Regles mfilter pour Free.fr (3/4)

Tutoriel non officiel pour mfilter de Free.fr.

Troisieme partie : mfilter, exemples prêt à l'emploi

Avertissement : cette page n'est pas officielle, il est recommandé de n'utiliser que des règles simples, de tester vos filtres, et d'évacuer les messages indésirables vers un répertoire créé a cet usage, car les destructions sont irréversibles.
Il est bien entendu que vous demeurez seul(e) responsable des filtrages que vous mettez en oeuvre, il vaut mieux ne rien faire, que de programmer n'importe quoi.

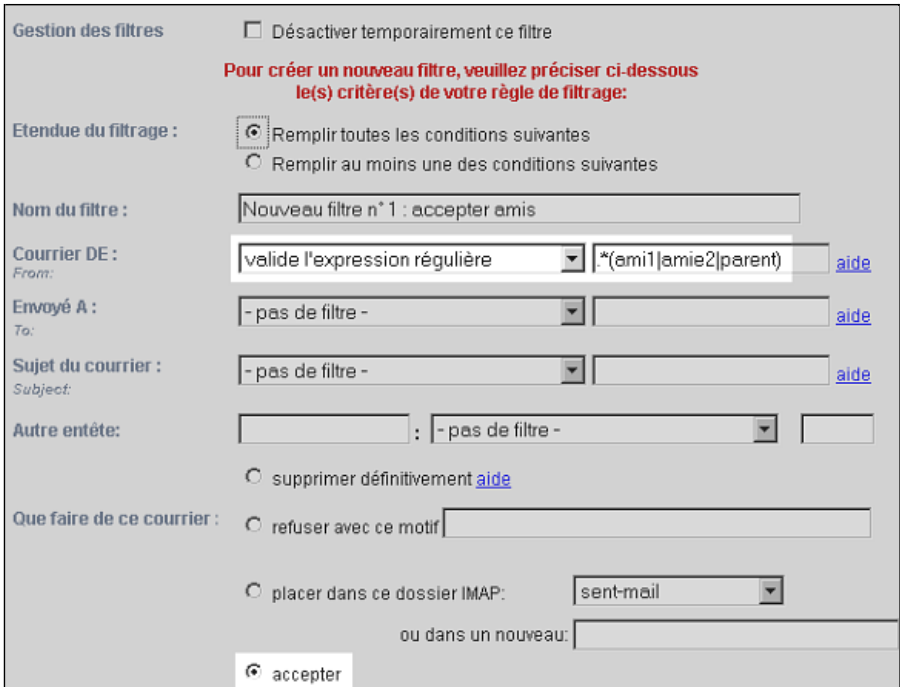
---

3. Exemples

3.A - Accepter les messages de mes amis

Principe : je veux accepter les expéditeurs qui ont les adresses : ami1@serveur.gt, amie2@domaine.ko et parent@maison.do

c'est un filtrage sur l'expéditeur(s) avec expression régulière



- figure d'écran : filtre, accepter les amis (ancienne version) -

Remplir au moins une des conditions suivantes

> Courrier DE : **valide l'expression régulière** **.***(ami1|amie2|parent)
> Que faire de ce courrier : **accepter** (cocher le rond blanc en face d'accepter) - autres actions

Notes :

- remplacer ami1, amie2, parent... par les noms qui conviennent.
- s'il y a de la place, on peut rédiger : **.***(ami1|amie2|parent)**@**
- inutile de saisir @serveur, la probabilité est faible, qu'un spam arrive avec exactement ami1 comme nom d'expéditeur, et surtout , il n'y a pas assez de place pour tout écrire. Par contre les messages venant de p**ami1** ou de gr**ami1**2 seront acceptés.
- noter l'emploi de | (sur PC, touche **AltGr** et **6** en meme temps) qui signifie OU, le message est accepté s'il vient de ami1@.... OU de parent@..... OU de...
- un bug d'ancrage oblige à écrire **.***(ami1|amie2|parent) . [*merci à Jacques*] - si l'on écrit ami1|amie2|parent alors "ami1 de free" est filtré, tandis que "mon ami1 de free" n'est pas filtré. Ce bug d'ancrage concerne toutes les entetes (to, from, received...), et comporte d'autres anomalies...

