



vaderetro

Anti spam Technology



GOTO Software
DEVELOPPEMENTS DURABLES

Les masses de courriers indésirables envoyées et reçues dans le monde entier ralentissent considérablement la productivité des employés et celle des infrastructures réseaux en entreprise. Le coût du spam est estimé entre 600 et 1000 dollars par an et par salarié et augmente de 100% chaque année.

Sensible au problème, GOTO Software développe Vade Retro depuis 2002, une technologie de protection contre les spams et autres formes de pollution de messagerie.

Efficace, rapide et autonome, la technologie Vade Retro 100% française protège de un jusqu'à plusieurs millions d'utilisateurs.

Grâce à son indépendance applicative, Vade Retro présente l'avantage inédit d'être "intégrable" sur tout système d'information qui traite ou fait transiter des courriers électroniques. Le composant de filtrage a donc été intégré sous différents outils pour messagerie (barre d'outils pour poste client, logiciel pour application de messagerie, boîtier Appliance...), de manière à répondre aux besoins et aux problématiques d'infrastructures de chaque entreprise.

De prestigieuses références comme Free, Club Internet, Ya.com... nous ont retenus pour le sérieux de nos applications et l'efficacité de notre travail. Comme eux, choisissez ce qui se fait de mieux pour protéger votre messagerie, choisissez Vade Retro Antispam.



Un fléau grandissant

■ Qu'est-ce que le spam ?

Il n'existe pas de définition officielle et universelle du mot "spam". Néanmoins, la CNIL (Commission Nationale Informatique et Libertés) le décrit ainsi :

Envoi massif et parfois répété de courriers électroniques non sollicités à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact au préalable, et dont il a capté l'adresse électronique de façon irrégulière.

Aussi appelé pourriel, pollurriel, courrier-rebut, il s'agit à l'origine d'une marque anglaise de corned-beef. Plus précisément, SPAM est un acronyme pour "Spiced Pork And Meat" (pâté épicé à base de porc et de viande). La théorie la plus courante veut que le terme provienne d'un sketch des Monty Python, dans lequel les comiques britanniques chantaient : "Spam spam spam spam, spam spam spam spam, spam spam spam spam...". La chanson, interminable et interprétée crescendo, couvrait les propos des autres protagonistes.

■ D'où vient le spam ?

Avec le développement exceptionnel de l'Internet et du courrier électronique, les spammeurs ont trouvé un formidable outil pour communiquer massivement : l'e-mail est universel et accessible sur de plus en plus de supports. De plus, il est instantané et interactif, il peut être archivé et renvoyé facilement, et son coût est quasi nul en comparaison à celui d'un mailing postal.

Les spammeurs profitent également de la lenteur judiciaire liée aux nouvelles technologies et de la relative inexpérience ou innocence des internautes face à ce fléau.

■ Combien coûte le spam ?

Le spam coûte beaucoup d'argent aux entreprises. Il est estimé entre 600 et 1000 dollars par an et par salarié. En fonction du nombre de postes et de la quantité moyenne de spams reçus, il est assez simple de réaliser une estimation du coût généré par le spamming pour une entreprise. Cette charge inutile nuit au bon fonctionnement de l'entreprise : elle paralyse l'activité des employés et monopolise les ressources informatiques utiles à d'autres tâches.

Le spam en quelques chiffres

- **100%** : croissance du coût du spam chaque année
- **42 milliards de \$** : coût global pour les entreprises au niveau mondial en 2004 (prévision : 200 milliards de \$ en 2007)
- **600 à 1000 \$** : coût par an et par salarié
- **Plus des 2/3** du volume total et mondial d'e-mails envoyés
- **85%** des spams reçus en France sont rédigés en langue anglaise (7% en français)
- **60%** proviennent des Etats-Unis

Sources : Basex, Radicati Group, Ferris Research, Postini, CNIL

■ Quels sont les différents types de courriers indésirables ?

