

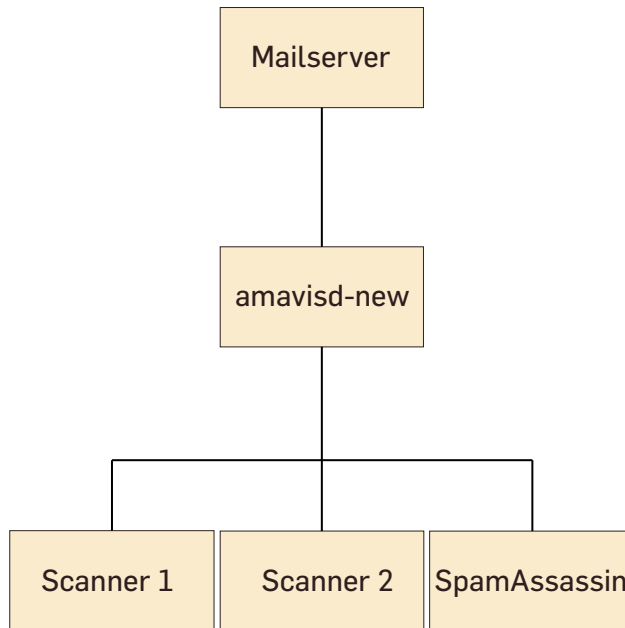
amavisd-new

Viren- und spam-Scanner im Überblick

Inhalt

- Beschreibung
- Historie
- Funktionalitäten
- Funktionsweise
- Konfiguration
- Integration
- Performance
- Ausblick

Beschreibung



amavisd-new ist ein in PERL geschriebener Daemon, der über

- (E)SMTP
- LMTP
- Skripte

angesprochen werden kann und

- Viren-Scanner
- SpamAssassin

einbindet. Maintainer und/oder Autor von amavisd-new ist Mark Martinec.

Download

<<http://www.ijs.si/software/amavisd/>>

Historie

1997

Shell-Skript (Rainer Link)

2000

PERL-Programm

2001

PERL-Daemon

2002

modulares Design

2002-03

PERL-Daemon, pre-fork, NET::Server (Mark Martinec)

Funktionalitäten

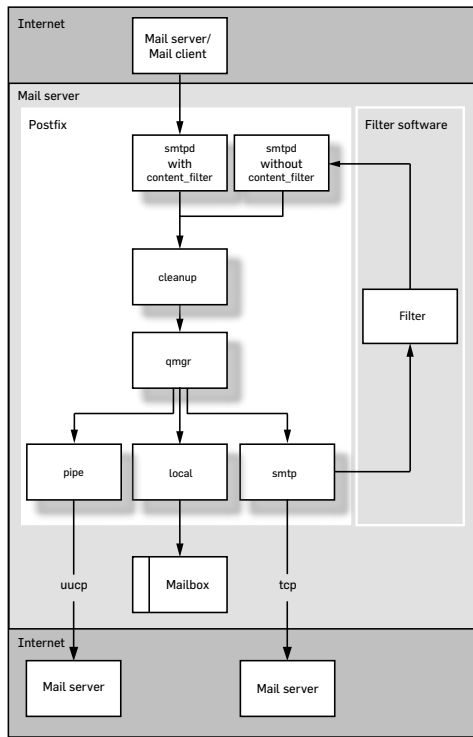
- E-Mail
 - DeKodieren
 - Auspacken
- Viren-Scanner
 - ClamAV
 - KasperskyLab AVP
 - H+BEDV AntiVir
 - NAI McAfee AntiVirus
 - ...
- E-Mail Quarantäne
- SpamAssassin
- Blacklists (DNS)
- Blacklists (DNS)
- Datenbank-Anbindung
 - Regeln
 - global
 - benutzer-spezifisch
 - Konfiguration
 - Logging
- Policy-Banks
- standard-komform
 - SMTP
 - MIME
 - DSN
- fehlertolerant

Funktionsweise

1. E-Mail per (E)SMTP oder LMTP entgegennehmen
Verbindung wird offen gehalten!
2. E-Mail dekodieren und/oder auspacken
Performance-Gewinn!
3. E-Mail nacheinander an Scanner und/oder SpamAssassin übergeben
4. Ergebnis auswerten
 - unschädliche E-Mail
E-Mail per SMTP zurückgeben
 - schädliche E-Mail
E-Mail in Quarantäne und Benachrichtigung
5. Eingehende Verbindung mit OK bestätigen
Trick macht amavisd-new-Integration fehlertolerant!