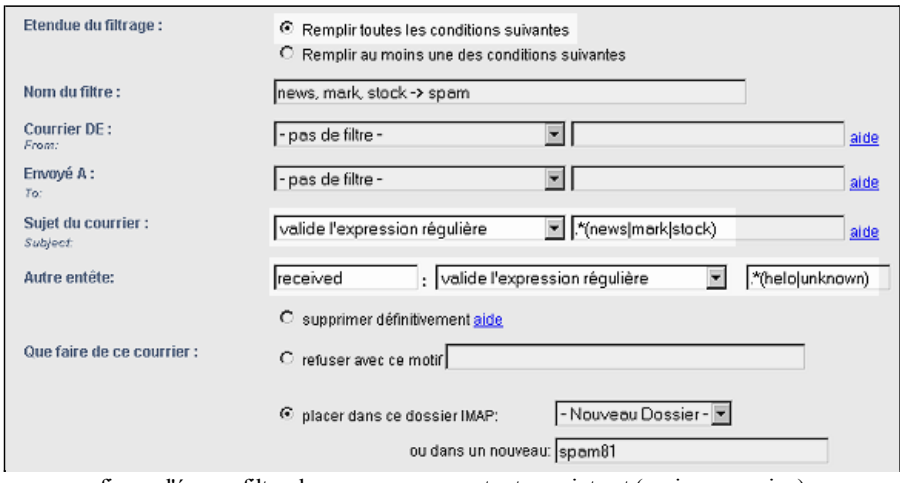
  - placer cette règle en premier, en utilisant les boutons sur le coté : faire remonter la règle en cliquant sur +1 ou +10.

retour haut de page

3.B - Filtrer les messages suspects ou sans interêt

Principe : refuser les messages avec mot clé. Les mots clé choisis seront typique de sujets qui ne vous interessent pas, comme des mots anglais (si vous n'attendez pas de correspondance en anglais) ou des mots typiques, comme par exemple, newsletter, stock, market, failure...

C'est un filtrage sur le sujet du message, avec expression régulière et mots-clé.



- figure d'écran : filtrer les messages suspects et sans interet (ancienne version) -

Remplir toutes les conditions suivantes

> Sujet du courrier : **valide l'expression régulière** **.***(newsl|mark|stock)
> Autre entête : Received **valide l'expression régulière** **.***(helo|unknown)
> Que faire de ce courrier : **placer dans ce dossier IMAP** - autres actions

Note:

- Il y a aussi des mots clé typiques présents dans les messages émis par intrusion (unknown, HELO -> voir la partie perfectionnement), et les messages qui ne contiennent pas d'expéditeur.
- received, helo peuvent etre en minuscules ou majuscules (mfilter insensible a la casse)
- la présence de HELO dans received n'est pas forcément une caractéristique d'un spam.
- **mark** va filtrer **mark**et, **mark**eting, Dane**mark**... (dans le sujet)
- dans cet exemple, le dossier IMAP 'spam81' est créé en meme temps que la règle.
- attention, ne pas écrire sans parenthèses, NI utiliser des mots réservés comme **from|invoked** (bug: dans cette situation, les mots *from* et *invoked* sont recherchés dans

toutes les entêtes et le message a de fortes chances d'être filtré à tort puisque ces mots existent)

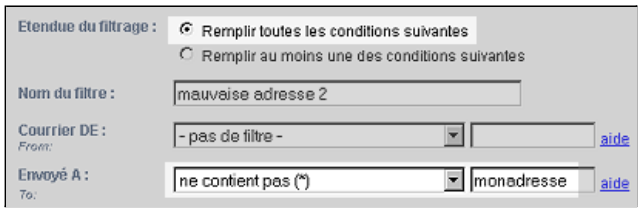
retour haut de page

3.C - Filtrer les messages qui ne me sont pas destinés

Principe : je refuse les messages qui ne me sont pas destinés, qui n'ont pas mon adresse dans l'entete **to** (Envoyé A).

voir aussi le filtre antispam de free.fr "les mails où je suis en copie cachée"

C'est un filtrage sur le destinataire du message.



- figure d'écran : refuser les messages qui ne me sont pas destinés -

Remplir **toutes** les conditions suivantes :

Envoyé A (To) : **ne contient pas** (*) monadresse (on peut mettre adresse@free.fr)
Que faire de ce courrier : **placer dans ce dossier IMAP** spam - autres actions

