Postfix

KFKI RMKI
Kadlecsik József
kadlec@sunserv.kfki.hu

Az E-mail működésének alapjai

- Levél küldés/fogadás: SMTP - MTA
- Levél olvasás mailbox-ból: POP/IMAP - MUA
- DNS
  - NS, MX, A (AAAA) rekordok
  - PTR, TXT rekordok

Simple Mail Transport Protocol I.

% telnet sunserv.kfki.hu smtp

...

220 sunserv.kfki.hu ESMTP Postfix

EHLO mentat.kfki.hu

250-mentat.kfki.hu

250-PIPELINING

250-SIZE 10240000

250-ETRN

250-XVERP

250 8BITMIME

SMTP II.

MAIL FROM: <kadlec@mentat.kfki.hu>

250 Ok

RCPT TO: <kadlec@sunserv.kfki.hu>

250 Ok

DATA

354 End data with <CR><LF>.<CR><LF>

blabla

.

250 Ok: queued as ACB571D3223

SMTP III.

- Végtelenül egyszerű protokoll, de
  - '.'-ra a '250' válasz azt jelenti, hogy a fogadó fél teljes mértékben átvette a levélkézbesítés feladatát
  - Levél nyomtalanul nem veszhet el, hurok nem lehet.
- 4xx hibaüzenetek
- 5xx hibaüzenetek
- Alapvetően proxy felépítés:

MUA $\rightarrow$ *SMTP* $\rightarrow$ MTA $\rightarrow$ *SMTP* $\rightarrow$ MTA (mbox) $\rightarrow$ *POP* $\rightarrow$ MUA

Boríték - levél

- Envelope sender/recipient:

  MAIL FROM, RCPT TO

- Levél-fejléc:

  Return-Path:

  Delivered-To:

  Received:

  From:

  To:

  Subject:

Postfix MTA

- Wietse Venema írta az IBM támogatásával, kezdetben VMailer-nek hívták.
- Közvetlen versenytárs a qmail Dan Bernstein-től
- Jelenlegi verziók
  - official: postfix-1.1.13
  - official: postfix-2.0.16
  - experimental: postfix-2.0.16-20031113

Fő célkitűzések

- A program terjedjen el minél szélesebb körben
- Nagy teljesítmény
- Sendmail-kompatibilitás az áttérés megkönnyítése érdekében
- Robusztus működés
- Rugalmasság
- Biztonság

Architekturális felépítés

- Szemi-rezidens, kölcsönösen kooperáló programok együttese, amelyek egy-egy feladat ellátására szolgálnak és nincs köztük merev szülő-gyerek viszony.
- A master program futtatja a programokat igény szerint: konfigurálható számú programot indíthat, amelyeket konfigurálható számban használ újra és konfigurálható idle time után dob el

IPC

- A programoknak kommunikálni kell egymással:
  - UNIX-domain socket
  - FIFO (védett könyvtárban)
- Minimális információ-átadás:
  - Queue file neve; címzettek listája; státus információk
- Információvesztés elleni védekezés:
  - Flush és fsync() adat elfogadása előtt
  - Minden rendszerhívás hibakódját ellenőrzi

Postfix mail queue

- Négy fő queue:
  - maildrop
  - incoming
  - active
  - deferred
- Három segéd queue
  - defer, hold
  - corrupt

Fair működés

- A TCP-hez hasonlóan
  - Slow start kézbesítés kezdésekor
  - Exponenciális visszavétel hiba esetén
  - Round-robin kiválasztás a kézbesítendők közül az active queue-ban

Biztonság

- Több mint 30000 kódsor: többszintű biztonság
- Elégséges legkisebb privilégium
- Processzek belső IPC-vel szeparáltak
- Processz-környezet a master daemon által szigorúan kontrollált
- Nincs setuid program
  - maildrop queue world-writable volt, helyette postdrop setgid-es lett

