Szerver üzemeltetés a Szent István Egyetemen

Lajber Zoltán

lajber.zoltan@ih.szie.hu

Szent István Egyetem Informatikai Hivatal

- Az egyetemi hálózat
- Hálózat és szerver felügyeleti segédprogramok
- Elektronikus levelezés szolgáltatás, mail gateway
- A storage

Az előadás letölthető: http://zeus.gau.hu/~lajbi/hbonetabor.pdf

Szervezti felépítés

- központi informatikai ”hivatal”: 6 mérnök, 3 technikus + telefonosok
- karok önálló szervezetek, saját rendszergazdák
- bevétel csak karoknál keletkezik, ”fizetnek” a szolgáltatásokért
- nincs közvetlen kontrolunk az oktatói gépek fölött
- semilyen kontrol nincs a hallgatók kollégiumi gépei fölött
- központi részlegek gépeit felügyeljük
- HBONE AUP

Központi szolgáltatások

- forgalom szűrés $\Rightarrow$”tűzfal”
- DNS - 12db C osztályú cím Gödöllőn
- SMTP gateway - kb 50 SMTP kiszolgáló, 1500 oktató
- lev. lista szolgáltatás - mailman
- web: virtualhost-ok - uml, adatbázis, php.
- címtár: HBONE cimtár szolgáltatás, Sun One LDAP szerver (iPlanet), 20 000 entry
- mail: Sun One Messenger webes és IMAP elérhetőség
- pénzügy: TüSZ: 2 netware, 4 win TS + Citrix
- tanulmányi rendszer: Neptun: 2 Oracle db, 6 win TS
- 4 nagyobb, sok kis telephely - karok önálló szervezeti egységek

