Laboratorul 2 – Filtrare de trafic și Control Acces (Firewall)

Obiectiv: Securizarea rețelei utilizând regulile de firewall Mikrotik

Teme:

- Diferențierea între lanțurile input, forward, output
- Blocarea traficului invalid, a porturilor nesigure (ex: Telnet)
- Permiterea accesului doar din IP-uri autorizate
- Logarea tentativelor suspecte

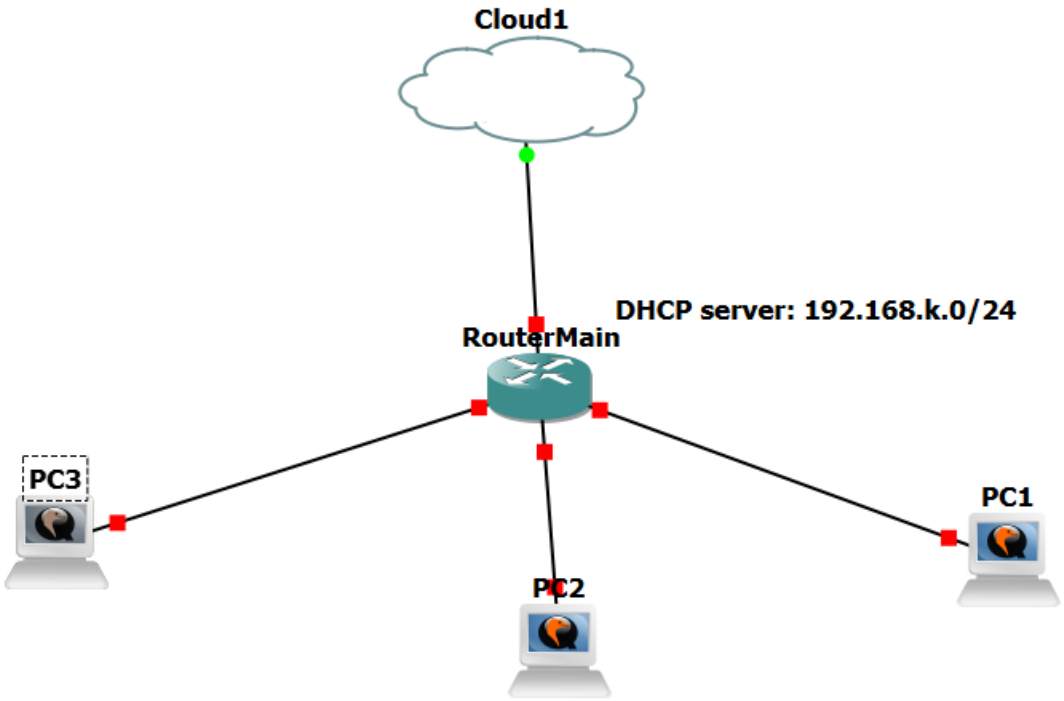
Dispozitive: Mikrotik CHR + Host-uri Ubuntu

Sustinere: Set de reguli firewall + justificare pentru fiecare regulă

Extensie Fortinet :

- Se poate adăuga un **FortiGate VM** ca firewall și router principal pentru a compara metodele de filtrare
- Configurare simplă: 2 reguli + logare trafic blocat

Topologia rețelei



Sarcini firewall (obligatorii)

1. **Reguli de bază**:
   - Permite `established, related` în input & forward.
   - Blochează `invalid`.
   - Politică implicită *drop* în input.
2. **Blocare porturi nesigure**:

    - Blochează **Telnet (TCP/23)** în input & forward.
3. **Acces administrativ doar din PC1**:
    - Permite-ți să acceseze routerul prin Winbox (8291), SSH (22) și ICMP.
    - Restul → deny + log.
4. **Restricții pe PC3 (Restricted)**:
    - PC3 (`10.10.k.x`) **NU are acces la anumite site-uri web**.
    - Lista site-urilor este stabilită în funcție de variantă (vezi mai jos).
    - Accesul la restul site-urilor și Internetului → permis.
5. **Logging**:
    - Toate deny-urile semnificative → log cu prefixe clare (`INPUT-DROP`, `FORWARD-DENY`, `BLOCKED-SITE`, etc.).

Site-uri blocate în funcție de variantă

Variante	Site blocat (PC3)
1, 5, 9, 13, 17	`facebook.com`
2, 6, 10, 14, 18	`wikipedia.com`
3, 7, 11, 15	`instagram.com`
4, 8, 12, 16	`tiktok.com`

Studentul cu **numărul de ordine k** configurează rețeaua `10.10.k.0/24` și blochează site-ul conform tabelului.

