policyd-weight

Policy-Daemon für Postfix

Agenda

- Einführung
- Features
- Funktionsweise
- Kriterien
- Setup

Einführung

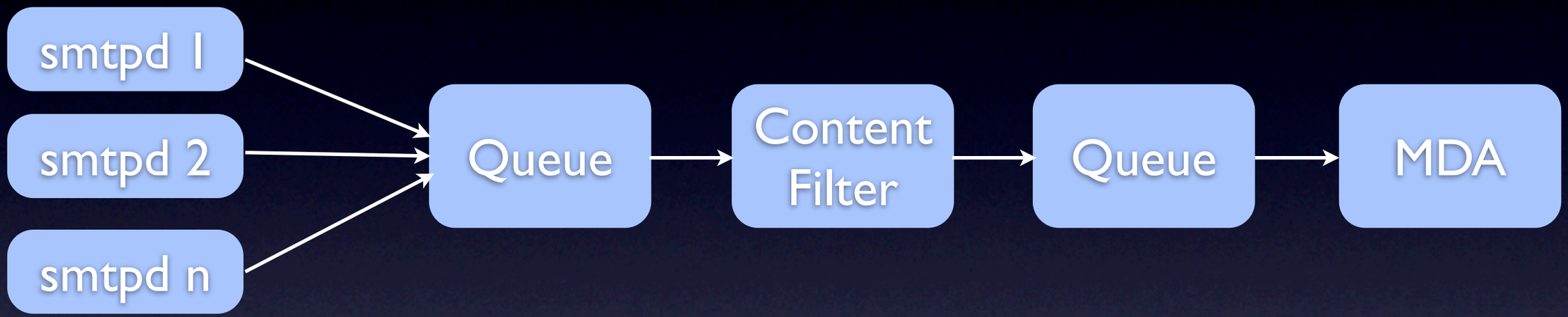
- 23. März 2005 bis (9. Februar 2008)
- Robert Felber
- Policy-Daemon für Postfix (>2.1)
- Perl
- GPL v2

Features

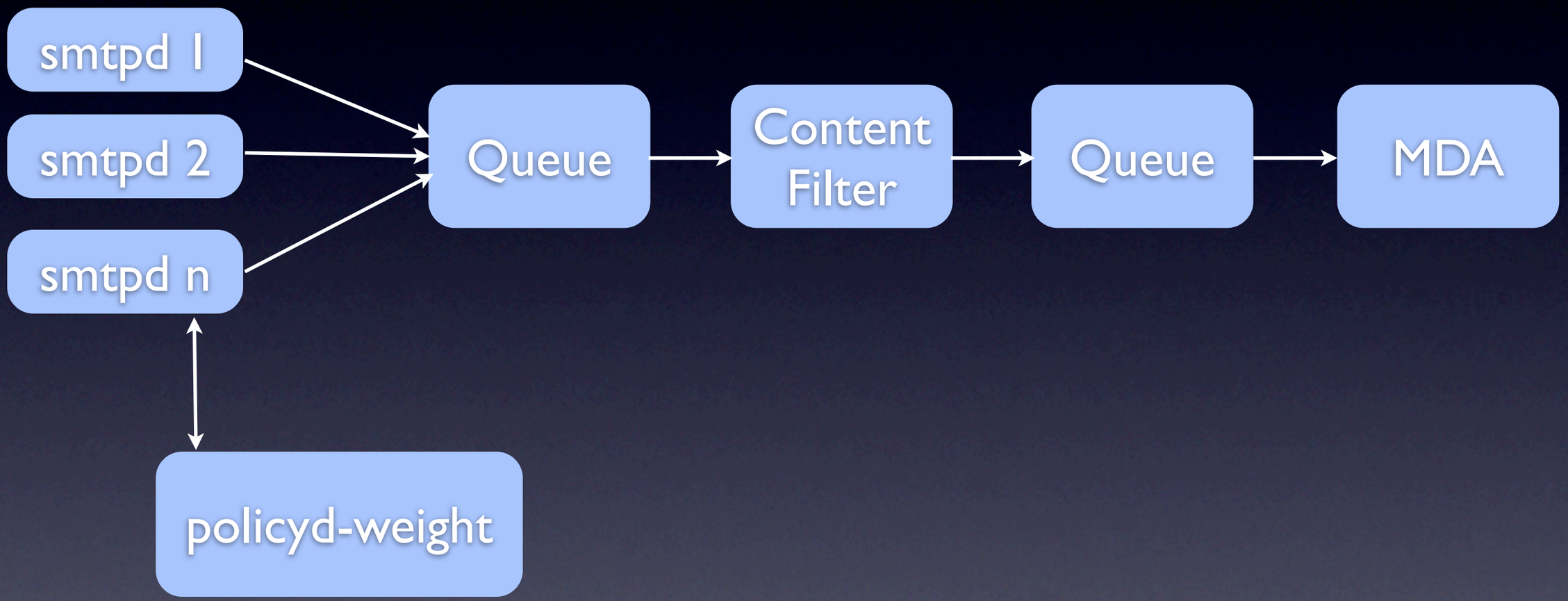
- Score-basierte Auswertung von DNSBL
- Score-basierte Auswertung der Beziehung und Korrektheit von DNS-Einträgen, HELO und MAIL-FROM und Client-IP
- Caching von DNS-Abfragen und Score-Ergebnissen
- eigene, schnelle DNS-Lookup Routine
- frei konfigurierbare Scores und RBLs

Funktionsweise

Funktionsweise



Funktionsweise



Kriterien

- RBL/RHSBL
- Beziehung zwischen IP, HELO MAIL-From
- DailUp-RegEx
- HELO-IP im Subnetz
- Random-Sender-Score

Setup

- Debian-Repositories bzw. FreeBSD-Ports oder Perl-Skript auf Homepage
- smtpd_recipient_restrictions =

  permit_mynetworks,

  ... weitere Anweisungen ...

  reject_unauth_destination,

  ... weitere Whiteliste Anweisungen ...

  check_policy_service inet:127.0.0.1:12525 # Policyd-weight

Beispiel

postfix/smtpd[8906]: connect from 82.198.60.144.dyn.user.ono.com[82.198.60.144]

postfix/policyd-weight[1604]: weighted check:
IN_DYN_PBL_SPAMHAUS=3.25
NOT_IN_SBL_XBL_SPAMHAUS=-1.5
NOT_IN_SPAMCOP=-1.5
CL_IP_NE_HELO=4.75
<client=82.198.60.144> <helo=gmx.de> <from=mail@gmx.de>
<to=ich@abwesend.com>; rate: 5.0

postfix/policyd-weight[1604]: decided action=550 Mail appeared to be SPAM or forged. Ask your Mail/DNS-Administrator to correct HELO and DNS MX settings or to get removed from DNSBLs; MTA helo: gmx.de, MTA hostname: 82.198.60.144.dyn.user.ono.com[82.198.60.144] (helo/hostname mismatch); <client=82.198.60.144> <helo=gmx.de> <from=mail@gmx.de> <to=ich@abwesend.com>; delay: 0s

Zusammenfassung

- vor dem Einsatz prüfen!
- abweisen während des SMTP-Dialog
  - verändert rechtliche Sachlage
  - spart CPU ;)
- Abweisung erst wenn mehrere Kriterien erfüllt sind

Vielen Dank für die Aufmerksamkeit

Fragen?