

iptables

```
192.168.101.254 - PuTTY

Chain INPUT (policy DROP 68 packets, 5895 bytes)
  pkts bytes target     prot opt in     out     source            destination
 2266 251K ipac~o      all  --  *      *        0.0.0.0/0         0.0.0.0/0
 2266 251K BADTCP   all  --  *      *        0.0.0.0/0         0.0.0.0/0
 2266 251K CUSTOMINPUT all  --  *      *        0.0.0.0/0         0.0.0.0/0
 2266 251K GUIINPUT  all  --  *      *        0.0.0.0/0         0.0.0.0/0
 995 88471 ACCEPT     all  --  *      *        0.0.0.0/0         0.0.0.0/0          state RELATED,ESTABLISHED
1253 161K IPSECVIRTUAL all  --  *      *        0.0.0.0/0         0.0.0.0/0
1253 161K OPENSSELVIRTUAL all  --  *      *        0.0.0.0/0         0.0.0.0/0
   4 277 ACCEPT     all  --  lo     *        0.0.0.0/0         0.0.0.0/0          state NEW
   0 0 DROP       all  --  *      *        127.0.0.0/8       0.0.0.0/0          state NEW
   0 0 DROP       all  --  *      *        0.0.0.0/0         127.0.0.0/8       state NEW
 772 92166 ACCEPT     !icmp --  eth0   *        0.0.0.0/0         0.0.0.0/0          state NEW
 477 68388 DHCPBLUEINPUT all  --  *      *        0.0.0.0/0         0.0.0.0/0
 477 68388 IPSECPHYSICAL all  --  *      *        0.0.0.0/0         0.0.0.0/0
 477 68388 OPENSSELPHYSICAL all  --  *      *        0.0.0.0/0         0.0.0.0/0
 477 68388 WIRELESSINPUT all  --  *      *        0.0.0.0/0         0.0.0.0/0          state NEW
   68 5895 REDINPUT  all  --  *      *        0.0.0.0/0         0.0.0.0/0
   68 5895 XTACCESS  all  --  *      *        0.0.0.0/0         0.0.0.0/0          state NEW
   10 1120 LOG       all  --  *      *        0.0.0.0/0         0.0.0.0/0          limit: avg 10/min burst 5 LOG flags 0 level 4 prefix `INPUT '

Chain FORWARD (policy DROP 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source            destination
   93 7812 ipac~fi     all  --  *      *        0.0.0.0/0         0.0.0.0/0
   93 7812 ipac~fo     all  --  *      *        0.0.0.0/0         0.0.0.0/0
   93 7812 BADTCP     all  --  *      *        0.0.0.0/0         0.0.0.0/0
   0 0 TCPMSS      tcp  --  *      *        0.0.0.0/0         0.0.0.0/0          tcp flags:0x06/0x02 TCPMSS clamp to PMTU
   93 7812 CUSTOMFORWARD all  --  *      *        0.0.0.0/0         0.0.0.0/0
  17 1428 ACCEPT     all  --  *      *        0.0.0.0/0         0.0.0.0/0          state RELATED,ESTABLISHED
  76 6384 IPSECVIRTUAL all  --  *      *        0.0.0.0/0         0.0.0.0/0
  76 6384 OPENSSELVIRTUAL all  --  *      *        0.0.0.0/0         0.0.0.0/0
   0 0 ACCEPT     all  --  lo     *        0.0.0.0/0         0.0.0.0/0          state NEW
   0 0 DROP       all  --  *      *        127.0.0.0/8       0.0.0.0/0          state NEW
   0 0 DROP       all  --  *      *        0.0.0.0/0         127.0.0.0/8       state NEW
  22 1848 ACCEPT     all  --  eth0   *        0.0.0.0/0         0.0.0.0/0          state NEW
  54 4536 WIRELESSFORWARD all  --  *      *        0.0.0.0/0         0.0.0.0/0          state NEW
   0 0 REDFORWARD all  --  *      *        0.0.0.0/0         0.0.0.0/0
   0 0 PORTFWACCESS all  --  *      *        0.0.0.0/0         0.0.0.0/0          state NEW
   0 0 LOG       all  --  *      *        0.0.0.0/0         0.0.0.0/0          limit: avg 10/min burst 5 LOG flags 0 level 4 prefix `OUTPUT '

