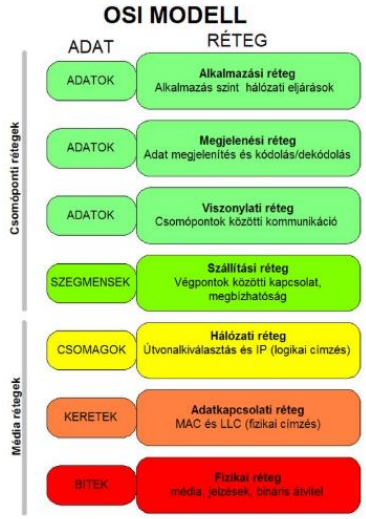
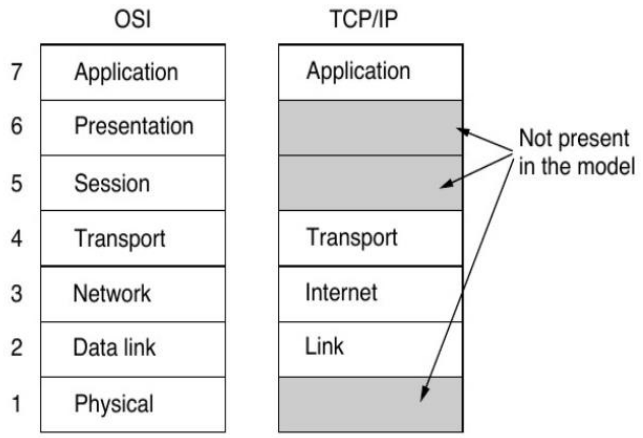
Hálózatok II jegyzet

Ismétlés

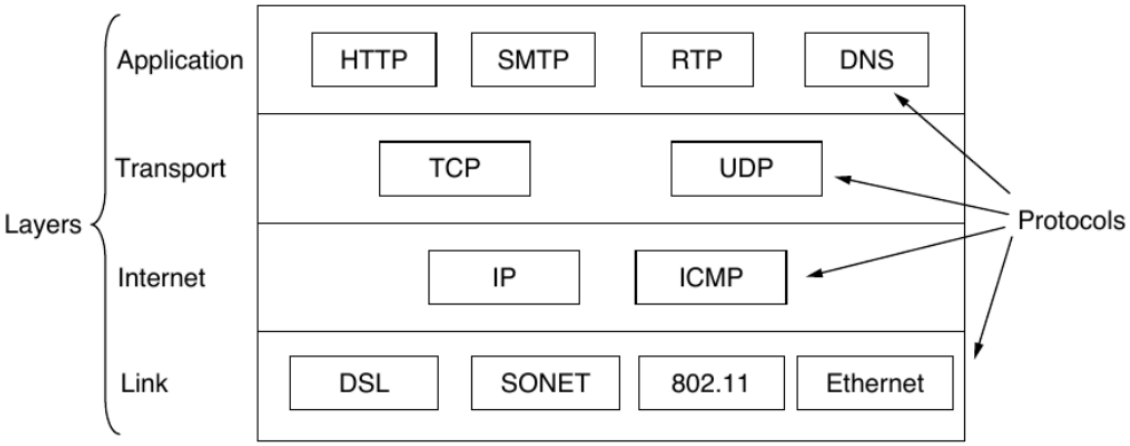
Protokoll rétegek





- Minden réteg célja, hogy szolgáltatásokat nyújtson a felette lévő rétegnek és annak megvalósításait elrejtse
- Az azonos szinten elhelyezkedő entitásokat társentitásoknak nevezzük, ezek protokollok segítségével kommunikálnak egymással

TCP/IP protokollok



Hálózati eszközök

Switch

Aktív számítógépes hálózati eszköz, amely a rácsatlakoztatott eszközök között adatáramlást valósít meg. Az OSI modell második rétegében működik, kereteket továbbít MAC cím alapján

Router

A számítógép-hálózatokban egy útválasztást végző eszköz, amelynek a feladata a különböző hálózatok (pl. otthoni vagy irodai hálózat és az internet), vagy egyes országok közötti hálózatok összekapcsolása, azok közötti adatforgalom irányítása. Csomagokat továbbít IP cím alapján.

