

# Session N°: 5

## Relais de messagerie sécurisé et libre

**Denis Ducamp**

**[Denis.Ducamp@hsc.fr](mailto:Denis.Ducamp@hsc.fr)**

**Hervé Schauer Consultants**

**<http://www.hsc.fr/>**

# Introduction

- Aujourd'hui un seul serveur de messagerie ne peut assumer toutes les fonctions :**
  - **relayage SMTP sécurisé**
  - **anti-virus**
  - **anti-spam**
- il est donc nécessaire de combiner plusieurs briques.**
- Si l'antivirus permet de protéger les postes clients**
  - **l'architecture doit elle même être solide (séparation des privilèges...)**
  - **et fournir certaines fonctionnalités (anti-relayage, smtp/tls...)**
  - **pour s'adapter aux contraintes de l'Internet.**
- Il est enfin possible de n'utiliser que des logiciels libres**
  - **pour monter une telle architecture.**

# Plan

## □ Présentation des logiciels utilisés

- postfix/tls
- amavisd-new
- SpamAssassin
  - ⇒ DNSBL
  - ⇒ bases de spams
- clamav

## □ Administration

- Côté client
- Clients et serveurs Windows
- Mises à jour anti-virales et anti-spam
- Statistiques

## □ Conclusion

# postfix

- ❑ **Écrit par Wietse Venema (auteur de TCP-Wrapper, Satan et TCT)**
  - <http://www.postfix.org>
- ❑ **Compatibilité sendmail maximale**
- ❑ **Écrit avec la sécurité comme principale préoccupation :**
  - **modulaire :**
    - ⇒ programmes petits et lisibles
    - ⇒ chaque fonction est isolée
  - **chaque module est restreint au maximum :**
    - ⇒ utilisateur postfix
    - ⇒ exécution dans une cage
  - **files d'attente multiples**
  - **pas de programme SUID**
  - **l'architecture est difficile à casser**

