A kiterjesztett ACL-ek

A kiterjesztett ACL-ek sorba egymás után összehasonlítják az IP csomagok forrás és cél címeit az ACL-ben beállítottakkal, ami alapján szabályozzák a forgalmat. A kiterjesztett ACL segítségével lehetőség van a következők szűrésére is:

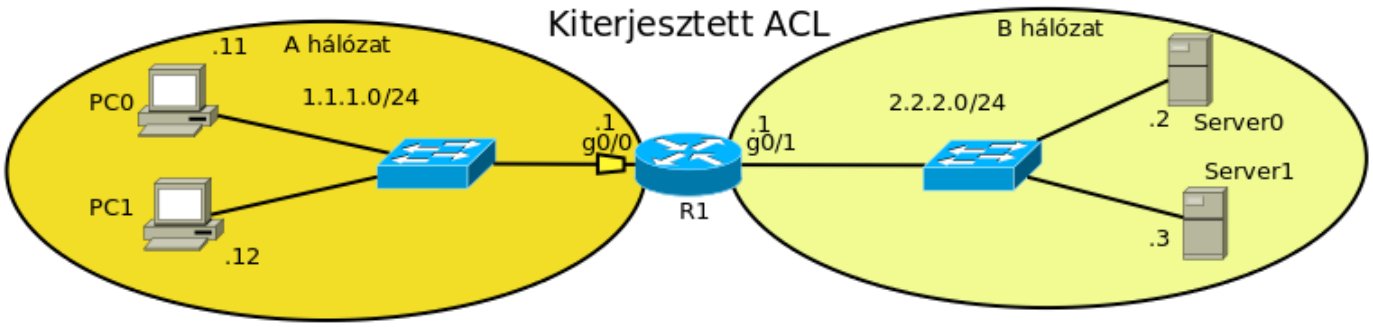
- protokoll
- port szám
- különböző szolgáltatáskódok (DSCP)
- precedencia alapján
- a szinkronizáló sorszám állapot alapján (SYN bit)

A parancs általános szintaxisa:

```
access-list lista_száma {deny | permit} protocol
forrás forrás_helyettesítő_maszk [forrásport]
cél cél_helyettesítő_maszk [célport]
```

Adott port tiltása

Szeretnénk egy adott szolgáltatás forgalmát letiltani. Legyen a példa kedvéért két hálózat, A és B. Mindként hálózatban két gép:



Szeretnénk tiltani a routeren a telnet elérését.

```
R1(config)#int g0/0
R1(config-if)#ip access-group 120 out
R1(config-if)#exit
R1(config)#access-list 120 deny tcp any any eq 23
R1(config)#access-list 120 permit ip any any
```

A szervereken a web tiltása a forgalomirányítón:

```
R1(config)#int g0/0
R1(config-if)#ip access-group 100 in
R1(config-if)#exit
R1(config)#access-list 100 deny tcp any any eq 80
R1(config)#access-list 100 permit ip any any
```

Elemezzük a tiltó parnacsot:

```
R1(config)#access-list 100 deny tcp any any eq 80
```

- 100 - az ACL bejegyzés száma - ACE (Access Control Entry)
- deny - tiltás

- Illeszkednie kell a csomagnak a következőkre:
  - tcp - TCP forgalom legyen
  - any - (első any) bárhonnan jön - forrás
  - any - (második any) bárhova megy - cél
  - eq 80 - célport 80 (webszerver)

Láthatjuk, hogy csak a webes elérés van tiltva. Bármelyik PC-ből ha böngészőben megpróbáljuk megnézni a bármelyik szerver weblapját, az nem elérhető.

