Mailserver mit Spam- und Virenfilter für den Hausgebrauch

Exim4/Cyrus/Squirrelmail und ein paar Kniffe

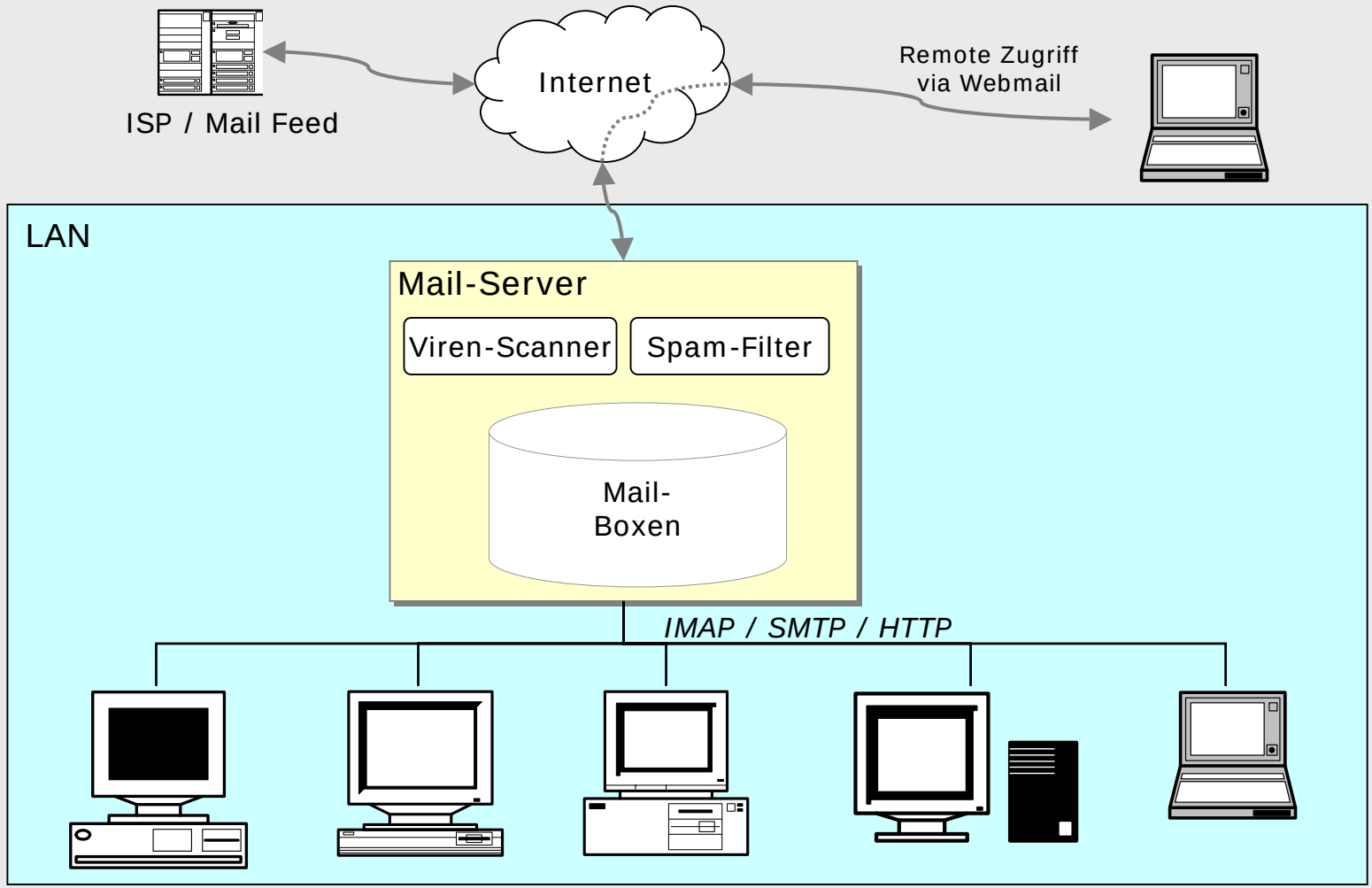
Hans-Jürgen Beie <hjb@pollux.franken.de>

