# sieve-router

# Summary

sieve-router je SMTP proxy. Treba raditi kao komponenta mail sustava koja se integrira u Postfix MTA, i omogućiti sljedeću funkcionalnost:

* provjeru sadrzaja zaglavlja, bodyja, i envelope po: točnoj vrijednosti, regular expression matchu (ERE ili Posix RE ili PCRE) te kombinacije uvjeta (and, or, not)
* prihvaćanje, routanje ili odbacivanje poruke ovisno o tim uvjetima na različiti SMTP destination ili bacanje u smeće uz logiranje sadrzaja u .mbox ili Maildir
* podrška za različito routanje poruke u više kopija u slučaju da se na ulazu dobije poruka sa više od jednog RCPT TO

# Deliverables

Iskonu treba pripadati kompletni source kod. Stroga preferencija na implementaciju u Perl, Python ili drugom čestom skriptnom jeziku koji omogućava jednostavne izmjene po potrebi od strane administratora, osim ukoliko to ruši niže navedene performansne zahtjeve. Dozvoljena je uporaba open-source komponenti.

# Funkcijska specifikacija

smtp proxy treba izgledati kao TCP servis koji sluša na konfigurabilnoj IP adresi i portu, i raditi kao Postfix content\_filter[1]. Mailove treba prosljeđivati natrag MTA također na konfigurabilnoj IP adresi i portu. Proxy treba moći servirati barem 40-4000 zahtjeva istovremeno, sa podesivim limitom. Servis se treba moći pokretati pod običnim korisnikom, i raditi na bar jedan od ova dva načina:

* tipični Debian standalone servis koji se sam daemonizira, spremi pid file po /var/run/servicename.pid, i koristi syslog za logiranje (mail.\* ili local2.\* facility), ili kao
* servis pod DJB daemontoolsima (u foregroundu i log daje na stdout).

Log kod uspješno proslijeđene poruke treba sadržavati akciju ili niz akcija izvedenih nad porukom, message-id poruke, envelope from i to, interni queue id za korelaciju Postfix i sieve-filter logova. Log slati na syslog, podesivi syslog facility i po defaultu mail. Queue id može sadržavati npr. unix timestamp, process id klijentskog, neka jedinstvena vrijednost (npr. redni broj ulazne poruke koju je taj proces obradio) i redni broj primatelja ukoliko je poruku trebalo razdvojiti na više od jedne kopije, ili bilo kakvu drugu shemu. Bitno da se može pratiti tok za svaku kopiju poruke i svakog primatelja.

Prijedlog formata:

# dvije jednostavne poruke

2011-09-14T06:25:20 id=4E702CB0\_1337\_39\_1 f=<blah@example.com> t=<foo@example.org> action=pass

2011-09-14T06:25:20 id=4E702CB0\_1337\_40\_1 f=<glubglubglub@iskon.hr> t=<bar@example.com> action=pass

# poruka routana sa action route

2011-09-14T06:25:21 id=4E702CB1\_1337\_41\_1 f=<> t=<bedrockssvj@tcsn.net> action=route:mxout.iskon.hr

# poruka sa tri primatelja

2011-09-14T06:25:22 id=4E702CB2\_1337\_42\_1 f=<jelly@iskon.hr> t=<iskon.test@gmail.com> action=pass

2011-09-14T06:25:22 id=4E702CB2\_1337\_42\_2 f=<jelly@iskon.hr> t=<jelly@iskon.hr> action=route:127.0.0.1:10028,copyid=4E702CB2\_1360\_1\_1

2011-09-14T06:25:23 id=4E702CB2\_1337\_42\_3 f=<jelly@iskon.hr> t=<devnull@iskon.hr> action=discard

# poruka sa dvije akcije

2011-09-14T06:25:25 id=4E702CB5\_1338\_43\_1 f=<support@inet.hr> t=<naivec@yahoo.com> action=fileinto:spam-fake-support,discard

# kopija poruke sa tri primatelja u lokalnom queueu

2011-09-14T06:27:26 id=4E702CB2\_1360\_1\_1 f=<jelly@iskon.hr> t=<jelly@iskon.hr> action=route:127.0.0.1:10028\_(deferred:connection refused)

2011-09-14T06:32:28 id=4E702CB2\_1360\_1\_1 f=<jelly@iskon.hr> t=<jelly@iskon.hr> action=route:127.0.0.1:10028\_(250\_2.0.0\_Ok:\_queued\_as\_4C44B2E379B)

## Konfiguracijske datoteke

Primjer konfiguracijske datoteke /etc/sieve-router/sieve-router.conf:

# server stuff

# bind ip:port

listen = 127.0.0.1:10025

# default route for pass action

destination = 127.0.0.1:10026

# limit number of child processes

maxchildren = 100

# fileinto action destination, eg.

# fileinto "suspicious" would store mails into

# /opt/home/bccuser/Maildir/suspicious/ Maildir

mboxhome = /opt/home/bccuser/Maildir

mboxtype = Maildir # Maildir ili mbox

Točna sintaksa globalne konfiguracijske datoteke nije toliko bitna.

