mxallowd

Anti-Spam mit nolisting und iptables

Spammer

- sind blöd
- wollen viel spammen
- können nicht programmieren und sich anscheinend keine Programmierer leisten

→ sie benutzen schlechte Mailer und haben anscheinend besseres zu tun als Standards zu lesen...

nolisting

- Man gibt zwei Mailserver an für eine Domain
- einer davon weist alle Verbindungen ab und ist folglich "down"
- der andere nimmt Mails an
- Spammer k(onnten|önnen) nicht programieren und nehmen nur den ersten

nolisting

- Mittlerweile haben Spammer gelernt und nehmen halt gleich den zweiten ("direct-to-second-mx")
- "gelernt"

mxallowd

- na dann tun wir halt so als wären beide down :-)
- klappt das mit iptables? leider nicht...

mxallowd

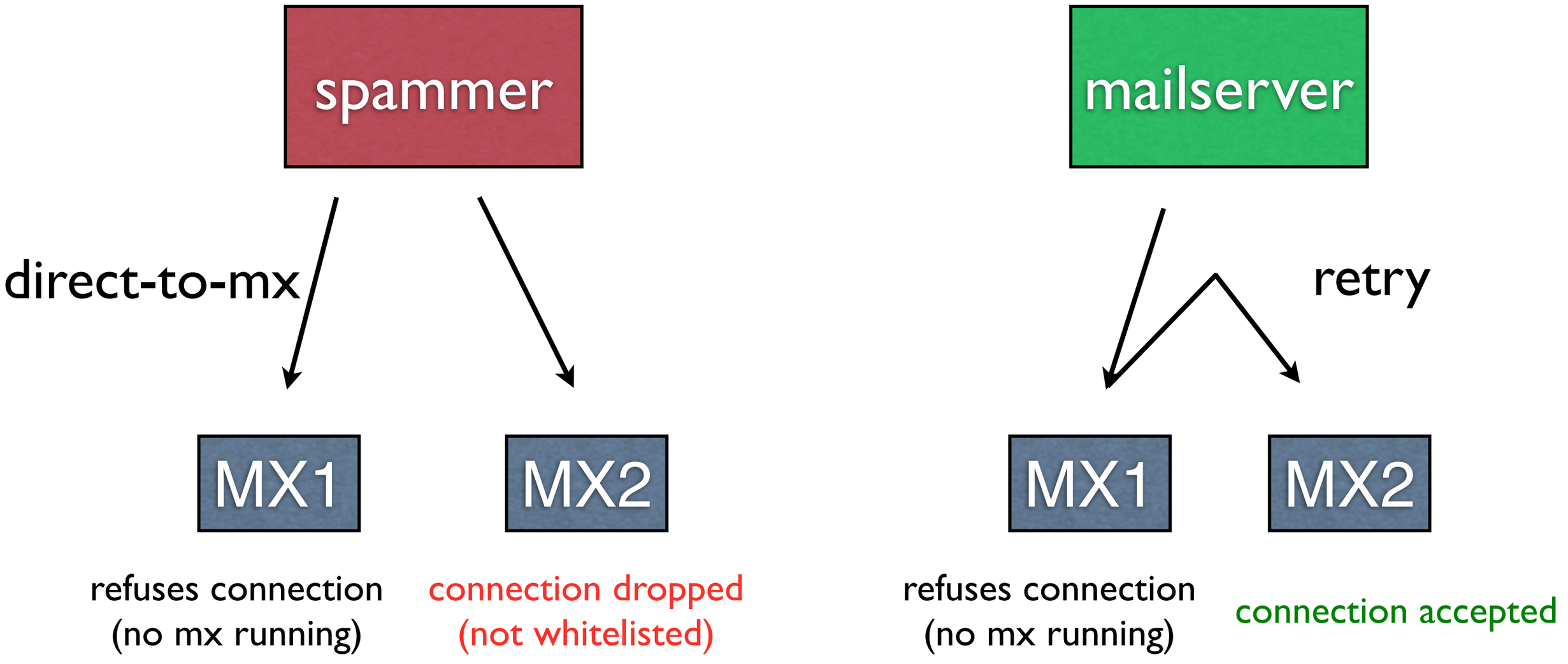
- iptables hat die Möglichkeit, die Pakete einer Regel an ein Userspace-Programm weiterzureichen, dieses kann entscheiden
- dann bauen wir halt unseren eigenen Filter, mit Blackjack und...

mxallowd

- in C geschrieben
- 666 lines of code
- extrem schnell (bis auf das Resolving, das liegt in der Natur der Sache)
- Debian-Paket vorhanden, Gentoo-ebuild vorhanden

setup

- `apt-get install mxallowd`
- ```
  iptables -A INPUT -p tcp \
  --dport 25 -m state \
  --state NEW -j NFQUEUE \
  --queue-num 23
  ```
- ```
  mxallowd \
  -s \
  -f 192.168.1.3 \
  -r 192.168.1.4 \
  -n 23
  ```


spammer
direct-to-mx
MX1
refuses connection
(no mx running)
MX2
connection dropped
(not whitelisted)
mailserver
retry
MX1
refuses connection
(no mx running)
MX2
connection accepted