iptables/Netfilter CheatSheet

ALLGEMEIN

- **Netfilter** ist eine Softwareschicht innerhalb des Linux-Kernels, die **Netzwerkpakete** *abfangen* und *manipulieren* kann
- Netfilter werden meist als **Firewall** eingesetzt
- **iptables** ist das Programm zum Konfigurieren der Netfilter
- iptables benötigt erweiterte Systemprivilegien → **root**
- iptables bestehts aus **Tabellen**, **Ketten** und **Regeln**

REGELN; KETTEN; TABELLEN

- **Regeln** entscheiden, was mit dem Paket passieren soll
  ACCEPT, REJECT, LOG, DROP, REDIRECT; MASQUERADE
- **Ketten** sind Sammlungen von Regeln. Eine Kette kann mehrere Regeln haben
  5 Standardketten:
  PREROUTING: betrifft alle Pakete, bevor Routing-Entscheidung getroffen wird
  FORWARD: Pakete, die von einer zu einer anderen NIC geleitet werden (Routing)
  INPUT: Hereinkommende Pakete, die einen lokalen Prozess betreffen
  OUTPUT: Ausgehende Pakete, die von einem lokalen Prozess stammen
  POSTROUTING: alle Pakete kommen am Ende hier durch
  Regeln einer Kette werden nacheinander abgearbeitet
  INPUT, FORWARD und OUTPUT besitzen Standardregeln
- Die Verarbeitung der Netzwerkpakete ist in 3 Tabellen aufgeteilt:
  Mangle (Paketmanipulation; alle Ketten)
  Nat (Network Adress Translation (PRE-, POSTROUTING und OUTPUT)
  Filter (Paketfilter, FORWARD, INPUT; OUTPUT)

STANDARDBEFEHLE

Regeln löschen:
`iptables -F`
(alle Regeln)
`iptables -F INPUT`
(nur die Regeln in der Kette INPUT)

Regeln auflisten
`iptables -L`
(listet die Filter-Tabelle)
`iptables -L -line-numbers`
(Nummeriert die Einträge)
`Iptables -t [nat|mangle] -L`
(zeigt Einträge aus nat/mangle)
Weitere Parameter:
-verbose | -v (Details)
- numeric| -n (keine DNS-Resolves)
--zero [KETTE] | -z (Zähler zurücksetzen)

Standard verhalten
`iptables -P FORWARD ACCEPT`
(Standardeinstellungen werden angewandt, wenn keine Regel vorhanden ist: Bsp. Erlaubt das Routing komplett)

Regeln anhängen
`iptables -A INPUT -p icmp -j DROP`
(hängt eine Regel an, INPUT gibt die gewünschte Kette an, -p das Protokoll (icmp, tcp, udp,...) und mit –j wird die Aktion angegeben)

Regeln enfügen
`iptables -I INPUT 3 -p icmp -j DROP`
(entspricht Append, jedoch muss die Positioon noch angegeben werden)

Regeln ersetzen: -r
(wie insert, jedoch wird die Regel ersetzt)

Regeln ersetzen: -r
`iptables -D 3`
(löscht die Regeln Nr. 3)
`iptables -D INPUT -p icmp -s 192.168.0.0/24 -j ACCEPT`
(löscht die Regeln, die auf die gleiche Syntax passt.)

IPTABLES PARAMETER

`iptables -A INPUT -p icmp -src 192.16.0.0/24 -j ACCEPT`
(Neue Regel an die Kette INPUT. Da kein –t definiert wurde gilt filter. Die Regel lässt Ping-Pakete aus dem src-Netz zu)

`iptables -I INPUT 1 -p udp -dst 127.0.0.1 -j DROP`
(fügt neue Regel an erster Stelle ein)

`iptables -A INPUT -p icmp -i eth0 -j DROP`
(verbietet alle icmp-Pakete auf der Netzwerkschnittstelle eth0)

`iptables -A INPUT -p icmp -fragment -j LOG`
(vermerkt Fragmente, die das Protokoll ICMP benutzen)

`iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE`
(maskiert alle Pakete, die über eth1 gesendet werden (nur in nat möglich)

