```
#!/bin/bash
# Verbessertes Skript für einen Einzelrechner
# fuer Sie von J. Meese
#
echo ---------------Firewall wird eingerichtet---------------
#
# Definition wichtiger Umgebungsvariablen
INT_IFACE=eth0          # interne Schnittstelle zum LAN
EXT_IFACE=eth1          # externe Schnittstelle ins Internet
LOOP_IFACE=lo           # Loopback
OWN_IP=192.168.1.1      # unsere IP-Adresse
MYNET=192.168.1.0/24    # unsere Netzadresse
ANYWHERE=any/0          # jede Adresse im Netz
UNPRIVPORTS=1024:65535  # unprivilegierte Ports
INT_TCP_ALLOWED="22 80 443"   # Zugriff auf eigene TCP-Ports
EXT_TCP_ALLOWED="21 22 25 53 80 110 443"  # Zugriff auf fremde TCP-Ports
INT_UDP_ALLOWED="53"    # Zugriff auf eigene UDP-Ports
EXT_UDP_ALLOWED="53"    # Zugriff auf fremde UDP-Ports
NAMESERVER=192.168.32.1 # aus /etc/resolv.conf
#
# Default Policies und Loeschen der Regeln
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP
#
iptables -F
iptables -X
iptables -Z
#
################################################################################
#
# Protokollieren abgelehnter Pakete durch syslog
# Erzeugen einer eigenen Regelkette mit -N:
iptables -N log_drop
iptables -A log_drop -p icmp -j LOG --log-prefix "Abgewiesenes ICMP-Paket: "
iptables -A log_drop -p udp -j LOG --log-prefix "Abgewiesenes ICMP-Paket: "
iptables -A log_drop -p tcp -j LOG --log-prefix "Abgewiesenes ICMP-Paket: "
iptables -A log_drop -j DROP
#
################################################################################
#
WHITELIST=/usr/local/etc/whitelist
BLACKLIST=/usr/local/etc/blacklist
#
# Akzeptieren des Vollzugriffs aller Rechner und Netze in WHITELIST
if [ -r $WHITELIST ]; then
for x in `grep -v ^# $WHITELIST | awk '{print $1}'`; do
      echo Genehmigen von $x
      iptables -A INPUT -s $x -j ACCEPT
done
fi
#
# vollständiges Blocken der BLACKLIST-Rechner und -Netze
if [ -r $BLACKLIST ]; then
for x in `grep -v ^# $BLACKLIST | awk '{print $1}'`; do
      echo Blockieren von $x
      iptables -A INPUT -s $x -j DROP
done
fi
#
################################################################################
#
# Erlauben der Kommunikation lokaler Prozesse ueber loopback
```

```
iptables -A INPUT -i $LOOP_IFACE -d 127.0.0.1 -p ALL -j ACCEPT
iptables -A OUTPUT -o $LOOP_IFACE -d 127.0.0.1 -p ALL -j ACCEPT
#
# ausgehendes ping erlauben und eingehendes ping verbieten
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
iptables -A INPUT -p icmp --icmp-type echo-request -j log_drop
#
################################################################################
#
# Zugriff auf eigene TCP-Dienste fuer LAN freigeben (INT_TCP_ALLOWED)
echo TCP Eingang:
for port in $INT_TCP_ALLOWED; do
      echo Zugriff auf eigenen TCP-Port $port erlauben
      iptables -A INPUT -i $INT_IFACE -d $OWN_IP \
             -p tcp --dport $port -j ACCEPT
      iptables -A OUTPUT -o $INT_IFACE -s $OWN_IP \
             -p tcp --sport $port -j ACCEPT
done
#
################################################################################
#
# Zugriff auf fremde TCP-Dienste (EXT_TCP_ALLOWED)
# Hinweis: Mailserver kann man zusaetzlich mit -d $MAILSERVER absichern
echo TCP Ausgang:
for port in $EXT_TCP_ALLOWED; do
      echo Zugriff auf fremden TCP-Port $port erlauben
      iptables -A OUTPUT -p tcp --sport $UNPRIVPORTS \
             --dport $port -j ACCEPT
      iptables -A INPUT -p tcp --dport $UNPRIVPORTS \
             --sport $port ! --syn -j ACCEPT
      iptables -A INPUT -p tcp --sport $port \
             --syn -j log_drop
done
#
################################################################################
#
# passive Datenverbindung auf fremden FTP-Server erlauben
      iptables -A OUTPUT -p tcp --sport $UNPRIVPORTS \
             --dport $UNPRIVPORTS -j ACCEPT
      iptables -A INPUT -p tcp --sport $UNPRIVPORTS \
             --dport $UNPRIVPORTS ! --syn -j ACCEPT
#
################################################################################
#
# Alle anderen Verbindungswünsche wegfiltern gegen SYN_Flooding
iptables -A INPUT -p tcp --syn -j DROP
#
################################################################################
#
# Zugriff auf eigene UDP-Dienste fuer LAN freigeben (INT_UDP_ALLOWED)
echo UDP Eingang:
for port in $INT_UDP_ALLOWED; do
      echo Zugriff auf eigenen UDP-Port $port erlauben
      iptables -A INPUT -i $INT_IFACE -d $OWN_IP \
             -p udp --dport $port -j ACCEPT
      iptables -A OUTPUT -o $INT_IFACE -s $OWN_IP \
             -p udp --sport $port -j ACCEPT
done
#
################################################################################
#
# Zugriff auf fremde UDP-Dienste (EXT_UDP_ALLOWED)
```

```
echo UDP Ausgang:
for port in $EXT_UDP_ALLOWED; do
      echo Zugriff auf fremden UDP-Port $port erlauben
      iptables -A OUTPUT -p udp --sport $UNPRIVPORTS \
             --dport $port -j ACCEPT
      iptables -A INPUT -p udp --dport $UNPRIVPORTS \
             --sport $port -j ACCEPT
      iptables -A INPUT -p udp --sport $port \
             -j log_drop
done
#
# Alle anderen Verbindungswünsche wegfiltern gegen SYN_Flooding
iptables -A INPUT -p tcp --syn -j DROP
#
################################################################################
#
# Zeitsynchronisation mit NTP über gleichen s- und dport
iptables -A OUTPUT -p udp --sport 123 --dport 123 -j ACCEPT
iptables -A INPUT -p udp --dport 123 --sport 123 -j ACCEPT
#
################################################################################
#
# die restlichen Pakete werden gesperrt bzw. geloggt
iptables -A INPUT -j log_drop
iptables -A FORWARD -j log_drop
#
# ausgehende eigene Pakete werden mit Fehlermeldung abgewiesen,
# somit wartet unser Client nicht auf Antwort
iptables -A OUTPUT -j REJECT
#
################################################################################
#
#
echo ----------------------Firewall steht----------------------
#
exit 0
```