Manuel de SpamPal : Contenu

Contenu > Introduction

SpamPal est un système de classement de courrier qui vise à séparer votre Spam du courrier que vous voulez vraiment lire. En employant SpamPal vous pouvez filtrer le Spam dans un dossier séparé et le supprimer facilement, tout en préservant votre attention pour le reste du courrier!

SpamPal travaille en tant que serveur proxy POP3/IMAP4. En d'autres termes, SpamPal est situé entre votre programme email et le serveur de votre fournisseur d'accès. Quand vous recevez du courrier, SpamPal traite le message que vous recevez, détermine si ces messages sont du spam, les marque alors comme spam, soit en ajoutant **SPAM** à la ligne Sujet:, soit en ajoutant un entête, X-SpamPal: SPAM

Ce traitement est principalement conduit en comparant vos messages à des listes de messages connus, utilisant des listes noires publiques (aussi appelées listes DNSBL) comme par exemple SpamCop

Vous pouvez aussi utiliser des plugins supplémentaires, comme les filtres Bayesian ou RegEx, pour fournir à SpamPal des moyens supplémentaires de déterminer si un message est ou non du spam sans s'appuyer sur les DNSBLs. En utilisant le plugin HTMLModify, vous pouvez retirer de vos messages les erreurs de syntaxe, il renomme aussi les pièces jointes dangereuses (comme .bat,.scr), qui indiquent souvent un virus!

SpamPal utilise très peu de ressources et a une configuration minimale très petite:

- Une machine tournant sous Windows 95, 98, ME, NT, 2000 ou XP (les utilisateurs de Win95 auront besoin de IE 3.0 ou supérieur)
- un compte POP3/IMAP4.
- Un programme email standard comme Outlook Express, Outlook ou Eudora

Note: accès aux comptes email non-standard
Les utilisateurs de Hotmail devraient consulter cette page et consultez les instructions d'utilisation d'un outil (tiers-partie) Hotmail popper, puisque SpamPal ne peut actuellement être utilisé avec MSN (cela pourrait être corrigé dans une version ultérieure)

SpamPal ne peut être utilisé directement avec AOL, mais il peut fonctionner si vous lisez cette page et consultez les instructions d'utilisation d'un outil (tiers-partie) YahooPOPs! pour récupérer votre courrier AOL en utilisant POP3.

Pour voir comment SpamPal se comporte face à d'autres logiciels anti-spam populaires, vous pouvez consulter ce tableau de comparaison.

Comme le Spam est un sujet brûlant dans l'actualité, que ce soit dans les journaux papier ou en ligne, les articles publiés sur SpamPal sont disponibles ici.

Contenu > Guide de démarrage rapide

Index

1. Téléchargez et installez SpamPal

Télécharger SpamPal et lancez l'installation en double-cliquant sur l'icône du programme d'installation de SpamPal (spampal.exe ou spampal-***.exe) et suivez les instructions affichées à l'écran. A la fin de l'installation, SpamPal se lance, montrant son icône (un parapluie rose) dans votre barre de tâches.

Si cette installation est une mise à jour, la configuration existante est conservée et le processus est terminé. Sinon, c'est à dire pour une nouvelle installation, suivez les instructions ci-dessous.

::Début::

2. Démarrer SpamPal

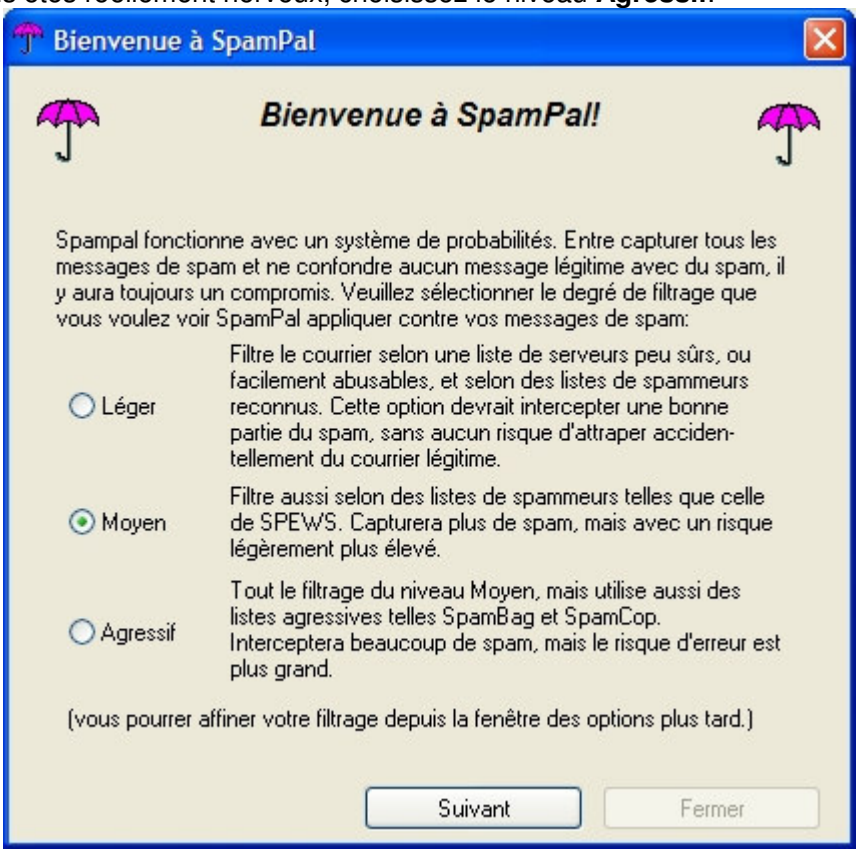
La première fois que SpamPal se lance, vous allez voir l'écran de bienvenue suivant:

Note 1: Ports Standards

Vous pouvez, ici, avoir un message d'erreur disant que SpamPal ne peut écouter le port POP3 standard. Il ne faut pas s'inquiéter; notez juste le numéro de port que SpamPal vous donne et continuez à suivre ce guide.

Ce message signifie que SpamPal utilise le Port **1110** au lieu du **110**. Vous n'avez pas besoin de le lui dire parce que SpamPal sait déjà qu'il utilise le port **1110**. A la place, vous devrez dire à votre programme email (par exemple Outlook Express) d'utiliser le port **1110** au lieu du **110**.

Ensuite, vous devez choisir le niveau de filtrage avec lequel SpamPal va commencer, par défaut, le niveau **Moyen** est choisi, néanmoins, si vous êtes réellement nerveux, choisissez le niveau **Agressif**.



Note 2: Stratégie de filtrage

Le niveau que vous choisissez, peut être modifié ensuite, si le niveau choisi ne filtre pas assez ou filtre trop.

Une fois que SpamPal est installé, il se lance tout seul et vous devriez voir l'icône en forme de parapluie de SpamPal dans la barre des tâches :

::Début::

3. Configuration de votre programme email

Maintenant que vous avez réglé SpamPal, vous devez configurer votre programme email, de telle manière que tous les emails soient reçus au travers du proxy POP3 / IMAP4 de SpamPal, et non directement depuis le serveur POP3 de votre fournisseur d'accès.

Les instructions de réglage générique suivantes peuvent être utilisées pour configurer votre programme email, néanmoins, des **configurations spécifiques** à votre programme email peuvent être trouvées **ici.**

Vous devrez changer les deux réglages suivants dans la configuration de votre programme email (si vous avez plusieurs boite aux lettres POP3 à protéger, répétez cette étape pour chaque compte):

Par exemple, **avant** d'utiliser SpamPal, la configuration de votre programme email est la suivante:

POP Server:	pop3.yourisp.com	**Port:**	110
Utilisateur:	my_login_name		
Mot de passe:	********		

Après, voici les **nouveaux** réglages de votre programme email:

POP Server:	**127.0.0.1**	**Port:**	110
Utilisateur:	my_login_name**@pop3.yourisp.com**		
Mot de passe:	********		

Avant d'utiliser SpamPal	Après configuration pour SpamPal
Exemple 1	
Nom du serveur POP3 entrant: **pop3.yourisp.com**	Nom du serveur POP3 entrant: localhost
Utilisateur: name@surname	Utilisateur:name@surname**@pop3.yourisp.com**
Example 2	
Nom du serveur POP3 entrant: **mail.yourisp.com**	Nom du serveur POP3 entrant: 127.0.0.1
Utilisateur: my_login_name	Utilisateur: my_login_name**@mail.yourisp.com**
Example 3 (using LAN IP Address)	
Nom du serveur POP3 entrant: **192.168.1.1**	Nom du serveur POP3 entrant: 127.0.0.1
Utilisateur: my_login_name	Utilisateur: my_login_name**@192.168.1.1**

Note 1: Noms de serveur

Le "Nom du serveur POP3 entrant", ci-dessus, peut, selon votre programme email aussi être appelé : serveur mail entrant, serveur POP3, Nom d'utilisateur POP3 ou Nom du compte.

Il y a aussi deux façons de préciser le nom du serveur local, qui veulent dire la même chose toutes les deux (mais, avec certains programmes, une seule fonctionne): **localhost** ou **127.0.0.1**

Note 2: Ports Standards

Vous pouvez, ici, avoir un message d'erreur disant que SpamPal ne peut écoute le port POP3 standard. Il ne faut pas s'inquiéter; notez juste le numéro de port que SpamPal vous donne et continuez à suivre ce guide.

Ce message signifie que SpamPal utilise le Port **1110** au lieu du **110**. Vous n'avez pas besoin de le lui dire parce que SpamPal sait déjà qu'il utilise le port **1110**. A la place, vous devrez dire à votre programme email (par exemple Outlook Express) d'utiliser le port **1110** au lieu du **110**.
La manière de configurer votre programme email pour utiliser un port non standard est précisée **ici.**

Maintenant, cliquez sur **Envoyer**/**Recevoir** dans votre programme email, vous devriez voir l'icône de SpamPal dans la barre des tâches s'animer :

Note 3: Programmes Firewall

Votre programme firewall va probablement vous informer que SpamPal.exe essaye d'accéder à internet, ceci est **tout à fait normal** et vous devriez lui dire d'autoriser Spampal à accéder à internet.

SpamPal va aussi, de temps en temps, accéder à sa propre page de démarrage pour vérifier les mises à jour, encore, votre firewall peut vous avertir à ce propos, là encore, vous devriez lui dire d'autoriser Spampal à accéder à internet.

Vous devriez maintenant voir des emails reçus normalement, cependant, si SpamPal pense qu'un message est du spam, alors le sujet commencera par ****SPAM**** et un entête supplémentaire sera ajouté à votre message, **X-SpamPal: SPAM.**

Example: Message Spam

From: i_am_a@spammer.co.uk
To: yourname@yourisp.co.uk
Subject: ****SPAM**** FREE $ FOR YOU !!!
Date: Tue, 24 Jun 2003 13:30:40 +0100
X-SpamPal: SPAM SPCOP xxx.xxx.xxx.xxx

De manière à vous aidez à séparer ce spam de votre courrier normal, vous devriez configurer une règle de message, dans votre programme email, pour déplacer ces messages marqués vers un dossier **spamtrap**.

Pour plus de détails sur la façon de le faire pour votre programme email, cliquez ici.

::Début::

4. Utiliser SpamPal

S'il vous plait, n'utilisez pas de listes noires massives avec SpamPal, en particulier, pas celles de sites à usage général. Celles sont prévues pour détecter le spam dans des systèmes qui n'utilisent pas les listes noires DNS, les expressions régulières ou d'autres méthodes avancées de détection du spam.

Utiliser une liste noire massive n'est généralement pas utile, puisque les spammers créent généralement leur adresse et n'utilisent jamais la même adresse deux fois. Si vous recevez régulièrement du courrier depuis l même adresse et, pour une raison ou une autre, elle n'est pas signalée dans les listes noires publiques, alors il peut être utile de l'ajouter à votre liste noire personnelle.

Cependant, la plupart des utilisateurs n'ont que quelques adresses dans leur liste noire. Si vous en avez de trop, vous ralentirez SpamPal de façon significative, et vous vous ajoutez du travail sans obtenir de résultat significatif.

Ce raisonnement s'applique aussi aux programmes, comme Outlook et Outlook Express qui offrent la possibilité de bloquer les émetteurs par adresse email (appelée Emetteurs bidon/Emetteurs de contenu pour adulte). Il vaut généralement mieux arrêter d'utiliser ces fonctions et laisser SpamPal faire son travail.

Pour vous assurer que vous tirez le maximum de SpamPal, il faut absolument lire lies pages suivantes du manuel:
Comment utiliser SpamPal
Guide détaillée de réglage
Comment configurer SpamPal
Comment optimiser SpamPal
Guide des entêtes
Guide des plugins de SpamPal

Maintenant que vous avez réglé SpamPal, vous devez configurer votre programme email, de telle manière que tous les emails soient reçus au travers du proxy POP3 / IMAP4 de SpamPal, et non directement depuis le serveur POP3 de votre fournisseur d'accès.

Pour plus de détails sur la manière de faire travailler votre programme avec SpamPal, choisissez dans la liste suivante le programme standard email que vous utilisez.

Programmes Standards Email

- Mozilla / Netscape 7 / Thunderbird
- Outlook
- Outlook Express

Cette page donne les étapes à suivre pour installer et régler SpamPal pour une utilisation avec les programmes Mozilla, Netscape (à partir de la version 7) et Thunderbird.

Index rapide

1. Installation de SpamPal

Télécharger SpamPal et lancez l'installation en double-cliquant sur l'icône du programme d'installation de SpamPal (spampal.exe ou spampal-***.exe) et suivez les instructions affichées à l'écran. A la fin de l'installation, SpamPal se lance, montrant son icône (un parapluie rose) dans votre barre de tâches.

Si cette installation est une mise à jour, la configuration existante est conservée et le processus est terminé. Sinon, c'est à dire pour une nouvelle installation, suivez les instructions ci-dessous.

::Début::

2. Configurer SpamPal

Tout ce que vous avez besoin de savoir pour configurer SpamPal peut être trouvé ici.

::Début::

3. Configurer votre programme Email

Maintenant que vous avez réglé SpamPal, vous devez configurer votre programme email, de telle manière que tous les emails soient reçus au travers du proxy POP3 / IMAP4 de SpamPal, et non directement depuis le serveur POP3 de votre fournisseur d'accès.

Vous n'avez besoin de changer que les paramètres que vous utilisez réellement pour récupérer le courrier depuis le serveur mail de votre fournisseur d'accès. Par exemple, si vous n'utilisez que le format POP3 pour lire votre courrier , vous n'avez besoin de modifier que vos réglages POP3.

::Début::

3.1 Changer les réglages POP3

Démarrez votre programme, puis sélectionnez **Comptes courrier et forums** dans le menu **Edition**.

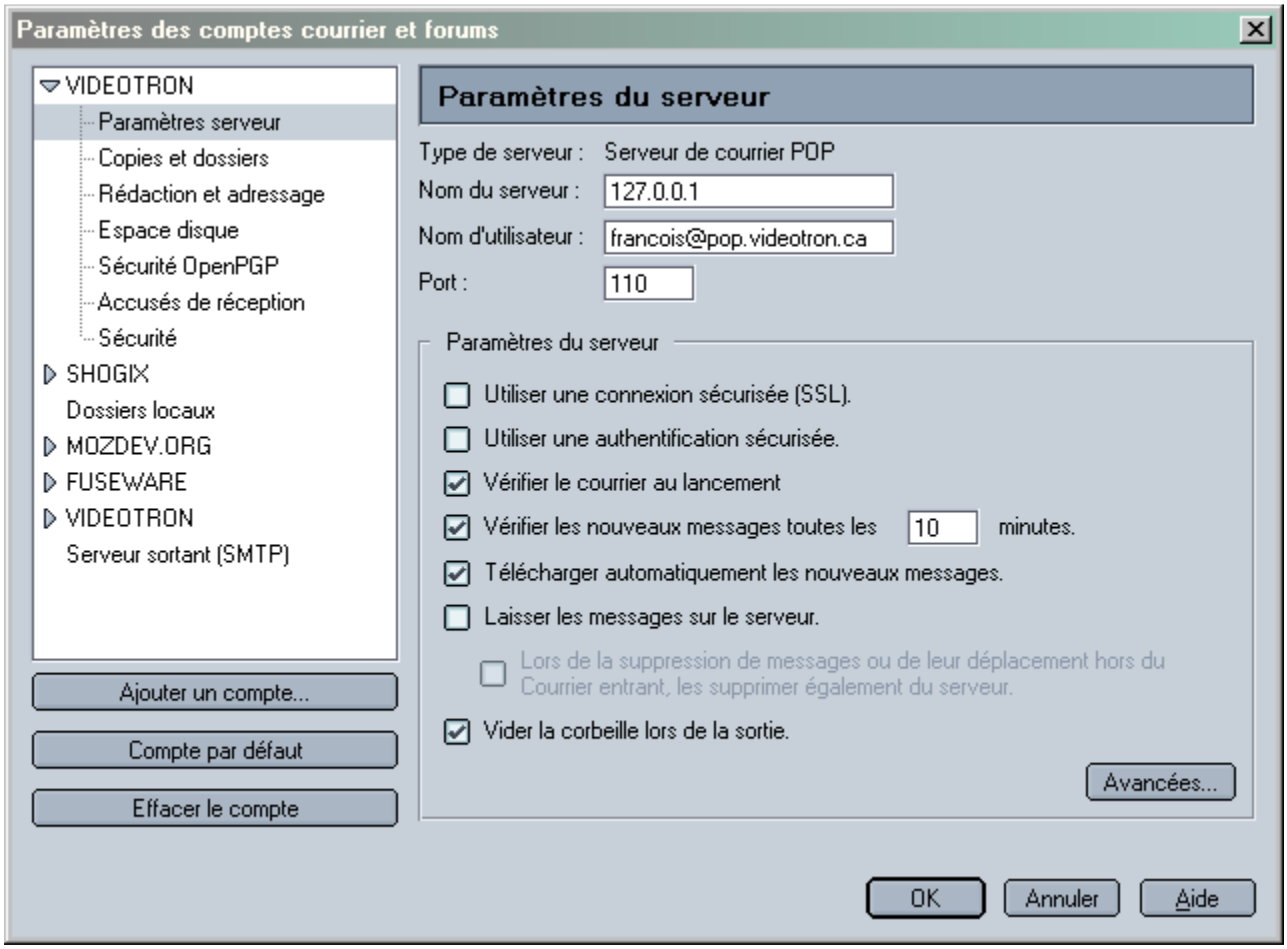
Cliquez sur **Paramètres serveur** sous le premier de vos comptes (la plupart des utilisateurs n'en ont qu'un).