Útválasztás

Útválasztó módszerek

Direkt csatolt interfész: A router valamely interfészén konfigurált IP és alhálózati maszk alapján számolja ki a router

Statikus: Minden elérési utat a rendszer adminisztrátor ír be a routerbe manuálisan, ezt szükséges managelni

Dinamikus: A routerek egymás közt osszák meg az elérési utakat valamely dinamikus útválasztó protokollt használva

Útválasztás típusok

Belső útválasztó protokollok:

IGP (Internal Gateway Protocol): egy autonóm hálózaton belül használják (AS – autonomous system), olyan hálózat aminek egy adminisztrátora van pl. egy cég belső hálózata

Külső útválasztó protokollok:

EGP (Extenral Gateway Protocol): A különböző autonóm hálózatok összeköttetésére használják

Adminisztratív távolság, metrika

Adminisztratív távolság: a router által meghatározott érték, hogy mennyire tart megbízhatónak egy útválasztó protokollt.

Metrika: egy adott elérési út minőségét határozza meg.

Mindkét esetben a kisebb érték a jobb.

Útválasztó protokollfajták

Distance Vector Routing

A hálózat minden egyes csomópontja egy olyan táblázatot vezet, amely a hálózat minden más csomópontjának távolságát és irányát tartalmazza. A távolságot a DVR protokollban általában a két csomópont közötti ugrásszámban (azaz a közbenső csomópontok számában) mérik. Célja, hogy megtalálja a hálózatban az egyes célállomásokhoz vezető legrövidebb utat.

Advanced Distance Vector

Legfontosabb jellemzője a Classless Inter-Domain Routing (CIDR) támogatása, amely lehetővé teszi a hálózatok kisebb alhálózatokra való felosztását.

Hitelesítést és változó hosszúságú alhálózati maszkot (VLSM) használ. Támogatja a multicast útválasztást.

Link State Routing

A távolságvektoros útválasztással ellentétben, amely egyes csomópontnak a teljes hálózati topológiát tartalmazó táblázatot kell vezetnie, az LSR protokollok csak az igénylik, hogy minden csomópont rendelkezzen a közvetlen szomszédjainak és a hozzájuk tartozó kapcsolatoknak a térképével.

A protokoll a legrövidebb útvonalat határozza meg a forráspontból a célcsomópontba egy legrövidebb útvonal algoritmus, pl. a Dijkstra algoritmus segítségével.

Útválasztó protokollok

Routing Information Protocol – RIP

- A RIP távolságvektoros útválasztási protokoll.
- Az ugrásszámot használja metrikaként a célállomáshoz vezető legjobb útvonal meghatározásához.
- Minden RIP protokollt futtató router útválaszót táblát vezet, amely a hálózat minden más útválasztójától való távolságot tartalmazza.
- A RIP routerek rendszeres időközönként útválasztási információkat cserélnek szomszédos routerekkel.
- Az útválasztási frissítés fogadásakor az útválasztó frissíti az útválasztási táblázatát, ha a célállomáshoz tartozó új ugrásszám alacsonyabb, mint a táblázatban szereplő.
- A RIP a maximális ugrásszámot 15-re korlátozza, ami problémás lehet olyan nagy hálózatok esetében, ahol sok ugrás van az útválasztók között.
- A RIP nem támogatja az osztály nélküli útválasztást.

Open Shortest Path First – OSPF

- Az adatok egyik hálózatból a másikba történő továbbításának legjobb útvonalának meghatározására szolgál
- Linkállapotú útválasztási protokoll, ami azt jelenti, hogy a teljes hálózati topológiára vonatkozó információkat használja fel az adatok legjobb útvonalának meghatározásához.
- Ebben az esetben a metrika az útvonalban lévő összes kapcsolat összes interfészköltség-beállításának az összege
- Alapértelmezés szerint az interfész sávszélességén alapul.

