

Sujet

Passerelle anti-spam et anti-virus haute performance

par

ALIXEN

Présentation de Etienne Etournay - info@alixen.fr

Plan

- **Introduction : le besoin**
- **Architecture et outils**
 - Principes
 - Description des outils utilisés
- **Exemple live : le MEN**
 - Volumétrie
 - Problèmes et Solutions
- **Évolutions**

Le besoin

- **Plateforme anti-spam et anti-virus basée sur des logiciels libres :**
 - Protection SMTP périmétrique
 - Forte volumétrie
 - Multi-domaines
 - Multi-sites
 - Haute disponibilité
 - Intégration (optionnelle) d'outils commerciaux

Architecture et outils

Schéma de principe

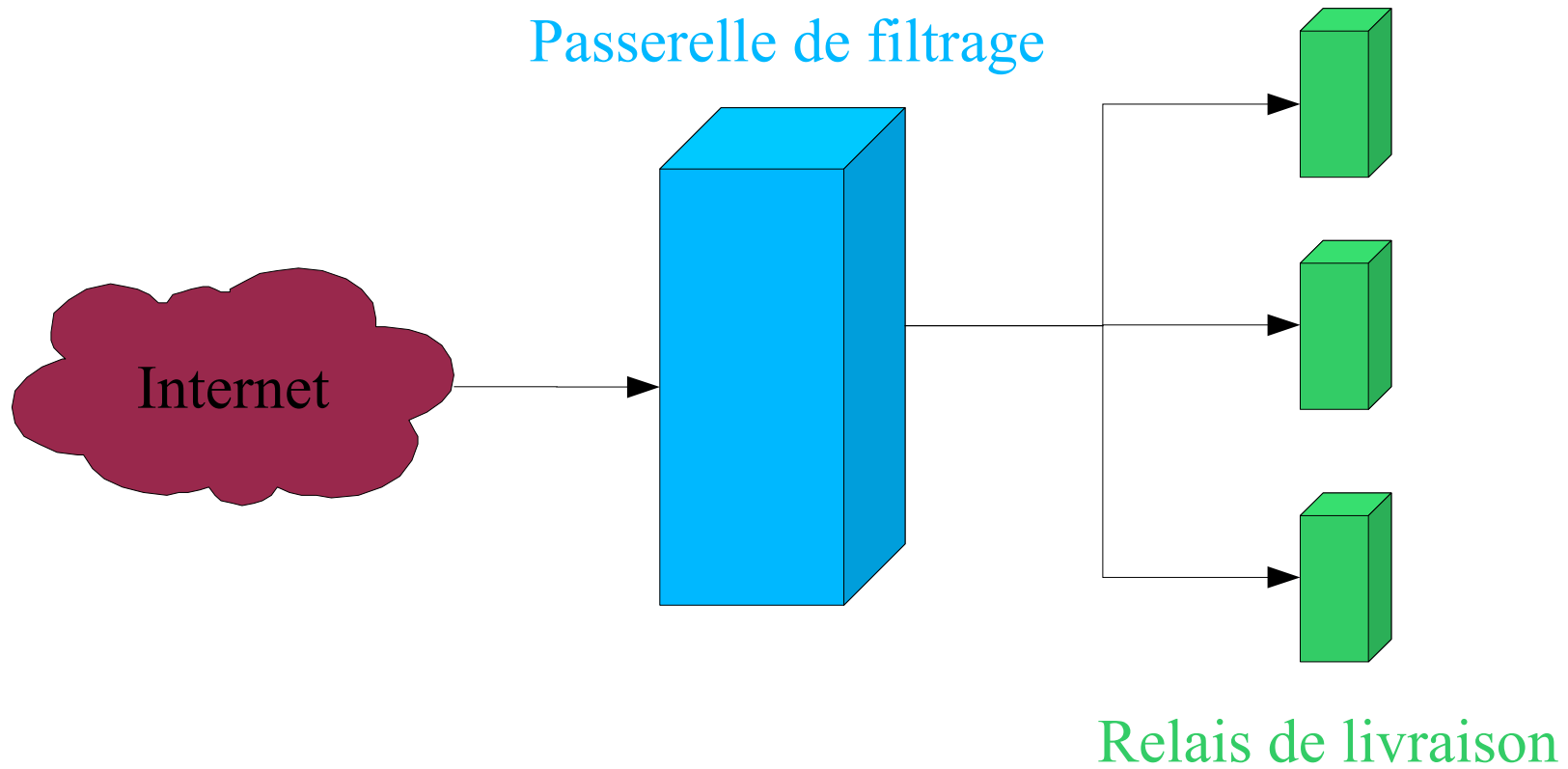
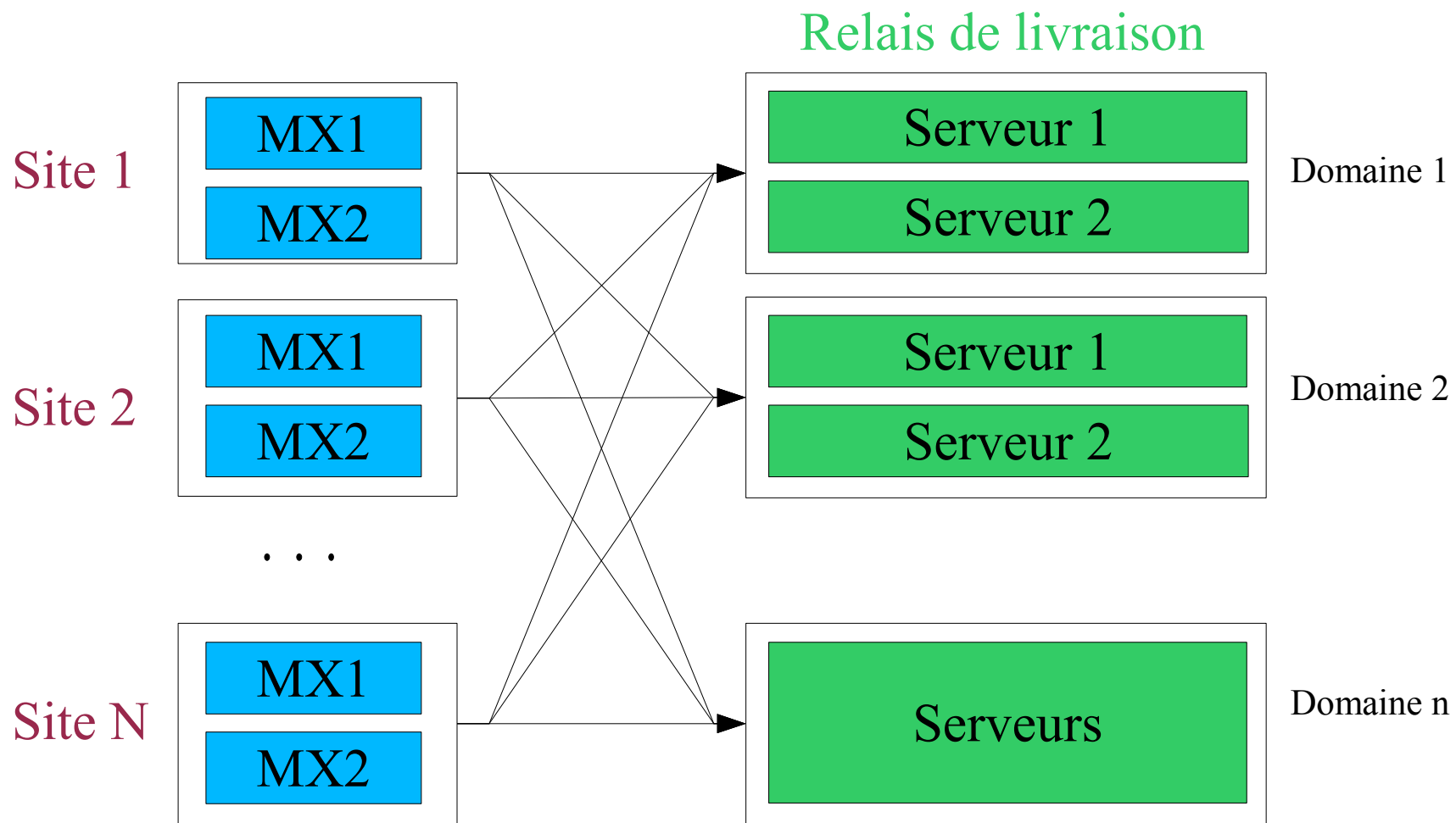