Vous n'avez besoin de modifier que les lignes **Courrier entrant (POP3)** et **Nom du compte**.

Notez le nom du serveur de votre serveur POP (c'est à dire, **pop.videotron.ca**) et remplacez-le par **localhost** ou **127.0.0.1**

Maintenant, ajoutez le symbole @ suivi du nom de votre serveur POP que vous avez noté, à la suite du nom du compte, c'est à dire : nom_utilisateur**@pop.videotron.ca**).

N.B. : le fournisseur d'accès "Vidéotron" n'est utilisé ici que pour l'exemple. Remplacez l'adresse **pop.videotron.ca** par celle indiquée par votre fournisseur d'accès.



Note 1: Si vous avez eu un message d'erreur disant que SpamPal ne peut écouter le port POP3 standard...

Vous pouvez, ici, avoir un message d'erreur disant que SpamPal ne peut écouter le port POP3 standard. Il ne faut pas s'inquiéter; notez juste le numéro de port que SpamPal vous donne et continuez à suivre ce guide.

Ce message signifie que SpamPal utilise le Port **1110** au lieu du **110**. Vous n'avez pas besoin de le lui dire parce que SpamPal sait déjà qu'il utilise le port **1110**. A la place, vous devrez dire à votre programme email (par exemple Outlook Express) d'utiliser le port **1110** au lieu du **110**.

Note 2: Si le nom du serveur est déjà localhost ou 127.0.0.1

Pas de problème, ajoutez simplement @localhost au nom du compte et laissez le nom du serveur intact.

Note 3: Si le nom du compte comporte déjà un @

Vous pouvez continuer sans problème, SpamPal sait gérer les noms de compte qui contiennent 2 @ sans difficulté.

Avant d'utiliser SpamPal	Après la configuration pour SpamPal
Exemple 1	
Courrier entrant (POP3) : **pop3.yourisp.com**	Courrier entrant (POP3) : localhost
Nom du compte : name@surname	Nom du compte :name@surname**@pop3.yourisp.com**
Exemple 2	
Courrier entrant (POP3) : **mail.yourisp.com**	Courrier entrant (POP3) : 127.0.0.1
Nom du compte: my_login_name	Nom du compte: my_login_name**@mail.yourisp.com**
Exemple 3 (utilisant une adresse IP locale)	
Courrier entrant (POP3) : **192.168.1.1**	Courrier entrant (POP3) : 127.0.0.1
Nom du compte: my_login_name	Nom du compte: my_login_name**@192.168.1.1**

Note 4: Nom du serveur

Le "Nom du serveur POP3 entrant", ci-dessus, peut, selon la version aussi être appelé : serveur mail entrant, serveur POP3, Nom d'utilisateur POP3 ou Nom du compte.

Il y a aussi deux façons de préciser le nom du serveur local, qui veulent dire la même chose toutes les deux (mais, avec certains programmes, une seule fonctionne): **localhost** ou **127.0.0.1**

::Début::

3.2 Changer les réglages IMAP4

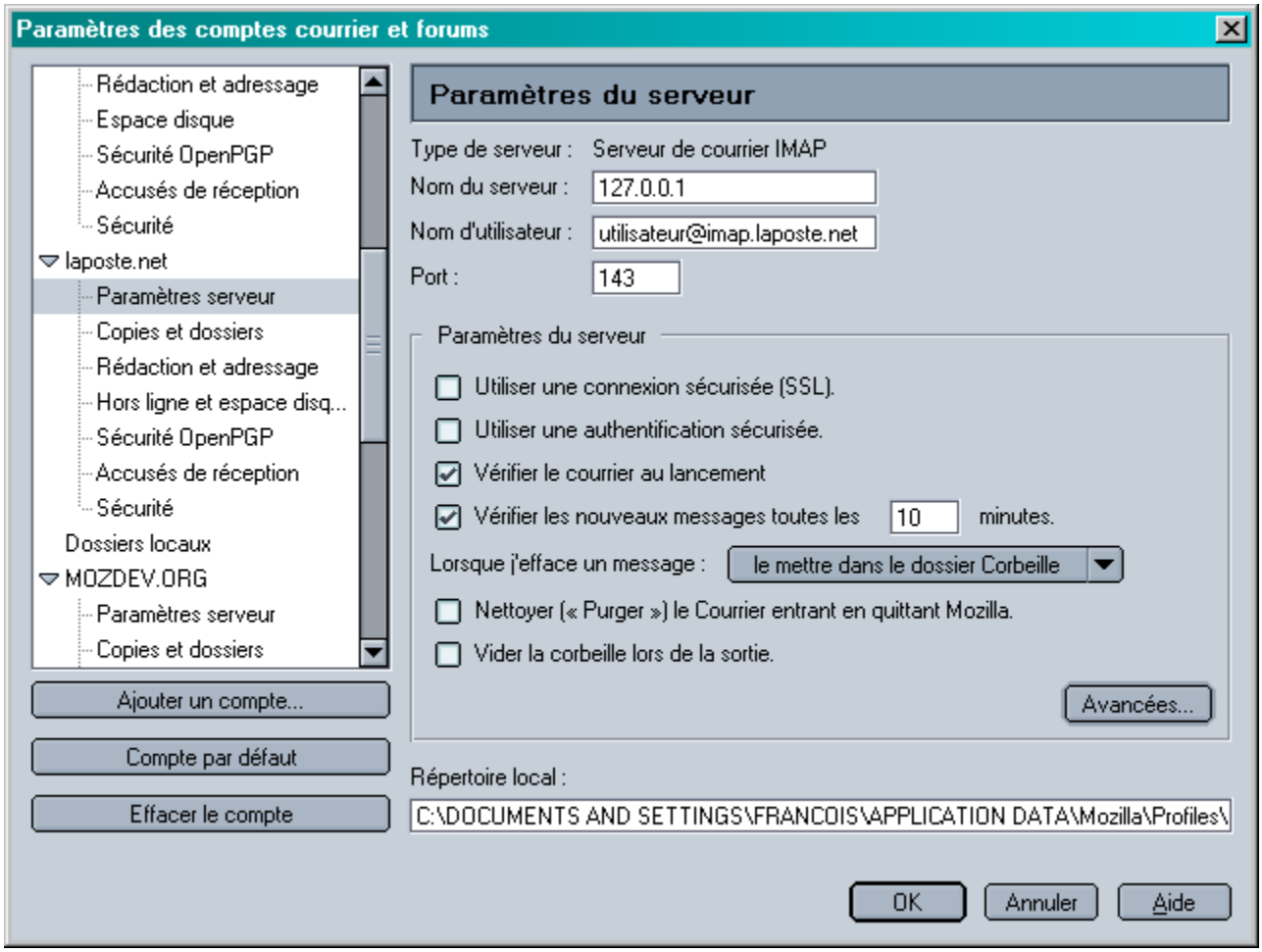
Démarrez votre programme, puis sélectionnez **Comptes courrier et forums** dans le menu **Edition**.

Cliquez sur **Paramètres serveur** sous le premier de vos comptes (la plupart des utilisateurs n'en ont qu'un).

Vous n'avez besoin de modifier que les lignes **Courrier entrant (IMAP)** et **Nom du compte**.

Notez le nom du serveur de votre serveur IMAP (c'est à dire, **imap.yourisp.com**) et remplacez-le par **localhost** ou **127.0.0.1**

Maintenant, ajoutez le symbole @ suivi du nom de votre serveur IMAP que vous avez noté, à la suite du nom du compte, c'est à dire : nom_utilisateur**@imap.yourisp.com**)



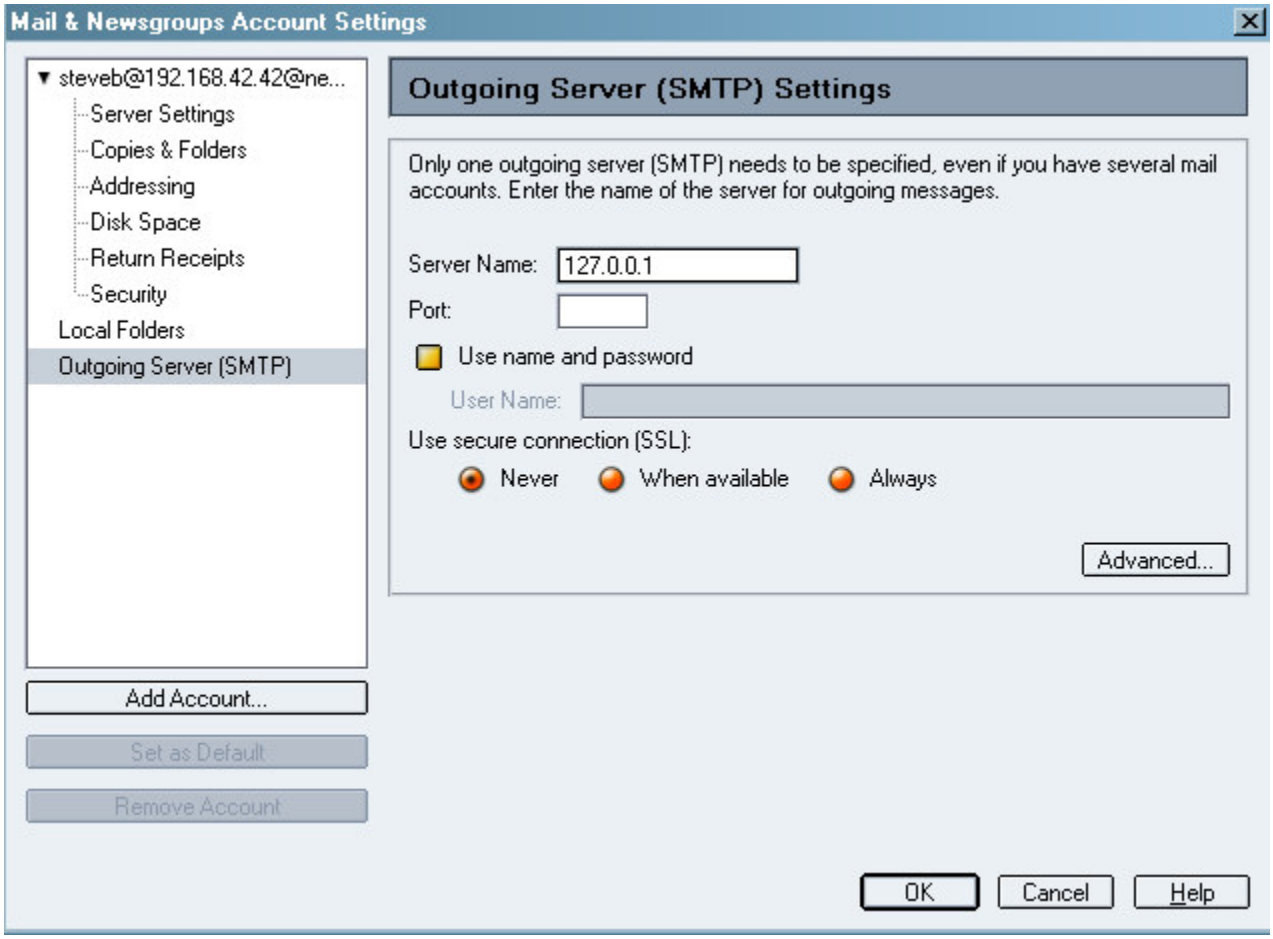
Pour plus de détails sur la manière de modifier les réglages **IMAP** dans SpamPal, consultez la page Configuration du proxy IMAP4 du manuel.

::Début::

3.3 Changer les réglages SMTP

Si vous souhaitez utiliser le proxy SMTP de SpamPal pour ajouter automatiquement à la liste blanche toute adresse email à laquelle vous envoyez un courrier, vous devez changer les réglages SMTP de Outlook, selon les instructions suivantes.
Démarrez votre programme, puis sélectionnez **Comptes courrier et forums** dans le menu **Edition**.

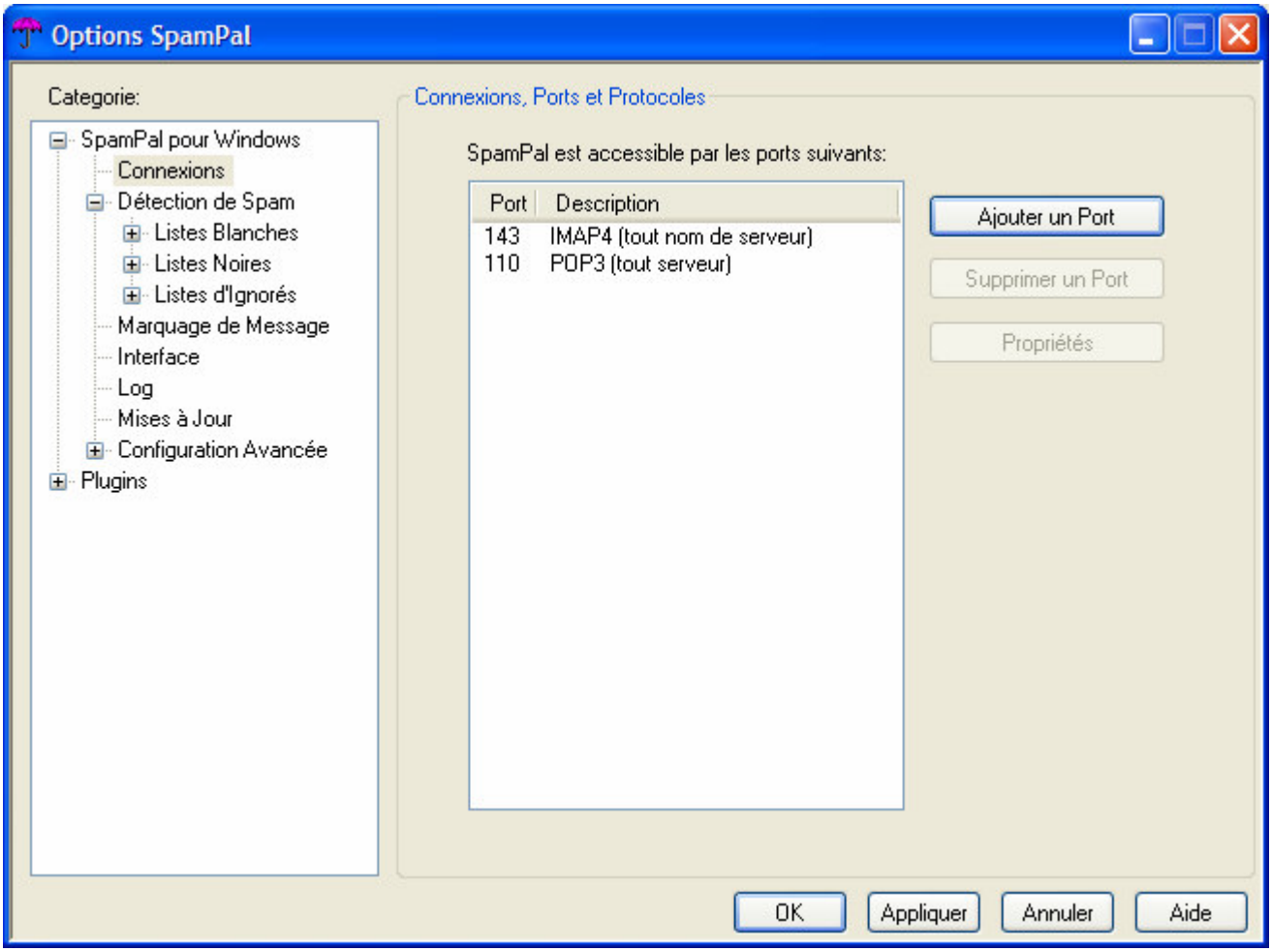
Cliquez sur **Paramètres serveur** sous le premier de vos comptes (la plupart des utilisateurs n'en ont qu'un).



Maintenant, notez l'adresse de votre **Serveur de courrier sortant (SMTP)**, par exemple : **smtp.myisp.com**

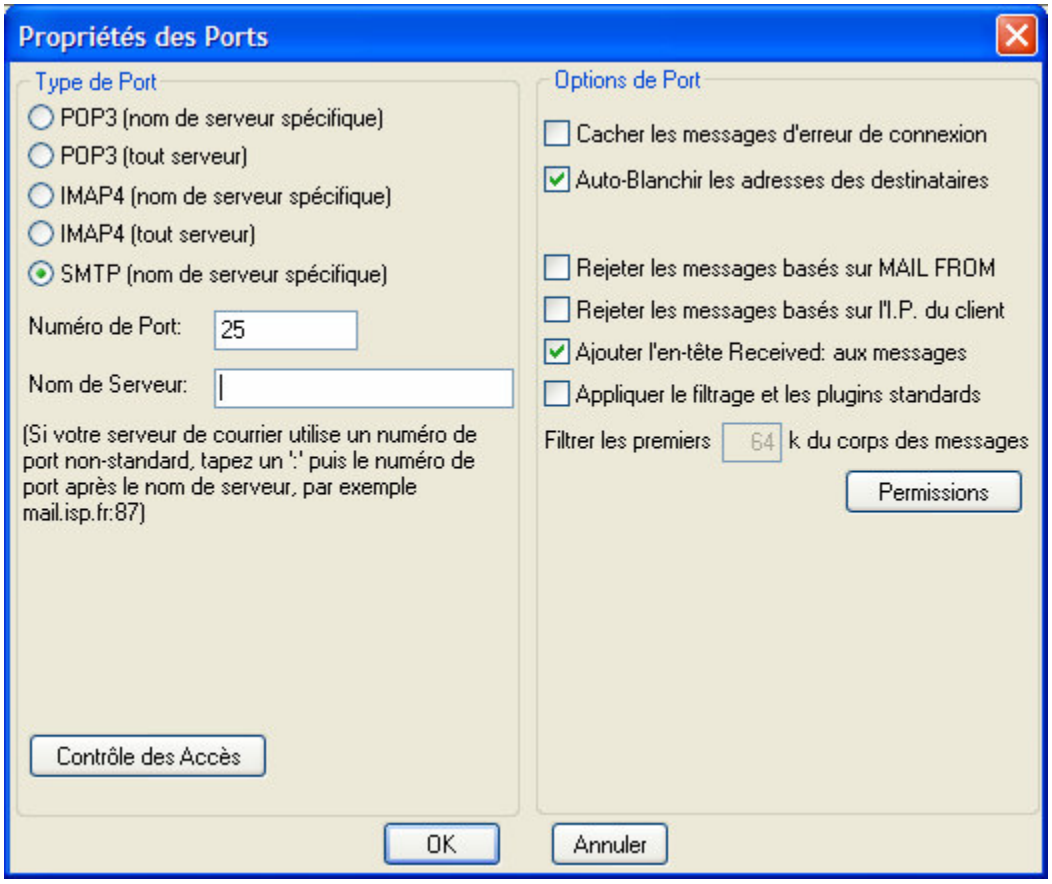
Remplacez cette valeur par : **127.0.0.1**

Allez maintenant à la page **Connections** de SpamPal :



Cliquez sur **Ajouter un port** et changer le type de Port pour **SMTP.**

Changer le **Nom de serveur** pour le **Serveur de courrier sortant (SMTP)** que vous avez noté plus tôt, **smtp.myisp.com**



Maintenant, dès que vous envoyez un email, SpamPal va automatiquement ajouter l'adresse du ou des destinataires à la liste blanche.

