Service Anti-Spam de Renater
Retour d'expérience

Boris Valera
(boris.valera@insa-toulouse.fr)

9 juin 2011

INSA de Toulouse • 135, Avenue de Rangueil • 31077 Toulouse
Tél. : +33(0)5.61.55.95.13 • Fax : +33(0)5.61.55.95.00 • www.insa-toulouse.fr

L'environnement

- L'INSA
  - École d'ingénieur
  - 8 spécialités
  - 8 laboratoires
  - 2500 étudiants et 800 personnels actifs
- La messagerie
  - 3 domaines principaux
  - environ 6000 comptes
  - plus de 17000 adresses différentes
  - environ 1,2 M de messages reçus par mois

L'évolution du filtrage

- Spamassassin + greylisting
  - Résultats satisfaisants
  - Chronophage pour l'administrateur
  - Complexité du traitement
- Tests de divers matériels
  - Ironport
  - Mirapoint
  - SonicWall
- Choix de basculer vers une solution "clés en main"

Ironport

- En production depuis 2 ans
- Résultats très bons
- Utilisateurs contents

Les raisons de la bascule

- Fin de la garantie initiale de l'Ironport
- Gain financier évident

Mise en place

- Les annuaires
  - Deux annuaires synchrones
  - Alimentation par des scripts maison
- Temps de bascule
  - Rapide et efficace
  - Il faut juste éviter de se tromper de 15 jours dans les dates de fin de licence...
- Modifications des MX

Fonctionnement

- Logs qui demandent une certaine étude mais clairs par la suite
- Un léger manque de documentation
- Système d'apprentissage pratique
- Statistiques mensuelles complètes

Quelques chiffres

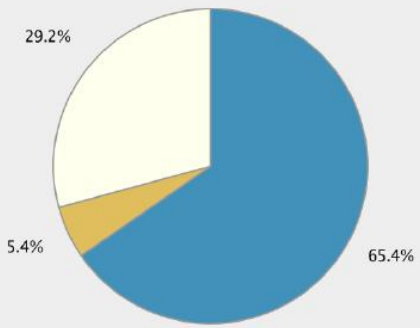
- Quelques résultats (Ironport vs Renater)

	Janvier	Février	Mai
Messages reçus	1098406	1144431	1102205
Rejetés par RBL/Reputation filter	718003	793568	692478
Adresse RCPT TO en erreur	231	155	28140
Virus détecté	13	20	0
Rejets temporaires	0	0	4986
Messages transmis	380159	350688	347857
Messages commerciaux	0	0	98985
Messages marqués spam	59313	47286	5177

Les rapports (Ironport)

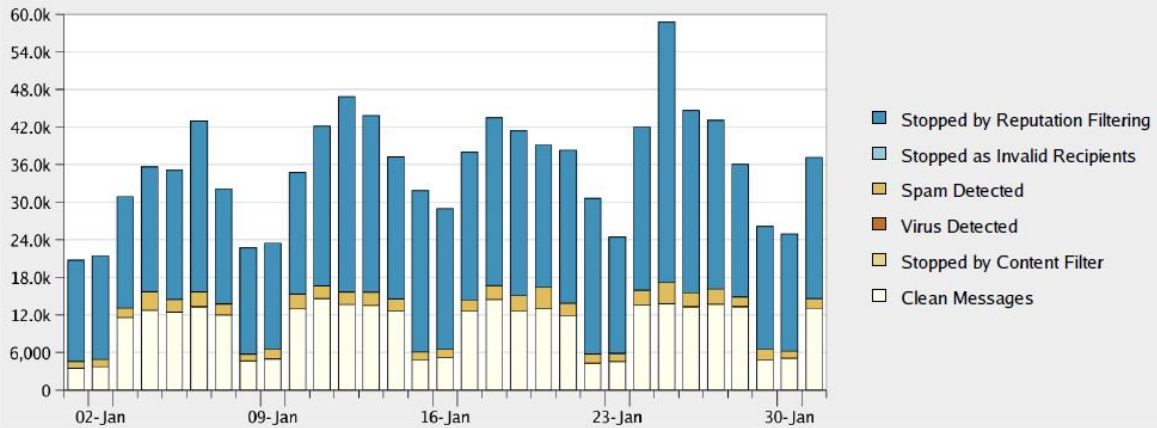
01 Jan 2011 00:00 to 31 Jan 2011 23:59 (GMT +0100) — Data in time range: 100.0 % complete

