firewalling mit iptables

Eine erste Einführung

Seinen Rechner oder sogar ganze Netzwerke vor ungewollten Eindringlingen zu schützen, gehört in den heutigen Zeiten leider zu einer der wichtigsten Aufgaben von Administratoren.

Angriffsmethoden

- Denial-of-Service
- Spoofing
- Hijacking
- Bufferoverflow
- Formatstring
- Race-Condition
- SQL-Injection

Möglichenkeiten einer Firewall

Begrenzung der zugriffberechtigten Rechner
Blockade von ungewollten Diensten
Erkennen von Angriffen
Gezielte Abschaltung von Netzen und/oder Routen

Komponenten

netfilter
- Kernelnahe Struktur zur Einbindung von Filterfunktionen

iptables
- Definition und Verwalten von Tabellen, Regeln und Ketten

Drei Tabellen

filter
- Pakete filtern
- Default Tabelle

mangle
- Änderungen im IP-Header von Paketen

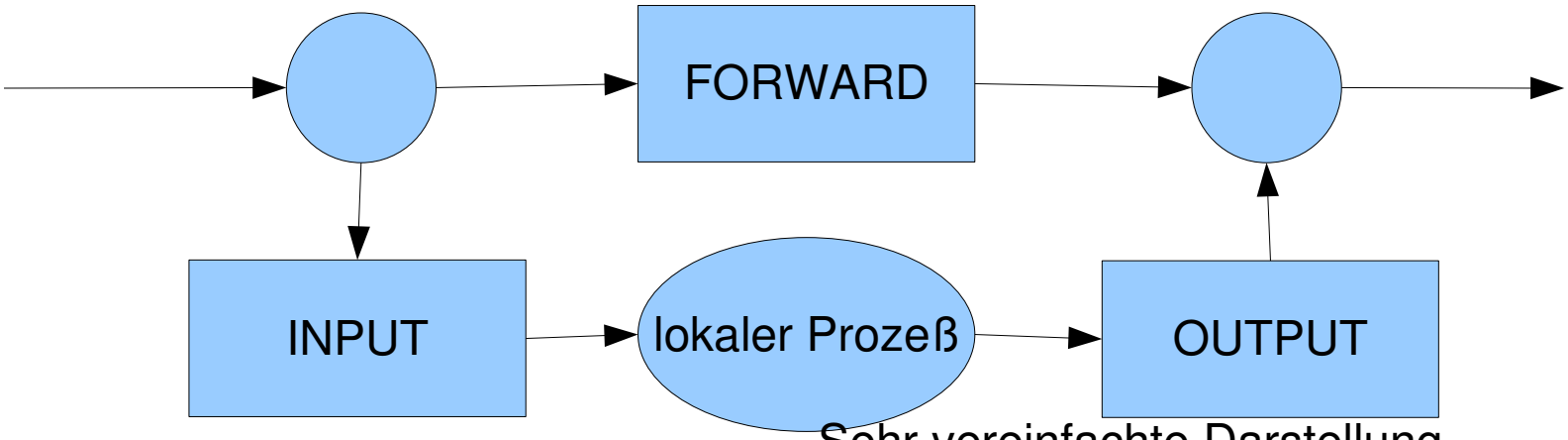
nat
- IP-Masquarading

Wir werden uns vornehmlich mit der **filter**-Tabelle beschäftigen.

Die drei Ketten der filter-Tabelle

INPUT
OUTPUT
FORWARD

Jedes Netzwerkpaket, das den Rechner von außen erreicht durchläuft die **INPUT**-Kette.
Jedes Netzwerkpaket, das der Rechner lokal erzeugt, durchläuft die **OUTPUT**-Kette.
Die **FORWARD**-Kette dient zum Weiterleiten/Routen von Netzwerkpaketen.



Sehr vereinfachte Darstellung

Eigene Ketten können zur besseren Strukturierung der FW-Regeln erzeugt werden.

Regeln

Jede Kette kann eine Liste von Regeln enthalten.
Jedes Netzwerkpaket durchläuft die Regeln der entsprechenden Kette. Trifft die Beschreibung einer Regel auf das Paket zu, wird die in der Regel beschriebene Aktion ausgeführt.
Trifft keine Beschreibung zu, greift schlußendliche die Default Policy.

iptables selber ist ***keine*** Firewall.
Erst die richtigen Regeln machen aus den gebotenen Strukturen ein wirkungsvolles Instrument zum Schutz des Rechners.