Inhalt

Mailserver für den Hausgebrauch

- Einführung
  - Szenario - Warum? - Komponenten
- Exim 4
  - Konfiguration - Access - Lists - RouterTransports
- Cyrus
- SquirrelMail
- SpamAssassin
- ClamAV
- Wie geht das alles zusammen?
- Helferlein
- Hinweise
- Referenzen

Szenario: Zentraler Mail-Server für ein lokales Netz



Einführung – Warum?

Warum ein eigener Mail-Server für zu Hause?

- Mails mehrerer Mail-(Postfächer/Konten) können in EINE lokale Mailbox gesammelt werden
- Server-seitiges Scannen und Filtern
- Einfachere und einheitliche Handhabung für den Anwender
- Die Sicht auf die persönlichen Postfächer ist (bei IMAP) unabhängig vom Client immer gleich (praktisch für mobile Anwender)

Was soll der Mail-Server können?

- Mail von externen Postfächern (für mehrere User) automatisch sammeln (POP3/IMAP/UUCP)
- Spam und infizierte Mails filtern
- IMAP/SMTP-Server für lokale Clients
- zentraler Mail-Versand nach außen (SMTP/UUCP)
- Webmailer (optional Zugriff von außen)

Server-Komponenten

- Exim 4 / exiscan

  MTA, übersichtliche und flexibel Konfiguration, hervorragende Dokumentation, Schnittstellen für flat files und verschiedene Datenbanken.
  exiscan ist eine Erweiterung des ACL-Systems von Exim. Damit lassen sich Mails bereits während einer noch aktiven SMTP-Session analysieren und ggf. zurückweisen.
- Cyrus IMAPD

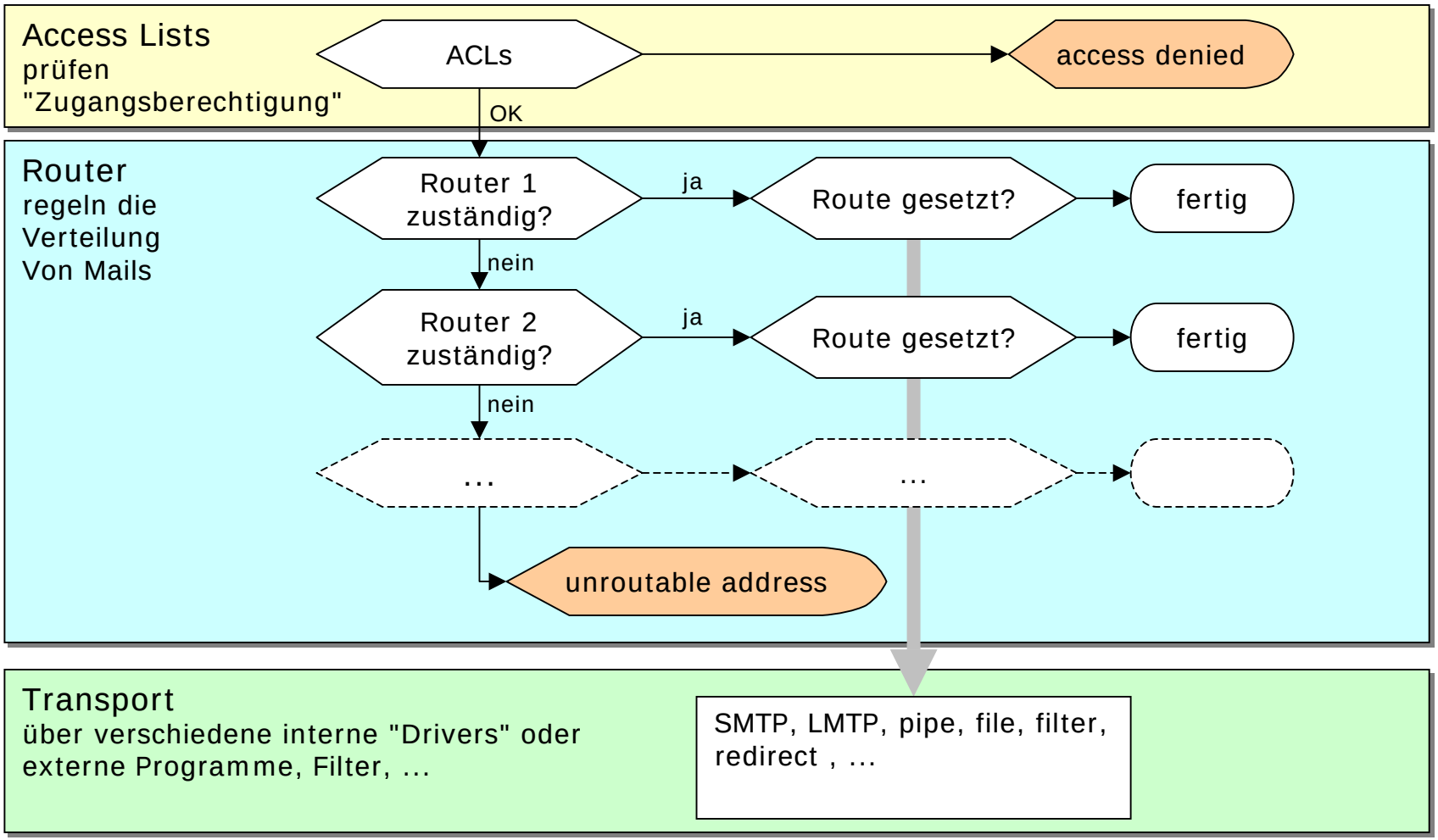
  IMAP / POP3 Server mit integrierter Filtersprache (Sieve) und Mailbox-Datenbank
- SpamAssassin

