Netfilter unter Linux

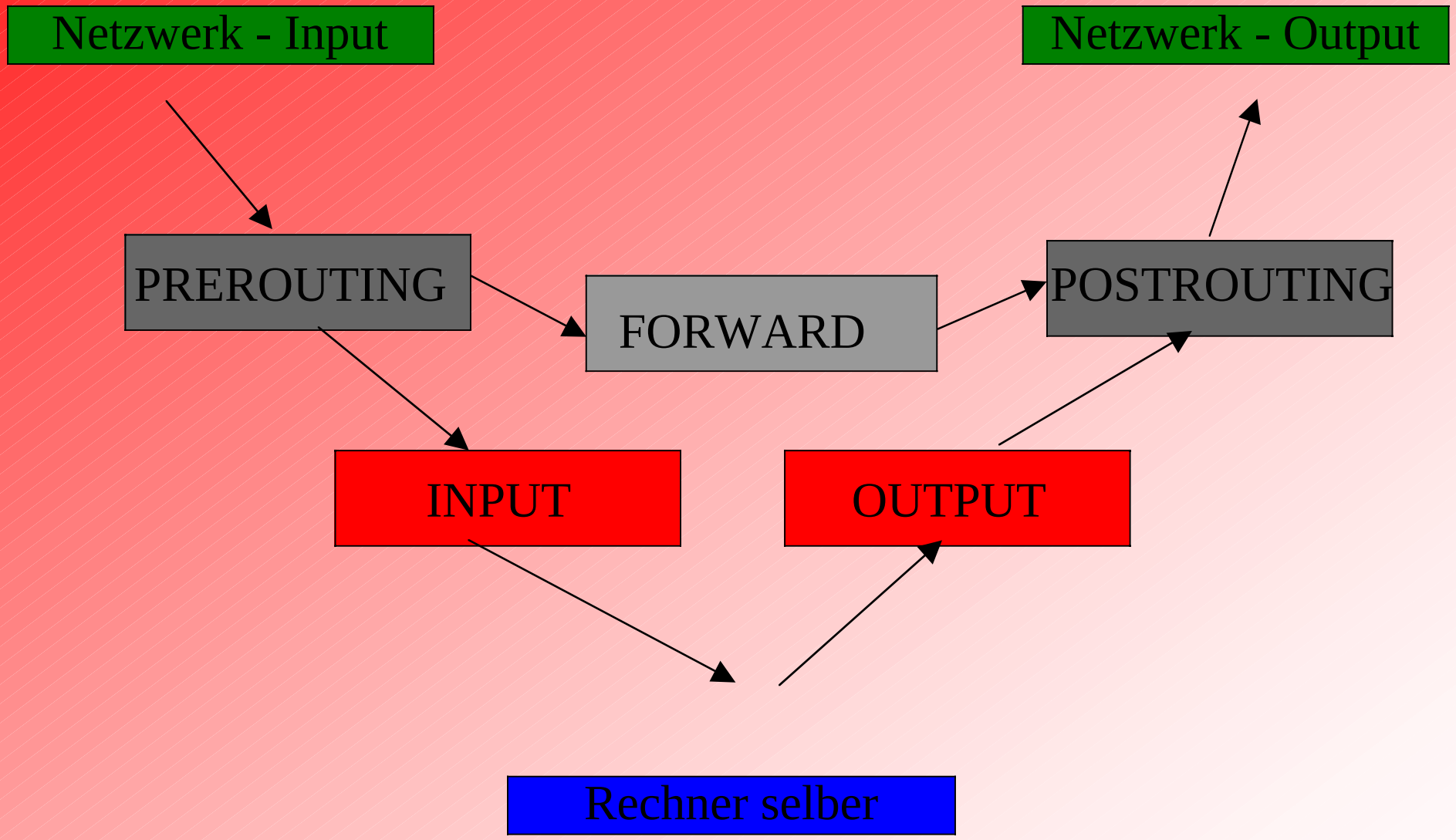
Was ist Netfilter

- Der neue Linux-Packetfilter seit Kernel 2.4
- Auch für 2.2 als externer Patch erhältlich
- Kompatibiltätsmodule zu ipchains und ipfwadm
- Viele Neuerungen -> dazu später mehr

Features von Netfilter

- Statefull Inspection
- Richtiges NAT (SNAT, DNAT, MASQUARADE)
- Erweitere LOG-Fähigkeiten (Userlevel Tools)
- Modulares Design, damit extrem erweiterbar
- Modulares Regeldesign