Schéma de principe (détail)



Solution logicielle

• Plateforme système

- Système d'exploitation : Linux

• Serveur SMTP

- Postfix
- Greylisting : Postgrey/Milter-greylist

Solution logicielle

• Solution de filtrage

- Logiciel de filtrage avancé : MailScanner
- Anti-virus : Clamav
- Anti-spam : SpamAssassin
- Solution commerciale optionnelle

Mailscanner

• **Coordinateur des outils**

- **Sous traite les analyses (« plugins »)**
- **Interface vers les anti-virus propriétaires**
- **Modifie les entêtes des courriels**
- **Modifie les contenus**
- **Gestion directe de listes blanches et noires**
- **Accès direct aux files d'attente Postfix**

Clamav

• **Anti virus libre**

- **Mises à jour des signatures par Internet**
- **Ne modifie pas les fichiers**
- **Fonctionne aussi en mode poste de travail**
- **Linux et Windows**

Spam assassin

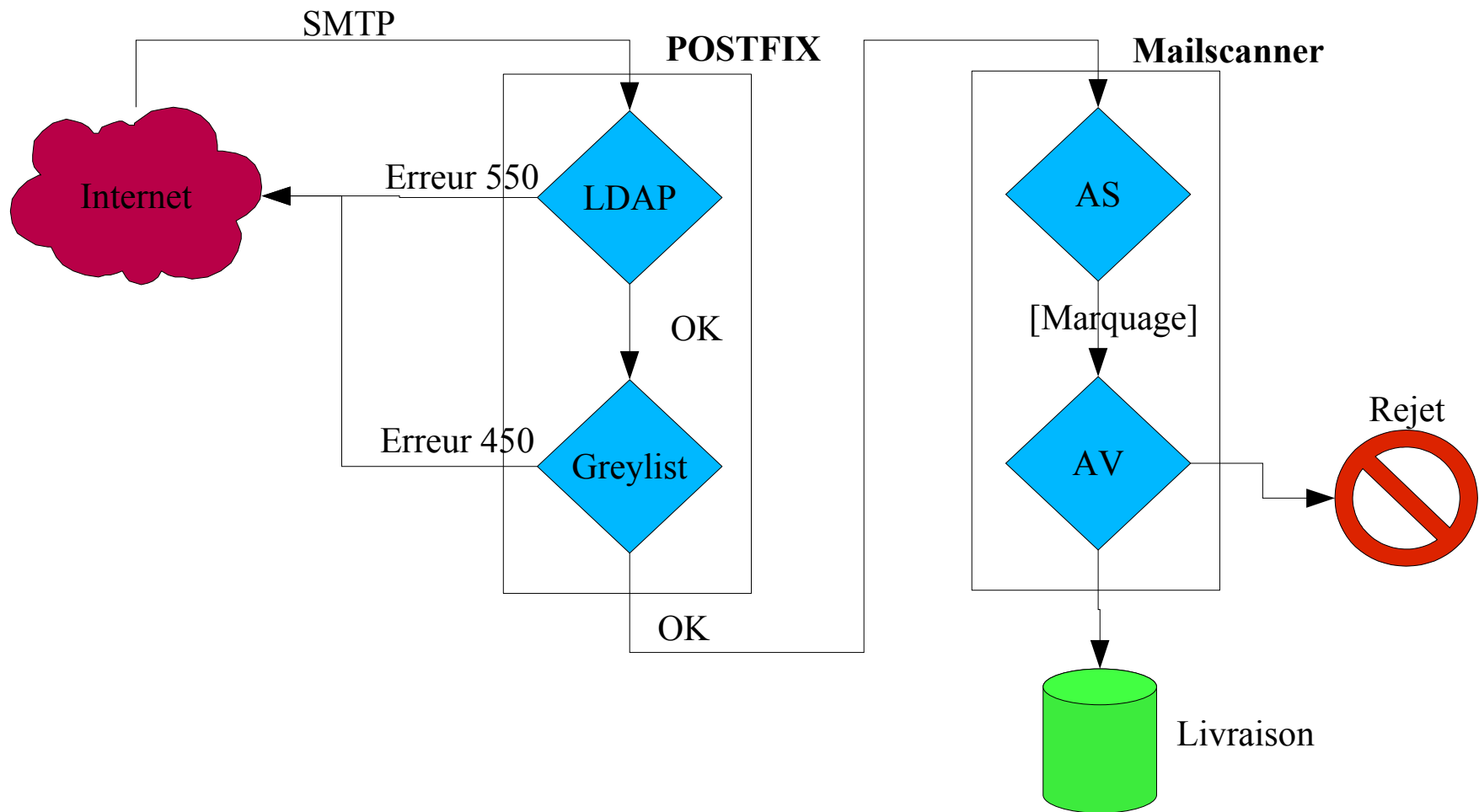
☛ Analyse des courriels

- Collection de filtres (plusieurs dizaines)
- Calcul d'une note pondérée

☛ Liste des filtres principaux

- Bayésien
- DCC (Distributed Checksum Clearinghouse Checksum Clearinghouse)
- RBL (Realtime Black Lists)
- ...

Schéma de flux



Exemple live : le MEN

Présentation

• En production

- 3 serveurs sur 2 sites
- 2 domaines (350.000 boîtes)

• En cours de déploiement

- 2 serveurs sur 1 site supplémentaire
- ~30 domaines (15.000 boîtes)