OSPF működése

- Hello üzenetek minden interfészen (többesküldés)
- Társak, virtuális pont-pont linkek
- Link State Advertisement (LSA) küldés
- Link State Database
- Továbbküldés
- Minden forgalomirányító azonos LSD-vel rendelkezik
- SPF algoritmus a legrövidebb utak kiszámítására
- Forgalomirányító tábla az SPF fából

OSPF Hello protokoll

- Ezzel derítik fel a szomszédokat, azok jelenlétét
- Néhány paramétert hirdet amelyben meg kell egyezniük, egyébként nem folytatják a kapcsolatot
- Az életjelent jelentik
- Kétirányú kapcsolat
- Minden interfészen 10, 30 másodpercenként
- Tartalmazza a forrás forgalomirányító ID-ját, adminisztratív zónáját, hálózati maszkját stb.

OSPF szomszédok feltérképezése

- Miután létrejött a szomszédok közötti kapcsolat, megosszák egymással az adatbázisukat LSA csomagok segítségével.
- Adatbázis csere csak a DR (Designated router) és a többi router közt történik meg.

OSPF kijelölt és kijelölt tartalék forgalomirányítók

- Designated Router, Backup Designated Router
- Enélkül: n(n-1)/2 társi kapcsolat lenne felépítve minden üzenetszórási tartományban
- Pszeudo csomópont
- A kijelölt forgalomirányító feladata:
    - Az üzenetszórási hálózatrész képviselete a külvilág felé
    - Az üzenetszórási hálózatrész elárasztásának managelése
    - A funkció interfészhez kötődik: egyik interfészén DR a másikon nem
    - A prioritás és az ID dönti el a DR és a BDR szerepkört

OSPF DR, BDR választás

- Amikor egy forgalomirányító aktív lesz megnézi van-e aktív DR és BDR.
- Ha van akkor azok is maradnak
- Ha nincs akkor választanak
- Prioritás és IP cím szerint
- DR-nek lennie kell, a BDR nem kritikus
- Választás után a többi forgalomirányító társi kapcsolatot létesít a DR-el és a BDR-el.

OSPF Dijkstra algoritmus

- Fa adatbázis, jelölt adatbázis, link állapot adatbázis
- Az algoritmus:
    1. a forgalomirányító inicializálja a fa adatbázist hozzáadva saját magát és a 0 költségű szomszédjait
    2. A gyökér forgalomirányítóhoz vezető linkeket beleteszi a jelölt táblába
    3. A gyökértől a jelölt adatbázisban lévő linkekhez vezető költségeket kiszámítja, a legkisebb költségűt a fa adatbázisába teszi, az azonos céllal de különböző költséggel rendelkezők közül csak a legrövidebbet hagyja benn, a többit törli
    4. A Link szomszéd ID-ját átnézi és aki még nem szerepel a jelölt adatbázisban azt odateszi
    5. Ha van még jelölt akkor folyatja a 3. lépéssel, ha üres akkor befejezi az algoritmust.

OSPF zónák

- Az azonos alhálózathoz csatlakozó összes interfész ugyanabba a zónába kerül
- Egy zónának egybefüggőnek kell lennie.
- Néhány útválasztó lehet egy zónának belső része, és az összes interfész az adott zónához van rendelve

- Néhány útválasztó lehet zónahatár-útválasztó (ABR), mivel egyes interfészek a zónához tartozó gerinchálózati zónához, néhány pedig a nem gerinchálózati zónához csatlakozik.
- Minden nem gerinchálózati zónának rendelkeznie kell a gerinchálózati zónának (0. terület) eléréséhez vezető útvonallal.

