Mailová brána na FJFI

Petr Vokáč

březen 2005

http://kmlinux.fjfi.cvut.cz/~vokac/activities/2005/mailgw/

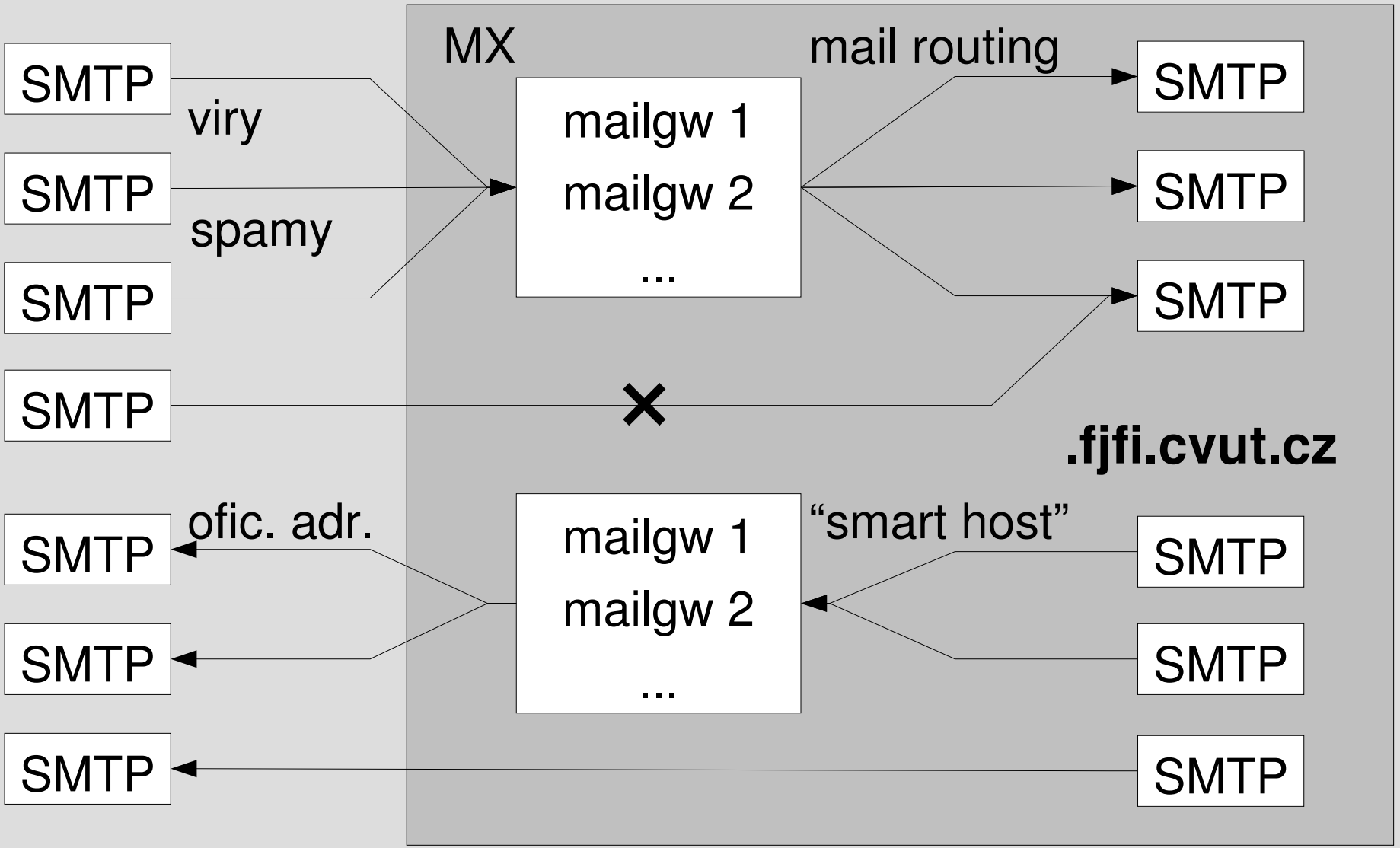
Obsah

- Příjem/odesílání mailů přes mailgw
  - základní vlastnosti
  - data flow
- Konfigurace
  - postfix, amavis (viry, spamy), openldap, DNS
  - konfigurace strojů “za” mailgw
- Hardware
  - analýza současného provozu