Note: Option "Exclusions" de la liste blanche

De temps en temps, un spammer peut utiliser l'adresse de quelqu'un qui est dans votre liste blanche automatique - un collègue ou une autre de vos adresses email, par exemple. D'un coté, vous ne voulez pas ajouter l'adresse de cette personne dans la liste noire parce qu'elle vous envoie beaucoup d'emails légitimes, d'un autre coté, vous ne voulez pas qu'elles finissent dans la liste blanche automatique et court cuitent les protections anti-spam de SpamPal.

En cliquant sur le panneau **Exclusions**, une fenêtre va apparaître et vous permettre de saisir les adresses de personnes qui ne doivent jamais être ajouter à la liste blanche automatique. Ajouter vos collègues, vos propres adresses, et vous n'aurez plus à vous inquiéter des spammers utilisant ces adresses pour contourner le filtrage de SpamPal. Vous pouvez même ajouter des domaines entiers - *@acme-widgets.com

::Début::

3.4 Créer des filtres ou des règles de messages

Si vous utilisez un serveur **IMAP4**, vous n'avez pas besoin de mettre en place de règle ou de filtre, puisque SpamPal déplace tout message marqué "spam" dans un dossier **inbox.spamtrap** sur votre serveur.

Si vous utilisez un serveur **POP3** et voulez que Outlook Express filtre automatiquement les messages marqués dans une boîte de réception séparée, afin que vous puissiez plus facilement les passer en revue, suivez les étapes suivantes.

Sélectionnez les **Filtres de messages** dans le menu **Outils**. Cliquez sur **Nouveau** pour en créer un et appelez-le SpamPal.

Dans la liste des entêtes (qui affiche par défaut **Sujet**), choisissez **Personnaliser**. Tapez `X-SpamPal` dans le dialogue qui apparaît puis cliquez sur **Ajouter**, pour l'ajouter à la liste.

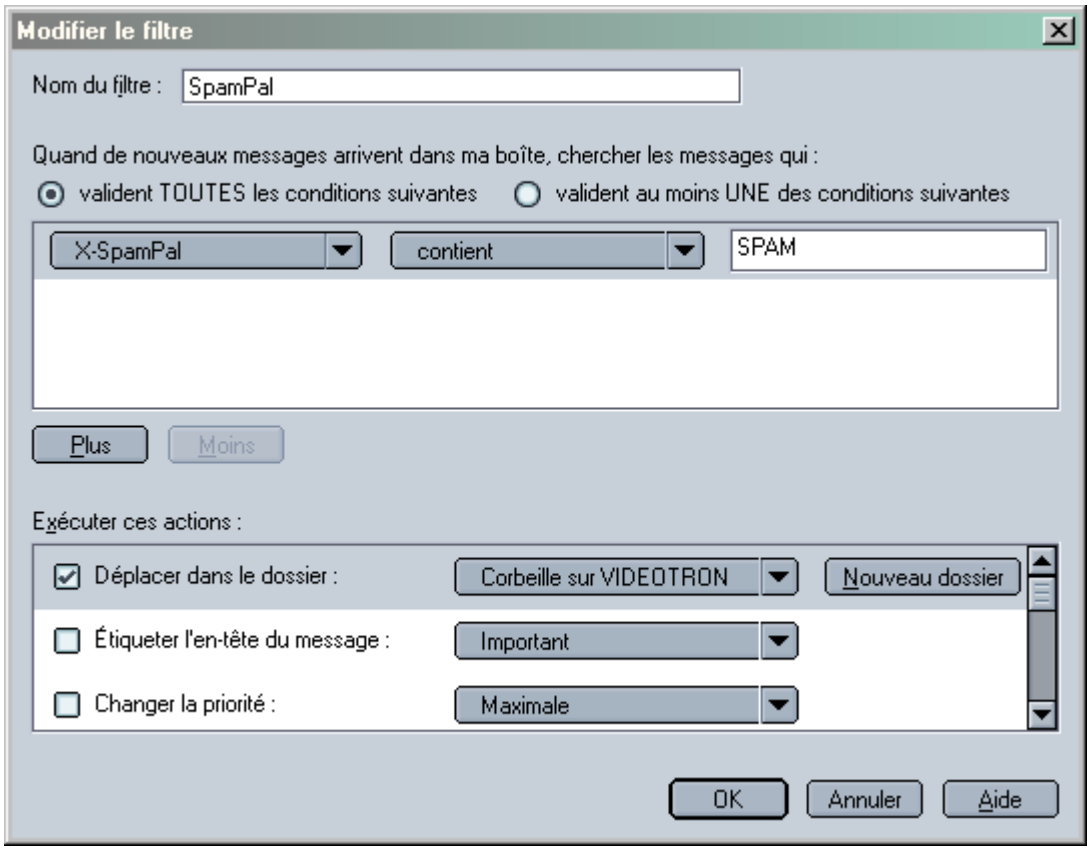
Cliquez sur **OK** pour fermer la fenêtre puis sélectionnez **X-SpamPal** dans la liste des entêtes. Laissez la boite suivante sur **contient** et entrez **SPAM** dans la boite la plus à droite.

Maintenant remplacez l'action par **déplacer vers le dossier** et cliquez sur **Nouveau dossier**. Appelez le dossier **Spam Trap** (ou un autre nom) et placez le où vous voulez.

Cliquez sur **OK** pour créer le dossier, puis de nouveau pour créer la règle, et enfin pour sauvegarder vos changements de filtres (donc, 3 fois **Ok**).

Si vous avez plusieurs comptes, vous devrez créer une règle selon la même méthode pour chacun d'entre eux.

Votre filtre devrait ressembler à quelque chose comme ça :



::Début::

4. Programmes anti-Virus & Firewalls

Des instructions spécifiques pour utiliser une variété de programmes anti-virus avec SpamPal peuvent être trouvées sur la page d'installation principale

Quelques filtres anti-virus ont besoin de se situer entre votre programme email et votre serveur de mail, juste là où se trouve SpamPal. Il n'y a en fait aucune raison qu'ils ne le puissent pas; vous devez juste les mettre en série afin qu'ils puissent récupérer le courrier au travers de SpamPal au lieu de directement, puis votre programme email récupère le courrier à travers le filtre anti-virus.

::Début::

5. Mettre vos amis et contacts en liste blanche

Afin d'accélérer le traitement de vos emails et d'éviter que SpamPal marque les emails de vos amis ou contacts comme spam, c'est une bonne idée à ce point de l'installation de mettre en liste blanche l'adresse de tous vos contacts

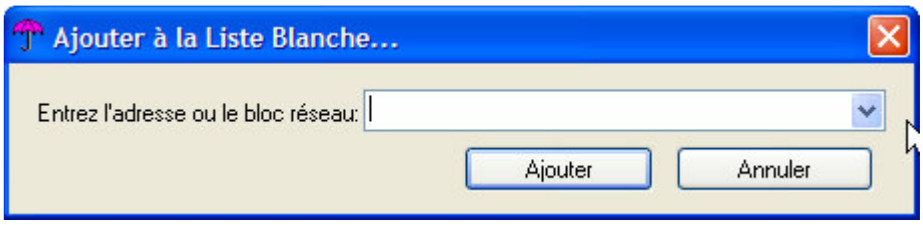
importants.

Pour cela, il y a quatre manières de faire :

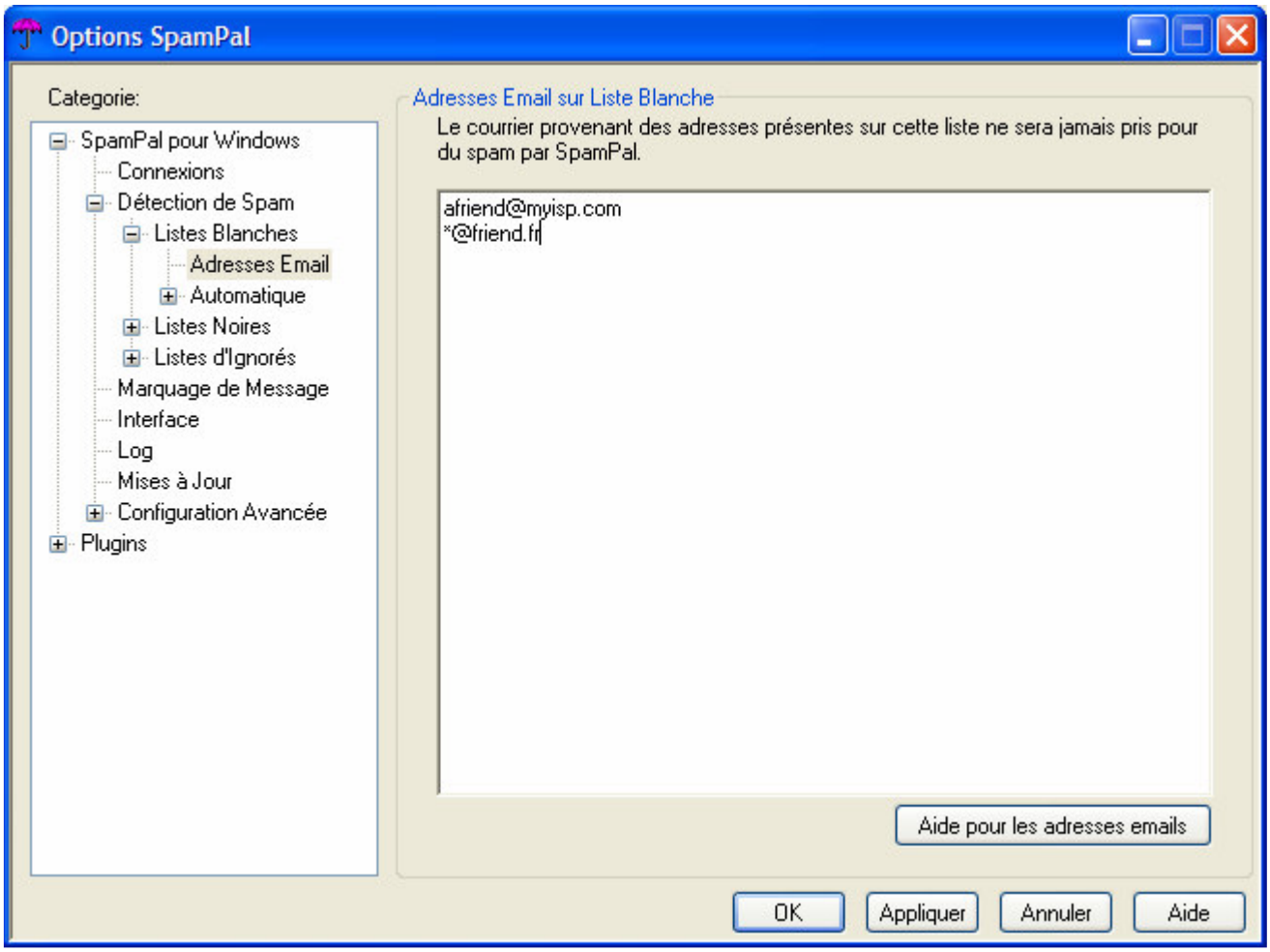
a) Utiliser la liste blanche automatique **pop3** : cela va ajouter à la liste blanche les adresses dont vous recevez fréquemment du courrier non-spam,
b) Utiliser la liste blanche automatique **smtp** : si configurée en **3.3**, elle ajoute à la liste blanche les adresses auxquelles vous envoyez du courrier,

> **Note 1:** Vie privée : liste blanche automatique smtp
>
> Si vous utilisez cette possibilité, spécialement dans un bureau, comme cela va enregistrer toutes les adresses de messages sortants, cela pourrait constituer une atteinte à la vie privée (au Royaume-Uni, vous devez prévenir une personne si vous placez son adresse dans un fichier), ou la constitution d'un fichier (soumis à la loi française "Informatique et libertés").

c) utiliser le menu **Ajouter à la liste blanche** sur l'icône de SpamPal dans la barre des tâches: pour ajouter manuellement à la liste blanche, vous pouvez la taper manuellement, ou la copier :



d) Vous pouvez utiliser la page des **adresses email en liste blanche** de SpamPal, pour ajouter manuellement vos adresses email :



Note 2: Entêtes auxquels la liste blanche est comparée

La fonction liste blanche ne regarde que dans certains entêtes de vos emails.

Actuellement, ce sont : **From:**, **Reply-To:**, **Sender:, Mailing-List:** et **Return-Path**:

Au départ, vous remarquerez que l'utilisation de SpamPal rend la récupération du courrier un peu plus longue. C'est parce que SpamPal doit vérifier la présence de chaque adresse dans chaque liste DNSBL (liste noires publiques) pour voir quels emails viennent d'un spammer.

Néanmoins, grâce à sa fonction liste blanche automatique, SpamPal va rapidement apprendre qui vous envoie beaucoup de messages, et va les ajouter à une liste des émetteurs de confiance. Parce qu'ils sont de confiance, SpamPal ne perd pas de temps à les vérifier dans les listes DNSBL. Pour ceux-là, plus vous utilisez SpamPal, plus il deviendra rapide.

Vous pouvez trouver d'autres trucs et astuces pour optimiser SpamPal ici.

Ceci termine l'installation et la configuration de SpamPal.

::Début::

Cette page donne les étapes à suivre pour installer et régler SpamPal pour une utilisation avec le programme Outlook Express.

Index rapide

1. Installation de SpamPal

Télécharger SpamPal et lancez l'installation en double-cliquant sur l'icône du programme d'installation de SpamPal (spampal.exe ou spampal-***.exe) et suivez les instructions affichées à l'écran. A la fin de l'installation, SpamPal se lance, montrant son icône (un parapluie rose) dans votre barre de tâches.

Si cette installation est une mise à jour, la configuration existante est conservée et le processus est terminé. Sinon, c'est à dire pour une nouvelle installation, suivez les instructions ci-dessous.

::Début::

2. Configurer SpamPal

Tout ce que vous avez besoin de savoir pour configurer SpamPal peut être trouvé ici.

::Top::

3. Configurer votre programme Email

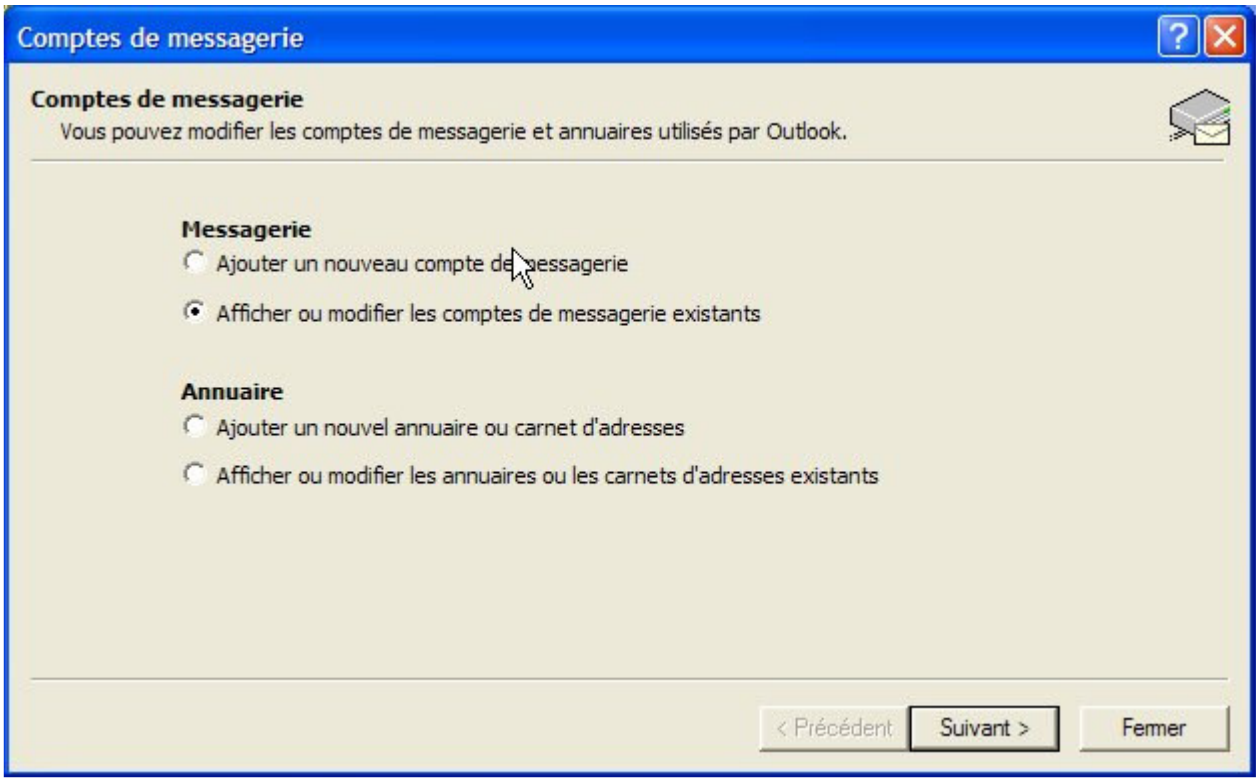
Maintenant que vous avez réglé SpamPal, vous devez configurer votre programme email, de telle manière que tous les emails soient reçus au travers du proxy POP3 / IMAP4 de SpamPal, et non directement depuis le serveur POP3 de votre fournisseur d'accès.

Vous n'avez besoin de changer que les paramètres que vous utilisez réellement pour récupérer le courrier depuis le serveur mail de votre fournisseur d'accès. Par exemple, si vous n'utilisez que le format POP3 pour lire votre courrier , vous n'avez besoin de modifier que vos réglages POP3.

