Filtrez vos spams avec Rmilter et Rspamd

RMLL Montpellier

8 Juillet 2014

Maxime Graff

Contexte

Pourquoi auto-héberger ses données ?

Contexte

- Participer à la construction d'un Internet décentralisé et résistant

Contexte

- Participer à la construction d'un Internet décentralisé et résistant
- Eviter de stocker ses données chez des sociétés privées

Contexte

- Participer à la construction d'un Internet décentralisé et résistant
- Eviter de stocker ses données chez des sociétés privées
- Avoir le contrôle et la responsabilité de ses propres données

Contexte

- Participer à la construction d'un Internet décentralisé et résistant
- Eviter de stocker ses données chez des sociétés privées
- Avoir le contrôle et la responsabilité de ses propres données
- Apprendre et progresser, pour les technophiles

Serveur de messagerie

Comment est architecturé un serveur de messagerie ?

Serveur de messagerie

- MTA (**Mail Transfert Agent**)
  Programme chargé des transferts des messages

Serveur de messagerie

- MTA (**Mail Transfert Agent**)
  Programme chargé des transferts des messages
- MDA (**Mail Delivery Agent**)
  Programme chargé de stocker les messages dans des boîtes aux lettres

Serveur de messagerie

- MTA (**Mail Transfert Agent**)
  Programme chargé des transferts des messages
- MDA (**Mail Delivery Agent**)
  Programme chargé de stocker les messages dans des boîtes aux lettres
- **Programmes tiers**
  Anti-Virus, Anti-Spam, etc.

Solutions

Quelles solutions existent ?

