



Outils anti-spam de MDAEMON

Distributeur de valeur ajoutée - www.watsoft.com

Watsoft Distribution
3 allée de la Crabette
33600 Pessac FRANCE

Tél +33 (0)5 56 15 75 70
Fax +33 (0)5 56 15 75 71
info@watsoft.com

Sommaire

1.	Introduction	3
2.	Filtre anti-spam	4
	Configuration par défaut	4
	Résultats constatés avec la configuration par défaut	4
	Comment obtenir de meilleurs résultats.....	4
	Utiliser le dossier « Piège à spam »	5
	Gestion du dossier « Piège à spam »	6
	Gestion du dossier « Piège à spam » avec WebAdmin.....	6
	Augmenter « l'agressivité » du Filtre anti-spam	7
	Permettre aux utilisateurs de signaler le courrier indésirable	8
	Activation de l'authentification SMTP dans Outlook Express	9
	Activation de l'authentification SMTP dans Outlook	10
	Transfert d'un message en tant que pièce jointe dans Outlook Express	11
	Transfert d'un message en tant que pièce jointe dans Outlook	11
	Listes blanches, listes noires et exceptions	12
	Liste blanche automatique	12
3.	Listes noires DNS	14
	Hôtes DNS-BL.....	14
4.	Répulsion	15
5.	Liste grise (MDaemon Pro uniquement)	15
6.	Écran dynamique	16
7.	SPF/Sender ID	16
	Principe de fonctionnement	16
8.	DomainKeys/DKIM (MDaemon Pro uniquement).....	16
	Principe de fonctionnement	16
9.	Pièges à spam (MDaemon Pro uniquement)	17
10.	Protection instantanée (MDaemon Pro uniquement)	17
11.	Autres conseils permettant d'éviter le spam.....	18

1. Introduction

MDaemon contient de nombreux outils de lutte contre le spam afin de protéger au mieux vos utilisateurs contre ce fléau. Un seul d'entre eux ne suffit pas pour déceler tous les spams ; mais utilisés ensemble, ils en détectent la quasi-totalité, sans pour autant rejeter les messages légitimes.

Les paramètres par défaut de chaque outil ont été configurés de façon à bloquer une majorité de spams tout en évitant les faux positifs (messages légitimes considérés comme du spam). Toutefois, pour une utilisation optimale, il est recommandé de les adapter aux spécificités de votre système.

Ce document présente brièvement les outils anti-spam de MDAemon et leur fonctionnement. Des informations plus détaillées sont disponibles dans le manuel d'utilisation du logiciel. Ce manuel est disponible en cliquant sur **Aide** dans MDAemon ou bien en le téléchargeant sur le site <http://www.watsoft.com/mdaemon/>.

2. Filtre anti-spam

Configuration par défaut

Une fois installé, MDaemon attribue automatiquement un « score » à tous les messages reçus, à l'aide des outils anti-spam intégrés.

Par défaut, les messages possédant un score supérieur ou égal à 5.0 sont considérés comme du spam. Un indicateur est alors inséré dans l'objet du message, mais celui-ci n'est pas renvoyé, filtré ou supprimé. Pour choisir l'une de ces options, l'administrateur doit modifier la configuration du Filtre anti-spam.

De plus, les messages reçus par SMTP avec un score supérieur ou égal à 12.0 sont automatiquement refusés. En effet, un tel score indique de façon quasiment infaillible qu'il s'agit d'un spam. N'oubliez pas que refuser un message ou l'accepter puis le renvoyer ensuite à l'expéditeur sont deux procédures bien distinctes. **Il est fortement déconseillé de renvoyer les spams à l'expéditeur** car les spammeurs n'utilisent généralement pas d'adresse d'expédition valide.

Résultats constatés avec la configuration par défaut

En règle générale, si l'on conserve les paramètres définis lors de l'installation, MDaemon détecte 70 % du spam et le nombre de faux positifs est négligeable.

Comment obtenir de meilleurs résultats

Afin d'obtenir un meilleur filtrage, il est nécessaire d'améliorer l'efficacité du Filtre anti-spam, tout en augmentant graduellement son « agressivité ».

L'efficacité du système dépend surtout des utilisateurs, qui doivent signaler les spams non détectés ainsi que les faux positifs. Pour renforcer son agressivité, il suffit de diminuer progressivement le score à partir duquel un message est considéré comme du spam.

Toutefois, plus le Filtre anti-spam est agressif, plus le nombre de faux positifs risque d'être élevé. Il est donc important de contrôler également les faux positifs et de les signaler, afin d'augmenter la fiabilité du système.

En appliquant les méthodes recommandées dans ce document, le taux de détection des spams augmentera jusqu'à environ 95 %, tandis que celui de faux positifs sera dérisoire.

Distributeur de valeur ajoutée – www.watsoft.com

Watsoft Distribution
3, allée de la Crabette
33600 Pessac FRANCE

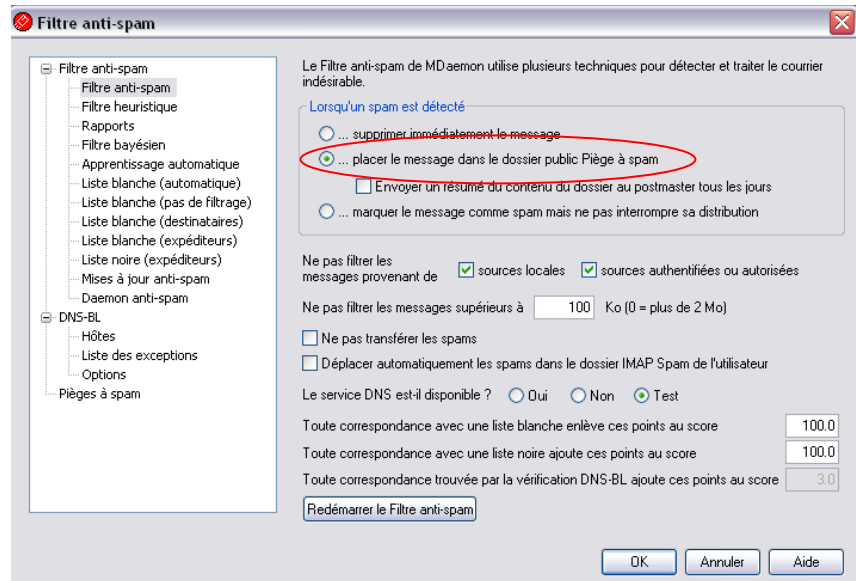
Tél +33 (0)5 56 15 75 70
Fax +33 (0)5 56 15 75 71
info@watsoft.com