• Évolutions

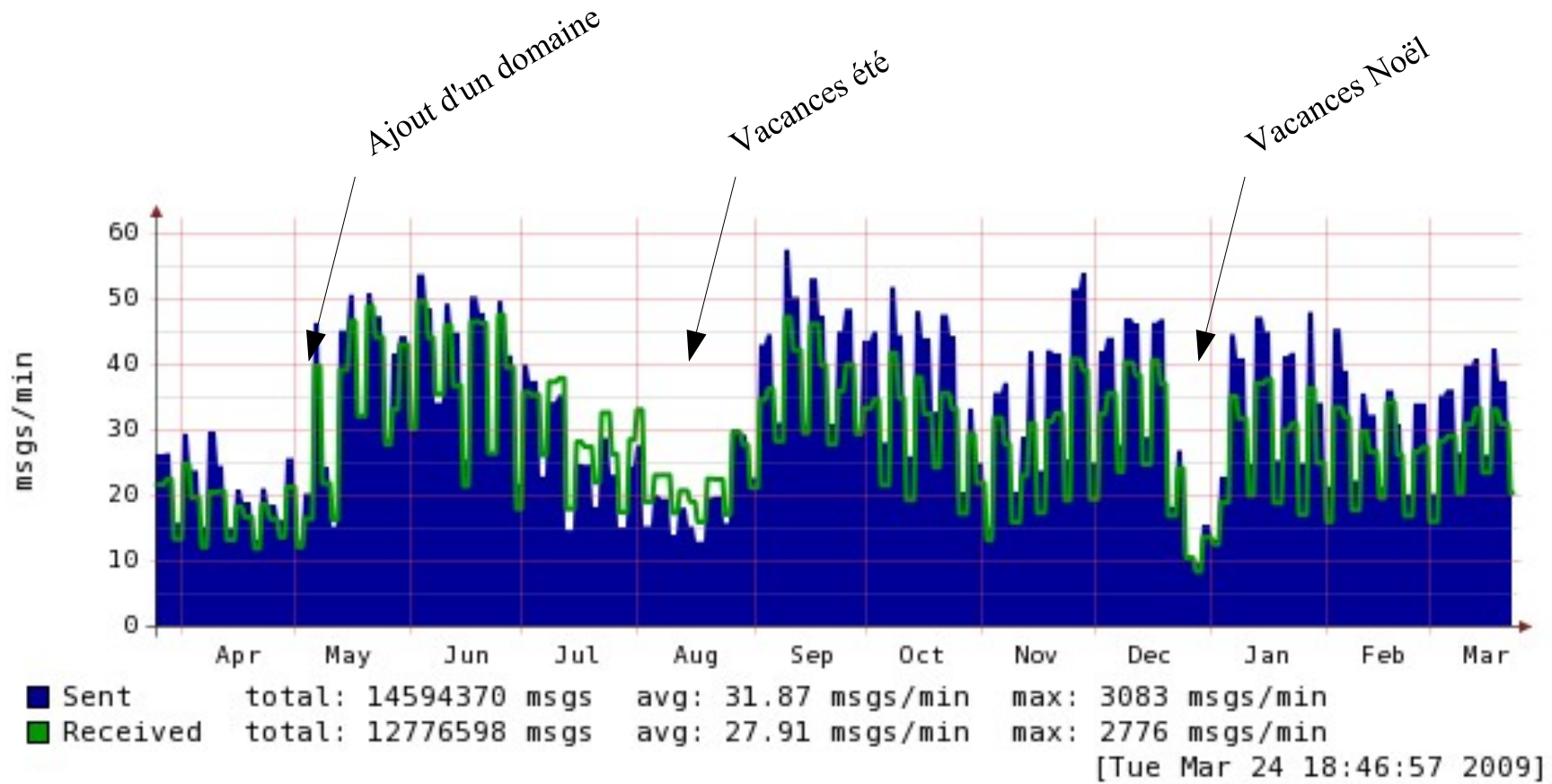
- > 1 M de boîtes multi-domaines