Solutions

- MTA : Sendmail, Postfix, Exim

Solutions

- MTA : Sendmail, Postfix, Exim
- MDA : Dovecot, Courier, Cyrus

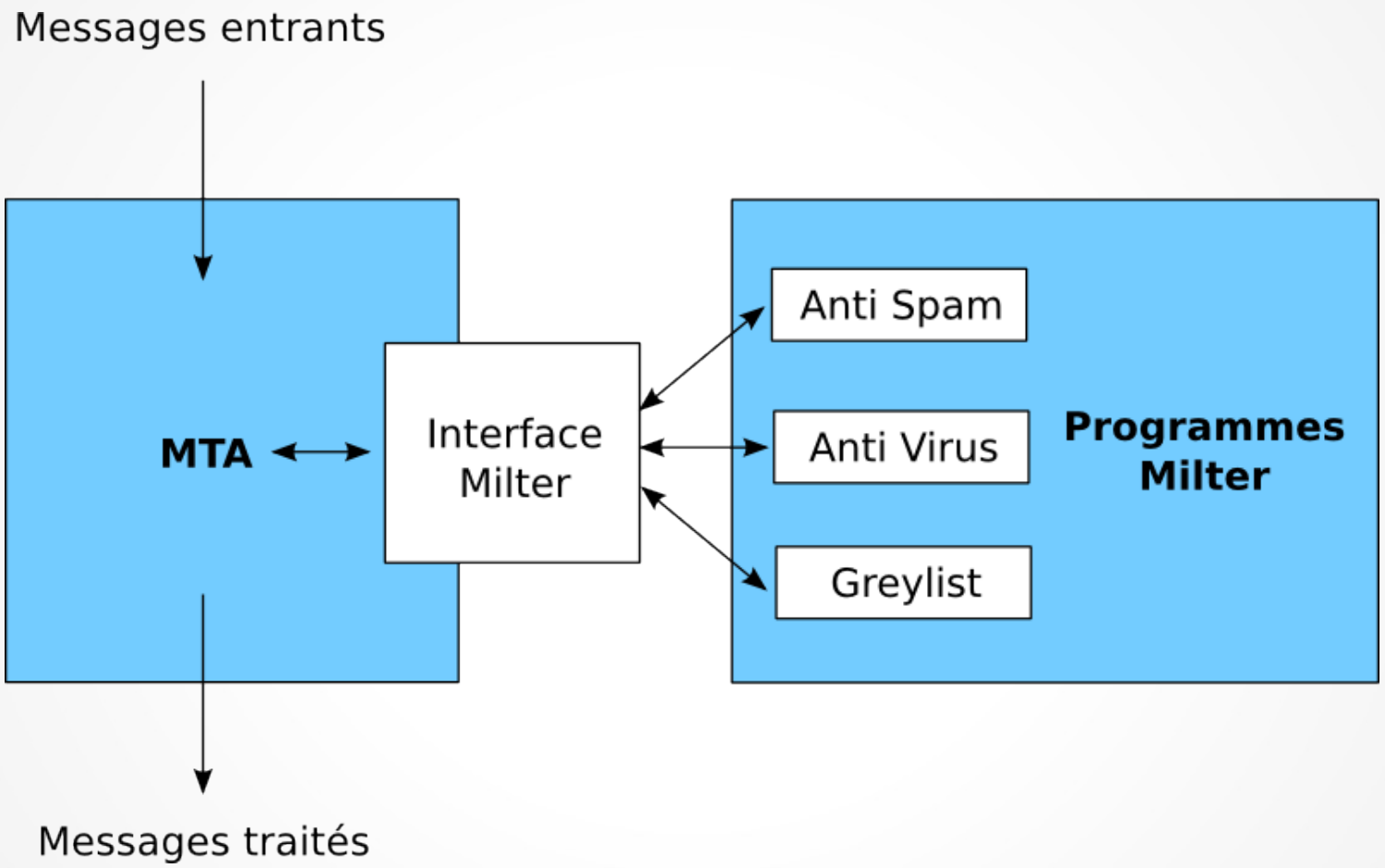
Solutions

- MTA : Sendmail, Postfix, Exim
- MDA : Dovecot, Courier, Cyrus
- Anti-Spam : SpamAssassin, Dspam, Rspamd

Solutions

- MTA : Sendmail, Postfix, Exim
- MDA : Dovecot, Courier, Cyrus
- Anti-Spam : SpamAssassin, Dspam, Rspamd
- Anti-Virus : ClamAV

Architecture



Milter

Qu'est-ce que le protocole Milter ?

Milter

- API

Milter

- API
- Permet une communication entre le MTA et des programmes tiers

Milter

- API
- Permet une communication entre le MTA et des programmes tiers
- Les programmes tiers agissent comme des filtres

Milter

- API
- Permet une communication entre le MTA et des programmes tiers
- Les programmes tiers agissent comme des filtres
- Evite au MTA d'avoir à gérer cette tâche

Milter

- API
- Permet une communication entre le MTA et des programmes tiers
- Les programmes tiers agissent comme des filtres
- Evite au MTA d'avoir à gérer cette tâche
- La liste des filtres qui doivent être utilisés est fixée dans la configuration du MTA

Milter

Pourquoi Milter ?

Milter

- **Sécurité**

  Pas de privilège particulier nécessaire

Milter

- **Sécurité**

  Pas de privilège particulier nécessaire

- **Stabilité**

  L'indisponibilité d'un programme milter n'entraîne pas d'indisponibilité totale du service

Milter

- **Sécurité**

  Pas de privilège particulier nécessaire

- **Stabilité**

  L'indisponibilité d'un programme milter n'entraîne pas d'indisponibilité totale du service

- **Simplicité**

  Chaque programme milter effectue une tâche dédiée

Milter

- **Sécurité**

  Pas de privilège particulier nécessaire

- **Stabilité**

  L'indisponibilité d'un programme milter n'entraîne pas d'indisponibilité totale du service

- **Simplicité**

  Chaque programme milter effectue une tâche dédiée

- **Performance**

  Pas de pénalisation globale des performances du MTA

Critères de filtrage

Sur quels critères s'appuient les filtres ?

Critères de filtrage

- **Les informations de connexion**

  Adresses IP source et destination

Critères de filtrage

- **Les informations de connexion**

  Adresses IP source et destination

- **L'enveloppe**

  Adresses expéditrice et destinataire(s), serveurs intermédiaires, horodatage

Critères de filtrage

- **Les informations de connexion**

  Adresses IP source et destination

- **L'enveloppe**

  Adresses expéditrice et destinataire(s), serveurs intermédiaires, horodatage

- **Les en-têtes**

  From, To, Date, Subject, etc.

Critères de filtrage

- **Les informations de connexion**

  Adresses IP source et destination

- **L'enveloppe**

  Adresses expéditrice et destinataire(s), serveurs intermédiaires, horodatage

- **Les en-têtes**

  From, To, Date, Subject, etc.

- **Le corps du message**

Rmilter

Qu'est-ce que Rmilter ?