Vlastnosti mailové brány

- Všechny potřebné součásti duplikovány
  - stejná konfigurace (image, synchronizace)
  - standardně load-balancing
  - v případě nedostupnosti použit druhý stroj
- Umístění
  - zatím Trojanka, výhledově Trojanka + Břehovka
    - kvůli případnému výpadku konektivity
- Systém
  - linux – pořád nemám jasno v distribuci ($50 RHEL4)

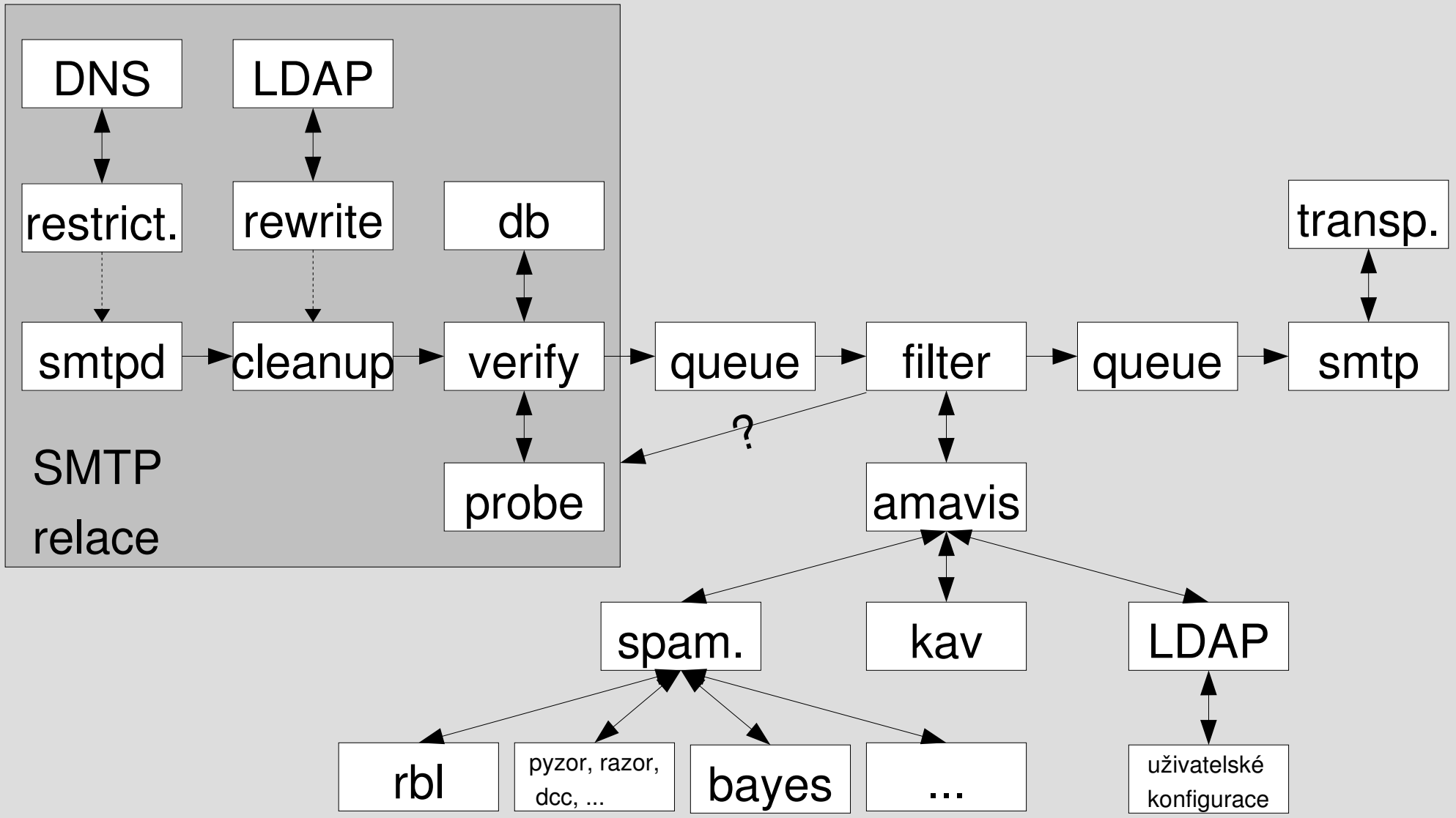
Příjem/odesílání mailů



Konfigurace mailové brány 1

- postfix
  - restrikce, verifikace
  - přepis na oficiální adresy (zdroj dat LDAP)
  - amavis (antivir, značkování spamu)
    - uživatelské nastavení
  - smtp auth?
  - konfigurace “za” mailgw (postfix, sendmail)
- openldap
  - synchronizace, přístupová práva, ...
- DNS

