RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

# Konzeption und Umbau der Mail-Infrastruktur der Universität Mannheim

Dr. Heinz Kredel, Matthias Merz, Marko Krüger
mit
Manfred Schreckenberger, Dr. Werner Aufsattler, Tillmann Bahls, Peter Mühlenpford, David Reinig, Helmut Fränznik, Rudi Müller, Andreas Baust, Markus Krämer, Sebastien Kreuter, Steffen Hau und andere

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

# Inhalt

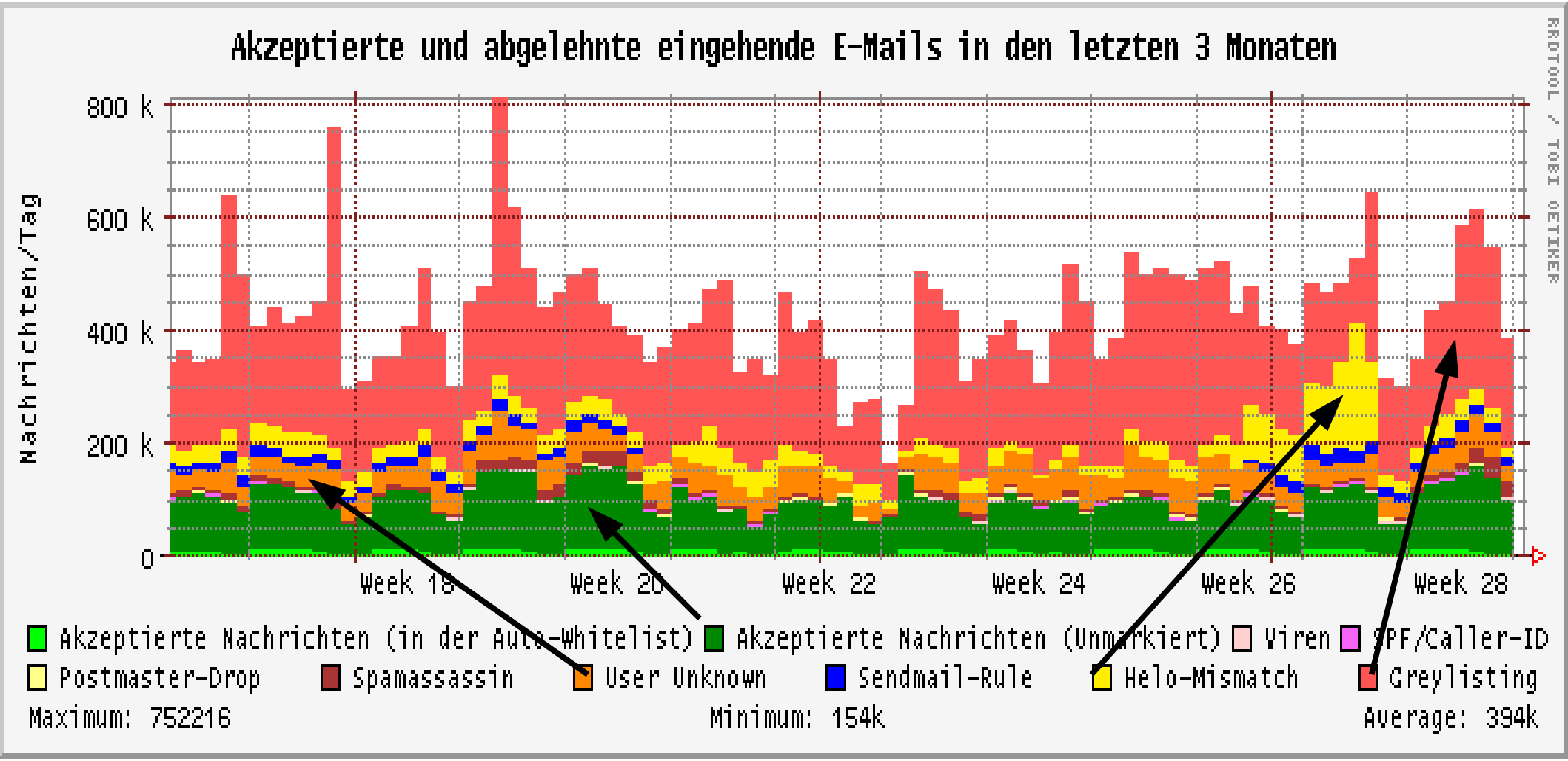
- Konzept, Ziele, Umsetzung und Historie
- LDAP, Horde und Migration
- Benutzerprobleme

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

# Stand

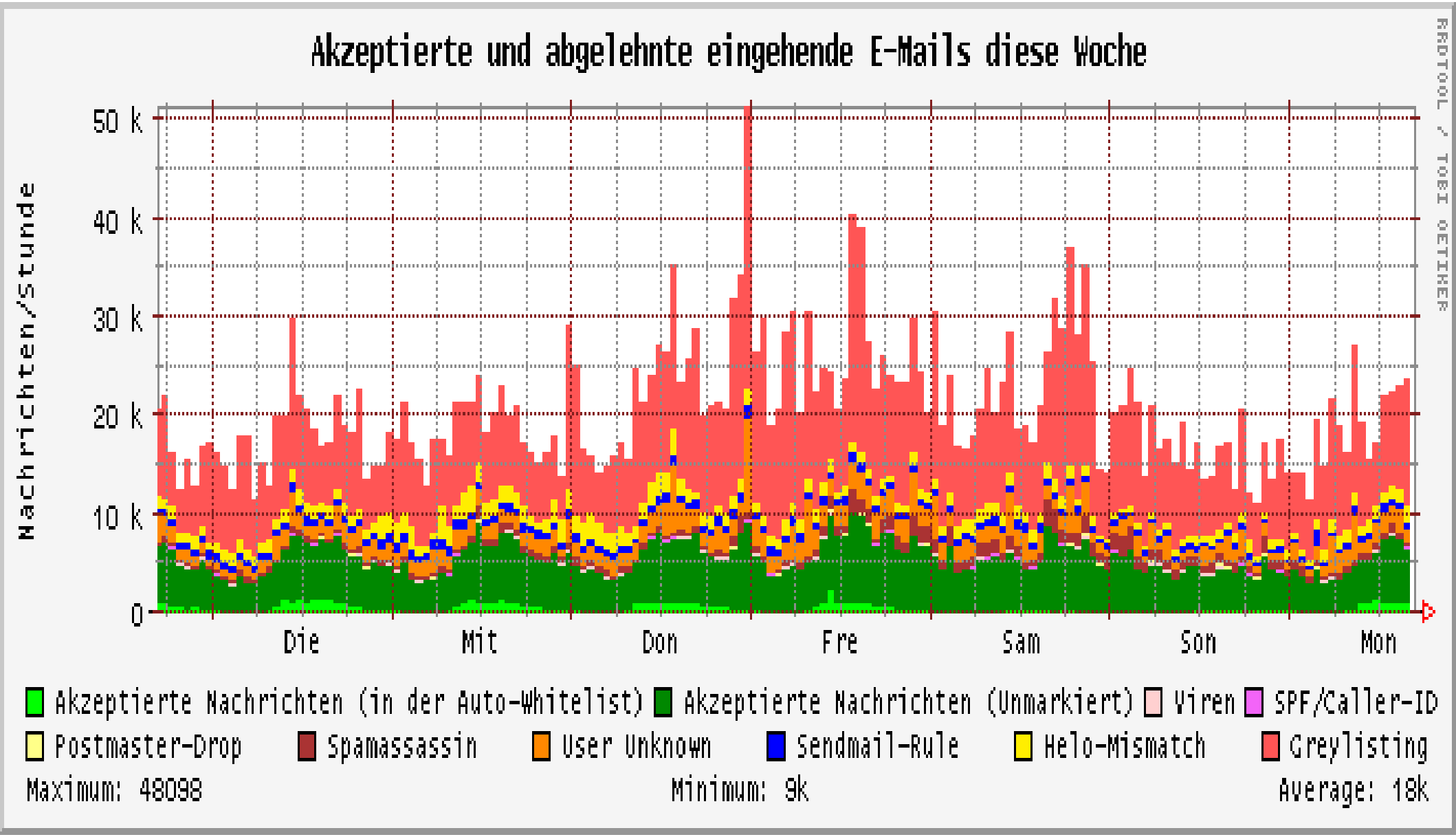
- Situation im Mailbereich seit einigen Jahren
  - spam > 95%
  - viruses
  - phishing
  - ham < 5%
- folgende Folien zeigen die Struktur des Mailaufkommens in 2005 an der Uni Heidelberg