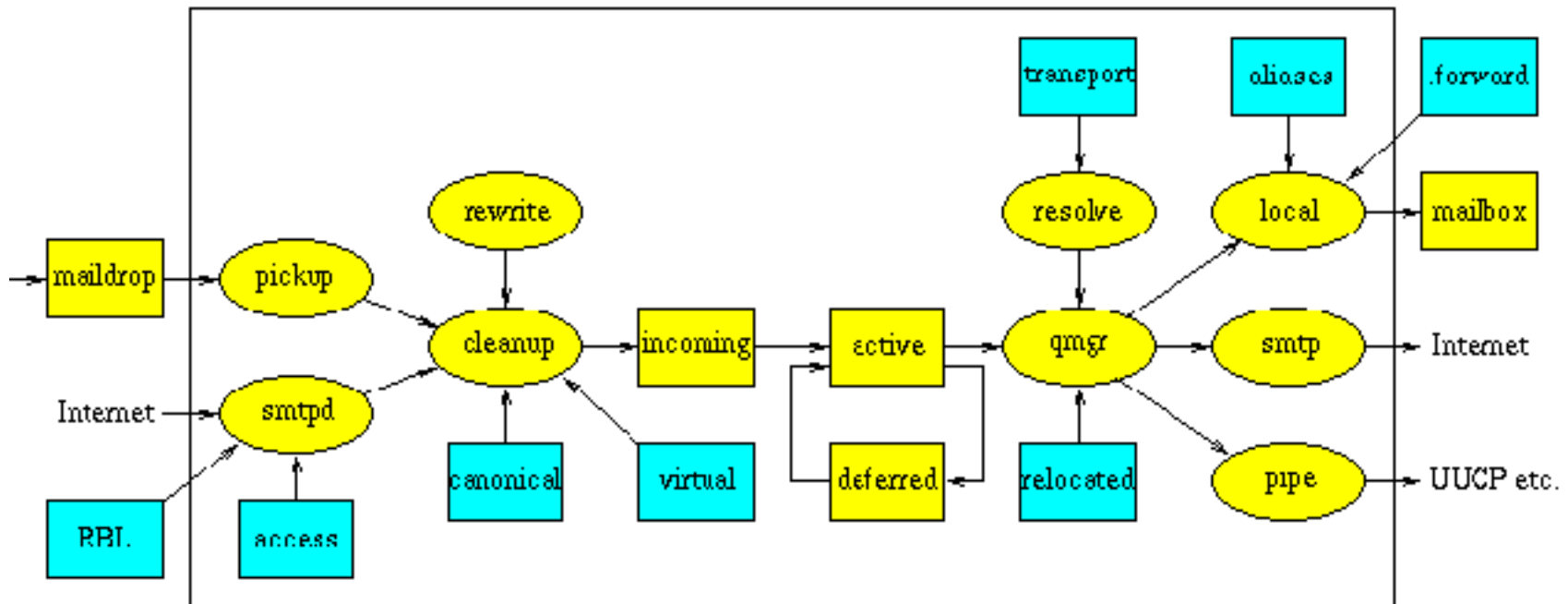
# postfix : architectures

rond jaune : processus

carré bleu : fichier de configuration

carré jaune : file d'attente

*local*, le seul démon privilégié, peut être désactivé sur un relais de



# postfix : anti-spam / anti-relayage

## □ Mécanismes de sécurité anti-spam

### ➤ Liste noire :

#### ⇒ Client

- × adresse IP
- × RBL <http://www.mail-abuse.org/rbl/>
- × absence d'enregistrement inverse dans le DNS.

#### ⇒ HELO (format, domaine)

#### ⇒ MAIL FROM: (adresse, domaine, DNS).

### ➤ Autres :

#### ⇒ Utilisation d'expressions rationnelles dans les entêtes des messages

- × arrêt de certains virus jusqu'à ce que la base anti-virale soit mise à jour
- × interdiction temporaire de certaines extensions de fichiers
  - bagle, mydoom, netsky...

#### ⇒ et dans le corps des messages.

## □ Anti-relayage :

### ➤ Vérification de l'adresse IP cliente ou du RCPT TO:

# postfix : filtrage de contenu

## ❑ Possibilités de filtrage via l'interface `content_filtering`

- “ *Simple content filtering* ” (script de filtrage réexécutant la commande `sendmail` pour réinjecter le message “ marqué ”)
- “ *Advanced content filtering* ” (postfix exécute 2 démons `smtpd`, le marquage est effectué par un relais `smtp` tiers)
- voir le fichier `FILTER_README` dans la distribution.

## ❑ Il est possible d'utiliser avec le filtrage de contenu avancé :

- un relais SMTP anti-virus commercial
- une “ *glue* ” qui communique en SMTP et utilise des outils tiers
  - ⇒ ex : `amavisd-new` utilisant `Mail::SpamAssassin` et plusieurs anti-virus dont `clamav`
- l'envoi en LMTP vers le relais filtrant permet d'avoir des résultats différents pour chaque destinataire
  - ⇒ postfix peut alors générer lui même les avis de non distribution nécessaires
  - ⇒ sinon c'est le relais filtrant qui doit les générer.

## postfix : SMTP/TLS (postfix/tls)

- ❑ **Le chiffrement se fait entre deux serveurs**
- ❑ **SMTP-TLS n'est pas une encapsulation de SMTP dans TLS :**
  - **Le serveur contacté émet l'annonce STARTTLS**
  - **Le client envoie la commande STARTTLS**
  - **Négociation TLS entre les deux parties**
  - **Session SMTP normale dans le flux TLS**
  - **Retour à la bannière (EHLO) à la fin de chaque mail**
- ❑ **Grâce à TLS, il est possible :**
  - **d'authentifier un utilisateur à partir d'un certificat client**
  - **d'imposer un certificat valide dans un réseau privé**
  - **de permettre le relayage depuis et vers l'Internet si le certificat est valide**
- ❑ **Voir <http://www.hsc.fr/ressources/breves/postfix-tls.html>**
  - **comment patcher postfix et configurer la partie TLS.**

