

## Filtre Sendmail

*Christophe Wolfhugel*

Hervé Schauer Consultants

142 Rue de Rivoli

75039 Paris Cedex 01

Tél: +33 (1) 46 38 89 90

Fax: +33 (1) 46 38 05 05

Christophe.Wolfhugel@hsc-sec.fr

Le courrier électronique sur Unix, outre ses grandes qualités, souffre hélas d'un gros défaut : le manque de possibilités de régulation dans la gestion du trafic. Nombreux sont les utilisateurs qui désirent avoir un contrôle sur le courrier électronique transitant par leur site, notamment celui à destination ou en provenance de réseaux extérieurs.

Le filtre présenté dans cet article a pour but de remédier en partie à ce défaut. Il ne faut cependant pas croire qu'il va apporter la sécurité idéale, pour cela il faudrait commencer par changer le protocole SMTP ou au minimum apporter de sérieuses modifications à la façon dont il est utilisé.

Le *MTA (Mail Transport Agent)* choisi pour l'implémentation de ce filtre est *Sendmail*. D'une part c'est le plus utilisé, d'autre part il apparaît comme mieux adapté aux configurations de relais courriers que certains autres MTA.

### 1. Objectifs

Les objectifs du filtre Sendmail sont de pouvoir contrôler et limiter l'utilisation qui est faite du courrier électronique entre le réseau interne et les réseaux externes auxquels est connecté l'organisme.

L'utilisation du filtre implique comme première mesure une centralisation du courrier sur un serveur dédié en lequel on a confiance, c'est à dire dont l'administration est effectuée très sérieusement. Ce serveur peut bien entendu être utilisé à d'autres tâches du moment que celles-

ci ne compromettent pas le fonctionnement de la passerelle de courrier électronique.

L'ensemble des machines internes seront configurées afin que tout le courrier sortant (et pourquoi pas local au site) soit redirigé vers le *mailhost* (relais courrier). Une politique de routage cohérente permettra de s'assurer qu'il n'est pas possible de court-circuiter le relais pour toutes les relations courrier vers l'extérieur.

Dans le sens opposé (courrier entrant) on s'assurera, en configurant proprement le serveur de noms par exemple, que tout courrier entrant transitera par le relais. Le routage encore une fois interviendra afin de filtrer les indésirables qui voudraient ignorer ces dispositions.

Le filtre interdira tout transit non autorisé de courrier en consultant la table d'autorisations gérée par l'administrateur courrier. Les messages rejetés sont bien entendu envoyés en copie au *postmaster* du site à des fins de contrôle.

Le filtre agit également en routeur politique. Un message pour un même destinataire pourra être routé différemment en fonction de critères tels que adresse de l'expéditeur, taille du message ou tout autre critère jugé utile.

Le code du filtre peut très facilement être étendu à de nombreuses autres fonctions comme par exemple la facturation. Il est également possible de modifier le corps du message ainsi que les entêtes afin de masquer totalement la structure interne du réseau.

## 2. Deux approches techniques

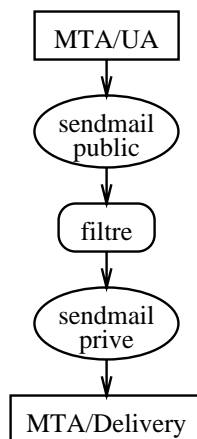
Deux solutions techniques ont été retenues. L'une est quasiment indépendante de la plateforme, la seconde impose l'utilisation d'un Sendmail-IDA, à partir de la version 5.65c, ce qui en soit n'est pas une mauvaise idée. La mise en place de 5.65c-IDA demande cependant un travail d'installation car n'étant pas (encore ?) livrée en standard par les constructeurs. L'utilisation de cette version permet également de s'affranchir des exotismes souvent inutiles rajoutés par les constructeurs.

### 2.1 Filtre externe

Le filtre externe correspond à l'approche la plus simple de mise en oeuvre de filtrage : intercaler l'outil de contrôle entre deux occurrences du MTA, chacune utilisant son propre fichier de configuration. La deuxième occurrence est protégée du monde extérieur afin que les utilisateurs ne puissent pas court-circuiter le filtre comme cela peut-être le cas lorsque le critère de validation d'une adresse est contenu dans l'adresse elle même.

Dans la suite de l'exposé nous utiliserons le terme de *Sendmail public* pour caractériser la première occurrence de Sendmail, celle qui peut être invoquée par tous. La deuxième occurrence étant le *Sendmail privé* et accessible au seul filtre.

