Retour d'expérience sur le choix d'une solution *antispam* au LAPP

Sylvain Garrigues
LAPP – Service informatique – Support système et réseaux
9 chemin de Bellevue 74941 Annecy-le-Vieux Cedex
sylvain.garrigues@lapp.in2p3.fr

Muriel Gougerot
LAPP – Service informatique – Support système et réseaux
9 chemin de Bellevue 74941 Annecy-le-Vieux Cedex
muriel.gougerot@lapp.in2p3.fr

Résumé

Depuis plusieurs mois, on note une nette recrudescence du pourriel. Le système antispam en place au LAPP – Postfix/SpamAssassin – ne donnant plus vraiment satisfaction, nous avons décidé de lancer une étude afin de mettre en place une solution commerciale, qui offrirait un meilleur service aux utilisateurs tout en réduisant le besoin de maintenance pour les administrateurs. Au cours de la présentation, nous ferons un rapide rappel sur les spams et les différentes architectures possibles pour réduire leur nuisance, avant de décrire le système actuellement en place au LAPP. Nous verrons alors la démarche qui nous a permis, après un premier tour d'horizon des solutions possibles, de choisir et de tester plus en détail 7 solutions au cours de l'été 2007 : MailInBlack, Aladdin eSafe, Norman Email Protection, Sophos PureMessage (versions appliance et serveur), Ironport et Symantec Mail Security (Brightmail). Après avoir présenté de notre point de vue - rappelons que l'objet de ce retour d'expérience n'est pas de faire un comparatif exhaustif de ces solutions – quelques points saillants pour chaque matériel, nous résumerons les fonctionnalités qu'il nous semble important de mentionner dans notre cahier des charges.

Mots clefs

Spam, *antispam*, pourriel, filtrage de messagerie électronique, *message digest*.

1 Contexte

Le LAPP (Laboratoire d'Annecy-le-Vieux de Physique des Particules) est une unité mixte de recherche (UMR5814) de l'université de Savoie et du CNRS/IN2P3. Le laboratoire héberge dans ses murs un laboratoire de physique théorique. Les équipes du LAPP participent, dans le cadre de collaborations internationales, à la préparation et à l'exploitation des expériences qui tentent de sonder la matière et de répondre aux grandes questions de la physique. Sur le site, environ 200 personnes utilisent quotidiennement la messagerie électronique et le *spam* représente une véritable nuisance.

2 Etat des lieux

Depuis plusieurs mois, on note une nette recrudescence du pourriel (ou *spam*). Au niveau mondial, ce trafic est passé d'environ 30 milliards de *spam*s par jour en octobre 2005 à plus de 60 milliards en octobre 2006 (ce trafic devrait doubler fin 2007) [MA]. Ces pourriels sont de plus en plus difficiles à détecter et éliminer. On observe une évolution constante des types d'attaques (*spam* images[1], PDF etc…) nécessitant une adaptation permanente des techniques de détection.

3 Objet de l'étude

Le système *antispam* en place – basé sur une solution libre – ne donnant plus vraiment satisfaction nous avons décidé de lancer une étude afin de mettre en place une solution commerciale qui offrirait un meilleur service aux utilisateurs tout en réduisant le besoin de maintenance pour les administrateurs. Après un premier tour d'horizon des solutions possibles, nous avons pu étudier plus en détail 7 solutions au cours de l'été 2007 : MailInBlack, Aladdin eSafe, Norman Email Protection, Sophos PureMessage (versions *appliance* et serveur), Ironport et Symantec Mail Security. L'objet de ce document n'est pas de faire un comparatif exhaustif de ces solutions, mais de présenter les points saillants des produits évalués.

4 Rappels sur les *spam*s

Le courriel non sollicité prend de nombreuses formes. Outre les canulars (utilisant par exemple le *spoofing*[2]) et autres sollicitations commerciales connues depuis les débuts de la messagerie électronique, on note une « professionnalisation » des *spammeurs*. Ceux-ci disposent désormais de moyens conséquents fournis par des organisations mafieuses intéressées par les gains de l'escroquerie à distance. Désormais, le *spam* prend des formes beaucoup plus dangereuses que les techniques classiques par attachement/téléchargement de logiciels

[1] Pour tromper les *antispam* qui recherchent les mots clés, le message est affiché sous forme d'image.