  Inhaltliche Bewertung von Mails mit Hilfe schematisierter Regeln und Wichtungen. Kann manuell/automatisch trainiert werden (Bayes-Datenbank).
- ClamAV

  Einer der wenigen frei verfügbaren Viren-Scanner (GPL).
- SquirrelMail / Avelsieve (optional)

  Webmailer. Braucht HTTP-Server (Apache) mit PHP. Avelsieve ist ein Plugin für SM, mit dem sich sehr einfach Filterregeln für Cyrus-Sieve erstellen lassen.

Wie arbeitet Exim eine Mail ab?

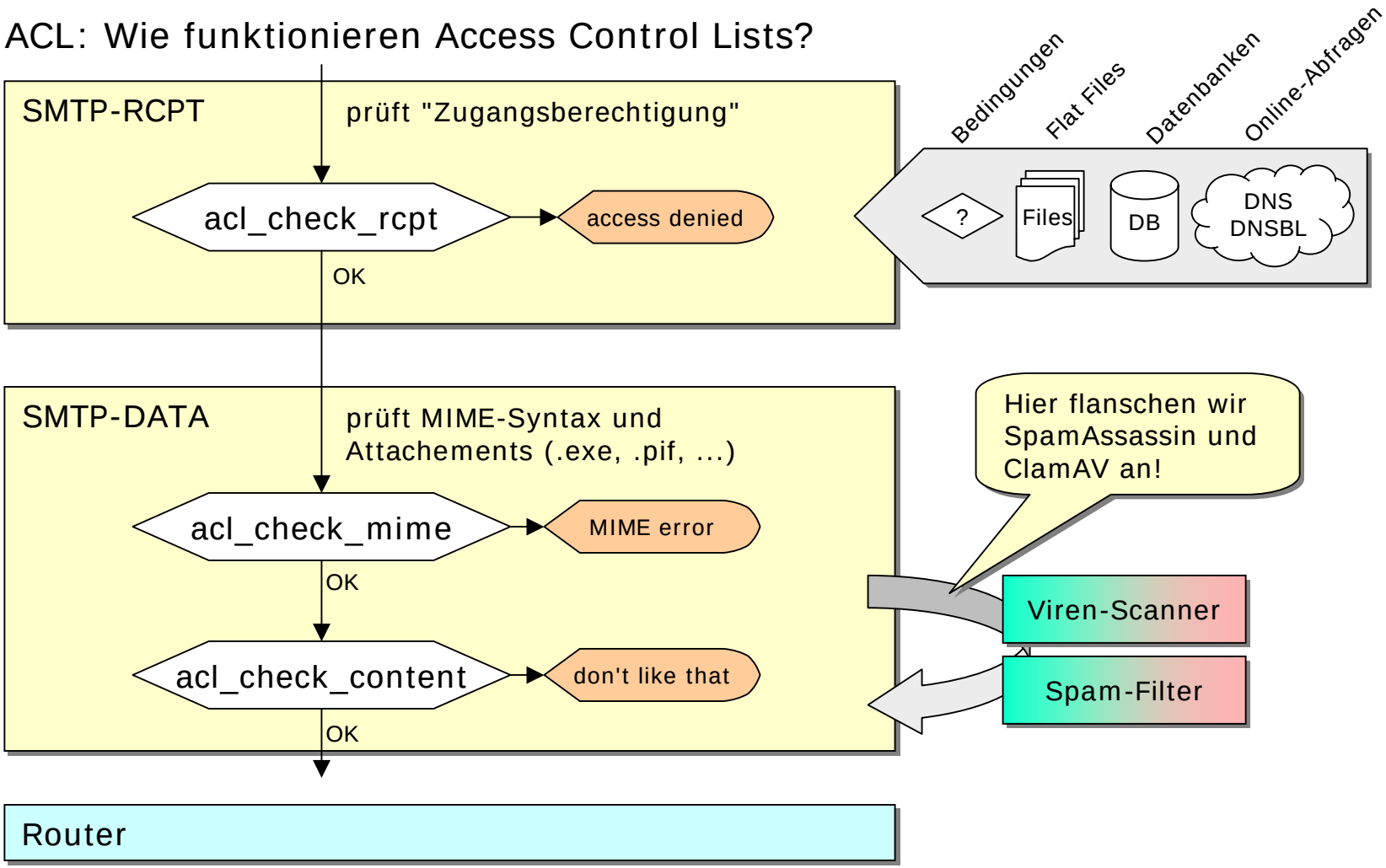


Konfigurationsdatei exim4.conf

Ist nach funktionale Sektionen geliedert:

- Grundeinstellungen und Makros
- ACLs
  Access Control Lists: Was wird angenommen?
- ROUTER
  Wohin werden Mails ausgeliefert?
- TRANSPORTS
  Wie werden Mails ausgeliefert?
- RETRY
  Wie oft und wie lange werden Zustellungen versucht?
- REWRITE
  Adressen manipulieren
- AUTHENTICATORS
  Mechanismen zur Authentisierung

ACL: Wie funktionieren Access Control Lists?



Exim 4 – ACL-Beispiel: Spam aussondern

ACL: Spam an eine spezielle Mailbox umleiten oder zurückweisen

```
# exim4.conf
...

 # Spam umleiten, wenn die Spam-Schwelle erreicht wurde ...

 warn  message = X-Redirect-To: SPAM_TRAP
       log_message = Message probably contains spam, redirected
       spam = nobody
       condition = ${if >{$spam_score_int}{SPAM_REDIRECT_THRESHOLD}{1}{0}}

 # ... oder stattdessen die Annahme verweigern

 deny  message = This message scored $spam_score spam points. Congratulations!
       log_message = Message denied, contains too much spam: $spam_score
       condition = ${if <{$message_size}{SPAM_SCAN_MSG_SIZE_MAX}{1}{0}}
       spam = nobody:true
       condition = ${if >{$spam_score_int}{SPAM_REJECT_THRESHOLD}{1}{0}}
```