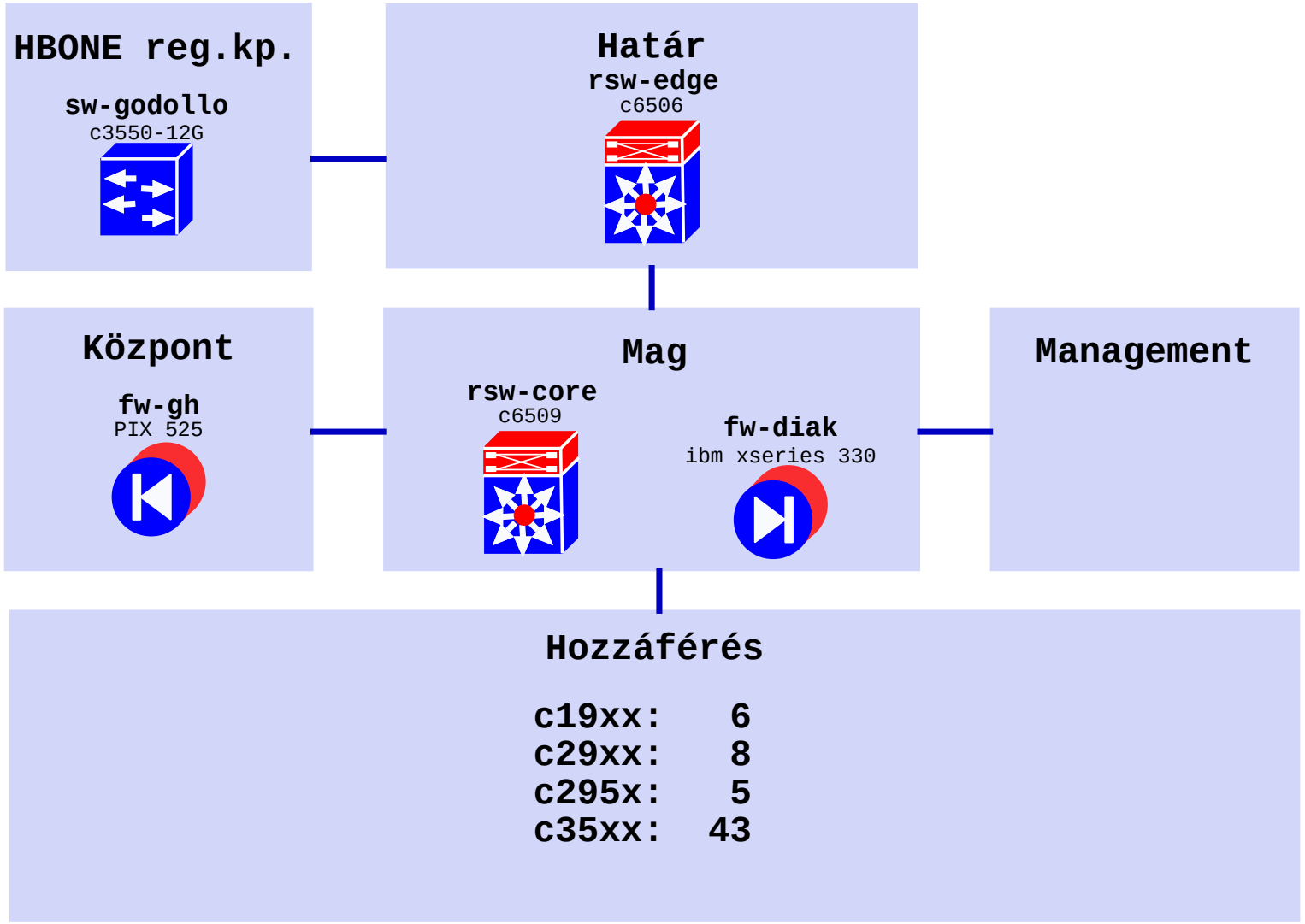
A gödöllői hálózat felépítése

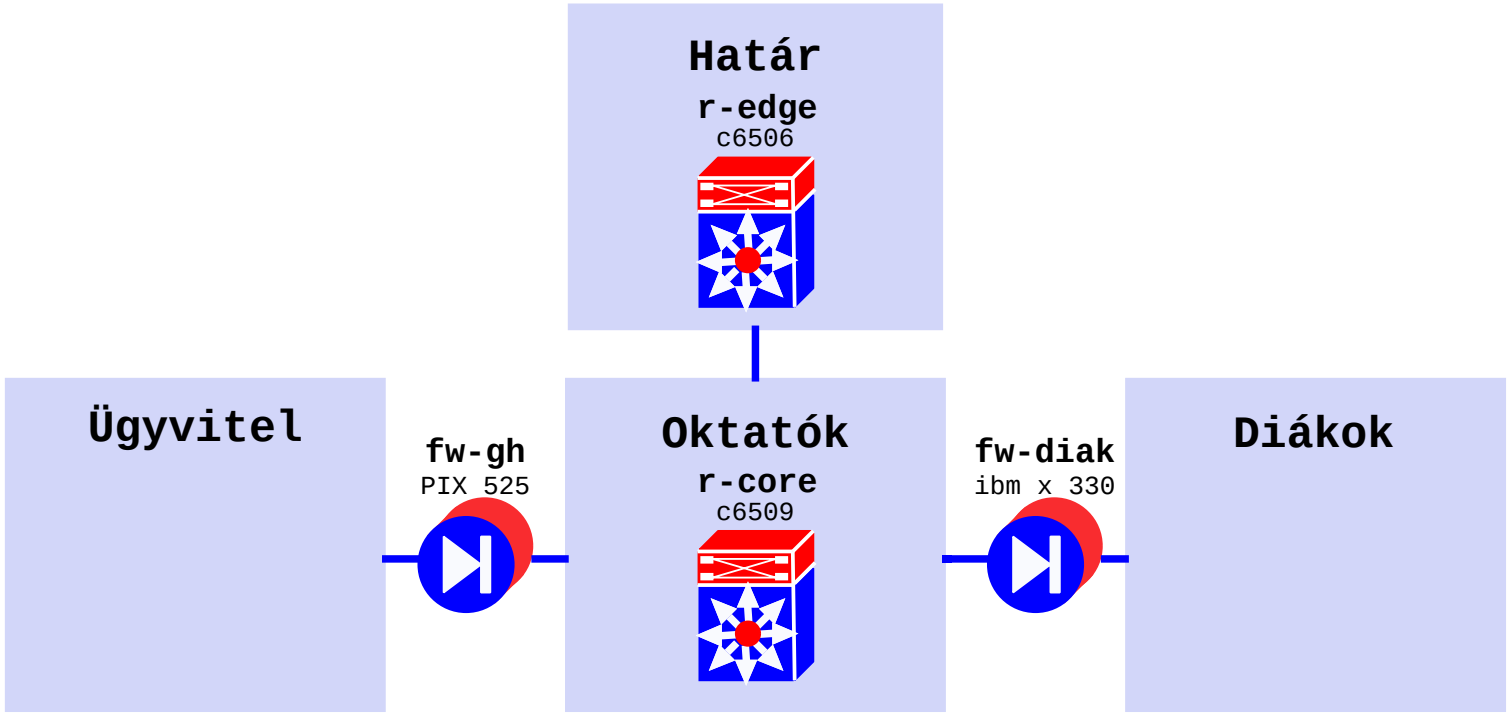
– kétrétegű (core, access) felépítés, kiegészítve határ (edge) modullal