[2] Usurpation d'identité utilisée depuis les débuts du mail.

malveillants (virus, *spyware*[3], trojans[4]) ou redirection vers des sites plus ou moins légaux en vue d'augmenter ses revenus publicitaires (souricières[5], …). Aujourd'hui, le *spam* est également utilisé pour le hameçonnage (*phishing*[6] *spear phishing*[7],… éventuellement associés à des techniques de *pharming*[8]), ou même pour la manipulation des cours boursiers[9]. Face à la montée du *spam*, la plupart des entreprises ont désormais mis en place un système de protection anti-pourriel. Les techniques actuelles de détection combinent : listes blanche et noire, liste grise (demande de réémission du courrier [TU]), mots clés, analyse contextuelle, reconnaissance de caractères pour analyser les images, filtrage bayésien ou encore signatures [TE]… Pour passer ces barrières, les *spammeurs* utilisent maintenant des techniques de plus en plus sophistiquées, de la technique de modification aléatoire des images pour tromper les signatures (*polka dots*[10], découpage par morceaux…), à l'utilisation de *botnets* : ces réseaux de plusieurs centaines ou milliers d'ordinateurs piratés et contrôlés à distance pour - entre autres - envoyer du *spam* (déjouant ainsi le filtrage sur l'expéditeur).

5 Les architectures *antispam*

Il existe plusieurs solutions pour réduire le trafic de *spam* reçu par les utilisateurs :

- La messagerie externalisée, un hébergeur gère le trafic mail. Attention à la disponibilité de l'hébergeur, à la confidentialité du courrier et au service proposé : accès ou non à une quarantaine, adéquation de la politique de traitement des *spam*s aux souhaits de l'entreprise…

- Les modules clients, souvent embarqués sur les clients de messagerie (type Thunderbird, VadeRetro…). Ils n'agissent évidemment que sur le(s) compte(s) de l'utilisateur final, il faut donc un module par poste à protéger.

- Les analyseurs de trafic, qui filtrent tout le trafic réseau de l'entreprise. Généralement, ces solutions bloquent le trafic mail (SMTP, POP, IMAP), HTTP et FTP posant des problèmes de sécurité (téléchargement de virus, JavaScript, ActiveX, etc…). Cette solution filtrant tout le trafic réseau, ceci nécessite une grosse configuration pour ne pas faire baisser les performances des connexions à très haut débit (Gigabit).

- Les solutions logicielles anti-pourriel, à installer sur le serveur de mail (ex : SpamAssassin). Tous les comptes de messagerie de la société sont filtrés mais cela affecte les performances du serveur, qu'il faut dimensionner en conséquence.

- Les passerelles anti-pourriel, déclarées en relai (MX) dans le DNS. Tout le trafic mail entrant (et éventuellement sortant) passe par ce boîtier. Il élimine le *spam* et transmet le courrier qu'il juge légitime au serveur de messagerie (quel qu'il soit : Postfix, Exchange, Sendmail …). Ces passerelles peuvent se présenter sous une forme serveur classique (type PC sous Windows ou Unix et logiciel *antispam*) ou sous la forme *appliance*[11].

L'*appliance* présente l'avantage d'être un produit spécialement développé pour l'utilisation qui en est faite. Ceci laisse supposer une configuration matérielle optimisée, de meilleures performances, une interface étudiée pour une prise en main plus facile et un faible besoin de maintenance, notamment grâce à une mise à jour automatique, moyennant un forfait annuel.

6 Le système actuel

Par choix et en partie du fait de notre relatif isolement (nous ne sommes pas situés sur un campus), nous gérons notre propre serveur de messagerie. Nous disposons pour cela d'un serveur sous Linux Redhat avec les logiciels libres Postfix [PF] et SpamAssassin [SA] intégrés grâce au module Amavisd. Le principe de base de SpamAssassin repose sur le calcul d'un score pour chaque mail traité. Le calcul se fait par l'application de règles qui peuvent prendre en compte le contenu du mail (mots clés, typographie, comparaison à une base d'empreintes de *spam*, apprentissage de type bayésien) et son origine (ORBL[12], listes blanches, inscription DNS). Certains de ces traitements (DNS, ORBL) ou d'autres comme le *greylisting* sont possibles directement au niveau du serveur Postfix lui-même. Néanmoins, ils fonctionnent de façon binaire contrairement à SpamAssassin qui effectue une corrélation et une pondération de chaque critère. Selon le score obtenu, les mails considérés comme *spam* sont soit délivrés après marquage (entêtes, modification du sujet), soit - au dessus d'un certain seuil - placés dans une quarantaine accessible uniquement par l'administrateur. Les utilisateurs configurent ensuite leur client de messagerie pour filtrer les mails marqués et utilisent souvent en complément le module *antispam* intégré sur le client.