Exim 4 –Router: Umleiten markierter Mails

Router: Infizierte Mails und/oder Spam umleiten

```
# exim4.conf
...
begin routers

# Dieser Router leitet Mails mit dem Header 'X-Redirekt-To' um.
# Dies ist i.d.R der erste Router in der Folge!

scan_redirect:
     driver = redirect
     condition = ${if def:h_X-Redirect-To: {1}{0}}

     # Wir merken uns sicherheithalber den urspruenglichen Empfaenger
     headers_add = X-Original-Recipient: $local_part@$domain

     # Den neuen Empfaenger holen wir aus den Header-Daten
     data = $h_X-Redirect-To:

     # Diesen Eintrag brauchen wir jetzt nicht mehr.
     headers_remove = X-Redirect-To

     # Das ist der Router, der als naechstes an der Reihe ist.
     redirect_router = my_next_router
```

Router/Transport: Cyrus

```
begin routers
...
# Cyrus router fuer lokale Postfaecher

local_user_cyrus:
    driver = accept
    check_local_user
    transport = cyrus_delivery
...
```

```
begin transports
...
# Cyrus via LMTP beliefern

cyrus_delivery:
    driver = lmtp
    socket = /var/run/cyrus/socket/lmtp
    batch_max = 20
    user = mail

...
```

Was ist Cyrus?

- Cyrus ist ein IMAP/POP3-Server (Daemon)
- Verwaltet Postfächer in einer Datenbank (Berkley-DB)
- Mails sind in einem Verzeichnisbaum in Form einzelner Dateien abgelegt.
- Authentisierung der Benutzer kann mit verschiedenen Mechanismen erfolgen, u.a. PAM, SASL, eigene Benutzerdatenank, SQL, LDAP
- Eigene Filtersprache (Sieve) ist integriert

SquirrelMail, wozu ist das gut?

- SquirrelMail ist ein IMAP/POP3-Client mit HTTP-Bedienoberfläche ("Webmailer")
- In PHP geschrieben, braucht neben PHP einen HTTP-Server (z.B. Apache)
- Es gibt zahlreiche Plugins für SquirrelMail
- Interessantes Plugin für unsere Zwecke: Avelsieve
  Damit lassen sich auf sehr einfache Weise Filterregeln für Cyrus-Sieve "zusammenklicken". Ist auch für Sieve-Unkundige einfach bedienbar.
- Ist für unsere Zwecke kein Muss aber sehr praktisch, z.B. wenn man auch von "irgendwo" auf seine Mailbox zu Hause zugreifen möchte.

Was macht SpamAssassin?

- SpamAssassin (SA) bewertet Mails nach bestimmten Regeln (reguläre Ausdrücke) und Blacklists.
- Die Regeln lassen sich ändern bzw. ergänzen.
- Eigene Black/Whitelists können hinzugefügt werden.
- Optional werden auch Online-Datenbanken, die Blacklists anbieten, abgefragt.
- SA ist "lernfähig": kann mit guten (Ham) und schlechten (Spam) Mails trainiert werden.
- Man kann User-Spezifische SA-Profile verwenden, man kann aber auch ein systemweit gültige Konfiguration einsetzen.
- SA filtert nicht, sondern bewertet nur. Die Bewertung wird in den Mail-Header geschrieben.

