Le service antispam de RENATER est arrivé !

Jean-Luc Munier, Franck Simon, Serge Aumont, Olivier Hussenet

Le service antispam de RENATER est arrivé !

Franck Simon & Olivier Hussenet
GIP RENATER
ENSAM – 151 Boulevard de l'Hôpital – 75013 PARIS

Serge Aumont
Comité Réseau des Universités
Campus de Beaulieu – 35042 RENNES Cedex

Jean-Luc Munier
Université Pierre et Marie Curie
4 Place Jussieu – 75252 PARIS Cedex 05

Résumé

L'objet de cet article est de présenter le service antispam proposé à l'ensemble des établissements connectés au réseau RENATER.

Après une présentation du contexte, et notamment les avantages d'une solution mutualisée pour lutter contre le spam plutôt que de répliquer les efforts dans chaque établissement, la démarche adoptée est exposée (groupe de travail antispam, appel d'offres...).

Dans une deuxième partie, l'article précise la solution technique retenue en termes d'architecture et détaille l'ensemble des fonctionnalités offertes par la plateforme, avec un accent particulier sur les fonctions de délégation d'administration proposées (mise à disposition des traces, administration décentralisée pour laisser aux établissements la maîtrise de règles spécifiques de filtrage...).

Enfin, sont abordées les différentes options pouvant être souscrites par les établissements et les spécifications d'interconnexion au service antispam. Afin d'illustrer cet aspect, un site « pilote », à savoir l'Université Pierre et Marie Curie (UPMC) apporte son témoignage. L'architecture de messagerie de l'UPMC est décrite ainsi que les changements apportés pour l'inclusion du service antispam de RENATER.

Mots clefs

antispam, antivirus, SMTP, LDAP, DNS

1 Introduction

Quand un site souhaite se connecter au réseau RENATER (soit directement sur un point de présence RENATER, soit via un réseau de collecte), il se voit attribuer par le GIP RENATER un certain nombre de ressources : des adresses IP, un ou plusieurs noms de domaines… Contrairement à un FAI « grand public », les ressources ainsi attribuées doivent permettre au site en question de disposer d'une grande autonomie car les services tels que la messagerie, le DNS, l'hébergement de pages Web ne font pas partie du panier de prestations fournies par le GIP RENATER. Le premier objectif assigné au réseau RENATER est d'assurer une interconnexion à haut débit de sites (universités, centres de recherche...) eux-mêmes organisés pour offrir le service aux usagers. La constitution des briques de base pour les services réseaux essentiels (DNS, messagerie...) relève du site lui-même. Ainsi, chaque site est amené à mettre en place, soit à son niveau, soit au niveau de l'entité dont il dépend, des solutions de messagerie, mais aussi des solutions de lutte contre le spam.

À ce jour, il n'est pas déraisonnable d'affirmer qu'en moyenne, dans l'Internet, plus de 90% des flux de messagerie sont du spam. Une campagne de mesures effectuée en 2008 par le GIP RENATER au niveau des interfaces d'interconnexion entre le réseau RENATER et les éléments extérieurs (réseaux « commerciaux ») a montré une volumétrie d'environ 1500 ouvertures de sessions SMTP par seconde (pour les flux de messagerie entrants), soit au minimum 130 millions de sessions SMTP par jour ou encore 3,9 milliards de sessions par mois.

Dans ce contexte, les serveurs de messagerie déployés à l'échelle de chaque site nécessitent des ressources matérielles et humaines de plus en plus importantes, uniquement pour être en mesure d'appliquer un filtrage antispam efficace prenant en compte des volumétries importantes pour les flux entrants. Le cumul de l'ensemble des moyens techniques et surtout des ressources humaines déployé est considérable. Pourtant, la qualité du filtrage antispam obtenue est hétérogène, car les moyens mis en œuvre par chaque établissement diffèrent. Souvent les compétences techniques au sein de l'établissement sont fragiles car reposant sur un seul individu ou parce que personne dans l'établissement n'a le « loisir » de maintenir ses connaissances sur ce domaine évolutif. Les sites concernés sont condamnés à renouveler sans cesse ces efforts ou à acheter des équipements dédiés de filtrage dont le coût par boîte aux lettres est d'autant plus élevé que ces achats sont faits par petites quantités.

