Règles mfilter pour Free.fr (2/4)

Tutoriel non officiel pour mfilter de Free.fr.

Deuxieme partie : mfilter, perfectionnement

introduction - mfilter : pour quoi faire ?
1. L'antispam standard (réglages "usine" de Free)
2. Tutoriel mfilter : <u>perfectionnement</u>
 A - pour quoi faire ? B - connexion C - les scores pour mfilter D - modifier les filtres antispam E - rédaction d'un <u>filtre simple</u> F - principes de base G - <u>liens</u>
3. Exemples concrets (prêts à l'emploi)
4. Documentation mfilter pour experts et chercheurs

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 <u>les destructions sont irréversibles</u>.

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.

2. Tutoriel mfilter : perfectionnement

2.A - mfilter : pour quoi faire ?

Avec mfilter, il n'y a pas :

- de fonction répondeur (style : message pour indiquer que vous êtes en vacance).
- de transfert vers une autre boite (mais pour grouper tous vos messages : utilisez les fonctions disponibles dans votre logiciel de messagerie, ou les options de certains FAI).
- de collecte de mails d'autres comptes (ni de Free, ni d'autres FAI).
- de test sur la taille des pièces jointes.
- de test sur le contenu du message, ni du contenu des pièces jointes.
- d'utilitaire permettant de dupliquer les filtres, d'un compte email à un autre: pour l'instant il faut tout recopier à la main (d'ou l'interet d'optimiser vos filtres). [en mai 2005]

Après filtrage et <u>destruction</u> définitive d'un message indésirable, il y a possibilité de le signaler à l'expéditeur par un message automatique (très technique, en anglais). Déconseillé car encombre le réseau, et risque de géner d'autres internautes.

2.B - connexion à mfilter

Sur free.fr, l'accès aux règles de filtrage de votre boite email est à l'adresse <u>http://mfilter.free.fr</u>. Pour accéder au filtre de votre compte adresse@free.fr, il faut indiquer l'identifiant (c'est le début de "l'adresse" email) et le mot de passe (celui qui est utilisé pour accéder au compte email).

Attention, ne pas confondre **mfilter** avec les filtres du webmail (image cidessous). Car mfilter agit dès que le message arrive, meme si vous n'etes pas en ligne, alors que les filtres du webmail n'agissent <u>que</u> lorsque vous vous connectez au webmail.

📥 Réception	Ş Nouv	eau Dos:	siers O	ptions R	,● Recherche C	Carnet (📕 d'adresse	s Sortir	Cuvrir le do	ssier	INBOX	•
Règles	de	filtra	ge				A	ppliquer	toutes les règle	85		
1)	с	Supprim	er des r	message	es , où le cha	amps Ci	orps conti	ent See th	he attached file	for d	etails	
2)	2) C Supprimer des messages , où le champs De : ou Objet : ou Corps contient stock											
3)	C	Supprim	er des r	nessage	es , où le cha	amps O l	bjet : cont	ient IP wa	is logged			
4)	C	Supprim	er des r	nessage	es , où le cha	amps D	e:contien	t elene				
5)	۲	Supprim	er des r	nessage	es , où le cha	amps O	bjet:cont	ient watcl	hes			

	Supprimer Descendre Remonter							
Dáfinit								
Definition de regie								
Champ	hamp 🗌 À: 🗍 Cc: 🗍 De: 🗹 Objet: 🗍 Corps Texte Vatches							
Texte								
Action	Action 🕫 supprimer le message 🗢 déplacer le message vers 🛛 choisissez un dossier 💌							
	Modifier Valeurs initiales Annuler							

cet écran correspond aux filtres du webmail, ce n'est pas mfilter.

figure d'écran : connexion sur http://mfilter.free.fr

Cette fonctionnalité permet de mettre directement sur le ser sur votre boite aux lettres.	rveur des filtres qui seront appliqués sur votre courrier au moment d'être déposé
Ainsi vous pourrez, selon certain critères, refuser des courri utiliser ces filtres pour rediriger vos emails dans différents d <u>En savoir plus</u>	iers paur qu'ils n'encombrent pas vatre boites aux lettres ; ou encore vous paurrez dossiers IMAP, si vous utilisez ce protocole pour relever vos mails.
1	Connexion Quitter
Merci de remplir les champs s	sulvants
Votre Identifiant	
Votre mot de passe	
	envoyer

figure d'écran : saisie de l'identifiant et du mot de passe

r les champs suivants	
login	
ISSE Water and the second seco	
envoyer	
ISSE BOUNDARY BOUNDAR	

on arrive sur l'écran suivant, qui liste tous les filtres existants (vide au début) :