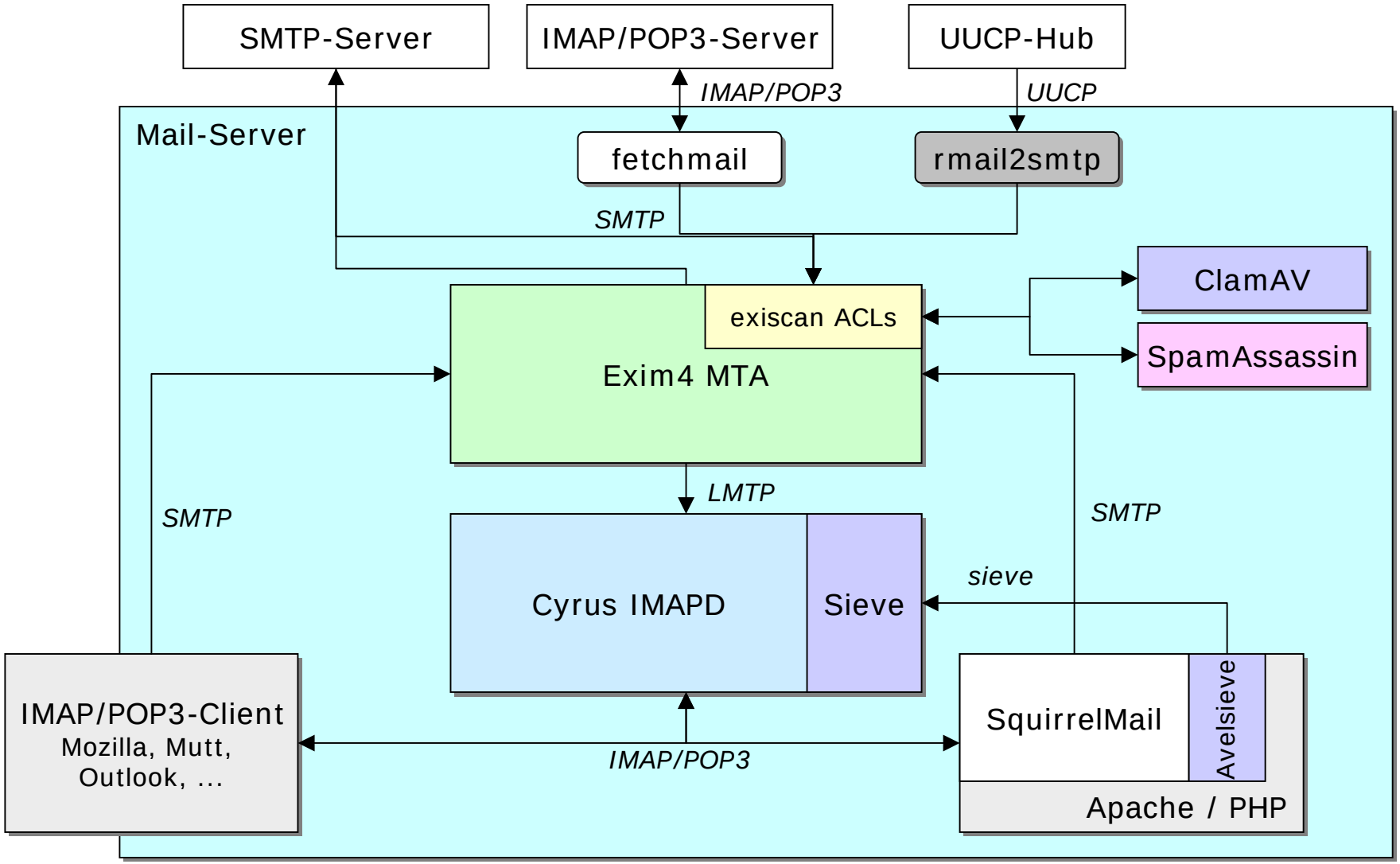
Header-Einträge einer als Spam klassifizierte Mail

```
X-Spam-Score: 15.8 (+++++++++++++++)
X-Spam-Level: 158
X-Spam-Report: Spam detection software, running on the system "cebulon.franken.de", has
      identified this incoming email as possible spam.  The original message
      has been attached to this so you can view it (if it isn't spam) or block
      similar future email.  If you have any questions, see
      the administrator of that system for details.
      Content preview:  This marketing message was delivered to you on behalf
      of Ascentive by BlueStream Media E-mail Marketing Division. [...]
      Content analysis details:   (15.8 points, 5.0 required)
      pts rule name              description
      ---- ---------------------- --------------------------------------------------
      5.4 BAYES_99               BODY: Bayesian spam probability is 99 to 100%
      [score: 1.0000]
      0.1 HTML_MESSAGE           BODY: HTML included in message
      2.0 WLS_URI_OPT_716        URI: URI contains sites starting with l
      2.0 WLS_URI_OPT_202        URI: URI contains sites starting with b
      3.0 BigEvilList_979        URI: Generated BigEvilList_979
      1.0 RCVD_IN_NJABL_SPAM     RBL: NJABL: sender is confirmed spam source
      [208.184.55.48 listed in combined.njabl.org]
      1.5 RCVD_IN_BL_SPAMCOP_NET RBL: Received via a relay in bl.spamcop.net
      [Blocked - see <http://www.spamcop.net/bl.shtml?208.184.55.48>]
      0.9 RCVD_IN_SBL            RBL: Received via a relay in Spamhaus SBL
      [208.184.55.48 listed in sbl-xbl.spamhaus.org]
X-Spam-Flag: YES
```