```

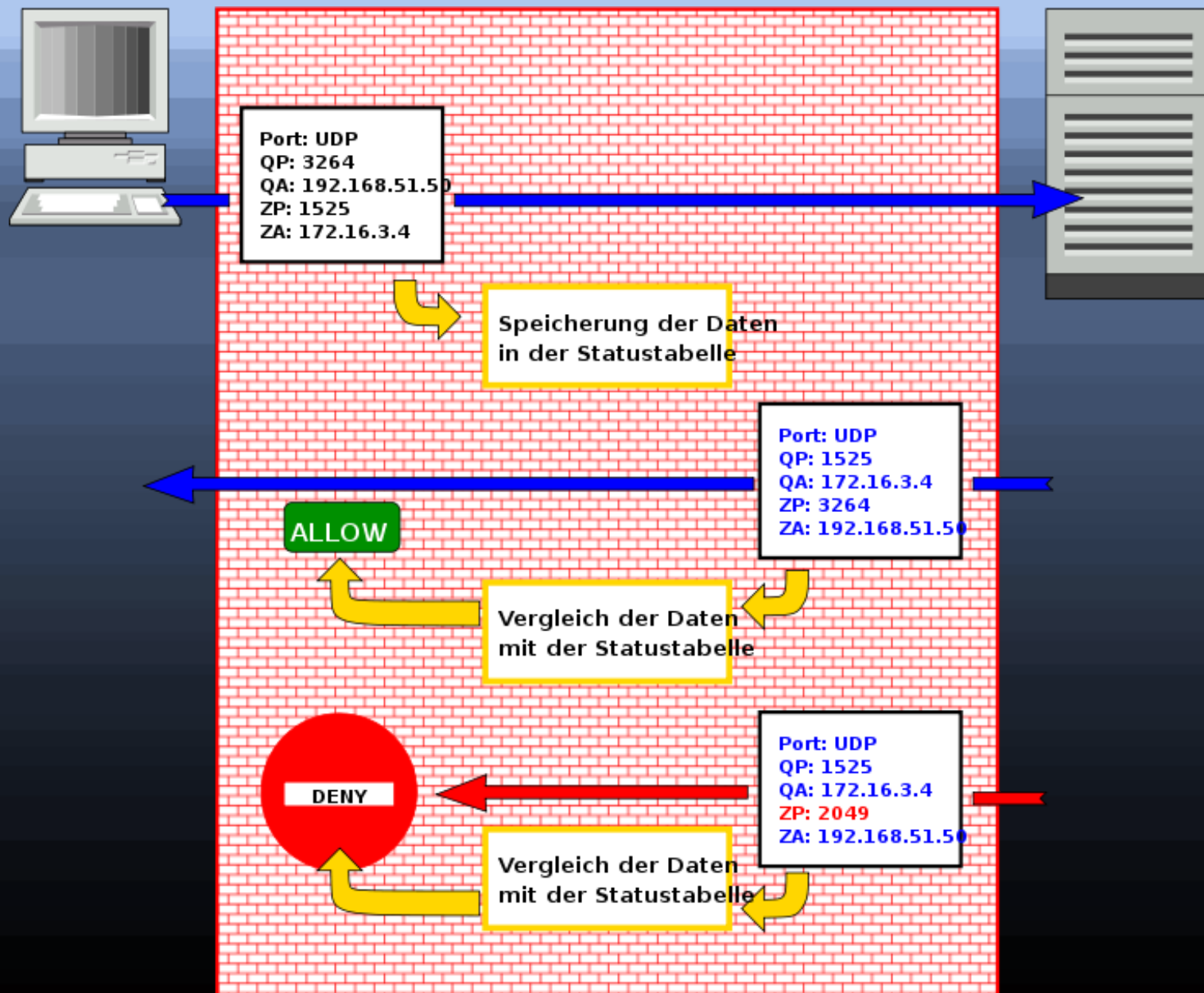
Gliederung

- Firewall-Technologien (Filtertechnologien)
- Stateful Packet Inspection (SPI)
- Iptables
- DEMO

Firewall-Technologien (Filtertechnologien)

- Proxyfilter
- Contentfilter
- Paketfilter (Stateless Packet Inspection)
- Stateful Packet Inspection

Stateful Packet Inspection



Was ist „iptables“ ?