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

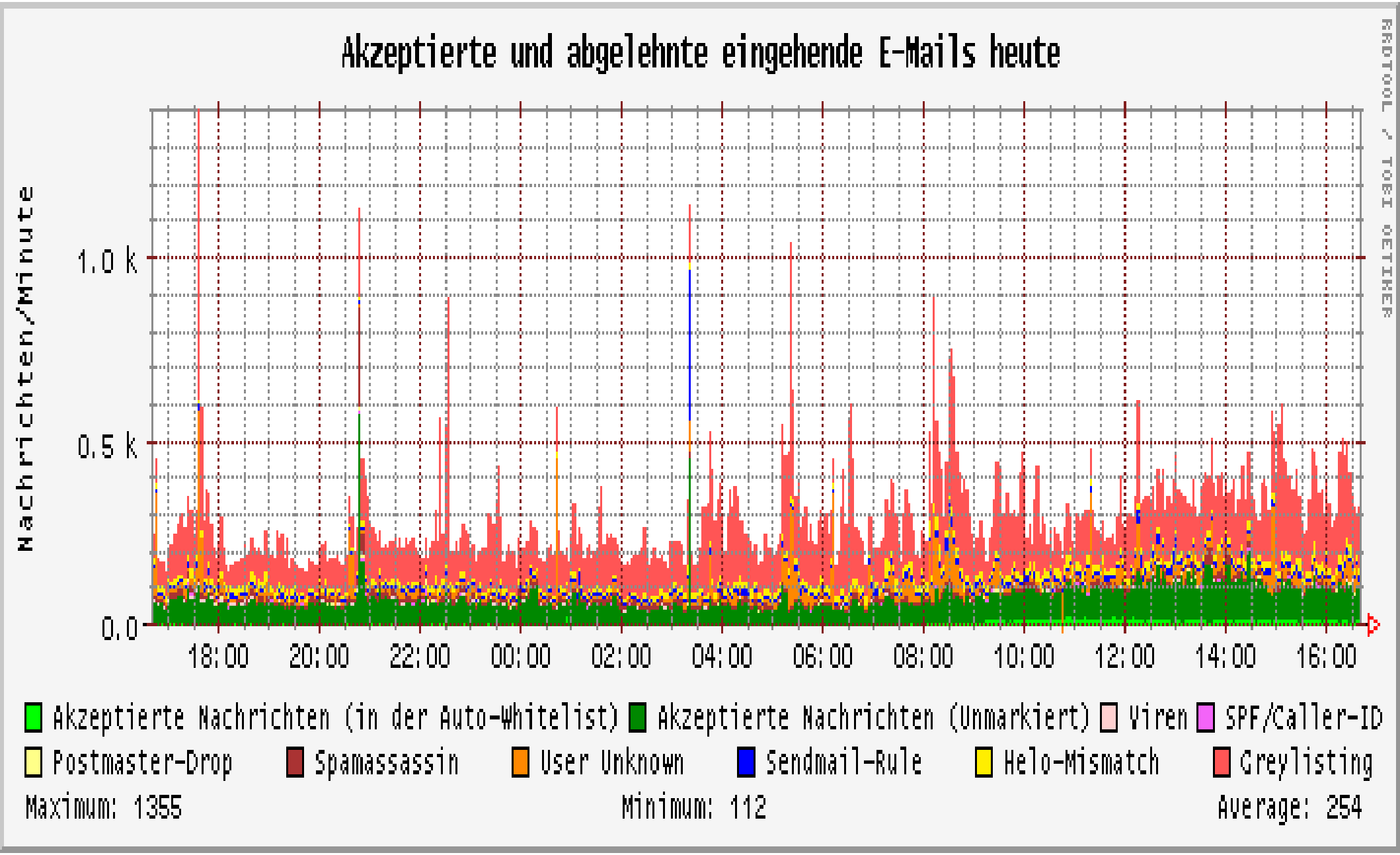



from University of Heidelberg

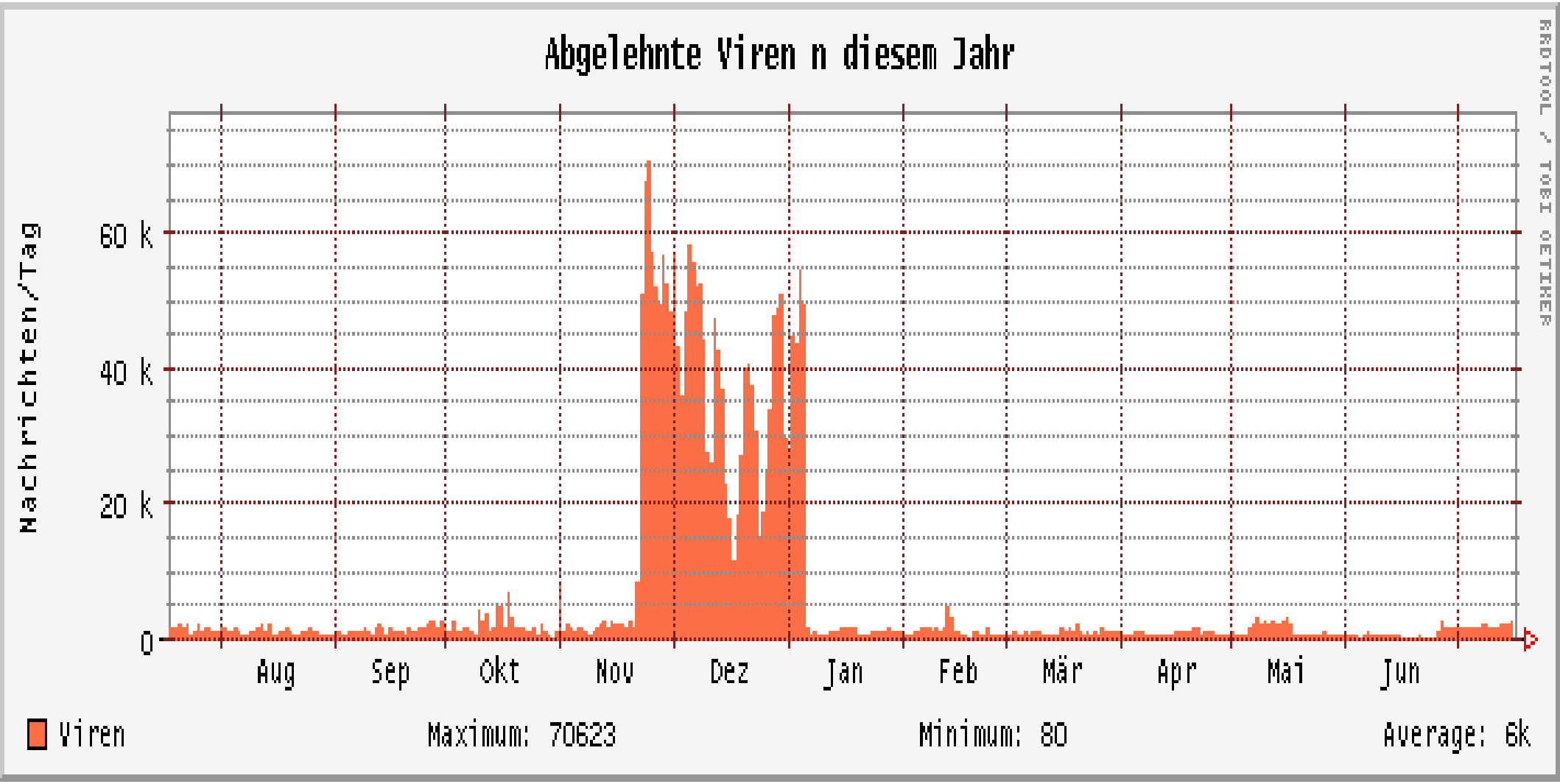
RECHENZENTRUM der
UNIVERSITÄT MANNHEIM



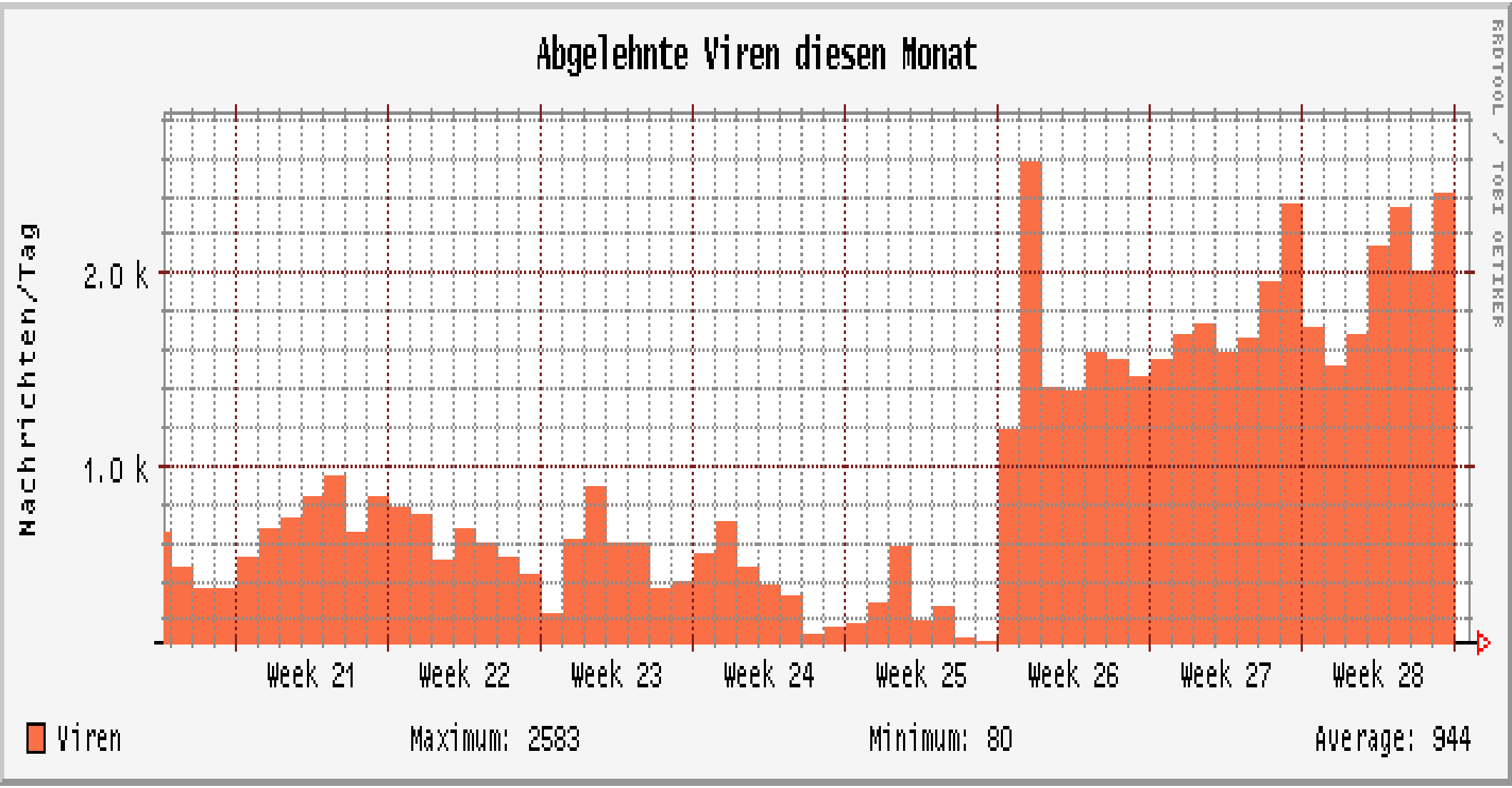
RECHENZENTRUM der
UNIVERSITÄT MANNHEIM



RECHENZENTRUM der
UNIVERSITÄT MANNHEIM



RECHENZENTRUM der
UNIVERSITÄT MANNHEIM



RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

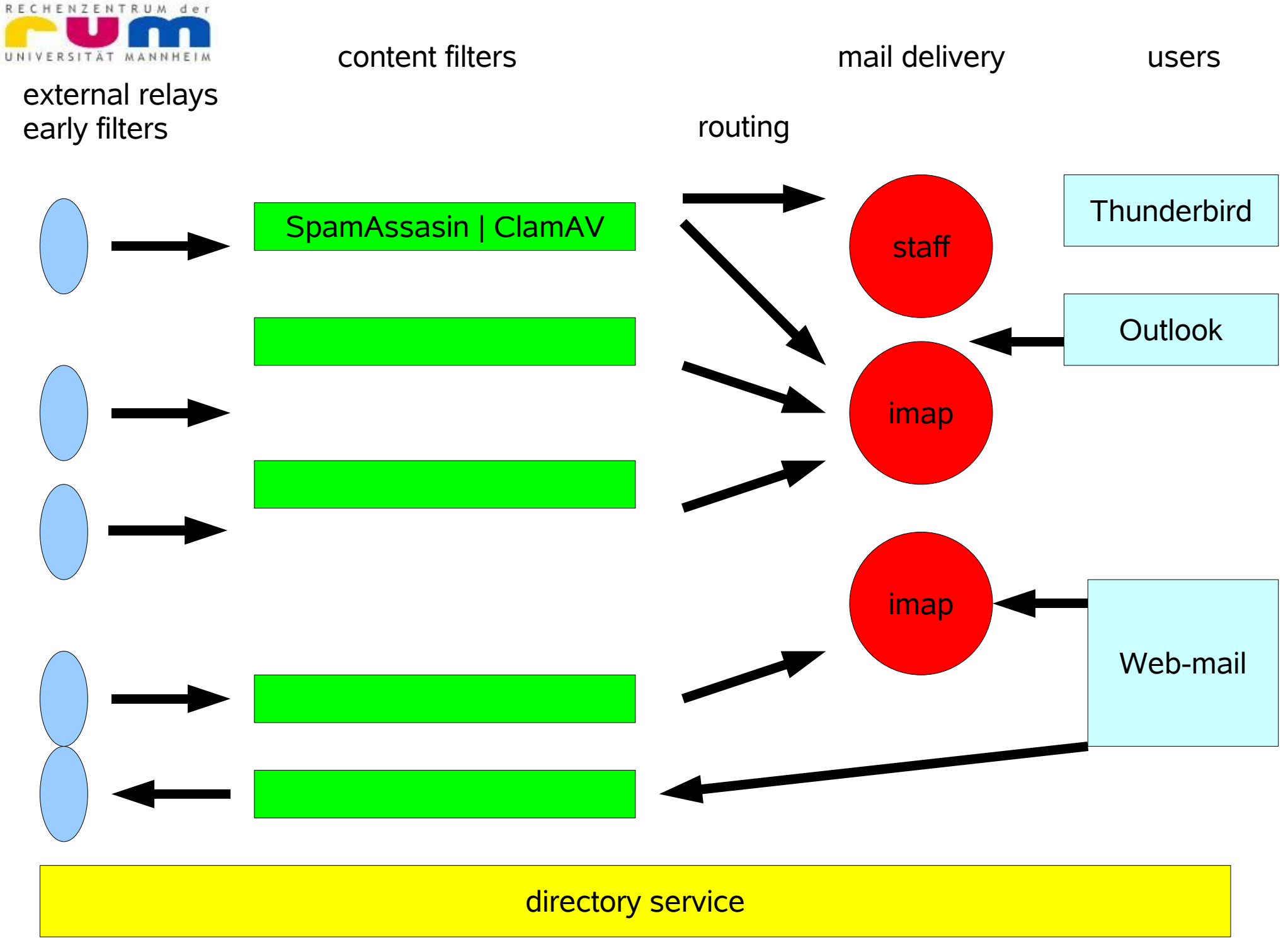
# Evaluation

- unvorhersehbare Peeks
  - up to 800k per day
  - up to 50k per hour
  - up to 1500 per minute
- unvorhersehbare Last und wirksame Gegenmaßnahmen
  - greylisting
  - helo missmatch
  - user unknown
- Virus Wellen über Wochen

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

# Entwurf einer Lösung

- folglich brauchen wir eine flexible und skalierbare Mail-Infrastruktur als Lösung
- Standard PC Hardware x86_64
- auf Standard Linux Betriebssystem
- basierend auf Open Source Email Software


RECHENZENTRUM der
UNIVERSITÄT MANNHEIM
content filters
