

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



# 21 Die Mangle-Tabelle

Die Mangle-Tabelle ist der Ort, wo Sie spezielle Paket-Modifikationen vornehmen können. Sie können hier die Type-of-Service-Bits ändern, Pakete markieren oder das ECN-Bit abschalten.

## 21.1 Die Ketten der Mangle-Tabelle

Je nach Ihrem Kernel weist die Mangle-Tabelle zwei oder fünf Ketten auf. Bis einschließlich 2.4.17 gab es nur die beiden Ketten PREROUTING und OUTPUT in der Mangle-Tabelle. Anschließend kamen auch noch die Ketten INPUT, FORWARD und POSTROUTING hinzu. Diese Ketten werden immer vor ihren entsprechenden Brüdern in den Tabellen NAT und Filter durchlaufen. Das bedeutet, dass Sie die Pakete modifizieren können, bevor die NAT-Regeln und die Filter-Regeln das Paket verarbeiten.

## 21.2 Aktionen der Mangle-Tabelle

Es gibt einige Aktionen (Targets), die nur in der Mangle-Tabelle erlaubt sind. Hierbei handelt es sich um: CLASSIFY, CONNMARK, DSCP, ECN, IPMARK, IPV4OPTSSTRIP, MARK, ROUTE, TOS, TTL und XOR. Dabei ist das Target CONNMARK ein Sonderfall, da es sowohl in der NAT- als auch in der Mangle-Tabelle mit unterschiedlichen Optionen genutzt werden kann.

Diese Targets möchte ich nun in diesem Kapitel vorstellen. Natürlich können Sie auch ACCEPT, DROP, REJECT etc. in der Mangle-Tabelle nutzen. Diese Targets habe ich aber bereits an anderer Stelle vorgestellt.

### 21.2.1 CLASSIFY

Linux unterstützt Class-based Queueing (CBQ). Mit diesem Ziel können Sie direkt ohne Firewall-Markierung ein Paket einer bestimmten Klasse zuweisen. Hierzu geben Sie mit der zusätzlichen Option `--set-class` die Major:Minor-Klasse an:

```
$IPTABLES -t mangle -A POSTROUTING -p tcp --dport 22 \  
-j CLASSIFY --set-class 1:10
```

Sie müssen mit dem Kommando `tc` natürlich auch eine entsprechende Klasse angelegt haben.

### 21.2.2 CONNMARK

Mit diesem Target können Sie eine Verbindung markieren. Dies ist nicht dasselbe wie die Markierung eines Pakets mit dem `MARK`-Target (siehe Abschnitt 21.2.7). Wenn Sie dennoch die Markierung auf das Paket übertragen möchten, können Sie das mit der Option `--restore-mark` des `CONNMARK`-Targets erreichen. Diese Option dürfen Sie nur in der Mangle-Tabelle verwenden.

```
iptables -t nat -A PREROUTING -p tcp --dport 80 -j CONNMARK --set-mark 80
iptables -t mangle -A FORWARD -m connmark --mark 80 -j CONNMARK --restore-mark
```

### 21.2.3 DSCP

Mit diesem Target können Sie die Diffserv-Class-Point-Bits im ToS-Header eines IP-Pakets setzen. Dieses DSCP-Feld wird in RFC 2474 beschrieben. Diese Werte werden häufig von Routern und Switches verwendet, um die Priorität von Paketen festzulegen.

Hierfür stehen Ihnen zwei Optionen zur Verfügung:

- `--set-dscp <wert>`. Hiermit können Sie das DSCP-Feld mit einem numerischen Wert füllen.
- `--set-dscp-class <klasse>`. Hiermit können Sie eine DiffServ-Klasse auswählen.

### 21.2.4 ECN

Die Explicit Congestion Notification ist eine neue Methode, die in dem RFC 3168 beschrieben wurde. Hiermit können zwei Kommunikationspartner, wenn beide ECN unterstützen, Verstopfungen der Verbindung vor deren Auftreten erkennen und durch eine Reduktion der Sendeleistung reagieren. So ist die Wahrscheinlichkeit sehr groß, dass die Verstopfung erst gar nicht auftritt.

Leider verwerfen viele alte und auch noch einige moderne Firewalls Pakete, die ECN verwenden, da die hier verwendeten Bits im IP- und TCP-Header bis zur Definition des RFC 3168 reserviert waren und lediglich von Werkzeugen wie Nmap verwendet wurden.