L'enchaînement est donc systématiquement le suivant :



### 2.1.1 Sendmail public

La première occurrence de Sendmail va se comporter de façon tout à fait classique, à l'exception que dans tous les cas le processus de sélection du *mailer* doit toujours arriver sur le filtre.

Pour arriver à ceci, il faut modifier la règle S0 du fichier de configuration *sendmail.cf* afin de définir le nouveau routage vers le *mailer* du filtre. Il n'y aura donc plus d'utilisateurs locaux connus du Sendmail public. Ceci implique notamment que la base des alias (*/etc/aliases* ou */usr/lib/aliases*) doit être reconstruite depuis le Sendmail privé, car celle-ci exige que la résolution locale des utilisateurs puisse être faite.

Extrait de règle S0 modifiée :

```

# Try immediate delivery
R<$*>$+                $:>26 <$1>$2  find mailer
R$#$*$@$+<:>$*         $$filter $:<@$2>$3
R$#$*$@$+<+>$*        $$filter $:<@$2>,$3$4
R$#$*$@$+:$*          $$filter $:<@$2>,$3
  
```

La partie droite des règles aboutissant au filtre réécrit les adresses dans un format canonique propre au filtre : le paramètre entre les signes < et > correspond au relais auquel sera envoyé le courrier, le reste étant la suite du chemin à parcourir pour arriver à destination.

Il faut bien entendu redéfinir le *mailer* correspondant au filtre afin qu'il soit appelé avec les bons paramètres lui permettant d'effectuer sa tâche :

```

Mfilter, P=/usr/ucplib/mail/filter/filter, F=lsDMmn,
S=15/11, R=15/11, A=filter$s $f $u
  
```

On remarquera que le drapeau 'F' n'est pas présent dans la définition des *flags* (champ *F=*). En effet, celui-ci force le MTA à rajouter une ligne *From:* dans l'entête du message si celle-ci n'en a pas déjà. Nous laissons ce soin au Sendmail privé tout simplement parce que Sendmail n'ira pas extraire le GECOS (Prénom et Nom) d'un utilisateur si le mailer lui correspondant ne s'appelle pas *local*. Il n'aurait pas été possible non plus de remplacer *local* par le filtre en raison de règles de réécriture différentes.

Les règles définies par *S=* et *R=* correspondent respectivement à la réécriture de l'adresse de l'expéditeur et des destinataires. Dans notre cas

nous avons choisi que les adresses de l'enveloppe, qui sera fournie au filtre par les paramètres  $\$f$  et  $\$u$ , soient réécrites en *bang path* UUCP tout simplement afin de faciliter le travail du filtre dans sa sélection.

Le champ *Received*: habituellement rajouté à chaque occurrence de Sendmail (notamment pour éviter les boucles) sera mis dans l'entête du message lors du passage dans le Sendmail privé. Il n'y a aucun risque de créer une boucle infinie puisque le passage par le Sendmail privé est obligatoire. Ceci nous évite l'inesthétique et révélateur doublement du champ sur la machine passerelle.

A noter que la base des alias n'est pas utilisée par le Sendmail public et qu'il faut en tenir compte lors de l'établissement des règles du filtre.

En résumé, le Sendmail public fournit au filtre :

- l'enveloppe du message en paramètres (machine source, expéditeur, destinataires);
- le corps du message sur l'entrée standard.

### 2.1.2 Sendmail privé

Une fois approuvé et modifié par le filtre, le message est transmis au Sendmail privé qui va assurer la délivrance finale du message à son destinataire ou bien à la machine relais choisie. Ce Sendmail doit bien entendu être protégé afin que seul le filtre (ou un utilisateur privilégié) puisse y accéder.

L'exécutable en lui-même ne change pas, c'est le fichier de configuration qui fait la différence de comportement. En fait, le Sendmail privé est tout simplement celui qui tournait avant la mise en place du filtre. Quelques modifications de paramètres ont cependant été effectuées afin de différencier certains fichiers. La *mail queue* et le fichier de statistiques doivent bien entendu être distincts :

OQ/var/spool/mqueue-sec  
OS/usr/lib/sendmail-sec.st

On veillera également à ce que le Sendmail privé ne soit pas lancé en démon SMTP, ce qui oblige la mise en place d'un cron afin de traiter la *mail queue* à intervalles réguliers.