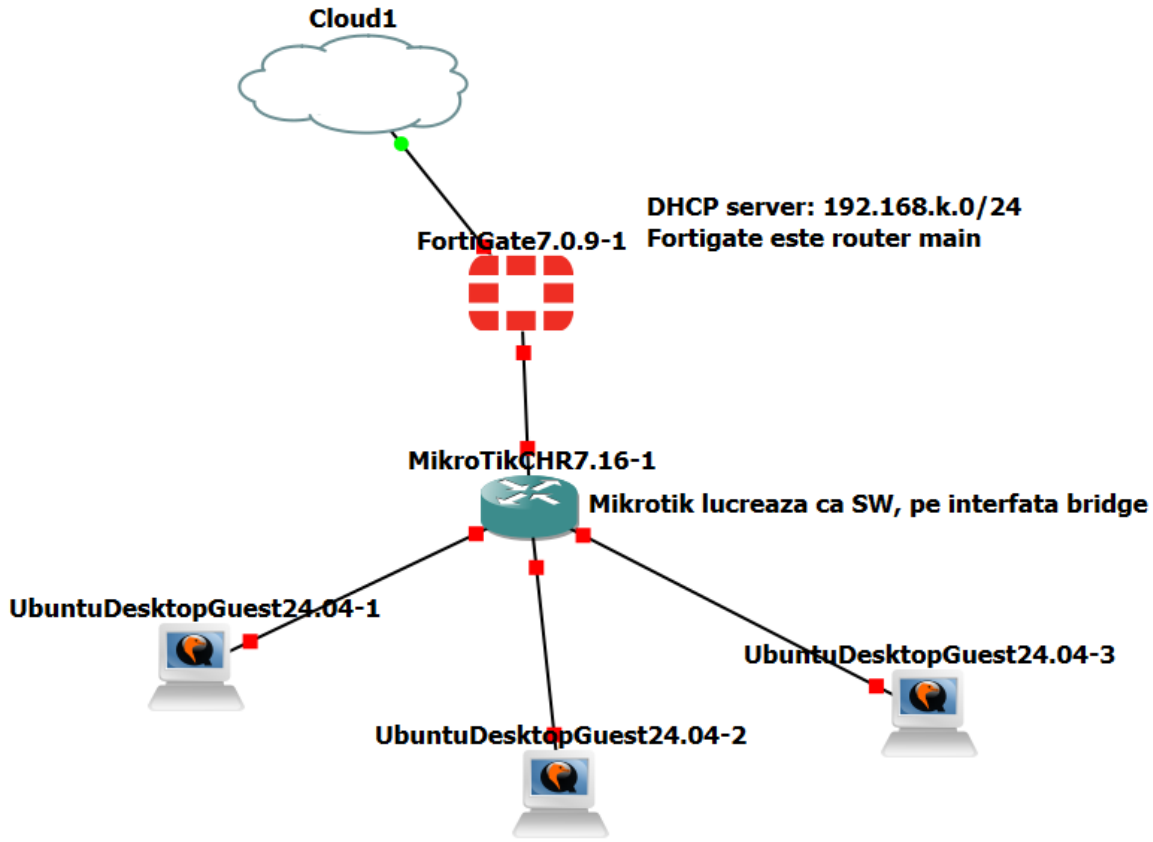
Teste obligatorii

1. **Input (către router)**:
    - PC1 → ping/SSH/Winbox router = **ALLOW**
    - PC2/PC3 → ping/SSH/Winbox router = **DENY + log**
2. **Forward (prin router)**:
    - PC2 → acces Internet = **ALLOW**
    - PC3 → acces la site blocat = **DENY + log**
    - PC3 → acces la alt site (ex. google.com) = **ALLOW**
3. **Porturi nesigure**:
    - `telnet 10.10.k.1` → **DENY + log**

Susținere

- Export reguli firewall (`/ip firewall export`) cu comentarii.
- Capturi de ecran:
    - tabel de teste (cine → ce → rezultat).
    - loguri cu prefixe.
    - acces reușit / acces blocat.
- Justificarea fiecărei reguli (1–2 fraze/regulă).

Extensie (opțională) – FortiGate VM



- Configurează 1 politică firewall similar pentru blocarea accesului la site-uri web:
- Demonstrează logarea traficului blocat.
- Compară modul de configurare față de MikroTik (GUI vs CLI, ordine politici, implicit deny, logging).
- Diferența dintre statefull firewall și stateless firewall.

!!! **Această extensie este opțională și se realizează doar de cei care doresc nota 9 sau 10.**