Starten/Stoppen von iptables

Stoppen

```
[root@home ~]# service iptables stop
```

Starten

```
[root@home ~]# service iptables start
```

Module

```
modprobe ip_tables              # wird wahrscheinlich aut. geladen
modprobe iptable_filter         # wird wahrscheinlich aut. geladen
modprobe nf_conntrack           # wird wahrscheinlich aut. geladen
modprobe nf_conntrack_ftp
modprobe ipt_state
modprobe ipt_LOG
#modprobe iptable_mangle        # wird hier nicht benoetigt
#modprobe iptable_nat           # wird hier nicht benoetigt
#modprobe ip_nat_ftp            # wird hier nicht benoetigt
#modprobe ipt_MASQUERADE        # wird hier nicht benoetigt
```

```
lsmod | sort | grep ip
lsmod | sort | grep nf
```

Ein paar erste Befehle

Auflisten der bisherigen Regeln

```
[root@home ~]# iptables -nL
```

Hinzufügen von Regeln

```
[root@home ~]# iptables -A INPUT -p icmp -j DROP
```

Befehle

Befehl		Beschreibung
-A	--append	Anhängen einer Regel
-I	--insert	Eine Regel einfügen
-F	--flush	Löschen aller Regeln
-L	--list	Auflisten aller Regel
-Z	--zero	Zurücksetzen von Zählern
-P	--policy	Setzen der Default Policy
-R	--replace	Ersetzen einer Regel
-D	--delete	Löschen einer Regel
-N	--new-chain	Anlegen einer benutzerdefinierten Kette
-X	--delete-chain	Löschen einer benutzerdefinierten Kette

Parameter

Parameter		Beschreibung
-t	--table	Tabele, auf die sich der Befehl bezieht
-p	--protocol	Protokol, auf das die Regel achten soll
-s	--source	Quelladresse
-d	--destination	Zieladresse
-i	--in-interface	Eingangs-Schnittstelle
-o	--out-interface	Ausgangs-Schnittstelle
-f	--fragment	Betrachten von fragmentierten Teilpaketen
- j	--jump	Ziel der Regel

Ziele

Ziel	Bedeutung
DROP	Das Paket wird ohne Antwort verworfen
ACCEPT	Das Paket darf passieren
LOG	Eintrag im syslog
REJECT	Das Paket wird mit Fehlerantwort verworfen
REDIRECT	Die Zieladresse wird umgesetzt
MAQUERADE	Die Quelladresse wird auf die Adresse der Schnittstelle umgesetzt

Bei Regeln ohne Ziele werden die betroffenen Pakete nur gezählt.

Erweiterungen

Erweiterung	Beschreibung
TCP	
--sport	Port an der Quelle
--dport	Port am Ziel
--tcp-flags	TCP-Flags suchen
--syn	spezielle TCP-Flags (SYN,REST, ACK SYN)
--tcp-option	??
UDP	
--sport	Port an der Quelle
--dport	Port am Ziel
ICMP	
--icmp-type	
-m limit --limit	Limit pro Zeiteinheit
-m mac --mac-source	MAC-Adresse
-m state --state	Paketstatus (NEW, ESTABLISHED, RELATED, INVALID)
-m time --timestart	
-m time --timestop	Zeitliche Begrenzung von Regeln
--log-prefix	Für Ziel LOG: Kennzeichen festlegen
--log-level	Logelevel festlegen

Aufbau einer Firewall

```
iptables -A $CHAIN \
 -i $IFACE \
 -d $LOCIP \
 -p $PROT \
 -dport $PORT \
 -j $GOAL
```

Für stationäre Rechner (z.B. Desktops) ist das Interface wie auch die lokale IP-Adresse in Normalfall statisch. Zunehmend kommen aber mobile Rechner mit mehreren abwechselnden Schnittstellen zum Einsatz. Bei denen kann weder das Interface noch die eigene IP-Adresse für eine FW-Definition berücksichtigt werden.

Definieren von Regeln

Fangen wir mal ganz einfach an: Erstmal löschen wir alles was bisher definiert wurde und richten die Default Policies restriktiv ein.

```
iptables -t filter -P INPUT DROP
iptables -t filter -P FORWARD DROP
iptables -t filter -P OUTPUT DROP

iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT
iptables -t nat -P OUTPUT ACCEPT
iptables -t mangle -P PREROUTING ACCEPT
iptables -t mangle -P INPUT ACCEPT
iptables -t mangle -P FORWARD ACCEPT
iptables -t mangle -P OUTPUT ACCEPT
iptables -t mangle -P POSTROUTING ACCEPT

iptables -t filter -F
iptables -t nat -F
iptables -t mangle -F
```

Jetzt geht erstmal zu gut wie nix mehr!

Drucker/Loopback

```
iptables -A INPUT -i lo -s 127.0.0.1 -d 127.0.0.1 -j ACCEPT
iptables -A OUTPUT -o lo -s 127.0.0.1 -d 127.0.0.1 -j ACCEPT

iptables -A INPUT -sdort 9100 -p UDP -j ACCEPT
iptables -A OUTPUT -dport 9100 -p UDP -j ACCEPT

#iptables -A OUTPUT -d 192.168.1.99 -dport 9100 -p UDP -j ACCEPT
```

Logging

```
iptables -A INPUT -m state --state INVALID \
    -j LOG --log-prefix "FW-INCM: => " --log-level 5

iptables -A INPUT -m state --state INVALID -j DROP
```

Ablehnen privater Adressbereiche

```
#iptables -A INPUT -s 192.168.0.0/16 -j DROP

iptables -A INPUT -s 172.16.0.0/12 -j DROP
iptables -A INPUT -s 10.0.0.0/8 -j DROP

iptables -A INPUT -s 127.0.0.0/8 -j DROP
```