– erős tartalékok az access rétegben - jelenleg 30 db 1Gbps, könnyen 2Gbps, kábelezés lehetővé teszi a 10Gbps-et is.

– core router és switch egy eszközben (Cisco 6509, MSFC2, SFM, 2db X6516-GBIC, X6548-TX), 256Gbps kapacitás

– edge router és switch egy eszközben (Cisco 6506, MSFC2, X6516-TX), 30Mpps kapacitás


HBONE reg.kp.
sw-godollo
c3550-12G
Határ
rsw-edge
c6506
Központ
fw-gh
PIX 525
Mag
rsw-core
c6509
fw-diak
ibm xseries 330
Management
Hozzáférés
c19xx: 6
c29xx: 8
c295x: 5
c35xx: 43


Határ
r-edge
c6506
Ügyvitel
fw-gh
PIX 525
Oktatók
r-core
c6509
fw-diak
ibm x 330
Diákok

Szerverszoba

- $60m^2$
- 3x15kW klima
- két APC Symmetra 16 kVA UPS
- álpadlós elrendezés, padló alatti levegő befújás, kábelezés
- riasztó és automatikus tűzoltó berendezés
- kártyás beléptető rendszer

Felügyeleti megoldások

Leválasztás

– VLAN 1, RFC 1918-as cím, de nem NAT-olt

– csak a management hálózatból érhető el

– DNS zónaja csak management hálózatból kérdezhető le

– következetes nevezéktan: asw-f2g1 : access switch, főépület 2. emelet, G rendező, 1. eszköz.

– SNMP comm. mellé ACL:

```
snmp-server community titok RO 98
snmp-server community ubertitok RW 99
snmp-server contact nagytudasu@email.cim
access-list 98 permit host noc.gep.ip.cime
access-list 99 permit host noc.gep.ip.cime
```

AAA-TACACS+

– minden aktiv eszközre belépéshez TACACS+ auth

– minden kiadott parancs loggolodik

konfiguráció kezelés

– központi tftp szerver: konfig és OS image

– elöző konfig dátum szerint átnevezve

– alias az eszközökben:

```
alias exec wrnet copy running-config tftp://noc.gep.ip.cime/asw-f2
```

Syslog

– központi syslog: syslog-ng

– csacsogó eszközöknél (PIX) többfelé szétszedve

```
destination pix_err  file("/var/log/routers/pix_err.log"
  owner("root") group("adm") perm(0640)); ;
destination pix_crit  file("/var/log/routers/pix_crit.log"
  owner("root") group("adm") perm(0640)); ;
filter f_pix_crit        host(192.168.242.246) and
  match("PIX-[12]");;
filter f_pix_err         host(192.168.242.246) and
  match("PIX-[34567]");;
log  source(net); filter(f_pix_crit); destination(pix_crit); ;
log  source(net); filter(f_pix_err); destination(pix_err); ;
```

– napi rotálás, 365 nap őrzése

Monitorozás - nagios

– jelenleg 134 host

– GSM modemmel sms küldés noc-ról

Terhelés figyelés

cricket: halózati eszközök, UPS-ek SNMP-n. Jelenleg 305 paraméter

`http://cricket.sourceforge.net/`

`http://noc.gau.hu/cgi-bin/cricket/grapher.cgi`

munin: hostok: 1256 paraméter

`http://www.linpro.no/projects/munin/`

`http://noc.gau.hu/munin/`

Forgalom mérés - netflow

- linuxon flow-tools: `http://www.splintered.net/sw/flow-tools/`
- adatmennyiség: 50G -as partición 45G, ez kicsit több 1 hónap
- archiválás eleinte havonta CD-re, később DVD-re, majd feladtuk
- PFC full flow export, V5 formátumban tároljuk, ev/honap/nap/ könyvtárszerkezettel, óránként egy fájlba.
- a tüzfal által NAT-olt VLAN-ok bridge-elt forgalmát exportáljuk

