# **9.a** Ismertesse a VPN-ek (Virtual Private Network) célját, feladatát és fajtáit! Milyen megvalósításait ismeri? Miben különböznek a különböző rétegekben megvalósított VPN-ek?

# 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.

# VPN megvalósítások a különböző OSI rétegekben

A képen szöveg, képernyőkép, diagram, sor látható

Automatikusan generált leírás

## L2 VPN

* Független a felső protokolltól
* Adatkapcsolati rétegben helyezkedik el
* Egy-egy kapcsolatot véd, így minden összeköttetésre külön alkalmazni kell.
* MITM támadás lehetséges

## L3 VPN

* Hálózati rétegben helyezkedik el
* Média és alkalmazás független
* IPSec, GRE, MPLS

## L4 VPN

* SSL-lel biztosítja a titkosságot, a felhasználók hitelességét és az adatok sértetlenségét a TCP alkalmazások számára.
* Nem rugalmas, nehéz megvalósítani
* Nem alkalmazás független

## L7 VPN

* Az alkalmazás rétegbeli VPN-t minden alkalmazásban külön-külön meg kell valósítani.

# GRE

## GRE kapcsolat szolgáltatásai

* Hálózati protokollok közötti átjárás
* Többszintű hálózatok összekapcsolása
* Hálózatok közötti tűzfalak átjárásának lehetősége
* Hálózatok közötti VPN-ek létrehozása

## Jellemzők

* Nem alkalmaz titkosítást, így IPSec-et kell alkalmazni.
* Támogatja a routing protokollokat
* Több protokollos alagutakat is támogat
* Multicast csomagokat is kezel
* Alkalmas irányító protokollok irányítási információinak szállítására és cseréjére.

# 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

# SSL

## SSL célja

* Titkosított kommunikációt biztosító protokoll, ami nyílt hálózatokban, kapcsolatorientált kommunikációban nyújt védelmet.
* Csak egy-egy kommunikációs csatornát biztosít.
* Gyakran használják a weboldalak biztonságos titkosítására is.

## SSL szerkezeti felépítése

* Minden egyes kapcsolat egyedi kulccsal titkosít.
* Tanúsítvány igazolja a szervert.
* Biztosítja az adatintegritást. (MD5, SHA-1)

## SSL működése

1. Kliens csatlakozik a kiszolgálóhoz.
2. Kiszolgáló elküldi a hitelesítési tanúsítványt a kliensnek.
3. Kliens ellenőrzi a tanúsítvány hitelességét, majd létrehozza a titkosított kapcsolatot a kiszolgálóval.
4. Kliens és kiszolgáló között így már biztonságosan lehet adatokat cserélni.
5. Ha az SSL kapcsolat megszakad, akkor a kliens és a kiszolgáló kapcsolata is megszakad.

## SSL alprotokolljai

### Rekord protokoll

* Feladata a kliens és a szerver és a felsőbb SSL protokoll entitások védelme:
  + Titkosítás, integritásvédelem, üzenet-visszajátszás elleni védelem

### Handshake protokoll

* Rekord protokollban használt kriptográfiai algoritmusok és paramétereik egyeztetése.
* Kulcscsere és hitelesítés

### Change-Cipher-Spec protokoll

* Egyetlen üzenetből áll, ami a Handshake protokoll kulcscsere részének végét jelzi.
* Ezt az üzenetet elküldi, utána az adott fél az új algoritmusokat és kulcsokat kezdi használni a küldése.
  + A vétel még mindig a Handshake előtti állapot szerint történik.

### Alert protokoll

* Figyelmeztető és hibaüzenetek továbbítása.

# A handshake, valamint a record alprotokoll feladata, működése és üzenetei

## Rekord protokoll működése

* A felsőbb protokoll rétegektől érkező üzeneteket:
  + Fragmentálja, ha szükséges.
  + Fragmenseket tömöríti
  + Tömörített fragmenseket fejléccel látja el
  + Fejléccel ellátott, tömörített fragmensre üzenethitelesítő kódot/MAC-et számol és azt a fragmenshez csatolja.
  + Az üzenethitelesítő kóddal ellátott fragmenst rejtjelezi.

### Rekord üzenetei

* **type**: Rekord üzenetben melyik felsőbb protokoll található.
* **version:** SSL verzió
* **length:** Fragmens hosszát tartalmazza bájtban mérve.
* **MAC:** Üzenethitelesítő kód generálása

## Handshake protokoll működése

1. **fázis:** Kliens és szerver elküldi a tulajdonságait, megállapodnak
2. **fázis:** 
   1. Kulcscseremódszertől függ
   2. Szerver elküldi a tanúsítványát és kéri a kliens tanúsítványát.
3. **fázis:** Tanúsítvány ellenőrzés és kulcscsere folytatása
4. **fázis:** Kulcscsere életbelépése, befejezése

### Handshake üzenetei

* **KliensHello:** 
  + Kliens küldi ezt az üzenetet az SSL Handshake kezdeményezésére.
  + Kliens verzió, véletlenszám, viszonyazonosító, biztonsági algoritmusok, tömörítő algoritmusok
* **SzerverHello:** 
  + Kiszolgáló küldi a **KliensHello** üzenetre válaszul.
  + Szerver verzió, véletlenszám, viszonyazonosító, biztonsági algoritmusok, tömörítő algoritmusok
* **Szerver kulcscsere üzenet**
* **Tanúsítvány kérés**
  + Előfordulhat olyan eset is, amikor a tanúsító hatóságok listája üres.
    - Ilyenkor a kliens eldöntheti, hogy elküldi-e az ügyféltanúsítványt vagy sem.
* **Kliens tanúsítvány**
  + A kliens bemutatja a tanúsítványláncát a kiszolgálónak.
* **Kliens kulcscsere üzenet**
  + Lényege, hogy létrehozza a közös kulcsot a kliens és a kiszolgáló között anélkül, hogy azt egy kívülálló számára felfedné.
* **Kész üzenet**
  + Első olyan üzenet, ami már az új algoritmusokat használva, az új kulcsokkal van kódolva.