Firewalls mit Iptables

Firewalls für den Linux Kernel 2.4

Was ist eine Firewall?

- Kontrolliert den Datenfluss zwischen dem internen Netz und dem Rest der Welt.

Es gibt 2 grundsätzliche Typen:

- Packet-Filter (z.B. Iptables)
- Capability-based Firewalls

TCP/IP Grundlagen

- TCP
- UDP
- Ports
- ICMP

Wichtige Begriffe

- NAT (Network Address Translation)
- SNAT (Source NAT)
- DNAT (Destination NAT)
- Masquerading
- Redirect
- Port Forwarding
- Accounting

Compilieren des Kernels (2.4.20)

- Networking Options
  - Network Packet Filtering (on)
  - IP Netfilter Configuration
    - <M> Connection tracking (required for masq/NAT)
    - <M> FTP protocol support
    - <M> IP tables support (required for filtering/masq/NAT)
    - <M> limit match support
    - <M> MAC address support
    - <M> netfilter MARK match support
    - <M> Multiple port match support
    - <M> Connection state match support

Compilieren des Kernels (2.4.20)

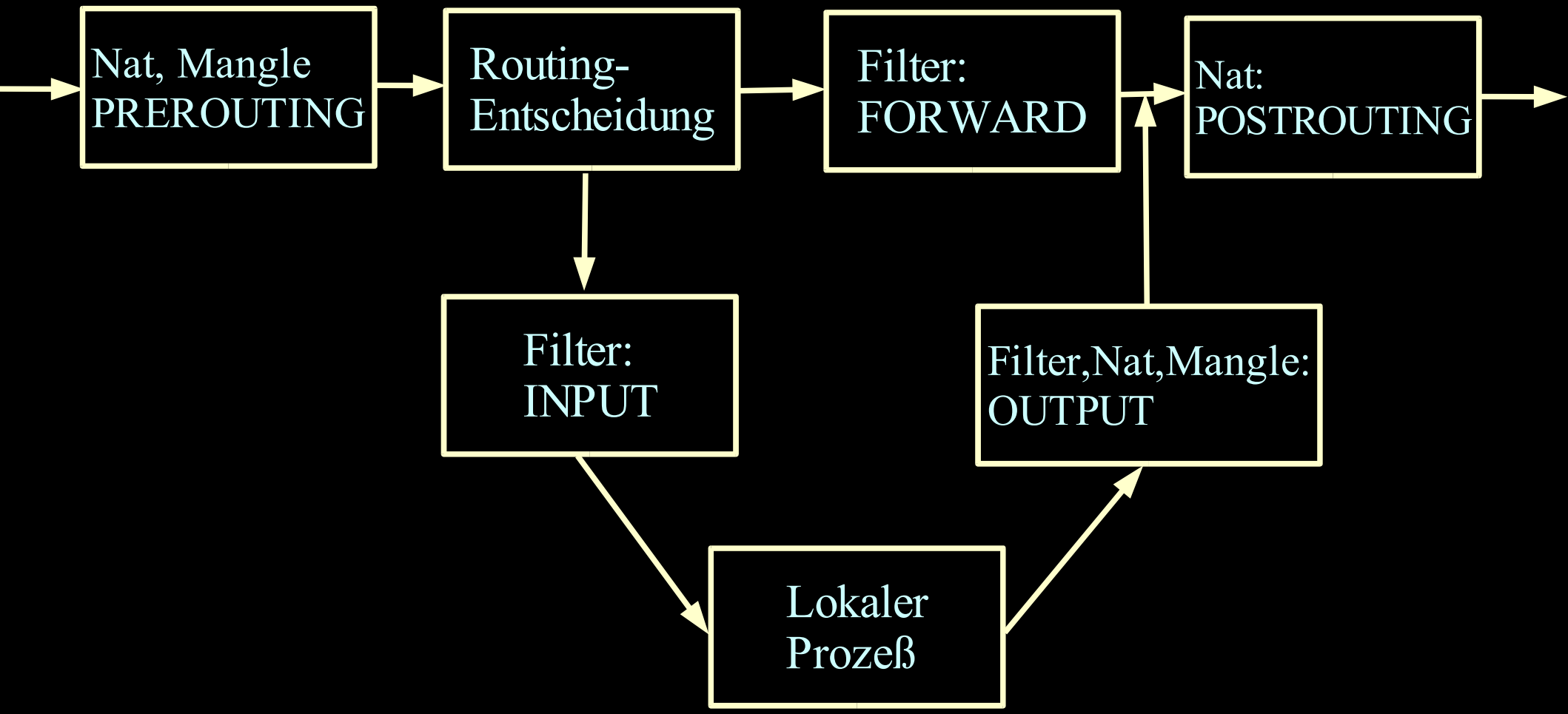
- <M> Packet filtering
- <M> REJECT target support
- <M> MIRROR target support
- <M> Full NAT
- <M> MASQUERADE target support
- <M> REDIRECT target support
- <M> LOG target support
- <M> TCPMSS target support