Utiliser le dossier « Piège à spam »

Par défaut, MDAemon marque les spams mais les distribue tout de même aux destinataires, qui peuvent configurer des filtres au niveau de leur boîte aux lettres. Toutefois, il est souvent préférable de configurer MDAemon afin que le courrier indésirable soit filtré au niveau du serveur et ainsi géré par un administrateur.

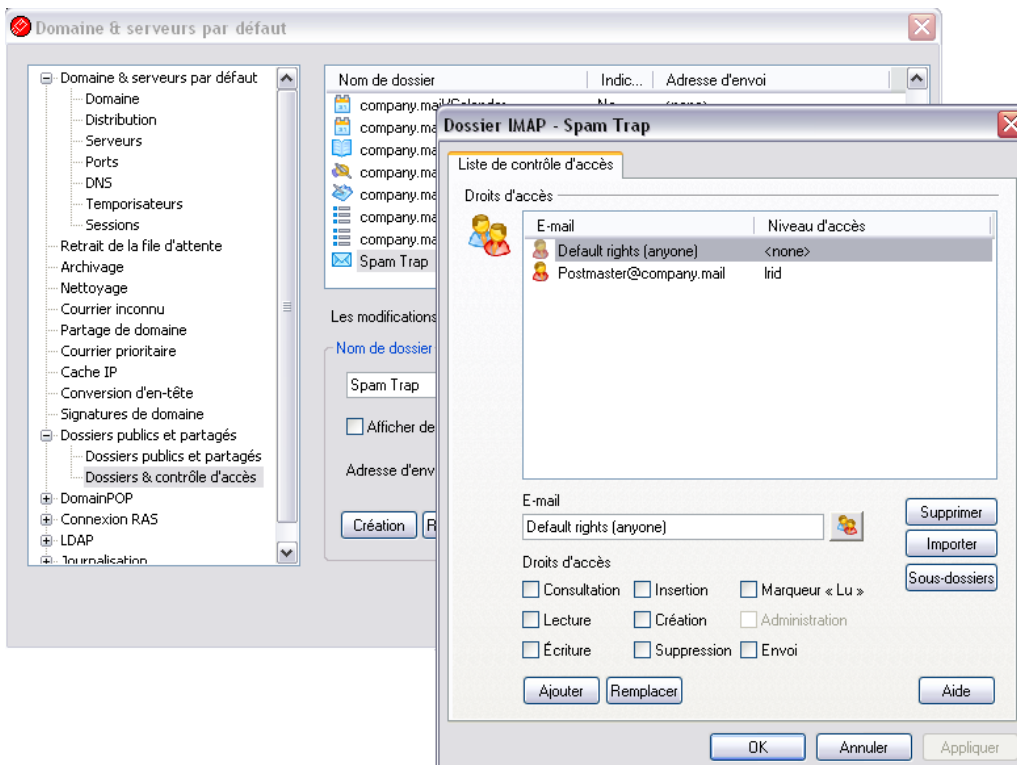
Il est possible de diriger automatiquement ces messages dans un dossier « **Piège à spam** ». Pour cela, cliquez sur **Sécurité -> Filtre anti-spam** et cochez l'option comme indiqué contre.

Tout les messages possédant un score correspondant au seuil choisi seront alors dirigés dans un dossier public appelé « **Spam Trap** » (par défaut, seul le postmaster peut consulter ce dossier).



ci-

Remarque : pour modifier les droits d'accès aux dossiers publics, cliquez sur **Configuration -> Domaine/serveurs par défaut -> Dossiers publics et partagés -> Dossiers & contrôle d'accès**.



Gestion du dossier « Piège à spam »

Plusieurs méthodes sont possibles pour accéder à ce dossier :

- Client IMAP : WorldClient, Outlook, Outlook Express ou client Outlook avec Outlook Connector
- Gestionnaire de files d'attente et de statistiques (depuis l'interface de MDAemon)
- WebAdmin (méthode recommandée)

Gestion du dossier « Piège à spam » avec WebAdmin

WebAdmin est un module additionnel gratuit permettant d'administrer MDAemon à distance par le biais d'une interface web conviviale et simple d'utilisation. WebAdmin est inclus dans MDAemon depuis la version 9. Pour la version 8, il est disponible à l'adresse suivante :

http://www.watsoft.com/dload/dload_login.asp

Une fois le logiciel installé sur le serveur, saisissez l'URL suivante dans votre navigateur pour accéder à WebAdmin :

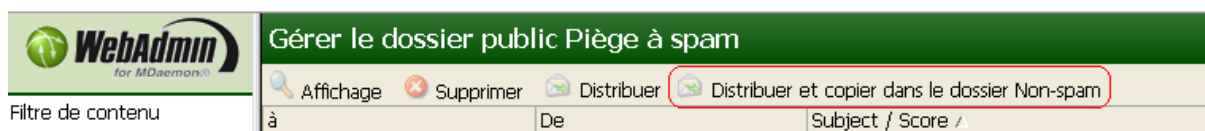
http://192.168.0.1:1000

...en remplaçant 192.168.0.1 par l'adresse IP de votre serveur. Vous devrez alors vous authentifier à l'aide de l'identifiant et du mot de passe de votre compte MDAemon.