Les courriers indésirables peuvent revêtir divers aspects ; voici quelques déclinaisons possibles :

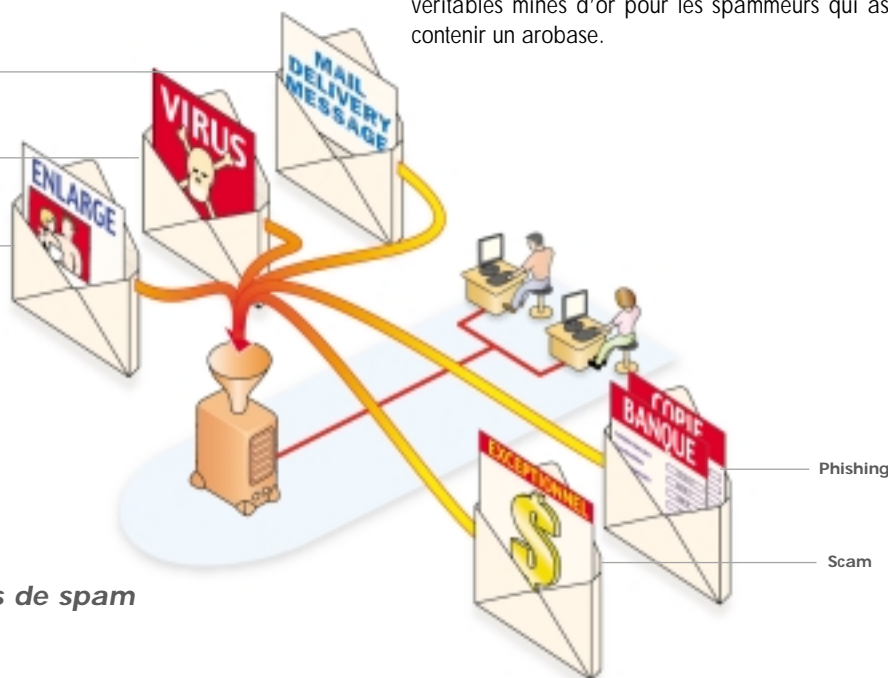
- Spams

Il s'agit d'e-mails publicitaires vantant l'intérêt d'un produit ou d'un service. Généralement rédigés en anglais, ils représentent la majeure partie des courriers indésirables envoyés. Ces spams concernent essentiellement la santé, les loisirs, la finance et les services web, mais peuvent également présenter un contenu choquant (messages à caractère pornographique, politique, religieux, racial...).

Notifications de serveurs

Virus à propagation automatique

Spams commerciaux



Les différents types de spam

- Virus à propagation automatique

Ils exploitent les carnets de contacts des machines infectées et se propagent extrêmement facilement. Ils sont souvent inclus dans un e-mail simple contenant quelques mots et une pièce jointe.

De surcroît, les créateurs de virus travaillent de plus en plus main dans la main avec les spammeurs, contribuant ainsi à leur diffusion.

- Notifications de serveurs

Egalement appelés "Mail Delivery Message", ces e-mails sont envoyés automatiquement sur l'adresse de l'expéditeur pour le prévenir qu'un destinataire n'a pas reçu son message. Avec la prolifération des virus utilisant les carnets de contacts, ces messages sont de plus en plus nombreux.

- Scam

C'est une escroquerie qui repose le plus souvent sur des propositions de participation à une opération financière internationale très alléchante. Initialement pratiqués par courrier traditionnel ou par fax, les scams ont aujourd'hui leur déclinaison par e-mail.

- Phishing

Cette technique consiste à prendre l'apparence visuelle d'un service en ligne connu et à demander à un internaute réellement client du site de mettre à jour ses données personnelles dans un formulaire factice afin de les intercepter.

Le montant total des fraudes attribuables au phishing en 2004 s'élève à 137 millions de dollars, occasionnés par 31 000 attaques (source : TowerGroup).

■ Comment les spammeurs collectent-ils les adresses e-mail ?

- Achat ou échange d'adresses

Il devient facile de se procurer des fichiers d'adresses nominatives auprès d'acteurs douteux pratiquant l'art de la collecte déloyale.

- Robots ou "crawlers"

Ce sont de petits logiciels programmés pour rechercher et stocker automatiquement toutes les adresses e-mail que l'on peut trouver sur le web.

- Usenet, mailings list, Chat room...

Ces places de discussion aux mécaniques parfois archaïques sont de véritables mines d'or pour les spammeurs qui aspirent tout ce qui peut contenir un arobase.

- Sites Internet

Certains exploitants ou webmasters peu scrupuleux transmettent les informations personnelles d'internautes à des tiers, en détournant le but de la collecte.

- Chaînes ou "Hoax" (rumeurs)

Messages faisant appel au bon cœur et à la naïveté des internautes pour répandre de fausses informations. Beaucoup de gens n'hésitent pas à relayer ce type de message parfois même sur tous leurs contacts. Les chaînes sont de véritables pots de miel pour les spammeurs.

