

Admins - Anomalie #5662

Tous les mails en provenance de la VM mail ne sont pas signés par DKIM

22/11/2021 11:52 - François Poulain

Statut:	Fermé	Début:	22/11/2021
Priorité:	Normale	Echéance:	
Assigné à:	François Poulain	% réalisé:	0%
Catégorie:		Temps estimé:	0.00 heure
Version cible:	Novembre 2021	Temps passé:	0.00 heure
Difficulté:	2 Facile		

Description

Le milter rspamd ne semble pas signer ce qui n'est pas en relay.

Ce qui est envoyé en cli depuis lamp est signé.
Ce qui est envoyé en cli depuis mail n'est pas signé.
Ce qui est envoyé en relayhost depuis fred n'est pas signé.

Je soupçonne que l'interco postfix rspamd est court-circuitée en local.

Reste à comprendre pour le mail de fred. Il passe bien par rspamd pourtant.

```
### conf.d/60-anti-spam.conf

##
## Rspamd
##

smtpd_milters = inet:localhost:11332
milter_protocol = 6
milter_default_action = accept
```

Historique

#1 - 22/11/2021 12:07 - François Poulain

La doc de postfix indique que le protocole Milter a été initialement développé pour filtrer les messages indésirables arrivant du réseau. Pour les messages qui n'arrivent pas via le serveur smtpd(8), Postfix utilise les applications Milter qui sont listées avec le paramètre `cleanup_milters`.

Ça explique la différence entre les deux premiers tests.

https://postfix.traduc.org/index.php/MILTER_README.html

#2 - 22/11/2021 12:12 - François Poulain

Avec une version plus récente de la doc ça exige `non_smtpd_milters`. :)

#3 - 22/11/2021 12:29 - François Poulain

Ça marche. Reste à comprendre pk madix contourne le milter.

```
Nov 22 12:26:10 mail postfix/submission/smtpd[1222]: connect from ...
Nov 22 12:26:10 mail postfix/submission/smtpd[1222]: Anonymous TLS connection established from ...: TLSv1.3 with cipher TLS_AES_256_GCM_SHA384 (256/256 bits) key-exchange X25519 server-signature RSA-PSS (4096 bits) server-digest SHA256
Nov 22 12:26:10 mail postfix/submission/smtpd[1222]: CD9A3CC1: client=..., sasl_method=LOGIN, sasl_username=mail
Nov 22 12:26:10 mail postfix/cleanup[1203]: CD9A3CC1: message-id=<87sfvo77ou.fsf@april.org>
Nov 22 12:26:11 mail postfix/qmgr[1126]: CD9A3CC1: from=<fcouchet@april.org>, size=1188, nrcpt=1 (queue active)
Nov 22 12:26:12 mail postfix/smtp[1225]: CD9A3CC1: to=<fpoulain@metrodoire.fr>, relay=spool.mail.gandi.net[217.70.178.1]:25, delay=1.5, delays=0.64/0.02/0.71/0.16, dsn=2.0.0, status=sent (250 2.0.0 Ok: queued as 39A1FAC096C)
Nov 22 12:26:12 mail postfix/qmgr[1126]: CD9A3CC1: removed
```