OSPF LSA csomagok

LSA neve	LSA típusa	Elsődleges cél	Tartalom
Router	1	Leír egy routert	RID,interfészek,IP címek-maszk,jelenlegi interfész státusz
Hálózat	2	Leír egy hálózatot amely tartalmaz egy DR-t	DR és BDR IP címe, alhálózati id és maszk
Összegző	3	Leír egy alhálózatot egy másik zónaban	Alhálózati ID, maszk, ABR RID

OSPF összefoglaló

- Szomszédsági kapcsolatok felépítése – Hello csomag
- Kapcsolatállapot hirdetés – Link-State Advertisements – LSA
- Az LSA tartalmazza:
- minden közvetlenül kapcsolódó hálózat költségét
- a router elárasztja a szomszédokat
- a szomszéd azonnal továbbítja
- Topológia tábla építése
- SPF-algoritmus futtatása, így létrejön az SPF fa
- Területekre bontás, kell legyen mindig egy 0 terület, kevesebb számítás szükséges
- DR BDR választás, ezáltal az adatforgalom csökkenthető

Border Gateway Protocol – BGP

- Az IGP-k hátránya, hogy nem skálázódnak olyan nagy hálózatokban, mint az internet
- Ezzel ellentétben a BGP az útvonalak stabilitása és a skálázhatósága felé hajlik
- A BGP nem küld rendszeresen útvonalfrissítéseket, mint az OSPF
- A BGP útvonalvektor protokoll: ahelyett, hogy a legrövidebb távolságot próbálná megkeresni egy adott előtaghoz, inkább a legkevesebb AS-en keresztül vezető utat próbálja megtalálni.

BGP AS számolás

- A BGP egy AS-t (Autonomous System) AS-számmal azonosít. Jelenleg az AS számok 4 bájtosak, a tartomány 0-4 milliárd között van
- A gyakorlatban az AS számok sokkal korlátozottabbak. A IANA osztja ki ezeket a számokat a nyilvános interneten való használatra.

- A BGP két fő célra használja az AS-számokat:
    - Az előtaghoz vezető legjobb útvonal meghatározására
    - Az AS-ek közötti útválasztási hurkok megelőzésére

BGP útválasztás hurkok

- Ha egy BGP-router a saját AS-ét látja egy másik AS-től kapott útvonal AS-útvonalában, akkor egyszerűen elveti az útvonalat.

BGP munkamenet állapotok

- Mielőtt a BGP-routerek útvonalakat cserélhetnének, peering-munkamenetet kell léterhozniuk
- Amikor különböző AS-számú BGP-routerek peeringet létesítenek, azt külső BGP (eBGP) peeringnek nevezzük
- Ha két azonos AS-számú BGP-útválasztó társul, azt belső BGP (iBGP) peeringnek nevezzük

BGP legjobb útvonal

- Az AS-útvonal hossza nem az egyetlen attribútum, amelyet a BGP az előtaghoz vezető legjobb útvonal meghatározásához használ. A Cisco routerekben a BGP attribútumok sorrendben történő figyelembevételével határozza meg a legjobb útvonalat:
    - Súly: lehet vele szabályozni, hogy melyik útvonal legyen erősebb, a nagyobb súly előnyösebb
    - Helyi preferencia: Ha pl. két BGP router van ugyanabban az AS-ben, és mindkettő egy külső AS-ből tanulja az 5.0.0.0/8 prefixet, akkor helyi preferenciával szabályozhatja, hogy melyik router legyen a következő ugrás az előtag eléréséhez.
    - Legrövidebb AS-útvonal: a legrövidebb számú AS-ugrással rendelkező útvonal az előnyben részesített.
    - Eredet típus: a BGP hogyan tanulta meg az útvonalat
    - Multi-exit diszkriminátor: azt befolyásolja, hogy a forgalom hogy lép be az AS-be, minél kisebb annál jobb
    - eBGP az iBGP FELETT
    - Legalacsonyabb IGP költség a BGP következő ugrásáig
    - Legrégebbi útvonal: a BGP nagyobb hangsúlyt fektet a stabilitásra, a legrégebbi útvonalat részesíti előnyben
    - Legalacsonyabb RID

Virtuális privát hálózatok – VPN

- A VPN valahol a LAN és a WAN között helyezkedik el, a WAN gyakran szimulálja a LAN-kapcsolatot. Alapvetően az egyik LAN-on lévő számítógép egy másik, távoli LAN-hoz csatlakozik, és távolról használja annak erőforrásait. A VPN-ek használata nagy kihívás – a biztonság. Ez nagyon úgy hangozhat, mintha egy LAN (vagy VLAN) és egy WAN összekapcsolása lenne, de a VPN ennél sokkal több.
- A VPN-eket aszerint kategorizálják, hogy milyen szerepet játszanak egy vállalkozásban, mint például a vállalati menedzselt VPN-ek és a szolgáltató által menedzselt VPN-ek.

