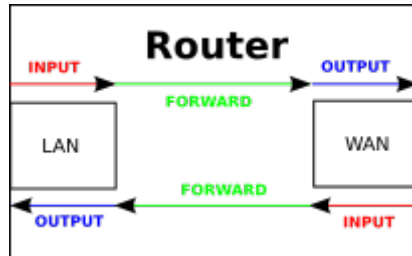


IPTables



IPv4

```
#alle vorherigen Regeln löschen
```

```
{ipt} -F
{ipt} -X
{ipt} -t nat -F
{ipt} -t nat -X
{ipt} -t mangle -F
{ipt} -t mangle -X
```

```
# standard-Regel für IPv4: alles dropen
```

```
{ipt} -P INPUT DROP
{ipt} -P OUTPUT DROP
{ipt} -P FORWARD DROP
```

```
# policy für TCP-Reset/UDP-Reject als Alternative für "-j DROP"
```

```
{ipt} -N ABGELEHNT
if [[ ! "${LOG}" = "" ]];
then
    echo "enable IPv4-Firewall-Logging (all)...";
    {ipt} -A ABGELEHNT -m limit --limit 10/min -j LOG --log-prefix
"NETFILTER4-ABGELEHNT: " --log-level 4
fi
{ipt} -A ABGELEHNT -p tcp -j REJECT --reject-with tcp-reset
{ipt} -A ABGELEHNT -p udp -j REJECT --reject-with icmp-port-unreachable
{ipt} -A ABGELEHNT -j DROP
```

```
# localhost
```

```
{ipt} -A INPUT -i lo -j ACCEPT
{ipt} -A OUTPUT -o lo -j ACCEPT
```

```
{ipt} -A OUTPUT -j ACCEPT
{ipt} -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT #
angeforderte, bestehende Verbindungen eingehend
{ipt} -A INPUT -p icmp -m limit --limit 5/s --icmp-type echo-request -j
```

ACCEPT # ICMP eingehen, max 5/s

```
#Block Teredo-Stuff
#{ipt} -I FORWARD -p udp --dport 3544 -j ABGELEHNT
#{ipt} -I FORWARD -p udp --sport 3544 -j ABGELEHNT
#http://en.wikipedia.org/wiki/List_of_IP_protocol_numbers
#{ipt} -A FORWARD -p 41 -j ABGELEHNT #IPv6 Encapsulation
#{ipt} -A FORWARD -p 43 -j ABGELEHNT #Routing Header for IPv6
#{ipt} -A FORWARD -p 44 -j ABGELEHNT #Fragment Header for IPv6
#{ipt} -A FORWARD -p 58 -j ABGELEHNT #ICMP for IPv6
#{ipt} -A FORWARD -p 59 -j ABGELEHNT #No Next Header for IPv6
#{ipt} -A FORWARD -p 60 -j ABGELEHNT #Destination Options for IPv6
```

```
#ssh mit rate-limit
#{ipt} -I INPUT -p tcp --dport 22 -i ${if_ext} -m state --state NEW -m recent --set
#{ipt} -I INPUT -p tcp --dport 22 -i ${if_ext} -m state --state NEW -m recent --update --seconds 60 --hitcount 4 -j ABGELEHNT #4 verbindungen in 1 Minute
#{ipt} -A INPUT -p tcp --dport 22 -j ACCEPT #SSH eingehend
```

```
#{ipt} -A FORWARD -i ${if_int} -o ${if_ext} -j ACCEPT #Forwarding Int->Ext
#{ipt} -A FORWARD -i ${if_ext} -o ${if_int} -m state --state ESTABLISHED,RELATED -j ACCEPT #Forwarding Ext->Int (nur bestehende/angeforderte Verbindg.)

#{ipt} -A INPUT -i ${if_int} -j ACCEPT #erlaubt alle Anfragen von Intern
```

port-forwardings

```
# REJECT/RESET fuer alles andere
#{ipt} -A INPUT -j ABGELEHNT
#{ipt} -A OUTPUT -j ABGELEHNT
#{ipt} -A FORWARD -j ABGELEHNT
```

zusätzliche Optionen:

```
#Kernel-Option fuer SYN-Cookies
echo 1 > /proc/sys/net/ipv4/tcp_syncookies #enable syn cookies (prevent against 'syn flood attack')

if [ -f /proc/sys/net/ipv4/conf/all/accept_redirects ]; then
    echo "    Kernel ignores all ICMP redirects"
    echo 0 > /proc/sys/net/ipv4/conf/all/accept_redirects
fi

if [ -f /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts ]; then
    echo "    Kernel ignores ICMP Echo requests sent to broadcast/multicast addresses"
    echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
```

```
fi
```

Port-Forwardings

einrichten

port 522 auf Client 192.168.0.5 port 22 weiterleiten

```
${ipt} -t nat -A PREROUTING -p tcp --dport 522 -j DNAT --to-destination 192.168.0.5:22
```

anzeigen

```
iptables -L -t nat
```

```
Chain PREROUTING (policy ACCEPT)
```

```
target      prot opt source
```

```
DNAT        tcp  --  anywhere
```

```
to:192.168.0.5:22
```

```
destination
```

```
anywhere
```

```
tcp dpt:522
```

active-FTP

damit Clients FTP im ACTIVE-Modus nutzen können müssen 2 Module geladen und eine 1 iptables-Regel angewandt werden

```
modprobe ip_conntrack_ftp
modprobe ip_nat_ftp ports=21
```

```
${ipt} -A INPUT -p tcp --sport 20 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

IPv6

From:

<https://wiki.fw-web.de/> - **FW-WEB Wiki**

Permanent link:

<https://wiki.fw-web.de/doku.php?id=bpi-r2:network:iptables>

Last update: **2023/06/08 17:06**