Wenn Sie dennoch ECN verwenden möchten, stellen Sie wahrscheinlich fest, dass die Kommunikation mit einigen Zielen nicht funktioniert. Dann können Sie für diese Ziele die ECN-Bits entfernen lassen:

```
iptables -t mangle -A PREROUTING -p tcp -d $ECN_BLACKHOLE -j ECN --ecn-tcp-remove
```

### 21.2.5 IPMARK

Dieses Target aus dem Patch-O-Matic erlaubt es, automatisch Pakete entsprechend ihrer IP-Adresse zu markieren. Dieses Target darf in der Mangle-Tabelle in den `PREROUTING`-, `FORWARD`- und `POSTROUTING`-Ketten angewendet werden. Da es bereits in Abschnitt 18.4.2 besprochen wurde, verweise ich an dieser Stelle darauf.

### 21.2.6 IPV4OPTSSTRIP

Mit diesem Target aus dem Patch-O-Matic können Sie sämtliche IP-Optionen eines Pakets entfernen. Es erlaubt Ihnen nicht, zwischen den verschiedenen IP-Optionen zu unterscheiden. Daher ist die Anwendung sehr einfach:

```
iptables -t mangle -A PREROUTING -j IPV4OPTSSTRIP
```

### 21.2.7 MARK

Hiermit können Sie eine Netfilter-Markierung des Pakets vornehmen. Diese Firewall-Markierung können Sie später mit dem Test `-m mark --mark` wieder prüfen oder auch in Zusammenhang mit dem `iproute2`-Paket nutzen. Um zum Beispiel für bestimmte Pakete eine andere Routing-Tabelle zu nutzen, können Sie die folgenden Befehle nutzen:

```
iptables -t mangle -A PREROUTING -p tcp --dport 25 -j MARK --set-mark 25
ip route add table 25 default via 192.168.0.5
ip rule add fwmark 25 table 25
```

Hiermit markieren Sie alle TCP-Pakete an den Port 25 mit der entsprechenden Markierung. Anschließend erzeugen Sie eine zusätzliche Routing-Tabelle mit der Nummer 25, in der Sie ein weiteres Default-Gateway eintragen. Damit diese Routing-Tabelle auch genutzt wird, definieren Sie eine Regel, die alle Pakete mit der Markierung 25 über diese Tabelle routet.

### 21.2.8 ROUTE

Mit dem `ROUTE`-Target aus dem Patch-O-Matic können Sie die beim `MARK`-Target beschriebene Problemstellung leichter lösen, da Sie ohne zusätzliche Routing-Tabelle und Regel direkt in der Firewall-Regel ein neues Gateway für die Pakete angeben können. Die Verwendung dieses Targets wird in Abschnitt [18.4.3](#) genauer beschrieben.

### 21.2.9 TOS

Hiermit können Sie die Type-of-Service-Bits im IP-Header modifizieren. Einige Betriebssysteme, wie Linux, werten diese Bits aus. Hierfür verwenden Sie `-j TOS --set-tos <wert>`. Die zur Verfügung stehenden Werte zeigt Ihnen der Befehl `iptables -j TOS -h` an:

```
TOS target v1.3.0 options:
  --set-tos value
```

```
Set Type of Service field to one of the
following numeric or descriptive values:
Minimize-Delay 16 (0x10)
Maximize-Throughput 8 (0x08)
Maximize-Reliability 4 (0x04)
```

```
Minimize-Cost 2 (0x02)  
Normal-Service 0 (0x00)
```

### 21.2.10 TTL

Dieses Target ermöglicht es Ihnen, den TTL-Wert eines IP-Pakets zu modifizieren. Das Netfilter-Team rät stark von der Verwendung dieses Targets ab. Bei falscher Anwendung erzeugen Sie hiermit Endlosschleifen!

Mit diesem Target können Sie auf Ihrer Firewall den TTL-Wert jedes Pakets, das die Firewall passiert, um eins erhöhen. Wenn Ihre Firewall selbst nicht auf den `traceroute`-Befehl reagiert, aber die `Time-Exceeded`-Mitteilungen durchlässt, ist die Firewall scheinbar für `Traceroute` unsichtbar, da für jeden TTL-Wert eine Antwort zurückkommt. Die Reduktion des TTL-Wertes durch die Firewall, die zum Ausfall dieser Antwort führen würde, wird von `Iptables` durch die Erhöhung wieder rückgängig gemacht.

Das Target hat drei Optionen:

- `--ttl-set <wert>`. Hiermit setzen Sie fest einen neuen Wert fest.
- `--ttl-dec <wert>`. Hiermit ziehen Sie den Wert von dem aktuellen TTL-Wert ab.
- `--ttl-inc <wert>`. Hiermit addieren Sie die angegebene Zahl zum aktuellen TTL-Wert hinzu.

### 21.2.11 XOR

Dieses Target aus dem `Patch-O-Matic` kann eine »Verschlüsselung« des Pakets mittels einer XOR-Verknüpfung durchführen. Da dieses Target bereits in Abschnitt [18.4.6](#) beschrieben wurde, gehe ich hier nicht näher darauf ein.