	Connexion Quitter					
Pour ordonner vos filtres par priorité, sélectionnez à gauche votre filtre puis ajustez avec les boutons '+' et '-' Aucun filtre n'existe pour le moment. Pour en créer un, cliquez sur le bouton 'Ajouter'						
	Oréer un nouveau filtre ▲ +10 ▲ +1 ▼ -1 ▼ -10 ▼ -10 ▼ -10 ▼ -10 ▼ -10 ▼ -10 ▼ -10 ▼ -10 ▼ -10 ▼ -10 ▼ -10 ▼ -10					

- figure d'écran : arrivée sur la gestion des filtres -

2.C - Les scores pour mfilter

Fin 2004, Free a mis en place une fonction de notation des emails reçus : le score (scoring). En même temps, l'option de filtrage sur la valeur du score, a été ajoutée dans mfilter.

Qu'est-ce que ce score ? Il s'agit, de l'examen automatique de chaque message reçu par le serveur de Free. Après cet examen, un score est attribué à chaque message. Il n'est pas possible de voir les scores des messages détruits.

Lorsque le score est supérieur à 100 (seuil standard), le message est suspecté d'être un spam.

Pour voir la valeur des scores, il suffit d'accéder au compte email par l'interface internet webmail,

<u>http://imp.free.fr/</u> comme pour lire les mails (ne pas utiliser outlook ou d'autres applications de messagerie, elles ne permettent pas de voir les scores).

Une fois arrivé dans le compte de messagerie,

🗈 Suppression de tous les message	s de repertoire6.	
Explorateur des dossi	nrs Ø	
Choisir une action :	2 ?	Développer tout Replier Tou
🗖 🖻 🎰 INBOX		
repertoire1		
repertoire2		
repertoire3		
repertoire4		
repertoire5		
repertoire8		
repertoire7		
Tresh		
Choisir une action :	- 2	Développer tout Replier Tou

il suffit de cliquer sur [%] Espace disque

on arrive alors sur une page spéciale : on voit la taille de chaque répertoire...

Réce	🖕 🦉 💌 🦌 🥵 🕈 🦉 🕅 %6 Iption Vider la corbeile Nouveau Doseiers Options Recherche Aide Carnet d'adresses Espace disqu	identifiant 😑 repartoira4 💌							
Vol	tre espace disque								
Espa	Espare occupă sur la bolle auxilethes: 4% (872 Ko).								
ø	identifiant	Taile							
Q	Dossier WebMail (Répetoire (NBOX)	792 Ko							
P	S repertoiret	352 Ko							
P	repertoire2	56 Ka							
P	Eariotrager @	20 Ko							
P	repertoire4	16 Ka							
P	Courriers envoyés (Répertoire sent-mail)	20 Ko							
Q	S repertoire5	120 Ko							
P	Sanitzine6	16 Ko							
P	repertoire7	188 Ko							
P	Courriers reçus (Répertoire Meiloit)	36 Ka							
Q	Trash	32 Ka							

Pour voir les scores, il faut **cliquer sur la petite loupe** qui se trouve à gauche, en regard du nom de répertoire.



Le répertoire s'ouvre et liste les 100 premiers emails, avec leur score :

Subject: You can quit smoking in 2 weeks. Money Back Guarantee.
From: "Darek" <darek@anomok.com></darek@anomok.com>
To: Train@free.fr
Date: Fri, 05 Aug 2005 12:47:49 -0900
Score: 500
Description: Timezone -800 (+);money+back refund back in subject (+);to unsubscribe
(+);do not reply to this email (+);tuture+mailing&;marketing (+);pills (+);HERBAL (+)
Cubicate New Indexe continence are been likel
Subject: New bulgari repliccas are nere bind
From: "Stella Packett" <lugghbenqk@telaplanet.net></lugghbenqk@telaplanet.net>
10; SCRAHUL@HEE.H2 Data: Sup. 07 Aug 2005 04:06:45, 0700
Sente: 230
Description: ANTIRAYES (+):Timezone .700 (+):1 ink to domain (+):Only one part (+)
beschpton, Arthornes (1), finite one -rob (1), enix to domain (1), only one part (1)
Subject: CiALIS _ now generation of sexual beasters!
Subject: GMEIS - New generation of Sexual boosters: From: "omory" <klonov3@hotmail.com5< td=""></klonov3@hotmail.com5<>
To: <route@free fr=""></route@free>
Date: Sun. 07 Aug 2005 18:08:34 GMT
Score: 378
Description: Url TLD (+);here in link words (+);[tips] remove in link words (+)
Subject: It is a smart choice for wonderful sawings on tablets.
From: "james coisner" <sekene@clickitmail.com></sekene@clickitmail.com>
To: "Scandal" <aistdrebgf@free.fr></aistdrebgf@free.fr>
Date: Sun, 07 Aug 2005 19:45:41 -0300
Score: 159
Description: Timezone -200 (+);Regex Msgld (+);check+our the+store * store site *
site website * website pahe homepage * page webpage * forum shop club online *
sitejoniine ^ storejonarmacy (+)