Conséquence de cette absence quasi totale de mutualisation, le coût global de la protection antispam dans notre communauté est élevé.

2 Présentation du contexte

2.1 Démarche adoptée

Un groupe de travail a été créé en 2008, à l'initiative notamment du Comité Réseau des Universités (CRU), en coordination avec le GIP RENATER. Ce groupe comprend des représentants des Universités, du CNRS, mais aussi des organismes tels que l'INRA, le CIRAD ou encore le CRIHAN.

2.1.1 Lancement d'une enquête

Pour démarrer, une enquête a été lancée en janvier 2008 auprès de la communauté des administrateurs système/réseau et des RSSI, afin d'établir un panorama des différentes solutions déployées à l'échelle des sites RENATER, et évaluer l'ampleur du besoin quant à la fourniture d'une solution de filtrage antispam centralisée.

Cette enquête, à laquelle près de 190 personnes ont répondu (représentant près de 600 domaines DNS et un potentiel de 1 200 000 boîtes aux lettres), a notamment mis en évidence les éléments suivants :

la grande majorité des sites utilise des solutions à base de logiciels libres, notamment SpamAssassin, postgrey, milter-greylist, J-chkmail... Quelques sites seulement ont recours à des solutions commerciales logicielles ou à base d'équipements spécifiques ;

pas ou peu de vérification/filtrage pour les flux de messagerie sortants (uniquement pour les flux entrants) ;

le greylisting reste une technique de filtrage assez largement répandue, malgré une efficacité en baisse et des effets indésirables bien connus ;

la plupart des sites appliquent une politique de type « tag and deliver » (marquage puis envoi) plutôt que de rejeter les messages ;

la gestion d'une « quarantaine » est très peu répandue.

2.1.2 État de l'art et identification des solutions techniques

La première étape de recensement des solutions utilisées dans la communauté RENATER terminée, il a été décidé d'identifier et d'étudier les solutions techniques existantes sur le marché. Des réunions ont donc été organisées avec les différents prestataires/fournisseurs de solutions logicielles et matérielles durant les 2ème et 3ème trimestres 2008, afin d'avoir le panorama le plus complet possible des offres disponibles. En parallèle de ces rencontres, il était important d'obtenir un retour d'expérience de sites, notamment auprès de ceux qui avaient opté pour des solutions commerciales.

2.1.3 Établissement d'un service « pilote »

Il est apparu de façon naturelle le besoin de bâtir un service « pilote » sur lequel serait connecté un échantillon représentatif de sites RENATER (une dizaine de sites), l'ensemble constituant une masse critique de plus de 200 000 boîtes aux lettres. Les objectifs de ce « pilote » étaient notamment de :

définir techniquement les grandes lignes du service antispam afin d'élaborer un cahier des charges en vue d'un appel d'offres ;

qualifier les différentes étapes du traitement à appliquer pour un filtrage antispam centralisé efficace (sachant que les règles pertinentes pour un site RENATER ne le sont pas forcément pour un autre, et que donc gérer un filtrage sur une plateforme mutualisée ne se fait pas de la même façon qu'un filtrage déporté sur chaque site) ;

vérifier le rôle complémentaire des moteurs antivirus par rapport aux moteurs antispam ;

identifier et consolider les paramètres de configuration nécessaires pour le raccordement des sites sur la plateforme en vue d'établir par la suite des spécifications d'interconnexion au service et commencer à définir en conséquence les procédures administratives nécessaires pour adhérer au service ;

consolider les informations nécessaires devant être fournies aux sites pour le suivi de la qualité et de la pertinence du filtrage (mise à disposition de statistiques, accès aux traces respectives des différents domaines...) ;

quantifier la part de travail nécessaire pour l'administration, la configuration, la supervision de la plateforme et le support technique aux sites usagers, afin de mieux appréhender une phase future de production.

Cette phase « pilote » préparatoire s'est déroulée sur le 1er trimestre 2009 et une partie du 2ème trimestre.

2.1.4 Cahier des charges et appel d'offres

Enfin, la dernière étape du processus a consisté en un appel d'offres pour une mise en concurrence des différentes solutions.

Le cahier des charges ayant été élaboré en parallèle du service « pilote », la consultation a pu être lancée au tout début du 3ème trimestre 2009, pour un déploiement au plus tard le 30 septembre 2009.