mail delivery
users
external relays
early filters
routing
SpamAssasin | ClamAV
staff
Thunderbird
Outlook
imap
imap
Web-mail
directory service

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

# External relays

- SMTP relay to mailboxes from world wide
- Postfix mailer software
- early Spam detection and blocking
  - user existence check, DNS existance checks
  - RFC conformance checks
  - greylisting (later)
- load balanceing using MX records and packet filter
- separate relay for own external users via SASL and SSL/TLS

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

# Content filter farm

- based on amavisd-new framework
- SpamAssassin spam filter
  - bayesian filters
  - regular expressions
  - RFC conformance
  - Razor distributed spam detection
- ClamAV virus checker or others
- etc.

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

# Mail delivery to mailboxes

- Cyrus IMAP software
  - no unix accounts
  - one file per email
- SASL authentication and OpenSSL security
- Sieve filters, user configurable
- Horde Webmail with SSL/TLS
- no POP3  (?, yes)
- mailbox server for different user groups
  - students, personal
  - professors, administration

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

# Directory service

- OpenLDAP software
- based on inetOrgPerson schema
- additional attributes for mail system
  - mail delivery host
  - alias resolution, generic addresses
  - routing through filter farm
  - relay domains
  - virtual domains
- user information from ADMD and Benutzer DB

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

# Hardware

- flexible assignment of hardware to mail software components
- uses cluster filesystems in Hitachi FC storage system
- flexible, dynamic configurable,  grouping of related pipeline steps
- possible virtualization on blade systems

RECHENZENTRUM der
rum
UNIVERSITÄT MANNHEIM

# Vor- und Nachteile

- komplizierter als ein einziges System wie rumms
- Routing der Mails ist schwieriger
- aber flexibler
- und skalierbar
- Kosten können besser mit dem Bedarf skalieren