Cliquez ensuite sur **Sécurité -> Dossier Piège à spam**.

Les messages peuvent être classés par score (colonne **Subject / Score**) ce qui permet de repérer rapidement les faux positifs.

Pour les distribuer et les marquer comme « non spam », sélectionnez-les et cliquez sur **Distribuer et copier dans le dossier Non-spam** (utilisez la touche CTRL pour en sélectionner plusieurs) :



Les messages restants peuvent alors être supprimés afin de vider le dossier.

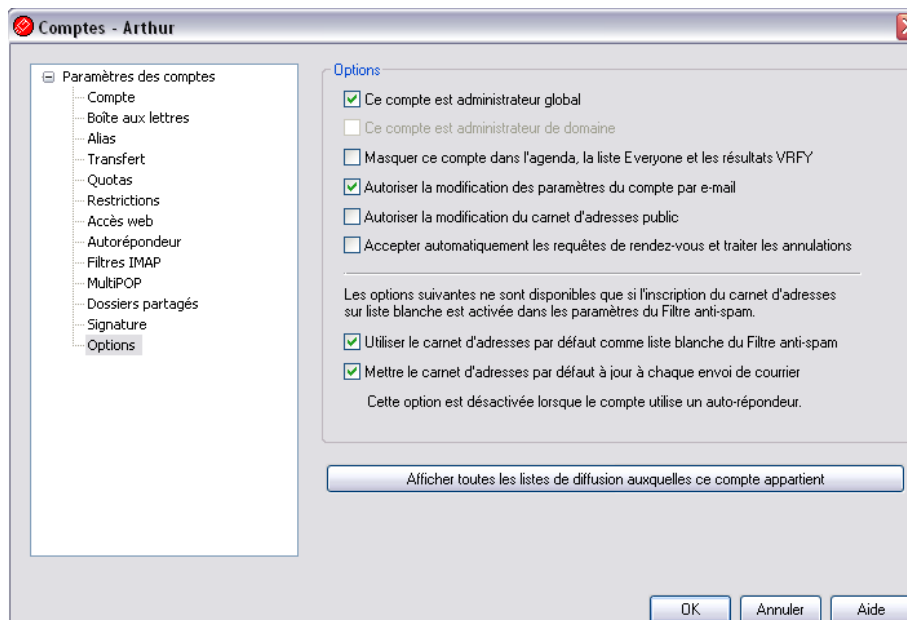
Cette tâche est très importante et doit être effectuée régulièrement (quotidiennement sur les sites de grande taille) par un « **administrateur global** ».

Remarque : pour attribuer à un compte le statut d'administrateur global dans MDAemon, cliquez sur l'onglet **Options** de l'Éditeur de comptes.

Distributeur de valeur ajoutée – www.watsoft.com

Watsoft Distribution
3, allée de la Crabette
33600 Pessac FRANCE

Tél +33 (0)5 56 15 75 70
Fax +33 (0)5 56 15 75 71
info@watsoft.com

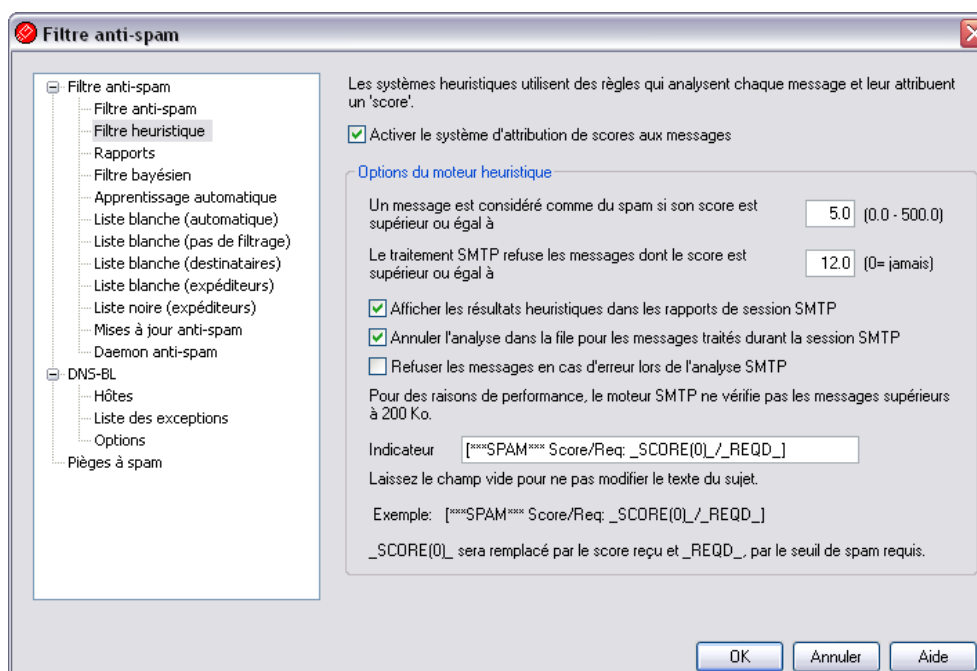


Le compte **postmaster** créé lors de l'installation possède ce statut par défaut.

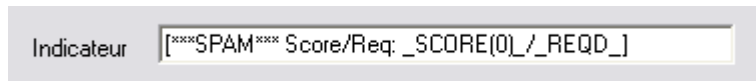
En suivant ces conseils, vous pourrez progressivement diminuer le score à partir duquel un message est considéré comme du spam. Il est également important de copier les faux positifs dans le dossier Non-spam comme indiqué précédemment car cela permet d'améliorer la précision du filtre.

