

**AUFGABE :**

Beschreiben Sie die Bedeutung der unten aufgelisteten iptables Befehle (siehe : Syntax-Beschreibung) :

```
iptables -F
iptables -A INPUT -p tcp -s 192.168.1.0/24 -j ACCEPT
iptables -A INPUT -p tcp !-syn -j DROP
iptables -A INPUT -p tcp -dport 113 -j ACCEPT
iptables -A INPUT -p udp -s 192.168.1.0/24 -j ACCEPT
iptables -A INPUT -p udp -sport 53 -j ACCEPT
iptables -P FORWARD DROP
iptables -A FORWARD -s 192.168.1.0/24 -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Löscht alle Regelketten (-F = flush)

Alle TCP-Datenpakete der Source-IP Netz-Adresse werden akzeptiert (input)

Alle TCP-Pakete die kein SYN-Flag enthalten werden verworfen

Alle TCP-Pakete mit dem Zielport 113 werden akzeptiert

Alle UDP-Pakete der Source-IP Netz-Adresse werden akzeptiert (input)

Alle UDP-Pakete mit dem Source-Port 53 werden akzeptiert

Default Policy: Alle Forward Datenpakete werden DROP verworfen (Whitelist)

Forward Datenpakete aus dem o.g. Netz (Source-IP) werden erlaubt

Alle Datenpakete einer bereits aufgebauten Verbindung werden akzeptiert (input)

Entwerfen Sie selbst Befehlsfolgen für folgende Szenarien :

Erlauben des loopback Datenverkehrs

Alle Rechner aus dem internen Netz (192.168.1.0/24) werden am Interface eth0 und eth1 explizit erlaubt

Alle Rechner mit externer IP-Adresse werden am Interface eth0 abgewiesen und protokolliert

Alle Rechner mit interner IP-Adresse (192.168.1.128/23) werden am Interface ppp0 abgewiesen mit Rückmeldung

```
iptables -A INPUT -i lo -j ACCEPT    iptables -A OUTPUT -o lo -j ACCEPT
```

```
iptables -A INPUT -i eth0 -s 192.168.1.0/24 -j ACCEPT
```

```
iptables -A INPUT -i eth1 -s 192.168.1.0/24 -j ACCEPT
```

```
iptables -A OUTPUT -o eth0 -d 192.168.1.0/24 -j ACCEPT
```

```
iptables -A OUTPUT -o eth1 -d 192.168.1.0/24 -j ACCEPT
```

```
iptables -A INPUT -i eth0 -s !192.168.1.0/24 -j LOG -j DROP
```

```
iptables -A INPUT -i eth0 -s !192.168.1.0/24 -j LOG-DROP
```

```
iptables -A INPUT -i ppp0 -s 192.168.1.128/23 -j REJECT
```