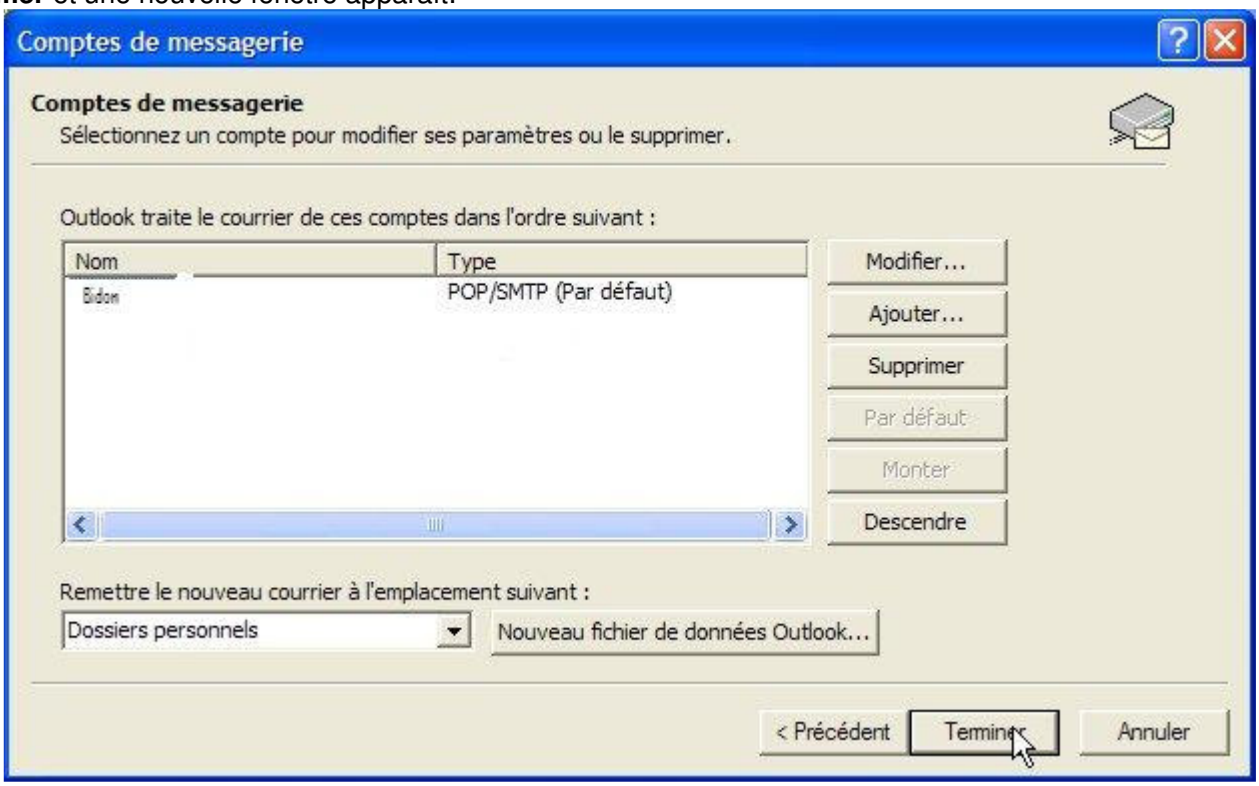
::Début::

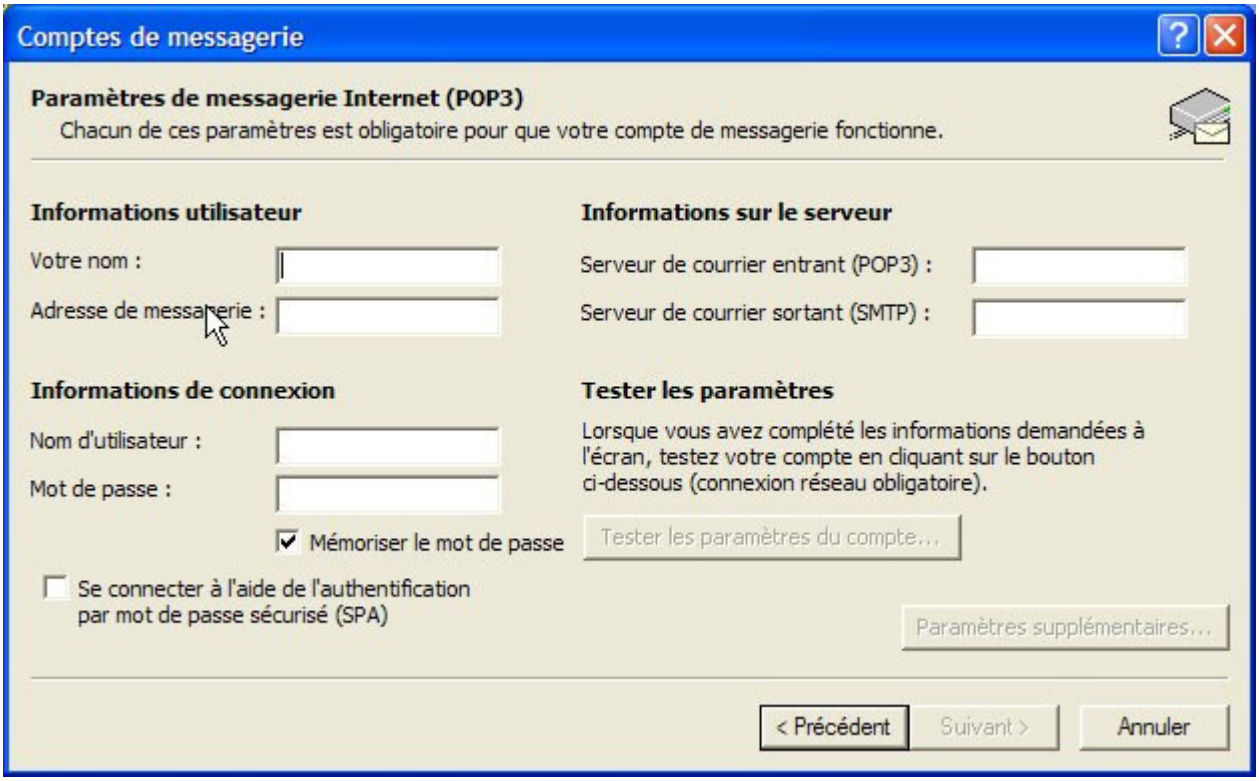
3.1 Changer les réglages POP3

Démarrez Outlook, puis choisissez **Comptes de messagerie** dans le menu **Outils**, vous devriez vous cette fenêtre :



Nous allons commencer par le premier compte (la plupart des internautes n'en ont qu'un). Sélectionnez-le et cliquez sur **Modifier** et une nouvelle fenêtre apparaît:





Vous n'avez besoin de modifier que les lignes **Courrier entrant (POP3)** et **Nom du compte**.

Notez le nom du serveur de votre serveur POP (c'est à dire, **pop3.serveur.com**) et remplacez-le par **localhost** ou **127.0.0.1**

Maintenant, ajoutez le symbole @ suivi du nom de votre serveur POP que vous avez noté, à la suite du nom du compte, c'est à dire : nom_utilisateur**@pop3.serveur.com**)

Note 1: Si vous avez eu un message d'erreur disant que SpamPal ne peut écouter le port POP3 standard...

Vous pouvez, ici, avoir un message d'erreur disant que SpamPal ne peut écouter le port POP3 standard. Il ne faut pas s'inquiéter; notez juste le numéro de port que SpamPal vous donne et continuez à suivre ce guide.

Ce message signifie que SpamPal utilise le Port **1110** au lieu du **110**. Vous n'avez pas besoin de le lui dire parce que SpamPal sait déjà qu'il utilise le port **1110**. A la place, vous devrez dire à votre programme email (par exemple Outlook Express) d'utiliser le port **1110** au lieu du **110**.

Note 2: Si le nom du serveur est déjà localhost ou 127.0.0.1

Pas de problème, ajoutez simplement @localhost au nom du compte et laissez le nom du serveur intact.

Note 3: Si le nom du compte comporte déjà un @

Vous pouvez continuer sans problème, SpamPal sait gérer les noms de compte qui contiennent 2 @ sans difficulté.

Avant d'utiliser SpamPal	Après la configuration pour SpamPal
Exemple 1	
Courrier entrant (POP3) : **pop3.yourisp.com**	Courrier entrant (POP3) : localhost
Nom du compte : name@surname	Nom du compte :name@surname**@pop3.yourisp.com**
Exemple 2	

Courrier entrant (POP3) : **mail.yourisp.com**	Courrier entrant (POP3) : 127.0.0.1
Nom du compte: my_login_name	Nom du compte: my_login_name**@mail.yourisp.com**
Exemple 3 (utilisant une adresse IP locale)	
Courrier entrant (POP3) : **192.168.1.1**	Courrier entrant (POP3) : 127.0.0.1
Nom du compte: my_login_name	Nom du compte: my_login_name**@192.168.1.1**

Note 4: Nom du serveur

Le "Nom du serveur POP3 entrant", ci-dessus, peut, selon votre programme email aussi être appelé : serveur mail entrant, serveur POP3, Nom d'utilisateur POP3 ou Nom du compte.

Il y a aussi deux façons de préciser le nom du serveur local, qui veulent dire la même chose toutes les deux (mais, avec certains programmes, une seule fonctionne): **localhost** ou **127.0.0.1**

Cliquez maintenant sur **OK** pour confirmer la modification, et répétez ceci pour chaque compte que vous souhaitez protéger. Lorsque vous avez fini, fermer la fenêtre "Comptes".

Maintenant, essayez de récupérer votre courrier; si vous n'avez pas d'erreurs, continuez avec l'étape suivante. Il peut vous être demandé de ressaisir vos mots de passe POP3; rien d'inquiétant. Si vous obtenez une erreur d'Outlook Express, vérifiez que vous avez correctement configuré le Nom du serveur POP3 entrant à **localhost** et, si nécessaire, que le port a été modifié avec la bonne valeur. Si vous obtenez une erreur de SpamPal, vérifiez que vous avez bien ajouté le nom du serveur au nom du compte, et que la connexion a Internet est active.

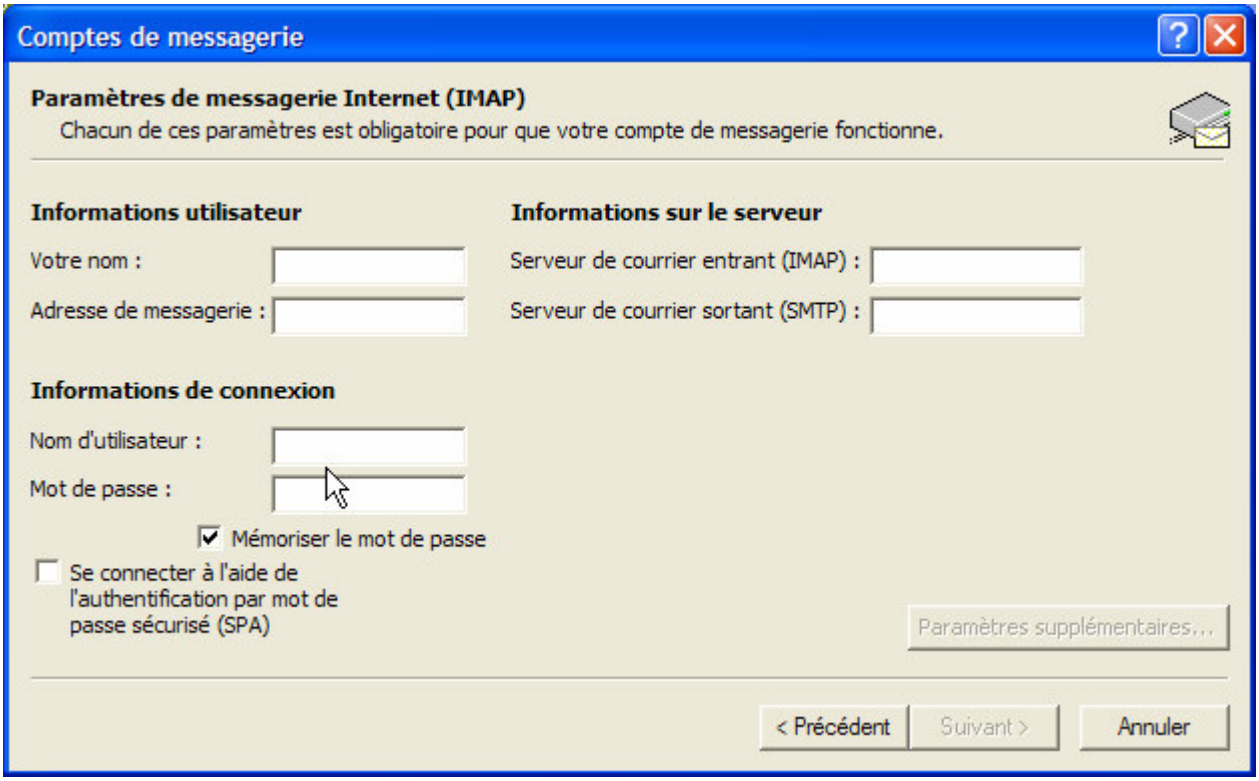
::Top::

3.2 Changer les réglages IMAP4

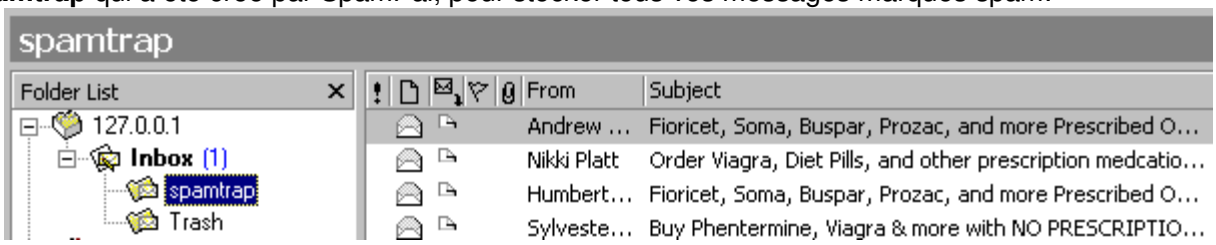
Vous n'avez besoin de modifier que les lignes **Courrier entrant (IMAP)** et **Nom du compte**.

Notez le nom du serveur de votre serveur IMAP (c'est à dire, **imap.yourisp.com**) et remplacez-le par **localhost** ou **127.0.0.1**

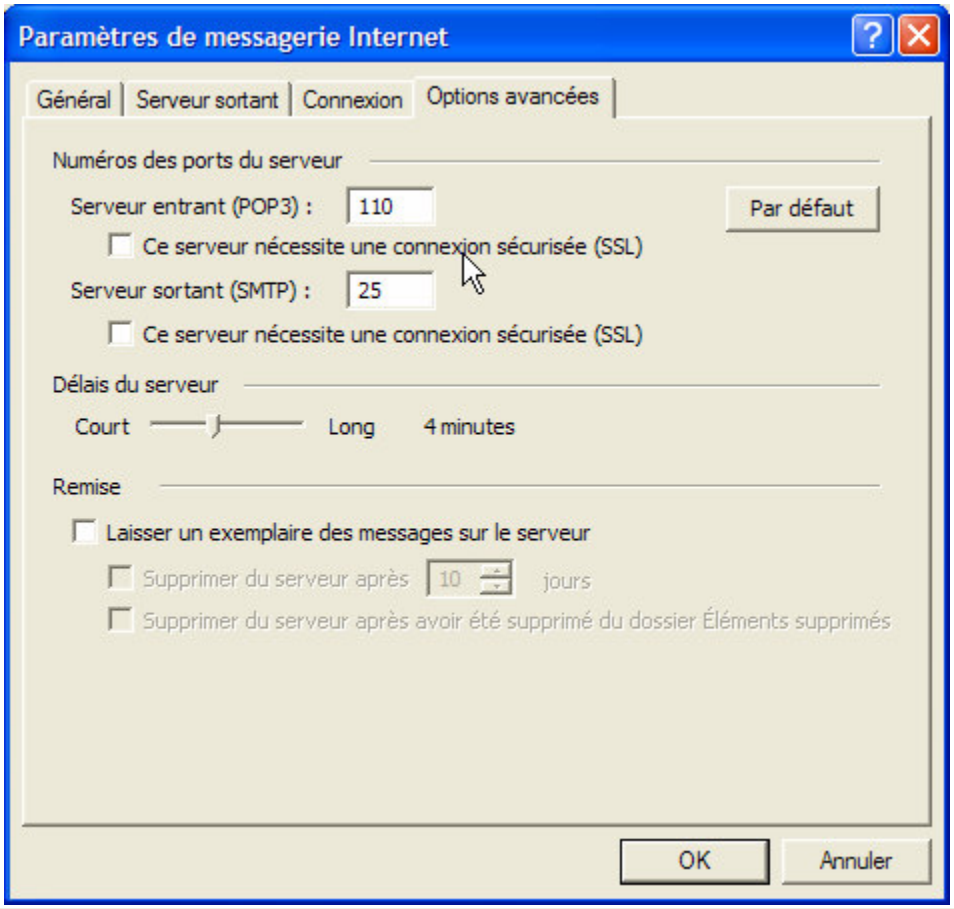
Maintenant, ajoutez le symbole @ suivi du nom de votre serveur IMAP que vous avez noté, à la suite du nom du compte, c'est à dire : nom_utilisateur**@imap.yourisp.com**) Démarrez Outlook puis appelez la liste des comptes email, démarrez par le premier (la plupart des internautes n'en ont qu'un). Sélectionnez-le dans la liste et cliquez sur **Modifier...**



Vous devriez maintenant pouvoir vérifier vos emails; vous devriez remarquer que vous avez un nouveau dossier appelé **spamtrap** qui a été créé par SpamPal, pour stocker tous vos messages marqués spam:



Si vous avez besoin de changer les ports **POP3**, **SMTP** ou **IMAP**, commencez par le premier compte (la plupart des internautes n'en ont qu'un). Sélectionnez-le puis cliquez sur **Propriétés**. Allez dans l'onglet **Avancé**, qui devrait ressembler à ceci :



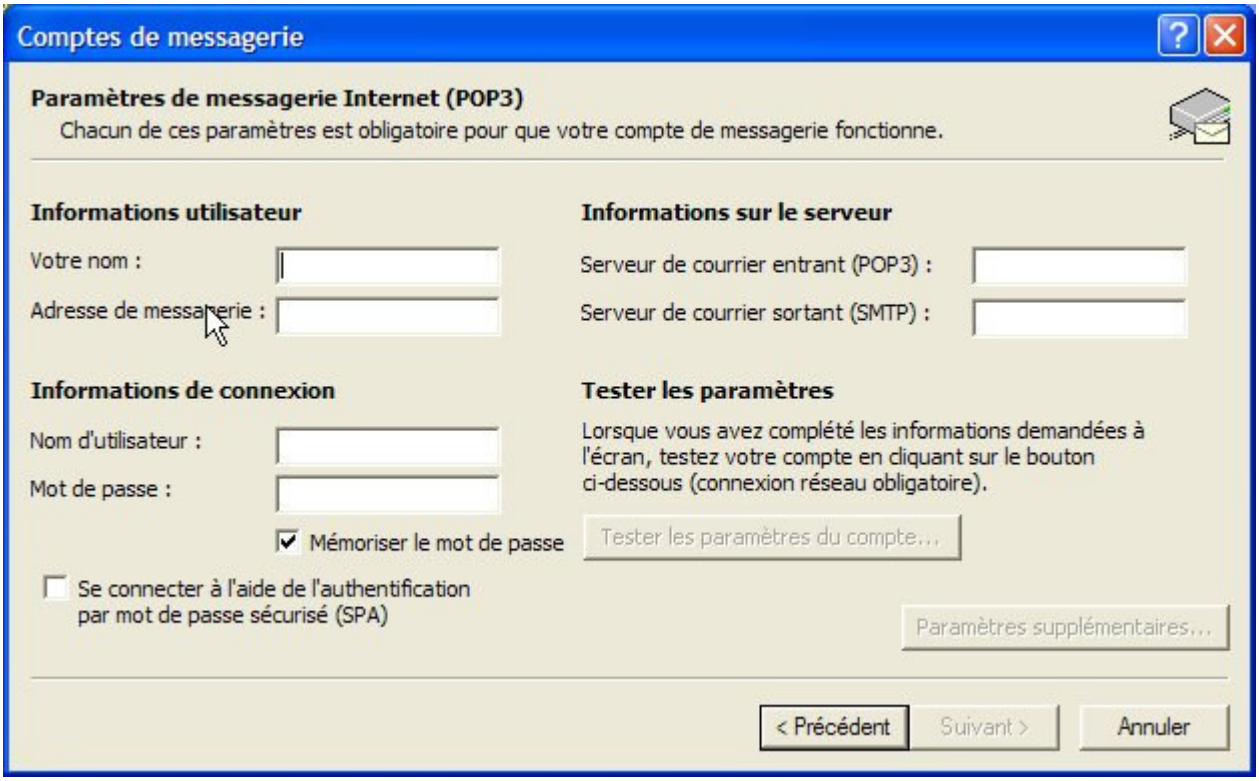
Note: Délais d'expiration du serveur

Le **Délai d'expiration du serveur** par défaut de 1 minute peut être un peu juste pour une utilisation avec SpamPal. Si vous trouvez que le serveur n'a pas le temps de répondre alors, peut-être, vous pourriez augmenter cette valeur à **4 minutes**.

