

Kurzreferenz zur Wartung des Sicherheitssystems des DN-Netzes

1. Erstellen neuer iptables-Regeln

- Iptables Regeln bestehen aus Aufruf, (Tabelle), Kette, Protokoll, Quelle/Ziel, Match und Target.
- Pakete die von Snort-Inline inspiziert werden sollen, müssen hinsichtlich ihres Zustandes markiert werden, bevor sie in die Queue geschoben werden.

```
iptables -t mangle -A FORWARD Protokoll Quelle Ziel -m state --state NEW -j MARK --set-mark 1
```

- Grundsätzlicher Aufbau einer iptables-Regel:



