Postfilter

Kadlecsik József
KFKI RMKI
<kadlec@sunserv.kfki.hu>

Tartalom

- Bevezetés
- Postfilter rendszer felépítése
- Szűrési feltételek
- CGI felületek
- Demo

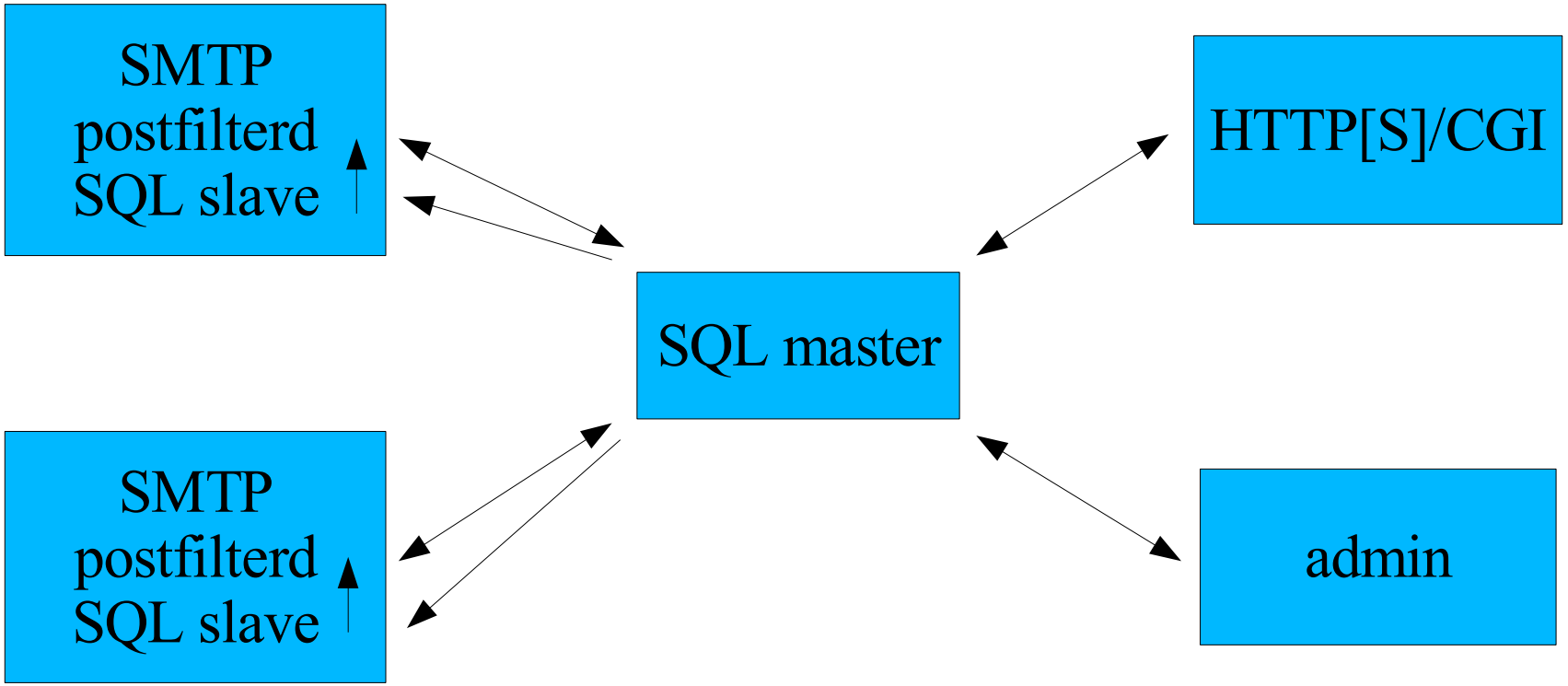
Előzmények

- Postfix per_user_uce patch: 1999-2002
- postfilter 1.x: 2003-2004
- postfilter 2.x: 2005-

Postfilter rendszer felépítése

- Komponensek:
  - Postfix SMTP szerver a postfilterd policy daemonnal
  - HTTP szerver a CGI script-ekkel
  - SQL adatbázis szerver
  - naplózó szerver
  - adminisztratív szerver (pfadm)
- Minden egy szerveren vs teljes disztributivitás

