Règles mfilter pour Free.fr (4/4)

Tutoriel non officiel pour mfilter de Free.fr.

Quatrieme partie : mfilter, niveau "expert"

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.

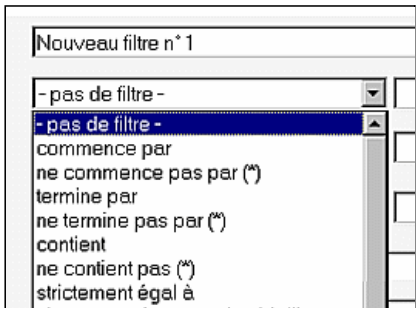
Mieux vaut ne rien faire que de programmer n'importe quoi.

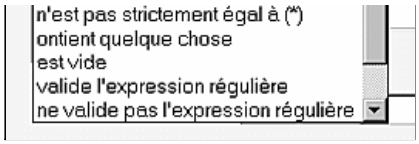
3. Emploi d'expressions régulières (perfectionnement)

3.A - Syntaxe des expressions régulières

Pour réduire le nombre de règles, il est possible d'utiliser des caractères spéciaux associés aux mots clés : ce sont des **expressions régulières**.

- on ajoute des caractères spéciaux aux mots, pour constituer des expressions régulières.
- sur mfilter de free.fr , on peut écrire des **majuscules ou des minuscules** dans les règles, cela n'a pas d'importance (indifférence à la casse).
- Associativité : (**.***Re: hello|**.***Re: hi) équivaut à **.***Re: h(ello|i)
- Portion de mot : si je filtre sur la portion de mot **you** alors le filtre va opérer dès qu'il trouve la chaine de caractère you : **your, you!, cayou, yougourt**... C'est utile pour gagner de la place mais risqué.
  A l'extrême, si je filtre sur une seule lettre, le risque de rejet à tort est trop grand.
  A l'inverse, si je filtre sur une phrase: enjoy your viagra, le filtre va servir une fois par an.
- Attention aux caractères codés comme é (codé =E9), à, è ... ces caracères perturbent mfilter : faites vos essais. Noter qu'il y a aussi des codages particuliers, parfois utilisés pour camoufler des mots clés comme *viagra*, mais présents aussi dans des messages légitimes.
  Exemple en base64 :
  test é,è,ç,à,ù,%,$,*,@,ê,â,£,µ,§ est codé ainsi
  test =?iso-8859-1?b?6SzoLOcs4Cz5LCUsJCwqLEAs6iziLKMstSyn?=
- pour mettre en place une expression régulière, il faut choisir un des deux critères : "**valide l'expression régulière**" ou "ne valide pas l'expression régulière" qui figurent aux deux dernières lignes de la case -pas de filtre- :





Rappel : (*) signifie qu'il faut nécessairement cocher "Remplir **toutes** les conditions suivantes"

3.B - Caractères spéciaux courants

.	le point représente n'importe quel unique caractère exemple : v.agra filtre viagra , v1agra , mais pas v**i**agra défaut : accepte véagra (!) quand é est un caractère codé.
?	le point d'interrogation est un multiplicateur de l'élément précédent (zéro ou une fois) - exemple : vi?agra filtre vagra ou viagra - ne filtre pas v**ii**agra autre exemple : viag? filtre via, viagra, viaggra - eviter le ? en fin de règle
*	l'astérisque est un multiplicateur de l'élément précédent, même zéro fois exemple : vi*agra filtre vagra, viagra v**i**agra, v**iii**agra ... mais pas vi**aa**gra
+	le plus est un multiplicateur de l'élément précédent, au moins une fois exemple : vi+agra filtre viagra v**i**agra, v**iii**agra ... mais pas **vagra**, ni vi**aa**gra
.*	représente une chaine de caractères de longueur quelconque (y compris rien du tout, chaine de zéro caractères)
|	OU logique - (ALT GR 6 sur le clavier d'un PC) - très utile !
{ }	les accolades contenant un nombre qui précise le nombre exact d'occurences du précédent caractère ou mot - exemple : viag{2}ra filtre viaggra - mais pas via**ggg**ra viag{2,4}ra filtre viaggra, viagggra et viagggggra - mais pas via**ggggg**ra (viag){2}ra filtre viag**viag**ra - mais pas viagra viag{2,}ra filtre viaggra, viaggggra ... sur free : {2} signifie "exactement 2" , et {2,} signifie "2 ou plus"
[]	les crochets contenant une liste de caractères parmi lesquel on ne peut choisir qu'un seul caractère. exemple : v[i1!]agra va filtrer viagra, v1agra, v!agra mais pas v|agra ni vi1agra
[b-f] [^b-f]	tout caractère compris entre b et f, c'est a dire b,c,d,e,f - attention, peut contenir des caractères avec accent : a tester tout caractère sauf ceux compris entre b et f, c'est a dire sauf b,c,d,e,f
[0-9]	n'importe quel chiffre
[^]	les crochets avec accent circonflexe en premier, filtre n'importe quel caractère sauf le(s) caractère(s) immédiatement derrière l'accent circonflexe exemple: **[^@]** n'importe quel caractère sauf @ exemple: [^@]+@free
\.	antislash et point - l'antislash transforme les caractères spéciaux $. ^ ? [ ] { } ( ) \ | * + en caractère ordinaires. exemple : free\\. filtre **free.** écrit avec un point, mais pas **free**z
\< \>	fin de mot début de mot - via\> filtre via gra en début de sujet - poursuivre le test
$	dollar - fin de ligne - exemple1: **va$** filtre "**va**" exactement exemple2: .*va$ filtre "ca **va**" mais pas "ca **va** bien"