::Début::

3.3 Changer les réglages SMTP

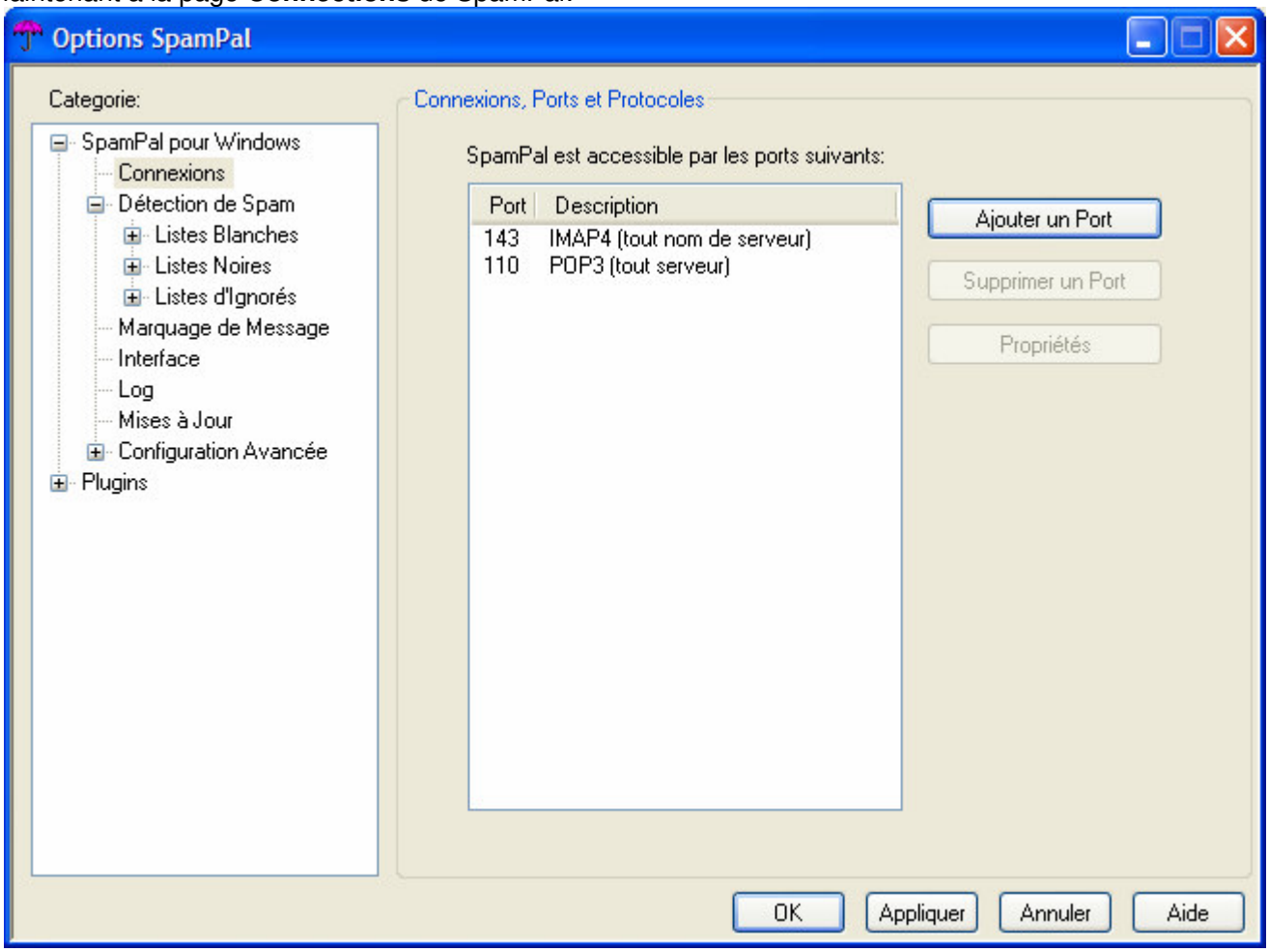
Si vous souhaitez utiliser le proxy SMTP de SpamPal pour ajouter automatiquement à la liste blanche toute adresse email à laquelle vous envoyez un courrier, vous devez changer les réglages SMTP de Outlook, selon les instructions suivantes.



Maintenant, notez l'adresse de votre **Serveur de courrier sortant (SMTP)**, par exemple : **smtp.myisp.co.uk**

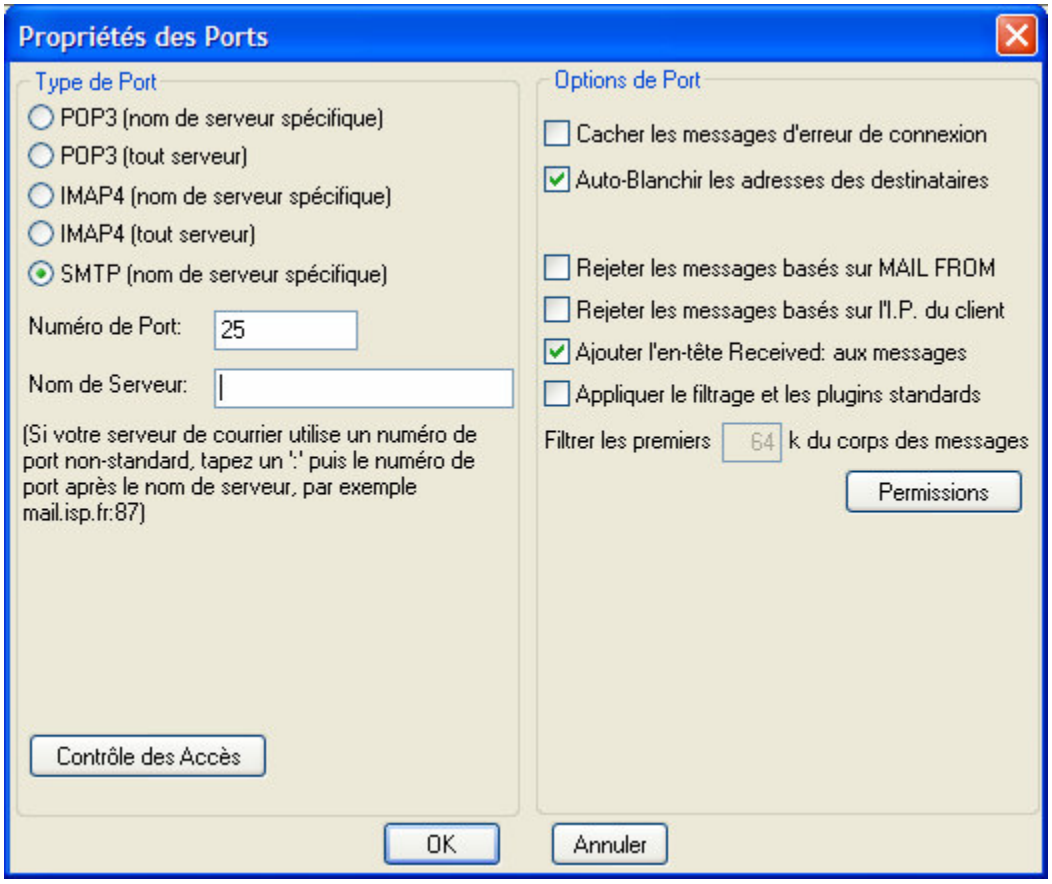
Remplacez cette valeur par : **127.0.0.1**

Allez maintenant à la page **Connections** de SpamPal:



Cliquez sur **Ajouter un port** et changer le type de Port pour **SMTP.**

Changer le **Nom de serveur** pour le **Serveur de courrier sortant (SMTP)** que vous avez noté plus tôt, **smtp.myisp.co.uk**



Maintenant, dès que vous envoyez un email, SpamPal va automatiquement ajouter l'adresse du ou des destinataires à la liste blanche.

Note: Option "Exclusions" de la liste blanche

De temps en temps, un spammer peut utiliser l'adresse de quelqu'un qui est dans votre liste blanche automatique - un collègue ou une autre de vos adresses email, par exemple. D'un coté, vous ne voulez pas ajouter l'adresse de cette personne dans la liste noire parce qu'elle vous envoie beaucoup d'emails légitimes, d'un autre coté, vous ne voulez pas qu'elles finissent dans la liste blanche automatique et court-cuitent les protections anti-spam de SpamPal.

En cliquant sur le panneau **Exclusions**, une fenêtre va apparaître et vous permettre de saisir les adresses de personnes qui ne doivent jamais être ajouter à la liste blanche automatique. Ajouter vos collègues, vos propres adresses, et vous n'aurez plus à vous inquiéter des spammers utilisant ces adresses pour contourner le filtrage de SpamPal. Vous pouvez même ajouter des domaines entiers - *@acme-widgets.com

::Début::

3.4 Créer des filtres ou des règles de messages

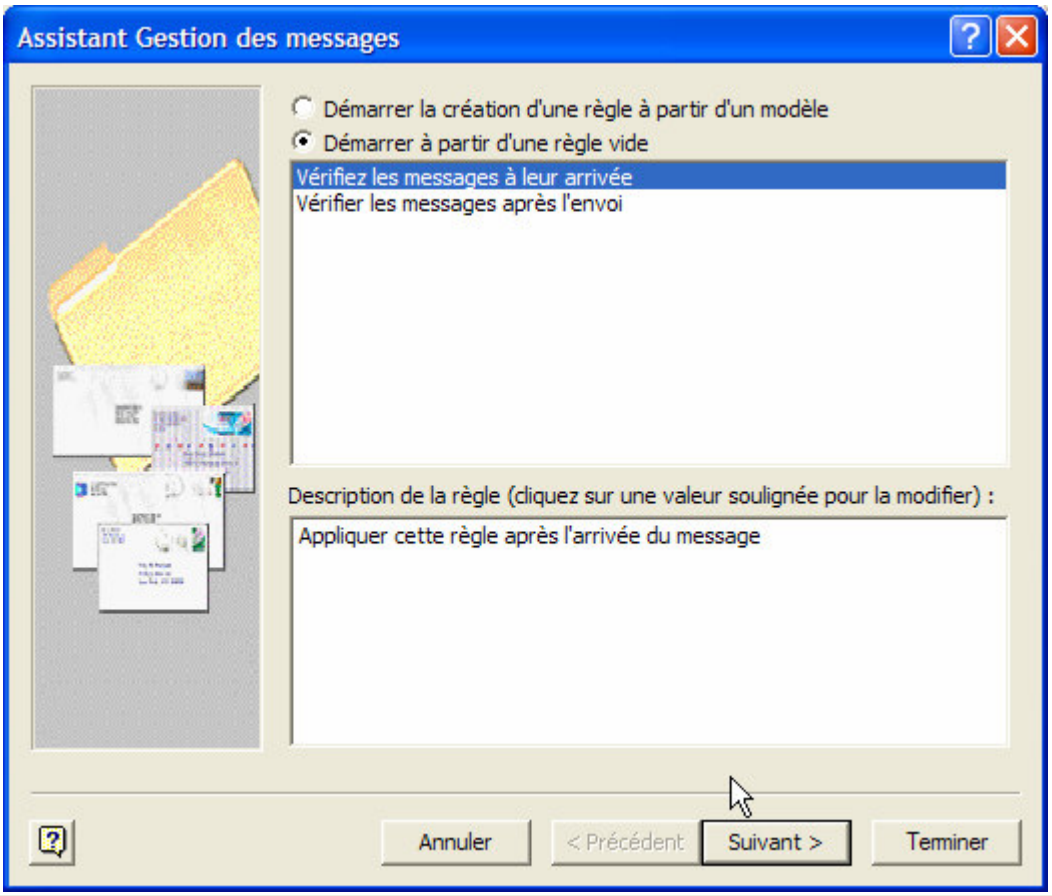
Si vous utilisez un serveur **IMAP4**, vous n'avez pas besoin de mettre en place de règle ou de filtre, puisque SpamPal déplace tout message marqué "spam" dans un dossier **inbox.spamtrap** sur votre serveur.

Si vous utilisez un serveur **POP3** et voulez que Outlook Express filtre automatiquement les messages marqués dans une boîte de réception séparée, afin que vous puissiez plus facilement les passer en revue, suivez les étapes suivantes.

Ouvrez l'**assistant Gestion des messages** dans le menu **Outils**, cela va ouvrir une fenêtre contenant la liste de tous les filtres (ou comme Outlook les appelle, des règles) déjà configurées. Cliquez sur **Nouveau** pour en créer une

nouvelle.

Choisissez "**Vérifiez les messages à leur arrivée**" puis cliquez sur **suivant**.



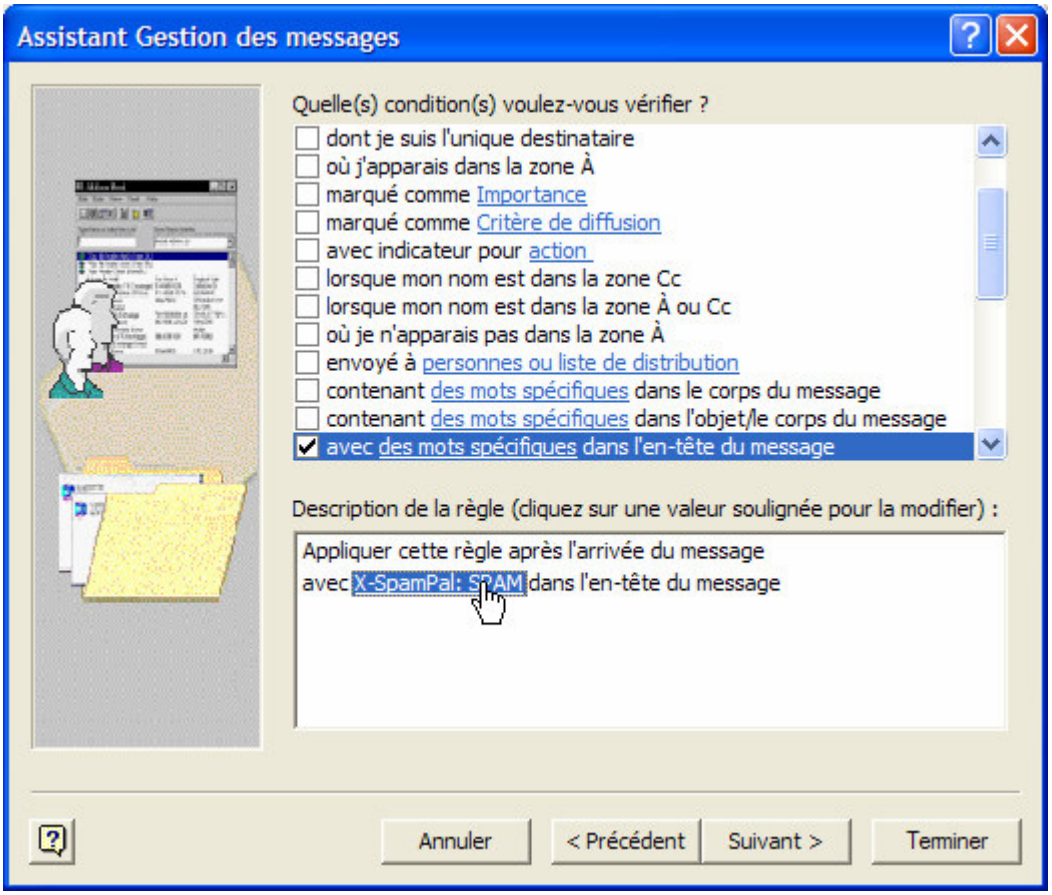
Note 1: Assistant de Gestion des messages de Outlook XP (2002)

Dans les versions les plus récentes de Outlook, vous devez créer la nouvelle règle en utilisant :
"**Démarrez à partir d'une règle vide**"

Maintenant, nous allons créer un filtre pour transférer tout ce qui contient l'entête spécial de SpamPal dans un dossier spam.