---

[3] Logiciel espion parfois fourni avec des logiciels « légitimes » et permettant de récupérer les informations personnelles à l'insu de l'utilisateur.

[4] Code malveillant permettant d'ouvrir une « porte dérobée » sur le système compromis.

[5] Site *web* qui augmente artificiellement le nombre de visites en empêchant les utilisateurs d'en sortir (redirection systématique vers le site, ouverture automatique de nouvelles fenêtres, etc…).

[6] Technique consistant à rediriger (au moyen d'un lien hypertexte dans un *spam*, par exemple) vers un site *web* pirate identique à un site légitime (ex: site de banque, …) afin de tromper un client et de récupérer ses informations personnelles.

[7] *Phishing* ciblé sur une entreprise précise (mail aux employés redirigeant vers une copie de l'intranet…).

[8] Compromission d'un serveur DNS pour rediriger les requêtes DNS d'un site légitime vers un site pirate. Associé généralement au *phishing*, ce type de fraude est particulièrement difficile à détecter par le client.

[9] Envoi de fausses informations pour faire monter ou baisser artificiellement les cours de la bourse en vue d'une plus-value.

[10] Insertion de points aléatoires dans l'image pour modifier sa signature.

[11] « Boîte noire », généralement sous la forme d'un serveur au format 1U et dotée d'une interface d'administration à distance simplifiée.

[12] *Open Relay Black Lists* (listes noires de relais ouverts).

7 Pourquoi changer ?

Nous recevons environ 400.000 mails par semaine dont environ 80% sont du spam. Pour conserver une bonne efficacité de détection, Spamassassin nécessite un suivi quasi quotidien (surveillance, mise à jour des règles de filtrage…) ainsi que des interventions régulières (ajouts d'expéditeurs en liste blanche, recherches dans les traces et la quarantaine à la demande des utilisateurs…). Tout ceci représente une charge de travail dont nous souhaitons nous affranchir. De leur côté, les utilisateurs souhaiteraient bien sûr une meilleure efficacité et fiabilité mais aussi une plus grande transparence (en particulier la possibilité de consulter la quarantaine).

8 La démarche

Au début de cette étude, notre besoin était donc exprimé de façon très grossière, basé uniquement sur les reproches que nous faisions au système actuel (administration lourde, pas de quarantaine utilisateur). En étudiant les systèmes commerciaux disponibles sur le marché français, nous avons pu identifier des fonctionnalités spécifiques dont nous n'avions pas connaissance : en plus de la fonction antispam (plus ou moins efficace selon les techniques utilisées), certains matériels proposent par exemple des quarantaines personnalisables, des résumés de quarantaine, de la détection de *phishing* ou d'autres types d'attaques que nous détaillerons par la suite. Nous avons établi et envoyé à différents distributeurs un questionnaire d'une soixantaine de points visant à comparer les possibilités des produits tels que la compatibilité Postfix et Exchange, le matériel, la capacité de traitement des mails, les caractéristiques de la quarantaine, la langue des interfaces, la possibilité pour l'utilisateur de créer ses propres listes blanche/noire, le prix public de la solution ou encore des captures d'écran… A noter que l'envoi du questionnaire à plusieurs revendeurs concernant le même matériel n'est pas inutile car on obtient généralement des réponses différentes (ce qui permet d'améliorer la connaissance du produit et renseigne sur les compétences du fournisseur). Nous avons assisté à plusieurs présentations commerciales et démonstrations. Enfin, certains fournisseurs ont accepté de nous prêter leur produit pour faire un test. Cette pré-étude nous a permis de connaître les possibilités offertes par ces solutions commerciales, de vérifier leur efficacité par rapport à notre solution actuelle et de lister les fonctionnalités utiles au laboratoire.