Les principaux éléments techniques retenus dans l'expression des besoins pour le cahier des charges sont les suivants :

fourniture d'un service de filtrage antispam et antivirus pour les flux entrants ;

localisation/répartition des équipements de filtrage antispam dans les nœuds de cœur de réseau RENATER afin de garantir une haute disponibilité du service ;

architecture évolutive supportant au démarrage 500 000 boîtes aux lettres et pouvant évoluer par paliers jusqu'à 2 000 000 de boîtes aux lettres, et suffisamment performante pour absorber des pics de trafic importants, tout en reposant sur un nombre limité de boîtiers ;

MTA[1] respectueux des RFC et d'architecture modulaire et évolutive composée des briques suivantes :

- service de validation pendant les sessions SMTP des adresses locales au moyen d'annuaires LDAP,
- services de réputation et/ou filtrage protocolaire permettant le rejet de sessions SMTP entrantes sur la base de critères tels que la réputation d'une adresse IP ou le contrôle de validité de l'adresse de l'émetteur,
- moteurs de filtrage de contenus, avec capacité à faire la distinction entre un spam et un UCE[2],
- moteurs antivirus.

support d'un très grand nombre de domaines et sous-domaines DNS (plusieurs milliers), avec la possibilité d'établir des variantes dans la politique de filtrage propre à chaque domaine ;

prévention et filtrage du « backscattering[3] » ;

intégration de l'IPv6 requise avant fin 2010 au plus tard ;

génération de journaux informatiques et statistiques ; traçabilité des décisions de filtrage ;

souplesse, facilité d'administration (possibilité d'automatiser les configurations par scripts) et supervision de la plateforme ;

sécurité de la plateforme et des données ;

[1]MTA : Mail Transfer Agent

[2]UCE : Unsollicited Commercial Email : se dit d'une catégorie de spams diffusés avec des moyens légitimes (pas de botnet, pas d'usurpation de l'adresse d'expéditeur)

[3]Backscattering : utilisation par les spammeurs d'adresses de messagerie légitimes en usurpant l'identité d'utilisateurs

maintenance (garantissant une GTR) de 4h et support technique associé.

3 Solution technique mise en œuvre dans RENATER

3.1 Architecture de la solution

La solution retenue, suite à la consultation, répond aux critères du cahier des charges. Elle s'appuie sur un équipement Bizanga[4], un MTA puissant et souple. Cet équipement permet de solliciter autant de RBL[5] que souhaité pour le filtrage par adresse IP. La RBL retenue est SpamHaus (mais d'autres RBL peuvent venir compléter ou remplacer celle choisie). Au MTA Bizanga, viennent se greffer les briques suivantes (intégrées dans l'équipement) :

un moteur antispam VadeRetro ;

un moteur antivirus VadeRetro : antivirus « OutBreak filter », qui consiste en un filtrage de type heuristique (pour traiter les cas de virus non encore connus ou non référencés dans les bases de définition de virus) ;

un deuxième moteur antivirus : DocteurWeb, pour un filtrage basé sur des signatures de virus, et donc complémentaire au premier moteur.

La plateforme assure un filtrage antispam sur les flux entrants pour l'instant. La mise en place d'un filtrage sortant pourra être étudiée dans un deuxième temps en fonction des demandes exprimées par les usagers.

Il a été volontairement fait le choix de ne pas mettre en œuvre une gestion de quarantaine, cet aspect étant laissé dans le périmètre de responsabilité des sites usagers.

Les figures ci-après représentent le mode de circulation/traitement des flux de messagerie avant la mise en place du service antispam RENATER (cf. Figure 1) et après la mise en place (cf. Figure 2) :