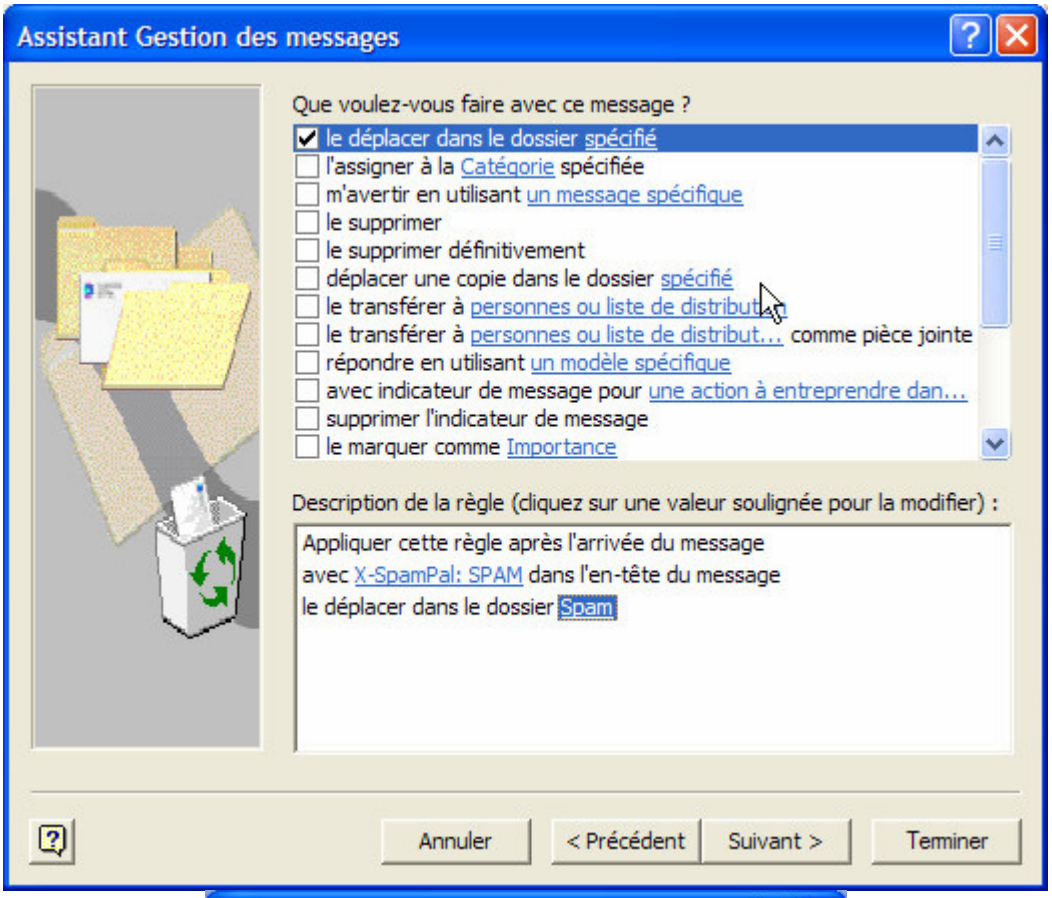
D'abord, sélectionnez la condition **avec des mots spécifiques dans l'en-tête du message**

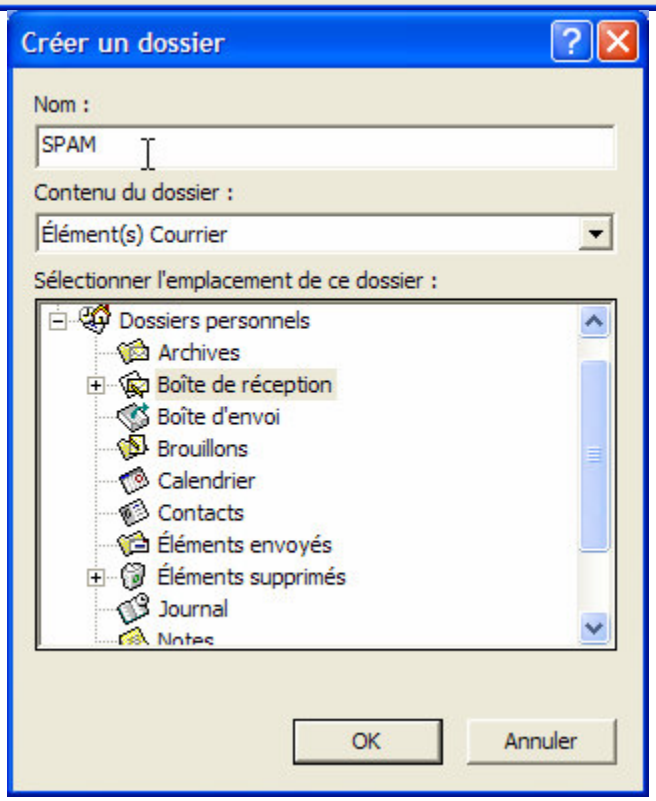
Cliquez sur les mots soulignés en bleu **des mots spécifiques** dans la partie inférieure; tapez **X-SpamPal: SPAM** dans le champ en haut de la fenêtre qui apparaît, cliquez ensuite sur **OK** puis sur **Suivant.**



Sélectionnez l'action **le déplacer dans le dossier spécifié**. Cliquez sur le mot en bleu **spécifié** puis sur **Nouveau** pour créer un dossier appelé **Spam** (ou n'importe quel nom que vous avez choisi).

Vérifiez que la sélection **contenu du dossier** montre **Elément(s) courrier**, et sélectionnez où vous voulez placer le nouveau dossier. Puis cliquez sur **OK**.



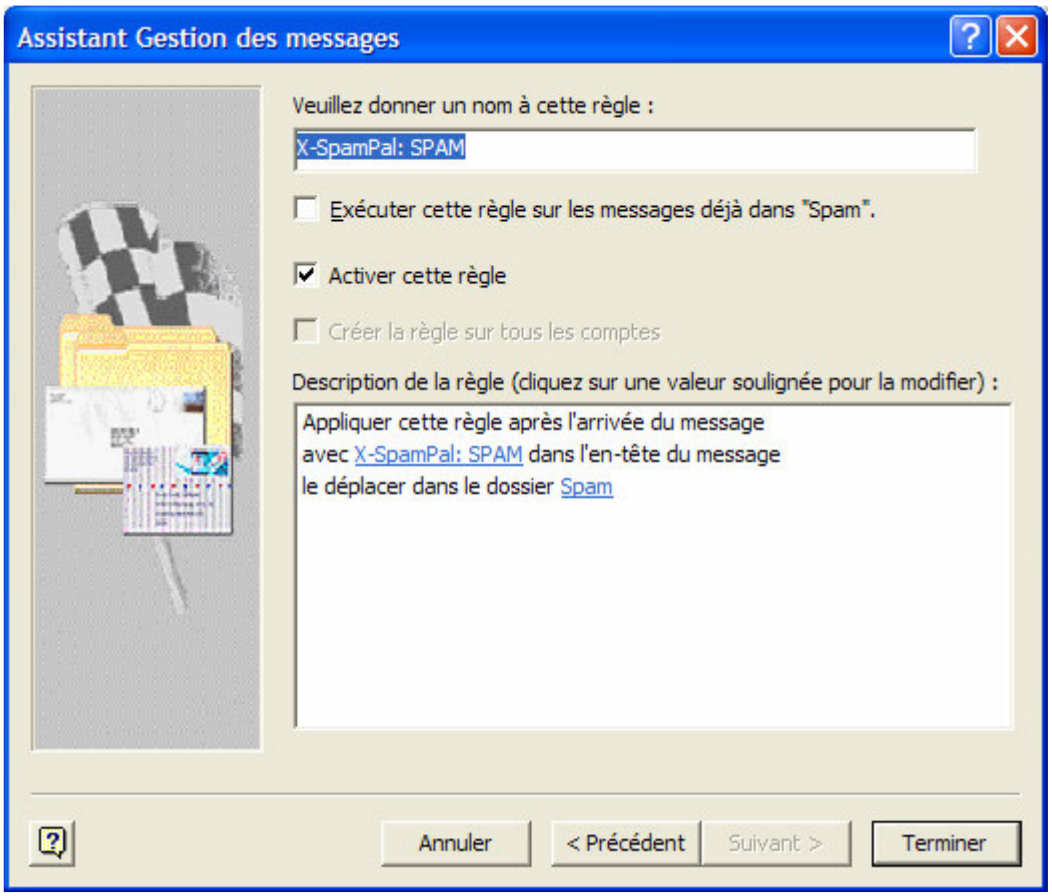


Si vous voulez ajouter un raccourci dans la barre Outlook, cliquez sur **Oui**, sinon sur **Non**.

Cliquez sur **OK** puis **Suivant**.

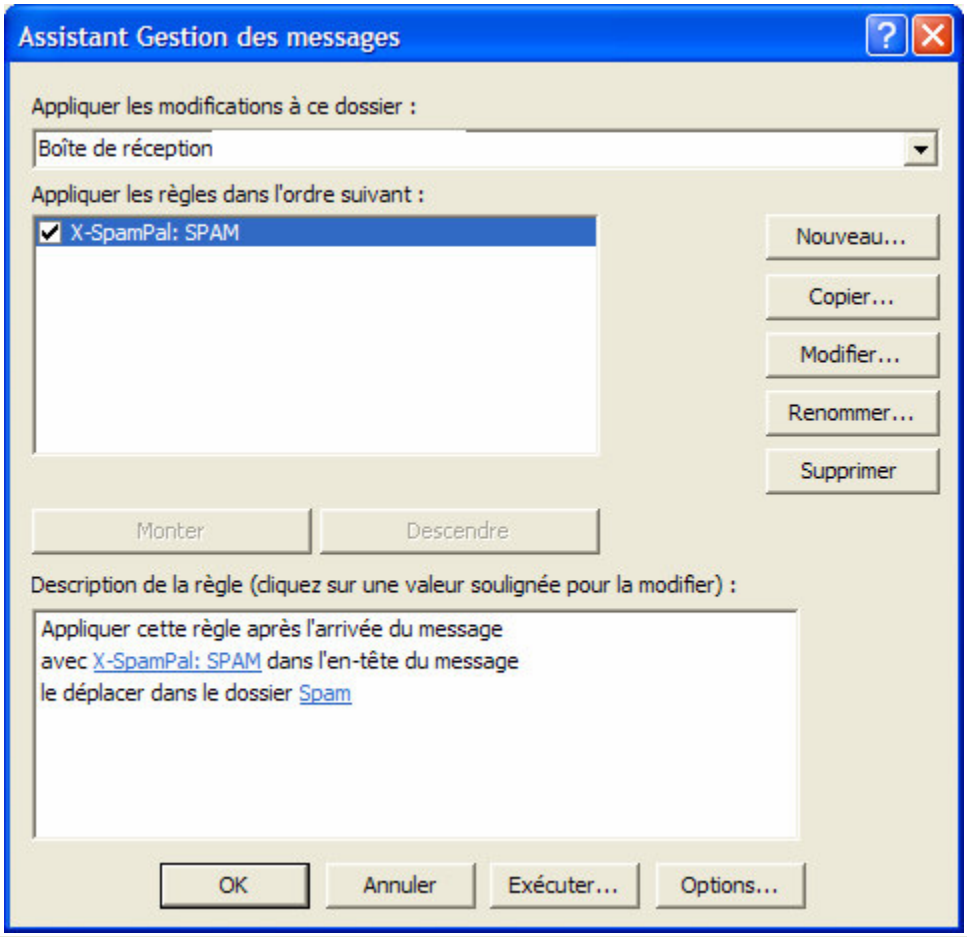
Sélectionnez les exceptions à la règle que vous voulez utiliser (il est recommandé de n'en choisir aucune) puis cliquez sur **Suivant**.

Vous devriez au final avoir une règle qui ressemble à ceci :



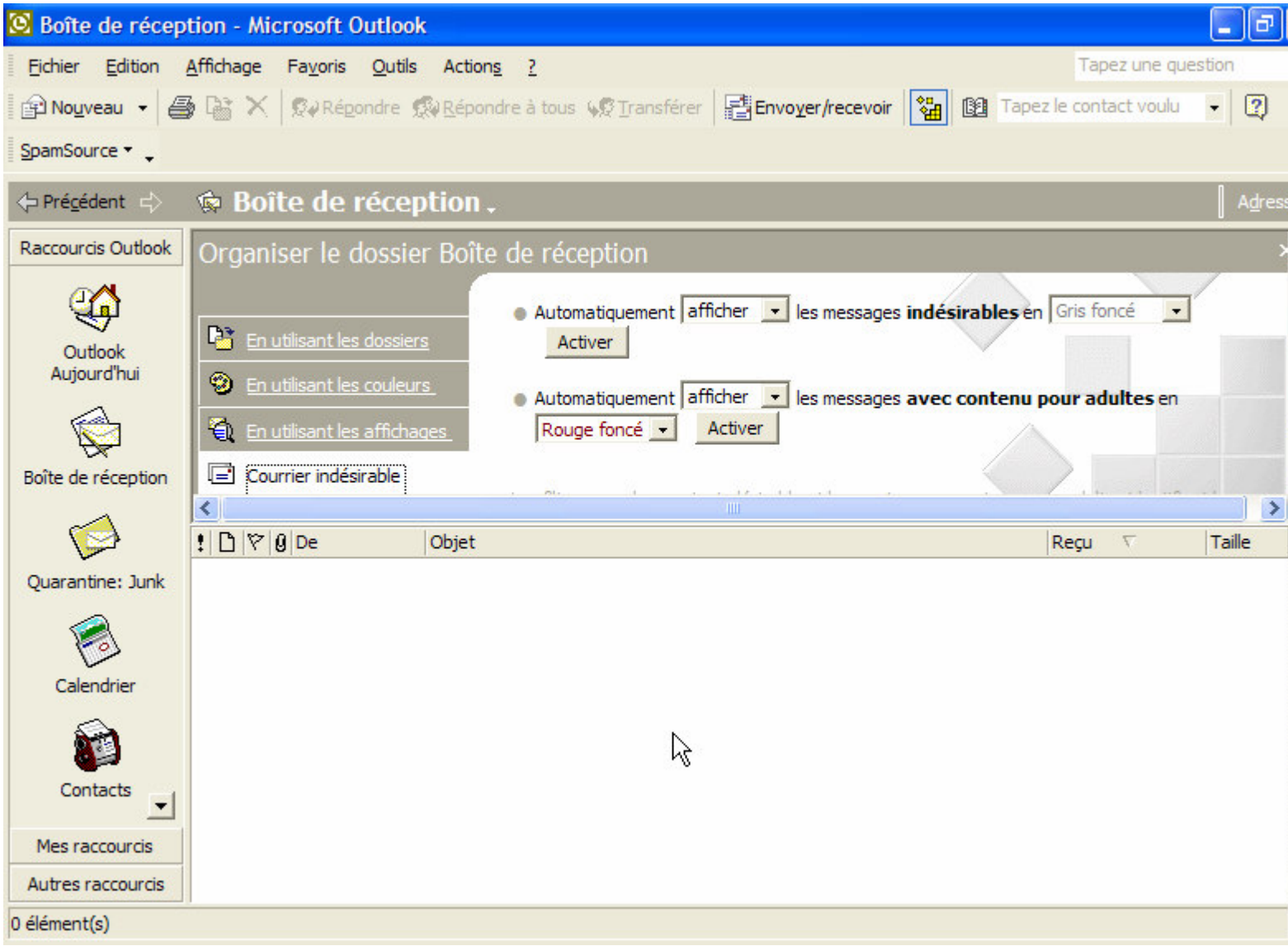
Donnez à votre filtre un nom approprié, par exemple, SpamPal et cliquez sur **Terminer** pour la créer, puis sur **OK** pour fermer la fenêtre de l'assistant de gestion des messages.

Donc, votre(s) règle(s) devrai(en)t ressembler à ceci:



Note 2: Ordre des règles de message

Soyez sûr que votre nouvelle règle pour SpamPal soit la **première** dans la liste, si vous avez beaucoup d'autres règles de message.



Note 3: Expéditeurs bloqués

Si vous avez beaucoup d'expéditeurs bloqués, il vaut mieux les retirer de la liste, parce que SpamPal fait un meilleur travail. Les retirer de la liste va aussi accélérer le traitement du mail.

::Début::

4. Programmes anti-Virus & Firewalls

Des instructions spécifiques pour utiliser une variété de programmes anti-virus avec SpamPal peuvent être trouvées sur la page d'installation principale

Quelques filtres anti-virus ont besoin de se situer entre votre programme email et votre serveur de mail, juste là où se trouve SpamPal. Il n'y a en fait aucune raison qu'ils ne le puissent pas; vous devez juste les mettre en série afin qu'ils puissent récupérer le courrier au travers de SpamPal au lieu de directement, puis votre programme email récupère le courrier à travers le filtre anti-virus.

::Début::

5. Mettre vos amis et contacts en liste blanche

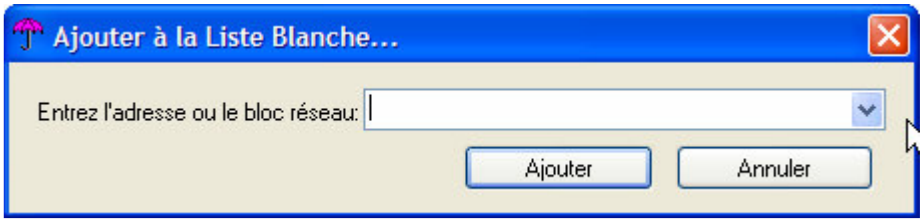
Afin d'accélérer le traitement de vos emails et d'éviter que SpamPal marque les emails de vos amis ou contacts comme spam, c'est une bonne idée à ce point de l'installation de mettre en liste blanche l'adresse de tous vos contacts importants.