Incoming Mail Summary



Message Category	%	Messages
Stopped by Reputation Filtering	65.4%	718,003
Stopped as Invalid Recipients	0.0%	231
Spam Detected	5.4%	59,313
Virus Detected	0.0%	13
Stopped by Content Filter	0.0%	0
Total Threat Messages:	**70.8%**	**777,560**
Clean Messages	29.2%	320,846
Total Attempted Messages:		**1,098,406**

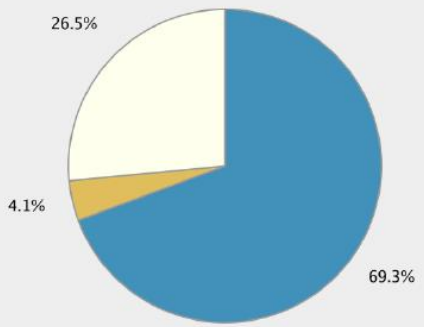
Incoming Mail Over Time



Les rapports (Ironport)

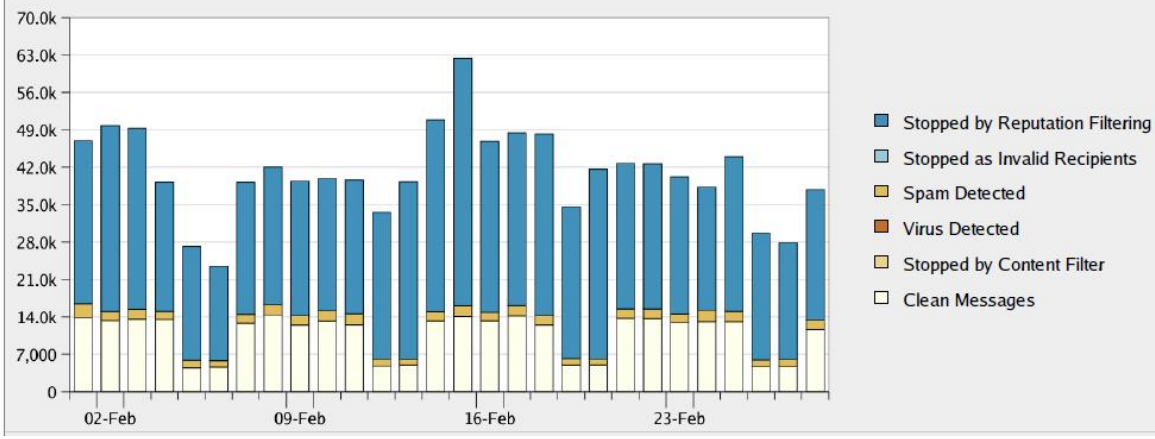
01 Feb 2011 00:00 to 28 Feb 2011 23:59 (GMT +0100) — Data in time range: 100.0 % complete

Incoming Mail Summary



Message Category	%	Messages
Stopped by Reputation Filtering	69.3%	793,568
Stopped as Invalid Recipients	0.0%	155
Spam Detected	4.1%	47,286
Virus Detected	0.0%	20
Stopped by Content Filter	0.0%	0
Total Threat Messages:	**73.5%**	**841,029**
Clean Messages	26.5%	303,402
Total Attempted Messages:		**1,144,431**

Incoming Mail Over Time



Les rapports (Renater)

Diagramme des messages traités en mai 2011 :

Total des messages traités : 1 102 205
Taux de filtrage : 68,910% (31,090% des messages traités sont valides)

Rejets permanents : 749 362 (67,988%)
Rejets temporaires : 4 986 (0,452%)
Messages routés : 347 857 (31,560%)

Analyse du contenu :
17 080 spams identifiés et éliminés (2,279% des rejets permanents)
5 177 messages marqués, spams suspectés (1,488% des messages routés)
98 985 messages marqués, type UCE (28,456% des messages routés)
239 646 messages valides non whitelistés (68,892% des messages routés)