Konfiguration

Postfix: store first - filter later



Postfix nimmt E-Mail an und übergibt sie dann mit einem `content_filter` an amavisd:

- SMTP
- LMTP

Postfix nimmt E-Mail über einen smtpd-Daemon *ohne* `content-filter` wieder entgegen.

Postfix: store first - filter later

Details

Service mit content_filter in main.cf definieren:

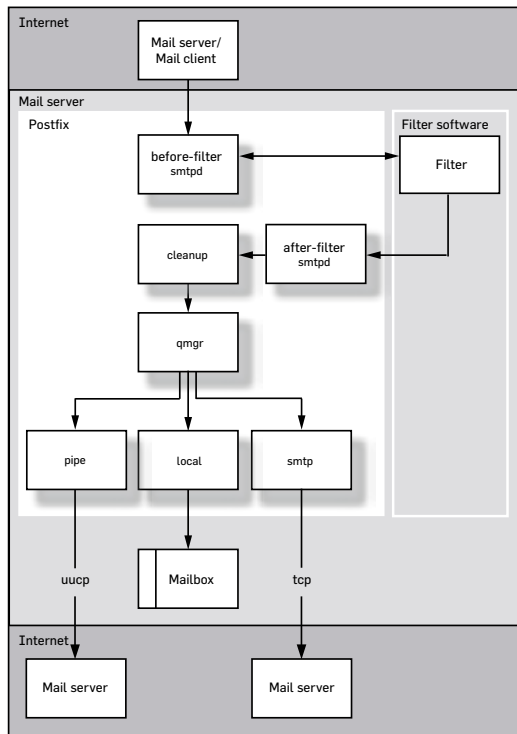
```
content_filter = amavisd:[127.0.0.1]:10024
```

Service und Wiedereintritt in master.cf konfigurieren:

```
# =====  
# service    type  private    unpriv    chroot    wakeup    maxproc    command + args  
#           (yes)    (yes)    (yes)    (never)    (100)  
# =====  
amavisd      unix  -          -         n         -         2          lmtpl  
    -o lmtpl_data_done_timeout=1200s  
    -o disable_dns_lookups=yes  
  
127.0.0.1:10025 inet n          -         n         -         -          smtpd  
    -o content_filter=  
    -o local_recipient_maps=  
    -o relay_recipient_maps=  
    -o smtpd_restriction_classes=  
    -o smtpd_client_restrictions=  
    -o smtpd_helo_restrictions=  
    -o smtpd_sender_restrictions=  
    -o smtpd_recipient_restrictions=permit_mynetworks,reject  
    -o mynetworks=127.0.0.0/8  
    -o strict_rfc821_envelopes=yes
```

Konfiguration

Postfix: filter first - store later



Postfix übergibt E-Mail sofort mit einem `smtpd_proxy_filter` per SMTP an `amavisd`.

Postfix nimmt E-Mail über einen `smtpd`-Daemon wieder entgegen.

Problem: Timeout des Mail-Clients!

