5.a Ismertesse a tűzfalak különböző generációit és hasonlítsa össze őket!

Tűzfalak feladata és rendeltetése

- Szoftveres vagy hardveres hálózatbiztonsági eszköz.
- A tűzfalak a hálózatba be és kimenő kapcsolatokat figyelik, és csak azokat engedélyezik, amik megfelelnek a beállított szabályoknak.
- **Előnyei:**
  - Nem befolyásolják negatívan a hálózat működését és biztonságot nyújt
- **Hátrány:**
  - Általános szabályok alapján működnek.
  - Letilt olyan kapcsolatokat, amik nem is veszélyesek.
  - Lehet, hogy lassítja a hálózat működését, így a szolgáltatások minősége romolhat.
  - Nem megfelelő konfiguráció esetén, nem lesz jó a védelem.
  - Nem véd olyan kapcsolatoktól, amik nem mennek rajta keresztül

Tűzfalak generációi és fejlődésük

Első generáció – Packet Filtering Firewall

- **Döntését ezekre alapozza:**
  - Forrás / Cél MAC címe, ip címe és port száma
  - IP csomagba beágyazott protokoll

Működése

- A csomag fejlécben lévő információt **összeveti a tűzfalban megadott szabályokkal.**
- A hálózati és szállítási rétegben működik, adattartalmat nem figyel.
- Alacsony szintű biztonságot nyújt, mert nem vizsgálja a csomag tartalmát.
- Nem kezeli a kapcsolatállapotot
- Kétirányú forgalmat külön szabályokkal kell megadni.
- Egész port tartományt engedélyezni kell, mert sok protokoll dinamikusan választ portot kliens oldalon.

Második generáció – Stateful Firewalls (OSI 5. rétegben dolgozik)

- Tartalmakat vizsgál és figyelembe veszi a felépített kapcsolatokat.
- Figyeli az összes áthaladó hálózati csomagot és megállapítja, hogy:
  - melyik már egy meglévő kapcsolat része
  - melyik kezdeményez új kapcsolatot
  - melyik csomag nem része egyik kapcsolatnak sem
- A felépített kapcsolat információt gyorstárolóban tárolja.
- A kapcsolat csomagjait a gyorsítótárban lévő bejegyzésekkel hasonlítja össze (hatékony)
- Figyeli a dinamikus protokollok állapotát.

Előnyei

- Jobban le lehet írni a hálózati szabályokat (állapotokat).
- Nagyobb biztonságot nyújt, mint a csomagszűrő tűzfalak (sorszámokat folyamatosan követi)

Hátrányai

- Állapotok kezelése miatt erőforrás igényes és nem mindig képesek megkülönböztetni a biztonságos és a veszélyes adatokat a csomagokban.

Harmadik generáció – Application Level Firewall

- **Két kategóriája van:** Proxy tűzfalak – Proxy Firewalls, Mély csomag ellenőrző – Deep Packet Inspection

Előnyei

- Biztonságos, és a puffer túlcsordulás típusú támadásoknak ellenáll, mert figyeli a protokoll fejléc mezőinek hosszát.

Hátrányai

- Erőforrás igényes, nem megfelelő megvalósításnál gyenge teljesítmény
- Transzparencia hiánya

Proxy firewalls

- A közvetlen kapcsolat megszakad, a továbbítandó csomagot újraelőállítják, átmásolják az összes protokollréteg szükséges mezőit.
- Alkalmazás szinten képes a parancsok szűrésére.

Deep Packet Inspection Firewalls

- Transzparensen működik, nem épít fel külön kapcsolatot a két kommunikáló fél között.
- Egyszerre szűri az OSI modell mind a 7 rétegét.
- Figyeli a protokollnak nem megfelelő csomagokat és szűri azokat.
- Csomagokat az alkalmazásoknak megfelelően osztályozza.

Next Generation Firewalls

- Több hálózatbiztonsági technológia együttes integrációja.
- Olyan megoldás, ami DPI tűzfalat, IDS/IPS eszközöket, antivirus átjárót, proxy megoldást, VPN kiszolgálót, QoS és sávszélesség menedzsmentet biztosít, hogy a lehető legjobban kielégítse a mai kor igényeit.

Lehetséges Tűzfal topológiák

Dual-Homed

- Két interfésszel rendelkezik, amik külön hálózatba csatlakoznak és közöttük szűri a hálózati forgalmat.
- Speciális esete, amikor a router a tűzfal (screening router)

Single-Homed - Screened host

- A szolgáltatást nyújtó (bástya) gép csak a belső hálózatra csatlakozik.
- Elsődleges biztonságot a csomagszűrő forgalomirányító adja, ami megakadályozza, hogy a felhasználói gépek közvetlenül hozzáférjenek az internethez.
- Csomagszűrő forgalomirányítót úgy konfigurálják, hogy az internet gépei csak a bástya géppel léphetnek érintkezésbe.
- Bástya gép biztonsága fontos és proxy-ként működik.
- **Előnyei:**
    - A screened host architektúra nagyobb biztonságot nyújt, mint a dual-homed host architektúra és nincs Single Point Of Failure
- **Hátránya**
    - Screened subnet architektúra biztonságosabb
    - Ha a támadó betört a bástya gépre, onnan már a többi gépet is eléri a LAN hálózaton.