Példa


SMTP
postfilterd
SQL slave
SMTP
postfilterd
SQL slave
SQL master
HTTP[S]/CGI
admin

postfilterd

- Teljes értékű policy daemon Postfix-hez:
  - szintaktikai és DNS ellenőrzések
  - RBL, RHSBL listák
  - whitelist, blacklist, greylist. DHA
  - captcha kihívás (**c**ompletely **a**utomated **p**ublic **T**uring test to tell **c**omputers and **h**umans **a**part)
  - egyéni kivétellisták
  - egyéni szűrési feltételek
- standalone – nem a master.cf-en keresztül indul

Postfilterd integrálása Postfix-be

```
smtpd_recipient_restrictions =
    reject_non_fqdn_sender,
    reject_non_fqdn_recipient,
    reject_unknown_sender_domain,
    reject_unknown_recipient_domain,
    check_policy_service inet:127.0.0.1:10255,
    permit_mynetworks,
    reject_unauth_destination
smtpd_end_of_data_restrictions =
    check_policy_service inet:127.0.0.1:10255
```

CGI script-ek

- postfilter.cgi
  - felhasználói felület az egyéni beállítások módosításához
  - jelszóval védett, https fölött
- captcha.cgi
  - captcha feladat teljesítéséhez

SQL szerver

- Jelenleg csak mySQL támogatott
  - Egyszerű portálhatóság más adatbáziskezelőre
- “read-only” és “read-write” táblázatok postfilterd szempontjából:
  - rw: greylist, captcha, automatikus black/whitelisták
  - ro: user, user_whitelist, nem automatikus listák
- “read-only” táblák replikálhatók az SMTP szerverekre

Naplózás

- mySQL táblába
- report script
  - összesítő a kiszűrt levelekről a felhasználóknak
  - statisztika az adminisztrátoroknak

Adminisztratív szerver I.

- Konfiguráció három részben
- root.conf
  - minden szerveren ott kell lenni
  - minimális beállitások az SQL szerverekről
- schema.conf
  - minden szerveren ott kell lenni
  - integrálás létező SQL alapú autentikációs rendszerekbe, beágyazott táblanevek felülbírálása, jelszó-titkosítás
- root.conf, schema.conf: kézi frissítés

Adminisztratív szerver II.

- main.conf
  - összes komponens minden beállítási paramétere, ~250
  - Postfix main.cf-hez hasonló szintaxis
  - Perl-re fordított és **adatbázisban tárolt**
- pfadm script

Postfilter szűrési beállításai

- Több réteg a maximális rugalmasság érdekében
  - Elemi szűrési feltételek és Postfix-szintű szűrési ítéletek
  - Szűrési policy-k
  - Szűrési osztályok
- Saját E-mail címek: user tábla
  - PUBLIC és HIDDEN
  - REAL és VIRTUAL
  - STANDALONE és SLAVE

Postfix-szintű szűrési ítéletek

- permit [opcionális szöveg]
- dunno [opcionális szöveg]
- [45]nn [opcionális szöveg]
- discard [opcionális szöveg]
- hold [opcionális szöveg]
- prepend szöveg

Makró támogatás

- $sender, $recipient
- $client, $client_name, $client_address
- $helo_name
- $rbl_domain, $txt_record
- $lookup_type, $lookup_subject, $lookup_what
- $captcha_url
- $date

Szűrési policy-k

- Elemi szűrési feltételek és ítéletek:

```
policy_név = feltétel [,feltétel ...] [ítélet]
```

- AND kapcsolat az elemi feltételek negatív ítéletei között
- Catch-all ítéletek: `daemon_template_*`

Szűrési osztályok

- Szűrési policy-kből

```
class_név = policy [,policy ...]
```

- OR kapcsolat a policy-k eredménye között

postfilterd kiindulási pontok

- daemon_default_recipient_class = class, ...
  - quota: levelek száma és címzettek száma
- daemon_default_end_of_data_class = class, ...
  - quota: levelek mérete – elvileg

Elemi szűrési feltételek

- <type>:<subject>[:arguments]
  - argumentum: kulcsszó=érték
- Három visszatérési érték
  - reject: negatív találat
  - permit: pozitív találat
  - dunno: nincs találat

Elemi szűrési feltételek I.