Augmenter « l'agressivité » du Filtre anti-spam

L'agressivité du Filtre anti-spam de MDAEMON dépend essentiellement du score de spam requis. Par défaut, sa valeur est de 5.0. Ce paramètre peut être modifié dans MDAEMON (ou WebAdmin) en cliquant sur **Sécurité -> Filtre anti-spam -> onglet Filtre heuristique**.



Il est également recommandé de modifier le champ **Indicateur**, c'est à dire le texte ajouté dans l'objet des messages, afin de faciliter leur consultation.



En diminuant le score requis, vous réduisez le nombre de spams manqués mais augmentez aussi le risque de faux positifs.

L'expérience montre que la meilleure conduite à tenir est de **diminuer le score requis de 0,1 tous les 3 ou 4 jours jusqu'à obtenir un filtrage efficace ainsi qu'un taux de faux positifs suffisamment faible.** Évitez d'effectuer d'importantes modifications en une seule fois. Après 2 ou 3 semaines, vous devriez atteindre une valeur comprise entre 3.5 et 4.5 répondant aux besoins spécifiques de votre installation.

Enfin, n'oubliez pas que ce système est dynamique : il « apprend » à distinguer le spam des messages légitimes lorsque les messages sont copiés dans les dossiers **Spam** et **Non spam**. Ainsi, un score requis de 4.3 entraînant au début un filtrage assez agressif, peut devenir permissif au fur et à mesure que le moteur « apprend ».

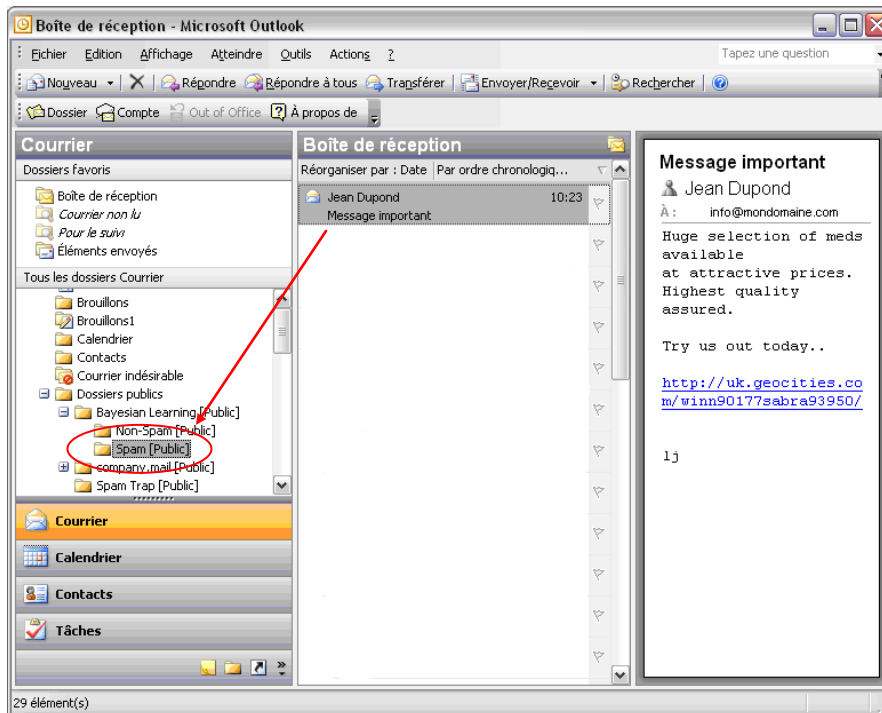
Permettre aux utilisateurs de signaler le courrier indésirable

En signalant les spams qui n'ont pas été détectés, les utilisateurs contribuent en grande partie à améliorer les performances du filtrage.

Pour cela, deux méthodes sont disponibles (utilisateurs IMAP : méthode 1 ou 2 au choix, utilisateurs POP3 : méthode 2 uniquement).

Méthode 1 (clients IMAP uniquement) – copie des messages dans le dossier d'apprentissage

Il suffit de copier les spams non détectés dans le dossier public **Bayesian Learning -> Spam** comme indiqué ci-après :



Remarque : les permissions de ces dossiers sont configurées de façon à ce que les utilisateurs puissent y copier des messages mais pas en consulter le contenu.

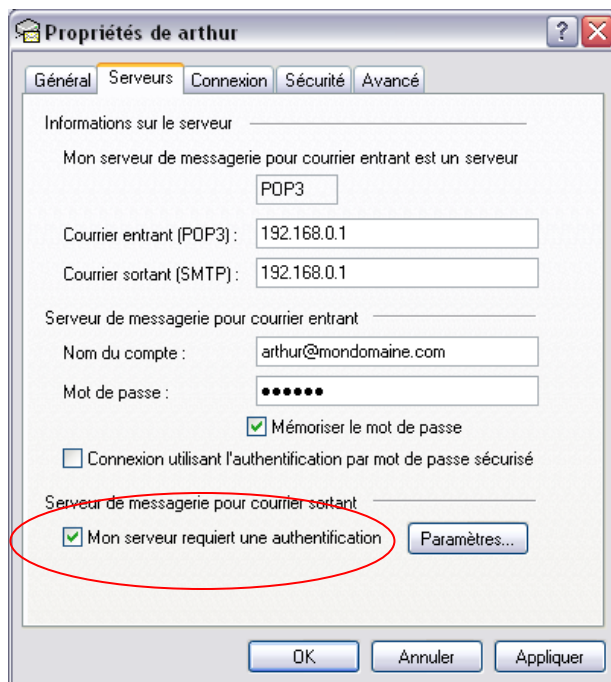
Méthode 2 (clients POP3 ou IMAP) – transfert des messages vers une adresse d'apprentissage

Les clients POP3 n'ayant pas accès aux dossiers publics partagés, les utilisateurs doivent dans ce cas transférer les spams non détectés au serveur **en tant que pièce jointe**, à l'adresse **spamlearn@mondomaine.com** (en remplaçant bien sûr « mondomaine.com » par le nom de votre domaine).

Veillez noter que les messages envoyés à l'adresse **spamlearn@...** ne seront acceptés que s'ils utilisent une session SMTP authentifiée. Pour des raisons évidentes de sécurité, **l'utilisation de l'authentification SMTP est fortement recommandée pour tous les clients de messagerie**. Il suffit généralement de cocher une case dans les propriétés du client pour activer l'authentification.

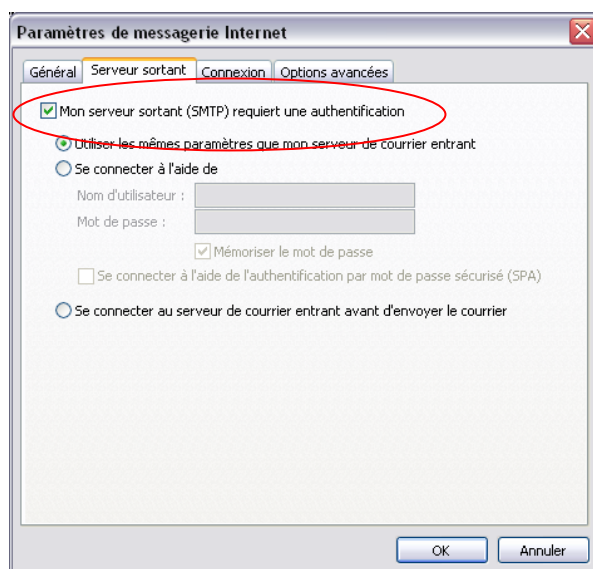
Activation de l'authentification SMTP dans Outlook Express

Cliquez sur **Outils -> Comptes -> bouton Propriétés -> onglet Serveurs :**



Activation de l'authentification SMTP dans Outlook

Dans Outlook, cliquez sur **Outils -> Comptes de messagerie -> Afficher ou modifier les comptes existants -> Modifier -> Paramètres supplémentaires -> onglet Serveur sortant :**



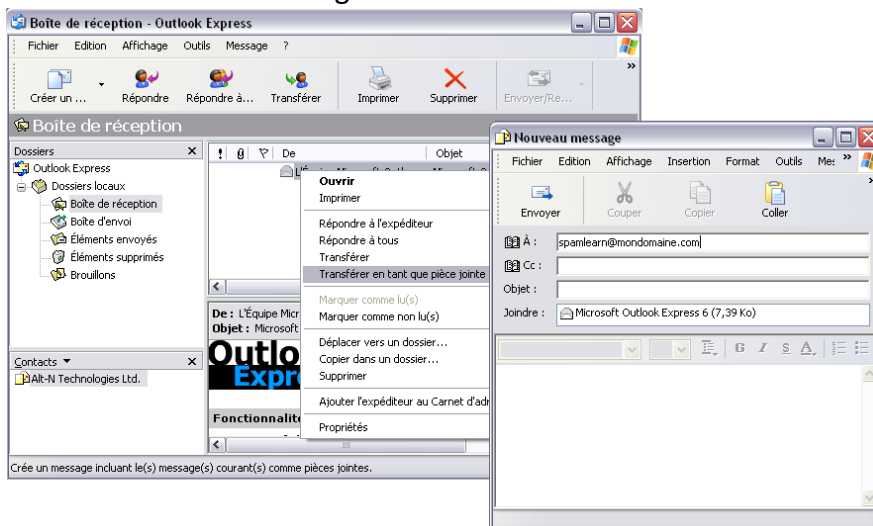
Distributeur de valeur ajoutée – www.watsoft.com

Watsoft Distribution
3, allée de la Crabette
33600 Pessac FRANCE

Tél +33 (0)5 56 15 75 70
Fax +33 (0)5 56 15 75 71
info@watsoft.com

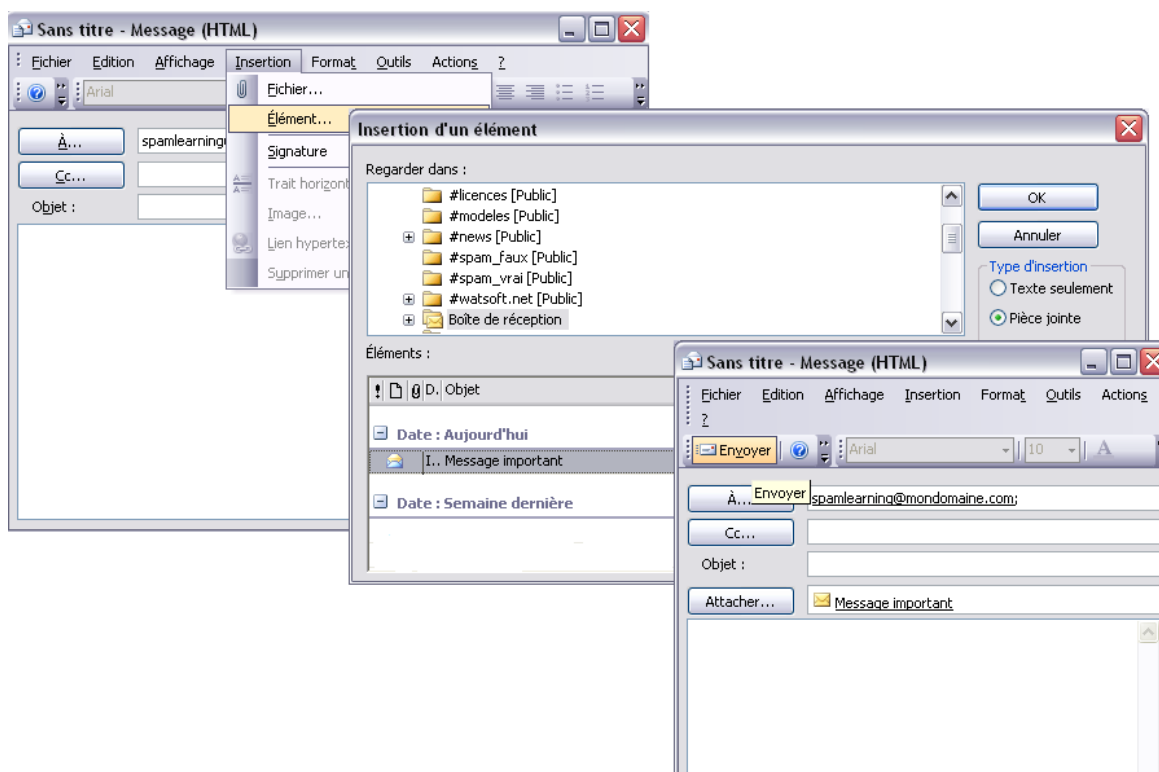
Transfert d'un message en tant que pièce jointe dans Outlook Express