On distingue les critères du scoring en rouge, comme par exemple : le décalage horaire, un certain nombre de mots clé, l'URL d'origine, l'intitulé des liens présents dans le message... Et le score. Dans cet exemple on voit bien que tout ces spams ont un score supérieur a 100.

Cette observation des scores permet de corriger le seuil de filtrage dans mfilter (à laisser à la valeur 100, en cas de doute)

2.D - modifier les filtres antispam

Nous avions vu, lors du tutoriel sur les <u>filtres antispam standards</u>, qu'il était possible de créer 3 filtres de façon simple et automatique. Ces filtres sont des règles-type qu'il est possible d'éditer à volonté (à condition de ne pas écrire n'importe quoi).

Nous avions expliqué

- comment stocker les messages filtrés dans un répertoire,
- comment désactiver un filtre, temporairement

Regardons maintenant la syntaxe des filtres antispam, avec l'indication [preset] dans leur nom

 le filtre "les mails indésirables (SPAM)" s'appelle : [preset] Scoring qui contient la règle suivante :

Score: supérieur à 100

Analyse

Le serveur calcule le score de chaque email reçu, si la valeur obtenue dépasse 100, alors l'email est filtré.

 le filtre "les mails contenant des fichiers attachés exécutables" s'appelle : [preset] Attachements exécutables qui contient la règle suivante :

Autre entête: Content-(Disposition|Type) valide l'expression régulière

.*name *= *("[^"]*\.(exe|vbs|pif]scr|bat|cmd|com|cpl) "][^";]*\.(exe|vbs|pif]scr|bat|cmd|com|cpl)) *(\$|;)

<u>Analyse</u>

On recherche dans les en-têtes Content-Disposition ou Content-Type le mot name (comme name ou filename) puis un nom entre guillemets, nom de fichier exécutable (.exe, .vbs, .pif, .scr, .bat, .cmd, .com, .cpl)

le filtre "les mails où je suis en copie cachée" s'appelle :
 [preset] Pas de copie cachée qui contient la règle suivante :

Autre entête: (To|Cc) ne valide pas l'expression régulière .*identifiant(\+[^@]*)?@(free|online)\.fr

<u>Analyse</u>

On recherche si l'identifiant est absent des en-têtes To et Cc

Donc il est possible d'ajuster ces régles pour qu'elles conviennent mieux.

- orienter les messages filtrés vers un dossier séparé, plutôt que de tout détruire
- modifier le seuil du <u>score</u> (valeur standard de 100 [en mai 2005])
- et bien sur ajouter des règles de filtrage pour accepter les messages de vos amis, collègues... ces règles sont a placer AVANT les règles de l'antispam.

2.E - rédaction d'un filtre simple

Cliquer sur le bouton "Ajouter" pour ajouter un filtre. On arrive alors sur la page d'édition du filtre :

	Connexian Quitter 44 39 Ajouter Liste	
Gestion des filtres	Désactiver temporairement ce filtre	
	Pour créer un nouveau filtre, veuillez préciser ci-dessous le(s) critère(s) de votre règle de filtrage:	
Etendue du filtrage :	Remplir toutes les conditions suivantes	
	C Remplir au moins une des conditions suivantes	
Nom du filtre :	Nouveau filtre n° 1	
Courrier DE :	- pas de filtre -	aide

- pas de filtre -			aide
1	pas de filtre -		
Supprimer définitiver	ient <u>aide</u>		
C refuser avec ce motif]
C placer dans ce dossi	er IMAP: sent-mail		
ou da	ns un nouveau:		
C accepter			
		(Demièr	Enregistre res modification
	 supprimer definitiver refuser avec ce motif placer dans ce dossion ou da accepter 	supprimer definitivement <u>aide</u> C refuser avec ce motif placer dans ce dossier IMAP: sent-mail ou dans un nouveau: C accepter	supprmer definitivement alde c refuser avec ce motif c placer dans ce dossier IMAP: sent-mail ou dans un nouveau: C accepter (Demiki

- figure d'écran : parametrage d'un filtre (ancienne version) -

L'écran de rédaction se divise en trois parties.