- Virus

Certains virus, plus particulièrement les vers, aspirent et utilisent les listes de destinataires des internautes mal protégés pour se propager. Beaucoup de spammeurs profitent de ces propagations pour collecter.

- Reconstitution d'adresse e-mail (e-mail address harvesting)

Piratage mené par certains spammeurs pour dérober le répertoire complet des adresses E-mail d'une entreprise. Le principe est de reconstituer aléatoirement (prénom.nom@domaine.com par exemple) des adresses et de les tester. La gratuité de l'envoi de mail rend cette technique très pratiquée.

Une protection indispensable

■ Quelles sont les nuisances du spam ?

- Sollicitation des infrastructures

Les spams encombrant le réseau Internet et consomment de la bande passante.

- Perte de temps et de productivité

Le filtrage des spams s'avère long et laborieux, faisant perdre un temps précieux aux employés .

- Perte d'attention et de messages utiles

Les salariés risquent de supprimer des messages importants noyés sous la masse de spams.

- Risque sécuritaire

Les spams sont parfois porteurs de virus pouvant infecter l'ordinateur et le carnet d'adresses.

- Abandon d'adresses e-mail

L'abandon ou le changement d'une adresse trop ciblée par les spammeurs est parfois difficile voire impossible dans certaines entreprises. De plus, cette pratique n'est qu'un contournement du fléau, elle ne le résout pas. Bien souvent les spams reviennent au galop.

NB : 39% des internautes ont changé ou aimeraient changer d'adresse e-mail à cause des spams qu'ils reçoivent chaque jour.

(source : étude AOL / Novatris).

- Changement d'habitude

La réception de spams en grande quantité influence le comportement des salariés, qui ont tendance à vérifier de manière moins régulière leurs e-mails (au lieu de lire chaque message entrant instantanément).

Certains spammeurs vont même jusqu'à menacer au chantage les entreprises et leurs employés... "Payez ou vous serez infectés" : en plus de spammer, il s'agit d'extorquer de l'argent aux salariés en les menaçant d'effacer des fichiers importants sur leur ordinateur ou d'y copier des photographies obscènes.

■ Une solution anti-spam : pour qui ?

- **Pour les ISP** (Internet Service Provider) souhaitant alléger le trafic de messagerie et offrir à tous leurs clients un service de protection contre les spams.

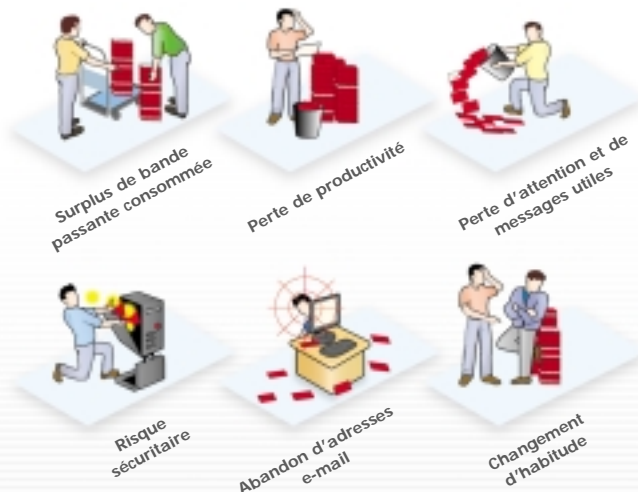
- **Pour les grandes entreprises et administrations** nécessitant l'installation d'une protection généralisée sur les serveurs locaux sans intervenir sur les postes clients ni sur l'infrastructure existante.

- **Pour les PME** voulant sécuriser rapidement tous les postes de leurs employés.

- **Pour les TPE et indépendants** possédant quelques postes informatiques à protéger des spams.

>> Pour toute entreprise ou organisation souhaitant éradiquer le spam et permettre à ses collaborateurs ou clients de tirer le meilleur profit de leur messagerie électronique.

Les différentes nuisances du spam



vaderetro

une technologie innovante

La technologie Vade Retro développée par GOTO Software et reconnue innovante par l'Anvar est spécialisée dans le filtrage des spams. Le moteur d'analyse, indépendant de l'application qui le supporte, permet aux solutions Vade Retro de vous apporter efficacité, rapidité, précision et flexibilité quelle que soit l'infrastructure sur laquelle repose votre messagerie.