Volumétrie

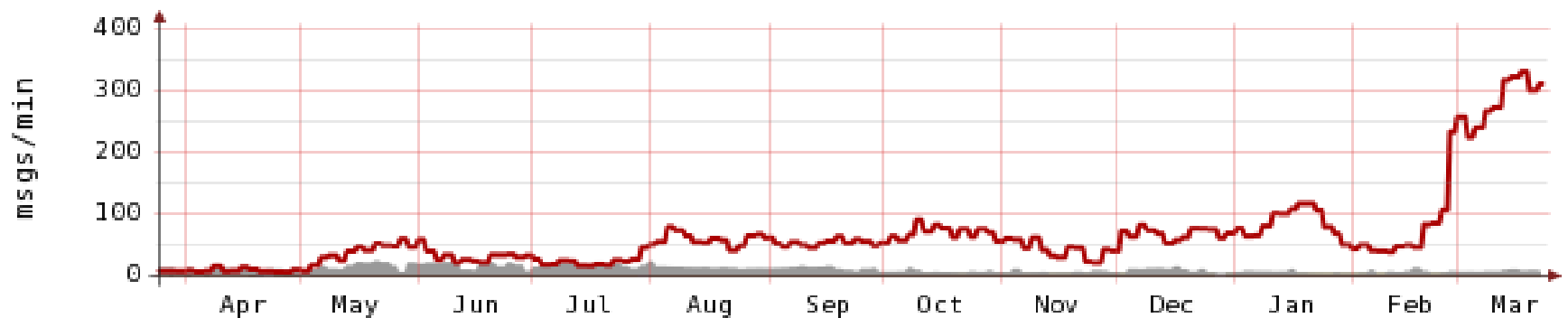
• Trafic (à ce jour)