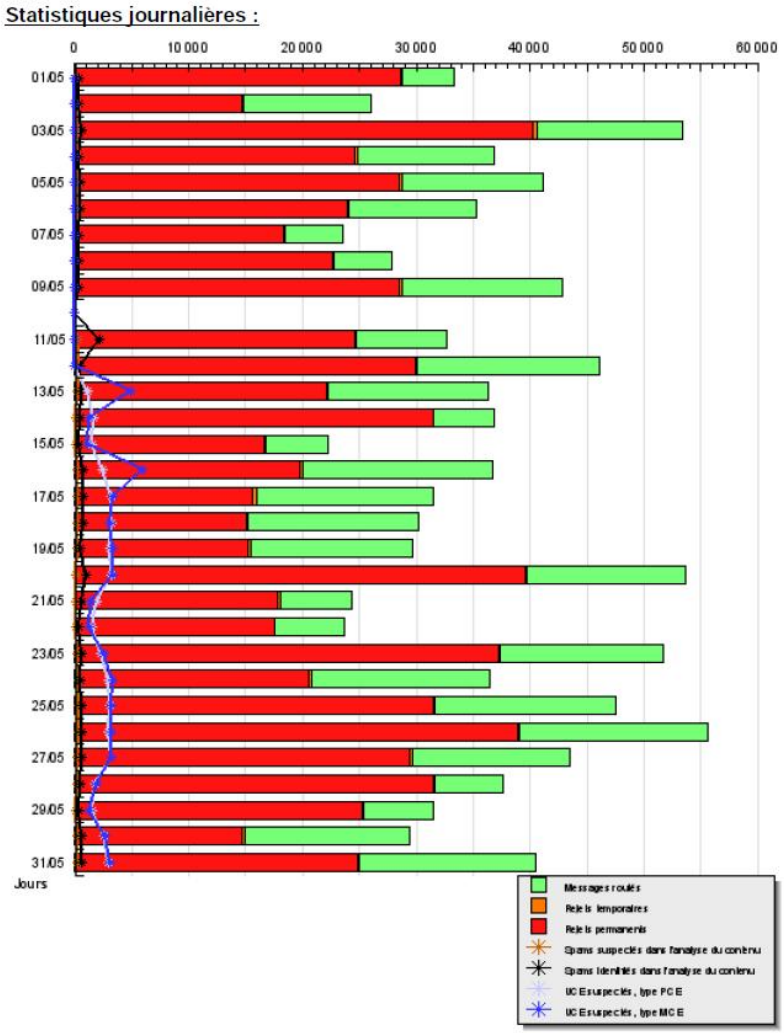
Détail :

Causes des rejets permanents	Quantité (%)
Serveur émetteur dans la RBL SpamHaus	692 478 (92,409%)
Adresse "RCPT TO:" inconnue du LDAP	28 140 (3,755%)
Spams identifiés dans le contenu (score > seuil de rejet)	17 080 (2,279%)
MX/A invalide pour le domaine du "MAIL FROM:"	7 954 (1,061%)
SPF Hardfail	3 346 (0,447%)
Taille du message supérieure à la taille max autorisée	352 (0,047%)
Extensions de pièces jointes non autorisées	12 (0,002%)
Adresse "MAIL FROM:" inconnue du LDAP	0 (0%)
Bounces rejetés	0 (0%)
Messages provenant d'un serveur en blacklist	0 (0%)
Plus de 100 destinataires pour le message	0 (0%)
Messages avec virus détecté	0 (0%)

Causes des rejets temporaires	Quantité (%)
Adresse IP du serveur émetteur non résolue (liste grise)	2 692 (53,991%)
Anti-moissonnage (taux d'adresses invalides trop élevé)	1 481 (29,703%)
Résolution dynamique du serveur émetteur (liste grise)	813 (16,306%)
Trop de messages en queue (plus de 1000)	0 (0%)