- ne pas confondre les caractère spéciaux (^ $ [...), avec les caractères éventuellement codés (é, à, è, ù...)
- éviter les caractères facultatifs (?, * , +) en fin de filtre, risque d'erreur, et consomme de la place (la règle est limitée en taille)

-> voir les exemples avec expressions régulières

Pour mémoire : autres caractères spéciaux (non testés sur free - rappel: les erreurs de syntaxes "cassent" tous les filtres) :

< > : ; , ' ! & %	caractères normaux
?!	negation (non testé ne fonctionne probablement pas sur free - a tester) exemple : pot(?!age|iron) signifie tout ce qui commence par pot sauf

	potage et **potiron**
[:alpha:] [a-z]	n'importe quelle lettre a tester?
[:digit:]	n'importe quel chiffre - à remplacer par [0-9]
[:blank:]	espace ou tabulation
^	accent circonflexe - début de ligne premier mot - exemple: **^via** filtre **via**gra ou **v a**gra en début de ligne mais pas oli**via** ni **v**elo faites des test (ne fonctionne pas comme on s'y attend)
^$	accent circonflexe et dollar - ligne vide faites des test (ne fonctionne pas comme on s'y attend)
 \s \S \d \D \b \B \w \x00	-- non testés sur mfilter de free -- espace blanc pas d'espace chiffre n'est pas un chiffre mot - bordure de mot en Perl n'est pas un mot - non-bordure de mot en Perl mot caractère hexadécimal

Caractères codés ("quoted-printable")

é	=E9
	il y a d'autres caractères

retour haut de page

3.C - Autres entêtes

Sur chaque message, les entêtes peuvent etre vues en validant l'option "voir tous les entêtes" de votre outil de messagerie, ou encore en regardant le code source du message (accessible sur Webmail également).

> *Les en-tetes ne sont pas forcément authentiques, puisque l'expéditeur expert peut mettre ce qu'il veut (pour améliorer l'exploitation ou pour déjouer les protections). Ainsi il est possible de se faire passer pour quelqu'un d'autre, en mettant une fausse adresse de retour (c'est pour cela que renvoyer un message de refus ne sert a rien sinon à encombrer)...*

Si vous observez bien les emails indésirables qui vous parviennent, vous pouvez déterminer les éléments les plus communs. En effet, il est vain de définir une règle pour chaque message reçu tant l'imagination des spammeurs est grande. L'idée est donc de trouver ce point commun, qui permettra de filtrer, à l'aide d'**une seule règle**, des centaines de mails, dont le sujet est pourtant différent d'un message a un autre.

entête	contenu	quels critères de filtrage?
Return-Path	adresse de retour	utilisable pour des filtres acceptants (si contient *monboulot.com* alors accepter)
Delivered-To	serveur online.fr	est renseigné, meme lorsque le message est envoyé en bcc (Blind Carbon Copy) Est renseigné lorsqu'il n'y a aucun destinataire dans les entetes - permet de savoir si l'adresse utilisée (meme en bcc) est @free ou @online ou si elle est "plussée". login+site@free.fr
Received	serveurs intermédiaires (cheminement du message)	si unknown ou HELO, EHLO, présence de @ -contient le chemin du message s'empile a l'envers (dernier en haut) -peut être fictif (créé ou modifié par spammeur)
Message-ID		parfois "added-by" -souvent signe d'un spam quand absent -peut être ajouté par le serveur -peut ne pas exister
From	expéditeur	vérifier que l'adresse est connue, suspect si l'entête est vide (pas d'expéditeur)
Reply-To	adresse de réponse	si c'est .ru la réponse ira en Russie ... à moins d'y avoir des amis, a jetter.
To	destinataire(s) principal	si l'adresse est fausse (n'est pas la votre)
Cc	destinataires en copies	si trop de co-destinataires (free ou autre)