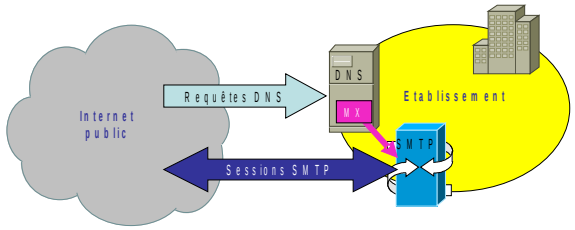

Figure 1 - *Flux avant solution RENATER antispam*

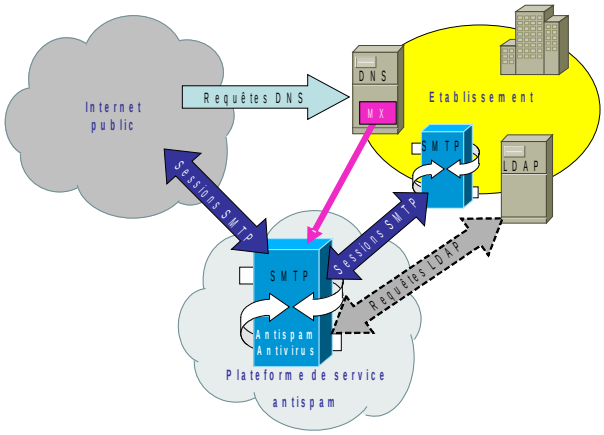

Figure 2 - *Flux après solution RENATER antispam*

Afin d'assurer une haute disponibilité, deux équipements Bizanga ont été installés respectivement sur les deux NRI[6] de Paris. Il faut noter qu'un seul équipement Bizanga suffit à tenir la charge, même pour deux millions de boîtes aux lettres, mais deux boîtiers ont été déployés afin d'assurer une continuité de service et rendre la solution « transparente » en cas d'indisponibilité de l'un des deux (maintenance ou incident). Dans la mesure où le nombre d'équipements est réduit, la répartition du trafic se fait sur la base d'un algorithme de type « round-robin » géré directement au niveau DNS. Il n'a donc pas été utile d'insérer des boîtiers « hardware » spécialisés pour assurer cette répartition. Ce point pourra être revu le jour où un plus grand nombre d'équipements sera nécessaire du fait du succès du service.

[4]http://www.bizanga.com/index.php

[5]RBL : Real-time Black List

[6]NRI : Nœud RENATER International – nœud de cœur de réseau RENATER

3.2 Fonctionnalités et algorithme de traitement simplifié

L'algorithme de traitement mis en place est le même pour tous les domaines : il est appelé ici « workflow ». Par contre, la plateforme permet de positionner des conditions au sein de l'algorithme pour déclarer ou non certaines actions, de façon à ce que le traitement final puisse être différencié par domaine, sans pour autant modifier les règles globales.

Les grandes lignes du « workflow » sont résumées ci-après :

application de listes blanches/noires globales[7] ;

rejet des sessions entrantes en fonction de l'historique de l'adresse IP du MTA distant (nombre et pourcentage des adresses invalides, taux des messages détectés comme du spam ou des virus par le moteur d'analyse de contenu) ;

rejet de la session SMTP si le serveur émetteur est contenu dans la RBL SpamHaus ;

rejet de la session SMTP si le serveur émetteur n'est pas compatible avec l'enregistrement SPF du domaine du MAIL From: (SPF-hardfail) ;

si le serveur émetteur a une adresse IP dynamique ou si une résolution inverse ne donne pas de résultat, rejet du message ou application d'un « greylisting » (au choix du domaine d'opter pour l'une ou l'autre des politiques) ;

rejet temporaire si la file d'attente du domaine destinataire est trop pleine ;

limitation de la cadence d'établissement de nouvelles sessions, limitation du nombre de messages par session et du nombre de destinataires par message ;

contrôle de l'existence du destinataire dans l'annuaire LDAP. Si l'émetteur appartient à un domaine géré par le service, sa validité sera aussi contrôlée. En cas d'inexistence dans l'annuaire, les messages sont refusés ;

application des listes blanches et noires par domaine[8] ;

analyse du message par le moteur antispam VadeRetro ;

selon la note obtenue et le seuil de rejet défini pour le domaine[8], rejet du message ou ajout des marqueurs[8] identifiant le message comme étant du spam ;

en option, analyse du message par le moteur antivirus DocteurWeb ;

livraison du message au serveur du site.

3.3 Gestion des journaux (logs)

Les équipements permettent de journaliser un grand nombre d'informations, et ceci est largement paramétrable et adaptable. Les journaux générés par les équipements sont exportés via « syslog » vers deux serveurs spécifiques, lesquels sont également répartis sur les deux NRI de Paris, afin de garantir une haute disponibilité quant à l'accès aux journaux. Cet accès peut se faire, pour les administrateurs système/réseau des sites utilisateurs, soit via un accès FTP sécurisé, soit via « syslog ». Cette mise à disposition des journaux est un élément essentiel du dispositif dans la mesure où même si la plateforme de filtrage antispam est mutualisée, il est important de garantir une transparence vis-à-vis des sites utilisateurs afin d'autoriser une visibilité notamment sur les rejets ou non des messages.