Il suffit d'effectuer un clic droit sur le message et de sélectionner **Transférer en tant que pièce jointe** :



Transfert d'un message en tant que pièce jointe dans Outlook

Dans Outlook, vous devez créer un nouveau message, puis cliquer sur **Insertion -> Élément** et sélectionner le message que vous souhaitez transférer :



Listes blanches, listes noires et exceptions

En plus de la détection de courrier indésirable et de l'apprentissage, le Filtre anti-spam offre la possibilité de mettre certaines adresses et/ou noms de domaine en liste blanche, liste noire ou liste d'exceptions.

Lorsqu'un domaine ou une adresse figure dans la liste blanche, 100 points sont enlevés au score des messages correspondants : ils ne sont donc pas considérés comme du spam. Il existe deux types de listes blanches :

- Adresses ou noms de domaine expéditeurs – onglet **Liste blanche (exp.)**
- Adresses ou noms de domaine destinataires – onglet **Liste blanche (dest.)**

Inversement, 100 points sont ajoutés au score des messages provenant de domaines ou d'adresses en liste noire : ils sont donc considérés comme du spam.

Ces listes ne sont pas fréquemment employées, mais peuvent s'avérer utiles dans certains cas :

- messages légitimes systématiquement considérés comme du spam, par ex. : réservations de billets d'avion, informations sur des voitures de location, etc. ;
- messages provenant d'une source indésirable, mais n'étant pas interceptés par le filtre car ils ne s'apparentent pas à du spam.

La liste des exceptions contient les adresses ou domaines pour lesquels les messages reçus ne seront pas analysés. Cette fonctionnalité est rarement utilisée.

Les listes blanches, la liste noire ainsi que celle des exceptions sont accessibles en cliquant sur **Sécurité - > Filtre anti-spam**.

Liste blanche automatique

MDaemon comporte certaines fonctionnalités avancées permettant d'inscrire automatiquement sur la liste blanche les adresses et domaines expéditeurs légitimes afin de diminuer le risque de faux positifs.

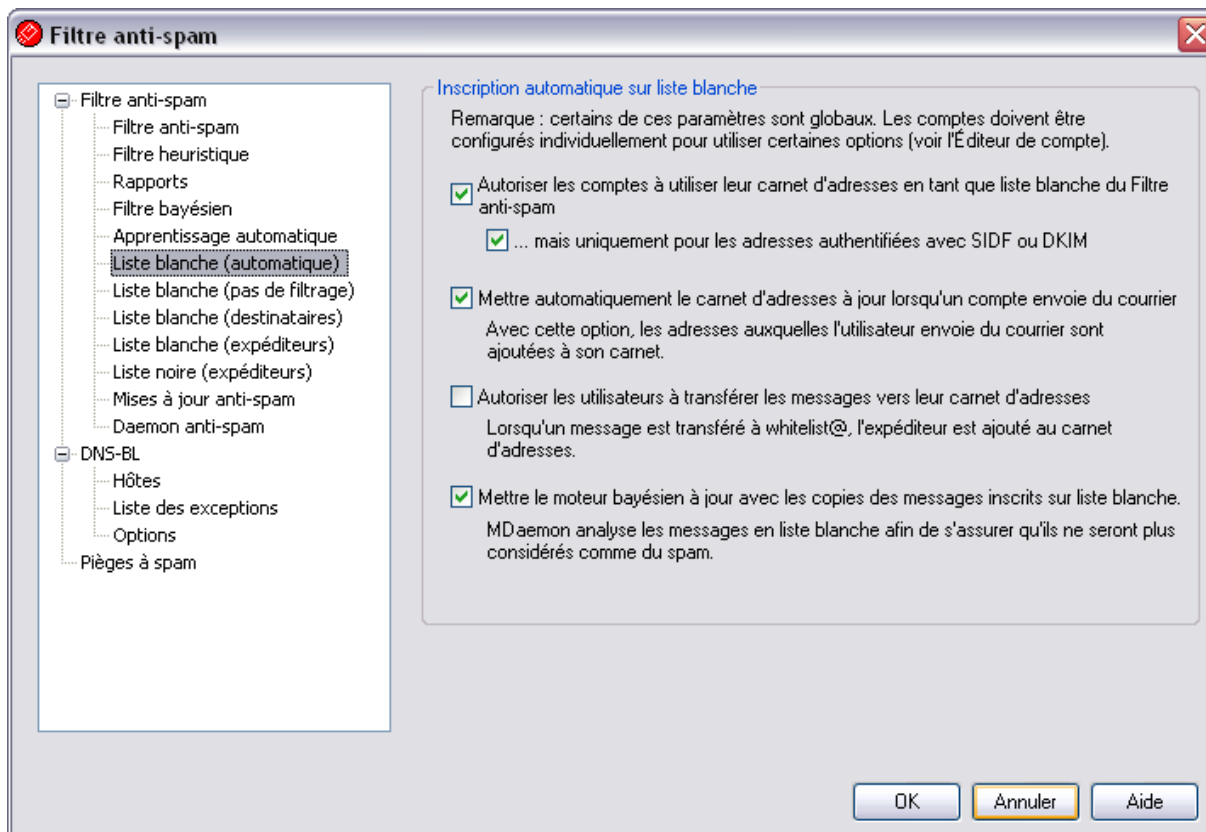
Ainsi lorsqu'un utilisateur de votre domaine envoie un e-mail, il est possible d'ajouter automatiquement l'adresse du destinataire dans son carnet d'adresses, puis de mettre en liste en blanche tous les contacts figurant dans ce carnet.