Le module de filtrage fournit à l'application une évaluation de la spamicité de chaque message au travers d'un score indiquant le degré d'illégitimité de celui-ci.

Le principe de scoring permet à l'application utilisant le moteur de filtrage Vade Retro d'effectuer des actions distinctes (transmission, marquage, quarantaine, suppression, ...) en fonction de plages de scores pré-déterminées.

Le module d'analyse est totalement autonome. Il ne nécessite aucune connexion à un serveur externe ni aucun accès à une base de données. La détermination du score de chaque message est réalisée par une analyse de contenus purement algorithmique qui ne requiert pas de stockage d'informations.

Sa base de connaissances interne lui permet de détecter de nouveaux types de messages indésirables, sans avoir besoin d'un apprentissage de la part de l'utilisateur.

Sans réglages fastidieux, le filtre est immédiatement opérationnel dès sa mise en place.

Destiné à être intégré sous divers environnements et applications, le module d'analyse a été développé pour être le plus efficace, le plus rapide et le plus transparent possible.

La prise en compte de ces contraintes lors du choix des méthodes d'analyse, ainsi que l'utilisation de techniques spécifiques pendant toute la phase de développement, ont permis d'atteindre ces objectifs.

L'équipe de développement de GOTO Software continue de travailler sans cesse à l'amélioration du système de filtrage en fonction des nouveaux types de messages indésirables qui apparaissent.

A l'instar des anti-virus, des mises à jours régulières du code et des données associées permettent d'assurer au filtre une continuité dans l'efficacité.

L'accès aux mises à jour du filtre dépend de l'application qui le supporte. Le rythme de production de nouvelles versions est actuellement de cinq par mois.

A titre d'exemple, plus de 100 messages à la seconde peuvent être analysés sur une machine équipée d'un Pentium 4 cadencé à 1.9Ghz.

Cette rapidité permet bien souvent l'intégration du filtrage dans une application existante sans changer d'infrastructure matérielle.

Vade Retro :

- Protection autonome et immédiatement efficace
- Aucun paramétrage ou apprentissage du filtre
- Détection importante des spams (95%)
- Seul filtre antispam français sur le marché
- Une rapidité de traitement incroyable



vaderetro

Un filtrage exclusif

■ Comment déterminer la spamicité d'un message e-mail ?

La technologie de filtrage Vade Retro est composée de plusieurs milliers de règles de natures diverses, toutes appliquées à chaque message entrant.

La détermination du coefficient de spamicité (qui mesure les probabilités que le message soit un spam) est basée sur un calcul de score global, somme des scores élémentaires de toutes les règles de filtrage. Les scores élémentaires sont positifs (spam) ou négatifs (message légitime), et sont déterminés à la fois empiriquement (pour les nouveaux critères) et sur la base d'un calcul statistique appliqué aux corpus de référence.

Le score global est compris entre - 5000 (très légitime) et + 5000 (très spam), avec un pivot à 100. Cette notion de score permet de classer plus finement les messages par tranches de résultats, avec éventuellement un traitement différent selon la tranche.

Le résultat du module de filtrage est le score global, et optionnellement une chaîne de caractères décrivant l'ensemble des règles qui entrent en jeu dans le calcul de ce score global.

Ces informations peuvent être, à la demande, enregistrées dans l'en-tête du message sous forme de champs spécifiques supplémentaires (x-spam-state, x-spam-score, ...). Le sujet du message peut être également modifié par le filtre pour refléter l'état de spam du message.

■ Quels sont les différents types de filtres utilisés ?

- Les règles heuristiques

Ce sont des règles empiriques, non prédictibles, déduites à partir de l'analyse approfondie de tous les composants du message (champs d'en-tête, texte du sujet, corps du texte, html, pièces jointes, ...). Les règles heuristiques sont déterminées par des experts qui recherchent des caractéristiques originales, communes à certains types de messages (souvent envoyés par des robots), dans le but de repérer les prochains messages possédant les mêmes caractéristiques.

L'expert utilise en permanence des corpus de messages spams et légitimes qui lui servent à valider les règles. Ces corpus ont été constitués progressivement depuis le début du développement de Vade Retro.

Après validation, une nouvelle règle est intégrée directement dans le code du système de filtrage, permettant à la protection anti-spam d'être des plus efficaces.