3.4 Gestion des configurations

Chaque domaine utilisateur est susceptible de demander des règles de filtrage spécifiques. Appliquer uniquement un même filtrage global n'est donc pas satisfaisant. La plateforme Bizanga offre une grande souplesse à ce niveau.

Pour l'instant, la configuration de la plateforme est effectuée semi-automatiquement par les équipes du GIP RENATER, ce qui est acceptable dans une phase de montée en charge progressive.

D'ici la fin de l'année, il est prévu la mise en place d'une interface de type Web, accessible par les administrateurs systèmes/réseau des sites, permettant de saisir et modifier la politique de filtrage demandée pour tout ou partie des domaines DNS associés à un site. Les données saisies via cette interface seront ensuite stockées dans une base de données. Des scripts seront mis en place afin de générer dynamiquement les configurations à partir des éléments communiqués. Cette étape est très

[7]Listes complétées en fonction des demandes émanant des sites

[8]Paramètres totalement configurables par domaine

importante pour atteindre un régime de croisière et éviter des erreurs de manipulation. Cette automatisation offrira également la possibilité d'appliquer de façon très réactive des filtres à la volée en cas de problème de sécurité ou autres. Si l'on considère en outre la mise à disposition des journaux par domaine, telle que mentionnée précédemment, cela permet d'établir en fait un système d'administration déporté pour les sites utilisateurs.

4 S'interconnecter au service RENATER antispam

4.1 Spécifications techniques d'interconnexion

Chaque site souhaitant bénéficier du service RENATER antispam devra être capable de répondre à un certain nombre de points, lesquels sont nécessaires pour la mise en place technique du service :

liste des domaines gérés par le site ;

description du MTA gérant la messagerie entrante de chaque domaine du site ;

description de l'annuaire LDAP contenant les adresses valides de chaque domaine du site. Il a été décidé de rendre obligatoire ce service de validation des adresses car c'est une pièce maîtresse de la prévention du « backscattering ». Un tel annuaire LDAP peut être déclaré auprès de la plateforme antispam avec plusieurs adresses IP pour assurer facilement la haute disponibilité de cet élément de service. En outre, le MTA gère un cache des consultations LDAP déjà faites. Enfin, en cas d'absence temporaire de l'annuaire d'un domaine, les messages adressés vers son domaine sont temporairement rejetés (code SMTP 4XX) et de ce fait ils ne sont que retardés et non perdus ;

description du serveur « syslog » recevant les journaux pour chaque domaine (pour les sites qui souhaitent recevoir les journaux par « syslog ») ;

listes blanches et noires pour chaque domaine ;

marqueurs à ajouter à un message reconnu comme spam (ou UCE) ;

liste des extensions de fichiers à refuser ;

seuils de classification d'un message comme spam (d'après la note obtenue suite à l'analyse de contenu) ;

mention du souhait ou non de bénéficier du service antivirus (lequel peut être désactivé pour être géré par le site directement via ses propres serveurs et avec son propre moteur).

Outre ces paramètres à communiquer au GIP RENATER, le site devra effectuer les actions suivantes à son niveau :

autoriser les flux entrants entre ses serveurs et la plateforme RENATER antispam, à savoir les sessions SMTP pour la livraison des messages à son MTA. Bien entendu le domaine doit veiller à désactiver le « greylisting » pour les sessions provenant des MTA de RENATER mais aussi désactiver toute limitation de cadence de connexion ;

autoriser les requêtes LDAP afin de vérifier dans son annuaire la validité des adresses des destinataires ;

autoriser les flux FTP et « syslog » (si besoin) pour récupérer ou recevoir les traces de l'activité concernant ses domaines.

Dès que la prise en compte de sa configuration lui aura été notifiée par le GIP RENATER, le site devra réaliser un test d'envoi de message vers chacun de ses domaines, afin de valider l'ensemble de la chaîne de traitement (ce test peut être réalisé en configurant un client de messagerie avec l'adresse d'un des MTA antispam comme serveur sortant).