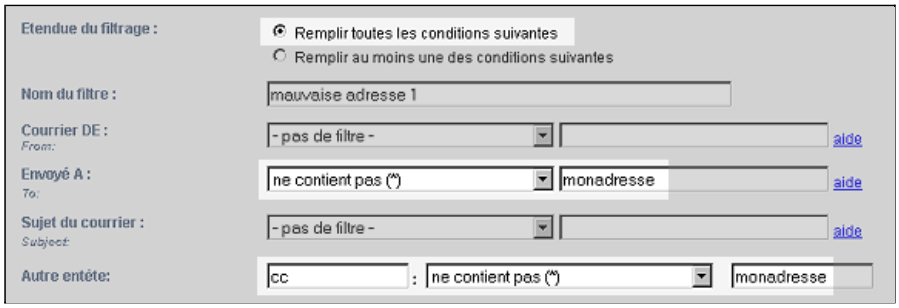
Notes :

(*) rappelle qu'il faut nécessairement choisir "Remplir **toutes** les conditions suivantes"; il ne sera pas possible d'ajouter d'autres règles dans ce filtre.

- créer le dossier "spam" dans imap, s'il n'existe pas (ou un dossier avec un autre nom).
- l'entête **bcc** n'apparait pas dans les en-tetes de message.
- ne teste pas l'entête **cc** (copie conforme)

Variante :

ajouter la règle pour **cc** :
Autre entete : **cc** **ne contient pas** (*) monadresse (on peut mettre adresse@free.fr)



- figure d'écran : refuser les messages qui ne me sont pas destinés ni en **to**, ni en **cc** -

important : pour que ce filtre fonctionne, il faut que l'entête **cc** soit présente dans le message qui arrive, sinon le filtre est ignoré.

Combinaison de filtres qui ne fonctionne pas correctement :

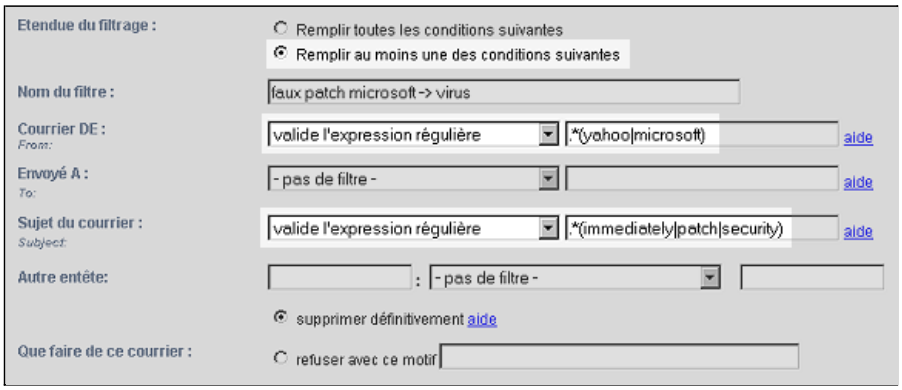
- en premier un filtre avec deux règles qui testent **to** et **cc** (rejet si mon adresse n'est ni dans **to** ni dans **cc**; regle ignorée si un des deux champ **to** ou/et **cc** manque)
- puis juste après, un second filtre qui teste **to** seulement (au cas ou le premier filtre serait ignoré par manque de **cc**) =>**n'est pas correct** car, si mon adresse n'est pas dans **to**, je ne peux pas détruire car je n'ai pas encore testé **cc** qui existe peut-etre et contient peut-etre mon adresse (*merci a Phil pour avoir signalé cette erreur - 3 juin 2004*)
- et eventuellement juste après un troisieme filtre qui teste **cc** seulement (rares cas de messages en **cc** sans **to**) => meme remarque

retour haut de page

3.D - Filtrer les messages des messageries gratuites

Principe : je rejette tous les expéditeurs provenant de yahoo, microsoft, gawab, et je rejette les messages avec virus connus, dont le sujet contient les mots immediately, patch, security...

C'est un filtrage sur l'expéditeur et le sujet (deux règles), avec expression régulière



- figure d'écran : filtrer les messageries gratuites -

Remplir au moins une des conditions suivantes

> Courrier DE : **valide l'expression régulière** .*(yahoo|microsoft)
> Sujet du courrier : **valide l'expression régulière** .*(immediately|patch|security)
> Que faire de ce courrier : **supprimer définitivement** - autres actions

Notes :

