

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 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

postfilterd

- Teljes értékű policy daemon Postfix-hez:
 - szintaktikai és DNS ellenőrzések
 - RBL, RHSBL listák
 - whitelist, blacklist, greylist. DHA
 - captcha kihívás (**completely automated public Turing test to tell computers and humans apart**)
 - 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
- `captcha.cgi`
 - captcha feladat teljesítéséhez
- `captcha-test.cgi`:
 - segéd CGI a captcha képek paramétereinek beállításához

SQL szerver

- Jelenleg csak mySQL támogatott
 - Egyszerű portálhatóság más adatbáziskezelőre
- “read-only” és “read-write” táblázatok
 - 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

- Konfiguráció két részben
- root.conf
 - minden szerveren ott kell lenni
 - minimális beállítások az SQL szerverekről
- main.conf
 - összes komponens minden beállítási paramétere
 - Postfix main.cf-hez hasonló szintaxis
 - Perl-re fordított és adatbázisban tárolt változat
- pfadm script

Postfilter szűrési beállításai

- Több réteg a maximális rugalmasság érdekében
 - Elemi szűrési feltételek és Postfix-szintű szűrési ítéletek
 - Szűrési policy-k
 - Szűrési osztályok

Postfix-szintű szűrési ítéletek

- permit [opcionális szöveg]
- deny [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

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

Elemi szűrési feltételek II.

- `rbl:client_address`
 `:domain=rbl.domain.name[:match=d.d.d.d]`
- `rhsbl:client_name|sender_domain`
 `:domain=rhsbl.domain.name[:match=d.d.d.d]`
- `unknown:client_name|helo_name|sender|recipient`
 `[:match=<value>][:nomatch=<value>]`

Elemi szűrési feltételek III.

- `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 IV.

- `update:<subject>:table=tablename`

`[:netblock=8|16|2432][: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:netblock=24`

- automatikus kivétellistára helyezés:

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

Elemi szűrési feltételek V.

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

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

Elemi szűrési feltételek VI.

- throttle:<subject>:count_max=number
:rcpt_max=number:quota_max=number
:time_period=number
 - sender, client_address, client_name, client,
sasl_username

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

Elemi szűrési feltételek VII.

- `counter:client_address:table=tablename`
 `:limit=number:time_period=number`
 `[:netblock=8|16|24|32]`
 `[:match=<value>][:nomatch=<value>]`

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

Elemi szűrési feltételek VIII.

- `counter:client_address:table=tablename`
 `:limit=number:check`
 `[:netblock=8|16|24|32]`
 `[:match=<value>][:nomatch=<value>]`

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

Elemi szűrési feltételek IX.

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

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

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>]`
 - `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`
 `[:match=<value>][:nomatch=<value>]`
`user_list:recipient`
 `:table=user_whitelist`
 `:lookup=sender`

Elemi szűrési feltételek XIII.

- Pszeudo szűrési feltételek:
 - and_group
 - or_group

Szűrési policy-k

- Elemi szűrési feltételek és ítéletek:

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

- AND kapcsolat az elemi feltételek negatív ítéletei között

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 =
```

```
    greylist:client:delay=4:white=3
```

```
    401 Service is unavailable, try again later.
```

```
policy_greylisted =
```

```
    whitelist:client:table=greylist_white
```

Szűrési osztályok

- Szűrési policy-kből

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

- OR kapcsolat a policy-k eredménye között

```
class_greylist = greylisted, greylist
```

postfilterd kiindulási pontok

- `daemon_default_class`
- `daemon_default_recipient_class`
- `daemon_default_end_of_data_class`

Demo

- `postfilter.cgi` felhasználói felület
- `captcha.cgi` felhasználói felület

Letöltési cím

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