Konfigurace mailové brány 2



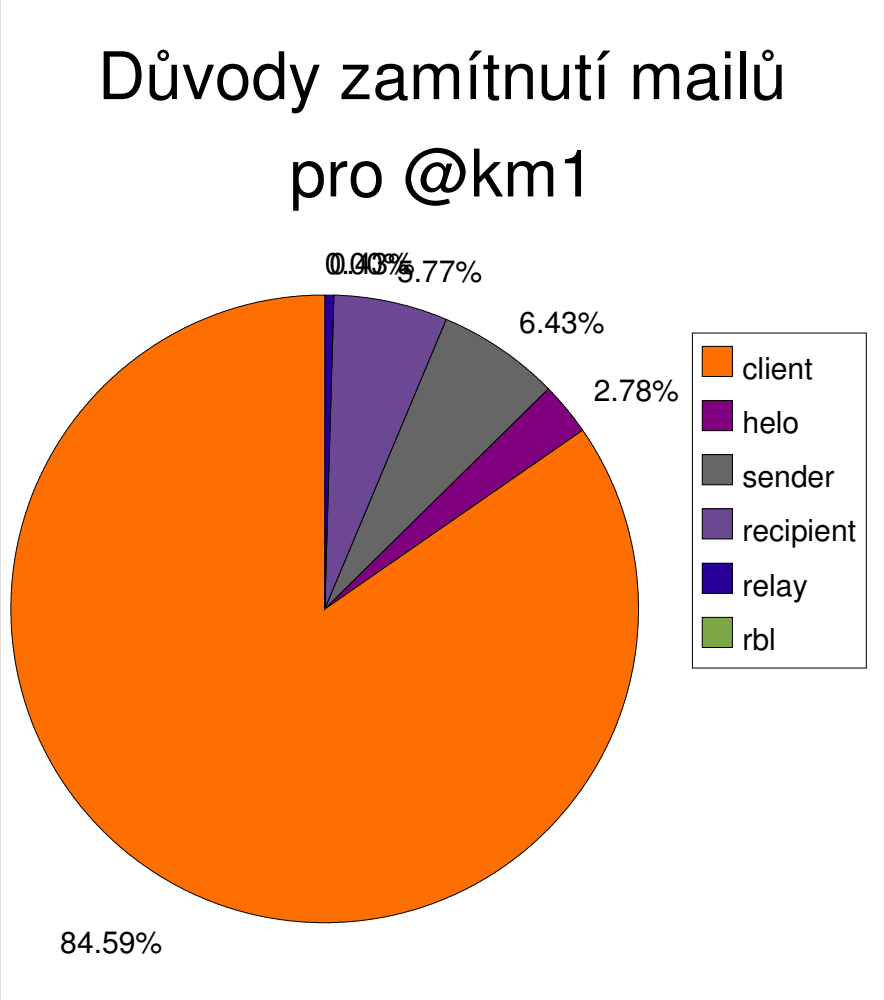
Postfix restrictions 1

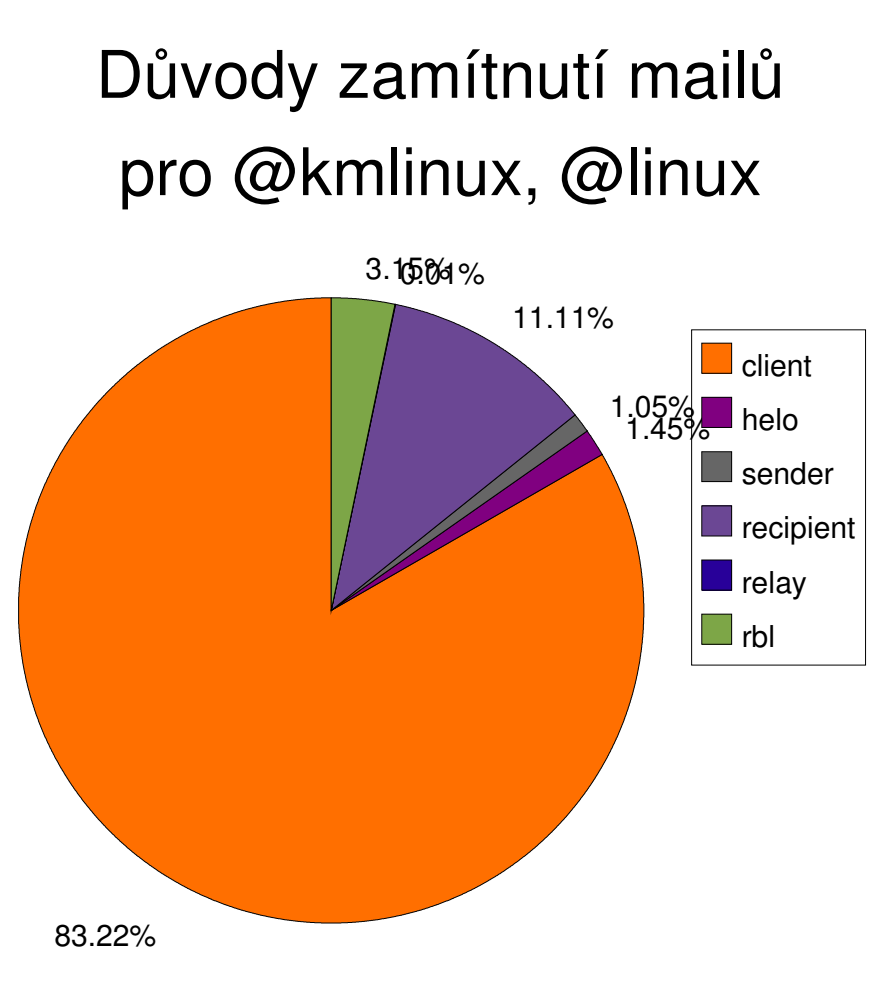
- client -> hello -> etrn -> sender -> recipient -> data
  - povoleno pro
    - .fjfi.cvut.cz
    - smtp auth?
  - přijato ke zpracování 60% @km1, 11% @kmlinux, @linux

```
220 mx1.fjfi.cvut.cz CTU FNSPE 1st MX
   ESMTP NO UCE
EHLO linux.fjfi.cvut.cz
250-mx1.fjfi.cvut.cz
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250 8BITMIME
MAIL FROM: <vokac@linux.fjfi.cvut.cz>
250 Ok
RCPT TO: <vokac@kmlinux.fjfi.cvut.cz>
250 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: <vokac@linux.fjfi.cvut.cz>
To: <vokac@kmlinux.fjfi.cvut.cz>
Subject: testovaci mail

telo mailu
.
250 Ok: queued as 13AC237620E7
```