`iptables -t nat -A PREROUTING -I eth0 -p tcp -dport http -j REDIRECT -to-port 3128`
(Transaparenter Proxy: leitet alle Anfragen auf Port 80 auf Adapter eth0 an Port 3128)

`Iptables -A INPUT -s 255.0.0.0/8 -j LOG -log-prefix "Gefaelschte Quell-IP"`
`Iptables -A INPUT -S 255.0.0.0/8 -j DROP`
(Zuerst werden gefälschte IP-Adresse im Logging vermerkt, danach wird das gefälsche Paket verworfen)

`Iptables -A INPUT -p tcp ! -syn -m state -state NEW -j DROP`
(Alle TCP-Sessions müssen ordnungsgemäß mit SYN beginnen)

BEFEHLSLISTE:

(Teilweise aus man iptables)
Iptables is used to set up, maintain, and inspect the tables of IP packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also contain user-defined chains.

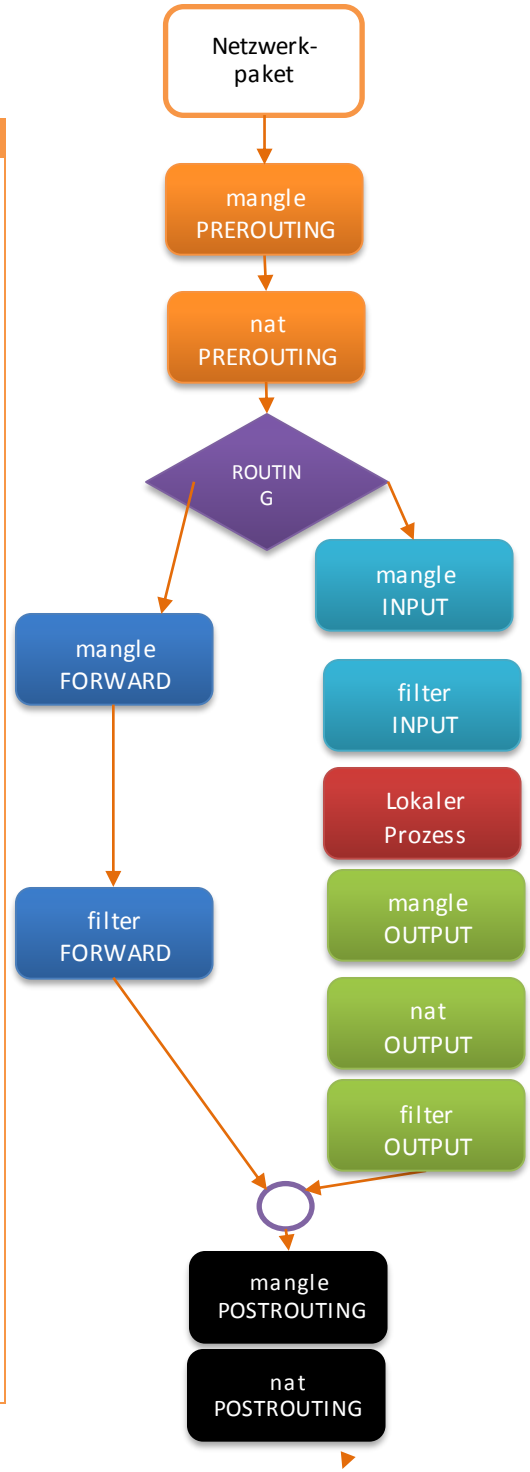
Befehl	Wirkung
-F/--flush	Regeln löschen
-L/--list	Anzeigen
-Z/--zero	Zähler auf 0
-P/--policy	Standardmethode einer Kette
-A/--append	Anhängen einer Regel
-I/--insert	Einfügen einer Regel
-R/--replace	Ersetzt eine Regel
-D/--delete	Löscht eine Regel
-N/--new-chain	Benutzerdef. Kette
-X/--delete-chain	Benutzerdef. Kette löschen

PARAMETER:

-t/--table	**Tabelle, auf die sich der Befehl bezieht: Std: filter**
-p/--protocol	Protokoll
-s/--src	Quelladresse des Pakets
-d/--dst	Zieladresse des Pakets
-i	Netzwerkschnittstelle, die das Paket empfängt
-o	Netzwerkschnittstelle, die das Paket sendet
-f	Zu große Pakete fragmentieren
-j	Legt fest, was mit Paket geschehen soll: DROP, ACCEPT,....