9 Description des solutions étudiées

Nous ne donnerons aucune information concernant les prix des solutions étudiées, ceux-ci dépendant évidemment des conditions tarifaires négociées et du dimensionnement de la solution. En général, le prix est défini en fonction du nombre de boîtes-aux-lettres personnelles (par lots de 50 ou 100 boîtes), sans compter les listes de diffusion, sachant que l'on bénéficie souvent d'un « Gentleman Agreement » : le boîtier continue son travail même si on dépasse temporairement le nombre de boîtes-aux-lettres le temps de la régularisation. On peut toutefois donner, à titre purement indicatif, une fourchette de prix public entre 10 et 25 euros par utilisateur et par an.

Bien que ceci ne soit pas l'objet de notre étude, on peut signaler que les boîtiers intègrent en général une option antivirus et éventuellement une option de « détection proactive » des virus (rétention des mails avec attachements suspects et délivrance après un certain temps de quarantaine pour laisser le temps à l'antivirus de se mettre à jour, dans le cas où il s'agirait d'un virus encore inconnu).

Nos tests ont été effectués d'avril à août 2007. Lors de la lecture de ce document, il faudra garder à l'esprit que les solutions testées ont sans doute évolué depuis.

Nous n'avons pas cherché à évaluer la performance *antispam* de ces solutions mais nous nous sommes surtout intéressés aux fonctionnalités, en particulier la souplesse d'administration et la quarantaine. Le niveau d'approfondissement de ces différentes évaluations est très variable selon que nous avons pu :

- seulement assister à une présentation commerciale ;
- faire des tests sur une maquette ;
- tester le produit en grandeur nature.

9.1 MailInBlack [MB]

Ce système original se distingue complètement des autres solutions testées. Même si nous avons choisi de ne pas parler du coût des solutions, il faut signaler que cet outil est moins cher que les autres formules testées. Ce système est basé sur le principe de l'authentification de l'expéditeur. Si votre messagerie est protégée par MailInBlack, chacun de vos correspondants devra s'authentifier la première fois qu'il vous adressera un courriel. Cette identification se fait en recopiant dans un formulaire le code alphanumérique qui est affiché dans une image (CAPTCHA[13]), ce qu'un moteur de *spam* ne peut pas faire. Si cette étape est franchie, votre correspondant est inscrit une fois pour toutes dans votre liste blanche et n'aura plus à refaire cette opération. Vous avez aussi la possibilité d'inscrire par avance vos correspondants habituels dans votre liste blanche personnelle pour leur éviter cette opération (une liste globale est également gérée par l'administrateur du site). Ce système est efficace mais peut dérouter vos correspondants même si l'interface d'identification est entièrement personnalisable pour le site (logo, message d'accueil). Cela peut également être pénible si votre correspondant envoie un mail à plusieurs personnes sur votre site : il lui faudra s'identifier autant de fois que de correspondants puisque les listes sont individuelles. Certains utilisateurs pourraient craindre de perdre des messages si l'identification se passait mal. Si on utilise un client de messagerie en mode texte (pine sous Unix par exemple), l'enregistrement est impossible (il faut un environnement graphique et un navigateur web pour pouvoir accéder au formulaire). D'autre part, la pérennité

[13] **CAPTCHA** : Completely Automated Turing Test To Tell Computers and Humans Apart. Un Captcha est une forme de test de Turing permettant de différencier de manière automatisée un utilisateur humain d'un ordinateur.

d'un tel mécanisme peut être mise en doute car les robots d'envoi de *spam* sont de plus en plus efficaces et peuvent s'adapter. En outre, ce système ne règle pas le problème des mails en provenance d'une adresse usurpée qui aurait déjà été légitimement autorisée.

9.2 Esafe de Aladdin [AL]

Ce produit est disponible à la fois sous forme de logiciel sous Windows ou d'*appliance* (grâce à un CD *bootable* avec noyau Linux optimisé). Nous avons pu assister à une démonstration complète de la version 5 sur un système en exploitation et disposer ensuite d'une version de démonstration (non opérationnelle, uniquement une simulation permettant de parcourir les interfaces). Le paramétrage nous a paru lourd. Le mail récapitulatif permet d'accéder aux fonctions de la quarantaine uniquement depuis un client Outlook (utilisation de VBScript). La quarantaine n'est accessible qu'au travers de ce mail : un utilisateur attendant un mail n'aura donc aucun moyen de vérifier si celui ci a été marqué comme *spam* avant la réception du prochain mail récapitulatif. Tout le paramétrage se fait de façon globale par l'administrateur, l'utilisateur ne peut donc pas paramétrer son profil (langue de l'interface…) ou des listes noire/blanche (cela peut aussi être vu comme un avantage car cela évite des incohérences possibles entre le paramétrage global et celui de l'utilisateur[14]).