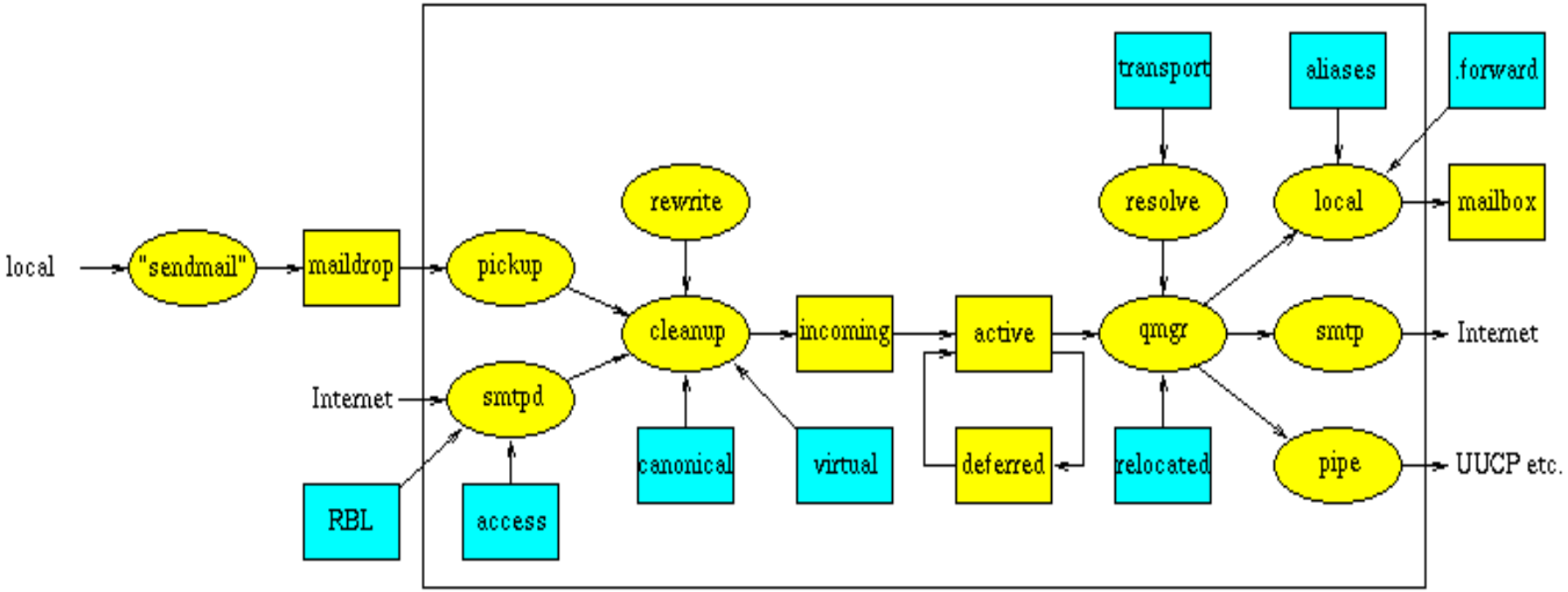
Biztonság II.

- Bizalom
  - Postfix nem bízik a queue file tartalomban vagy az IPC üzenetekben
  - Hálózatról érkezett adatokat filterezi
- Nagy inputok kezelése
  - Dinamikus string és buffer allokálás
  - Hosszú sorok kezelhető méretűre darabolása
  - Diagnosztikai üzenetek korlátozottak a rendszer syslog(3) interfész miatt