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

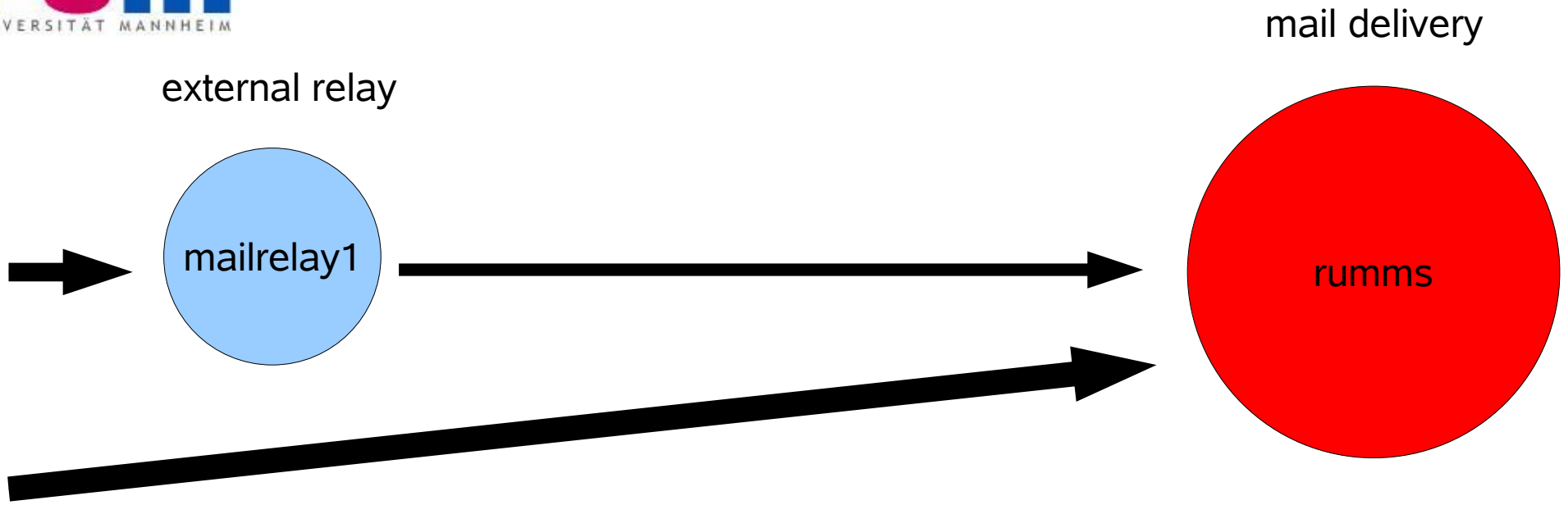
# zu lösende Probleme

- LDAP muss entworfen, aufgebaut und angebunden werden
- Zuordnung zu Mailbox Rechner muss definiert werden
  - z.B. per Fakultät, Sudenten, Mitarbeiter, Verwaltung
- verschiedene Software lernen
  - Postfix
  - Cyrus IMAP und POP, MS Exchange
- Anbindung an Storage-System

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

# Historie Mai/Juni

- Probleme
  - verzögerter Mailtransport
  - sehr grosse Mailboxe, bis 1-2GB, viele bei 300MB
  - Engpass Disk IO auf rumms
- Massnahmen
  - Reduktion der Grössen der Mailboxen und der Spamblock Ordner
  - neuer Mailserver (MDA) für Professoren




rumms: 1,0 M mail connections per day, 2,8 GB transfer

mailrelay1: 95 k mail connections per day, 1,2 GB transfer

rumms: 600GB in mail boxes, one file per folder, 200MB, upto 1 GB per folder

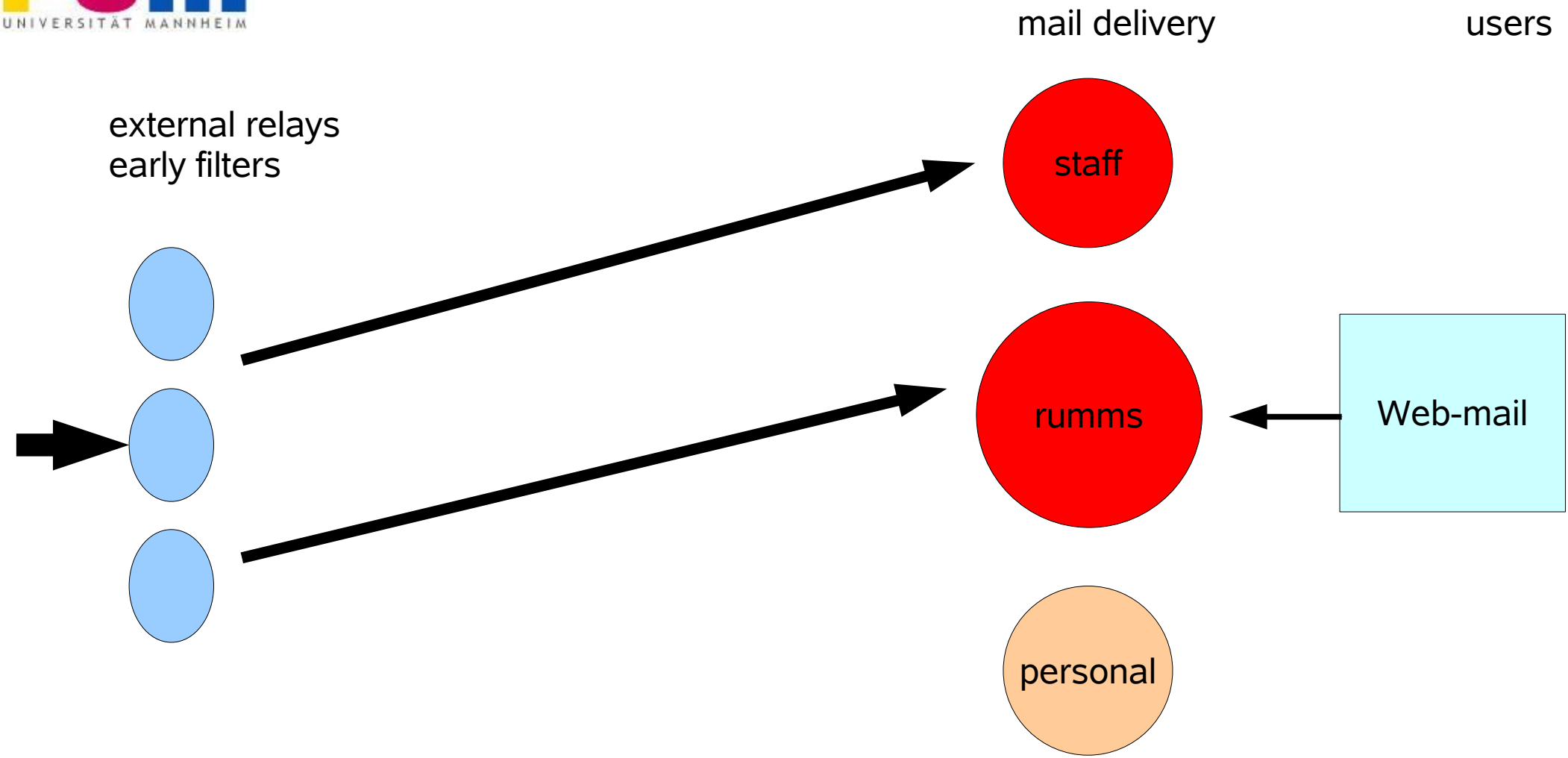
in May 2006

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

# Historie Juli/August

- Massnahmen
  - neuer Webmailer um die Last auf mailrelay1 zu reduzieren
  - Reduktion der Transport Delays auf mailrelay1
  - Migration der Professoren zum neuen Mailserver