9.3 NEP (Norman Email protection) de Norman [NO]

Nous avons pu disposer de la version complète du logiciel (V4.35) mais sans serveur, ce qui ne nous a pas permis de tester les performances du système en grandeur réelle mais uniquement de voir ses fonctionnalités sur un domaine de test. Ce logiciel s'installe sous Windows uniquement et nécessite une configuration avancée (serveur IIS avec plusieurs serveurs virtuels pour les interfaces web d'administration, d'accès aux quarantaines et de supervision). L'administration se fait également depuis une application Windows sur le serveur. L'inscription des utilisateurs se fait de façon simple (auto-alimentation à partir de la liste des boîtes sur le serveur de mail). La fréquence d'envoi des mails récapitulatifs est paramétrable (un par jour au maximum) mais l'administrateur peut déclencher ponctuellement un envoi global ou pour un utilisateur en particulier. Ce rapport de quarantaine est complet : il donne la liste des nouveaux *spam*s et reprend aussi la liste des anciens pourriels dont la mise en quarantaine a déjà été notifiée mais qui n'ont pas été libérés ni effacés. Il est paramétrable (plusieurs langues) par utilisateur, mais cela peut être lourd à gérer. La liste des mails est détaillée : sujet, date, émetteur mais aussi taille, indice de confiance pour la détection du *spam*, nature du *spam* identifié. Ce mail permet de libérer ou de détruire les *spam*s un par un ou globalement en cliquant sur des liens HTTP sans authentification. L'accès à la gestion de sa quarantaine depuis une page *web* avec authentification est également possible.

9.4 PureMessage de Sophos [SO], version *appliance*

Nous avons obtenu le prêt d'une *appliance* ES4000. Le paramétrage est très rapide et les interfaces d'une grande simplicité (chaque action se fait en 3 clics au maximum). Toutefois, il s'est avéré rapidement que le système ne pourrait pas être testé en grandeur réelle. Dans notre cas de figure (configuration Active Directory non standard), il était impossible de limiter le test à certains utilisateurs. Nous avons tout de même pu passer les fonctionnalités du système en revue en utilisant un domaine de test et une authentification locale. L'administrateur peut effectuer des recherches dans la quarantaine. Il peut, de façon globale pour tous les utilisateurs, autoriser la gestion d'un profil par utilisateur (possibilité de désactiver le filtrage, de ne pas recevoir le rapport de quarantaine, de gérer des listes blanche/noire). L'interface utilisateur est très simple et pratique, elle est disponible dans au moins 6 langues au choix de l'utilisateur. Un mail de rapport de quarantaine peut être envoyé à un moment et à une fréquence paramétrables. Il permet d'effectuer directement les opérations sur la quarantaine (effacement ou libération) sans avoir à s'authentifier (liens envoyant un mail de contrôle). Il est possible de se connecter sur l'interface de gestion de la quarantaine en s'authentifiant ou de demander à recevoir un mail comportant un lien d'accès sans authentification, valable quelques heures seulement. L'utilisateur ne peut pas effectuer de recherche sur les mails en quarantaine. Plusieurs tâches se font de façon asynchrone ce qui est parfois déroutant. Par exemple, nous avons observé un temps de latence de plusieurs minutes entre la libération d'un mail et son arrivée dans la boîte de l'utilisateur. De même, le contenu de la quarantaine n'est pas rafraîchi en temps réel (il s'agit de pages statiques pour des raisons de performance). Ainsi, si on accède à la quarantaine depuis un mail récapitulatif de quarantaine, les nouveaux messages qui ont pu arriver entre-temps n'apparaissent pas.

9.5 PureMessage de Sophos, logiciel pour Linux

Le logiciel PureMessage (dont l'*appliance* décrite ci-dessus est une version très simplifiée) est disponible en version Linux. Nous avons testé la version 5 dans une machine virtuelle sur un domaine de test ce qui ne nous a pas permis de tester les performances du produit. A l'inverse de l'*appliance*, ce produit est d'une grande complexité. Il intègre un serveur Postfix (qu'il faut être capable de configurer). L'installation se fait en mode texte mais on dispose ensuite d'une interface web pour l'administration. Le paramétrage se fait dans un langage de type script (il y a plusieurs centaines de règles) et le modifier demande un fort investissement (par exemple pour changer le type de rapports émis ou modifier les seuils de détection). Un module de test permet de générer des pourriels de façon automatique et de tester ainsi facilement la tenue en charge du serveur (ce qui peut se révéler pratique, mais ne doit pas

[14] Selon le bon vieil adage : « *It's not a bug, it's a feature* »…

être utilisé pour les statistiques de détection[15]). L'interface utilisateur est sensiblement la même que celle de la version *appliance*.