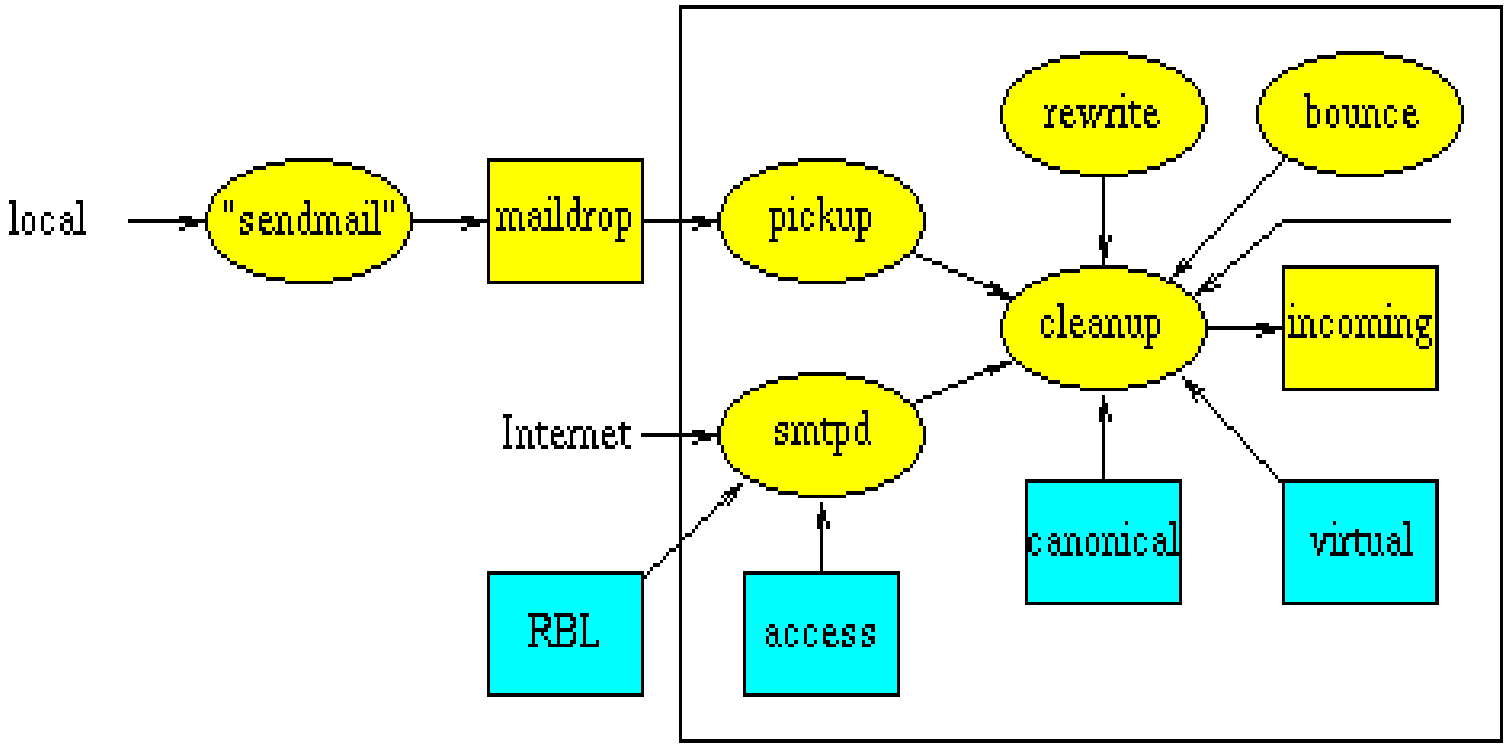
Biztonság III.

- Egyéb védelmek:
  - A memóriában levő objektumok száma korlátos.
  - Problémák esetén a rendszer szünetet tart, mielőtt hibaüzenetet küldene vagy megpróbálná újraindítani a leállt programot.