Vállalati egységek közti VPN (Site to Site VPN)

- Két autonóm hálózatot köt össze
- Az összeköttetés titkosított
- A kliensek szempontjából rejtett
- IKEv2-IPsec

Kliens-szerver felépítés

- A felhasználó gépe és egy privát hálózat közt létesít titkosított kapcsolatot
- A Cisco ASA eszközei által biztosít ilyen szolgáltatást
- Nyílt forráskódú elterjedt megoldás az OpenVPN

IP hozzáférési listák – IP Access List – ACL

- Egy lista, amely alapján eldönti egy router, hogy továbbítja az adott csomagot vagy nem
- A döntés történhet MAC cím, IP cím vagy TCP/UDP portszám alapján
- Minden router minden egyes interfészen, mind a bejövő, mind a kimenő irányban képes különböző ACL-t engedélyezni különböző szabályokkal

ACL alkalmazása bejövő vagy kimenő forgalomra

- Egy csomag szűréséhez engedélyeznie kell az adott interfészen egy ACL-t, amely feldolgozza a csomagot ugyanabban az irányban, ahogy a csomag átfolyik az adott interfészen

ACL felépítése

- Amikor IP ACL-eket használunk csomagok szűrésére, két művelet közül csak az egyiket választhatjuk. A konfigurációs parancsok a deny és a permit kulcsszavakat használják, a deny eldobja a csomagot, illetve a permit engedélyezi a csomag továbbhaladását, mintha az ACL nem is létezne.

- Az ACL-ek az első találat logikáját használják. Ha egy csomag megfelel az ACL egyik sorának, a router az adott sorában felsorolt műveletet hajtja végre, és nem keres tovább az ACL-ben.
- Minden ACL utolsó bejegyzése automatikusan blokkol minden csomagot.

Wildcard maszk

- A Wildcard maszk segítségével lehet egy IP tartományt tesztelni
- Ahol decimális 0: a router ezt az oktettet össze kell hasonlítsa
- Ahol decimális 255: a router figyelmen kívül hagyja ezt az oktettet, mivel úgy tekinti, hogy az már létezik
- Ahol a wildcard maszk bináris 1 azt a részt nem kell összehasonlítani

Kiterjesztett (Extended ACL)

- Ahogy a neve is mutatja, a forrás IP cím mellett további paraméterek alapján is képes szűrni
- A lehető legközelebb kell elhelyezni a csomagok forrásához, mivel ez sávszélességet takarít meg.

Nevezett (Named) ACL

- Számok helyett nevek használata az ACL azonosítására, így könnyebb megjegyezni

Tűzfalak

- Hagyományosan a tűzfal minden csomag továbbítási útvonalában van beágyazva, így a tűzfal képes eldönteni, hogy mely csomagokat dobja el, és melyeket engedje át.
- Ezáltal a tűzfal védi a hálózatot a különböző problémáktól azáltal, hogy csak a kívánt típusú csomagokat engedi át.
- Valójában a tűzfalak a legalapvetőbb formában ugyanazt a munkát végzik, mint a routerek az ACL-ekkel, de a tűzfalak sokkal több opcióval rendelkeznek, valamint más biztonsági feladatokat is elvégezhetnek.

Tűzfal zónák

- Három zóna: Bent (inside), Kint (outside), DMZ
- Általában ez alapján döntünk egy csomag blokkolásáról vagy átengedéséről.