Cette option ainsi que d'autres paramètres de liste blanche automatique sont accessibles en cliquant sur **Sécurité -> Filtre anti-spam -> Liste blanche (automatique)**.

Distributeur de valeur ajoutée – www.watsoft.com

Watsoft Distribution
3, allée de la Crabette
33600 Pessac FRANCE

Tél +33 (0)5 56 15 75 70
Fax +33 (0)5 56 15 75 71
info@watsoft.com



(Configuration par défaut recommandée.)

3. Listes noires DNS

Les hôtes DNS-BL contiennent des listes d'adresses IP de spammeurs présumés (listes noires). Cet outil vérifie que les adresses IP des serveurs qui se connectent ne se trouvent pas sur l'une de ces listes.

Lorsque le moteur DNS-BL est activé (menu **Sécurité** > **Filtre anti-spam** > **DNS-BL**), l'option **Le serveur SMTP refuse le courrier des IP en liste noire** (onglet **Options**) bloque les messages dont l'expéditeur figure sur une de ces listes.

Attention : une fois le moteur DNS-BL activé, si vous décochez cette option les messages provenant de serveurs sur liste noire sont acceptés mais un en-tête X-RBL-WARNING y est inséré. (Il est ensuite possible de contrôler les messages contenant cet en-tête à l'aide de règles du Filtre de contenu.)

Les options **Vérifier l'IP des en-têtes 'Received' [...]** vérifient les adresses IP contenues dans les en-têtes « Received » des messages reçus.

Hôtes DNS-BL

Cliquez sur l'onglet **Hôtes** pour définir les hôtes auprès desquels MDaemon effectue les vérifications. Il est également possible de renvoyer automatiquement un message à l'expéditeur afin de l'informer que son adresse IP figure sur liste noire.

4. Répulsion

Cet outil (menu **Sécurité > Paramètres de sécurité > Répulsion**) est destiné à « décourager » les spammeurs en ralentissant délibérément les connexions. En effet, contrairement aux serveurs légitimes, les serveurs utilisés pour l'envoi de spam n'assurent pas le suivi des messages et n'attendent pas longtemps la réponse aux commandes HELO/EHLO.

Il suffit donc de retarder cette réponse de dix secondes pour réduire considérablement le nombre de spams reçus.

Vous avez également la possibilité de ralentir les sessions si un hôte envoie un même message à un grand nombre de destinataires à l'aide de l'option : **Seuil de répulsion SMTP RCPT**.

Par exemple, si ce nombre est défini sur 10 et qu'un hôte tente d'envoyer un message à 20 adresses (c'est-à-dire 20 commandes RCPT), MDAemon autorise alors les 10 premières normalement et introduit entre chaque commande qui suit un temps de pause égal au nombre de secondes indiqué dans le champ **Délai de répulsion SMTP RCPT**.

5. Liste grise (MDaemon Pro uniquement)

La liste grise s'appuie sur la même hypothèse que les paramètres de répulsion, afin de décourager les spammeurs. Dans ce cas, une erreur temporaire est envoyée aux expéditeurs de messages provenant d'un domaine inconnu afin qu'ils renouvellent la tentative d'envoi ultérieurement. De plus, toute tentative de distribution de cet expéditeur est également refusée pendant la période définie dans l'option **Retarder les tentatives de distribution (code 451)**...

Attention ! Cette méthode doit être utilisée avec précaution car elle risque d'empêcher la réception de messages légitimes. En effet, il est impossible de savoir à quel moment le serveur renouvellera la tentative d'envoi. Ainsi, un message refusé temporairement par la liste grise peut aussi bien être retardé de quelques minutes que d'une journée entière.

De plus, lorsque le domaine expéditeur possède un pool de serveurs pour l'envoi de courrier, le moteur de la liste grise considère chaque envoi comme une nouvelle connexion, ce qui augmente considérablement le temps d'attente. Afin de résoudre ce problème, une option SPF a été ajoutée à la liste grise. Ainsi, si le domaine expéditeur publie des enregistrements SPF lors du premier envoi, les envois suivants ne seront pas mis en liste grise.

Plus d'informations sur les listes grises sont disponibles (en anglais) à l'adresse :

<http://projects.puremagic.com/greylisting/>.

6. Écran dynamique

Les options contenues dans cet onglet ont pour but de refuser temporairement les messages provenant de serveurs dont le comportement est « suspect ». Par exemple, il est possible de refuser temporairement les connexions d'une adresse IP si le nombre d'erreurs « destinataire inconnu » au cours de la session est trop important. De même, vous pouvez bloquer les IP qui se connectent trop souvent à votre serveur au cours d'une période définie, ainsi que celles dont l'authentification échoue un nombre de fois supérieur à celui indiqué.