9.6 Ironport [IR]

La société Ironport, qui proposait à l'origine des solutions *antispam* pour les FAI[16], se tourne désormais vers le marché des PME. Du fait de son implantation historique chez plusieurs grands fournisseurs d'accès, la société dispose d'une base de *monitoring* importante, appelée *SenderBase*. Certaines informations de la *SenderBase* sont consultables sur Internet [SE]. On peut ainsi connaitre l'évolution du trafic mail d'un domaine, ainsi qu'un score de réputation associé. A partir de ce type d'information (et d'autres non publiées, telles que les plaintes, les listes blanche/noire etc...), lorsque l'utilisation de la *SenderBase* est activée, le boîtier évalue dès l'établissement de la connexion SMTP la probabilité qu'un courrier soit un spam. Au-delà d'un certain score, la connexion est interrompue avant même la réception de l'en-tête du message. Le but est d'éliminer les connexions en provenance des domaines spammeurs sans avoir à traiter leurs messages afin de limiter l'utilisation du CPU du boîtier.

Une *appliance* C100 (AsyncOS version 5.0) nous a été prêtée. Après configuration et test, nous avons décidé de la mettre en place pendant deux semaines pour filtrer le trafic mail du laboratoire. Aucun utilisateur ne nous a signalé de perte de messages et le nombre de *spams* a chuté à quelques pourriels par semaine et par personne. Ce boitier permet une authentification SMTP afin d'envoyer du trafic depuis l'extérieur du laboratoire. Cette authentification peut utiliser LDAP/Active Directory, ou IMAP/POP (le boîtier vérifie les comptes par une requête au serveur de mail). Toutefois, le fonctionnement sans annuaire ne permet pas au boîtier de connaître les alias (sur la version testée, il était impossible de les déclarer manuellement). Dans ce cas, si l'utilisateur dispose de plusieurs boîtes-aux-lettres avec des *aliases* (ex : si prenom.nom@domaine.fr est un alias de nom@domaine.fr), l'*appliance* n'a aucun moyen de savoir qu'il s'agit de la même personne : elle créera donc autant de quarantaines que d'*aliases*, et donc autant de *message digest* (un à destination de nom@domaine.fr, et un à prenom.nom@domaine.fr, que le serveur de mail redirigera sur la même boîte). L'utilisateur recevra donc plusieurs résumés de quarantaine, depuis lesquels il pourra libérer les éventuels messages valides en cliquant sur les liens, mais il ne pourra pas accéder directement aux quarantaines de ses *aliases* en passant par la page web de l'*appliance* (son identifiant/mot de passe donne accès à la quarantaine de sa boîte principale uniquement).

Le *message digest* est simple et clair, il indique pour chaque message retenu l'expéditeur, le titre du message et la date de réception. Un clic sur le lien « Pas un spam » en face d'un éventuel message légitime permet de le recevoir instantanément.

L'interface administrateur est assez complète et lisible. Ce boîtier n'est pas ouvert, dans le sens où Ironport garde assez jalousement le secret sur les différents procédés utilisés pour détecter les messages indésirables. Par exemple, le score des messages n'est pas visible de l'administrateur. On peut rajouter un marquage sur les messages (sujet ou entête) pour retrouver quelle politique a été appliquée sur un mail, mais le système reste relativement opaque. Il n'y a aucun moyen de retrouver le détail d'un message supprimé par l'action de la *SenderBase* : s'ils sont activés, on retrouvera dans les *logs* des informations sur la connexion (IP, heure, ...) mais aucune sur le message lui même puisque la connexion aura été coupée avant. Ceci signifie que si un utilisateur se plaint de ne pas avoir reçu un mail et met en doute le filtrage du laboratoire, l'administrateur n'a pas les moyens d'effectuer une recherche précise (sur l'émetteur ou le sujet par exemple) pour déterminer si le message a été rejeté par la *Senderbase* sur la réputation du site émetteur, ou s'il n'a simplement jamais été envoyé à la bonne adresse. Comme il est impossible d'exclure individuellement les utilisateurs qui le souhaitent de la politique de la *SenderBase*, une possibilité serait de désactiver cette dernière pour tout le laboratoire. Dans ce cas on perd alors le principal intérêt du boîtier, qui aura beaucoup plus de travail puisqu'il devra analyser tous les mails : durant nos tests, plus des deux tiers des messages ont été automatiquement supprimés par l'action de la *Senderbase*. Aucun utilisateur ne s'est plaint de la perte de mails, et nous n'avons détecté qu'un seul message légitime classé comme du *spam* probable (un simple clic dans le *message digest* a permis de le restituer instantanément).