Subject	sujet du message	sujet indésirable d'après le mot clé, présence de votre adresse dans le sujet
Date	date (formats divers)	fausse date, (absence de date= filtre ignoré)
X-Mailer		peut contenir le nom du programme de spam
MIME-Version		
Content-Type	text/plain	si ce champ est présent, il y a des pièce jointe (html ou texte), caractères typiques (ks_c_)
	text/html	présence d'une pièce jointe uniquement en html
	boundary	indique la présence d'une pièce jointe (un fichier, pas toujours un virus)
	audio/x-wav	meme chose, risque de virus
X-Priority		
X-MSMail-Priority		
Content-Transfer-Encoding	quoted-printable	
X-UIDL		
X-Mozilla-Status		

4. Pour les experts (liste de règles qui fonctionnent)

Les filtres qui suivent fonctionnent. A adapter à vos besoins.

Combiner plusieurs règles dans un même filtre, en faisant attention à la logique (grouper les mots clés, tronquer les mots clés, bien choisir "Remplir les conditions").

-> revoir le tutorial débutant, ou les caractères spéciaux.

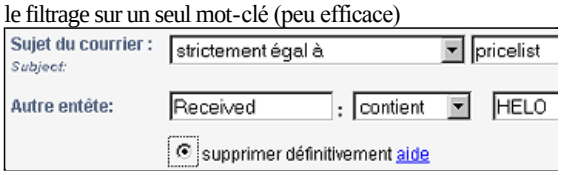
Filtrage des expéditeurs :

de (from)	contient	spammeur	détruire
de (from)	valide l'expression	.*(microsoft.com|spammeur)	détruire
return-path	contient	.ru>	détruire
de (from)	contient	ami	accepter
de (from)	valide l'expression	.*(patron|belle_mere)	accepter (ou répertoire!)

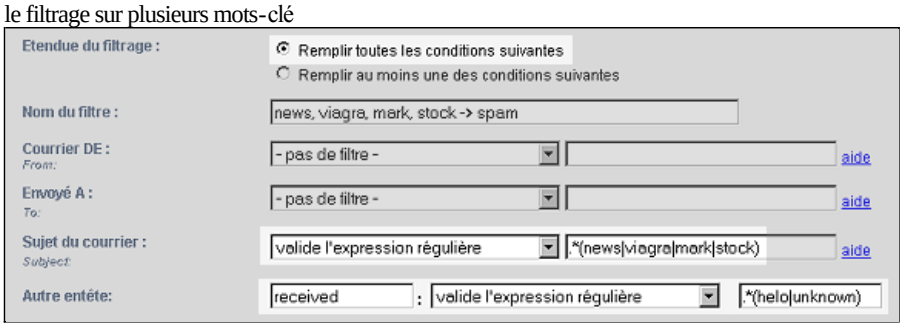
(rappel : on peut écrire en majuscules ou minuscules)

Filtrage sur le sujet

le filtrage sur un seul mot-clé (peu efficace)

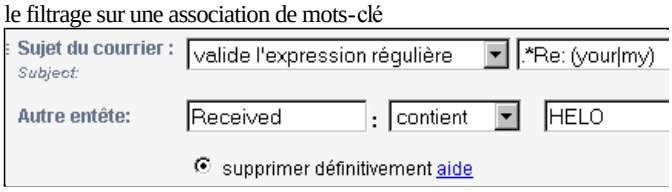


le filtrage sur plusieurs mots-clé



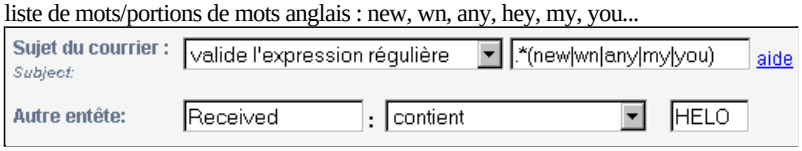
.* désigne n'importe quelle chaine de caractère (-> *voir caractères spéciaux*)
le test sur HELO et unknown est destiné a confirmer l'origine douteuse (cause pas valable avec Wanadoo, tele2... qui utilisent habituellement HELO -> ne mettre que unknown ?)

le filtrage sur une association de mots-clé



qui va filtrer Re: your mais aussi Re: Re: your ou Re: Re: my details ...
(préférer les mots singuliers, plus efficaces)

liste de mots/portions de mots anglais : new, wn, any, hey, my, you...