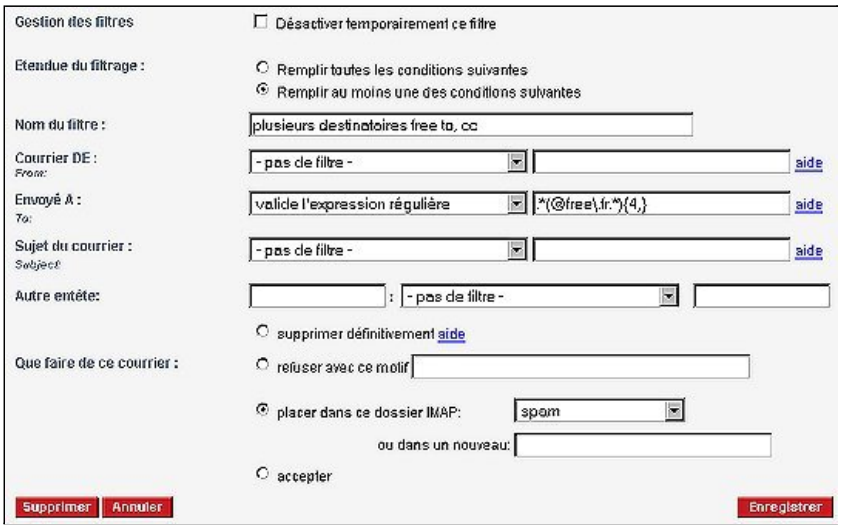
- le filtre sur le patch est utile si vous recevez fréquemment ce type de message.
- attention à vos amis qui utilisent ces messageries gratuites, il faut bien mettre un filtre qui accepte leurs adresses, filtre à placer en toute première position (c'est important). Eventuellement indiquer dans le message de rejet, pourquoi cela a été rejeté.
- je sais que Microsoft n'envoie jamais de patch, donc je supprime définitivement les mesages qui viennent de Microsoft OU qui proposent un patch de sécurité.

retour haut de page

3.E - Filtrer les mailings, directs (to) ou en copie (cc)

Principe : il y a fréquemment des spams destinés **à plusieurs emails free.fr** en meme temps; je filtre donc ces emails qui trahissent un spam qui travaille avec une base de données ayant ses adresses classées par serveur.

C'est un filtrage sur le destinataire du message, avec expression régulière.



- figure d'écran : filtrer les mailings -

Remplir au moins une des conditions suivantes :

> Envoyé A : **valide l'expression régulière** .*(@free\.fr.*){4,}
> Que faire de ce courrier : **placer dans ce dossier IMAP** spam - autres actions
>
> Ce filtre détecte les messages envoyés a 4, 5, ou plus destinataires **to** @free.fr

Notes :

- ajouter la même règle pour **cc**.
- noter que le filtre est ignoré si une des en-tete a tester est absente du message testé.
- il est possible de diminuer le seuil a 3 ou 2.
- a adapter si le spam est envoyé a d'autres serveurs que free.fr ce qui peut arriver à l'avenir.

- la syntaxe sur mfilter de free.fr : pour filtrer **4 ou plus** utiliser {4,} ou {4} sans virgule.
- ne fonctionne évidemment pas sur bcc, qui n'apparait jamais dans les entêtes.
- *d'après une idée de Jacques : merci !*

Variantes :

- (.*@free\.fr){4,}
- ([^@]+@free\.fr){4} pour filtrer les messages avec 4 destinataires @free consécutifs, ce qui distingue les spams d'un faire-part
- Pour filtrer les messages avec au moins 10 adresses en Cc (n'importe quels FAI) :
  Envoyé A : **valide l'expression régulière** ([^@]+@){10}

retour haut de page

3.F - Filtrer les faux rejets MAILER-DAEMON

Principe : conserver les rejets des messages que j'ai envoyés, pour cause d'erreur (mauvaise adresse), mais détruire les envois de virus.

C'est un filtrage sur l'entête "return-path".

Remplir au moins une des conditions suivantes :

> autre entête - return-path : **contient** < >
> Que faire de ce courrier : **placer dans ce dossier IMAP** rejet - autres actions

Notes :

- si quelqu'un / un virus a usurpé mon adresse, je vais recevoir le message de rejet d'un message que je n'ai jamais envoyé, parce que le Mailer-daemon croit que je suis l'epéditeur (alors que c'est un spammeur / virus qui s'est fait passer pour moi)

retour haut de page

3.G - Accepter les messages avec un code (contraignant)

Principe : j'indique à mes amis, qu'il faut mettre un code (un mot clé comme 1234) dans le **sujet** de leur message (de préférence à la fin). Je rejette les messages qui n'ont pas ce code.
Ceux qui utilisent le formulaire de free **form2mail.pl** sur leur site, peuvent filtrer sur tout ou partie du sujet du message.