9.7 Symantec Mail Security [SM]

Symantec a récemment lancé sa gamme d'*appliances* sur le marché français (fin 2006, nous avions des difficultés à trouver un fournisseur pour ce matériel). Le matériel testé durant le mois d'août est le modèle d'*appliance* Symantec Mail Security 8240 (logiciel version 7.5.0-15). La prise en main du produit est rapide. Une fois connecté sur l'Active Directory, il est possible d'appliquer une politique de filtrage particulière sur un groupe d'utilisateurs (le boîtier reconnaît les groupes AD). Ceci permet de le mettre en test facilement sur un groupe de boîtes-aux-lettres avant d'appliquer la politique sur l'ensemble du laboratoire, lorsque sa configuration est satisfaisante. En effet, il existe un groupe par défaut dans lequel tombent tous les courriels qui sont à destination des boîtes-aux-lettres qui n'appartiennent à aucun groupe. Lors des premiers tests, on pourra donc décider de ne pas appliquer de politique de filtrage sur le groupe par défaut. Ceci se révèle utile, car on peut ainsi tester sa politique de filtrage en environnement réel mais restreint à quelques utilisateurs, tout en restant transparent pour le reste du laboratoire. On peut également déclarer manuellement des aliases et des listes de diffusion, ou les importer depuis un fichier texte simple.

[15] Il est évident que le *spam* généré par l'outil Sophos sera forcément détecté comme tel par le boîtier Sophos, ce qui ne signifie pas que PureMessage détecte 100% du pourriel !

[16] Fournisseur d'Accès à Internet.

L’interface utilisateur est pratique : après authentification dans le domaine Active Directory, l’utilisateur accède à sa quarantaine. L’administrateur peut permettre aux utilisateurs de gérer leurs listes blanche et noire personnelles (avec éventuellement autorisation des jokers), ainsi qu’une liste des langues valides pour les e-mails (le système reconnaît 11 langues). Une option intéressante est la possibilité de filtrer les messages de la quarantaine sur l’expéditeur, sur l’objet ou l’ID du message. La possibilité d’afficher jusqu’à 500 messages par page se révèle utile pour rechercher un message particulier noyé dans le flot des *spams* lorsque la politique est de placer tous les messages indésirables en quarantaine. En pratique, après une période d’essai, on configurera le boîtier pour supprimer directement tous les *spams* jugés comme tels, et pour ne garder en quarantaine que les messages jugés comme « *spams* probables ». Durant notre période de test de deux semaines, environ 80% des messages se sont avérés être du *spam* (supprimés directement) et moins de 2% du *spam* probable (mis en quarantaine). Parmi ce *spam* probable, moins de cinq messages étaient des messages légitimes et ont été libérés. Les utilisateurs nous ont signalé une quasi disparition des *spams* (moins d'une dizaine par semaine et par utilisateur, en moyenne). A noter que le boîtier dispose d’une option de détection des *Directory Harvest Attack* qui permet de bloquer les expéditeurs qui envoient un flot de courriels à destination d’une majorité d’adresses inconnues, ainsi qu’une option similaire pour contrer les expéditeurs de virus (on peut par exemple rallonger le temps de réponse aux connexions SMTP).

10 Bilan des tests

A l’issue de ces tests, il est intéressant de souligner les points suivants, qui pourront influer sur le choix de la solution :

- Il préférable d’avoir un Active Directory complètement renseigné, notamment au niveau des adresses e-mails et des aliases, pour bénéficier d’un maximum de fonctionnalités offertes par les boîtiers.