Rmilter

- Ecrit en C

Rmilter

- Ecrit en C
- Sous license BSD

Rmilter

- Ecrit en C
- Sous license BSD
- Agit comme interface Milter unique pour Sendmail et Postfix

Rmilter

- Ecrit en C
- Sous license BSD
- Agit comme interface Milter unique pour Sendmail et Postfix
- Centralise les tâches de filtrage des messages

Fonctionnalités internes

- Vérification SPF (Sender Policy Framework)

Fonctionnalités internes

- Vérification SPF (Sender Policy Framework)
- Vérification DCC (Distributed Checksum Clearinghouses)

Fonctionnalités internes

- Vérification SPF (Sender Policy Framework)
- Vérification DCC (Distributed Checksum Clearinghouses)
- Greylist (liste grise)

Fonctionnalités internes

- Vérification SPF (Sender Policy Framework)
- Vérification DCC (Distributed Checksum Clearinghouses)
- Greylist (liste grise)
- Rate limiting (limitateur de débit)

Fonctionnalités internes

- Vérification SPF (Sender Policy Framework)
- Vérification DCC (Distributed Checksum Clearinghouses)
- Greylist (liste grise)
- Rate limiting (limitateur de débit)
- Auto-whitelisting

Fonctionnalités internes

- Vérification SPF (Sender Policy Framework)
- Vérification DCC (Distributed Checksum Clearinghouses)
- Greylist (liste grise)
- Rate limiting (limitateur de débit)
- Auto-whitelisting
- Expressions régulières

Fonctionnalités externes

- Filtrage des virus avec ClamAV

Fonctionnalités externes

- Filtrage des virus avec ClamAV
- Filtrage des spams avec SpamAssassin ou Rspamd

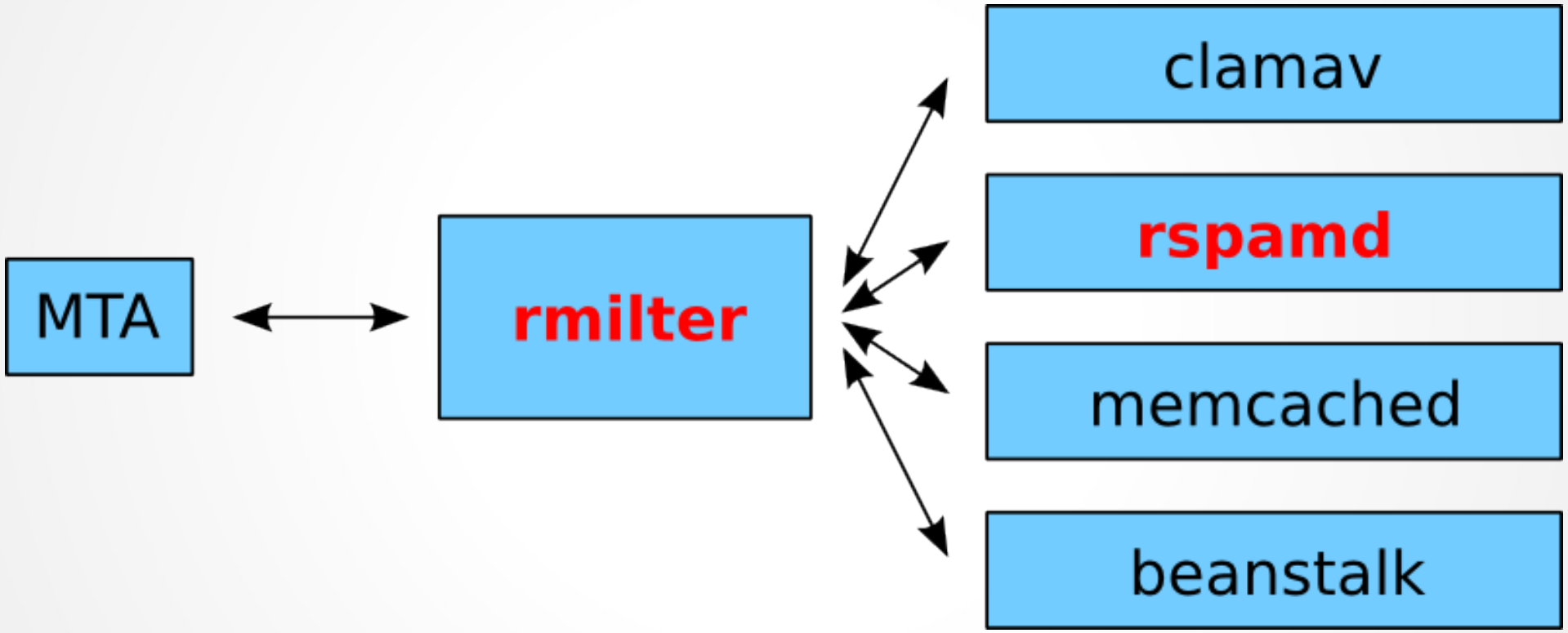
Fonctionnalités externes

- Filtrage des virus avec ClamAV
- Filtrage des spams avec SpamAssassin ou Rspamd
- Interfaçage avec un serveur memcached pour stocker les listes grises, blanches et le rate-limit

Fonctionnalités externes

- Filtrage des virus avec ClamAV
- Filtrage des spams avec SpamAssassin ou Rspamd
- Interfaçage avec un serveur memcached pour stocker les listes grises, blanches et le rate-limit
- Interfaçage avec un ou plusieurs serveurs Beanstalk (Message queues) afin d'envoyer des copies de messages

Architecture



Rspamd

Qu'est-ce que Rspamd ?