## amavisd-new

- ❑ **Démon en perl permettant d'appliquer un filtrage de contenu, anti-virus et anti-spam, à un flux SMTP (LMTP en entrée possible)**
  - <http://www.ijs.si/software/amavisd/>
- ❑ **Utilise le module Mail::SpamAssassin pour détecter les spams**
- ❑ **Sait utiliser de nombreux anti-virus :**
  - **démons ou ligne de commande**
  - **commerciaux et libres.**
- ❑ **Développé pour :**
  - **limiter les risques de perte de mails**
    - ⇒ **il ne prend jamais la responsabilité d'un mail**
    - ⇒ **il ne modifie pas les messages :**
      - × **ajoute un entête, met en quarantaine, rejette ou émet un avis de non délivrance.**
  - **optimiser les flux**
    - ⇒ **peut traiter plusieurs messages simultanément**
    - ⇒ **garde un cache des derniers résultats pour ne pas retraiter le même mail.**

# SpamAssassin

- Filtre en perl permettant de détecter les spams à partir d'un système de notations :**
  - utilise de nombreux tests de types différents, chacun possédant un certain score
  - les scores sont calculés pour maximiser le taux de détection (>>95%) tout en minimisant les risques de faux positifs (<<<0,1%)
- Logiciel libre de qualité professionnelle :**
  - McAfee SpamKiller Technology “ *Powered by McAfee SpamAssassin* ”
- Peut être utilisé**
  - par un utilisateur final depuis procmail ou via un relais pop3
  - dans un relais SMTP via le module Mail::SpamAssassin
- ATTENTION : le filtrage anti-spam prend beaucoup plus de ressources que le filtrage anti-virus :**
  - mémoire, temps réel et temps utilisateur.

# DNSBL

- Une DNSBL est une Black List DNS :**
  - Toutes les adresses IP que le serveur connaît sont suspectes
- Les natures des adresses IP peuvent différer :**
  - Adresses IP d'où des spams ont été envoyés
  - Adresses IP de serveurs relais ouverts sur Internet
  - Adresses IP de clients de FAI sur des plages d'adresses dynamiques
  - Etc.
- Les politiques de gestion de ces listes diffèrent :**
  - Modalités d'entrée/sortie, réactivité, etc.
- SpamAssassin et postfix peuvent tous les deux utiliser des DNSBL.**
- Site de test : <http://www.dnsstuff.com/>**
- Listes de DNSBL : <http://www.moensted.dk/spam/> et <http://www.declude.com/junkmail/support/ip4r.htm>**

# Bases de spams

- Des bases de spams sont confectionnées de façon collaborative**
  - Grâce à la collaboration de ses utilisateurs.
  
- Chaque message reçu est comparé à une base centrale**
  - Entre le “ *client* ” et le “ *serveur central* ” seuls des “ *hashs* ” sont échangés.
  
- Certains systèmes permettent de détecter des spams “ *mutants* ”**
  - en comparant des parties de messages
  
- Certains systèmes utilisent un “ *niveau de confiance/spammicité* ”**
  
- De telles bases sont Razor, Pyzor et DCC**
  - SpamAssassin sait les utiliser toutes les trois.

# clamav

- Anti-virus libre destiné à filtrer les messages électroniques**
  - <http://www.clamav.net>
- Peut aussi être utilisé en ligne de commande pour scanner une arborescence**
  - Sous Linux un module noyau (en cours de développement) permet de scanner tout fichier lors de son ouverture et d'en interdire l'accès s'il est infecté.
- Un démon clamd permet d'optimiser les performances en n'initialisant le moteur qu'une seule fois.**
- La priorité est portée sur la mise à jour des virus au fur et à mesure des nouvelles apparitions aidés par des ISP pour les détecter**
  - mais la base est aussi complétée avec les anciens virus qui ne sont plus (ou peu) en activité.
- Le support des fichiers office (word, excel...) est toujours désactivé.**



# Clients et serveurs Windows

- ❑ Pour les clients Windows il est possible d'y utiliser un relais
  - POP3 : <http://mcd.perlmonk.org/pop3proxy/>
  - IMAP : <http://sourceforge.net/projects/imapassassin>
- ❑ mais requière d'installer SpamAssassin sous Windows :
  - <http://www.openhandhome.com/howtosa.html>
- ❑ Il existe aussi des programmes et plugins payants :
  - Bloomba et SAproxyPro : <http://www.statalabs.com/>
  - Plugin eudora : <http://www.spamnix.com/>
  - SpamKiller : <http://www.nai.com/>

## Mises à jour anti-virales

- Les deux systèmes de filtrage de contenus installés doivent être mis à jour régulièrement pour s'adapter aux nouveautés.
  