- Iptables Software:
  - http://www.netfilter.org

Netfilter und Iptables

- Netfilter: Allgemeine Filterstruktur im Kernel
- Iptables (Ipv4 und IPv6)

Datenfluß durch den Kernel



Tabellen und Ketten

- Filter - INPUT,FORWARD,OUTPUT
- Nat - PREROUTING,OUTPUT POSTROUTING
- Mangle - PREROUTING,OUTPUT

Weiterführende Informationen

man iptables

Filter-Policies

- Accept
- Drop
- Queue (nicht weiter behandelt)

Wichtige Aktionen von Iptables

- Accept
- Drop
- Reject
- Log
- Return
- Mirror

Filter Rules – Struktur

- Module laden
- Hilfsvariablen definieren
- Default Policy
- Ketten anlegen
- Filterregeln für die Ketten definieren

Erstes Beispiel

```
#!/bin/sh
modprobe ip_tables

iptables -A INPUT -j DROP
iptables -A FORWARD -j DROP
```

Zweites Beispiel

```
#!/bin/sh
modprobe ip_tables
iptables -F
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -P FORWARD DROP
```

Drittes Beispiel

```
modprobe ip_tables; modprobe ipt_state
modprobe ip_conntrack; modprobe ip_conntrack_ftp
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -P FORWARD DROP
iptables -N block
iptables -A block -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -j block
iptables -A FORWARD -j block
```

Viertes Beispiel (Übersicht)

- Skript Kopf
- Module laden
- Erst mal alles Blocken
- Forwarding/Masquerading
- Pakete wegwerfen
- Tcpmss und Pakete zulassen
- Stateful
- DNAT
- Logging
- Rest
- Skript Ende

Skript Kopf

```
#!/bin/sh
test -x /sbin/iptables || exit 0
IP=/sbin/iptables
DSLMODEM=eth0
# mein netz: 192.168.23.0/24
MEIN_NETZ=eth1
# mein nachbar: 192.168.100.0/24
NOCHN_NETZ=eth2
#port mappings
port=(80          12345    6667)
dest=(3:80        5:22           6:6667)
```

Module laden

```
echo -n “Starting firewall: Modules”
modprobe -k iptable_filter
modprobe -k iptable_nat
modprobe -k iptable_mangle
modprobe -k ip_conntrack
modprobe -k ip_conntrack_ftp
modprobe -k ip_conntrack_irc
modprobe -k ip_nat_ftp
modprobe -k ip_nat_irc
modprobe -k ipt_LOG
...
```

Erst mal alles Blocken

```
echo -n “ Blocking All”

$IP -F

$IP -P INPUT DROP

$IP -P FORWARD DROP

$IP -I INPUT 1 -j REJECT

$IP -I FORWARD 1 -j REJECT
```

Forwarding/Masquerading

```
echo -n " Forwarding/Masquerade"

echo 1 > /proc/sys/net/ipv4/ip_forward

$IP -t nat -A POSTROUTING --out-interface ppp0 -j MASQUERADE

$IP -t nat -A PREROUTING -i $NOCHN_NETZ -p tcp --destination-port 80 -j
    REDIRECT  --to-port 8080
```

