

Block IPs /Docker

Docker umgeht teilweise die normalen iptables-Regeln, weil es eigene Regeln und Chains anlegt.

Docker setzt eigene Chains wie:

- DOCKER
- DOCKER-USER

☐ Traffic zu Containern wird oft **vor den normalen INPUT-Regeln verarbeitet**.

Deshalb greifen die Block-Regeln nicht wie erwartet.

Die Lösung: DOCKER-USER Chain nutzen

Docker hat extra eine Chain vorgesehen, damit man genau sowas machen kannst:

```
sudo iptables -I DOCKER-USER -s 192.168.1.100 -j DROP
```

☐ Wichtig:

- -I (insert) statt -A, damit die Regel **ganz oben** landet
 - Diese Chain wird **immer vor Docker-Regeln ausgewertet**
-