Exerciții de Firewall
- cu răspunsuri oferite -

(drd. Adam Mihai Gergely)

Scrieți regula sau regulile de firewall corespunzătoare enunțului problemei:

1. **Blocați total accesul calculatorului cu adresa 192.168.0.4 la Internet**

2. **Acceptați citirea de e-mail prin IMAP de la clasa de IP-uri 172.16.8.0/26 (serverul de e-mail se află pe sistemul local unde este și firewall-ul)**

3. **Blocați accesul pe toate porturile exceptând cel de navigat pe web pentru toate IP-urile, din orice clasă, care trec prin sistemul local**

4. **Blocați trimiterea de e-mail de peste tot către oriunde pentru traficul care trece prin sistemul local**

5. **Blocați interogările DNS de la clasa de IP-uri 192.168.0.0/24 către clasa de IP-uri 10.1.0.0/8**

6. **Accepați doar trafic de SSH către sistemul local, și doar de la computerul de management al unei companii, care are adresa IP 172.16.3.2**

7. **Blocați tot accesul la sistemul local**

8. **Permiteți tot accesul la sistemul local**

9. **Blocați tot traficul care trece prin sistemul local. Lăsați doar traficul care are ca destinație sistemul local sau care originează din sistemul local**

10. **Permiteți doar navigarea pe web către sistemul local, în rest tăiați orice alt trafic către sistemul local**

Răspunsuri

1. **iptables -t filter -I FORWARD -s 192.168.0.4 -j DROP**

2. **iptables -t filter -I INPUT -s 172.16.8.0/26 -p tcp --dport 143 -j ACCEPT**

3. **iptables -t filter -I FORWARD -p tcp --dport 80 -j ACCEPT**
   iptables -t filter -A FORWARD -j DROP

4. **iptables -t filter -I FORWARD -p tcp --dport 25 DROP**

5. **iptables -t filter -I FORWARD -s 192.168.0.0/24 -d 10.1.0.0/8 -p udp --dport 53 -j DROP**

6. **iptables -t filter -I INPUT -s 172.16.3.2 -p tcp --dport 22 -j ACCEPT**
   iptables -t filter -A INPUT -j DROP

7. **iptables -t filter -I INPUT -j DROP**

8. **iptables -t filter -I INPUT -j ACCEPT**

9. **iptables -t filter -I FORWARD -j DROP**

10. **iptables -t filter -I INPUT -p tcp --dport 80 -j ACCEPT**
    iptables -t filter -A INPUT -j DROP