Flussdiagramm der Regeln bei Netfilter

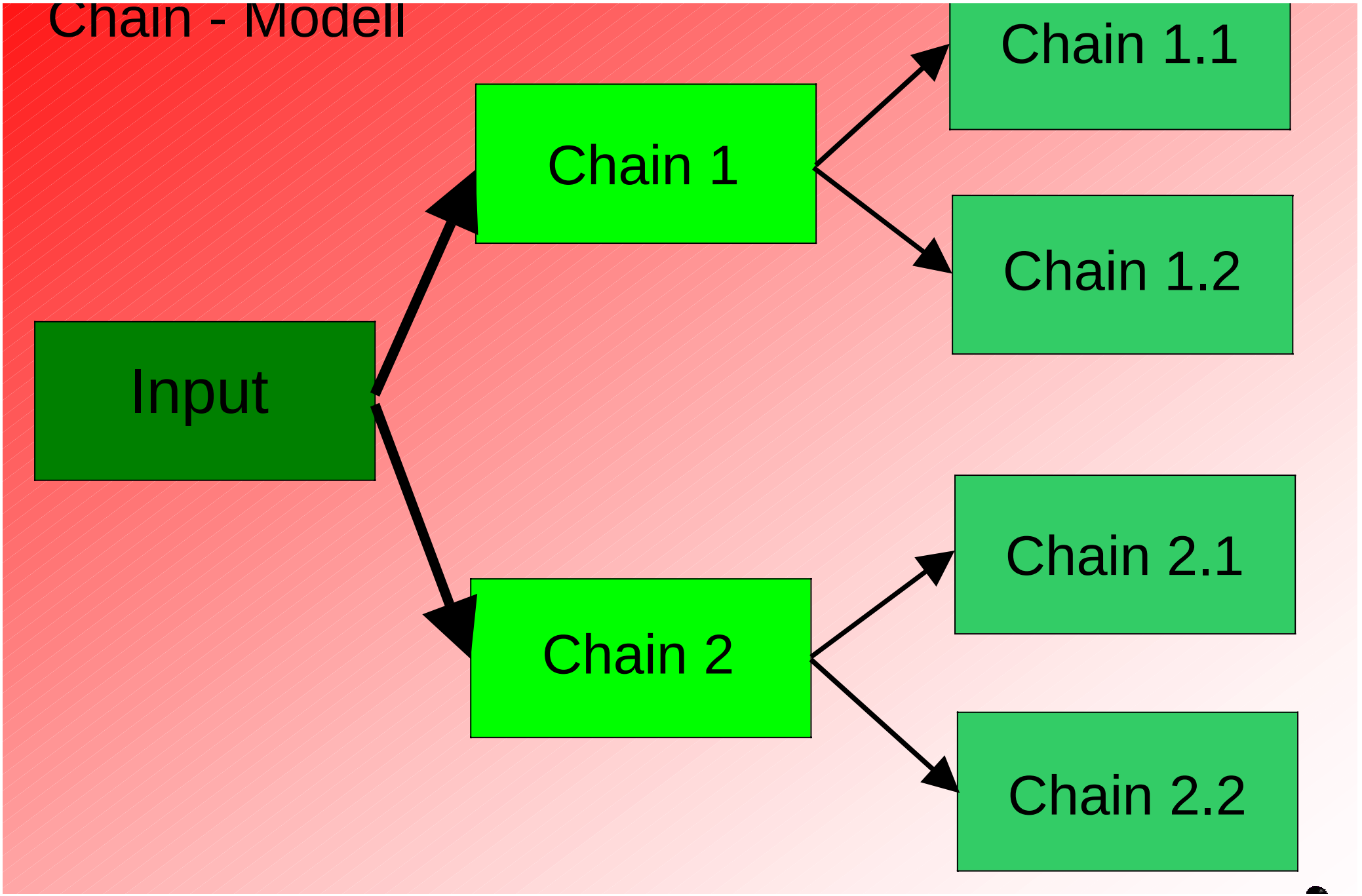


Wie funktioniert es technisch

- Es gibt 3 Hooks im Kernel, wo Packete „abgegriffen werden“
- Die Regelsätze werden top-down durchgelaufen
- Durchlauf TARGET-abhängig
- Es können Parameter über das /proc Filesystem geändert werden (Connection-Tracking)

Userspace

- Iptables heist das neue Tool, welches die Steuerung der Regeln übernimmt
- Ipchains und ipfwadm mit der jeweiligen Emulation
- Log-Deamon um über das Target LOG Daten zu erhalten


Chain - Modell
Input
Chain 1
Chain 2
Chain 1.1
Chain 1.2
Chain 2.1
Chain 2.2

Beispiele

- iptables -A FORWARD -s 194.94.249.2/32 -j HUBRREGEL
- iptables -A INPUT -d 194.94.249.2/32 -j ACCEPT
- iptables -A INPUT -p TCP -d 194.94.249.2 --dport smtp -j DROP
- iptables -A FORWARD -m state --state established, related -j ACCEPT
- iptables -t nat -A POSTROUTING -j MASQUERADE
- iptables -t nat -A POSTROUTING -j DNAT—to 194.94.249.2