ClamAV – ein Viren-Scanner

- ClamAV ist einer der wenigen freien AV-Scanner.
- Regelmäßig gepflegte Virensignaturen stehen online zur Verfügung. (automatische Updates möglich)
- Stabil und zuverlässig (nach meiner Erfahrung).
- Sehr einfach an Exim "anzuschließen" (mit Hilfe der exiscan-Erweiterung)

Wie geht alles zusammen?



Ein paar selbstgemachte Helferlein

- rmail2smtp
  Sendet Mails, die per UUCP von einem Feed bezogen werden, per SMTP an den MTA. Ersetzt rmail, das Mails per Pipe an den MTA (Exim) übergibt und damit exiscan und einige nützliche ACLs umgeht. Verhindert Bounces bei unzustellbaren Mails.

- cyrus-mbox
  Damit kann man Mailboxen nach einem konfigurierbaren Schema (inkl. Subfolder) und Quotas erzeugen, löschen und ändern.

- sa-learn-cyrus
  Trainer für Spamassassin, auf die Cyrus-Mailbox-Struktur zugeschnitten. Verfüttert, die von den Usern als Spam/Ham eingestuften Mails an die SA-Datenbank.

Ein paar Hinweise zum Schluss

- **Zugriffskonflikte** - Beim Zusammenspiel von ClamAV und SpamAssassin mit Exim kann es je nach den Konventionen des Basissystems zu Permission-Problemen. Der konfliktfreie Zugriff auf Spool-Files ist manchmal nicht ganz einfach zu regeln.

- **Filter-Profile** - Bei Home- und Workgroup-Servern sollte man auf user-spezifische Filter-Profile verzichten. Das ist relativ aufwendig zu warten.

- **LDAP** - Authentisierung über LDAP klingt für ein kleines Netz zwar übertrieben, hat aber selbst da seine Vorteile (größter Vorteil :"ein Konto für alles"). Es gibt mittlerweile sehr komfortable Administrationswerkzeuge dafür. Das ist also nicht nur im Zusammenhang Mail-Service eine Überlegung wert.

- Die hier genannten, selbstgemachten **Helferlein** sowie ein paar weiter Details kann man hier bekommen: *http://www.pollux.franken.de/hjb/mail-server/*

Referenzen

"The Exim Home Page", *http://www.exim.org/*

"Exim FAQ", *http://www.exim.org/exim-html-4.40/doc/html/FAQ.html*

"The Exim SMTP Mail Server", Philip Hazel, UIT Cambrige, ISBN 0-9544529-0-9

"exiscan - An email content scanner patch for the exim MTA", *http://duncanthrax.net/exiscan-acl/*

"Cyrus IMAP Server", *http://asg.web.cmu.edu/cyrus/imapd/*

"SquirrelMail", *http://www.squirrelmail.org/*

"Avelsieve", *http://www.squirrelmail.org/plugin_view.php?id=73*

"The Apache SpamAssassin Project", *http://spamassassin.apache.org/*

"Clam AntiVirus", *http://www.clamav.net/*

Material zu dieser Präsentation: *http://www.pollux.franken.de/hjb/mail-server/*