- lookup:<subject>:table=tablename

  :match=<value>:nomatch=<value>

  - client, client_name, client_address, helo_name, sender, recipient
  - SQL minták tárolhatók
    - %.domain.com
    - 10.%
- blacklist:<subject>:table=tablename
- whitelist:<subject>:table=tablename

Elemi szűrési feltételek II.

- rbl:client_address
  :domain=rbl.domain.name
  [:query_match=d.d.d.d]
  [:match=<value>][:nomatch=<value>]
- rhsbl:client_name|sender_domain
  :domain=rhsbl.domain.name
  [:query_match=d.d.d.d]
  [:match=<value>][:nomatch=<value>]

Elemi szűrési feltételek III.

- unknown:client_name|helo_name|sender|recipient
  [:match=<value>][:nomatch=<value>]
  [:nohide]

Elemi szűrési feltételek IV.

- invalid:helo_name
  [:match=<value>][:nomatch=<value>]
- non_fqdn:helo_name
  [:match=<value>][:nomatch=<value>]
- authenticated:sasl
  [:match=<value>][:nomatch=<value>]
- captcha:sender

Elemi szűrési feltételek V.

- update:<subject>:table=tablename

  [:netblock4=8*n][netblock6=4*n]

  [:type=user_list][:match=<value>]

  - client_name, client_address, helo_name, sender, recipient, sender_domain, recipient_domain
  - automatikus tiltólistára helyezés:

```
update:client_address:table=blacklist:netblock4=24
```

  - automatikus kivétellistára helyezés:

```
update:recipient:table=user_whitelist:type=user_list
```

Elemi szűrési feltételek VI.

- greylist:client:delay=secs[:train][:whitelist=num]
  - greylist és greylist_white táblák

```
greylist:client:delay=5*60
```

Elemi szűrési feltételek VII.

- throttle:<subject>:count_max=number
  :rcpt_max=number:quota_max=number
  :time_period=number
  [:match=<value>][:nomatch=<value>]
  [:noinsert]
  - sender, client_address, client_name, client, sasl_username

```
throttle:sender:count_max=10:rcpt_max=10
        :time_period=10*60
```

Elemi szűrési feltételek VIII.

- counter:client_address:table=tablename
  :limit=number:time_period=number
  [:netblock4=8*n][netblock6=4*n]
  [:match=<value>][:nomatch=<value>]

```
counter:client_address:table=dha
  :limit=4:time_period=2*60
```

Elemi szűrési feltételek IX.

- counter:client_address:table=tablename
  :limit=number:check
  [:netblock4=8*n][netblock6=4*n]
  [:match=<value>][:nomatch=<value>]

```
counter:client_address:table=dha
        :limit=4:check
```

Elemi szűrési feltételek X.

- regexp:<subject>:pattern=regexp[:not=regexp]
  [:match=<value>][:nomatch=<value>]
  - client, client_name, client_address, helo_name, sender, recipient

```
regexp:client_address
        :pattern=/^192\.168\./
```

Elemi szűrési feltételek XI.

- filter:recipient|sender:table=user
  [:enable=policyname][:disable=policyname]
  [:default=<value>][:nohide]

```
filter:recipient:table=user
  :enable=auto_whitelist:default=dunno
```

- user táblában
  - **class**_name
  - **policy**_name0[,**policy**_name1...]

Elemi szűrési feltételek XII.

- user_list:recipient:table=tablename
  :lookup=sender[:type=blacklist]
  [:match=<value>][:nomatch=<value>]

```
user_list:recipient
 :table=user_whitelist
 :lookup=sender
```

Elemi szűrési feltételek XIII.