Si la version de Sendmail utilisée le permet, l'option `-Z` permettra de spécifier un fichier de configuration alternatif précompilé. Si Sendmail ne supporte pas cette option ou ne supporte pas les fichiers de configuration compilés, l'option `-C` fera tout à fait l'affaire bien que légèrement plus lente.

## 2.2 Filtre interne

Afin de pallier certains défauts du filtre externe, notamment sa lourdeur (deux exécutions de Sendmail à chaque message, nécessité de deux fichiers de configuration), il faut que la fonction de filtrage fasse partie de Sendmail.

En contrepartie de cette facilité de gestion, il faut accepter de faire un sacrifice, mais en est-ce vraiment un? Remplacer son Sendmail par un 5.65c+IDA, si ce n'est pas déjà fait, mérite d'être envisagé vu les nombreuses facilités de gestion et d'administration ainsi que la puissance des nouvelles fonctionnalités offertes.

A priori le filtre pourrait s'intégrer dans des versions plus anciennes de Sendmail, sous réserve que la logique dans laquelle vient s'intégrer le filtre n'ait pas trop évolué.

### 2.2.1 Logique de fonctionnement

Lors du traitement d'un message, Sendmail va collecter les différentes lignes de l'entête de celui-ci ainsi que le corps du message. Chaque adresse (expéditeur et destinataire) sera traitée et se verra notamment appliquer les règles définies dans le fichier de configuration.

Ces règles vont transformer la représentation externe de l'adresse en une forme canonique interne plus ou moins complexe en fonction du type de fichier de configuration utilisé. Dans tous les cas, après traitements, des informations pertinentes sur chaque adresse peuvent être utilisées :

- *mailer* à utiliser,
- nom du premier relais auquel sera envoyé le message (celui-ci peut être la machine destination),

- partie locale de l'adresse (c'est à dire la partie qui sera examinée par le MTA distant).

Ces informations seront bien entendu utilisées par le filtre à des fins de filtrage et de routage politique.

### 2.2.2 Intégration du filtre

Le filtre interne vient se glisser dans le déroulement du code Sendmail afin d'effectuer ses opérations. La fonction nouvellement créée va se comporter comme toute autre fonction de Sendmail utilisée lors du processus final de délivrance d'un message. Un rejet se traduira tout simplement par un code de retour correspondant à une erreur prédéterminée que la logique saura interpréter.

La solution la plus simple consiste à faire une sélection par destinataire en ne laissant passer que ceux autorisés. Les concepteurs de Sendmail ont presque prévu cette option dans le code. La fonction `checkcompat()` est appelée à chaque adresse de destinataire et permet en fonction de son code de retour de traiter certaines adresses de façon particulière. En l'occurrence, il suffit d'introduire le code du filtre dans cette fonction vide à la livraison et d'ajouter quelques corrections dans le traitement de l'erreur pour que le tour soit joué.

Le principal inconvénient de cette méthode est qu'elle ne permet pas de faire de filtrage *tout ou rien* alors que dans le cahier des charges initial un message doit être intégralement rejeté si l'ensemble des destinataires n'a pas l'autorisation de franchir la passerelle.

Un contournement à ce problème peut être mis en place facilement, il suffit d'attaquer le code juste avant la boucle gestionnaire des dernières opérations de transport du message. Ceci nous permettra de générer un refus global en indiquant pour chaque destinataire s'il est autorisé ou non.

Bien entendu le filtre interne aura des performances incomparables avec la première version proposée puisque l'ensemble des traitement se fait en une seule passe.

## 3. Configuration du filtre

Cette partie s'applique aux deux types de filtres présentés. Le fonctionnement reste le même, seul la logique d'implémentation change en passant d'une solution à l'autre.

Le logique du filtre est basée sur un fichier de configuration unique contenant les règles qui seront appliquées aux différentes adresses. L'exemple ci-dessous montre des solutions de refus et de routage politique.

- Le champ de gauche correspond à l'expression régulière appliquée à l'adresse de l'expéditeur (enveloppe).
- La deuxième colonne est le masque qui sera appliqué à chaque adresse destination.
- En cas de concordance entre source et destination l'action de la troisième colonne est appliquée. Si le champ est vide, le message destinataire est accepté tel quel. Si le champ contient le mot-clé `null` le destinataire est rejeté, dans tout autre cas, l'adresse du destinataire est réécrite de telle sorte que le paramètre de la troisième colonne corresponde au relais vers lequel le message est rerouté.