Single-Homed - Screened subnet

- Screened subnet architektúra újabb biztonsági réteget helyez el az internet és a belső hálózat felé, ez a határ (perimeter) hálózat.
- **Bástya gép sebezhető**
    - Ha a támadó bejut a bástya gépre, még mindig útját állja a belső forgalomirányító.
- **Perimeter hálózat**
    - Ha a támadó bejut a bástya gépre, csak a perimeter hálózat forgalmát lehallgatja, a belső hálózat forgalmát nem láthatja.
    - A perimeter hálózaton megy keresztül a bástya gép és az internetre irányuló forgalom, de két belső gép egymás közötti forgalma nem.
- **Bástya gép**
    - A bejövő forgalom kezelésének helye
    - **A kifelé irányuló szolgáltatások két módon kezelhetők:**
        - Belső és a külső forgalomirányítók csomagszűrő szabályainak beállításaival.
        - Proxy szerverek futtatásával a bástya gépen.
- **Belső router (Choke router)**
    - Szabályozza, hogy a belső hálózatról melyik szolgáltatások érhetőek el közvetlenül.
    - Szabályozza a belső hálózat és a bástya gép közötti forgalmat.
- **Külső router (Access router)**
    - Védi a perimeter és a belső hálózatot az internet felől.
    - Minden forgalmat kienged a perimeter hálózatról.

Multi-Homed

- Három vagy több interfésszel rendelkezik, amik külön hálózatban csatlakoznak és közöttük szűri a hálózat forgalmát.

ASA tűzfal bemutatása, alapvető működése

- **Feladata**
  - Megvédje a hálózatot a külső támadásoktól és az engedély nélküli hozzáférésektől.
  - Ellenőrizze és szabályozza az összes kommunikációt, ami a hálózatba és onnan kifelé történik.
- **Két féle forgalmat kezel**
  - Kezdeményező forgalom, amit a hálózatban lévő eszközök indítanak.
  - Elfogadott forgalom, ami a külső hálózatokról érkező kérésre válaszolnak.

Működése

1. Ellenőrzi a forgalmat, hogy megfelel-e a szabályoknak.
2. Ha megfelel, akkor engedélyezi és továbbítja azt.
3. Ha nem felel meg, akkor blokkolja azt.

Biztonsági szintek szerepe és jelentősége ASA tűzfal esetén

- 0 és 100 közötti értékek, amik növekvő biztonsági szintet jelentenek.
- Szerepe, hogy meghatározzák milyen forgalom engedélyezett vagy tiltott.
- Alacsonyabb biztonsági szinten lévő számítógépek csak olyan forgalmat küldhetnek, és fogadhatnak, ami megfelel a szabályoknak.
- A magasabb szinten lévők szélesebb körű forgalmat küldhetnek és fogadhatnak.

Alapkonfigurációs megoldások ASA tűzfal esetén, ACL, NAT, PAT, AAA konfigurálása

5505

- Switch modul, vlan interfészeket kell létrehozni, de alap licensszel csak 2-t lehet.

IP cím lehet

- Kézzel beállított, DHCP vagy PPPoE

Minden port alapértelmezésben VLAN1 tag

- Vlan beállítása ugyanúgy, mint switcheken és utána be kell kapcsolni az interfészt.

ACL

- Hozzáférés szabályozás vagy hálózati forgalom szűrésére szolgál.
- Permit és deny állításokból épül fel.
- Forgalomirányító csomagszűrőként viselkedik, amikor továbbítja vagy eldobja a csomagokat.

NAT, PAT

- Belső, külső irány vagyis kétirányú
- **Dinamikus NAT:** Címcsoportok között fordít.
- **Dinamikus PAT:** Egy külső címhez fordít belső címet, portok alapján.
- **Statikus NAT:** Kézzel beállított 1:1 fordítás.
- **Szabály alapú NAT:** Szabály alapú címfordítás.

AAA

- Hálózatot felügyel, aminek három komponense van:
  - Authentication, Authorization, Accounting

Object, object group és a Modulár Policy Framework célja, jelentősége, működése és konfigurálása

Objects and Object Groups

- IP címeket, cím tartományokat, protokollokat, port számokat/tartományokat **Object**-ként definiálhatunk és ezután erre a névre hivatkozva konfigurálhatunk.
- **Előnye**, hogy az **Object** tartalma változik, akkor az **Object**-et használó konfigurációkat nem kell változtatni.

Network Object

- Egy elemet tartalmazhat**: IP** és **Maszk** páros, ami lehet host, subnet vagy range.

Service Object

- Tartalmazhat protokollt, port számot vagy intervallumot és csak egy elemet tartalmazhat.

Object Group

- Több **Object**-et csoportba lehet szervezni és a beállításai minden **Object**-re vonatkozik.

Modular Policy Framework

- **Class maps:** Forgalom figyelése
- **Policy maps:** Több **Class map**-et felvehetünk, amiket feladatokat rendelhetünk.
- **Service policy:** Alkalmazásra interfészre vagy a teljes rendszerre.