- L'analyse sémantique

L'analyse sémantique consiste à comparer le contenu textuel du message à un dictionnaire prédéfini de mots et locutions caractéristiques des spams ou des messages légitimes.

Cette recherche n'est possible qu'après une phase de décodage précis du message et d'extraction des mots qui le composent. Cette phase, importante, permet de reconstituer les mots du message même quand ils sont lisibles mais volontairement dissimulés par l'expéditeur.

La technologie de recherche de locution de Vade Retro est à la fois très rapide et très performante, puisqu'elle permet de rechercher des combinaisons logiques de mots mais aussi de détecter des mots avec une orthographe approchante.

Différentes langues sont représentées au sein du dictionnaire et une section spécifique permet de détecter les messages légitimes en français.

Le contenu du dictionnaire a été constitué progressivement tout au long du développement du filtre et, comme pour les règles heuristiques, il est enrichi régulièrement.



- Les contre-mesures

Les filtres de ce type constituent sans doute la partie la plus originale et la plus efficace du moteur de filtrage Vade Retro.

Ils consistent à détecter, dans les messages, les techniques qu'emploient les spammeurs pour déjouer les solutions anti-spams utilisant les méthodes de filtrage "classiques".

Voici une liste non exhaustive des types de filtres, des techniques utilisées par les spammeurs et des méthodes correspondantes dans Vade Retro :

Anti-spam : Filtres basés sur des listes noires de liens vers des sites webs

Spammeurs : Liens cachés par codage des URL

Vade Retro : Détection de la présence d'URL codées inutilement

Anti-spam : Filtres basés sur des empreintes de messages (type brightmail)

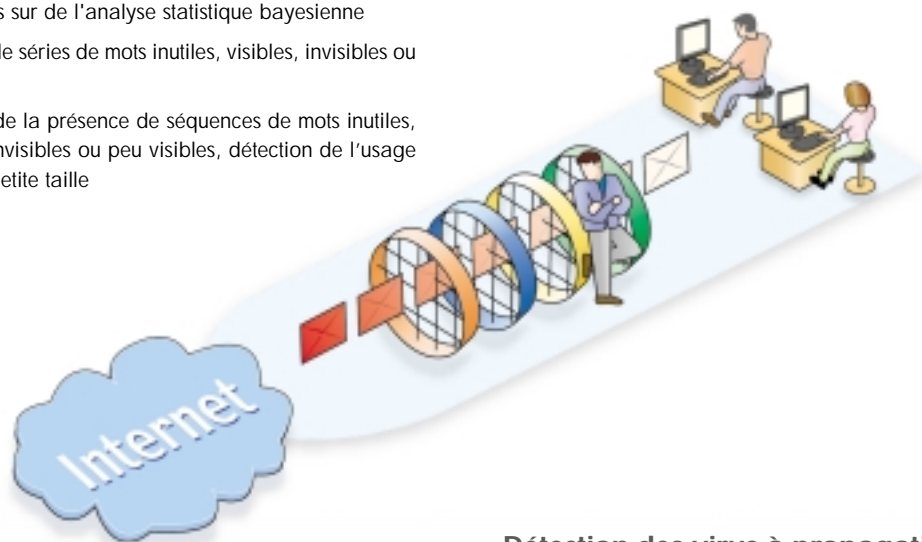
Spammeurs : Insertion de chaînes de caractères aléatoires dans les messages

Vade Retro : Détection de la présence de chaînes de caractères aléatoires

Anti-spam : Filtres basés sur de l'analyse statistique bayésienne

Spammeurs : Insertion de séries de mots inutiles, visibles, invisibles ou de très petite taille

Vade Retro : Détection de la présence de séquences de mots inutiles, détection des caractères invisibles ou peu visibles, détection de l'usage abusif des caractères de petite taille



Anti-spam :

Filtres basés sur des mots-clés

Spammeurs : Modification orthographique des mots tout en assurant leur lisibilité

Vade Retro : Détection d'anomalies dans l'orthographe des mots ou dans le code HTML :

- Lettres substituées par des chiffres (V1AGR4)
- Lettres substituées par des symboles (VI@GRA)
- Lettres substituées par d'autres lettres (VUAGRA)
- Lettres permutées (VAIGRA)
- Lettres manquantes (VAGRA, VIAGA)
- Lettres ou symboles superflus (V\$!AGRA)
- Voyelles remplacées par des équivalents accentués (VIÄGRA)
- Voyelles multipliées (VIIIAGRAAAA)
- Lettres séparées par des espaces ou des signes de ponctuation (V.I.A.G.R.A)
- Mots entrecoupés de balises HTML inutiles ou de commentaires HTML

- Les patterns HTML

Lorsque le message contient une partie HTML, une "empreinte" de ce code HTML est établie selon une méthode exclusive et comparée à une liste de "patterns" couramment utilisés par les spammeurs. Cette méthode, associée à une technique de statistiques sur les tailles d'images, permet d'identifier certains spams ne contenant pas de texte.