Pour celà, il y a quatre manières de faire :

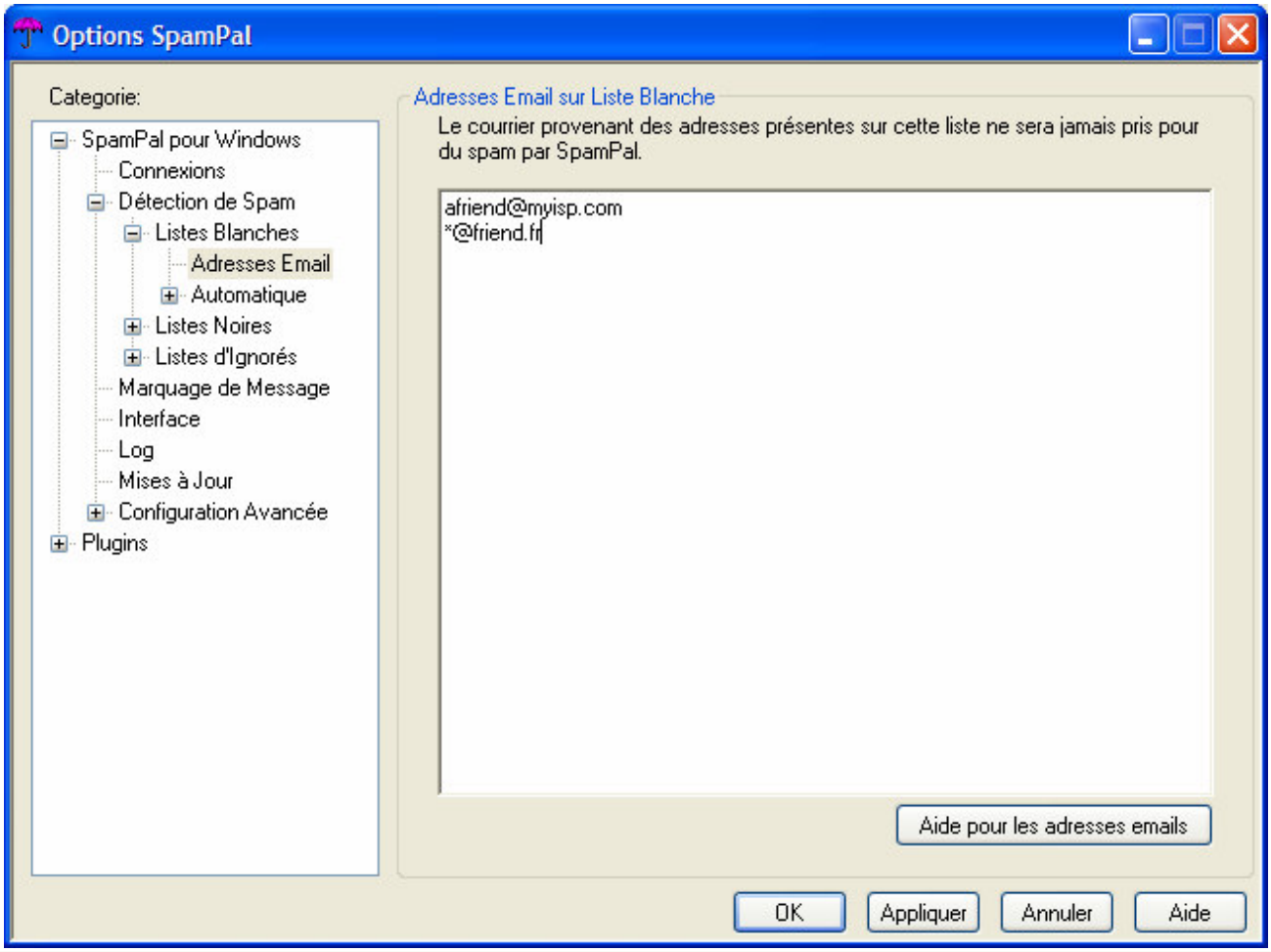
a) Utiliser la liste blanche automatique **pop3** : cela va ajouter à la liste blanche les adresses dont vous recevez fréquemment du courrier non-spam,
b) Utiliser la liste blanche automatique **smtp** : si configurée en **3.3**, elle ajoute à la liste blanche les adresses auxquelles vous envoyez du courrier,

> **Note 1:** Vie privée : liste blanche automatique smtp
>
> Si vous utilisez cette possibilité, spéciallement dans un bureau, comme cela va enregistrer toutes les adresses de messages sortants, cela pourrait constituer une atteinte à la vie privée (au Royaume-Uni, vous devez prévenir une personne si vous placez son adresse dans un fichier), ou la constitution d'un fichier (soumis à la loi française "Informatique et libertés")

c) utiliser le menu **Ajouter à la liste blanche** sur l'icône de SpamPal dans la barre des tâches: pour ajouter manuellement à la liste blanche, vous pouvez la taper manuellement, ou la copier :



d) Vous pouvez utiliser cette procédure pour exporter **automatiquement** vos contacts de Outlook Express ou vous pouvez utiliser la page des **adresses email en liste blanche** de SpamPal, pour ajouter manuellement vos adresses email :



Note 2: Entêtes auxquels la liste blanche est comparée

La fonction liste blanche ne regarde que dans certains entêtes de vos emails.

Actuellement, ce sont : **From:**, **Reply-To:**, **Sender:, Mailing-List:** et **Return-Path**:

Au départ, vous remarquerez que l'utilisation de SpamPal rend la récupération du courrier un peu plus longue. C'est parce que SpamPal doit vérifier la présence de chaque adresse dans chaque liste DNSBL (liste noires publiques) pour voir quels emails viennent d'un spammer.

Néanmoins, grâce à sa fonction liste blanche automatique, SpamPal va rapidement apprendre qui vous envoie beaucoup de messages, et va les ajouter à une liste des émetteurs de confiance. Parce qu'ils sont de confiance, SpamPal ne perd pas de temps à les vérifier dans les listes DNSBL. Pour ceux-là, plus vous utilisez SpamPal, plus il deviendra rapide.

Vous pouvez trouver d'autres trucs et astuces pour optimiser SpamPal ici.

Ceci termine l'installation et la configuration de SpamPal.

::Top::

Cette page donne les étapes à suivre pour installer et régler SpamPal pour une utilisation avec le programme Outlook Express.

Index rapide

1. Installation de SpamPal

Télécharger SpamPal et lancez l'installation en double-cliquant sur l'icône du programme d'installation de SpamPal (spampal.exe ou spampal-***.exe) et suivez les instructions affichées à l'écran. A la fin de l'installation, SpamPal se lance, montrant son icône (un parapluie rose) dans votre barre de tâches.

Si cette installation est une mise à jour, la configuration existante est conservée et le processus est terminé. Sinon, c'est à dire pour une nouvelle installation, suivez les instructions ci-dessous.

::Début::

2. Configurer SpamPal

Tout ce que vous avez besoin de savoir pour configurer SpamPal peut être trouvé ici.

::Début::

3. Configurer votre programme Email

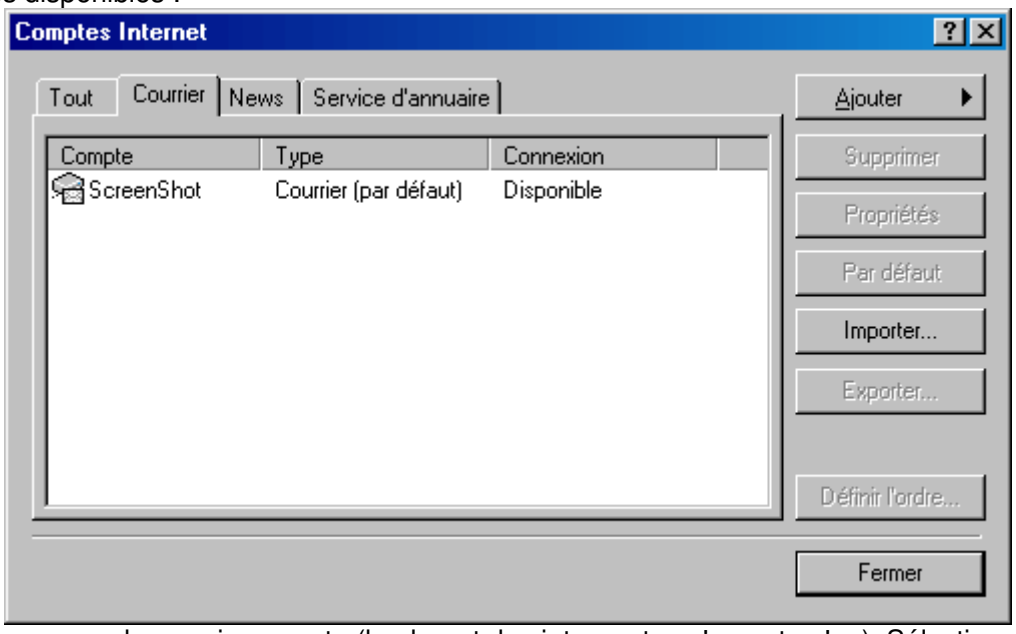
Maintenant que vous avez réglé SpamPal, vous devez configurer votre programme email, de telle manière que tous les emails soient reçus au travers du proxy POP3 / IMAP4 de SpamPal, et non directement depuis le serveur POP3 de votre fournisseur d'accès.

Vous n'avez besoin de changer que les paramètres que vous utilisez réellement pour récupérer le courrier depuis le serveur mail de votre fournisseur d'accès. Par exemple, si vous n'utilisez que le format POP3 pour lire votre courrier , vous n'avez besoin de modifier que vos réglages POP3.

::Top::

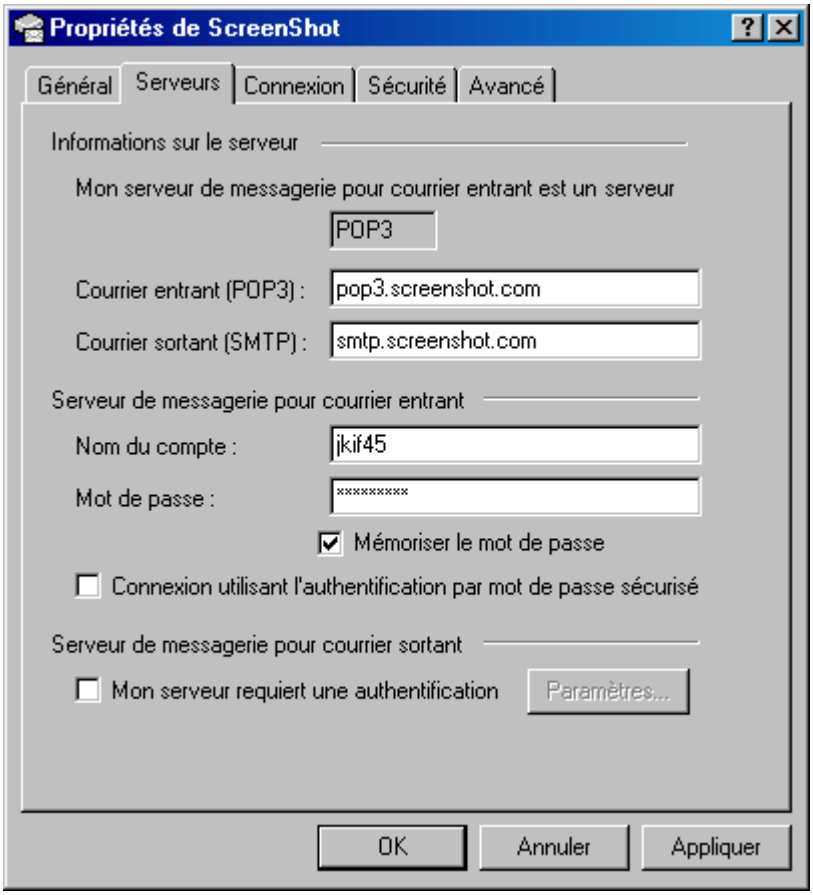
3.1 Changer les réglages POP3

Démarrez Outlook Express, puis choisissez **Comptes** dans le menu **Outils**, et sélectionnez l'onglet **Courrier** pour afficher les comptes disponibles :



Nous allons commencer par le premier compte (la plupart des internautes n'en ont qu'un). Sélectionnez-le et cliquez sur **Propriétés**. Allez dans l'onglet **Serveurs** de la fenêtre qui s'est ouverte, elle devrait ressembler à ceci:

Fenêtre **avant** changements:

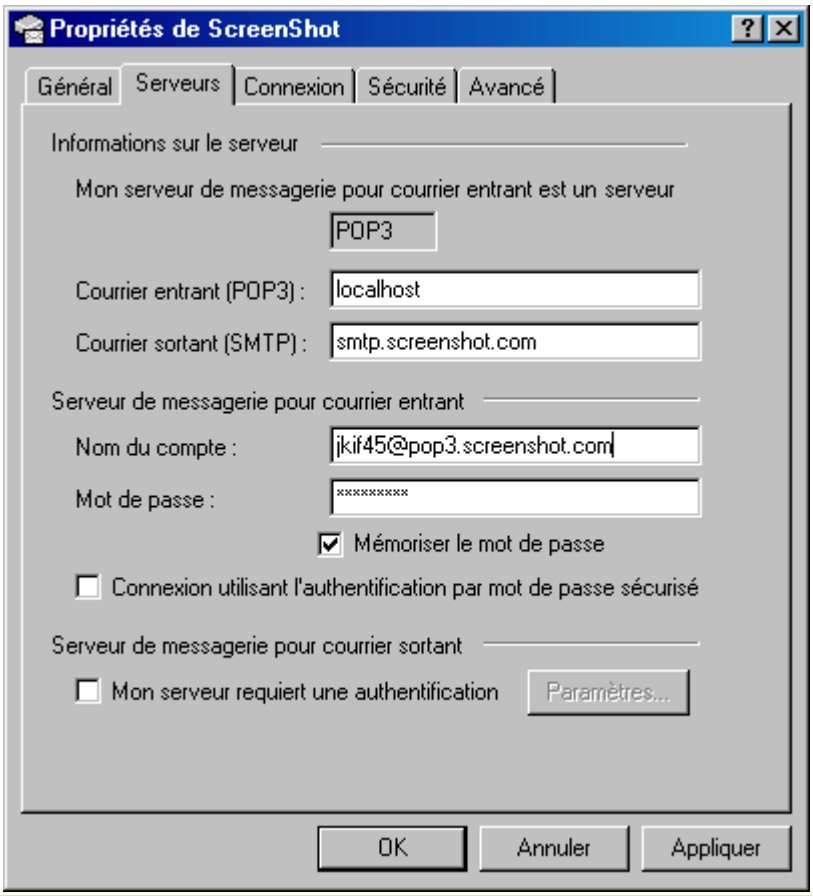


Vous n'avez besoin de modifier que les lignes **Courrier entrant (POP3)** et **Nom du compte**.

Notez le nom du serveur de votre serveur POP (c'est à dire, **pop3.serveur.com**) et remplacez-le par **localhost** ou **127.0.0.1**

Maintenant, ajoutez le symbole @ suivi du nom de votre serveur POP que vous avez noté, à la suite du nom du compte, c'est à dire : nom_utilisateur**@pop3.serveur.com**)

Fenêtre **après** changements :



Note 1: Si le nom du compte comporte déjà un @

Vous pouvez continuer sans problème, SpamPal sait gérer les noms de compte qui contiennent 2 @ sans difficulté.

Note 2: Si vous avez eu un message d'erreur disant que SpamPal ne peut écouter le port POP3 standard

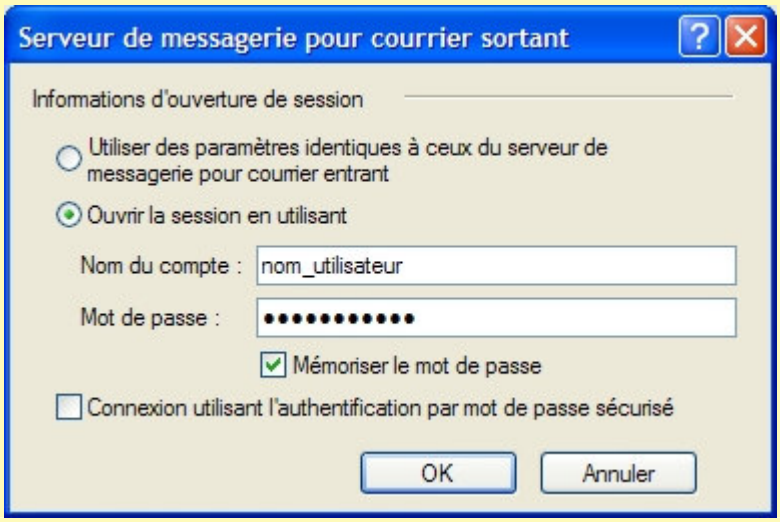
Vous pouvez, ici, avoir un message d'erreur disant que SpamPal ne peut écouter le port POP3 standard. Il ne faut pas s'inquiéter; notez juste le numéro de port que SpamPal vous donne et continuez à suivre ce guide.

Ce message signifie que SpamPal utilise le Port **1110** au lieu du **110**. Vous n'avez pas besoin de le lui dire parce que SpamPal sait déjà qu'il utilise le port **1110**. A la place, vous devrez dire à votre programme email (par exemple Outlook Express) d'utiliser le port **1110** au lieu du **110**.

Pour cela, allez dans l'onglet **Avancé** des propriétés du compte (la fenêtre dans laquelle nous sommes), il y a là une ligne **Courrier entrant (POP3)**, qui indique actuellement **110**. Vous devez changer cette valeur pour celle indiquée à l'installation de SpamPal, généralement **1110**. La procédure est rappelée plus loin.

Note 3: Si le serveur nécessite une authentification (case cochée sous "Serveur de messagerie pour courrier sortant)...

Cliquez sur le bouton **Paramètres...** situé à coté. Sélectionnez **Ouvrir la session en utilisant** et entrez votre **nom d'utilisateur et mot de passe originaux**, c'est à dire, ceux que vous aviez avant de les modifier pour installer SpamPal.



Note 4: Si votre serveur POP3 n'utilise pas le port POP3 par défaut (110)...

Ajoutez le numéro de port au nom du serveur dans la case "Nom du compte" en utilisant ":". Par exemple, si BlueYonder utilisait le port 8090 pour leur serveur POP3, j'aurais un nom d'utilisateur de la forme `jf004d7582@pop3.blueyonder.co.uk:8090`

Note 5: Si le nom du serveur est déjà localhost ou 127.0.0.1

Pas de problème, ajoutez simplement @localhost au nom du compte et laissez le nom du serveur intact.

Avant d'utiliser SpamPal	Après la configuration pour SpamPal
Exemple 1	
Courrier entrant (POP3) : **pop3.yourisp.com**	Courrier entrant (POP3) : localhost
Nom du compte : name@surname	Nom du compte :name@surname**@pop3.yourisp.com**
Exemple 2	
Courrier entrant (POP3) : **mail.yourisp.com**	Courrier entrant (POP3) : 127.0.0.1
Nom du compte: my_login_name	Nom du compte: my_login_name**@mail.yourisp.com**
Exemple 3 (utilisant une adresse IP locale)	
Courrier entrant (POP3) : **192.168.1.1**	Courrier entrant (POP3) : 127.0.0.1
Nom du compte: my_login_name	Nom du compte: my_login_name**@192.168.1.1**

Note 6: Nom du serveur

Le "Nom du serveur POP3 entrant", ci-dessus, peut, selon votre programme email aussi être appelé : serveur mail entrant, serveur POP3, Nom d'utilisateur POP3 ou Nom du compte.