#4 - 22/11/2021 12:34 - François Poulain

Non il ne le contourne pas.

```
2021-11-22 12:26:10 #1478(rspamd_proxy) <a2f022>; proxy; proxy_accept_socket: accepted milter connection from :::1 port 39686
2021-11-22 12:26:10 #1478(rspamd_proxy) <a2f022>; milter; rspamd_milter_process_command: got connection from ...:60486
2021-11-22 12:26:10 #1478(rspamd_proxy) <a2f022>; proxy; rspamd_message_parse: loaded message; id: <87sfvo77ou.fsf@april.org>; queue-id: <CD9A3CC1>; size: 722; checksum: <28bb585131d9979dca82375abf8ed2eb>
2021-11-22 12:26:10 #1478(rspamd_proxy) <a2f022>; proxy; rspamd_mime_part_detect_language: detected part language: fr
2021-11-22 12:26:10 #1478(rspamd_proxy) <a2f022>; lua; greylist.lua:204: skip greylisting for local networks and/or authorized users
2021-11-22 12:26:10 #1478(rspamd_proxy) <a2f022>; proxy; dkim_symbol_callback: skip DKIM checks for local networks and authorized users
2021-11-22 12:26:10 #1478(rspamd_proxy) <a2f022>; lua; spf.lua:185: skip SPF checks for local networks and authorized users
2021-11-22 12:26:10 #1478(rspamd_proxy) <a2f022>; lua; dmarc.lua:596: skip DMARC checks as either SPF or DKIM were not checked
2021-11-22 12:26:10 #1478(rspamd_proxy) <a2f022>; lua; once_received.lua:99: Skipping once_received for authenticated user or local network
2021-11-22 12:26:11 #1478(rspamd_proxy) <a2f022>; lua; greylist.lua:318: Score too low - skip greylisting
2021-11-22 12:26:11 #1478(rspamd_proxy) <a2f022>; proxy; rspamd_task_process: skip learning: <87sfvo77ou.fsf@april.org> is skipped for bayes classifier: already in class ham; probability 99.96%
2021-11-22 12:26:11 #1478(rspamd_proxy) <a2f022>; lua; neural.lua:311: skip ham sample to keep spam/ham balance; probability 0.8; 2 spam and 9 ham vectors stored
2021-11-22 12:26:11 #1478(rspamd_proxy) <a2f022>; proxy; rspamd_task_write_log: id: <87sfvo77ou.fsf@april.org>, qid: <CD9A3CC1>, ip: ..., user: mad, from: <fcouchet@april.org>, (default: F (no action): [-3.09/15.00] [BAYES_HAM(-2.99){99.96%};],MIME_GOOD(-0.10){text/plain};,ARC_NA(0.00){},ASN(0.00){asn:3215, ipnet:81.249.128.0/17, country:FR};,FROM_EQ_ENVFROM(0.00){},FROM_HAS_DN(0.00){},HAS_ORG_HEADER(0.00){},MID_RHS_MATCH_FROM(0.00){},MIME_TRACE(0.00){0:+};,NEURAL_HAM(-0.00){-1.000};,RCPT_COUNT_ONE(0.00){1};,RCVD_COUNT_ZERO(0.00){0};,TO_DN_ALL(0.00){},TO_MATCH_ENVRCPT_ALL(0.00){}), len: 722, time: 403.450ms, dns req: 8, digest: <28bb585131d9979dca82375abf8ed2eb>, rcpts: <fpoulain@metrodoire.fr>, mime_rcpts: <fpoulain@metrodoire.fr>
2021-11-22 12:26:11 #1478(rspamd_proxy) <a2f022>; proxy; rspamd_protocol_http_reply: regexp statistics: 0 pcre regexps scanned, 5 regexps matched, 174 regexps total, 53 regexps cached, 0B scanned using pcre, 1.28KiB scanned total
```

Ceci me déplaît car ce n'est pas ce qui est censé être en conf.

```
2021-11-22 12:26:10 #1478(rspamd_proxy) <a2f022>; proxy; dkim_symbol_callback: skip DKIM checks for local networks and authorized users
```

```
modules.d/dkim_signing.conf: sign_authenticated = true;
modules.d/dkim_signing.conf: sign_local = true;
```

#5 - 22/11/2021 12:42 - François Poulain

A priori c'est ce bug : <https://github.com/rspamd/rspamd/issues/1593>

<https://rspamd.com/rmilter/configuration.html>

strict_auth: strict checks for mails from authenticated senders (if it is no then messages originated from authenticated users and our_networks are NOT checked - that's a default value)

#6 - 22/11/2021 13:51 - François Poulain

Non je confonds signature et vérification. Rollback. La conf actuelle pour la signature dkim :

```
dkim_signing {
    use_esld = true;
    allow_hdrfrom_mismatch = false;
    selector = "dkim";
    symbol = "DKIM_SIGNED";
    allow_envfrom_empty = true;
    try_fallback = true;
    sign_authenticated = true;
    sign_networks [
        "127.2.4.7",
    ]
    use_redis = false;
    allow_username_mismatch = false;
    sign_local = true;
    key_prefix = "DKIM_KEYS";
    use_domain = "header";
    allow_hdrfrom_multiple = false;
```

}

#7 - 22/11/2021 13:55 - François Poulain

Ce message ci est signé mais le log de rspamd ne le mentionne pas (sauf coté score).

```
2021-11-22 12:11:53 #1478(rspamd_proxy) <249712>; proxy; proxy_accept_socket: accepted milter connection from
::1 port 38802
2021-11-22 12:11:53 #1478(rspamd_proxy) <249712>; milter; rspamd_milter_process_command: got connection from 1
72.16.0.11:49580
2021-11-22 12:11:53 #1478(rspamd_proxy) <249712>; proxy; rspamd_message_parse: loaded message; id: <2021112211
1151.9919E362@lamp.april.org>; queue-id: <0EE99C74>; size: 376; checksum: <2fac72d84ec879620eff2ec8d9ebebee>
2021-11-22 12:11:53 #1478(rspamd_proxy) <249712>; lua; greylist.lua:204: skip greylisting for local networks a
nd/or authorized users
2021-11-22 12:11:53 #1478(rspamd_proxy) <249712>; proxy; dkim_symbol_callback: skip DKIM checks for local netw
orks and authorized users
2021-11-22 12:11:53 #1478(rspamd_proxy) <249712>; lua; spf.lua:185: skip SPF checks for local networks and aut
horized users
2021-11-22 12:11:53 #1478(rspamd_proxy) <249712>; lua; dmarc.lua:596: skip DMARC checks as either SPF or DKIM
were not checked
2021-11-22 12:11:53 #1478(rspamd_proxy) <249712>; lua; once_received.lua:99: Skipping once_received for authen
ticated user or local network
2021-11-22 12:11:53 #1478(rspamd_proxy) <249712>; proxy; bayes_classify: skipped classification as there are n
o text tokens. Total tokens: 12
2021-11-22 12:11:53 #1478(rspamd_proxy) <249712>; lua; greylist.lua:318: Score too low - skip greylisting
2021-11-22 12:11:53 #1478(rspamd_proxy) <249712>; proxy; rspamd_task_write_log: id: <20211122111151.9919E362@l
amp.april.org>, qid: <0EE99C74>, ip: 172.16.0.11, from: <fpoulain@april.org>, (default: F (no action): [-0.10/
15.00] [MIME_GOOD(-0.10){text/plain;},ARC_NA(0.00){},DKIM_SIGNED(0.00){april.org:s=dkim;},FROM_EQ_ENVFROM(0.00
){},FROM_NO_DN(0.00){},MID_RHS_MATCH_FROMTLD(0.00){},MIME_TRACE(0.00){0:+;},NEURAL_HAM(-0.00){-1.000;},RCPT_CO
UNT_ONE(0.00){1;},RCVD_COUNT_ZERO(0.00){0;},TO_DN_NONE(0.00){},TO_MATCH_ENVRCPT_ALL(0.00){}]), len: 376, time:
3.186ms, dns req: 0, digest: <2fac72d84ec879620eff2ec8d9ebebee>, rcpts: <fpoulain@metrodoire.fr>, mime_rcpts:
<fpoulain@metrodoire.fr>
2021-11-22 12:11:53 #1478(rspamd_proxy) <249712>; proxy; rspamd_protocol_http_reply: regexp statistics: 0 pcre
regexps scanned, 1 regexps matched, 174 regexps total, 61 regexps cached, 0B scanned using pcre, 432B scanned
total
```