- 350 000 boîtes
- 50 000 messages par jour
- 250 000 rejets par jour
- 7200 msg/h aux heures de pointe
- 30% des messages marqués spam
- 25 mails contenant un virus par jour

Volumétrie



Volumétrie



RRDTOOL / TOBI OETIKER

■ Bounced	total:	4597 msgs	avg:	0.01 msgs/min	max:	81 msgs/min
■ Viruses	total:	6269 msgs	avg:	0.01 msgs/min	max:	54 msgs/min
■ Spam	total:	3810086 msgs	avg:	8.30 msgs/min	max:	420 msgs/min
■ Rejected	total:	29396795 msgs	avg:	64.49 msgs/min	max:	7994 msgs/min

[Tue Mar 24 18:46:57 2009]

Architecture générale

• Tenue en charge

- 1 ou 2 serveurs par site
- MX primaires des domaines locaux

• Haute disponibilité

- MX secondaires de domaines distants

Problèmes et Solutions

Problèmes rencontrés

- **Problème du greylisting**
 - Délais de livraison parfois très long
 - Pas de livraison
- **Forte charge système**
 - Forte charge sur les Entrées/Sorties
 - Mémoire saturée
- **Arrêt des livraisons lors de panne LDAP**
 - Plus de livraisons pendant la panne

Problème du greylisting

• Identification des causes

- Délai de re-soumission du serveur expéditeur très long (> 24h)
- Le même message est soumis successivement aux différents relais

Problème du greylisting

• Outil initial : Postgrey

- Intérêt : outil standard du MTA Postfix
- Inconvénients : message greylisté plusieurs fois (sur chaque MX)

• Outil remplaçant : Milter-greylist

- Partage de sa base de greylisting entre MX : message greylisté qu'une seule fois

• Liste blanche

- Ajout en liste blanche de FAI

Problème de charge

- **Diagnostic : Milter-greylst en cause**
 - Le processus dépasse souvent 4 Go
 - Milter-greylst sauve sa base toutes les 10 minutes dans un fichier, provoquant alors l'écriture sur disque de 200 Mo environ