Lorsqu'une adresse est bloquée, cette mesure n'est pas permanente : elle s'applique pendant le nombre de minutes choisi. Le bouton **Avancé** ouvre le fichier TARPIT.DAT, contenant la liste des IP bloquées ainsi que la durée appliquée pour chacune d'entre elles. Ce fichier reste en mémoire et peut être modifié en cliquant sur **Avancé** ou en l'ouvrant avec un éditeur de texte.

7. SPF/Sender ID

Ces deux technologies ont pour but de lutter contre un autre méfait lié à l'envoi de spams : l'usurpation d'adresse (ou *spoofing*). En effet, les spammeurs utilisent très fréquemment cette méthode pour envoyer leurs messages.

Principe de fonctionnement

La plupart des domaines publient dans les DNS des enregistrements MX indiquant les serveurs pouvant recevoir les messages qui leur sont destinés. Toutefois, ces enregistrements ne précisent pas quels serveurs peuvent *envoyer* des messages de la part du domaine. Avec SPF les domaines peuvent également publier des enregistrements identifiant les postes autorisés à envoyer des messages. En effectuant une vérification SPF sur les messages entrants, MDAEMON essaie de déterminer si le serveur expéditeur est autorisé à *envoyer* des messages au nom du domaine correspondant, et vérifie que l'adresse utilisée ne soit pas usurpée.

Sender ID est une technologie avancée qui analyse les en-têtes des messages reçus afin d'identifier le PRA (Purported Responsible Address) et ainsi déterminer l'origine du message.

Plus d'informations sur SPF sont disponibles (en anglais) sur le site : www.openspf.org.

8. DomainKeys/DKIM (MDAEMON Pro uniquement)

Ces technologies sont également des méthodes de lutte contre l'usurpation d'adresse.

Principe de fonctionnement

DomainKeys contrôle la validité et l'intégrité des messages grâce à un système de paires de clés publiques et privées. Une clé publique cryptée est publiée dans les données DNS du serveur expéditeur, puis ce serveur attribue à chaque message sortant une signature contenant une clé privée chiffrée correspondante. De même, lorsque le serveur voit qu'un message entrant a été signé, il cherche la clé publique dans les données DNS du serveur expéditeur ; et la compare à la signature DomainKeys du

Distributeur de valeur ajoutée – www.watsoft.com

Watsoft Distribution
3, allée de la Crabette
33600 Pessac FRANCE

Tél +33 (0)5 56 15 75 70
Fax +33 (0)5 56 15 75 71
info@watsoft.com

message. Si les clés ne correspondent pas, cela signifie qu'il s'agit d'une adresse usurpée ou que le message a été altéré. Le message est alors soit rejeté, soit accepté auquel cas son score spam est modifié.

Tout comme SPF et Sender ID, ces deux méthodes reposent en partie sur l'implication des autres administrateurs. En effet, plus le nombre de domaines utilisant ces outils sera important, plus ils seront efficaces.

Plus d'informations sur DomainKeys sont disponibles (en anglais) à l'adresse : <http://antispam.yahoo.com/domainkeys>.

9. Pièges à spam (MDaemon Pro uniquement)

Les pièges à spam (à **ne pas confondre avec le dossier public du même nom**) ne bloquent pas directement la réception de spams, mais ils contribuent à « alimenter » le filtre bayésien, et ainsi améliorer son efficacité.

Pour en savoir plus, cliquez sur le menu **Sécurité > Filtre anti-spam > Pièges à spam**.

10. Protection instantanée (MDaemon Pro uniquement)

Cette fonctionnalité fait partie du module additionnel **SecurityPlus for MDAEMON**. Elle est disponible uniquement avec MDAEMON Pro, à partir de la version 9.5.

Au lieu d'utiliser des outils traditionnels d'analyse de contenu ou basés sur des signatures, ce système s'appuie sur une analyse mathématique de "modèles" associés à l'envoi d'e-mails. Par conséquent, les techniques destinées à tromper les systèmes de protection (ajout de caractères, modifications orthographiques, différences de langue, ou de techniques de codage) n'ont aucun effet sur la détection des attaques. Les nouveaux spams sont ainsi détectés dans les minutes suivant leur création.

Attention, la Protection instantanée n'a pas pour but de remplacer les outils présentés dans ce document : il s'agit simplement d'un niveau de sécurité supplémentaire.

Pour en savoir plus sur la Protection instantanée ou télécharger une version d'évaluation de SecurityPlus, consultez le site : <http://www.watsoft.net/mdaemonav/>.

Distributeur de valeur ajoutée – www.watsoft.com

Watsoft Distribution
3, allée de la Crabette
33600 Pessac FRANCE

Tél +33 (0)5 56 15 75 70
Fax +33 (0)5 56 15 75 71
info@watsoft.com

11. Autres conseils permettant d'éviter le spam

Les spammeurs prennent souvent pour cible les serveurs de messagerie acceptant sans conditions tous les messages destinés à un nom de domaine et leur envoient des centaines de messages adressés à des comptes choisis au hasard.

Il est donc très important de ne pas accepter les messages envoyés à des adresses choisies au hasard sur votre domaine.

Il suffit pour cela d'appliquer quelques mesures simples :

- Essayez autant que possible de recevoir les messages directement sur votre serveur MDAEMON par SMTP plutôt que sur une adresse de collecte chez votre FAI par DomainPOP.
- Évitez d'utiliser des alias universels :
ex. : *@mondomaine.com = ventes@mondomaine.com
- Évitez d'utiliser des serveurs MX secondaires ne pouvant pas déterminer si les messages entrants sont destinés à des utilisateurs valides du domaine local (création automatique de passerelles).