#8 - 22/11/2021 14:14 - François Poulain

Avec verbose logs.

Un mail signé :

```
2021-11-22 14:06:33 #10906(rspamd_proxy) <72be62>; dkim_signing; lua_dkim_tools.lua:166: mail is from local ad
dress
2021-11-22 14:06:33 #10906(rspamd_proxy) <72be62>; dkim_signing; lua_dkim_tools.lua:382: use domain(header) fo
r signature: april.org
2021-11-22 14:06:33 #10906(rspamd_proxy) <72be62>; dkim_signing; lua_dkim_tools.lua:402: final DKIM domain: ap
ril.org
2021-11-22 14:06:33 #10906(rspamd_proxy) <72be62>; dkim_signing; lua_dkim_tools.lua:46: add key "/var/lib/rspa
md/dkim/$domain.$selector.key" using default path
2021-11-22 14:06:33 #10906(rspamd_proxy) <72be62>; dkim_signing; lua_dkim_tools.lua:51: set selector to "dkim"
using default selector
2021-11-22 14:06:33 #10906(rspamd_proxy) <72be62>; dkim_signing; lua_dkim_tools.lua:51: set domain to "april.o
rg" using dkim_domain
2021-11-22 14:06:33 #10906(rspamd_proxy) <72be62>; dkim_signing; dkim_signing.lua:128: using key "/var/lib/rsp
amd/dkim/april.org.dkim.key", use selector "dkim" for domain "april.org"
```

Un mail pas signé :

```
2021-11-22 14:07:17 #10906(rspamd_proxy) <0d89e1>; dkim_signing; lua_dkim_tools.lua:160: user is authenticated
2021-11-22 14:07:17 #10906(rspamd_proxy) <0d89e1>; dkim_signing; lua_dkim_tools.lua:382: use domain(header) fo
r signature: april.org
2021-11-22 14:07:17 #10906(rspamd_proxy) <0d89e1>; dkim_signing; lua_dkim_tools.lua:402: final DKIM domain: ap
ril.org
2021-11-22 14:07:17 #10906(rspamd_proxy) <0d89e1>; dkim_signing; lua_dkim_tools.lua:422: couldnt find domain i
n username
```

Le code concerné est

```
if auser and not settings.allow_username_mismatch then
  if not udom then
    lua_util.debugm(N, task, 'couldnt find domain in username')
```

```
    return false, {}
end
if settings.use_esld then
    udom = rspamd_util.get_tld(udom)
end
if udom ~= dkim_domain then
    lua_util.debugm(N, task, 'user domain mismatch')
    return false, {}
end
end
end
```

Je suppose est que le soucis est que nos users sont ivanni, fcouchet et n'ont pas le domaine inclut.

#9 - 22/11/2021 14:16 - François Poulain

Finalement l'astuce va être de mettre `allow_username_mismatch = false;`

```
# If true, username does not need to contain matching domain
allow_username_mismatch = false;
```

#10 - 22/11/2021 14:39 - François Poulain

- Statut changé de Nouveau à Résolu
- Assigné à mis à François Poulain
- Version cible changé de Backlog à Novembre 2021

#11 - 22/11/2021 14:48 - François Poulain

J'ai partagé nos investigations ici : <https://github.com/rspamd/rspamd/issues/1593#issuecomment-975540515>

#12 - 24/11/2021 21:15 - Quentin Gibeaux

- Statut changé de Résolu à Fermé