- Frontend zum editieren der Filtertabellen des Kernels
- Teil des Netfilter Softwareprojekts
- seit Linux Kernel 2.4 dabei (ca. 1999)
- Vorgänger ipchains (stateless)

Aufbau der Filter-Tabelle

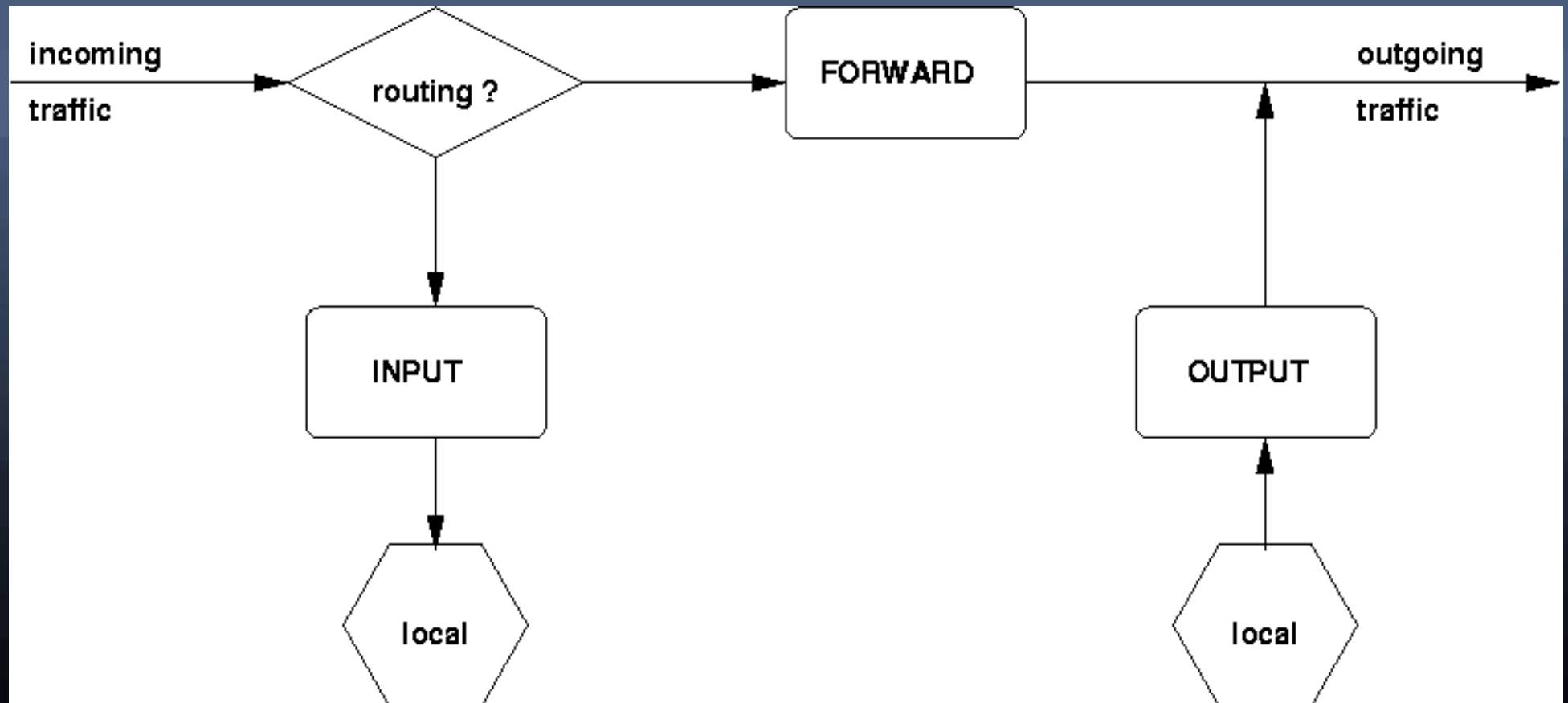
3 Ketten (chains)