- La totalité des matériels évalués est capable de gérer plusieurs domaines, ce qui permet notamment de faire des essais avec un domaine de test (ceci nécessite toutefois de mettre en place un serveur de mail de test – une machine virtuelle pourra faire l’affaire).

- Toutes ces *appliances* envoient un résumé des messages en quarantaine. Il faut vérifier que ce message HTML est compatible avec tous les clients de messagerie (et pas uniquement Outlook), ce qui exclut notamment l’utilisation de VBScript. Le *digest* informe des nouveaux messages mis en quarantaine. Certains proposent un affichage trié par score croissant (affichage des *spam*s les plus probables à la fin), l’utilisateur vérifiera donc en priorité les premiers messages et passera rapidement les autres.

- Les listes de diffusion sont sources de problèmes : doivent-elles avoir leur propre quarantaine, les utilisateurs des listes doivent-ils recevoir les *messages digests* ?

11 Le cahier des charges

L'expérience acquise au cours de cette pré-étude nous a permis d'affiner le besoin initialement exprimé et d'établir notre cahier des charges :

- Nous recherchons une solution de type *appliance* afin de ne pas avoir à installer et maintenir à la fois un logiciel et un serveur. Cette solution doit être indépendante de notre serveur de mail (Postfix actuellement mais susceptible d'évoluer vers Exchange). Le système doit être dimensionné pour gérer confortablement 300 boîtes-aux-lettres et avoir des possibilités d'évolution. Le matériel doit être robuste et fiable (offrir un mécanisme de redondance).

- Le système devra nécessiter une administration minimale et être administrable à distance par une interface de type *web*. Des pages récapitulatives, de préférence sous forme de graphiques, permettront de suivre l'activité du système.

- Le système doit fonctionner en toute transparence et ne doit pas rejeter de mail sans en garder une trace. Nous souhaitons pouvoir retrouver la trace de n'importe quel mail reçu et savoir quel traitement lui a été appliqué. Le paramétrage du système doit être suffisamment fin pour permettre aux utilisateurs qui le souhaitent de recevoir la totalité des mails qui leur sont destinés, sans aucun filtrage.

- Le système intégrera un mécanisme de quarantaine consultable à tout moment par l'utilisateur à partir d'une interface de type *web* avec authentification (au travers d'un serveur Active Directory).

- Les interfaces destinées aux utilisateurs devront être simples et pratiques d'emploi, disponibles au moins en anglais et en français (choix possible au niveau de chaque utilisateur).

- Un mail récapitulatif des *spam*s mis en quarantaine doit pouvoir être envoyé régulièrement aux utilisateurs concernés et doit pouvoir servir de point d'accès pour la gestion de la quarantaine (libération ou destruction des mails) quel que soit le client de messagerie utilisé.

- L'administrateur mais aussi l'utilisateur devront pouvoir effectuer des recherches et des tris dans la quarantaine ainsi que des opérations multiples (comme par exemple effacer un lot de messages sélectionnés).

- Eventuellement, l'utilisateur pourra gérer ses propres listes blanche ou noire.

12 Conclusion

Cette étude fut plus longue que prévu. Pour le choix de ce type d'équipement, il nous apparaît primordial de pouvoir faire des tests, si possible en grandeur réelle. Ceux-ci sont la meilleure façon de se rendre compte de la facilité d'administration et d'utilisation ainsi que des performances réelles d'un produit. Il est également important de recouper les informations provenant des éditeurs et des distributeurs car elles ne sont pas toujours cohérentes.

13 Références

[AL] Aladdin : http://www.aladdin.com/esafe

[IR] Ironport : http://www.ironport.com

[MB] MailInBlack : http://mailinblack.com

[NO] Norman : http://www.norman.com

[PF] Postfix : http://www.postfix.org

[SA] SpamAssassin, http://SpamAssassin.apache.org

[SE] *SenderBase* : http://www.*SenderBase*.org

[SM] Symantec Mail Security : http://www.symantec.com/enterprise/products/category.jsp?pcid=2242

[SO] Sophos : http://www.sophos.fr

[TE] Techniques de détection du pourriel : http://fr.wikipedia.org/wiki/Anti-pourriel

[TU] « Lutte *antispam* concrète et pratique avec du logiciel libre », tutoriel présenté lors des JRES2005 par S. Bortzmeyer et P. David

[MA]http://www.magsecurs.com/article.php3id_article=6897