Postfix restrictions 2





Postfix restrictions 3

- client
  - unknown client – addr->reverse->addr
    - ~15% se správnou adresou (z nich 1/3 špatné helo)
  - blacklisty – malá efektivita (většina zachyc. i jinak)
    - nebezpečné pro freemaily (seznam.cz, email.cz, ...)
    - využití pro obodování spamů
  - nekorekní záznamy v DNS
    - RFC1912 2.1 – Make sure your PTR and A records match. For every IP address, there should be a matching PTR record in the in-addr.arpa domain
    - vogelburda.cz (62.77.78.15), alzasoft.cz (80.250.15.11), ...
      - detekce špatně zkonfigurovaných mailserverů?

```
Mar 14 11:55:15 athena postfix/smtpd[7832]: NOQUEUE: reject: RCPT from unknown[80.250.15.11]:
450 Client host rejected: cannot find your hostname, [80.250.15.11]; from=<obchod@alzasoft.cz>
to=<jerie@linux.fjfi.cvut.cz> proto=ESMTP helo=<mail.dodax.cz>
```

Postfix restrictions 4

- helo – (fqdn, nekontroluje se – hromada nekorekt.)
  - fjfi.cvut.cz, ip, localhost
  - nnn.nnn.nnn, nnn-bbb-ccc, ip-bbb-ccc, host-bbb-ccc -> přidat ke client restrictions
- sender – kontrola existence domény
- recipient
  - verifycation (pouze pro .fjfi.cvut.cz)
    - canonical tables
- smtp auth
  - při současné konfiguraci nutný jiný stroj (technicky)
  - pozdržet do autentizace, RCPT TO? (špatní klienti)

Postfix přepis adres

- přepis “oficiálních” adres @fjfi, @br, @km1, @troja na Jmeno.Prijmeni@fjfi (případně username@fjfi)
  - při příjmu i odesílání mailů
    - uživatel nemusí nic měnit
  - mění se jen adresa (displayName zůstane původní)
  - možné problémy při přispívání do konferencí
  - adresy automaticky synchronizovány – viz. dále
    - možnost měnit cílovou adresu (www?)
    - není podporováno širší individuální nastavení
- ostatní adresy (+ routování) beze změny

Postfix parametry

- Maximální velikost přijímaných mailů
  - 50MB?
    - yahoo 32MB, gmail 20MB, hotmail 30MB, centrum 8MB, post 20MB, fnal 500MB, cern 10MB, cvut 50MB
- reject codes
  - unknown user 550
  - ostatní většinou 450
    - vysledovat, co je ještě možné/nutné zahazovat s 550
- hostname pro mailgw? (mailgw1 x mx1)
- další návrhy?

Amavis 1

- možnosti konfigurace
  - typy zpracování
    - spamy
      - hranice značkování, změny subjectu, zahazování
      - bounce message (content filter x smtp relace)
    - viry (antivir, backup, info mail)
    - filtrováni (dle přípon, “file”, MIME)
    - bad header
  - karanténa, přidané hlavičky, pro odchozí mimo fjfi?
  - individuální nastavení pro domény, uživatele
  - možnost kontroly mailů externím mailserverům

Amavis 2

- uživatelské konfigurace (dle mailRoutingAddress)
  - uloženy v LDAP (pouze změněné, pouze pro ofic.)
  - parametry
    - vir, spam, banned files, bad header
      - checks (on/off), lover, quarantine, warn recipient (exc. vir)
    - spam (tag, tag2, kill level, modify subject)
    - sender (blacklist, whitelist)
  - úpravy
    - vytvořit www rozhraní (authentizace?)
    - přímá úprava LDAP
  - pořád trochu zlobí

Antivir

- kav
  - kav for linux fileservers, daemon (backup stand.)
  - updatování každou hodinu
    - nové databáze ~ 4 hodiny
  - výpadky
    - stažení špatné databáze (stalo se 2x)
    - řešení
      - druhý antivir (např. clamav)
      - vlastní updatování kontrolující funkčnost
  - licence do 19.12.2005

Značkování spamu

- spamassassin
  - volán přes perl rozhraní přímo z amavisu
  - moduly – rbl, pyzor, razor, dcc, spf
  - bayes filtry
    - jak učit na mailgw?
- další možnosti
  - dspam
    - bayes filtr – jak učit?
    - napsané v c => rychlé (narozdíl od spamassassinu)