Ainsi, les deux premières lignes utiles du fichier de configuration vont autoriser tout courrier à destination des utilisateurs du domaine *hsc-sec.fr*. Le paragraphe suivant est utilisé pour rerouter le courrier venant de l'utilisateur *news* d'une quelconque machine du domaine *hsc-sec.fr*. Les messages à destination du domaine *.fr* et de la machine *corton* utilisent la route indiquée, tous les autres sont transmis à un autre relais.

La troisième partie du fichier autorise les utilisateurs du site *frwolf.gna.org* à expédier du courrier, mais celui-ci sera aiguillé par le relais *frelay*.

Pour terminer, tous les utilisateurs du domaine *hsc-sec.fr* sont autorisés à envoyer du courrier aux correspondants de leur choix.

```

# From          To          Relay
#
# We may receive our mail, at least!
.*              ^hsc-sec.fr![^!]*$
.*              ^[^!]*hsc-sec.fr![^!]*$
#
# Force news@hsc-sec.fr
# to send foreign mail via gna
#
^hsc-sec.fr!news$      ^corton![^!]*$
^[^!]*\.hsc-sec.fr!news$ ^corton![^!]*$
^hsc-sec.fr!news$      ^corton![^!]*\.fr!
^[^!]*hsc-sec.fr!news$ ^corton![^!]*\.fr!
^hsc-sec.fr!news$      ^corton!      gna
^[^!]*hsc-sec.fr!news$ ^corton!      gna
#
# *.frwolf.gna.org may not use Fnet
^frwolf.gna.org![^!]*$ .*          frelay
#
# Otherwise user@*.hsc-sec.fr
# can do what they want!
#
^hsc-sec.fr![^!]*$      .*
^[^!]*hsc-sec.fr![^!]*$ .*

```

Le fichier de configuration ne pose aucune difficulté pour qui connaît les expressions régulières Unix. Il faut cependant prendre garde à ne pas oublier d'autoriser le courrier vers les comptes de service (*root*, *postmaster*) dans tous les cas, ou bien comme indiqué dans l'exemple à la totalité du domaine de la passerelle.

La partie de traitement des expressions régulières est dépendante du système utilisé (vivement que POSIX passe par là). Sont pour l'instant fournies les versions pour SVR4, BSD et NeXT.

#### 4. Disponibilité - Autres axes de recherche

Au moment où vous lisez ces lignes, le filtre Sendmail devrait être disponible par ftp anonyme sur [grasp1.univ-lyon1.fr](http://grasp1.univ-lyon1.fr) sous le chemin `/pub/unix/mail/security/filter.shar.Z`. L'adresse IP de la machine est 134.214.100.25, le service de ftp anonyme est ouvert 24h/24.

D'autres axes de recherche sont actuellement étudiés et devraient aboutir à un résultat de filtre dont l'ensemble de la logique est comprise dans le fichier de configuration `sendmail.cf`. Les dernières versions de Sendmail permettent en effet d'évaluer des macros lors de l'exécution, notamment `$f` qui correspond à l'expéditeur. Un ensemble de jeu

de règles dont l'écriture canonique comprendra à la fois l'expéditeur et le destinataire permettra d'effectuer les actions de filtrage en utilisant la grammaire du langage définit par Eric Allman (auteur de Sendmail).

L'inconvénient principal à cette solution est qu'il ne sera pas possible de modifier le corps du message. Le filtrage se limitera donc aux adresses de l'enveloppe.

#### Glossaire

Alias	Synonyme pour une adresse, permet la redirection de messages.
Bang Path	Adresse UUCP donnée en chemin explicite. Exemple : ...!luupsi!tfd!gna!afp!frwolf!wolf
Gecos	Champ contenant les informations utilisateur dans <code>/etc/passwd</code> .
IDA	Institutionen for Datavetenskap (suédois), département Informatique en français. Extensions à Sendmail développées par Lennart Lovstrand du département informatique de l'université de Linköping, Suède.
Mailer	Transporteur de courrier dans la terminologie Sendmail.
Mail queue	File d'attente de messages, c'est à dire répertoire de travail où Sendmail stocke tous les messages en attente.
MTA	Mail Transport Agent. Outil de transport (et en fait aussi de routage) du courrier.
Sendmail	Probablement le plus utilisé des MTA.
SMTP	Simple Mail Transport Protocol, protocole de transport de courrier sur TCP/IP.
UA	User Agent. Interface utilisateur d'accès au courrier.