Rspamd

- Ecrit en C

Rspamd

- Ecrit en C
- Sous license BSD

Rspamd

- Ecrit en C
- Sous license BSD
- Fournit un système de filtrage des spams efficace (utilisation de la libevent)

Rspamd

- Ecrit en C
- Sous license BSD
- Fournit un système de filtrage des spams efficace (utilisation de la libevent)
- Possibilité d'étendre ses fonctionnalités avec des filtres et plugins écrits en Perl et LUA

Rspamd

- Ecrit en C
- Sous license BSD
- Fournit un système de filtrage des spams efficace (utilisation de la libevent)
- Possibilité d'étendre ses fonctionnalités avec des filtres et plugins écrits en Perl et LUA
- Fournit des statistiques détaillées

Rspamd

- Ecrit en C
- Sous license BSD
- Fournit un système de filtrage des spams efficace (utilisation de la libevent)
- Possibilité d'étendre ses fonctionnalités avec des filtres et plugins écrits en Perl et LUA
- Fournit des statistiques détaillées
- Interface web d'administration disponible

Filtres internes en C

regexp

Module central permettant de définir des règles basées sur des expressions régulières

Filtres internes en C

surbl

Module permettant d'extraire les URLs présentes dans le message et vérifier leur présence dans des listes noires publiques d'URLs malicieuses

Filtres internes en C

spf et **dkim**

Modules permettant la vérification des enregistrements SPF et des signatures DKIM

Filtres internes en C

fuzzy_check

Module permettant de vérifier la présence du fuzzy hash du message dans une liste

Filtres internes en C

chartable

Module permettant de vérifier les jeux de caractères utilisés dans le message

Modules LUA fournis

rbl

Module vérifiant la présence de l'expéditeur dans les RBL (listes noires)

Modules LUA fournis

maillist

Module spécialisé dans la vérification des messages issus de listes de diffusion

Rspamd

Comment fonctionne Rspamd ?

Rspamd

- Chaque module définit des règles (rules)

Rspamd

- Chaque module définit des règles (rules)
- Chaque règle correspond à une propriété

  Ex: `BAYES_SPAM` (signifie que le message est considéré comme un spam par le filtre statistique)

Rspamd

- Chaque module définit des règles (rules)
- Chaque règle correspond à une propriété
  Ex: `BAYES_SPAM` (signifie que le message est considéré comme un spam par le filtre statistique)
- Chaque règle est associée à un poids

Rspamd

- Chaque module définit des règles (rules)
- Chaque règle correspond à une propriété
  Ex: `BAYES_SPAM` (signifie que le message est considéré comme un spam par le filtre statistique)
- Chaque règle est associée à un poids
- Les poids positifs tendent à considérer le message comme un spam, et les poids négatifs comme un ham

Rspamd

- L'ordonnanceur de règles est optimisé pour les performances et la fiabilité

Rspamd

- L'ordonnanceur de règles est optimisé pour les performances et la fiabilité
- Dès qu'un message est considéré comme un spam, les vérifications s'arrêtent

Rspamd

- L'ordonnanceur de règles est optimisé pour les performances et la fiabilité
- Dès qu'un message est considéré comme un spam, les vérifications s'arrêtent
- Les règles négatives sont calculées avant les autres pour éviter les faux positifs

Rspamd

- L'ordonnanceur de règles est optimisé pour les performances et la fiabilité
- Dès qu'un message est considéré comme un spam, les vérifications s'arrêtent
- Les règles négatives sont calculées avant les autres pour éviter les faux positifs
- Les règles appliquées en priorité sont :
  - celles qui sont le plus souvent vérifiées
  - les règles aux poids les plus forts
  - celles qui s'exécutent le plus vite

Ressources

- **Rmilter** http://github.com/vstakhov/rmilter/
- **Rspamd** http://github.com/vstakhov/rspamd/

- **Syloé** http://www.syloe.fr/

- **Réseau libre entreprise**
  http://www.libre-entreprise.org/

Merci

Des questions ?