Ping Pong und Konsorten

Typ	Nachricht	Ausgehend	Eingehend
8	Echo Request (Ping)	Zulassen	Blockieren
0	Echo Reply (Pong)	Blockieren	Zulassen
3	Destination Unreachable	Blockieren	Zulassen
4	Source Quench	Blockieren	Zulassen
5	Redirect	Blockieren	Blockieren
11	Time Exceeded	Blockieren	Zulassen
12	Parameter Problem	Blockieren	Zulassen
30	Traceroute	Zulassen	Zulassen

Ping Pong und Konsorten

```
iptables -A INPUT -p ICMP --icmp-type 8 -j DROP
iptables -A INPUT -p ICMP --icmp-type 0 -j ACCEPT
iptables -A INPUT -p ICMP --icmp-type 3 -j ACCEPT
iptables -A INPUT -p ICMP --icmp-type 4 -j ACCEPT
iptables -A INPUT -p ICMP --icmp-type 5 -j DROP
iptables -A INPUT -p ICMP --icmp-type 11 -j ACCEPT
iptables -A INPUT -p ICMP --icmp-type 12 -j ACCEPT
iptables -A INPUT -p ICMP --icmp-type 30 -j ACCEPT

iptables -A OUTPUT -p ICMP --icmp-type 8 -j ACCEPT
iptables -A OUTPUT -p ICMP --icmp-type 0 -j DROP
iptables -A OUTPUT -p ICMP --icmp-type 3 -j DROP
iptables -A OUTPUT -p ICMP --icmp-type 4 -j DROP
iptables -A OUTPUT -p ICMP --icmp-type 5 -j DROP
iptables -A OUTPUT -p ICMP --icmp-type 11 -j DROP
iptables -A OUTPUT -p ICMP --icmp-type 12 -j DROP
iptables -A OUTPUT -p ICMP --icmp-type 30 -j ACCEPT

iptables -A OUTPUT -p UDP -dport 33435:33524 -j ACCEPT
```

Namensauflösung

```
iptables -A INPUT -p UDP -sport 53 \
    -m stat --state ESTABLISHED -j ACCEPT

iptables -A OUTPUT -p UDP -dport 53 \
    -m state --state NEW -j ACCEPT
```

Browser

```
iptables -A INPUT -p TCP -sport 80 \
   -m state --state ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p TCP -dport 80 \
   -m state --state NEW -j ACCEPT

iptables -A INPUT -p TCP -sport 443 \
   -m state --state ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p TCP -dport 443 \
   -m state --state NEW -j ACCEPT

iptables -A INPUT -p TCP -d $PROXY -sport 8081 -j ACCEPT
iptables -A OUTPUT -p TCP -s $PROXY -dport 8081 -j ACCEPT
```

Filetransfer

```
# passives FTP zulassen
iptables -A INPUT -p TCP -sport 21 \
   -m state --state RELATED -j ACCEPT
iptables -A OUTPUT -p TCP -dport 21 \
   -m state --state NEW -j ACCEPT

# Ports 1024:65535 - Data
iptables -A INPUT -p TCP -sport 1024:65535 \
    -m state --state ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p TCP -dport 1024:65535 \
    -m state --state RELATED,ESTABLISHED -j ACCEPT
```

ssh, scp, ntp

```
iptables -A INPUT -p TCP -sport 22 -j ACCEPT
iptables -A OUTPUT -p TCP -dport 22 -j ACCEPT

iptables -A INPUT -p UDP -sport 123 -j ACCEPT
iptables -A OUTPUT -p UDP -dport 123 -j ACCEPT
```

Pop3 und IMAP

```
# smtp
iptables -A INPUT -p TCP -sport 25 -j ACCEPT
iptables -A OUTPUT -p TCP -dport 25 -j ACCEPT

# pop3
iptables -A INPUT -p TCP -sport 110 -j ACCEPT
iptables -A OUTPUT -p TCP -dport 110 -j ACCEPT

# IMAP2
iptables -A INPUT -p TCP -sport 143 -j ACCEPT
iptables -A OUTPUT -p TCP -dport 143 -j ACCEPT

# IMAP3
iptables -A INPUT -p TCP -sport 220 -j ACCEPT
iptables -A OUTPUT -p TCP -dport 220 -j ACCEPT
```

VPN und VNC

Muß ich an dieser Stelle leider schuldig bleiben!
Wird nachgereicht.

Fazit

Das Konfigurieren einer Firewall mit iptables ist einfach, viel Getippe, aber grundsätzlich kein Problem.
Die eigentliche Herausforderung liegt in den Kenntnissen der Protokolle speziel IP, TCP und ICMP.
Regeln für Server oder gar Router sind nochmal deutlich komplexer und müssen wesentlich individueller gestalltet werden.

Links/Quellen

Firewallgenerator

http://harry.homelinux.org

Howto

http://www.64-bit.de/dokumentationen/netzwerk/e/002/DE-IPTABLES-HOWTO.html

Ralf Spenneberg

http://www.spenneberg.de/index.html

Personal Firewall

http://linuxseiten.kg-it.de/index.php?index=fw_personal