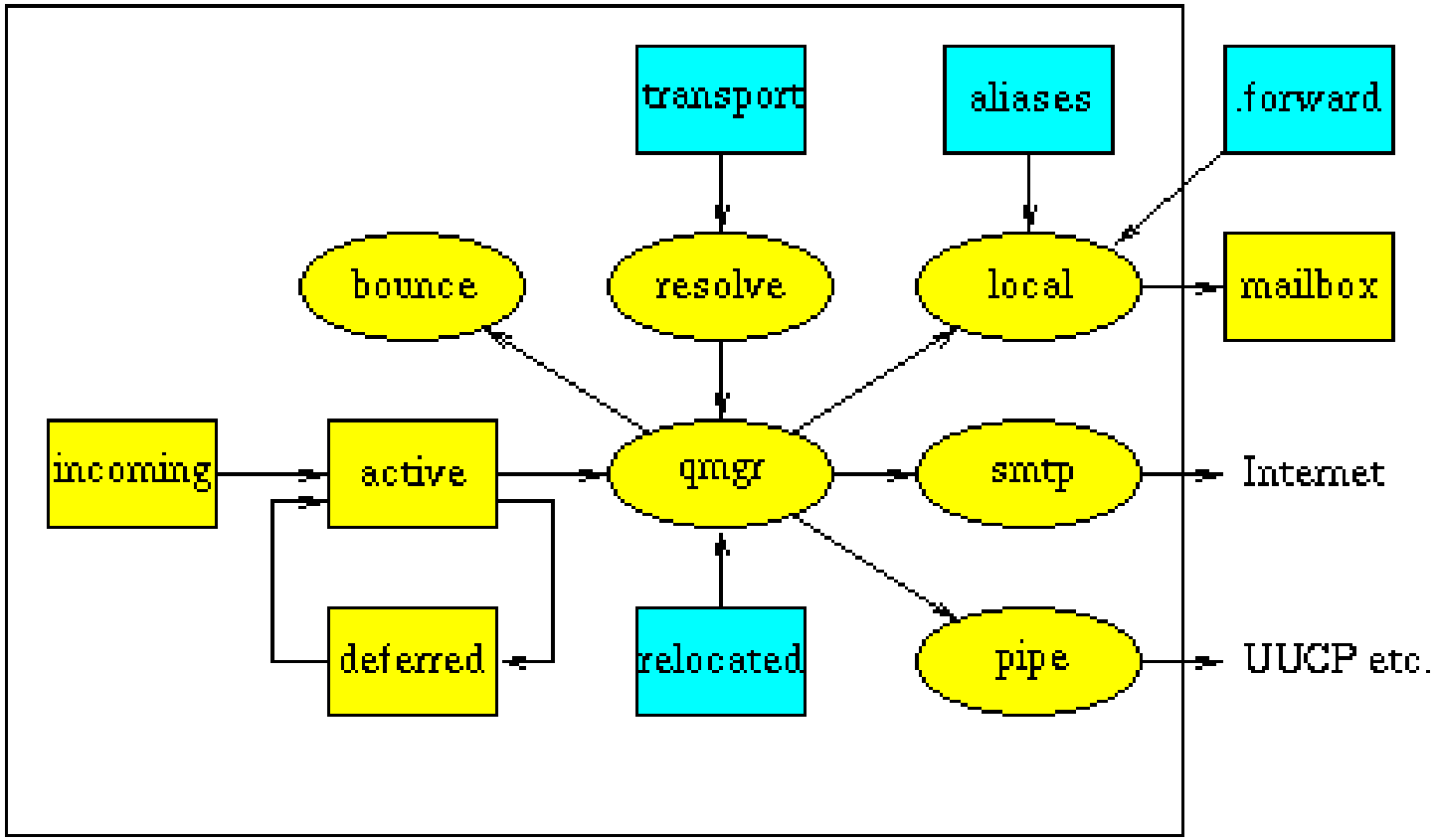
A rendszer maga



Levél fogadás



Levél küldés



Egyéb daemon programok

- master :-)
- showq daemon (a mailq-hoz)
- flush SMTP ETRN kérésekhez
- verify cím verifikáláshoz (UCE)
- proxymap: read-only tábla lookup szolgáltatás
- spawn: nem-Postfix programok indítása

Commandline programok

- sendmail, mailq, newaliases
- postfix start | stop | reload | check
- postalias (newaliases), postmap
- postcat, postqueue (sendmail list/flush queue)
- postconf
- postdrop
- postkick, postlock, postlog
- postsuper

Konfigurációs file-ok

- /etc/postfix/master.cf
- /etc/postfix/main.cf
  - változó = érték
  - Shell/Perl-szerű szintaxis --- de nem Perl/shell!
  - Loose kiértékelés: utolsó változó-értékadás számít!

A szükséges minimális beállítások

- Az adott gépről küldött levelekben milyen domain jelenjen meg a feladónál:

  myorigin = $myhostname

  myorigin = $mydomain

- Milyen domain-eknek címzett levelet fogadjon el úgy, mint a lokális gépnek címzetteket:

  mydestination = $myhostname, localhost.$mydomain

  mydestination = $myhostname, localhost.$mydomain,

  $mydomain

A szükséges minimális beállítások II.

- Milyen kliensek számára relay-ezek

  mynetworks_style = subnet [| class | host]

  vagy

  mynetworks = 168.100.189.0/28, 127.0.0.0/8

- Milyen hibáról menjen E-mail report a postmasternek:

  notify_classes = resource, software

  (resource, software, bounce, 2bounce, delay, policy, protocol)

A szükséges minimális beállítások III.