Hálózat kezelés

- netdisco `http://netdisco.org/`
- aktív eszköz leltár
- L2 traceroute
- IP ütközés kezelése, duplex missmatch keresés

Elektronikus levelezés szolgáltatás

- egyetlen, központi mail gateway
- történelmi okokból sok SMTP szerver
- régi felhasználók: sok cím 1993 óta működik $\Rightarrow$kéretlen levelek mennyisége nagy
- kapcsolodó szolgáltatások:
  - posterestante: LDAP, php, storage
    `http://hasznos.szie.hu/posta/posterestante.tgz`
  - lev. lista: mailman, storage

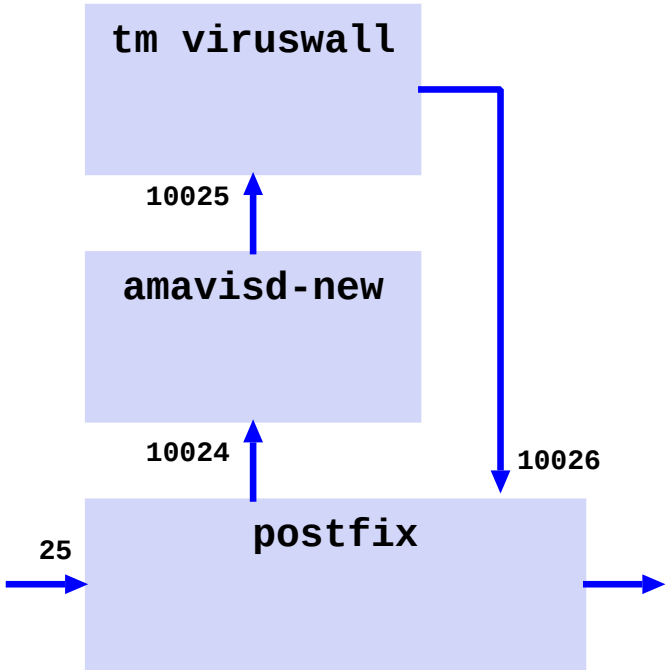
Az SMTP gateway története

Régi mail gateway

- DEC MicroVAX, MX Mailer
- SUN Enterprise Ultra 250, dual ultra SPARC II, 2G RAM, Solaris 8
- Solaris sendmail, TrendMicro VirusWall
- problémák:
  - tm vw minden programja (MTA, web management interface) csak root joggal futtatható
  - virusszűrő közvetlenül elérhető a 25-ös porton $\Rightarrow$sok támadás érte, ezt rosszul bírta
  - beszállító nem tudta megoldani, de végül ”egygépes szendvics”-et csináltunk belőle
  - a web management interface TCP portja open proxy volt

Javított mail gateway

- spam szűrés szükségessé vált
- hardver, op. rendszer adott
- keresés eredménye: OSS
  - postfix MTA
  - amavisd-new, spamassassin
  - Trendmicro Viruswall



Javított mail gateway tapasztalatok

- telepítés: linux-ra könnyű, solaris-ra közepesen nehéz (perl, CPAN)
- teljesítmény: jó
- szabályrendszer hangolás: a három kategória határainak meghatározása gyakorlatot igényel
- statisztikai elemző: automata, félautomata és kézi tanítás lehetséges
- kisebb felhasználói csoportok számára könnyen behangolható
- heterogén levelezési szokású, sok felhasználóhoz hangolás sok kreativitást, időt igényel (Állatorvosi kar)
- mellékhatás: jó spam szűrővel a vírusszűrő terhelése kb. két nagyságrenddel kisebb!