OpenLDAP

- dva stroje (ldap1.fjfi.cvut.cz, ldap2.fjfi.cvut.cz?)
  - pro bezproblemový běh stačí jeden (změny)
  - multimaster replikace
  - LDAP klienti automaticky komunikuji s dostupným
  - změny v informací v LDAP se projeví okamžitě
- data přebírána automaticky
  - Novell NDS + Windows AD + Usermap
- mapování adres na oficiální, uživatelské konfigurace, zdroj pro (LDAP) addressbook

OpenLDAP synchronizace 1

- zdroje dat
  - Windows AD, Novell NDS, OpenLDAP – zdroje účtů
    - doplnění informací (gan, jména)
  - Usermap – zdroj dalších (korektních) informací
- synchronizace – python skripty (komentované)
  - nutné aby běžela alespoň jedna mailgw LDAP
  - ostatní zdroje v při nedostupnosti z lokální cache
  - perioda synchronizace?, na vyžádání?
  - generování LDIF, přímé úpravy v LDAP – chyby?
  - korektnost závisí pouze na správných zdroj. datech

OpenLDAP synchronizace 2

- konflikty uživatelských jmen/adres
  - dlouhá adresa – Jmeno.Prijmeni@fjfi.cvut.cz
    - převzata z Windows AD
  - krátká adresa – username@fjfi.cvut.cz
    - pro každého (tj. včetně studentů)
    - na základně username
      - jednoznačnost (včetně údajů pro mail, mailLocalAddress)
        - AD, NDS, OpenLDAP
        - usermap
        - příjmení + první písmeno ze jména
        - příjmení + první písmeno ze jména + číslo

OpenLDAP synchronizace 3

- struktura synchronizovaných dat
  - plná synchronizace pro většinu položek mimo
    - mailRoutingAddress
      - jednorázový import na začátku
        - zahrnout novell přesměrování?
    - amavis*
  - skupiny
    - people – spojení přes GAN (korektní v NDS, AD, U?)
    - lists (groups) – bez spojování (jednoznačnost, AD)
    - special people – bez spojování (jednoznačnost, AD)
  - možnost prohlídnout LDAP browserem (přístup)

OpenLDAP přístup

- anonymní uživatel
  - lokální (vše krom rodného čísla)
  - vzdálený (pouze uid, cn, sn, givenName, mail)
- autentizovaný uživatel
  - vše krom rodného čísla
  - vlastní údaje včetně rodného čísla
- mail/amavis uživatel
  - pouze nezbytné údaje
    - uid, cn, mail, mailLocalAddress, mailRoutingAddress, amavis*

OpenLDAP authentizace

- není ještě implementováno
  - využití SMTP AUTH, eduroam, ...
  - bude nutné napsat vlastní pam modul
    - možnost ověřování proti zvolenému zdroji
      - LDAP, ale principielně cokoliv
      - prozatím NDS, AD, Usermap
      - postavit na pam_ldap + “pam_if”?
    - zápočet?
  - zkušenosti s cyrus-sasl ({SASL}username)
- dočasné řešení
  - vybrat jen jeden autentizační zdroj, který?

OpenLDAP addressbook

- podpora LDAP ve většině moderních klientů
  - OE, thunderbird, Pegasus Mail, pine, ...
  - uvedeny oficiální adresy
  - vyhledávání (cn, givenName, sn, mail, ...)
- anonymní přístup
  - atributy viz. přístupová práva
  - přístup pouze k “people”
- doména ldap.fjfi.cvut.cz?
- SRV záznamy v DNS?

Testování funkčnosti

- Statistiky pro mailové brány
  - bude přesunuto, nalinkováno z jednoho místa

    http://athena.fjfi.cvut.cz/admin/mailgraph/

    https://athena.fjfi.cvut.cz/admin/amavis-stats/

    http://nms.fjfi.cvut.cz/cgi-bin/mrtg-rrd.cgi/athena_load.html

    https://nms.fjfi.cvut.cz/admin/mailgraph/

    http://nms.fjfi.cvut.cz/admin/amavis-stats/

    http://nms.fjfi.cvut.cz/cgi-bin/mrtg-rrd.cgi/mail_load.html
- LDAP
  - ldapsearch případně libovolný LDAP browser
- log soubory
  - zpřístupnit? jak? logserver (secure – vpn)?