- A gép neve

  myhostname = host.local.domain

  mynetworks = host.virtual.domain

- A gép nevének a domain része (default $myhostname-ből származtatott)

  mydomain = local.domain

- Az intefészek, amelyeken figyelnie kell:

  inet_interfaces = all

  inet_interfaces = host.virtual.domain

Rate kontrol

- default_process_limit
  - smtpd, smtp, local, stb, processzek össz-számára
  - egyedi limit a master.cf-ben lehetséges
- [initial | default | local] _destination_concurrency_limit
- smtp_destination_recipient_limit
- smtpd_recipient_limit

Késletetett kézbesítés

- defer_transports = smtp [, uucp]
- A levélküldés a következő paranccsal indítható:

  sendmail -q

Deferred queue paraméterek

- queue_run_delay = 1000s
- maximal_queue_lifetime = 5d
- minimal_backoff_time = 1000s
- maximal_backoff_time = 4000s

Rosszul viselkedő kliensek lassítása

- smtpd_soft_error_limit
- smtpd_error_sleep_time
- smtpd_hard_error_limit

Erőforrás kontroll

- Határértékek objektum méretekre:
  - line_length_limit, hosszabbakat feltördeli
  - header_size_limit, az ezen túl levőket eldobja
  - header_address_token_limit, az ezen túl levőket eldobja
  - message_size_limit
  - bounce_size_limit

Erőforrás kontroll II.

- Határértékek objektumok számára
- Időlimitek
- File lockolási kísérletekre való limitek
- Error recovery

Postfix táblázatok

- db (hash, btree)
- dbm
- ldap, mysql, pgsql
- NetInfo, NIS, NIS+
- regexp, pcre
- cidr
- tcp, unix

Címátírás

- Beépített címátírás (trivial-rewrite)
  - @hosta,@hostb:user@site
    - source routing nem támogatott
  - site!user → user@site (swap_bangpath)
  - user%domain → user@domain (allow_percent_hack)
  - user → user@$myorigin (append_at_myorigin)
  - user@host → user@host.$mydomain (append_dot_mydomain)
  - user@site. → user@site

Kanonikus címátírás

- Kanonikus (login) nevek átírása az envelope/message fejlécekben, lokális/távoli címek esetén egyaránt (cleanup):

  canonical_maps = hash:/etc/postfix/canonical

  (sender_canonical_maps, recipient_canonical_maps)

  ```
  kadlec@blackhole.kfki.hu  Jozsef.Kadlecsik@kfki.hu
  kadlec                    Jozsef.Kadlecsik@kfki.hu
  ```

  ha a lehagyott @site-ból a site benne van $myorigin vagy $mydestination-ban

Address masquerading

- Összes belső gép címeinek átírása a gateway címére (cleanup):

  masquerade_domains = !foo.example.com, example.com

  masquerade_exceptions = root

- Default message fejlécekre és envelope sender címre, envelope recipient-re **nem**

Virtuális email aliasok

- Kanonikus átírás és masquerading után, csak az envelope recipient címekre (local/remote): virtuális/megszűnt E-mail címterek átirányítása valódiakra (használható kanonikus címekre való visszaírásra is)

```
virtual_alias_maps = hash:/etc/postfix/virtual
```

Mail transzport meghatározása

Címzett egyezik	Delivery agent	Kontrol param.
$mydestination	local	$local_transport
vagy $inet_interfaces		
$virtual_mailbox_domains	virtual	$virtual_transport
$relay_domains	relay (smtp)	$relay_transport
none	smtp	$default_transport

Mail transzport meghatározás felülbírálása

- Például belső mail szerverek felé való továbbításra, UUCP feletti továbbküldésre, stb.

transport_maps = hash:/etc/postfix/transport

```
.foo.org        smtp:[internal.foo.org]
foo.org         smtp:[internal.foo.org]
```

Relocated

- User has moved to üzenetek generálására

  relocated_maps = hash:/etc/postfix/relocated

```
@old.domain       new.domain
sacked@foo.com    sacked@bar.net
```

Lokális aliasek

- Jól megszokott aliasek:

  alias_database = hash:/etc/aliases

  - **newaliases**

  alias_maps = hash:/etc/aliases,
  hash:/etc/mailman/aliases

  - **postmap /etc/mailman/aliases**

Nem létező lokális címzettek

- Ismeretlen lokális címekre jövő leveleket a Postfix visszautasítja
- luser_relay paraméter az ilyen levelek másik mailbox-ba való átirányítására

UCE kontrol

- Két helyen történhet:
  - smtpd: smtpd_foo_restrictions
  - cleanup: header_checks, body_checks

header és body_checks

- Egyezés-keresés a message header és body **soraiban**: mit értünk egy sor alatt?
- regexp/pcre táblázatok: bal oldalon egyezést kereső regexp/pcre kifejezés
- Jobb oldalon állhat:
  - REJECT [text] utasítsd vissza a levelet
  - DUNNO [text] hagyd abba a keresést erre a sorra
  - IGNORE [text] **töröld** a sort az üzenetből
  - WARN [text] csak naplózz

header és body_checks II.