Pakete wegwerfen

```
echo -n “ Deny”
$IP -A FORWARD --in-interface $DSLMODEM -j DROP
$IP -A INPUT -i $DSLMODEM -j DROP
$IP -A FORWARD -i $MEIN_NETZ -o $NOCHN_NETZ -j DROP
$IP -A FORWARD -i $NOCHN_NETZ -o $MEIN_NETZ -j DROP
$IP -A FORWARD -i $NOCHN_NETZ -d 202.106.185.107 -j DROP
$IP -A FORWARD -i $NOCHN_NETZ -s 192.168.100.99 -j DROP
$IP -A FORWARD -p tcp --destination-port 137:139 -j DROP
$IP -A FORWARD -p udp --dport 137:139 -j DROP
```

Tcpmss und Pakete zulassen

```
echo -n " tcpmss"

$IP -A FORWARD -p tcp --tcp-flags SYN,RST SYN -j TCPMSS --clamp-mss-to-
    pmtu

echo -n " allow"

$IP -A INPUT -i ppp0 -p tcp -s 212.202.185.0/24 --dport ssh -j ACCEPT

$IP -A INPUT -i ppp0 -p tcp --dport ssh -j MIRROR

$IP -A INPUT -i ppp0 -p tcp --dport smtp -j ACCEPT

$IP -A FORWARD -m mark --mark 23 -j ACCEPT

$IP -A INPUT -i $MEIN_NETZ -s 192.168.23.0/24 -d 192.168.23.1 -j ACCEPT

$IP -A INPUT -i $NOCHN_NETZ -p tcp --dport 3128:3129 -s 192.168.100.0/24
    -d 192.168.100.1 -j ACCEPT

...
```

Stateful

```
echo -n " stateful"

$IP -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

$IP -A FORWARD -i $MEIN_NETZ -o ppp0 -s 192.168.23.0/24 -m state
    --state NEW -j ACCEPT

$IP -A FORWARD -i $NOCHN_NETZ -o ppp0 -s 192.168.100.0/24 -m state
    --state NEW -j ACCEPT
```

DNAT

```
echo -n " dnat"

x=0

for i in ${port[*]}; do

    $IP -t mangle -A PREROUTING -i ppp0 -p tcp --dport ${port[$x]} -j MARK
        --set-mark 23

    $IP -t nat -A PREROUTING -m mark --mark 23 -p tcp --dport ${port[$x]} -j
        DNAT --to-destination 192.168.23.${dest[$x]}

done
```

Logging

echo -n “ logging”

$IP -A INPUT -p icmp -j LOG --log-level notice --log-prefix “ICMP “ -m limit --limit 10/minute

$IP -A INPUT -p tcp --syn -j LOG –log-level notice --log-prefix “SYN “ -m limit –limit 1/s

Rest

```
echo -n “ finish”
$IP -A INPUT -i ppp0 -p tcp -j REJECT --reject-with tcp-reset
$IP -A INPUT -i ppp0 -p udp -j DROP
$IP -A FORWARD -i ppp0 -p tcp -j REJECT --reject-with tcp-reset
$IP -A FORWARD -i ppp0 -p udp -j DROP
$IP -P INPUT ACCEPT
$IP -P FORWARD ACCEPT
$IP -D INPUT 1
$IP -D FORWARD 1
echo “.”
;;
```

Skript Ende

```
stop)
        echo -n " Stopping firewall: Flush"
        $IP -F
        $IP -t nat -F
        $IP -t mangle -F
        echo -n " Policies"
        $IP -P INPUT DROP
        $IP -P FORWARD DROP
        $IP -A INPUT -p tcp --dport ssh -j ACCEPT
        echo "."
        ;;
```

Skript Ende (2)

```
restart)
        $0 stop
        $0 start
        ;;
*)
        echo “Usage: $0 {start|stop|restart}”
        exit 1
esac
exit 0
```