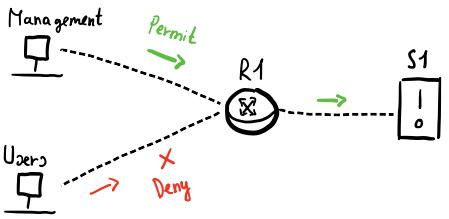
Forgalomirányítókon megvalósítható csomagszűrés

- Access Control List - ACL
  - Rendeltetése
    - Hozzáférés szabályozás vagy hálózati forgalom szűrésére szolgál.
    - Router csomagszűrőként viselkedik, amikor továbbítja vagy eldobja a csomagokat.
    - Egy ACL permit és deny állítások sorrendezett listája.



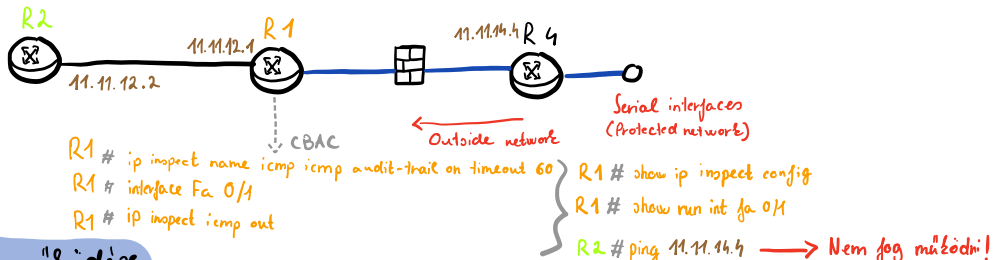
- ACL elhelyezése a hálózatban
  - Minden ACL-t oda kell elhelyezni, ahol a legnagyobb hatékonysággal képes szűrni.
  - Extended ACL -> Lehető legközelebbi forgalom forráshoz kell rakni.
  - Standard ACL -> Nem határozza meg a célcímet, ezért a célállomáshoz közel kell rakni.
- ACL típusok
  - Számozott -> Szűrés csak forráscím alapján
    - Standard ACL -> (1-99-ig és 1300-1999-ig) = 3. rétegbeli szűrés
    - Extended ACL -> (100-199-ig és 2000-2699-ig) = 3. és 4. rétegbeli szűrés
  - Nevesített -> Szűrés port, forrás/cél cím alapján
    - Csak betűk és számokból állhat a neve -> Javasolt nagybetűs
- ACL konfigurálás lépései

Konfiguráció:
- Szabályok
  - One ACL per Protocol -> Az interfészen értelmezett minden protokollhoz külön lista kell.
  - One ACL per Direction -> ACL-ek egyszerre csak egy irányban vizsgálnak forgalmat. (Egy interfészen a "kimenő"/"bemenő" irányba két külön ACL kell.)
  - One ACL per Interface -> ACL-ek egy adott interfészen értelmezendőek.

1. ACL céljának meghatározása
2. ACL létrehozása
3. ACL alkalmazása
4. ACL tesztelése, például tesztcsomagok küldésével.

• Context-Based Access Control - CBAC

- Fő funkciói
  1. Állapotfelső szűrés - Stateful Packet Filtering -> Nem csak hálózati és szállítási réteg információk alapján vizsgálja a visszonyok állapotát, hanem alkalmazási réteg információkat is.
  2. Forgalom figyelés - Traffic Inspection -> SYN Flood támadások, TCP sorszámozást figyel és gyanúsakat eldobja.
  3. Behatolás érzékelés - Intrusion Detection -> Syslog üzenetek átvizsgálásával ki lehet szűrni az SMTP támadások és SYN Flood támadások nagyságát, ezeket a kapcsolatokat eldobja és riasztást, értesítést küld a rendszernek.