Primjer konfiguracijske datoteke za /etc/sieve-router/sieve-router.siv

# Discard if probable spam and suspect From

if allof (header :contains ["X-SpamTest-Status"] ["SPAM"],

header :contains "From" "inet.hr support") {

fileinto "spam-from-fake-support";

discard;

stop;

}

# Discard if probable spam and from domain "@dsl.iskon.hr"

if allof (header :contains ["X-SpamTest-Status"] ["SPAM"],

address :all :matches :comparator "i;ascii-casemap" ["from"]

["\*\*@dsl.iskon.hr"]) {

fileinto "spam-from-dsl";

discard;

stop;

}

# Route messages with any recipients in .hr to :10028

if envelope :any :matches "to" "\.hr$" {

route "127.0.0.1:10028";

stop;

}

# Route all DSN messages to mxout.iskon.hr

if envelope :all :is "from" "" {

route "mxout.iskon.hr";

stop;

}

# Drop all messages for this recipient

if envelope :any :is "to" "devnull@iskon.hr" {

discard;

stop;

}

## Ponašanje SMTP servisa

SMTP proxy treba poštivati uobičajena pravila SMTP poslužitelja, sa naglaskom na čuvanje poruka po svaku cijenu.

SMTP proxy propušta svaku poruku kroz sieve ili sličan sustav pravila nakon DATA dijela SMTP dijaloga.

Kada poruka ima više od jednog envelope primatelja, poruku treba interno razdvojiti i razmatrati Sieve pravila za svakog primatelja zasebno. Da bi se spriječilo višestruko slanje istom primatelju, ove poruke treba čuvati u lokalnom queueu. Queue mora biti perzistentan, ukratko, mail se ne smije gubiti. Kao odgovor prethodnom MTA dovoljno je proslijediti rezultat za prvog primatelja iz liste envelope-recipienata. Za ostale primatelje rezultati će se vidjeti u logu servisa, a poveznica je sieve-filter queue id.

Primjer:

\* Connect to localhost:10025 (sieve-filter):

220 localhost ESMTP sieve-filter 0.5; Wed, 14 Sep 2011 15:18:00 +0200

> EHLO localhost

250-Pleased to meet you

250-ENHANCEDSTATUSCODES

250-8BITMIME

250 PIPELINING

> MAIL FROM:<jelly@iskon.hr>

250 2.1.0 Sender Ok

> RCPT TO:<iskon.test@gmail.com>

250 2.1.5 Recipient Ok

> RCPT TO:<jelly@iskon.hr>

250 2.1.5 Recipient Ok

> RCPT TO:<devnull@iskon.hr>

250 2.1.5 Recipient Ok

> DATA

354 3.3.0 Enter mail, end with <CRLF>.<CRLF>

> From: jelly <jelly@iskon.hr>

> To: testna adresa na GMailu <iskon.test@gmail.com>

> Cc: Zoran Dzelajlija <jelly@iskon.hr>,

> devnull@iskon.hr

> Subject: proba

> Date: Wed, 14 Sep 2011 15:27:32 +0200

> Message-ID: <1316006871.1337@mail.iskon.hr>

>

> proba.

> .

250 2.0.0 Ok id=4E702CB2\_1337\_42\_1 pass (2.0.0 Ok: queued as B96748A037 )

> QUIT

221 2.0.0 Good bye

\* Connection closed by foreign host.

Ukoliko dođe do neplanirane greške u tijeku rada nakon HELO/EHLO, MAIL FROM, RCPT TO ili DATA SMTP naredbe, filter treba SMTP klijentu vratiti adekvatnu 4xx poruku o grešci i zatvoriti sesiju.

Ukoliko je finalna akcija za primatelja pass, bilo eksplicitni ili implicitni, sieve-router treba proslijediti poruku sljedećem SMTP serveru u nizu. Tek nakon primljenog 2xx odgovora od odredišnog smtp servera sieve-router treba izvornom SMTP klijentu odgovoriti

250 2.0.0 Ok: id=4E702CB5\_1337\_666\_1 pass (odgovor odredišnog smtp servera)

i očekivati dovršenje SMTP sesije.

Ukoliko je finalna akcija za primatelja route, sieve-router treba proslijediti poruku sljedećem SMTP serveru u nizu. Tek nakon primljenog 2xx odgovora od odredišnog smtp servera sieve-router treba izvornom SMTP klijentu odgovoriti

250 2.0.0 Ok: id=4E702CB5\_1337\_666\_1 route "routeparam" (odgovor odredišnog smtp servera)

i očekivati dovršenje SMTP sesije.