- Jobb oldalon állhat:
  - HOLD [text] tedd az üzenetet a hold queue-ba
  - DISCARD [text] dobd el az üzenetet, de jelezz Ok-t
  - FILTER transport:nexthop queueing után zavard át az üzenetet egy content filteren
  - REDIRECT user@domain küldd a levelet a megadott címre

http://jimsun.linxnet.com/misc/header_checks.txt

http://jimsun.linxnet.com/misc/body_checks.txt

header_checks

```
# Veszélyes MS kiterjesztések
/^Content-(Disposition|Type):\s+.+?(?:file)?
   name=”?.+?\.(386|ba[st]|exe)\b/ REJECT “.$2” not allowed
# “.zip”-re warning
/^Content-(Disposition|Type):\s+.+?(file)?
   name=”?.+?\.zip\b/    WARN
```

body_checks

```
# EXE file-okra minták
/^TV[nopqr]....[AB]..A.A/i   REJECT Email with EXE denied
/^M35[GHIJK].`..`..*````/i   REJECT Email with EXE denied
# base64 nem érdekes
/^[A-Za-z0-9+\/=]{4,76}$/    OK
# Veszélyes kiterjesztések uuencode-olva
/^begin\s+\d+\s+.+?\.(386|ba[st]|exe)\b/
                          REJECT ".$1" not allowed
```

access táblák

- E-mail lookup esetén bal oldalon állhat:
  - user@domain
  - domain.tld ($parent_domain_matches_subdomains)
  - user@
- Hostname/IP cím lookup esetén bal odlalon állhat:
  - domain.tld
  - net.work.addr.ess
  - net.work.addr
  - ...

access táblák II.

- Jobb oldalon állhat:
  - [45]NN text — utasítsd vissza
  - REJECT [text] — utasítsd vissza
  - DEFER_IF_REJECT — tedd a defer queue-be ha később egy restriction REJECT kódot ad vissza
  - DEFER_IF_PERMIT — ugyanez PERMIT-el
  - OK — fogadd el
  - csak számok — fogadd el (POP before smtp)
  - DUNNO — tegyél úgy, mintha nem találtad volna (substring/IP egyezés-keresés kimarad)

access táblák III.

- Jobb oldalon állhat:
  - HOLD [text] tedd a hold queue-ba
  - DISCARD [text] tegyél úgy, mintha elfogadtad volna, de közben dobd el
  - FILTER transport:dest queueing után zavard át a megadott content filteren
  - REDIRECT user@domain küldd el a megadott címre
  - restriction hívd meg a definiált restriction class-t

Kliens hostname/IP cím megszorítások

- smtpd_client_restrictions
  - maptype:mapfile table lookup
  - reject_unknown_client (PTR ↔ A)
  - permit_mynetworks ($mynetworks)
  - reject_rbl_client rbl.domain[=127.0.0.2.]
  - reject_rhsbl_client rbl.domain[=127.0.0.2]
  - check_client_access maptype:mapfile

HELO/EHLO megszorítások

- smtpd_helo_required = yes
- smtpd_helo_restrictions
  - maptype:mapfile table lookup
  - reject_invalid_hostname, reject_non_fqdn_hostname
  - reject_unknown_hostname (A vagy MX)
  - check_helo_ns_access maptype:mapname
  - check_helo_mx_access maptype:mapname
  - reject_rhsbl_helo rbl.domain[=127.0.0.2]
  - check_helo_access maptype:mapfile

Sender address megszorítások

- strict_rfc821_envelopes = yes
- smtpd_sender_restrictions
  - maptype:mapfile table lookup
  - reject_non_fqdn_sender
  - reject_unknown_sender_domain (A vagy MX)
  - check_sender_ns_access maptype:mapname
  - check_sender_mx_access maptype:mapname
  - reject_rhsbl_sender rbl.domain[=127.0.0.2]
  - check_sender_access maptype:mapfile

Sender address megszorítások II.

