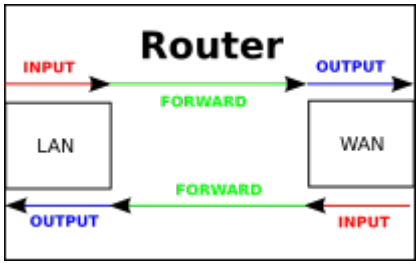
IPTables

🔧 Fix Me!



IPv4

```
#delete previous rules
${ipt} -F
${ipt} -X
${ipt} -t nat -F
${ipt} -t nat -X
${ipt} -t mangle -F
${ipt} -t mangle -X

# Default-Rule for IPv4: drop all
${ipt} -P INPUT   DROP
${ipt} -P OUTPUT  DROP
${ipt} -P FORWARD DROP
```

```
# policy for TCP-Reset/UDP-Reject as alternative to "-j DROP"
${ipt} -N REJECTED
if [[ ! "${LOG}" = "" ]];
then
  echo "enable IPv4-Firewall-Logging (all)...";
  ${ipt} -A REJECTED -m limit --limit 10/min -j LOG --log-prefix
"NETFILTER4-REJECTED: " --log-level 4
fi
${ipt} -A REJECTED -p tcp -j REJECT --reject-with tcp-reset
${ipt} -A REJECTED -p udp -j REJECT --reject-with icmp-port-unreachable
${ipt} -A REJECTED -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 # incoming
connetions which are requested
${ipt} -A INPUT  -p icmp -m limit --limit 5/s --icmp-type echo-request -j
```

```
ACCEPT # ICMP incoming, max 5/s
```

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

```
#ssh with rate-limit (replacing hosts.allow)
${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 REJECTED #4 connections in 1
minute
${ipt} -A INPUT  -p tcp --dport  22 -j ACCEPT #SSH incoming
```

```
${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 (only existing/requested
connections)

${ipt} -A INPUT -i ${if_int} -j ACCEPT #accept all request from internal
```

... (some other rules, e.g. port-forwardings)

```
# REJECT/RESET for everything else
${ipt} -A INPUT   -j REJECTED
${ipt} -A OUTPUT  -j REJECTED
${ipt} -A FORWARD -j REJECTED
```

additional options:

```
#Kernel-option for 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

setup

forward port 522 to Client 192.168.0.5 port 22

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

show

```
iptables -L -t nat

Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
DNAT       tcp  --  anywhere             anywhere             tcp dpt:522
to:192.168.0.5:22
```

active-ftp

to allow active-ftp from a client you need to load 2 modules and set 1 iptables-rule

```
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