- Langues étrangères non latines

Toutes les utilisations de jeux de caractères non latins sont identifiées, soit lors de la déclaration du jeu de caractères, soit lors de son utilisation effective, afin d'identifier les messages publicitaires de plus en plus nombreux rédigés en langues non latines, en provenance de l'Asie ou des pays de l'Est.

- Anti-Scams / Anti-phishing

Ces nouvelles formes d'escroquerie en ligne sont vite devenues très à la mode et très employées par les spammeurs. Les éléments caractérisant ces modèles de spam ont été pris en compte dans le développement de la technologie Vade Retro, qui inclut un module spécifique de détection de ces deux types de messages.

- Détection des virus à propagation automatique

L'analyse du contenu des messages permet à Vade Retro l'utilisation des heuristiques pour la détection des messages porteurs des virus se propageant automatiquement via le réseau de machines infectées.

Cette méthode d'identification permet de détecter sur-le-champ de nouveaux virus, sans mise à jour (ex : Sober, Bagle, Zafi...).

- Détection des notifications de non remise

Le traitement des messages de notification émis automatiquement par les serveurs SMTP fait l'objet d'un traitement personnalisé. Les applications utilisant la technologie Vade Retro peuvent alors activer des actions sur ce type de messages (suppression, marquage, quarantaine dans le dossier prévu à cet effet, ...).

A chaque application, sa solution

vaderetro

Plusieurs solutions logicielles et matérielles ont été conçues pour compléter les différentes applications de messagerie sur le marché. Le filtrage de chacune d'entre elles fonctionne avec le même moteur de filtrage, seul l'environnement d'intégration change. Voici la liste des solutions présentées par ordre de capacité de traitement.

1 vade retro pour Outlook et Outlook Express

Vade Retro Outlook est une application "add-on" qui protège des spams les comptes de messagerie sur les logiciels Outlook et Outlook Express. Efficace dès son installation, la barre d'outils ne nécessite aucun paramétrage. Idéale pour les petites et moyennes entreprises ne possédant pas leur propre infrastructure de messagerie, cette solution est la plus simple et la plus rapide à intégrer.