Postfix: filter first - store later

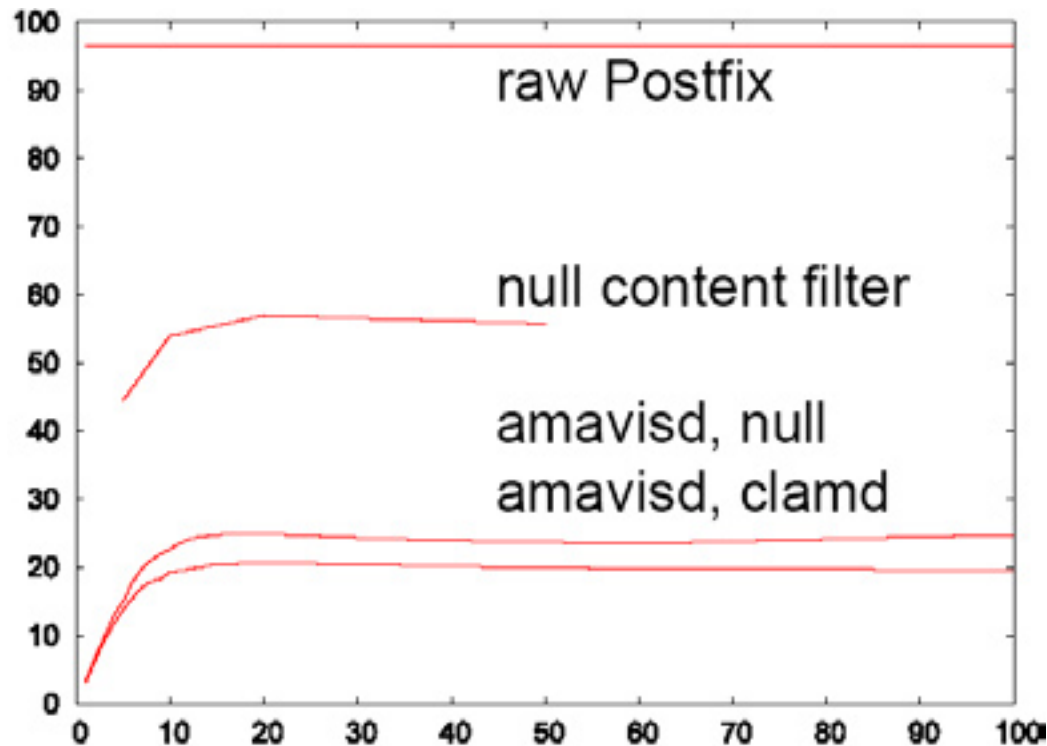
Details

smtpd_proxy_filter und Wiedereintritt in master.cf konfigurieren:

```
# =====
# service    type  private      unpriv      chroot      wakeup      maxproc      command + args
#           (yes)   (yes)       (yes)       (never)     (100)
# =====
smtp        inet  n            -           n           -           20           smtpd
    -o smtpd_proxy_filter=localhost:10024
    -o smtpd_client_connection_count_limit=10
...
127.0.0.1:10025 inet n            -           n           -           -           smtpd
    -o smtpd_authorized_xforward_hosts=127.0.0.0/8
    -o smtpd_client_restrictions=
    -o smtpd_helo_restrictions=
    -o smtpd_sender_restrictions=
    -o smtpd_recipient_restrictions=permit_mynetworks,reject
    -o mynetworks=127.0.0.0/8
    -o receive_override_options=no_unknown_recipient_checks
...

```

Performance



Festplatte ist das Problem:

- separate Disks für Mail-Queue und Amavis Temp-Verzeichnis
- RAM-Disk für amavisd-new
- separate Hosts
- Load-Balancing

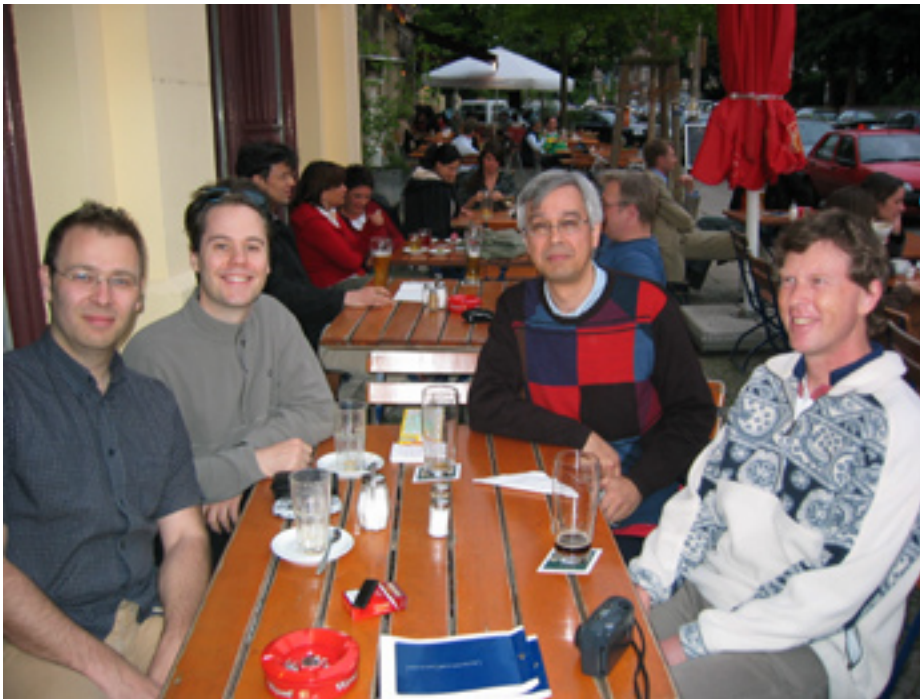
Viren-Scanner ist das Problem:

- Daemonisierte Viren-Scanner einsetzen

Syslogd ist das Problem:

- Asynchron schreiben lassen (Linux)

Ausblick



Von links nach rechts:
Patrick Koetter, Ralf Hildebrandt, Wietse Venema, Mark Martinec

amavid-new ist vor einer Konsolidierungsphase:

- Viren-Scanner Module vereinheitlichen
- Dokumentation
 - User Manual
 - Developer Manual
- Ecken und Kanten glätten

Jetzt sind Hilfs-Applikationen gefragt, die das Leben im Alltag leichter machen...