→ INPUT

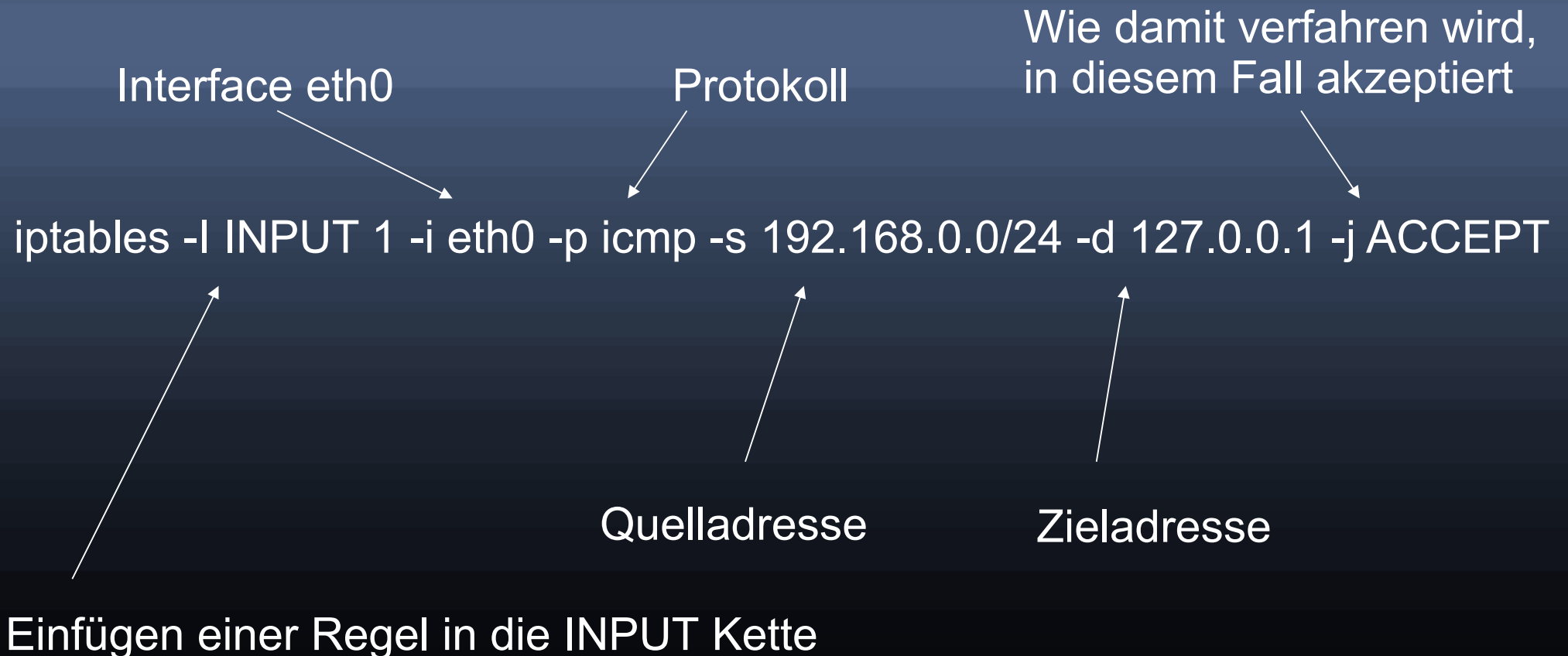
→ FORWARD

→ OUTPUT

Funktionsweise



Aufbau einer Regel



DEMO

Quellen

- www.netfilter.org
- www.wikipedia.de
- www.rrze.uni-erlangen.de
- Iptables manpage
<http://ipset.netfilter.org/iptables.man.html>