Új mail gateway

- lassan kinőttük a rendelkezésre álló hardvert, normál üzemben is 50 % CPU terhelés
- false positive problémák miatt lazítani kellet a szabályrendszeren
- SPARC vagy Intel, Solaris vagy Linux?
- vírusszűrőt mindenki tud készíteni
- jó spamfilter nincs, vagy nagyon drága?
- előírások miatt SMTP relay-es szolgáltatást nem vehetünk
- Sophos Puremessage 4.5 30 napos tesztüzem SPARC Solaris 8-on

A megoldás:

- SUN Fire V20Z: 1 RU, Dual AMD Opteron 252, 4G RAM, hotswap SCSI disk, szervízprocesszor
- Debian/GNU Linux 3.1 (Sarge), Linux kernel 2.6.x, szoftver RAID, LVM, XFS
- Postfix 2.1.5
- **Sophos Puremessage** 5.0 - egyetlen gép minden ”server role”-ra
  - Centralized Server Manager - web és cli
  - Database Server - postgresql
  - End User Web Interface Server - DB
  - Mail Filter - MTA
  - Mail Transfer Agent - CSM-re

A beveztés lépései

1. tesztüzem már hónapokkal korábban megvolt
2. a régi mail gw marad az ”éles”, néhány régi, de kevésbé kritikus SMTP szerver forgalmát az új gépen keresztűl kűldjük át egy héten át
3. az új rendszer lesz az ”éles”, teljes forgalom átmegy rajta, de csak jelöli a leveleket, nem dob el, nem karanténoz
4. normál üzemre áttérés: karantén, eldobás
5. folyamatos policy karbantartás