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM



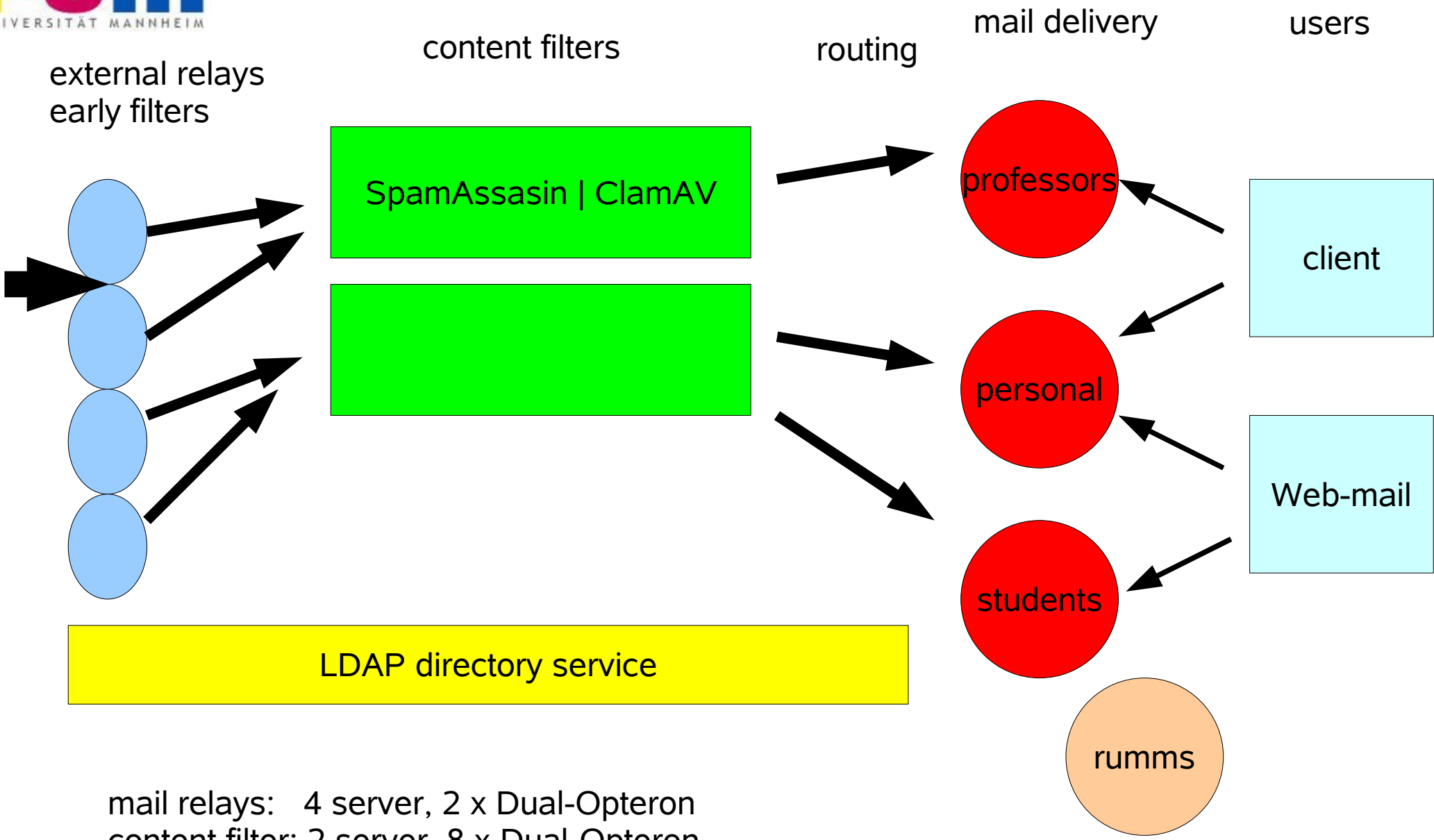

rumms: 0 external connections, 400.000 requests
mailrelay1: 130.000 connections, 1,9 GB transfer
mailrelay2: 400.000 connections, 1,3 GB transfer, to rumms 10%, 80% Spam
mailrelay3: 230.000 connections, 0.4 GB transfer, to rumms 10%

In October 2006

RECHENZENTRUM der UNIVERSITÄT MANNHEIM

# Historie September/Oktober

- Probleme
  - Beginn der Vorlesungen im Herbstsemester
  - lange Transport Delays am Tage zwischen 10.00 und 18.00 Uhr
  - CPU Überlast auf rumms
- Massnahmen
  - Migration der Benutzer zum neuen Webmailer
  - Last auf mailrelay1 deutlich reduziert
  - neue Relay-Hosts vor rumms geschaltet
  - Transport Delays auf ein erträgliches Mass reduziert




mail relays: 4 server, 2 x Dual-Opteron
content filter: 2 server, 8 x Dual-Opteron
mail delivery: 3 server, 4 x Dual-Opteron, connection to storage system
LDAP dir: 1 server, 4 x Dual-Opteron

Target January 2007

# scalable und flexible mail infrastructure

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

# Aufgaben im Oktober

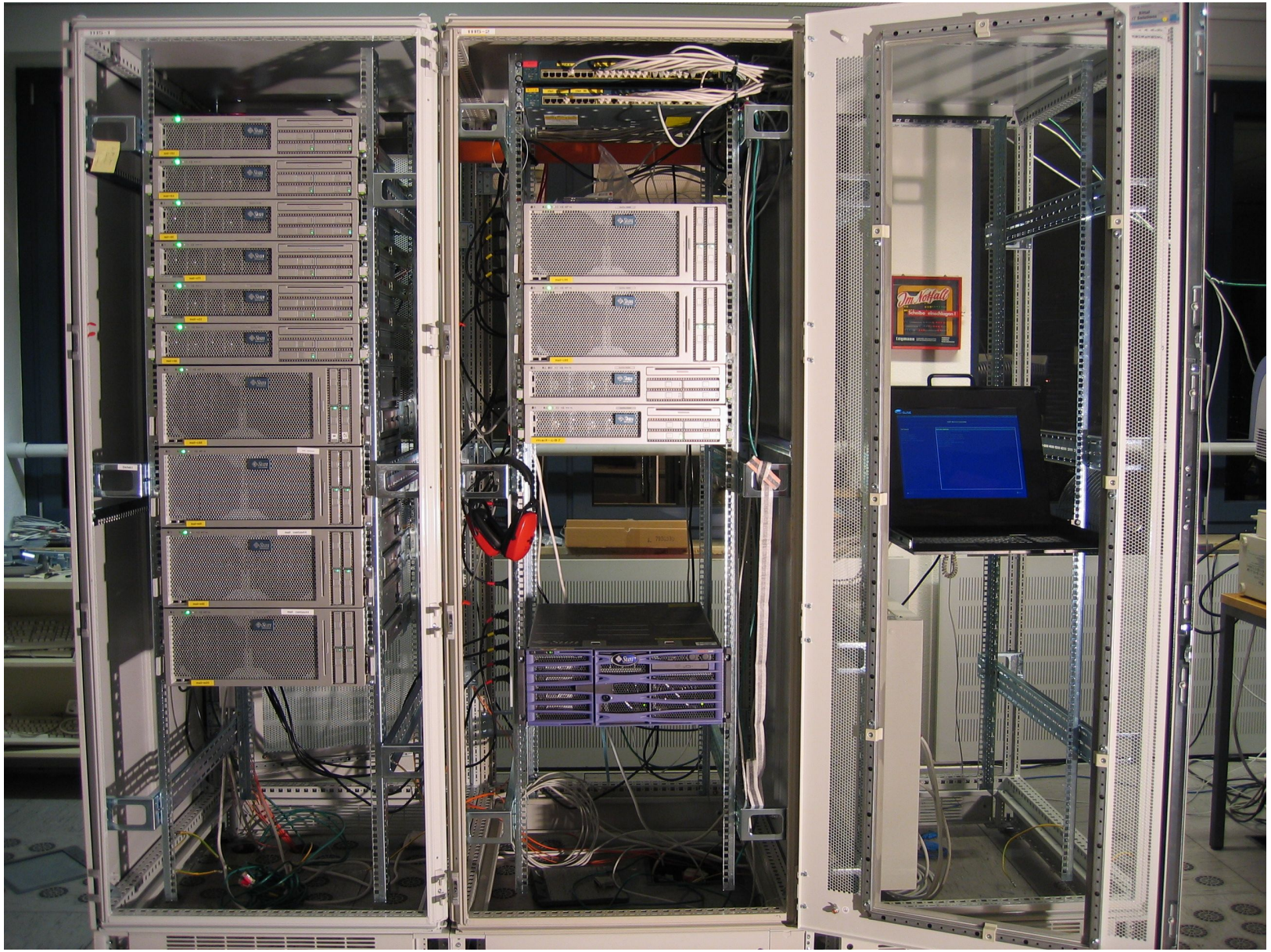
- Ende September ist die Hälfte des Gelds aus dem HBFG eingetroffen
- Spezifikation und Bestellung der neuen Hardware
- Ankunft der Server, Gehäuse, usw. Ende Oktober