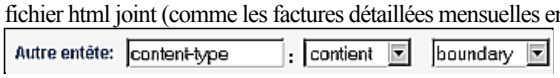
Mais attention, si un ami envoie un message avec de l'anglais ou des nom propres (**New**-York, B**any**uls, **my**stère...), cela risque de ne pas passer le filtrage, d'ou l'intérêt de mettre en premier, les filtres qui acceptent les amis.

Filtrage sur les destinataires

voir exemple 3.C

Filtrage sur les entêtes

le filtrage sur l'existence de pièce jointe **content-type - boundary** donne de mauvais résultats, parce que des bons messages (amis) peuvent etre envoyés sous forme de fichier html joint (comme les factures détaillées mensuelles envoyées en htm).



le filtrage sur le type de texte **content-type - text/plain** donne de mauvais résultats, parce que des bons messages (amis) peuvent etre envoyés sous forme de fichier html joint (comme les factures détaillées mensuelles envoyées en htm).

content-type	ne contient pas (*)	text/plain	répertoire ou supprimer

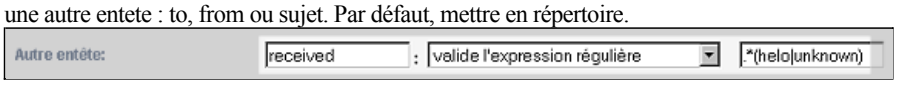
De la même manière, le filtrage sur le type de texte **content-type - text/html** donne d'assez bons résultats: le html seul étant très souvent du spam (contrairement au texte + html des outils de messagerie soit multipart) - a tester (idée de Jacques)

content-type	contient	text/html	répertoire ou supprimer

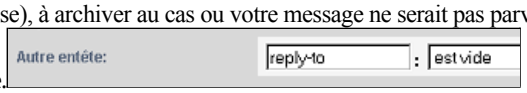
Message provenant de machines piratées a l'insu d'utilisateurs (freebox...) - a tester (observations et idée de Jacques)

to	contient	monadresse@free.fr	
sujet	contient	?B?	
received	valide l'expression	.*[0-9]+(-[0-9]+){3}.*mrelay[0-9-]+\.free	répertoire
		.*[0-9]+(-[0-9]+){3}.*mrelay.+\.free	

le filtrage sur **received - helo** n'est pas suffisant pour détecter un spam; wanadoo, tele2... envoient des messages contenant HELO dans l'entete Received. Comme le filtrage sur **received - unknown** . Utiliser ces règles en complément d'une autre sur une autre entete : to, from ou sujet. Par défaut, mettre en répertoire.



Cas d'un email rejetté par un serveur de messagerie, à cause d'une mauvaise adresse. A détruire si vous n'envoyez jamais de mail de ce compte (quelqu'un/ un virus a utilisé votre adresse), à archiver au cas ou votre message ne serait pas parvenu au destinataire.



autre solution (moins efficace, ou à utiliser conjointement avec la règle ci-dessus)

de (from)	contient	MAILER-DAEMON	répertoire

Syntaxes qui <u>ne fonctionnent pas</u> , ou mal sur mfilter free :

sujet	valide l'expression	^hi$\|^re: hi$ mettre: (Re: *)*hi!*$
sujet	valide l'expression	^Re: Your mettre: Re: *Your\>
a (to) ET cc	ne contient pas* ne contient pas*	monadresse@ monadresse@
sujet	valide l'expression	^Re: Your |^Re: hello

ET Received	contient	mettre: Re: *(Your |Hello\>) HELO

- Pour ceux qui utilisent une adresse login+truc@free [suggestion de Jacques]
  Envoyé A (To) : **valide l'expression régulière** .*adresse(\+[^@]*)?@free\.fr
  Que faire de ce courrier : **accepter**

Exemples NON VERIFIES (viagra) dont la complexité croissante peut inciter a filtrer sur d'autres critères!