• CBAC működése

- TCP, UDP és ICMP kapcsolatokról információt tárol az állapot táblában. (state table)
- Állapot tábla alapján dinamikusan ACL-t hoz létre a visszajövő csomagok számára.
- CBAC ideiglenes nyílásokat hoz létre megadott kapcsolathoz, amik beengedik a blokkolt forgalmat.
- Az állapottábla automatikusan frissül a forgalom áramlásának megfelelően.

• CBAC konfigurálása

1. Interfész kiválasztása -> Belső interfész ahonnan indulhat egy visszony felépítés.
2. ACL konfigurálás az interfészen -> Milyen típusú forgalmat engedélyezünk az interfészen
   - Alap konfiguráció, hogy a belső hálózatból a külső hálózatig mindent, de a külső hálózatból a belső hálózatig semmit.
   - Engedélyezzük azt a forgalmat, amit meg kell vizsgálni a CBAC-nak.
   - Implicit deny-t legyük explicitté a naplózás miatt.
3. Inspection rule megadása a vizsgált forgalomra
4. Alkalmazás a megfelelő interfészen.

• Zone-Based Policy Firewall - ZPF

- ACL-től független
- Mindent tiltunk, amíg külön nem engedjük.
- Házirend minden forgalomra hatással van, így nem kell külön több ACL / ellenőrzési művelet.

• ZPF funkciói

- Inspect
  - Automatikusan beengedi a válasz forgalmat.
  - Támogatja azokat a protokollokat, amik több párhuzamos kapcsolat felépítését igénylik.
- Pass
  - Hasonló az ACL permit-hez
  - Nem követi a kapcsolat állapotát
  - Csak egy irányban engedi át a forgalmat
  - Megfelelő szabályt kell alkalmazni a válasz forgalom beengedésére.
- Drop
  - Hasonló az ACL deny-hez
  - Blokkolt csomagok naplózása

• Tervezési szabályok

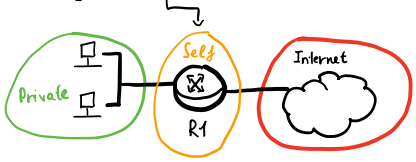
- Zónát kell konfigurálni, mielőtt interfészt hozzárendelhetünk.
- Egy interfész egy biztonsági zónához rendelhető → Implicitlen a forgalom közöttük engedélyezett.
- Különböző zónák közötti forgalom engedélyezéséhez policy-t kell konfigolni
  - Zónabeli és nem zónabeli közötti forgalom nem engedélyezett.
- Zónák közötti események megadása: pass, inspect, drop
- Nem zónához tartozó interfészen CBAC-ot lehet konfigolni.
- Ha egy interfészt nem akarunk zónához rendelni, akkor mindent átenged, amit policy-vel konfigolt zónába tehetünk.

• Konfiguráció

1. Tűzfal zónák létrehozása: # zone security
2. Forgalmi osztályok definiálása: # class-map type inspect
3. Tűzfal policy meghatározása: #
   - Alkalmazása zónapárok között: # zone-pair
4. Interfészek zónához rendelése: # zone-member securit

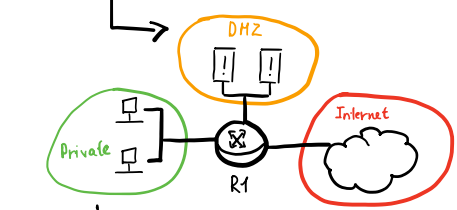
• ZPF zónák

- Self zóna → Ha a router, a forrása vagy a célállomása egy forgalomnak.



  - Alapértelmezetten a router interfészei a Self zóna tagjai.
  - Forgalomszabályok akkor is definiálhatóak, ha a zónapár egyik tagja se Self zóna.

- DMZ (perimeter hálózat) →
  - Szolgáltatásokat a külső hálózat irányába
  - Biztonságot nyújt, mivel a DMZ és a belső hálózatok között lesz még egy tűzfal



- Privát zóna
- Internet