RECHENZENTRUM der
rum
UNIVERSITÄT MANNHEIM

# rumms

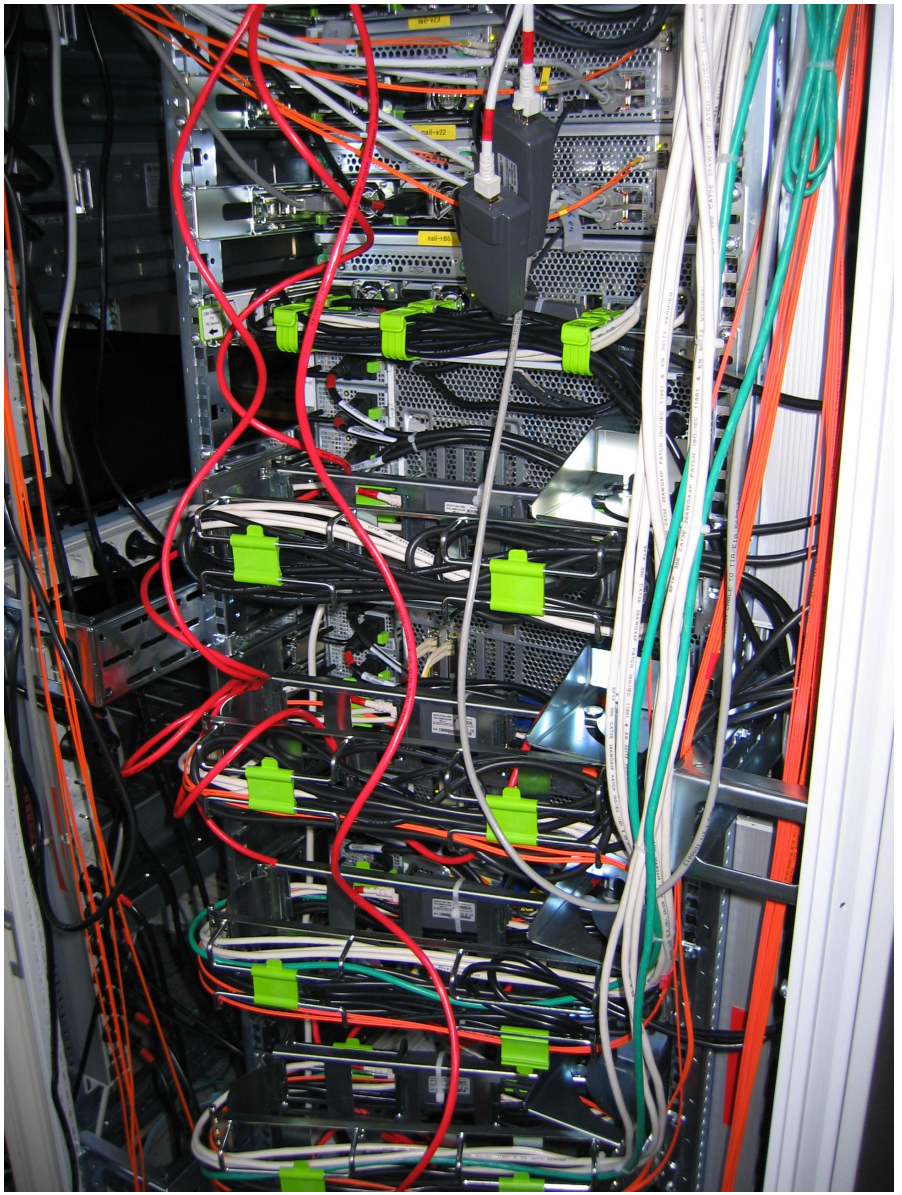
RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

# neue Hardware



RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

# Storage und Netz

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

# Aufgaben im November

- Installation der neuen Hardware
- Notstrom Anschluss
- Verbindung zum Storage-System via FC
- Installation von Linux OS
  - relay and content filter: SuSE
  - mail delivery: CentOS (RedHat)
- Konfiguration von vollwertigen Mail Relays
- Entwicklung der Web-Seiten zur Benutzerinformation, Testen der Clients mit den neuen Servern

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

# Aufgaben im Dezember

- Setup des Directory Service
  - OpenLDAP Verbindung zur RUM Benutzerverwaltung und ADMD
  - Mail Routing und Mailboxen
- Verbindung der Mailservices zum LDAP
- Konfiguration der Mailboxen
- Start der Tests der neuen Infrastruktur
- Aktivierung der Mail Relays und Tests
- Test Mailboxen und Mail Routing
- Entwicklung der Web-Seiten