PMX üzemeltetési tapasztalatok

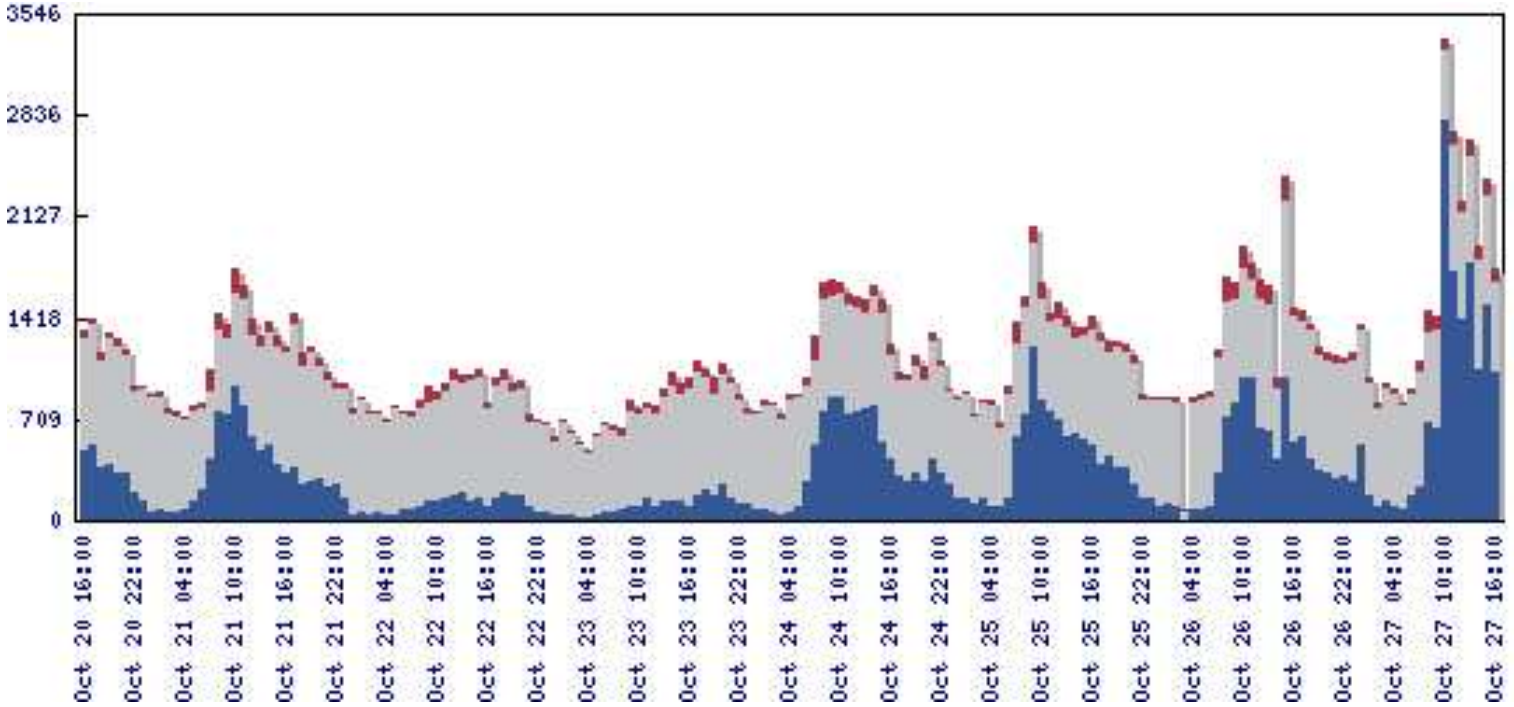
Hatékonyság

A bevezetés 2. fázisában egy régi címre érkező levelek eloszlása a két szűrő szerint:

paraméter	puremessage	spamassassin
biztos spam	625	316
valószínű spam	63	372
false negative	8	8
false positive	1	3

Teljesítmény

- 24 óra alatt: 17343 tiszta levél, 18236 spam, 1186 vírusos levél
- 7 nap alatt: 64580 tiszta levél, 122 248 spam, 7338 vírusos
- gép terhelése: 5 % CPU load, kb 6 GB karantén (adatbázis és fájlok együtt)



Statisztikák

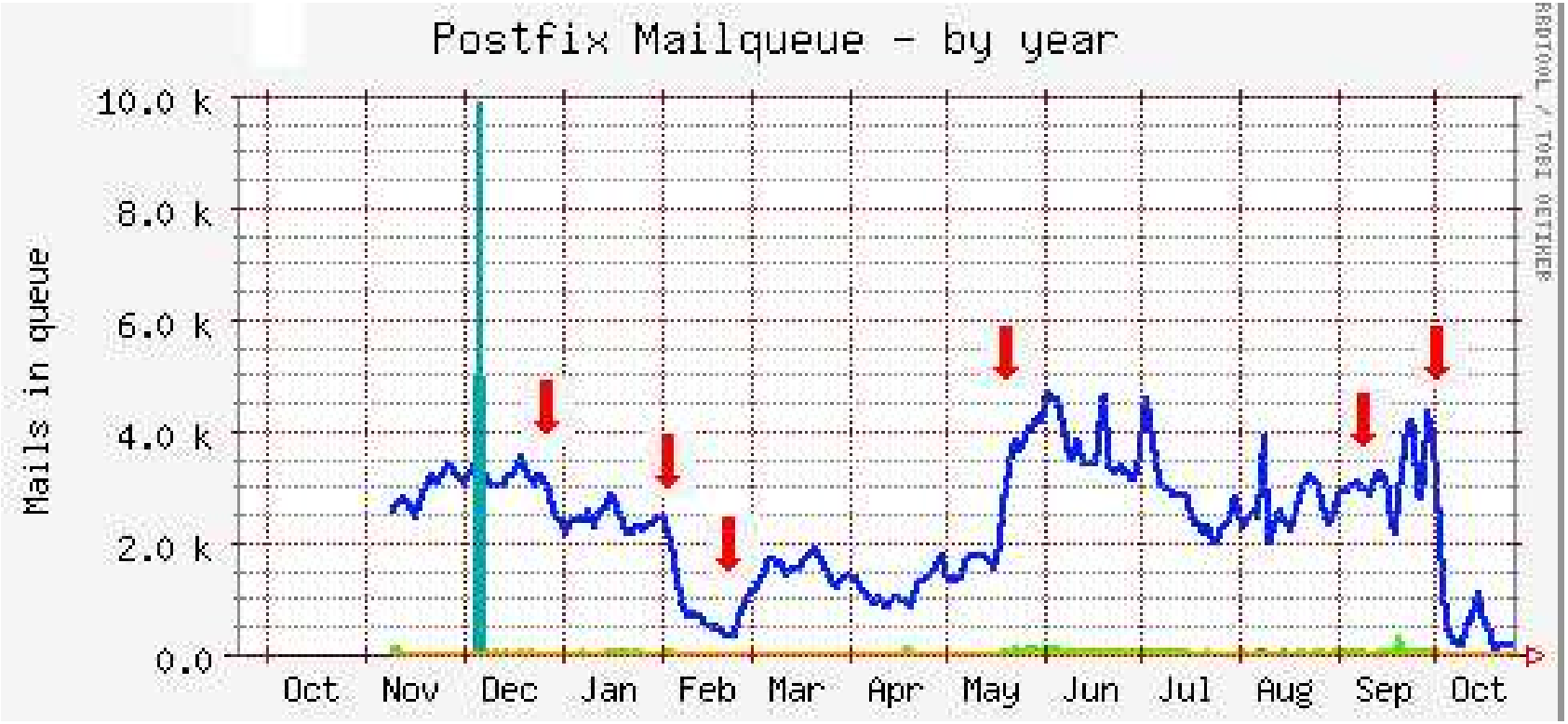
virus	darab
W32/Netsky-P	968
W32/Netsky-Y	281
W32/Mytob-GH	175
W32/Mytob-FB	164
W32/Netsky-AE	114
W32/Mytob-C	87
W32/Netsky-D	79
W32/Mytob-CU	73
W32/Mytob-BY	66
W32/Mytob-AV	65