- Pour clamav, lancer la commande *freshclam*
  - soit en mode démon
  - soit depuis la crontab de l'utilisateur amavis
  
- Il est aussi possible de déclencher la mise à jour lors de la réception d'un mail dans la liste [clamav-virusdb@lists.sourceforge.net](mailto:clamav-virusdb@lists.sourceforge.net)

## Mises à jour anti-spam

- ❑ Pour SpamAssassin l'utilisation des DNSBL et des bases de spams permet de faire contrepoids aux bases de règles statiques.
- ❑ Il est tout de même possible d'utiliser des bases de règles générées par d'autres personnes
  - le script *my\_rules\_du\_jour* permet de télécharger plusieurs listes de ce type :
    - ⇒ <http://www.exit0.us/index.php/RulesDuJour>
- ❑ **ATTENTION** : il est important de vérifier que des jeux de règles tiers utilisés ne génèrent pas de faux positifs
  - pour cela il faut essayer ces règles sur deux corpus de hams et spams, représentatifs des mails reçus et datant de moins de 6 mois
  - par exemples *chickenpox.cf* et *tripwire.cf* peuvent être la cause de faux positifs sur de longs mails en français
  - les raisons des faux positifs avec l'utilisation de nouvelles règles sont :
    - ⇒ que les scores du nouvel ensemble de tests n'ont pas été recalculés en incluant les nouvelles règles
    - ⇒ les corpus de hams utilisés pour tester les nouvelles règles sont souvent non significatifs des hams reçus par des tiers.

# Statistiques

- ❑ **Les graphes statistiques générés à partir des journaux permettent souvent**
  - **de détecter des problèmes ou**
  - **de voir les conséquences de modifications.**
- ❑ **Plusieurs outils existent, tous utilisant rrdtool**
  - <http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/> :
  - **amavis-stats** : <http://rekudos.net/amavis-stats/>
    - ⇒ **comptabilise pour 1 jour / semaine / mois / an les messages passés, infectés et les spams**
  - **mailgraph** : <http://people.ee.ethz.ch/~dws/software/mailgraph/>
    - ⇒ **comptabilise pour 1 jour / semaine / mois / an les messages envoyés et reçus, les rejets, les bounce, les virus et les spams**
  - **queuegraph** : <http://www.stahl.bau.tu-bs.de/~hildeb/postfix/queuegraph/>
    - ⇒ **comptabilise pour 1 jour / semaine / mois / an les messages dans la queue deferred et dans les autres queues.**

# Conclusion

- ❑ L'architecture ainsi construite permet d'effectuer un filtrage de contenu sur les mails reçus.
- ❑ Ainsi installé amavisd-new :
  - ajoute un marquage sur tous les messages avec un virus
    - ⇒ et envoie un avis à l'administrateur
  - ajoute un marquage à tous les spams destinés au domaine local
- ❑ Il est fait confiance à l'utilisateur pour filtrer ses messages
  - suivant les marques ajoutées par amavisd-new
- ❑ Il sera intéressant lorsque le système sera testé et optimisé :
  - de mettre en quarantaine les virus
  - de rajouter l'envoi d'un avis de mise en quarantaine aux destinataires dans le domaine local
  - de mettre en quarantaine les “ gros ” spams.