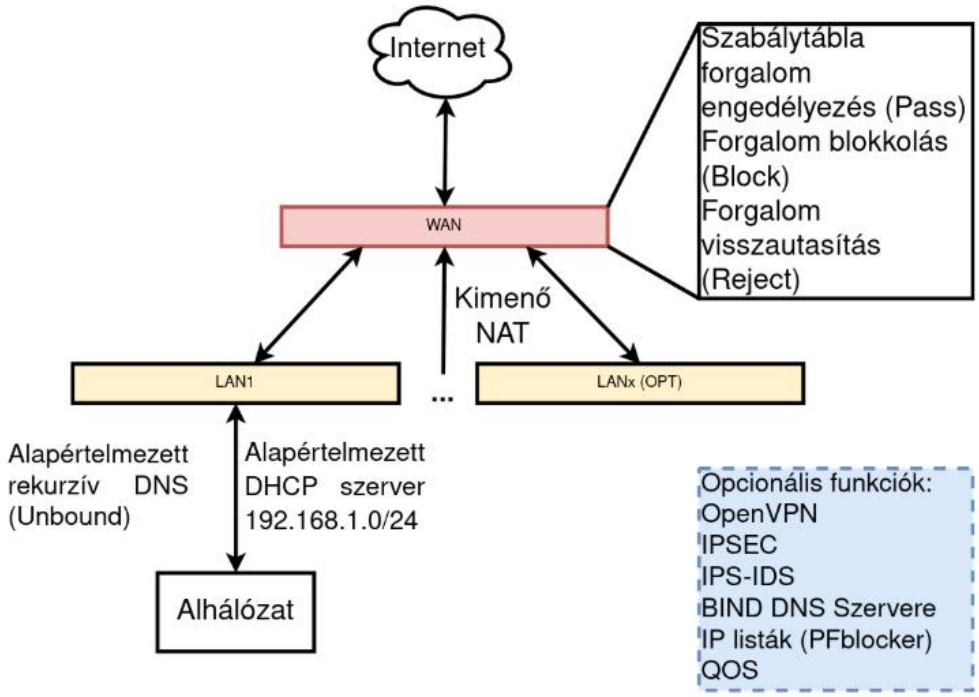
Behatolásmegelőző rendszer (Intrusion prevention Systems) – IPS

- Hagyományosan a tűzfal a felhasználó által konfigurált szabályok alapján működik, amellyel a csomagok a hálózaton belüli áramlást engedélyezni kell. A tűzfalnak a csomagok útjában kell állnia, hogy szűrni tudja a csomagokat,

átirányítsa őket gyűjtés és későbbi elemzés szempontjából, vagy hagyja, hogy a csomagok átjussanak a célállomás felé.

- A hagyományos IPS a csomagok útvonalában is állhat és szűrni tudja a csomagokat, de a döntéseket más logika alapján hozza meg. Az IPS először letölti az exploit adtbázisát. Ezután képes megvizsgálni a csomagokat, összehasonlítja őket az ismert exploitokkal, és észreveszi, ha a csomagok egy ismert exploit részei lehetnek. Ha azonosították, az IPS naplózhatja az eseményt, és eldobhatja a csomagokat, vagy akár átirányíthajtaj a csomagokat egy másik biztonsági alkalmazáshoz további vizsgálat céljából.

PFSense felépítés



Szerverek

- Hardver: A megfelelő hardver kiválasztása kulcsfontosságú szerepet játszik egy szerver telepítésekor. Megfelelő hardver kell a szolgáltatások biztosításához.
- Operációs rendszer: Az operációs rendszer kiválasztása fontos szempont a szerver telepítésekor. Az operációs rendszernek illeszkednie kell a szerver alkalmazásokhoz, és biztonságosnak kell lennie.
- Biztonság: A szerver biztonsága az egyik legfontosabb szempont a szerver telepítésekor. A szervernek biztonságosan kell működnie, és meg kell védenie az adatokat a károkozóktól és a jogosulatlan hozzáférésektől.
- Teljesítmény: A szerver teljesítménye az ügyfelek számára fontos szempont. A szervernek képesnek kell lennie arra, hogy nagy forgalmat kezeljen, és hatékonyan futtassa az alkalmazásokat.