Szabály	találat
RELAY_IN_CBL	24624
CTYPE_JUST_HTML	13198
HTML_50_70	11939
RELAY_IN_NJABL_DYNABLOCK	11490
NO_REAL_NAME	10542
URI_CLASS_HEALTH_DOMAIN	10386
IP_HTTP_ADDR	9540
KNOWN_SPAM_PARAGRAPH	8350
MIME_HEADER_CTYPE_ONLY	8100
HTML_MIME_NO_HTML_TAG	7001

Egyéb észrevételek

- az `eml` kiterjesztésű csatolásokat alapértelmezetten nem engedi át
- jelszavas fájlokat (zip, doc, xls) alapértelmezetten szűri
- karantént és felhasználói felületét nem tartottuk fontosnak, nem is kívántuk bevezetni, de beváll t
- karantén okot (Reason) át kell állítani, alapértelmezetten csak `spam`, tanácsos a `virus` is.
- a végfelhasználói felület a meglévő LDAP-al simán integrálható
- telepítéskor érdemes megfelelő particiókat kialakítani, a `/opt` mellé `/opt/pmx/var` vagy `/opt/pmx/postgres` és `/opt/pmx/var/qdir`
- `logrotate` nem kerül beállításra a telepítés során
- ”report” funkció nem kezeli a kirotált log-okat

Postfix deferred queue mérete és spam szűrés hatékonysága



Megoldásra váró feladatok

- bizonyos üzenetek feldolgozása után nagy CPU terhelés - support-al dolgozunk a problémán
- a végfelhasználói felület `mail` LDAP attributum melett a `mailAlternateAddress` és `mailEquivalentAddress` attributumot is használja
- karantén kezelés subdomain-re delegálható legyen
- adott címre, mintára, subdomain-re korlátozható legyen a maximális levélméret
- minden üzenetről kerüljön bejegyzés a `message_log` -ba (saját adatfeldolgozás, monitorozás egyszerübb)

Amit a felhasználók észrevettek

- nem kell saját MUA-ben szűrni, spam foldert űrítgetni. Karanténban 2 hétig megtalálhatók a levelek.
- spam szűréssel elégedettek
- karantén létét, működését és használatát tanítani kell $\Rightarrow$helpdesk
- egyszerű felhasználónak egyszerű, két kategória: spam, nem spam
- haladók használhatják a három kategóriát
- végfelhasználói felület egyéb funkcióit (per user white, black list, stb.) nem engedélyeztük

Miért SAN?

DAS: Direct-attached Storage: erősen korlátozott a bővíthetőség. Tipikus: 6x146G ⇒876G brutto, RAID5: 665G netto. U320 SCSI és 10k rpm-es diskek esetén csak a 4. disk okoz gyorsulást.

SAN: Storage Area Network: Diskek külső vezérlőn, blokk szintű elérés általában 2Gbps FiberChannel, vagy 1Gbps ethernet-iSCSI. Skálázható, gyors.