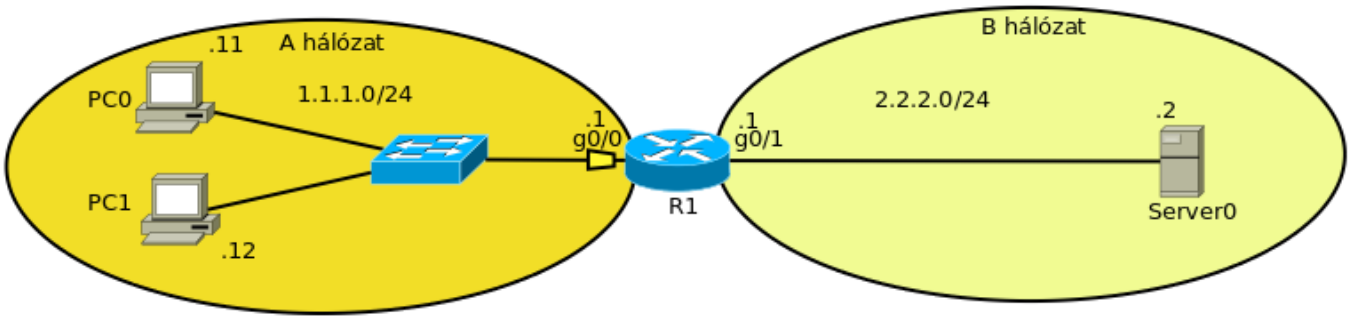
Ha viszont, bármely PC-ről a ping paranccsal megvizsgálom a kapcsolatot a szerverekhez, a kapcsolat működni fog. Működnie is kell mivel a ping ICMP protokollt használ.

FTP tiltása

Ha FTP-t használunk mindig két csatorna épül ki egy kapcsolathoz. Egy **vezérlő** és egy **adat** csatorna. Bármelyiket tiltjuk a a kapcsolatot megakadályoztuk.

A következő példában az FTP kapcsolat vezérlő és adat csatornáját tiltjuk.

Topológia:



Beállítások:

```
R1(config)#int g0/0
R1(config-if)#ip access-group 100 in
R1(config-if)#exit
R1(config)#access-list 100 deny tcp any any eq ftp
R1(config)#access-list 100 deny tcp any any eq ftp-data
R1(config)#access-list 100 permit ip any any
```

Lista ürítése:

```
R1(config)#no access-list 100
```

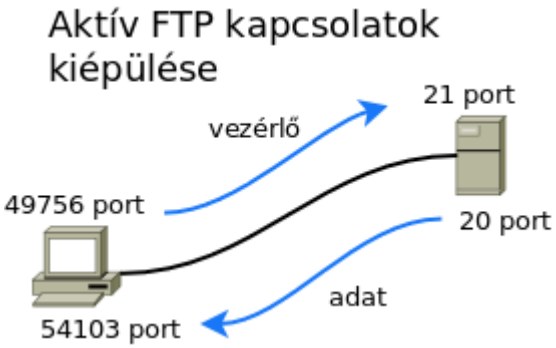
Szolgáltatások engedése

```
access-list 101 permit tcp 192.168.10.0 0.0.0.255 any eq 23
access-list 101 permit tcp 192.168.10.0 0.0.0.255 any eq 21
access-list 101 permit tcp 192.168.10.0 0.0.0.255 any eq 20
access-list 101 permit tcp 192.168.10.0 0.0.0.255 any eq telnet
access-list 101 permit tcp 192.168.10.0 0.0.0.255 any eq ftp
access-list 101 permit tcp 192.168.10.0 0.0.0.255 any eq ftp-data
```