**Ne jamais envoyer d'avis de non délivrance aux domaines extérieurs.**

## Références

Car rien ne remplacera une personne bien informée

☐ [http://www.admi.net/cgi-bin/wiki?Lutte\\_Contre\\_Le\\_Spam](http://www.admi.net/cgi-bin/wiki?Lutte_Contre_Le_Spam)

- ⇒ avec des actualités,
- ⇒ des liens et ressources,
- ⇒ des initiatives professionnelles et
- ⇒ des organismes de lutte contre le spamming

☐ <http://caspam.org>

➤ CASPAM - Collectif Anti Spam

- ⇒ avec “ 6 choses à faire ou ne pas faire pour lutter contre le spam !! ”

☐ [http://www.cnil.fr/thematic/internet/spam/spam\\_sommaire.htm](http://www.cnil.fr/thematic/internet/spam/spam_sommaire.htm)

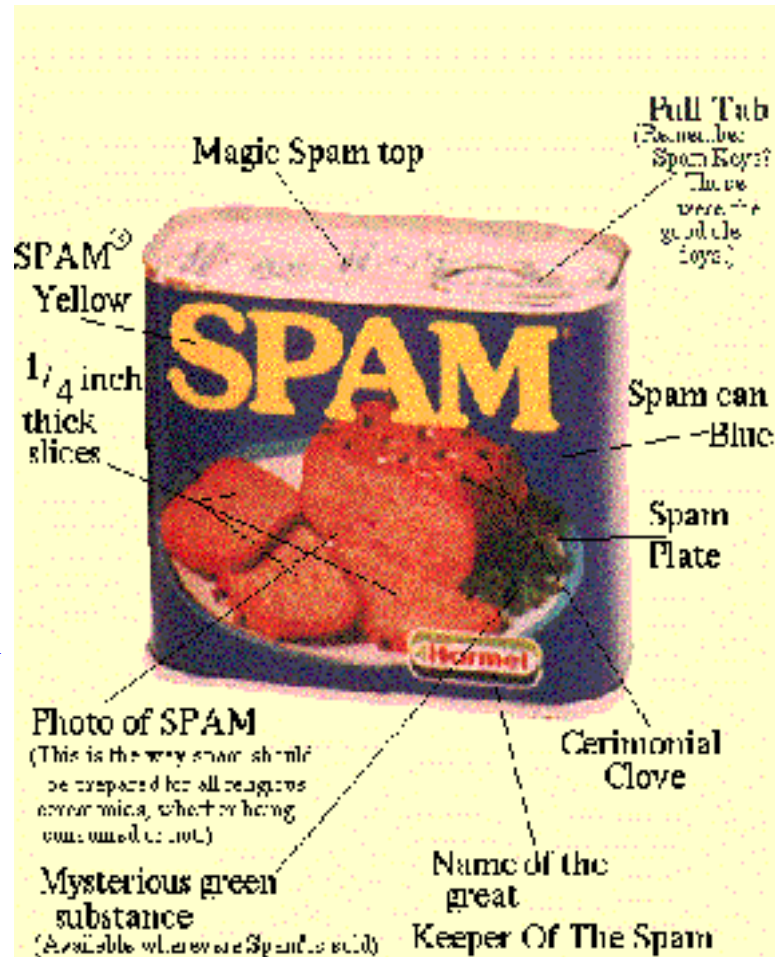
➤ CNIL - Halte au spam

- ⇒ avec “ comment se prémunir ? ”

☐ <http://www.hoaxbuster.com/>

➤ Première ressource francophone sur les hoax

- ⇒ les derniers canulars circulant sur le réseau



# Merci de votre attention

**N'hésitez pas à poser vos questions**

et à venir visiter le site WEB de HSC : <http://www.hsc.fr/>  
pour y lire les autres présentations sur le même sujet :

**Éléments de réflexion sur le spam**

➤ <http://www.hsc.fr/ressources/presentations/ddmspam/>

**SpamAssassin**

➤ <http://www.hsc.fr/ressources/presentations/spamassassin/>

**Serveur de messagerie sécurisé et libre (avec la partie installation)**

➤ <http://www.hsc.fr/ressources/presentations/SrvMessagSecLib/>

**et sur bien d'autres sujets de sécurité...**