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

IPSec – Internet Protocol Secure: protokoll csomag IP alapú kommunikáció biztonságossá tételére

1. Bizalmasság - titkosítás

2. Sértelenség – üzentpecsét (message digests) függvények

3. Hitelesítés – hitelesítő algoritmus

4. Visszajátszásos támadás elleni védelem

Két alprotokollból áll:

* AH - Authentication Header: IP csomagok integritásának védelme, eredetének hitelesítése, visszajátszásuk detektálása
* ESP - Encapsulated Security Payload: IP csomagok tartalmának rejtése, opcionálisan integritásvédelem

Az AH és az ESP kombinálhatók a teljeskörű védelem érdekében

Felépítés: SA (Security Association): az AH vagy ESP működéséhez a feleknek meg kell egyezniük mely eljárásokat használják, ezt SA-nak nevezzük

5 részből áll:

IPSec protocol AH | ESP ESP + AH

Bizalmasság nincs | DES, 3DES, AES, SEAL

Sértetlenség MD5 SHA

Hitelesítés PSK RSA

Diffie-Hellman DH1, DH2, DH5 ...

Az AH:

* nemtud titkosítani, emiatt kevésbé van hatással a rendszer teljesítményére.
* teljes adatcsomagot hitelesíti az ESP viszont nem hitelesíti a bevezető IP fejlécet, illetve az ESP fejléc előtti más információkat
* integritásvédelemet és az eredethitelesítést úgy éri el, hogy az IP fejléc és az azt követő protokoll fejléce közé beszúr egy AH fejlécet, ami a teljes IP csomagra számolt hitelesítő kód (MAC)
* Visszajátszások detektálása érdekében sorszámozza az IP csomagokat

Az ESP az IP csomag tartalmát rejtjelezéssel titkosítja

ISAKMP (Internet Security Association and Key Management Protocol): általános célú keretprotokoll, mely bármely konkrét kulcscsere protokoll üzeneteit képes szállítani.

IKE (Internet Key Exchange): az IKE protokoll építi fel az IPSec kapcsolatokat, miután az alapvető paraméterek megvitatásra kerültek, ez az IPSec hivatalos kulcscsere protokollja, két fázisból áll

1. Fázis: a host-ok hitelesítik egymást shared secret vagy RSA kulcs segítségével. Felépítenek egy kétirányú ISAKMP SA-t
2. Fázis: A biztonságos kommunikáció paraméterei kerülnek megvitatásra
   * A maximális idő, amíg a kulcs használatban lehet
   * A titkosítási algoritmus
   * A hitelesítési algoritmus
   * Előre megosztott kulcsok, azaz a kapcsolatban résztvevők gépein előre telepítve rendelkezésre állnak
   * Nyilvános kulcsok alkalmazása kriptografikus módszerekkel
   * Diffie-Hellman kulcscsere csoportjának megválasztása

Az ISAKMP SA-t alkalmazva megvitatják az egyirányú IPSec SA-kat

Üzemmódok: kettő van, mind AH mind ESP esetén

Szállítás (transport): az AH/ESP fejléc a csomag eredeti IP fejléce és a felsőbb szintű protokoll közé kerül

Alagút (tunnel): az eredeti IP csomagot teljes egészében beágyazzuk egy másik ip csomagba, az AH/ESP fejléc az új és az eredeti IP fejléc közé kerül

Konfiguráció:

1. ISAKMP policy konfigurálása az IKE 1. fázisához
2. IPSec policy konfigurálása az IKE 2. fázisához
3. Crypto map konfigurálása az IPSec policy-hoz
4. IPSec policy alkalmazása
5. Ellenőrizzük, hogy az IPSec tunnel működőképes