhatjuk ugyanazt a titkosítási és autentikációs kulcsot.
* **Pre-shared key:** Összes hálózati eszköz ismeri a kulcsot.
* **Perfect Forward Secrecy**: A régi kulcsok már nem használhatóak.

# IPsec üzemmódok jellemzői, működése, konfigurálása, tesztelése

## Üzemmódok

* **Szállítási (transport) mód**
  + Az AH vagy az ESP fejléc a csomag eredeti IP fejléce és a felsőbb szintű protokoll fejléce közé kerül.
* **Alagút (tunnel) mód**
  + Az eredeti IP csomagot teljesen beágyazzuk egy másik IP csomagba.
  + Az AH vagy az ESP fejléc az új és az eredeti IP fejléc közé kerül.
  + Az AH fejléc vagy az ESP trailer következő fejléc mezője IP-re utal.

## IPSec működése

* Adatgyűjtés
* Titkosítás
* Autentikáció
* Csomagolás
* Továbbítás
* Titkosítás feloldása
* Adatok fogadása

## Konfigurálása

* ISAKMP policy
* Pre-shared key
* Érdemleges forgalom definiálása ACL segítségével
* IPSec policy
* Alagút paraméterek
* Interfészek kiválasztása