Lokální mailserver 1

- Příjem pošty jen z mailgw (nebo .fjfi.cvut.cz)
  - některé viry a spamy se rozesílají přímo
- Odesílání pošty přes mailgw (“smart host”)
  - zajistí pro vybrané domény automatické přepisování adresy na oficiální (@fjfi, @br, @km1, @troja)
  - pro ostatní není nutné
- Výhody – konfigurace, méně mailů
- Nevýhody – při výpadku sítě nelze posílat ani lokální maily tam kde není/nebude mailgw (Troja)

Lokální mailserver 2

- Na mailové bráně nutné
  - přidat nový stroj do transportních map
    - lze jinak?
    - “automaticky” pro všechny MXka?
  - v případě potřeby uživatelské konfigurace postfixu a amavisu
- Úpravy v DNS
  - přepsat MX záznamy
    - pro každou mailovou bránu
    - stejná priorita z důvodu load-balancingu

Lokální mailserver – postfix

- Změny vzhledem k základní konfiguraci na FC3

```
/etc/postfix/access
fjfi.cvut.cz   OK       # případně zde mohou být pouze Mxka
                        # (dle preferencí)

/etc/postfix/main.cf
inet_interfaces = all
mynetworks_style = host
relayhost = mailgw.fjfi.cvut.cz      # odesílání mailů přes mailgw
mailbox_command = /usr/bin/procmail
smtpd_delay_reject = no
smtpd_client_restrictions =          # zprac. pošty pro FJFI resp.
      permit_mynetworks              # z mailové brány
      check_client_access hash:/etc/postfix/access
      reject
```

- Vhodné zakázat na úrovni IP (iptables)
- Pomocí transport map lze lokálně posílat bez gw

Lokální mailserver – sendmail

- Změny vzhledem k základní konfiguraci na FC3
  - nevim jak se povoluje přístup z určitých strojů
    - FEATURE(relay_hosts_only)?

```
/etc/mail/sendmail.mc
define(`SMART_HOST',`mailgw.fjfi.cvut.cz')dnl odesílání přes mailgw
dnl DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')
```

- Vhodné zakázat na úrovni IP (iptables)

```
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport smtp
  -j REJECT
```

Hardwarové nároky 1

- dle provozu pro @kmlinux, @linux, @km1 v průběhu posledního měsíce
- nastavení odmítání mailů dle dříve uvedených pravidel
- největší žrout zdrojů amavis (resp. spamassassin)
- postfix, kav, OpenLDAP
  - zanedbatelné nároky (na slabším hw)
    - postfix – jak změřit? (PR – 3x rychl. než sendmail ;-)
    - kav ~ 2minuty/den
    - OpenLDAP ~ 20M indexovaných dotazů (/10)

Hardwarové nároky 2

- amavis
  - jedna instance ~ 40MB RAM
  - zpracování mailu (kav, spam, DNS, ...)
    - údaje pro jednoho daemona (běží jich 8)
      - 16s (500MHz, 640MB RAM, 5400RPM HDD, avg load <0.5)
        - ve špičce zracován ~ 1 mail/s
      - 4,5s (1600MHz, 512MB RAM, 7200RPM HDD, load <0.2)
        - zatím maximální zátěž ~ 2 maily/s (není maximum)
  - ~ 10000 kontrolovaných mailů/den pro @km1, @kmlinux, @linux => na zprac. cca 8s
  - předpokládaný počet mailů pro ostatní adresy?

Plány do budoucna

- přehodit na oficiální železo
  - koordinace s recyklací/novými windows servery
  - časový plán realizace?
- vyřešit “?”
  - uživatelské konfigurace (www)
  - autentizace SMTP
- VLAN + serverový segment
- někdo dalšího, kdo se o to bude umět postarat
- kam směrovat postmaster@fjfi, abuse@fjfi, ...