iptables beobachten

```
watch -d iptables -nvL --line-numbers
```

- -L = List (auflisten)
- -n = no DNS-lookup
- -v = verbose (gesprächig)
- –line-numbers = Regeln Nummerieren (einzelne Regeln können anhand der Nummer z.B. gelöscht werden)

iptables Regeln zurücksetzen

filter

```
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -F
iptables -X
```

nat

```
iptables -t nat -F
iptables -t nat -X
```

iptables Syntax

table	command	chain	rule-specification			target	
-t filter	-A	INPUT	-s			-j	ACCEPT
	-C	OUTPUT	-d				DROP
	-D	FORWARD	-i				REJECT
	-I		-o				LOG
	-R						

table	command	chain	rule-specification			target	
-t nat	-L	PREROUTING	-p	udp	--dport	-j	SNAT
	-S	OUTPUT			--sport		DNAT
	-F	POSTROUTING		tcp	--dport		MASQUERADE
	-Z				--sport		
-t mangle	-N	PREROUTING		icmp	--icmp-type		
	-X	OUTPUT					
	-P	INPUT	-m	conntrack	--ctstate		
	-E	POSTROUTING					

[1)]

Einbindung von iptables in den Bootvorgang

CentOS (bis 6)

Paket: iptables-services

```
/etc/init.d/iptables save
```

speichert die aktuell aktiven iptables-Regeln in der Datei `/etc/sysconfig/iptables`. Beim Booten werden sie hier wieder ausgelesen.

CentOS (ab 7)

wie SuSE, oder `firewalld` nutzen

SuSE

SuSE setzt auf eine eigene, iptables-basierte Firewall. Wer volle Kontrolle über die verwendeten iptables-Regeln haben möchte, deaktiviert sie besser:

```
chkconfig SuSEfirewall2_init off
chkconfig SuSEfirewall2_setup off
```

Ein einfaches Beispiel für ein Startskript könnte so aussehen: [2)]

`/etc/init.d/iptables`:

```
#!/bin/bash
case $1 in
  start)
```

```
    iptables-restore /etc/sysconfig/iptables
  ;;
  stop)
    iptables -P INPUT ACCEPT
    iptables -P OUTPUT ACCEPT
    iptables -P FORWARD ACCEPT
    iptables -F
    iptables -X
  ;;
  restart)
    $0 stop
    $0 start
  ;;
  save)
  iptables-save > /etc/sysconfig/iptables
  ;;
  *)
    echo Hä?
  ;;
esac
```

Debian

Bei Debian gibt es mehrere [3] Möglichkeiten, iptables zu starten.

Ein einfaches Beispiel für ein Startskript könnte so aussehen:

`/etc/init.d/iptables`:

```
#!/bin/bash
case $1 in
  start)
    iptables-restore /etc/defaults/iptables
  ;;
  stop)
    iptables -P INPUT ACCEPT
    iptables -P OUTPUT ACCEPT
    iptables -P FORWARD ACCEPT
    iptables -F
    iptables -X
  ;;
  restart)
    $0 stop
    $0 start
  ;;
  save)
    iptables-save > /etc/defaults/iptables
  ;;
  *)
```

```
    echo usage: $0 [start] [stop] [restart] [save]
  ;;
esac
```

Und so wird es aktiviert:

```
update-rc.d iptables start 40 S . stop 89 0 6 .
```

Alternativ: `/etc/network/interfaces` :

```
auto eth0
iface eth0 inet dhcp
  up sh -c 'iptables-restore < /etc/iptables'
```

Einfacher Paketfilter mit NAT

`/etc/sysctl.conf`:

```
net.ipv4.ip_forward=1
net.ipv4.conf.default.rp_filter=1
net.ipv4.conf.all.rp_filter=1
```

Script:

```
#!/bin/bash

ext_dev="eth0"
ext_ip="212.202.240.174"
int_dev="eth1"
int_ip="192.168.1.1"
dmz_dev="eth2"

http_proxy=10.0.0.4
smpt_proxy=10.0.0.5
webserver=10.0.0.6

modprobe ip_nat_ftp
modprobe ip_conntrack_ftp

iptables -N proxy
iptables -N dmz
iptables -N icmp

iptables -P FORWARD DROP
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i $int_dev -m state --state NEW -j proxy
```

```
iptables -A FORWARD -i $ext_dev -m state --state NEW -j dmz
iptables -A FORWARD -p icmp -j icmp
iptables -A FORWARD -m limit -j LOG --log-prefix "FORWARD DROP"

iptables -A proxy -p tcp --dport 3128 -d $http_proxy -j ACCEPT
iptables -A proxy -p tcp --dport 25 -d $smtp_proxy -j ACCEPT
iptables -A proxy -m limit -j LOG --log-prefix "proxy DROP"
iptables -A proxy -j REJECT

iptables -A dmz -p tcp --dport 80 -d $webserver -j ACCEPT
iptables -A dmz -m limit -j LOG --log-prefix "dmz DROP"
iptables -A dmz -j REJECT

iptables -A icmp -p icmp --type echo-reply -j ACCEPT
iptables -A icmp -p icmp --type echo-request -j ACCEPT

iptables -t nat -A POSTROUTING -o $ext_dev -j MASQUERADE
iptables -t nat -A PREROUTING -i $ext_dev -p tcp --dport 80 -d $ext_ip -j
DNAT --to-destination $webserver
```

Doku

iptables Kurzanleitung:

```
iptables -h
```

Hilfe zu einem bestimmten Protokoll / Teilbereich:

```
iptables -p icmp -h
```

Links

- http://www.netfilter.org
- http://www.netfilter.org/documentation/HOWTO/netfilter-extensions-HOWTO.html
- http://www.frozentux.net/iptables-tutorial/iptables-tutorial.html
- https://gist.github.com/mcastelino/c38e71eb0809d1427a6650d843c42ac2

iptables und ssh

- http://www.debian-administration.org/articles/187 , aber: http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=332231

1)

inspiriert von:
2)

Das Beispiel ist so nicht LSB konform, eine Vorlage wie man es besser machen könnte findet sich unter `/etc/init.d/skel*`
[3)]

siehe /usr/share/doc/iptables/README.Debian.gz