Optimisation de Milter-Greylis

• Paramètres optimisés

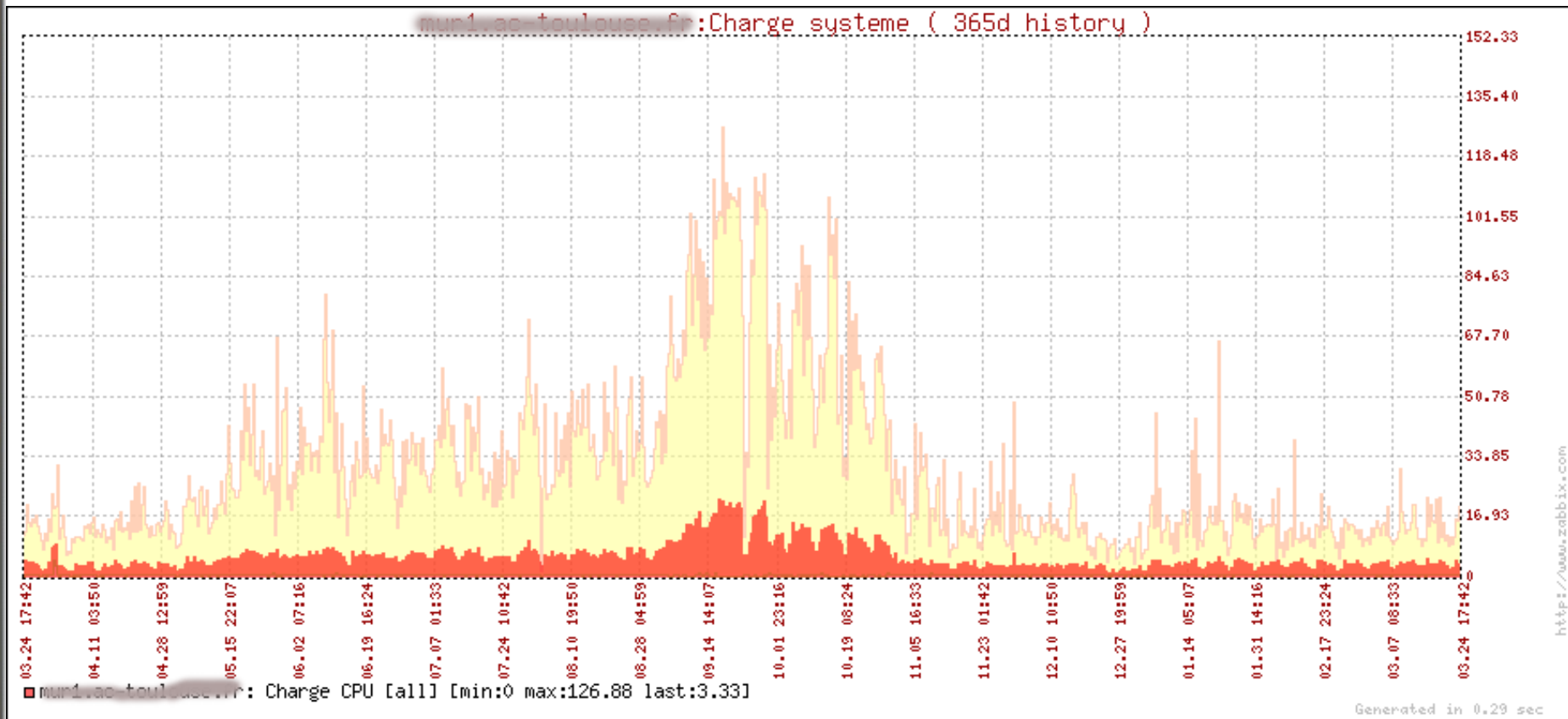
- Redémarrage du service une fois pas jour (rotation logs)
- La limite de conservation est définie par défaut à 5 jours : elle a été rabaissée à 2
- Sauvegarde une fois par heure
- Pas de formatage des dates dans le fichier

Optimisation de Milter-greylst

• Résultats obtenus

- **Mémoire : le processus consomme moins de 500 Mo au lieu de 4 Go**
- **Le taux d'écriture disque a fortement baissé**
- **La charge moyenne est passé de 11 à 2.5**