IPTables/Netfilter erlaubt jedoch noch viel mehr. Mit –match/-m gibt es noch umfangreiche Erweiterungen

ACCEPT=Erlauben; *REJECT*=Abweisen; *LOG*=Loggen; *DROP*=Verwerfen; *REDIRECT*=Ziel ändern; *MASQUERADE*=SRC ändern



This document was created by Christian Barthel <christian@barthel-connect.de>

Allgemeine iptables „match"-Kriterien

-t <-table->	Setzte eine Tabelle, Standard „filter"
-j <target>	Ziel <DROP|ACCEPT…>
-p	Protokoll <ICMP|UDP|TCP..>
-s <ip-adresse>	src-ipadresse (Quelle)
-d <ip-adresse>	Dst-ipadresse (Ziel)
-i <interface id>	Die Netzwerkschnittstelle eingehend
-o <interface id>	Netzwerkschnittstelle ausgehend

TCP/UDP match Kriterien

-p tcp –sport <port>	TCP-Quellport (src-port)
-p tcp –dport	TCP-Ziel-Port (destination-port)
-p tcp –syn	Identifiziert eine neue TCP-Verbindung ! –syn = keine neue Verbindung
-p udp –sport	UDP-Quellport
-p udp –dport	UDP Zielport

icmp match Kriterien

--icmp-type <type>	ICMP-Type, z. b. echo-reply oder echo-request

```
iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -A INPUT  -p icmp --icmp-type echo-reply   -j ACCEPT
```

Erlaubt eingehende/ausgehende pings

Weit verbreitete Match Kriterien

-m multiport –sports <port, port>	Reihe von TCP/UDP Ports
-m multiport –dports <port, port>	Siehe oben; nur für destination
-m multiport –ports <port, port>	Auflistung von Ports, getrennt durch Komma
-m –state <state>	ESTABLISHED: Packet ist Teil einer Verbindung in beide Richtungen NEW: Packet ist Teil einer neuen Verbindung RELATED: Packet startet eine neue 2. Verbindung, z. B. FTP-Datentransfer INVALID: Packet konnte nicht identifiziert werden.

Einfaches Blocken unerwünschter IP-Adressen

Manchmal gibt es IP-Adressen, die hartnäckig Ihre Angriffe auf Ihren Server ausführen. Diese können anhand der IP-Adresse sehr schön geblockt werden:

```
iptables -I INPUT -s 212.31.431.4 -j DROP
```

Logfile für iptables

Standardmäßig loggt iptables nach /var/log/messages. Um eine andere Log-Datei anzugeben sind folgende Schritte notwendig:

1. Editieren von /etc/syslog.conf
2. Folgende Zeile anhängen:

```
kern.warning /var/log/iptables.log
```

3. Den log-level korrekt setzen:

```
# DROP everything and Log it
iptables -A INPUT -j LOG --log-level 4
iptables -A INPUT -j DROP
```

4. Beispiel:

```
iptables -A INPUT -s 64.55.11.2 -m limit --limit 5/m --limit-burst 7 -j LOG --log-prefix '** HACKERS **'--log-level 4
iptables -A INPUT -s 64.55.11.2 -j DROP
```

5. Log kontrollieren: /var/log/iptables.log

SSH Brute Force Attacken abwehren

Häufig werden öffentliche SSH-Zugänge per BruteForce attackiert. Dies kann mit iptables sehr schön verhindert werden.

```
iptables -I INPUT -i eth1 -p tcp -m tcp --dport 22 -m state --state NEW -m recent --set --name DEFAULT -rsource
iptables -I INPUT -i eth1 -p tcp -m tcp --dport 22 -m state --state NEW -m recent --update --seconds 180 --hitcount 4 --name DEFAULT --rsource -j DROP
```

Dies verhindert, dass ein Angreifer mehr als 3 SSH-Verbindungen innerhalb 3 Minuten aufbaut.

This document was created by Christian Barthel <christian@barthel-connect.de>