> v.?[l1i].?[a@].?g.?r
>
> @.?g.?r
>
> .*v.?[l1i|:!].?[a@à].?g.?r.?[a@à]
>
> Filtrage sur une adresse IP (rarement identique) : received - contient - 123.456.789.012

Une syntaxe que je n'aime pas beaucoup : comme mfilter ne permet pas de couvrir tous les cas, au lieu de filtrer par un test, on accepte par le test complémentaire (mettre des règles négatives, puis des règles positives simples). Exemple, au lieu de rejetter si mon adresse n'est pas dans TO ET si mon adresse n'est pas dans CC, on accepte si mon adresse est dans TO OU si mon adresse est dans CC, on rejette sinon : casse gueule !
soit (non A) ET (non B) = non (A OU B)

---

5. Quand le filtre ne fonctionne pas

> Une seule erreur sur une règle et c'est tout le filtre qui est hors service !

Vérifications à faire :

- vérifier les dernières règles éditées (chaque règle est indiquée avec sa date de mise a jour)
- vérifier qu'il n'y a pas une règle antérieure ou postérieure qui parasite la règle testée
- vérifier que la règle n'est pas temporairement désactivée
- vérifier que la règle défaillante n'est pas victime du bug d'ancrage
- vérifier que les caractères spéciaux sont utilisés correctement (avec caractère d'échappement)
- vérifier qu'il n'y avait pas de caractère codé (é, è, à...), dans le message.
- vérifier l'orthographe : *vaigra* est différent de *viagra*
- vérifier le choix : **toutes** les conditions remplies ou **au moins une** condition remplie
- vérifier que l'entête existe dans le message non filtré, car si l'entête est absente, toute la règle est simplement ignorée.
- au besoin simplifier la règle en test, ou l'isoler sur un autre compte email

Bugs et défauts connus

- bug d'ancrage dans les expressions régulières, pour toute entete
- pas possible de tester la taille d'une pièce jointe
- pas possible de filtrer sur le texte du message (trop de travail du serveur); seules les entêtes sont scrutées.
- pas possible de tester la présence d'une entête.
- si l'entete à scruter est manquante, la règle est purement et simplement ignorée.
- il n'est pas possible d'accéder aux dossiers IMAP avec un logiciel de messagerie en POP.

---

6. Remarques

- Autres idées de filtrage :
  - dans le champ **to** : accepter les messages comportant votre prénom.
  - sur l'entête **X-Mailer** par exemple, s'il contient quelque chose. Risque d'éliminer aussi les publicités "utiles".
  - sur la présence de son propre login dans le sujet. Attention à ne pas filtrer les confirmation d'inscription... ; on prendra soin d'accepter les messages provenant des serveurs sur lesquels on s'est inscrit (filtre d'acceptation au début de la liste des règles). On acceptera aussi les messages dont l'entete Reply-To est ami.

- Il ne sert a rien de renvoyer un messager de refus aux adresses indiquées par les spammeurs. Ce message ne sera pas lu, **sauf** si vous voulez indiquer aux expéditeurs amis que votre adresse a changé.
  Aussi, renvoyer un message de refus augmentera l'encombrement du réseau.

- A quoi sert le spam? A faire de la publicité auprès d'un maximum de personnes sachant que dans la masse, il y aura des clients qui vont se manifester. Le petit pourcentage de clients suffit a amortir les frais de spam.

- Ne jamais répondre, meme pour se désinscrire, car cette action est utilisée pour confirmer l'existence de votre email, peut-etre meme, pour afiner votre profil (vous n'aimez pas le viagra, donc la prochaine fois on vous enverra un spam pour des jeux video?), et vous risquez de recevoir encore plus de spams.

- Les spammeurs emploient, ou sont des experts, professionnels, payés pour passer outre les filtres, utilisent des softs capables d'envoyer beaucoup de message a la chaine. N'espérez pas les contacter personellement en faisant une réponse ou un rejet avec message ! S'ils utilisent l'intrusion sur des serveurs tiers, c'est justement pour qu'on ne puisse pas les identifier. Et s'ils savent franchir les filtres, ils savent aussi filtrer les réponses, automatiques ou non, des personnes mécontentes.

- Ces règles de filtrage qui sont publiées, risquent d'etre obsoletes dès que les spammeurs auront trouvé d'autres astuces pour les contourner.

- Lorsque votre filtrage sera parfait, éviter la mélancolie en désactivant une règle, histoire de voir quelques spams passer ;-)

Ainsi, au début, il suffisait de filtrer le mot VIAGRA
Puis cela est devenu V1AGRA, puis V|AGRA, vi@gra,
v.i.a.g.r.a etc...

retour haut de page

Copie et duplication de cette page libre de droits.
publié sur : http://www.thailande.free.fr/mfilter.htm

notes : les copies d'écran proviennent du site de Free.fr, elles ont été adaptées par nécessité pédagogique.