NAS: Network Attached Storage - fájl szintű elérés LAN-on keresztül: nehezen tűzfalazható

SAN-ra épűlő Szolgáltatások

központi fálj kiszolgáló: Linux,SaMBa, LDAP segítségével kb 3000 gépnek **-** nagy növekedés várható

web hosting: Linux UML alapú virtual hosting **-** közepes növekedés

levelezési lista archivum: Linux, mailman számára archiválási terület **-** viszonylag szerény, de monoton növekedés

mentés: központi biztonsági mentés

SAN tervezési megfontolások

A probléma: nem hatékony a háttértár felhasználás: bizonyos gépekben sok van, más gépekben már nem tudunk bővíteni. Háttértár konszolidációra SAN-t választottunk. Föbb követelmények:

skálázhatóság: kis kiinduló méret, később jelentős bővítések várhatók

támogatás: Debian/GNU Linux és SUN Solaris op. rendszerek kell együtműködni

hibatűrés: bizonyos szolgáltatásokat nagy megbízhatósággal kell üzemeltetni

mentés: központi biztonsági mentés lehetősége

Megvalósítás

Kiválasztott hardver elemek

meglévő gépek: 2db IBM xSeries x345, 1db xSeries 330

új gép: 1db IBM xSeries x335 (PCI-X, hotswap...)

HBA: 5db Qlogic QLA2340

szalagos egység: IBM LTO2 200/400G SCSI tape külső házban.

storage: EMC^2 Clariion CX700, 4T brutto kezdő kiépítés, max 32T

Linux storage-ra kötése

- kernel fordítás HBA-hoz
- storage LUN scsi device-ként látszik
- particionálás: egyetlen Linux LVM típusú partició, XFS fájlrendszer

LUN méret növelés

Lehetséges módszerek:

1. LUN növelése: meta LUN létrehozás
2. új LUN létrehozás - RAID 0
3. új LUN létrehozás - LVM

Szükséges lépések LVM esetén:

```
pvcreate /dev/scsi/host0/bus0/target1/lun0/part1
vgextend emc /dev/scsi/host0/bus0/target1/lun0/part1
lvextend -L+100G /dev/emc/home
xfs_growfs /dev/emc/home
```

Hibatűrő csatlakozás storage-hoz

- 2.4 kernelhez speciális EMC cél szoftver
- 2.6 kernelben nyilt forráskódú támogatás
  - jelenleg multipath disk (SW RAID) szinten
  - multipath-tools `http://christophe.varoqui.free.fr/`
- storage megfelelő beállítása: failovermode 2, FC loop mode
- kernelbe multipath RAID
- többi lépés mind alapesetben, de particionálás helyett md, azaz:

```
cat /etc/mdadm/mdadm.conf
DEVICE /dev/sda /dev/sdb
ARRAY /dev/md3 level=multipath devices=/dev/sda,/dev/sdb
```

gép	típus	diskvezérlő	disk	írás	olvasás	átlag
fájlszerver	x345	qla2340/R5-8	cx700	85	127	106
desktop	PC	via k8t890/R0	7k/SATA	116	94	105
fájlszerver	x345	fusion/SW R5	10k/U320	75	110	92.5
mentés	x345	qla2340/R5-8	cx700	67	116	91
mailgw	v20z	lsi/mat3073nc	10k/U320	96	83	89.6
webszerver	x335	fusion/SW R1	15k/U320	72	75	73.5
mailgw	v20z	lsi/st373207lc	10k/U320	65	64	64.5
desktop	PC	via k8t890/R1	7k/SATA	48	60	54
desktop	PC	via k8t890	7k/SATA	58	46	52
noc	x330	aic7892/SW R1	10k/U160	44	53	48.5
mentés	x345	fusion/SW R1	10k/U160	26	40	33
mentés	x345	ibm 5i/R5	10k/U160	12	30	21

Összefoglalás

- alap infrastruktura jónak nevezhető
- szolgáltatások bevezetése folyamatos
  - LDAP
  - webmail, posterestante, mailman
  - spam szürés
  - uml-es hosting hasznos
  - storage soha nem elég nagy
- fájlszerver szolgáltatás a következő lépés

e-mail cím: `lajber.zoltan@ih.szie.hu`

Az előadás letölthető: `http://zeus.gau.hu/~lajbi/hbonetabor.pdf`