# LINUX RENDSZERFEJLESZTÉS ÉS ÜZEMELTETÉS

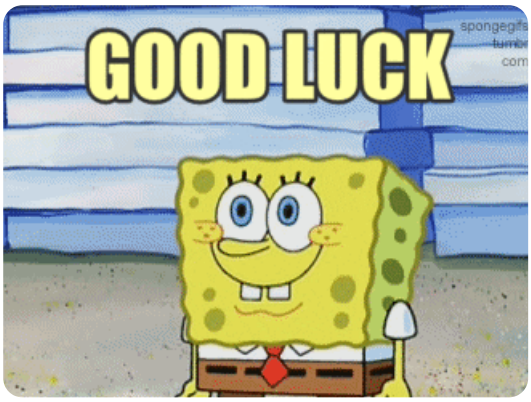
5. forduló

A kategória támogatója: One Identity - Quest Hungary

## Ismertető a feladatlaphoz

> Kezdj neki minél hamarabb, mert a feladatot a forduló záró időpontjáig lehet befejezni, nem addig lehet elkezdeni!

Sok sikert!




## 1. feladat 0 pont

Hogyan lehet megvalósítani egy olyan iptables szabályt, amely csak azokat a TCP kapcsolatokat engedi át, amelyek a 80-as vagy a 443-as porton kezdődtek, és amelyeknek a SYN, ACK és FIN csomagjai mind ugyanazon az interfészen érkeztek és távoztak?

### Válasz

- Ezt a szabályt úgy lehet megvalósítani, hogy használjuk a conntrack modult, amely képes nyomon követni a kapcsolatok állapotát és irányát, és használjuk a --ctstate és a --ctdir opciókat. Például:

```
iptables -A FORWARD -p tcp -m multiport --dports 80,443 -m conntrack --ctstate
iptables -A FORWARD -p tcp -m multiport --sports 80,443 -m conntrack --ctstate
iptables -A FORWARD -p tcp -m conntrack --ctstate RELATED,INVALID -j DROP
```

- Ezt a szabályt úgy lehet megvalósítani, hogy használjuk a state modult, amely képes nyomon követni a kapcsolatok állapotát, és használjuk a --state opciót. Például:

```
iptables -A FORWARD -p tcp -m multiport --dports 80,443 -m state --state NEW -
iptables -A FORWARD -p tcp -m multiport --sports 80,443 -m state --state ESTAE
iptables -A FORWARD -p tcp -m state --state RELATED,INVALID -j DROP
```

- Ezt a szabályt úgy lehet megvalósítani, hogy használjuk az interface modult, amely képes megadni az interfészek nevét vagy címét, és használjuk az -i és az -o opciókat. Például:

```
iptables -A FORWARD -p tcp -m multiport --dports 80,443 -i eth0 -o eth0 -j ACC
iptables -A FORWARD -p tcp -m multiport --sports 80,443 -i eth0 -o eth0 -j ACC
iptables -A FORWARD -p tcp ! -i eth0 ! -o eth0 -j DROP
```

## 2. feladat 1 pont

Egy Debian Linux rendszert használunk a lokális hálózatunk átjárójaként. Az átjáró két független internet vonali kapcsolattal rendelkezik.

```
eth0, gw:10.0.10.1
eth1, gw:10.1.0.1
LAN (eth2): 192.168.1.0/24
```

Az OpenVPN kapcsolat biztonsági megfontolásokból az eth1-es vonalon, míg az összes többi kimenő forgalmat az eth0 kapcsolaton szeretnénk továbbítani.

Az alábbi konfigurációt használjuk. Hogyan folytatódik az alábbi parancs, ha az iptables által megjelölt forgalmat szeretnénk kezelni?

```
iptables -t mangle -A OUTPUT -p tcp --dport 501 -j MARK --set-mark 2
```

route:

```
ip route add table 100 default via 10.1.0.1 dev eth1

ip rule add [???]

ip route flush table main
ip route add default via 10.0.10.1 dev eth0
```

## Válaszok

## 3. feladat 1 pont

Két szolgáltatás között szeretnénk TCP terhelés elosztást kialakítani Linux átjárón.

Melyik megoldás valósítja meg az egyenlő terhelés elosztást?

## Válasz

```
iptables -A PREROUTING -t nat -p tcp -d 192.168.1.1 --dport 27017 \
         -m statistic --mode random --probability 0.5             \
         -j DNAT --to-destination 10.0.0.2:1234

iptables -A PREROUTING -t nat -p tcp -d 192.168.1.1 --dport 27017 \
         -m statistic --mode random --probability 0.5             \
         -j DNAT --to-destination 10.0.0.3:1234
```

```
iptables -A PREROUTING -t nat -p tcp -d 192.168.1.1 --dport 27017 \
         -m statistic --mode random --probability 0.5             \
         -j DNAT --to-destination 10.0.0.2:1234

iptables -A PREROUTING -t nat -p tcp -d 192.168.1.1 --dport 27017 \
         -j DNAT --to-destination 10.0.0.3:1234
```

```
iptables -A PREROUTING -t nat -p tcp -d 192.168.1.1 --dport 27017 \
         -j DNAT --to-destination 10.0.0.2:1234
```

```
iptables -A PREROUTING -t nat -p tcp -d 192.168.1.1 --dport 27017 \
         -j DNAT --to-destination 10.0.0.3:1234
```

Megoldások beküldése