Optimisation de Milter-greylist



Pannes LDAP

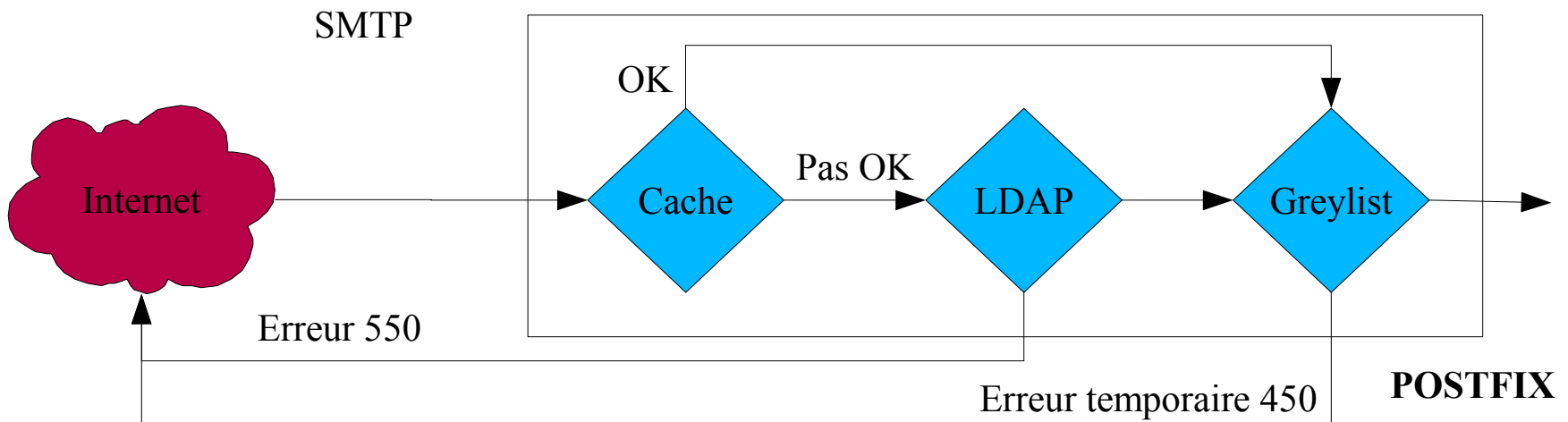
Diagnostic

- Postfix n'accepte plus les mails si l'annuaire LDAP consulté par la « relay_recipient_map » ne répond plus.

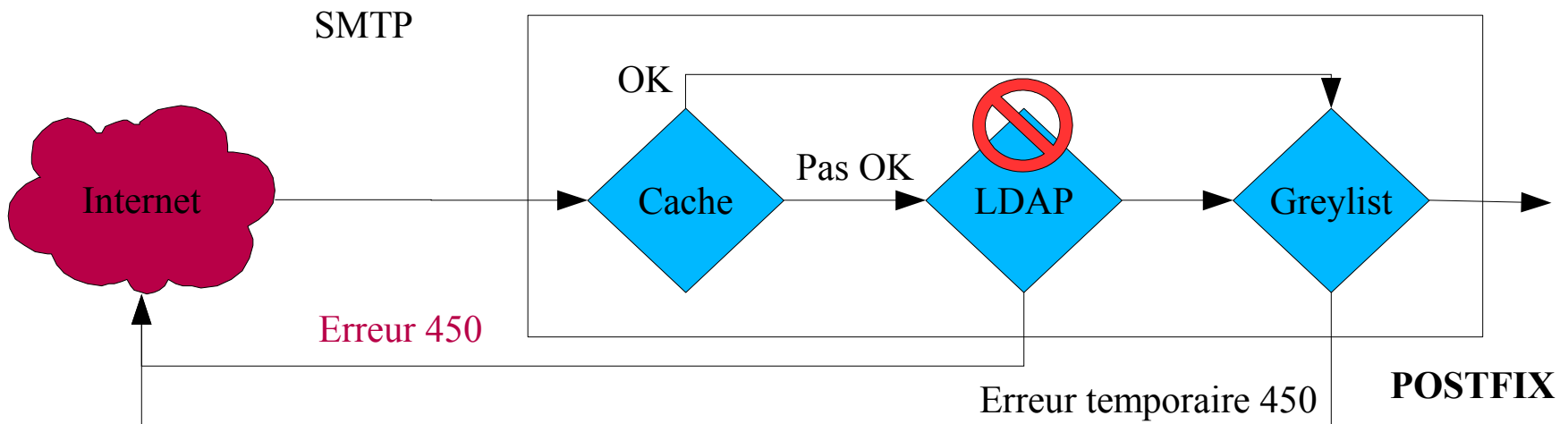
Correction

- Génération une fois par nuit d'un cache local à partir de l'annuaire LDAP.
- avantage supplémentaire : baisse des requêtes sur l'annuaire

Pannes LDAP



Panne LDAP



Évolutions

Statistiques

- **Mesures de pertinence des différents filtres Spamassassin**
 - Relever des poids
 - Cumuls et statistiques
 - Tracé de courbes
 - Influence des paramétrages

Retours des utilisateurs

- **Retour de HAM et de SPAM**
 - Vérification des pertinences des filtres
 - Listes blanches et listes noires

Merci de votre attention