Ukoliko za pass ili route akciju odredišni server timeouta, ili javi 4xx ili 5xx odgovor, izvornom SMTP klijentu odgovoriti privremenom greškom, npr:

450 4.4.1 Deferred: id=4E702CB5\_1337\_666\_1 remote ip.ad.re.ss:port timed out after DATA

450 4.4.1 Deferred: id=4E702CB5\_1337\_666\_1 remote ip.ad.re.ss:port timed out after RCPT TO

450 4.4.1 Deferred: id=4E702CB5\_1337\_666\_1 remote ip.ad.re.ss:port said odgovor-odredišnog-smtp-servera

U log umjesto action upisati tempfail= i akciju:

2011-09-14T06:25:25 id=4E702CB5\_1337\_666\_1 f=<pomoc@iskon.hr> t=<hmha@example.com> tempfail=route:ip.ad.re.ss:port

Ukoliko je finalna akcija discard, kao odgovor na DATA sieve-router treba SMTP klijentu javiti sljedeće:

250 2.0.0 Ok: id=4E702CB5\_1337\_666\_1 discarded

U log zapisati

2011-09-14T06:25:25 id=4E702CB5\_1337\_666\_1 f=<support@inet.hr> t=<hmha@example.com> action=discard

Ukoliko je akciji discard prethodila jedna ili više akcija fileinto, sieve-router treba kao odgovor na DATA SMTP klijentu javiti sljedeće:

250 2.0.0 Ok: id=4E702CB5\_1337\_666\_1 fileinto "mboxparam", discarded

250 2.0.0 Ok: id 4E702CB5\_1337\_666\_1 fileinto "mboxparam", fileinto "mboxparam2", discarded

Log:

2011-09-14T06:25:25 id=4E702CB5\_1337\_666\_1 f=<support@inet.hr> t=<naivec@example.com> action=fileinto:"spam-fake-support",discard

# Filter

Jezik za definiciju pravila za provjeru i finalnu akciju idealno neka bude podskup Sieve jezika (http://tools.ietf.org/html/rfc5228/) uz ekstenziju za provjeru tijela poruke (RFC 5173, http://tools.ietf.org/html/rfc5173/), i custom Action ekstenziju za routanje maila na proizvoljni SMTP server:port.

## Testovi koji MORAJU biti implementirani iz RFC5228:

5.1. Test address ..............................................26

5.2. Test allof ................................................27

5.3. Test anyof ................................................27

5.4. Test envelope .............................................27

5.5. Test exists ...............................................28

5.6. Test false ................................................28

5.7. Test header ...............................................29

5.8. Test not ..................................................29

5.9. Test size .................................................29

5.10. Test true ................................................30

## Akcije koje MORAJU biti implementirane:

4.1. Action fileinto ...........................................23

4.3. Action keep ...............................................24

4.4. Action discard ............................................25

## Sintaksa za kontrolu toka koja MORA biti implementirana:

3.1. Control if ................................................21

3.3. Control stop ..............................................22

## Test iz RFC5173:

4. Test body

## Odredišna putanja za 4.1. Action fileinto

Putanju za spremanje poruka računati na sljedeći način: umjesto standardnih putanja za korisnički inbox, fileinto treba foldere kreirati i zapisivati u direktoriju specificiranom u "mboxhome" varijabli u glavnoj konfogiuracijskoj datoteci.

Primjer. Ako u sieve-router.siv Sieve konfiguraciji piše

#

if envelope :all :matches :comparator "i;ascii-casemap" ["from"]

["\*\*@dsl.iskon.hr"]) {

fileinto "spam-from-dsl";

discard;

stop;

}

i u sieve-router.conf piše

mboxhome = /var/lib/sieve-filter/logs

mboxtype = Maildir

U tom slučaju bi poruke kojima je u envelope-from pisalo npr. [notspam@dsl.iskon.hr](mailto:notspam@dsl.iskon.hr)

trebaju biti spremljene u Maildir format folder

/var/lib/sieve-filter/logs/spam-from-dsl/

Servis prilikom pokretanja treba provjeriti ima li prava pisati u mboxhome i u slučaju greške istu treba logirati i ne pokrenuti servis.

## Custom akcija route

Ovo je nova akcija, nedefinirana u RFC5228 ni 5173:

Action route

route <string>;

obavezni string parametar treba podrzavati format:

( ip.ad.dre.ss | hostname ) [:port]

Akcija route za navedenu poruku umjesto globalne route postavke upućuje sieve-router da šalje poruku na specificirani SMTP server i port. Ukoliko je zadan hostname, treba resolvati A ili AAAA zapis, nikako ne MX zapis. Nije nužno implementirati interni caching sustav za zapise, na serveru se vrti lokalni dns cache.

Primjer:

# routaj sve poruke za primatelje u .hr na :10028

if envelope :any :matches "to" "\.hr$" {

route "127.0.0.1:10028";

stop;

}

# routaj sve DSN poruke na mxout.iskon.hr

if envelope :all :is "from" "" {

route "mxout.iskon.hr";

stop;

}

Reference:

[1] http://www.postfix.org/FILTER\_README.html

[2] RFC 5228 http://tools.ietf.org/html/rfc5228/

[3] RFC 5173 http://tools.ietf.org/html/rfc5173/