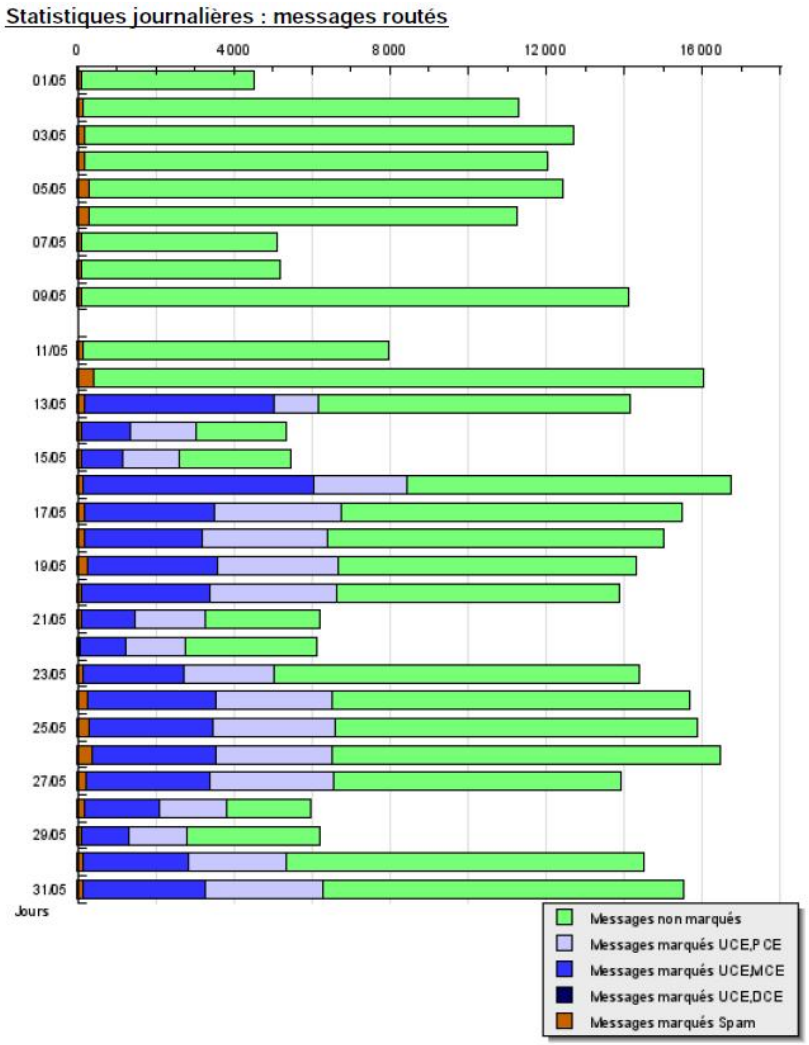
Types de messages routés	Quantité (%)
Messages valides non whitelistés, non marqués (ni spam, ni UCE)	239 646 (68,892%)
Messages commerciaux (UCE), Type MCE (Miscellaneous C. E.)	53 042 (15,248%)
Messages commerciaux (UCE), Type PCE (Professional C. E.)	45 943 (13,207%)
Messages suspectés dans le contenu (marquage SPAM)	5 177 (1,488%)
Messages whitelistés	4 049 (1,164%)
Messages commerciaux (UCE), Type DCE (Dirty C. E.)	0 (0%)

Les rapports (Renater)



INSA de Toulouse • 135, Avenue de Rangueil • 31077 Toulouse
Tél. : +33(0)5.61.55.95.13 • Fax : +33(0)5.61.55.95.00 • www.insa-toulouse.fr

Les rapports (Renater)



INSA de Toulouse • 135, Avenue de Rangueil • 31077 Toulouse
Tél. : +33(0)5.61.55.95.13 • Fax : +33(0)5.61.55.95.00 • www.insa-toulouse.fr

Conclusion

- Très bons résultats
- Quelques petites choses à améliorer
  - Modifications de la configuration plus pratique que d'ouvrir un ticket à chaque fois
  - Interface de réglage des seuils et exceptions
  - Suivi des logs en temps réel
  - Filtrage en sortie
- Actuellement, aucune raison de revenir à une autre solution