En dernier lieu, il devra modifier le champ MX du DNS dans lequel sont déclarés ses domaines, pour pointer vers les adresses IP de la plateforme RENATER antispam.

Les procédures de raccordement ont volontairement été simplifiées au maximum pour faciliter le raccordement des sites au service antispam. De plus amples informations sur ces procédures sont disponibles sur : http://www.renater.fr/antispam

4.2 Support technique

La maîtrise d'œuvre et le support technique du service antispam RENATER sont pour l'instant internalisés au GIP RENATER (pas d'externalisation vers un prestataire). Le GIP RENATER s'appuie sur les supports techniques respectifs de Bizanga pour

les problèmes matériels ou logiciels liés au MTA, et au support technique de VadeRetro pour les problèmes spécifiques au filtrage antispam.

5 Témoignage d'un site « pilote », l'Université Pierre et Marie Curie

5.1 Contexte

L'Université Pierre et Marie Curie est localisée sur le campus de Jussieu (Paris).

Le relais de messagerie, point incontournable de transit des courriels pour l'UPMC, traite à ce jour environ 1,5 millions de messages par jour et ce volume ne cesse de croître, phénomène essentiellement lié au spam.

Ce fléau mobilise de plus en plus de ressources matérielles et humaines, ce qui n'est plus acceptable à l'échelle d'un site.

5.2 L'architecture en place à l'UPMC

Initialement, le relais de messagerie du campus est composé d'un seul serveur formant la passerelle d'accès (entrée/sortie) pour l'ensemble des domaines du campus. Ceux-ci sont répartis sur une cinquantaine de serveurs de messagerie, eux-mêmes gérés soit par la DSI soit directement par les laboratoires du campus. L'architecture de la messagerie à l'UPMC a évolué au gré des menaces (antivirus) et... du spam. Actuellement elle se compose de sept serveurs physiques (certains assurant plusieurs fonctions) :

répartiteurs dédiés : un, plus un secours ;

SMTP + antivirus clamav : quatre serveurs ;

serveurs antispam J-chkmail dont « greylisting » : deux serveurs ;

serveurs LDAP dédiés au routage du domaine « upmc.fr » : un serveur plus un « réplica » ;

serveur contenant la base « greylisting » : un serveur.

Ne disposant pas de la liste exhaustive des intitulés de messagerie existants sur le campus, cette architecture est sujette au « backscattering ».

Planifier la migration de la totalité des sous-domaines du campus en une seule opération étant exclu, nous avons doublé l'infrastructure, avec pour objectif de :

bénéficier de la mutualisation sur l'antispam RENATER et stopper la course à l'investissement nécessitée par le volume sans cesse accru de spam ;

réserver ce relais aux domaines de messagerie participant à la collecte exhaustive des intitulés de messagerie afin de ne plus être sujet au « backscattering ». L'ajout de cette fonctionnalité via J-chkmail sur l'architecture historique était planifié mais pas encore réalisé.

Ce dernier point impose par conséquent la collecte exhaustive des intitulés de messagerie pour chaque serveur devant migrer de l'ancienne à la nouvelle architecture.

Des éléments existants, seuls les serveurs LDAP peuvent-être repris. Ils possèdent un schéma plat (dépourvu de hiérarchie) et listent exhaustivement les adresses électroniques du domaine institutionnel.

5.3 Intégration à l'antispam de RENATER

Aux deux serveurs LDAP, sont adjoints deux serveurs SMTP (dépourvus de traitement antispam).