Remplir au moins une des conditions suivantes :

> Sujet du courrier : **contient** 1234
> Que faire de ce courrier : **accepter** - autres actions

Notes :

- remplacer 1234 par le mot clé qui vous convient. Cela aurait très bien pu etre patron, papy ou belle-maman.
- placer cette règle dans les premières places de la liste des filtres (c'est important).
- indiquer au correspondant qu'il doit mettre le mot "1234", ou patron, papy... dans le sujet de son message. Très contraignant !
- élimine ceux qui ne connaissent pas le code, ou se trompent.
- cette règle peut etre ajoutée au filtre précédent.

3.H - Filtrer les messages sans expéditeur (inefficace)

Principe : refuser les messages sans expéditeur (le filtre précédent concernait le destinataire).

Remplir au moins une des conditions suivantes

> Courrier DE : **est vide**
> Que faire de ce courrier : **placer dans ce dossier IMAP** spam - autres actions

Note :

- le cas ou cette entête DE (from) manque n'a pas été testé. La règle est vraisemblablement ignorée en absence de l'entete DE dans le message à traiter, donc ce filtre présente peu d'intérêt.

3.J - Filtrer les messages sans date (peu efficace)

Principe : refuser les messages sans date, ou aux dates erronées.

Remplir **toutes** les conditions suivantes

Autre entete : date : **ne contient pas (*)** 200
Que faire de ce courrier : **placer dans ce dossier IMAP** spam

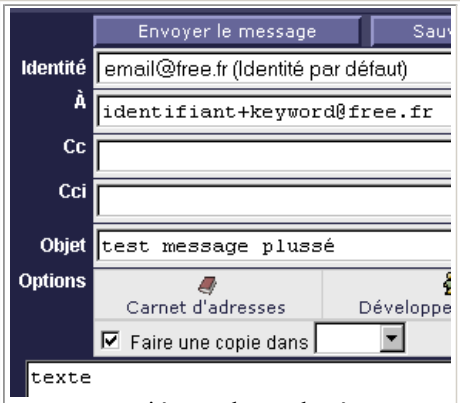
Note:

- l'absence de l'entête "date", fait que le filtre est ignoré : ce filtre a donc peu d'intérêt.
- attention des dates peuvent être de la forme **18 Jun 03 16:22:32 GMT**. Tester.
- il peut arriver que l'année n'apparaisse que sur deux chiffres (selon le serveur?) dans ce cas, ne pas utiliser la règle indiquée (qui rejetterait tous les messages).

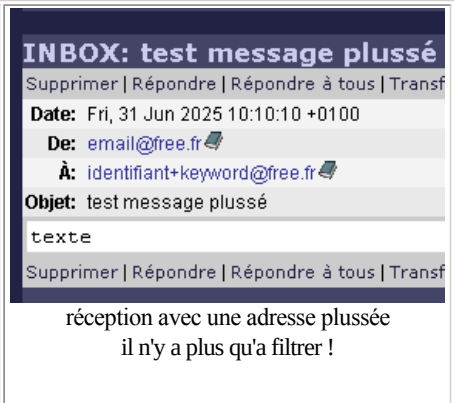
retour haut de page

3.K - Adresse plussée

Principe : comme un message envoyé a l'adresse identifiant+keyword@free.fr arrive dans le compte email identifiant@free.fr , il suffit d'appliquer un filtre sur le mot clé choisi ("keyword" dans cet exemple).



envoi à une adresse plussée



réception avec une adresse plussée
il n'y a plus qu'a filtrer !

Par exemple, il est possible de classer les emails reçus, en fonction du mot clé keyword choisi (on peut mettre un autre mot clé).

Attention, l'inverse keyword+identifiant@free.fr ne fonctionne pas

retour haut de page

3.L Que faire des messages filtrés ?

Dans un premier temps, recueillir les messages filtrés dans un répertoire séparé (au moins le temps de valider les règles de filtrage). Puis ré-écrire la règle avec "suprimer définitivement", ou éventuellement, en refusant avec motif au cas ou un message de vos amis serait rejetté par erreur. Attention, la destruction est irréversible.

Il ne sert a rien d'envoyer un message de rejet a l'attention du vilain spammeur (ou plutot de son logiciel). Cela encombre le réseau, et va peut-être causer du tort à un internaute innocent qui s'est fait usurper son email, ou vers qui le spammeur aura rerouté les réponses. Rappelons que la plupart du temps, l'objectif est de vous faire visiter un site ou lire une publicité,
et votre réponse... le spammeur n'en aura même pas connaissance !

Voir les remarques

Il est possible de gérer les répertoires dans votre compte de messagerie Free.
-> voir le tutorial gérer les répertoires

retour haut de page
