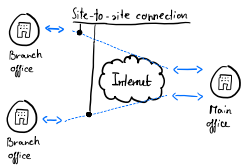
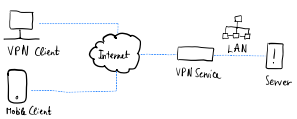
IPSec

- **VPN** -> Virtual Private Network
  - Virtuális -> A magán hálózat forgalma nyilvános hálózaton halad keresztül egy virtuális alagúton.
  - Védett -> Átmenő forgalom titkossága biztosított.
- **Rendeltetése**
  - Biztonság növelése, anonimitás
  - Nem elérhető tartalomhoz jutás
  - Adatvédelem
- **Alaptípusai**
  - IPSec – Internet Protocol Security
  - L2TP – Layer 2 Tunneling Protocol
  - PPTP – Point-to-Point Tunneling Protocol
  - SSL/TLS, OpenVPN, SSH
- **Topológiái**
  - Site-to-site VPN -> Két vagy több LAN kapcsolható össze.

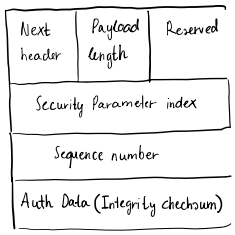


  - Client-to-Site VPN -> Kliens szerver kapcsolat, ahol kliens alkalmazás szükséges.



  - Client-to-Client VPN -> Közvetlen kommunikáció két számítógép között, központi szerver nélkül.

• IPSec



• AH - Authentication Header

- Sértetlenséget, hitelesítést, 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 értéke a sorszámot is védi

ESP - Encapsulated Security Payload

- Feladata az IP csomag tartalmának rejtése és opcionálisan a tartalom integritásának védelme.
- IP csomag tartalmának rejtését rejtjelzéssel 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.

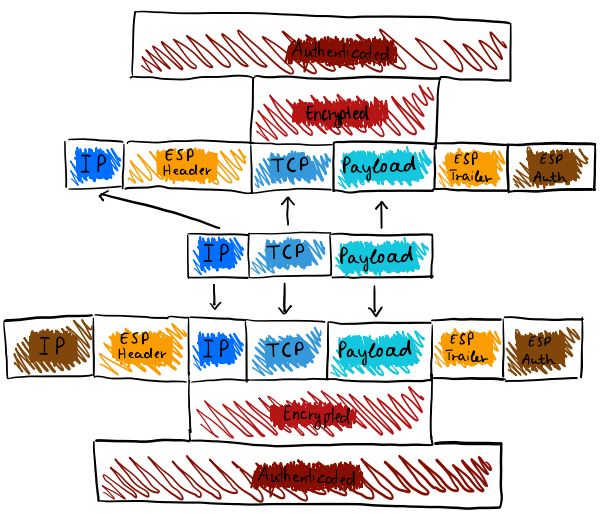
• ISAKMP -> Internet Security Association and Key Management Protocol

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

• IKE -> Internet Key Exchange

- IPSec hivatalos kulcscsere protokollja.
- A hosztok 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.

- Megfontolások
  - Titkosítási módszer -> DES, 3DES, AES
  - Autentizációs módszer -> SHA-1, MD5
  - Kulcsrotációs periódus -> Mennyi ideig használhatják a titkosítási, autentizációs kulcsot?
  - Pre-shared key -> Összes hálózati eszköz ismeri a kulcsot.
  - Perfect Forward Secrecy -> A régi kulcsok már nem használhatóak.
- 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
  1. Adatgyűjtés
  2. Titkosítás
  3. Autentizáció
  4. Csomagolás
  5. Továbbítás
  6. Titkosítás feloldása
  7. Adatok fogadása