- smtpd_sender_restrictions
  - reject_unverified_sender (verify daemon)
  - check_sender_login_mismatch (SASL)

Recipient address megszorítások

- smtpd_recipient_restrictions = permit_mynetworks
  reject_unauth_destination
  - maptype:mapfile table lookup
  - reject_non_fqdn_recipient
  - reject_unknown_recipient_domain (A vagy MX)
  - check_recipient_ns_access maptype:mapname
  - check_recipient_mx_access maptype:mapname
  - reject_rhsbl_recipient rbl.domain[=127.0.0.2]
  - check_recipient_access maptype:mapfile

Recipient address megszorítások II.

- smtpd_recipient_restrictions
  - reject_unverified_recipient (verify daemon)
  - reject_multi_recipient_bounce
  - permit_auth_destination ($relay_domains vagy aldomain; $mydestination, $inet_interfaces, $virtual_alias_domains, $virtual_mailbox_domains)
  - reject_unauth_destination
  - permit_mx_backup ($permit_mx_backup_networks)

Recipient address megszorítások III.

- smtpd_recipient_restrictions
  - check_recipient_maps

Címzett domain	Lookup táblázat
$mydestination	$local_recipient_maps
vagy $inet_interfaces	
$virtual_alias_domains	$virtual_alias_maps
$virtual_mailbox_domains	$virtual_mailbox_maps
$relay_domains	$relay_recipient_maps

SMTP ETRN megszorítások

- smtpd_etrn_restrictions
  - nem UCE: ki adhat ki ETRN parancsot

SMTP DATA megszorítások

- smtpd_data_restrictions
  - reject_unauth_pipelining

Általános megszorítások

- permit
- defer
- reject
- warn_if_reject
- check_policy_service inet:*host:port*
- check_policy_service unix:*pathname*

- smtpd_delay_reject = yes

Érvénytelen NS rekordok

/etc/postfix/main.cf:

check_sender_mx_access cidr:/etc/postfix/mx_access

/etc/postfix/mx_access

64.94.110.11	REJECT Verisign wildcard MX
0.0.0.0/8	REJECT Bogus address
127.0.0.0/8	REJECT Loopback address

Address verification

- reject_unverified_[sender|recipient]
- verify daemon kipróbálja a legközelebbi MTA-t vajon elfogadja-e a címet (de pl. yahoo nem visít RCPT TO-nál ismeretlen címre)

/etc/postfix/main.cf:

```
smtpd_sender_restrictions = hash:/etc/postfix/sender_access
unverified_sender_reject_code = 550
```

/etc/postfix/sender_access

```
aol.com             reject_unverified_sender
hotmail.com         reject_unverified_sender
```

Address verification II.

- Default memória cache az eredményekről
- Lehet használni file-t, de
  - ha a file korruptá válik/filerendszer betelik, akkor a Postfix a verifikálás működésképtelensége miatt leáll

Policy service

- Nyitottak a lehetőségek
- Greylisting sample daemon:
  - timestamp a (client, sender, recipient) triple-ről
  - addig mail nem jöhet be, amíg a timestamp legalább nem 3600 másodperces (spammerek nem küldik újra a 4xx-el visszautasított levelet)
  - az adatbázis file-t karban kell tartani

Spamtrap

- Elég egy érvénytelen E-mail cím egy weboldalon

/etc/postfix/main.cf:

```
check_recipient_access hash:/etc/postfix/spamtrap
```

/etc/postfix/spamtrap

```
spam_trap@foo.domain        DISCARD
```

Postfix ext3-on

- $queue_directory legyen önálló partíció
  - data=journal ext3 opció
  - mount noatime,sync opciókkal
  - write cache-t a diszken célszerű kikapcsolni:
    - hdparm -W0 /dev/hdx
  - I/O elevator-t érdemes hangolni:
    - elvtune -r 4096 -w 8192 /dev/hdx

Postfix tuningolás

- Legyen egy működő lokális DNS cache a gépen
- Ne legyünk open relay
- Ne fuldokoljunk a spam bounce-októl: használjunk RBL listákat:
  - inputs.relays.osirusoft.com Spammerek megölték!
  - proxies.relays.monkeys.com Spammerek megölték!
- Ha lehet ne fogadjunk el levelet érvénytelen domain-ekből (reject_unknown_sender_domain)

Postfix tuningolás II.

- Ne fogadjunk el levelet nem létező lokális/relayezett címekre

Dokumentáció

- Forráskóddal együtt jönnek README file-ok, sample konfigurációk alaposan kommentezve, manpage-k, Posfix dokumentáció html-ben
- http://www.postfix.org/