2 vade retro ASP

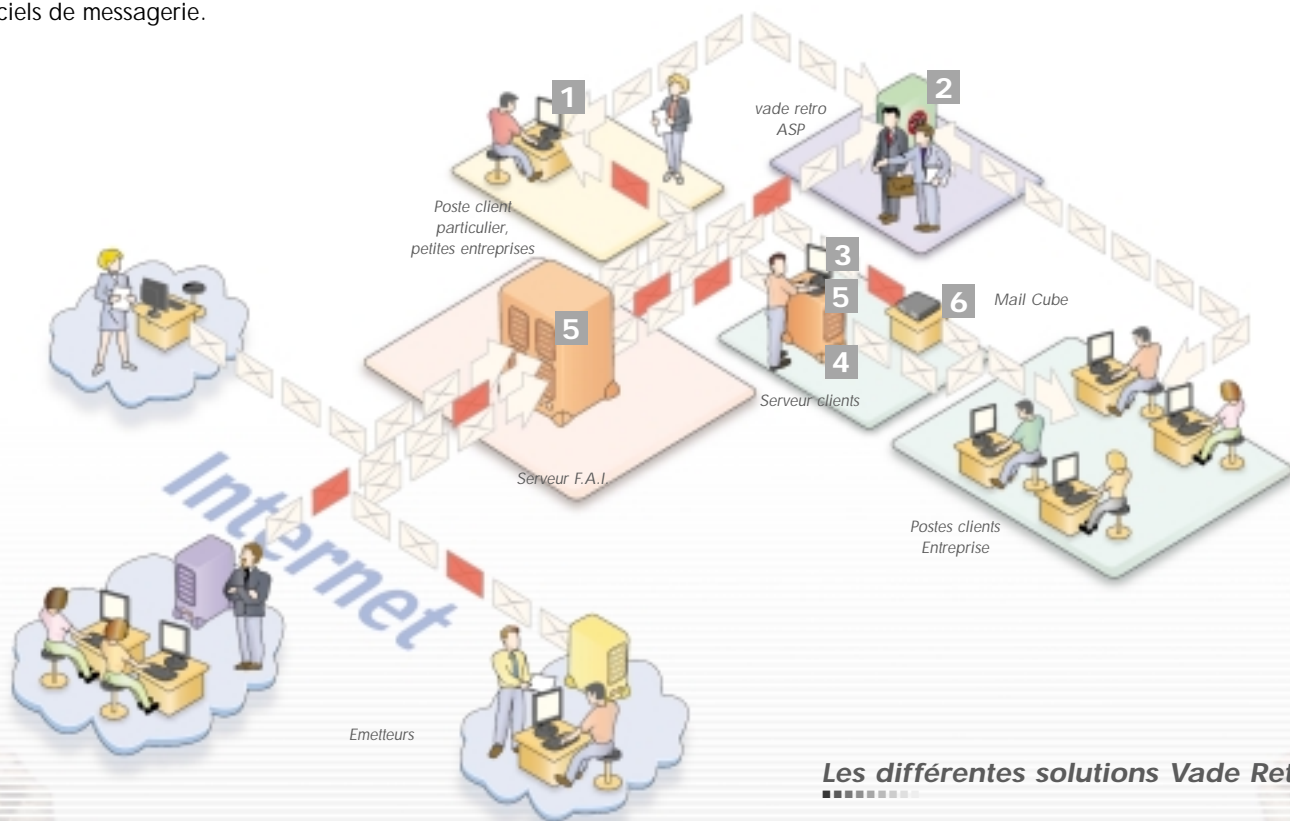
La solution ASP est un proxy POP3. Elle permet d'externaliser l'analyse et le traitement des spams envoyés sur les adresses électroniques. Le but étant de bloquer les spams avant que l'utilisateur ne les reçoive. Située entre le fournisseur d'accès et les postes clients, cette solution présente l'avantage de ne pas encombrer la bande passante et les logiciels de messagerie.

3 vade retro pour Lotus Domino

Cette solution intègre la technologie Vade Retro à l'environnement de messagerie du serveur Lotus Domino. Vade Retro pour Lotus Domino permet de garder le traitement des spams à l'intérieur de l'entreprise en centralisant le filtrage sur le serveur de messagerie. Une interface permet d'administrer le fonctionnement de Vade Retro sur le serveur pour toute l'entreprise.

4 vade retro pour Microsoft Exchange

Cette solution intègre la technologie Vade Retro à l'environnement de messagerie Microsoft Exchange 2000 et 2003. Cette solution ne nécessite l'installation d'aucun logiciel ou add-on sur les postes clients tout en permettant une gestion individualisée de certaines fonctions de filtrage.



Les différentes solutions Vade Retro

5 vade retro pour les serveurs SMTP en environnements Linux et Solaris

La technologie Vade Retro se décline également en tant que filtre de courrier entrant pour les serveurs SMTP (MTA) les plus fréquemment utilisés dans les environnements "Unix-like" : Sendmail, Postfix, Qmail, Exim, sans que le fonctionnement n'entraîne de ralentissements notables par rapport à la configuration logicielle d'origine.

6 l'appliance vade retro : Mail Cube

Mail Cube est un boîtier de filtrage paramétrable et administrable qui s'installe en DMZ en amont du serveur de messagerie. Son rôle est de filtrer et relayer le courrier au serveur SMTP de l'entreprise. Cette solution présente l'intérêt de désencombrer le trafic du serveur de messagerie sans avoir à en modifier le fonctionnement.

Efficacité :

un filtrage exclusif combinant rapidité et qualité de traitement.

Tranquillité :

éradique tous les courriers indésirables (spams, scams, phishing...).

Simplicité :

intégration et paramétrage rapide, aucun apprentissage du filtrage.

Souplesse :

des solutions qui s'adaptent aux besoins de chaque entreprise.

Sérénité :

des mises à jour automatiques et récurrentes pour un traitement optimum.

vade retro, une technologie 100% française, soutenue par l'ANVAR.





Avenue Antoine Pinay
Parc des quatre Vents - 59510 Hem
Tél. 0 328 328 325
Fax : 0 328 328 329
Site Web : www.antispam.fr