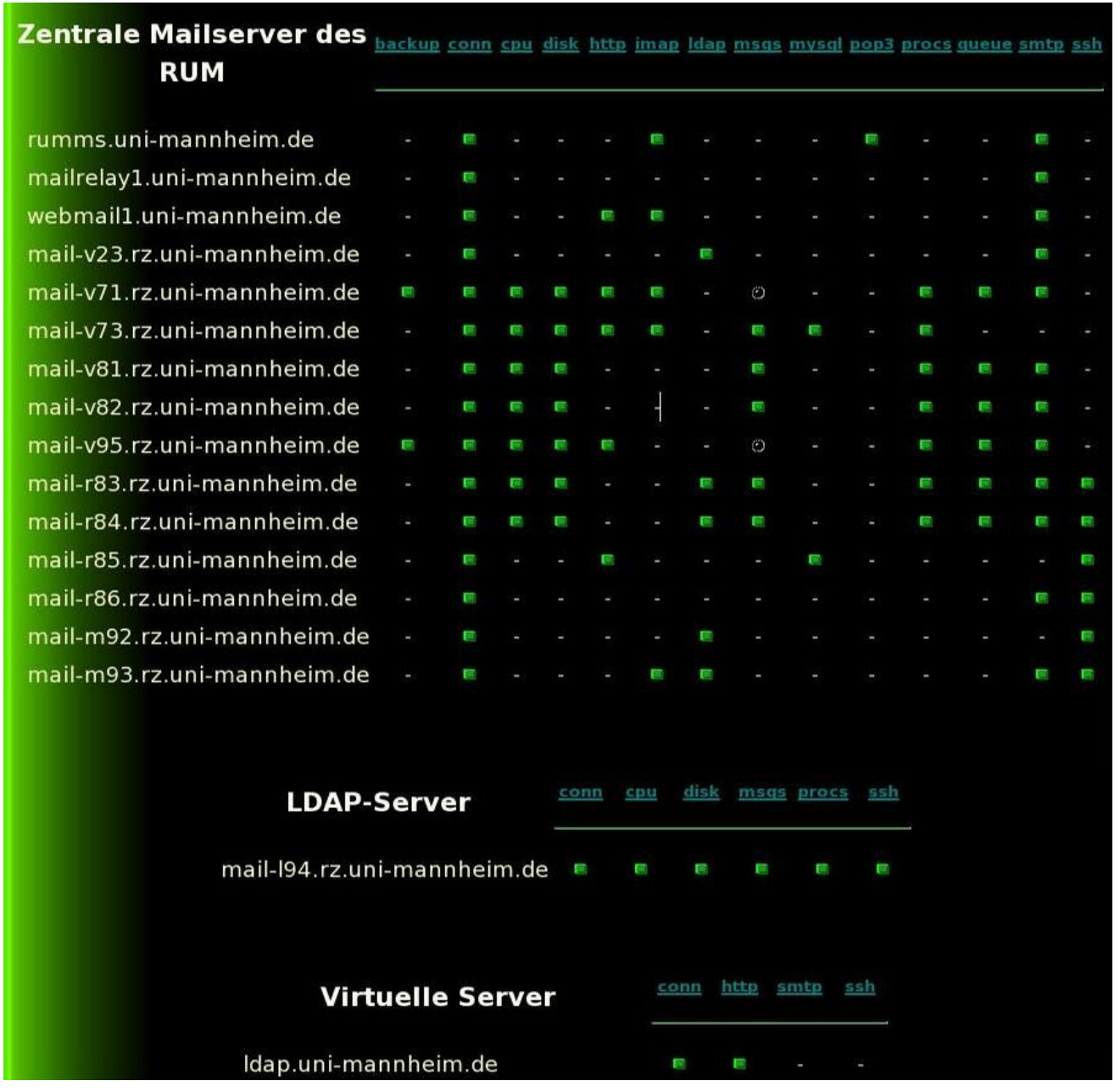
RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

# Aufgaben im Januar 2007

- Reduktion der Last auf mailrelay1
- Freischalten der Information und Empfehlungen im Web
- Aktivierung der Mailboxen
  - Öffnen der Mailserver für Benutzer
  - Schliessen der alten Mailboxen für neue Mail
- Freischalten des Migrations-Tools im Web
- Support für Benutzer beim Umzug

RECHENZENTRUM der UNIVERSITÄT MANNHEIM

# Stand Server Installationen



RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

# Aufgaben in 2007

- Umzug der Studierenden
- Support für Benutzer beim Umzug
- Bereithalten der alten Mailboxen als Archiv
- Shutdown des alten Systems Ende 2007, Anfang 2008
- Aufarbeiten aller Auslassungen
  - Schnittstelle zwischen ADMD, BenutzerDB und LDAP
  - Tivoli Backup
  - Spam Beobachtung und Anpassungen

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

# Anti-Spam Policy

- **alt**: Annahme fast aller Mails
- **neu**: Ablehnen von Allem was definitiv Spam ist
  - e.g. if sender domain is unknown
  - e.g. if no identification by a name server exists
  - e.g. if in spam blacklist
- **neu**: Spam-filter ist **eingeschaltet** per Default
  - spam index between 3 and 5 move to spam folder
  - delete if spam index >= 7 ???
  - clean spam folder automatically
- Nachjustierung der Parameter entsprechend dem Spamaufkommen

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

# Postfix

- Spam Block Konfiguration

```
smtpd_recipient_restrictions = permit_mynetworks,
        reject_invalid_hostname,
        reject_non_fqdn_sender,
        reject_non_fqdn_recipient,
        reject_unknown_sender_domain,
        reject_unknown_recipient_domain,
        reject_unauth_destination,
        reject_rbl_client list.dsbl.org,
        reject_rbl_client sbl.spamhaus.org,
        reject_rbl_client cbl.abuseat.org,
        reject_rbl_client dul.dnsbl.sorbs.net,
        reject_rbl_client zombie.dnsbl.sorbs.net,
        reject_rbl_client opm.blitzed.org,
        permit
```

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

# Amavis

- SpamAssassin und ClamAV

Mar 14 19:37:01 mail-r84 amavis[1878]: (01878-09) Blocked INFECTED (HTML.Phishing.Bank-1008), [71.248.119.122]
quarantine: virus-U0eycEdt-m6w, mail_id: U0eycEdt-m6w, Hits: -, 389 ms

Mar 14 19:37:19 mail-r84 amavis[312]: (00312-10) Passed SPAM, [64.183.173.191]
Hits: 28.858, 3101 ms

Mar 14 19:37:38 mail-r84 amavis[2581]: (02581-02) Passed CLEAN, [70.103.237.254]
Hits: -2.353, 3131 ms

X-Virus-Scanned: amavisd-new at uni-mannheim.de
X-Spam-Status: Yes, score=12.134 tagged_above=1 required=3
tests=[BAYES_99=3.5, FORGED_RCVD_HELO=0.135, HTML_MESSAGE=0.001,
RAZOR2_CF_RANGE_51_100=0.5, RAZOR2_CF_RANGE_E4_51_100=1.5,
RAZOR2_CF_RANGE_E8_51_100=1.5, RAZOR2_CHECK=0.5,
URIBL_SC_SURBL=4.498]
X-Spam-Score: 12.134
X-Spam-Level: **********
X-Spam-Flag: YES

RECHENZENTRUM der
UNIVERSITÄT MANNHEIM

# gleich geht’s weiter