- Pszeudo szűrési feltételek:
  - and_group:begin[:default=<value>]
    and_group:end
  - or_group:begin[:default=<value>]
    or_group:end

```
or_group:begin
authenticated:sasl:match=reject:nomatch=dunno
regexp:client_address:pattern=/^192\.168\.0\./
or_group:end
```

Példák policy definíciókra I.

- Érvénytelen EHLO/HELO név ellenőrzés

```
policy_invalid_helo =
   invalid:helo
   501 [{$helo_name}]: EHLO/HELO name rejected
```

- Spamtrap-ba gyűjtött kliensek leveleinek eldobása

```
policy_spamtrap =
   blacklist:client:table=spamtrap
   discard Client caught by spamtrap
```

Példák policy definíciókra II.

- Greylisting automatikus fehérlistával

```
policy_greylist =
  lookup:client_address:table=greylist_white
        :match=dunno:nomatch=reject
  greylist:client:delay=4:whitelist=3
  401 Service is unavailable, try again later.
```

Policy és class a felhasználók felé

- novice user: class
  - cgi_novice_classes
  - full, expert, slave
- expert users: policy
  - cgi_expert_policies
- mark támogatás:
  - cgi_expert_policies_without_mark
  - daemon_mark_template =

    X-Postfilter: SPAM marked by {$lookup_class}

Felhasználói felületek

- postfilter.cgi
- captcha.cgi

pfadm

- admin interfész
  - pfadm help [command]
  - pfadm list|add|del|mod|search|upload|cleanup <object> <args>
  - object: user, cookie, greylist, captcha, throttle
  - object: user_list, lookup
  - IPv4/IPv6 netblock konverzió

Integrálás más rendszerekkel SASL (SMTP Auth) I.

- Postfix master.cf:

```
# submission port
  hostname:587 inet n – n - - smtpd
        -o smtpd_use_tls=yes
        -o smtpd_sasl_auth_enable=yes
        -o smtpd_tls_auth_only=yes
```

Integrálás más rendszerekkel: SASL (SMTP Auth) II.

- SASL: /usr/lib/sasl2/smtpd.conf

```
#
pwcheck_method: auxprop
auxprop_plugin: sql
mech_list: plain login
sql_engine: mysql
sql_hostnames|user|passwd|database:
sql_statement: select _passwd from user where
        _address = '%u@%r' and _passwd != ''
```

Integrálás más rendszerekkel: PAM (OpenVPN)

- server.conf:

```
# pwfile PAM module
plugin /usr/lib/openvpn-auth-pam.so openvpn
```

- PAM: /etc/pam.d/openvpn

```
auth required pam_mysql.so user=foo passwd=foo
            host=sqlhost db=postfilter table=user
            usercolumn=user._address
            passwdcolumn=user._passwd crypt=0
            [where user._passwd != '']
account required pam_permit.so
```

Integrálás más rendszerekkel: FreeRADIUS I.

- radiusd.conf:

```
modules {
..
   $INCLUDE ${confdir}/sql.conf
authorize {
..
   sql
session {
...
   sql
```

Integrálás más rendszerekkel: FreeRADIUS II.

- sql.conf:

```
sql {
    driver|server|login|password| = ...
    radius_db = “postfilter”
    authcheck_table = “user”
    authreply_table = “user”
    groupcheck_table = “user”
    groupreply_table = “user”
    usergroup_table = “user”
```

Integrálás más rendszerekkel: FreeRADIUS III.

```
...
sql_user_name = “%{User-Name}”
authorize_check_query = “SELECT _userid, \
  _address, 'Password', _passwd, '==' \
  FROM ${authcheck_table} \
  WHERE _address = '%{SQL-User-Name}' \
  and _passwd != '' \
  ORDER BY _userid”
```

Integrálás más rendszerekkel: FreeRADIUS IV.

```
...
authorize_reply_query = “SELECT _userid, \
  _address, 'foo', 'foo', '==' \
  FROM ${authreply_table} \
  WHERE _address = '_never_match'”
authorize_group_check_query = ...
authorize_group_reply_query = ...
```

Integrálás más rendszerekkel: Spamassassin

- doc/SPAMASSASSIN

Letöltési cím

http://www.kfki.hu/cnc/projekt/postfilter