# ACL

ACCESS CONTROL LIST

# TŰZFALAK

- A tűzfalak védik a hálózatokat és azok állomásait a külvilág felől érkező nem kívánt és esetlegesen ártalmas üzenetek ellen.
- Azokat a tűzfalakat, amelyek hálózatokat védenek hálózati túzfalaknak nevezzük
- Amelyek állomásokat védenek személyi tűzfalaknak nevezzük

# HÁLÓZATI TŰZFALAK

- Hardveres tűzfal: gyors, nagy teljesítményű és drága célharver
- Szoftveres tűzfal: egy általános célú eszközön (számítógépen) telepítünk egy tűzfalszoftver és az látja el a túzfal funkciókat. Teljesítménye nagyban függ az eszköz hardverétől
- Beépített tűzfal: hálózati eszközökbe a gyártó által telepített tűzfal

Az ACL-ek ilyen beépített tűzfalak

# ACL

- Az ACL-ek listák, amelyeket soronként értékel ki a router
- Minden sorban van egy feltétel (milyen üzenettel?) és egy utasítás (mit tegyen: eldobás, továbbítás). Ha teljesül a feltétel a router végrehajta utasítást és befejezi az ACL-t
- Ha végigér a listán és nincs megfelelő feltétel a router eldobja az üzenetet (minden ACL-ben kell lennie egy továbbítást engedélyező utasításnak)!

# ACL-EK TÍPUSAI

- Normál ACL: csak az üzenet forrás IP címét ellenőrzi
- Kiterjesztett ACL: az üzenet forrás IP címét, forrás portját (küldő alkalmazás), cél IP címét, célportját (fogadó alkalmazás) és állapotát (ha van) képes szűrni.
- A normál ACL-ek 1-99-ig és
- A kiterjesztett ACL-ek 100-199-ig vannak számozva.

# ACL-EK SZERKESZTÉSE

- Az ACL-t minden sorát egy paranccsal adjuk meg
- Egy ACL megadásakor végig ugyanazt a számot használjuk pl:1
- Az új sorok mindig az ACL végére kerülnek
- A már beírt sorok nem módosíthatók, ha elrontottál valamit ki kell törölni az egész ACL-t! Érdemes a hosszabb ACL-t szövegszerkesztőben előre megírni!
- 1-es számú ACL törlése:

```
R1(config)# no acces-list 1
```

# NORMÁL ACL

- Létrehozása:

```
R1(config)# access-list 1 permit host 192.168.1.1
```

- Access-list 1: 1-es számú ACL, minden sorát az ACL-nek ezzel a számmal kell megadni
- Permit: engedélyezés (az üzenet eldobása: deny), ez az utasítás
- Host 192.168.1.1: ez a feltétel (lehet még any: mindenki, és 192.168.1.0 0.0.0.255 – ez a 192.168.1.0/24 –es hálózat helyettesítő maszkkal)

# NORMÁL ACL ELHELYEZÉSE

- Miután megvan a lista, meg kell adni, hogy hol használjuk. Ez lehet egy interfész, vonal, vagy egy szolgáltatás. **Mindig** a célhálózathoz **lehető legközelebb kell** elhelyezni! Oda ahol tiltott/engedélyezett a kiszűrt forrás!
- Interfész esetén:

```
R1(config-if)# ip access-group 1 out
```

Ip access-group 1: 1-es ACL-t akarjuk elhelyezni

Out: az interfész által kiküldött üzeneteket szűrjük (in: a bejövőket szűri)

- Vonal esetén (pl: line vty):

```
R1(config-line)#access-class 1 in
```

# KITERJESZTETT ACL

- Létrehozása:

```
R1(config)#Access-list 100 permit tcp any host
192.168.1.1 eq 80
```

Access-list 100: 100-as ACL egy sora

Permit: engedélyező utasítás (deny a tiltó)

tcp: protokoll megadása (ip: minden, tcp, udp, icmp … szolgáltatás adja meg)

Any: forrás IP, itt mindenki (és port csak itt nem szűrjük a portot)

Host 192.168.1.1: cél IP cím, lehet még any és hálózat megadása is

Eq 80: célport (eq jelentése egyenlő =) – ez a http protokoll szűrését jelenti: webszerver és ez használja a korábban megadott tcp-t!

# KITERJESZTETT ACL

- További célport szűrések:
- Eq = (egyenlő)
- Gt > (nagyobb)
- Lt < (kisebb)
- Neq  <> (nem egyenlő)
- Range x y: x és y közötti portszám

# KITERJESZTETT ACL ELHELYEZÉSE

- Ezt a listát a csomag haladási útja mentén bárhol elhelyezhetjük a hatása ugyanaz.
- A legjobb hely mégis a forráshoz lehető legközelebbi, mert így jelenti a legkisebb terhelést a hálózat számára egy esetlegesen eldobásra kerülő csomag.
- Az elhelyezési parancsok megegyeznek a normál ACL-el csak itt az ACL száma 100-199-ig tart.