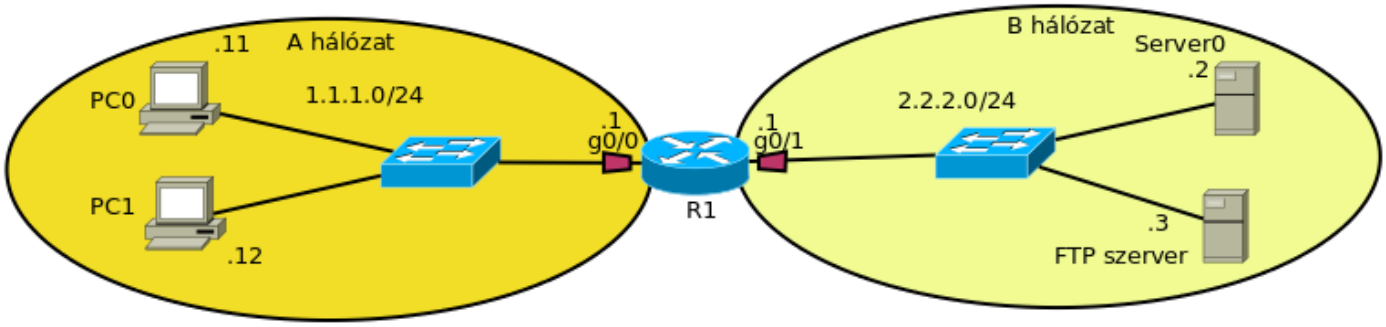
Aktív FTP engedése

Az FTP kapcsolat lehet aktív és passzív.

Aktív kapcsolat esetén a kliens kiépít egy kapcsolatot a szerver 21-es portjára. A szerver is kiépít saját 20-as portjáról egy adatkapcsolati csatornát a kliens felé.



Aktív FTP kapcsolat engedélyezése:

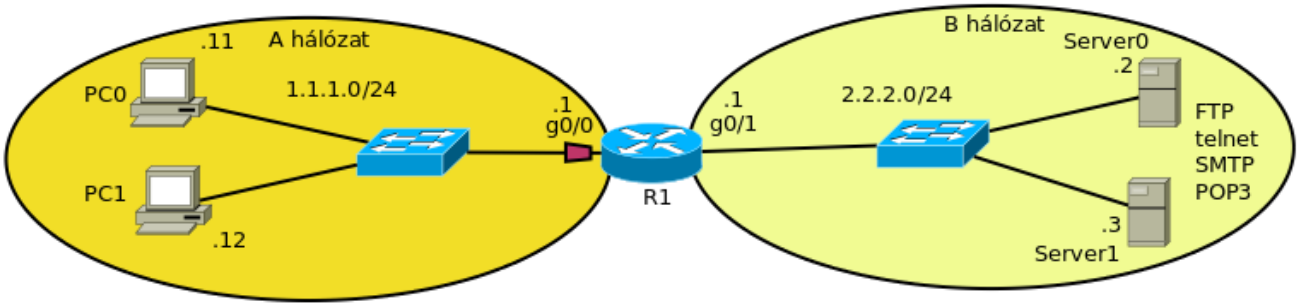



```
R1(config)#int g0/0
R1(config-if)#ip access-group 100 in
R1(config-if)#exit
R1(config)#access-list 100 permit tcp any host 2.2.2.3 eq ftp
R1(config)#access-list 100 permit tcp any host 2.2.2.3 eq 20

R1(config)#int g0/1
R1(config-if)#ip access-group 101 in
R1(config)#exit
R1(config)#access-list 101 permit host 2.2.2.3 eq ftp any
R1(config)#access-list 101 permit host 2.2.2.3 eq 20 any
```

Több szolgáltatás engedése

A www, telnet, smtp, pop3 és ftp engedése. Tegyük fel, hogy az előbbi szolgáltatásokat szeretnénk elérni a B hálózat egyik szerverén:



Megvalósítás a következő módon:

```
R1(config)#int g0/0
R1(config-if)#ip access-group 100 in
R1(config-if)#exit
R1(config)#access-list 100 permit tcp any any eq www
R1(config)#access-list 100 permit tcp any any eq telnet
R1(config)#access-list 100 permit tcp any any eq smtp
R1(config)#access-list 100 permit tcp any any eq pop3
R1(config)#access-list 100 permit tcp any any eq 21
R1(config)#access-list 100 permit tcp any any eq 20
```