<u>L'étendue du filtrage</u> : quelles conditions faut-il satisfaire pour que le filtre agisse? toutes ou au moins une?

Remplir toutes les conditions suivantes
 Remplir au moins une des conditions suivantes

Les <u>entêtes à tester</u> : destinataire, expéditeur, sujet... vous choisissez sur quelle(s) entête(s) vous voulez opérer le filtrage. A noter qu'il y a des entêtes cachées qui permettent d'afiner le filtrage (-> voir la partie <u>experts</u>).

L'<u>action</u> (unique) : soit diriger le message vers un répertoire (tri), soit l'effacer (définitif), ou l'accepter.

Il faudra bien vérifier ces <u>trois parties</u> de la règle avant de la mettre en service.

Voilà, il ne reste plus qu'a rédiger les règles.

Avant toute chose, bien définir vos besoins : qui est susceptible d'utiliser votre adresse (amis, inconnus qui visitent votre site web, appartenance à une liste de diffusion, inscription sur news.group...)

2.F - Principes de base

- lorsqu'un message arrive, les filtres sont testés dans l'ordre croissant (filtre 1 puis 2 ...).
- dès qu'un filtre est positif lors du test sur le message, le test cesse (autres filtres ignorés).
- si tous les filtres échouent, le message est accepté (dans inbox).
- mettre les filtres qui acceptent (les amis) en premier, et les filtres qui détruisent en dernier.
- la taille d'une règle est limitée (en nombre de caractères).
- la taille des règles mfilter-free étant limitée, n'utiliser que les <u>mots pertinents</u> (exemple: pour accepter votre amipaul@yaou.com, il suffit de ne filtrer que sur le mot amipaul).
- limiter le nombre de filtres (20 maximum) pour permettre la mise au point facilement.
- faire des essais, une règle à la fois (et utiliser la désactivation temporaire, en haut d'écran).
- il peut être utile de créer un répertoire IMAP pour déposer les messages filtrés. Accès à la messagerie de free pour créer un répertoire : <u>http://imp.free.fr</u> avec adresse et mot de passe, ou directement sur mfilter (ne fonctionne pas toujours).

O placer dans ce dossier IMAP:	- Nouveau Dossier - 💌
ou dans un nouveau:	bureau

voir le tutorial : créer un répertoire

- utiliser la mise en <u>répertoire</u>, plutôt que la destruction (au moins pendant les essais). Et si possible un répertoire par filtre pour bien voir ceux qui ne fonctionnent pas.
- dans la définition des règles, on peut écrire en majuscules ou minuscules (mfilter de free est indifférent à la casse)
- faire attention à "Etendue du filtrage" : il vaut mieux n'avoir pas assez filtré que de perdre des messages.
 - o Pour accepter des messages, choisir "Remplir au moins une des conditions suivante";
 - réciproquement, avant de supprimer définitivement, il est plus prudent de choisir "Remplir <u>toutes</u> les conditions suivantes" avec un second test "de confirmation" dans la même règle
 - (comme le test de présence de HELO -> voir la partie <u>experts</u>).
- 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- :

N1	Ch		



- figure d'écran : critères de filtre -

retour haut de page

2.G - Liens utiles

<u>bunkerhill.free.fr/spam.html</u> page perso qui donne des conseils pour éviter les spams <u>www.shellunix.com/regexp.html</u> initiation aux règles <u>www.sri.ucl.ac.be/SRI/jpk/manuelMacSOUP/regex.html</u> <u>www.teaser.fr/~sdupille/howto.html</u>

documentation Perl, non compatible avec mfilter : www.perldoc.com/perl5.8.0/pod/perlretut.html www.enstimac.fr/Perl www.mongueurs.net/perlfr/perlre.html

documentation sur les expressions régulières www.regular-expressions.info

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