

Ralf Spenneberg

# Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6  
für Linux-Server und -Netzwerke



 ADDISON-WESLEY

---

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England  
Don Mills, Ontario • Sydney • Mexico City  
Madrid • Amsterdam



# 22 Die Raw-Tabelle

Die Raw-Tabelle wurde eingeführt, um Pakete, bevor sie vom Connection Tracking erfasst werden, bereits behandeln zu können. Die wichtigste Idee ist hierbei die Umgehung des Connection Tracking für bestimmte Pakete. Dies ist erstmalig mit der Raw-Tabelle möglich.

## 22.1 Die Raw-Tabelle

Die Raw-Tabelle besitzt zwei Ketten: `PREROUTING` und `OUTPUT`. Außerdem existieren zwei Targets, die nur in der Raw-Tabelle verwendet werden dürfen: `NOTRACK` und `TRACE`.

Mit dem Erscheinen der Raw-Tabelle existiert nun auch ein neuer Zustand, der mit dem `state`-Test geprüft werden kann: `UNTRACKED`.

Die Raw-Tabelle bietet Ihnen den ersten Zugriff auf die ankommenden (`PREROUTING`) und die lokal erzeugten (`OUTPUT`) Pakete. Neben den beiden Spezial-Targets `NOTRACK` und `TRACE` können Sie natürlich auch die eingebauten Targets `DROP` und `ACCEPT` verwenden. Außerdem verfügen die Ketten natürlich auch über Default-Policies, die Sie mit dem Befehl `iptables -t raw -P PREROUTING DROP` setzen können.

Jedoch ist die Tabelle in erster Linie dazu gedacht, dass Sie Ausnahmen von der Verbindungsüberwachung definieren können. Damit können Sie bestimmte Pakete, bei denen eine Verbindungsüberwachung sinnlos oder überflüssig ist, von dieser ausnehmen. Diese Funktion wird zum Beispiel von dem `ct_sync`-Cluster-Modul (siehe Abschnitt 26.6) genutzt, damit die Synchronisationsmeldungen des Firewall-Clusters nicht ebenfalls in der Zustandsüberwachung landen. Auch weitere Protokolle, die Sie unbedingt annehmen möchten und bei denen eine Zustandsüberwachung nicht sinnvoll ist (zum Beispiel IPsec-ESP), können Sie so ausklammern.

```
iptables -t raw -A PREROUTING -p 50 -j NOTRACK
iptables -A FORWARD -p 50 -j ACCEPT
```

Die Möglichkeit der Paketverfolgung ist mit dem `TRACE`-Target aus dem Patch-O-Matic gegeben. Damit können Sie zu Testzwecken genau den Weg eines Pakets durch Ihr Regelwerk und durch alle Tabellen und Ketten genau verfolgen. Dieses Target wurde aber bereits im Patch-O-Matic Kapitel besprochen (siehe Abschnitt 18.4.5).