- Támogatás: A szerver telepítésekor fontos, hogy a szolgáltatótól megfelelő támogatást kapjunk. A szerver üzemeltetése és karbantartása bonyolult folyamatokat igényelhet, ezért fontos, hogy a szolgáltató megbízható támogatást nyújtson.
- Felhasználói interfész: A szerver telepítésekor opcionális szempont az is, hogy milyen felhasználói interfészt kínál. Az egyszerű és könnyen használható felhasználói felület lehetővé teszi, hogy könnyen konfigurálhassuk és kezeljük a szerverünket.

Szerver harver

- Raid vs ZFS (backup)
- CPU teljesítmény, biztonság (Spectre meltdown)
- RAM ECC
- PSU redundancia teljesítmény
- Grafikus gyorsító

Operációs rendszer

- Linux vs Windows
- Microsoft szolgáltatások (Windows preferált): Outlook, Active Directory, ASP.NET
- Biztonság: zártkörű vagy nyílt forráskód
- Feladat optimizált

RedHat Linux

- Vállalati környezetben nagyon népszerű
- Magas szintű biztonság: széles körben használják kritikus fontosságú környezetekben
- Stabilitás és megbízhatóság
- Csomagkezelés: RPM csomagkezelő rendszert használ, amely könnyíti a szoftvercsomagok telepítését, frissítését és kezelését
- Skálázhatóság
- Támogatás: részletes dokumentáció, illetve képzések

Selinux

- Biztonsági megerősítés a kernelbe építve
- MAC (Mandatory access control) alapú biztonság

Selinux típusok

- A selinux típusok (type) különböző fájlok és mappák csoportosítására szolgálnak, amelyek ugyanabba a biztonsági környezetbe, sémába tartoznak pl. httpd_sys_content_t objektumok a /var/www mappában

Selinux domain

- Minden folyamat egy ilyenben fut, amely meghatározza, hogy a folyamat mihez fér hozzá
- pl. named_t a named (DNS) folyamat domainje
- unconfined_t azon folyamatok amelyek nincsenek explicit a Selinux által meghatározva

Selinux szerepek

- A szerepek meghatározzák mely felhasználók vagy folyamatok milyen doméniumokat vagy milyen típusokat érhetnek el
- A folyamatok és felhasználók válthatnak szerepet ha ez meg van határozva a Selinux szabályrendszerében
- pl. user_r felhasználói domén, sysadmin_r rendszergazda

Selinux biztonsági indetitás

- Minden folyamathoz vagy objektumhoz hozzá van rendelve a rendszerben (security context)
- identity:role:domain
- identity:role:type
- pl. system_u:system_r:httpd_t

Szerep alapú hozzáférés

- A felhasználók szerepekhez vannak rendelve
- A szerepek doméniumokhoz és típusokhoz vannak rendelve

DAC vs MAC

- Directory Access Control
    - Unix csoportok, engedélyező bitek és kiterjesztett engedélyező bitek
    - A tulajdonos vezérli a hozzáférési jogokat
- Mandatory Access Control
    - Központi biztonsági szabályok
    - A felhasználók nem tudják módosítani
    - A rendszergazda határozza meg pontosan melyik folyamat mihez férhet hozza

SSH protokoll

- A Secure Shell egy kriptográfiai hálózati protokoll, amely biztonságos módot biztosít egy távoli számítógép vagy kiszolgáló elérésére egy nem biztonságos hálózaton keresztül.
- Alapértelmezetten TCP protokollra épül a 22-ed porton
- Az SSH szállítási réteg protokoll szimmetrikus titkosítási- és üzenethitelesítési algoritmusokat használ, illetve nyílvános kulcsú kriptográfiát.

- Az SSH felhasználói hitelesítési protokoll felelős az ügyfél hitelesítéséért a kiszolgálóval szemben. A felhasználói hitelesítési protokoll többféle hitelesítési módszer támogat, többek között a jelszó alapú, a nyilvános kulcs alapú és a host alapú.
- Az SHH-kapcsolati protokoll felelős az SSH-munkamenet kezeléséért az ügyfél és a kiszolgáló között. A kapcsolati protokoll számos funkciót tartalmaz, például X11-továbbítás vagy port-továbbítás, és SFTP

Apache Webszerver (httpd)