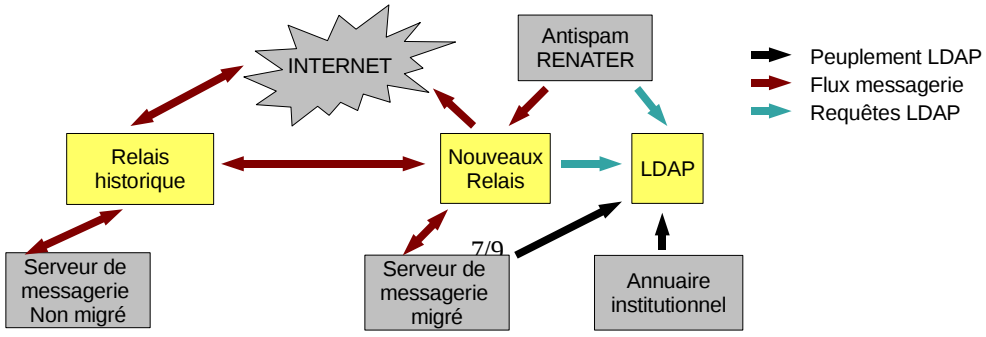

Figure 3 - *Intégration de l'antispam RENATER*

Le routage des domaines de messagerie se fait alors par configuration manuelle entre les deux architectures, lors de la migration de chaque domaine de messagerie à l'antispam RENATER.

Concernant la collecte des intitulés de messagerie, le serveur LDAP (OpenLDAP 2.3 et « réplica » slurpd) est alimenté par l'annuaire institutionnel via copie de fichiers (scp/sftp) :

- Exports XML événementiels

  Ils sont traités directement en LDAP.

- Exports LDIF (concernent les boîtes de service)

  Ils sont soumis à un différentiel pour être traités en LDAP.

- Exports calendaires

  À réception de ceux-ci, une nouvelle base de données (« backend » LDAP) est générée avec slapadd dans un nouveau répertoire. Si tout se passe bien, le serveur LDAP est relancé avec cette nouvelle base.

Le même procédé est repris pour le peuplement des autres domaines de messagerie : exports de fichiers « plats » à l'initiative des serveurs de messagerie et de listes (un fichier par domaine). Le différentiel est traité en LDAP, et régénère – le cas échéant – un fichier LDIF pour la confection périodique du backend LDAP. Dans la plupart des cas, de simples commandes « grep » dans les fichiers d'alias sur les serveurs de messagerie suffisent à confectionner la liste des adresses de messagerie devant être intégrées au serveur LDAP.

5.4 Premiers constats

La première vague de migration concernait les domaines gérés par la DSI, dont certains historiques étaient largement spammés. Bien que de gros domaines (en terme de volumétrie) restent à migrer, on peut constater l'allègement de la charge.

Le flux messagerie provenant de l'extérieur passe à quelques 50 000 messages par jour : moins qu'il y a 10 ans !

De son côté le relais historique, déchargé des quelques domaines migrés, voit sa volumétrie passer de 1 800 000 sollicitations par jour à un peu moins de 900 000.

Plusieurs indicateurs (nombre de messages en file d'attente, taille de diverses bases de données.) qui nous tenaient parfois en souci, repassent en deçà des seuils d'alerte. Cependant l'apport de fonctionnalités « anti-backscatting » sur le relais historique aurait probablement abouti à des constats similaires.

6 Conclusion

Le service antispam de RENATER est de nature à soulager les établissements du travail fastidieux de mise à niveau des techniques de filtrage. L'adopter peut être l'opportunité pour chaque site de repenser son architecture de messagerie même si, de par sa conception simple, il s'intègre facilement dans l'existant. Cet article décrit la définition initiale du service qui est amené à évoluer. La communauté des utilisateurs sera consultée sur les évolutions comme par exemple la constitution de listes blanches et de listes noires mutualisées, la mise en œuvre de raccordement en IPv6, l'activation de tests DKIM ou encore la mise en place d'une option de filtrage sortant pour les domaines qui le souhaitent.

7 Annexe

Glossaire

CNRS : Centre National de la Recherche Scientifique

CRIHAN : Centre de Ressources Informatiques de Haute-Normandie

CRU : Comité Réseau des Universités

DKIM : Domain Keys Identified Mail

DNS : Domain Name System

DSI : Direction des Systèmes d'Information

FAI : Fournisseur d'Accès Internet

FTP : File Transfer Protocol

INRA : Institut National de Recherche Agronomique

LDAP : Lightweight Directory Access Protocol

LDIF : LDAP Data Interchange Format

RENATER : Réseau National pour la Technologie l'Enseignement et la Recherche

RSSI : Responsable de la Sécurité des Systèmes d'Information

SCP : Secure Copy

SFTP : Secured File Transfer Protocol

SMTP : Simple Mail Transfer Protocol

SPF : Sender Policy Framework

UPMC : Université Pierre et Marie Curie

XML : eXtensible Markup Language