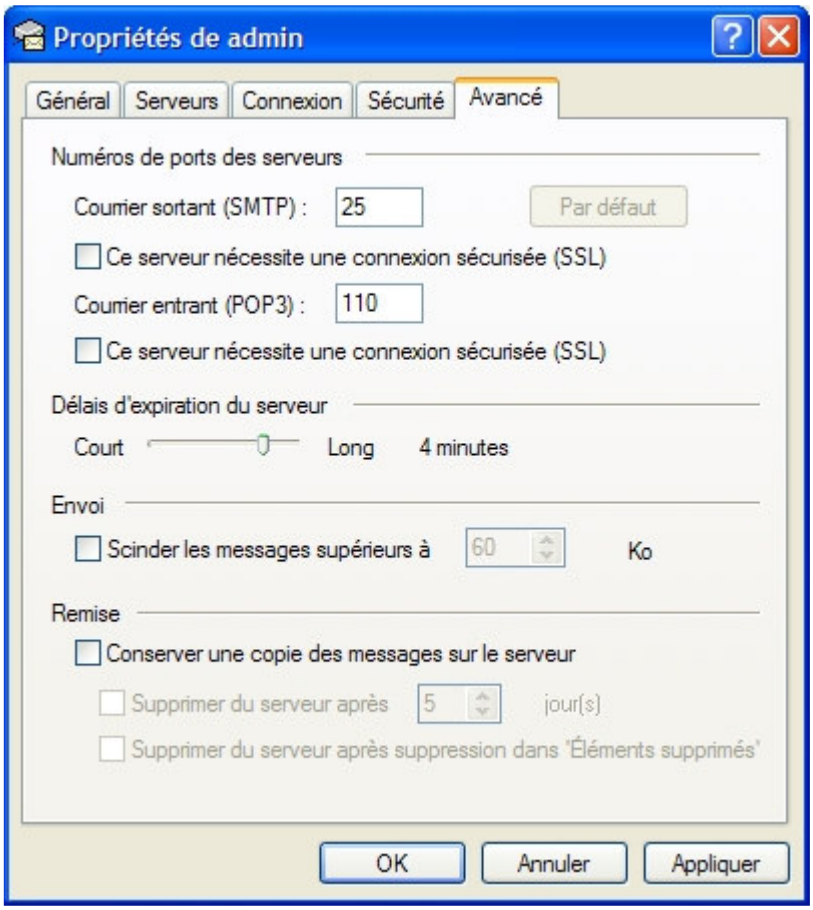
Il y a aussi deux façons de préciser le nom du serveur local, qui veulent dire la même chose toutes les deux (mais, avec certains programmes, une seule fonctionne): **localhost** ou **127.0.0.1**

Cliquez maintenant sur **OK** pour confirmer la modification, et répétez ceci pour chaque compte que vous souhaitez protéger. Lorsque vous avez fini, fermer la fenêtre "Comptes".

Maintenant, essayez de récupérer votre courrier; si vous n'avez pas d'erreurs, continuez avec l'étape suivante. Il peut vous être demandé de ressaisir vos mots de passe POP3; rien d'inquiétant. Si vous obtenez une erreur d'Outlook Express, vérifiez que vous avez correctement configuré le Nom du serveur POP3 entrant à **localhost** et, si nécessaire,

que le port a été modifié avec la bonne valeur. Si vous obtenez une erreur de SpamPal, vérifiez que vous avez bien ajouté le nom du serveur au nom du compte, et que la connexion a Internet est active.

Si vous avez besoin de changer les ports **POP3**, **SMTP** ou **IMAP**, commencez par le premier compte (la plupart des internautes n'en ont qu'un). Sélectionnez-le puis cliquez sur **Propriétés**. Allez dans l'onglet **Avancé**, qui devrait ressembler à ceci :



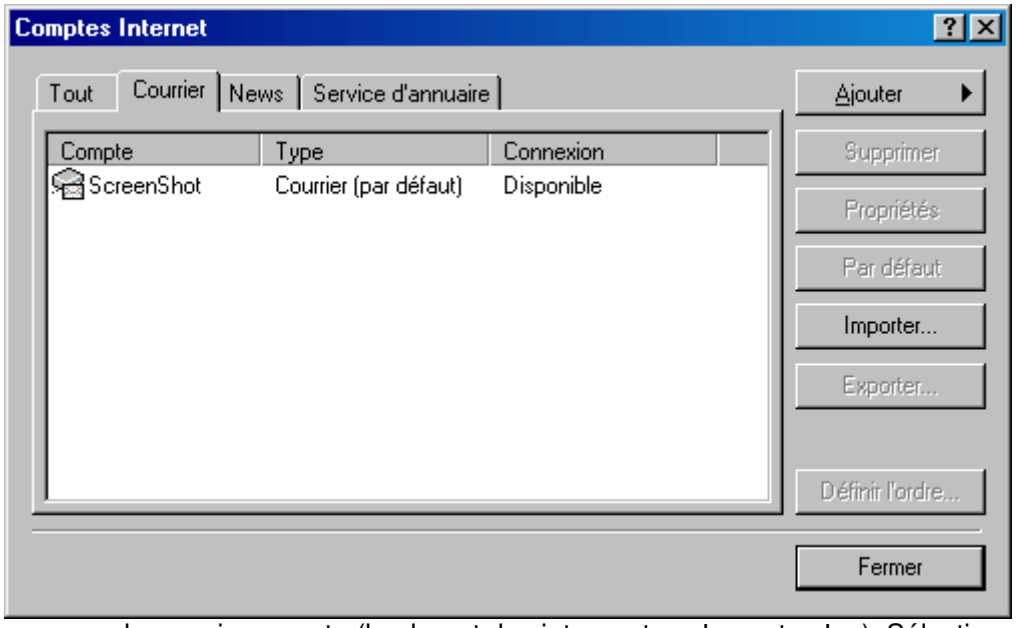
Note 7: Délais d'expiration du serveur

Le **Délai d'expiration du serveur** par défaut de 1 minute peut être un peu juste pour une utilisation avec SpamPal. Si vous trouvez que le serveur n'a pas le temps de répondre alors, peut-être, vous pourriez augmenter cette valeur à **4 minutes**.

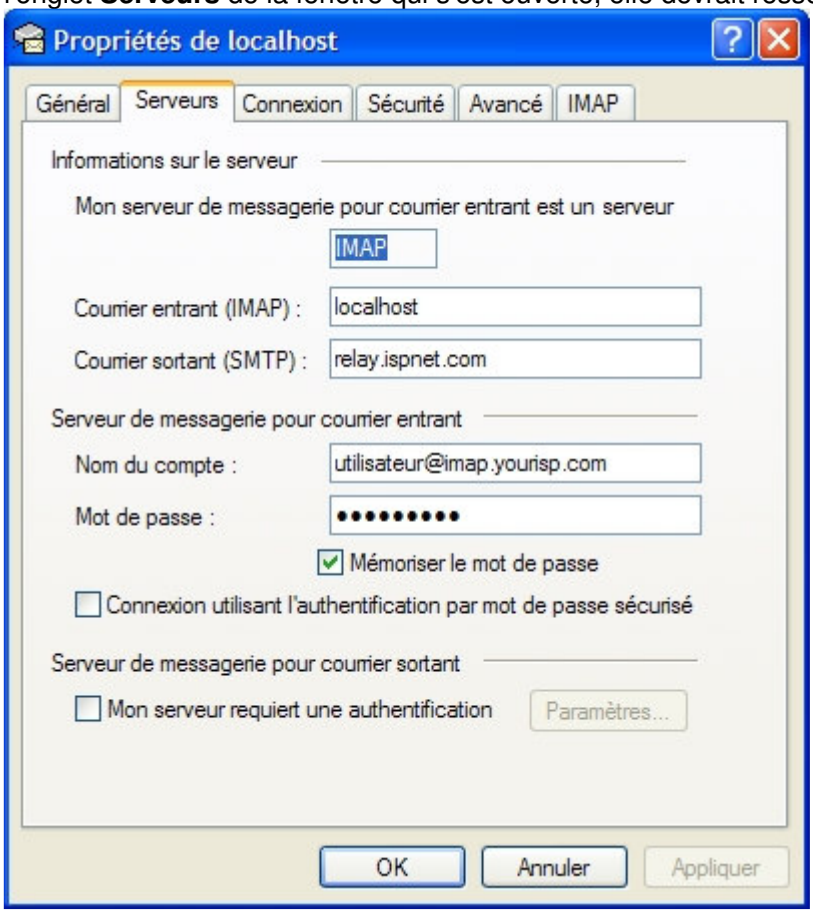
::Début::

3.2 Changer les réglages IMAP4

Démarrez Outlook Express, puis choisissez **Comptes** dans le menu **Outils**, et sélectionnez l'onglet **Courrier** pour afficher les comptes disponibles :



Nous allons commencer par le premier compte (la plupart des internautes n'en ont qu'un). Sélectionnez-le et cliquez sur **Propriétés**. Allez dans l'onglet **Serveurs** de la fenêtre qui s'est ouverte, elle devrait ressembler à ceci:



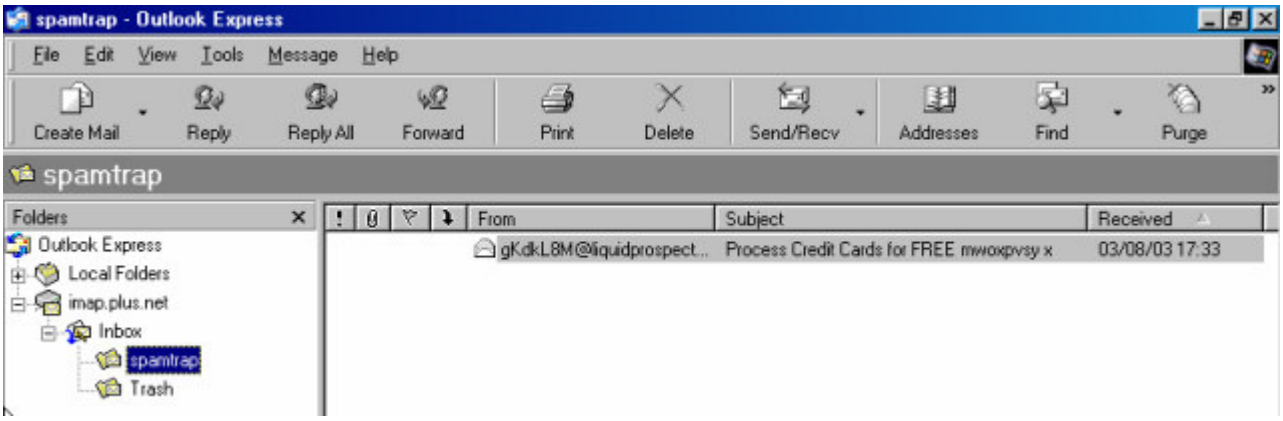
Vous n'avez besoin de modifier que les lignes **Courrier entrant (IMAP)** et **Nom du compte**.

Notez le nom du serveur de votre serveur IMAP (c'est à dire, **imap.yourisp.com**) et remplacez-le par **localhost** ou **127.0.0.1**

Maintenant, ajoutez le symbole @ suivi du nom de votre serveur IMAP que vous avez noté, à la suite du nom du compte, c'est à dire : nom_utilisateur@**imap.yourisp.com**)
Cliquez maintenant sur **OK** pour confirmer la modification, et répétez ceci pour chaque compte que vous souhaitez protéger. Lorsque vous avez fini, fermer la fenêtre "Comptes".

Maintenant, essayez de récupérer votre courrier; si vous n'avez pas d'erreurs, continuez avec l'étape suivante. Il peut vous être demandé de ressaisir vos mots de passe POP3; rien d'inquiétant. Si vous obtenez une erreur d'Outlook Express, vérifiez que vous avez correctement configuré le Nom du serveur POP3 entrant à **localhost** et, si nécessaire, que le port a été modifié avec la bonne valeur. Si vous obtenez une erreur de SpamPal, vérifiez que vous avez bien ajouté le nom du serveur au nom du compte, et que la connexion a Internet est active.

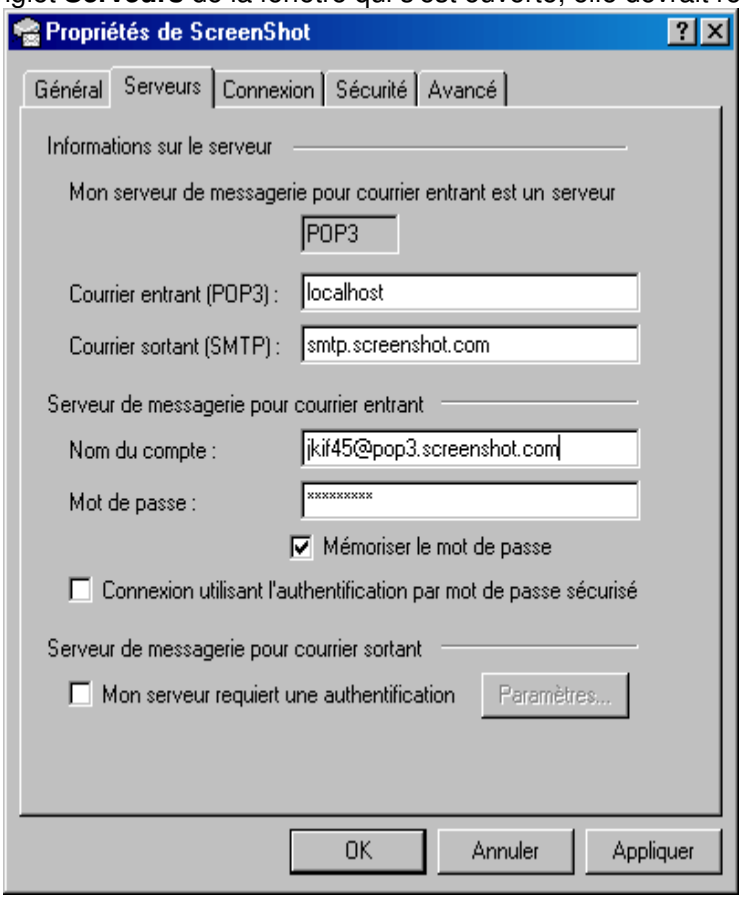
Vous devriez aussi remarqué que vous avez maintenant un nouveau dossier "spamtrap". Il a été créé par SpamPal pour stocker tous vos messages marqués "spam":



::Début::

3.3 Changer les réglages SMTP

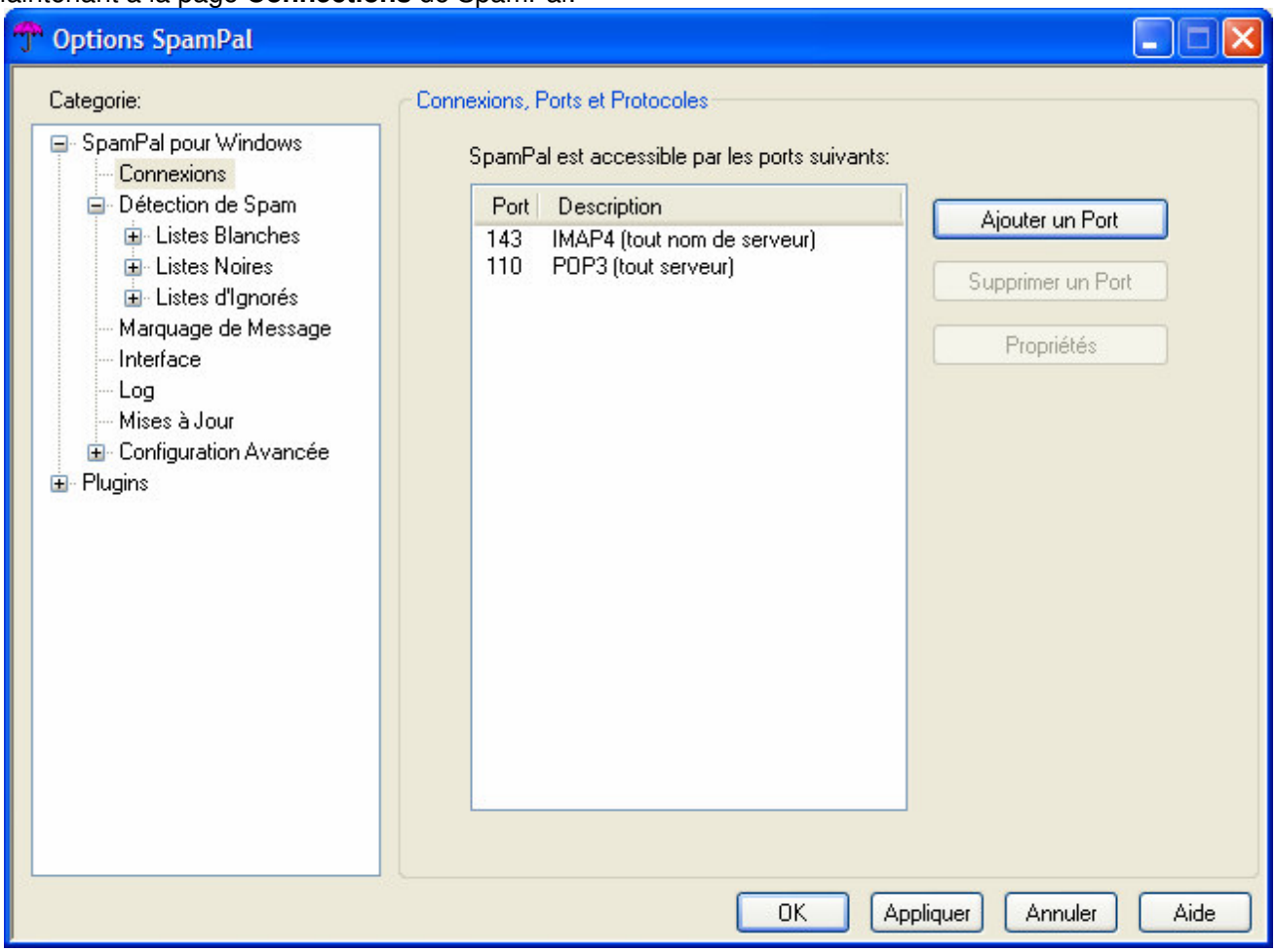
Si vous souhaitez utiliser le proxy SMTP de SpamPal pour ajouter automatiquement à la liste blanche toute adresse email à laquelle vous envoyez un courrier, vous devez changer les réglages SMTP de Outlook Express.
Nous allons commencer par le premier compte (la plupart des internautes n'en ont qu'un). Sélectionnez-le et cliquez sur **Propriétés**. Allez dans l'onglet **Serveurs** de la fenêtre qui s'est ouverte, elle devrait ressembler à ceci:



Maintenant, notez l'adresse de votre **Serveur de courrier sortant (SMTP)**, par exemple : **smtp.myisp.co.uk**

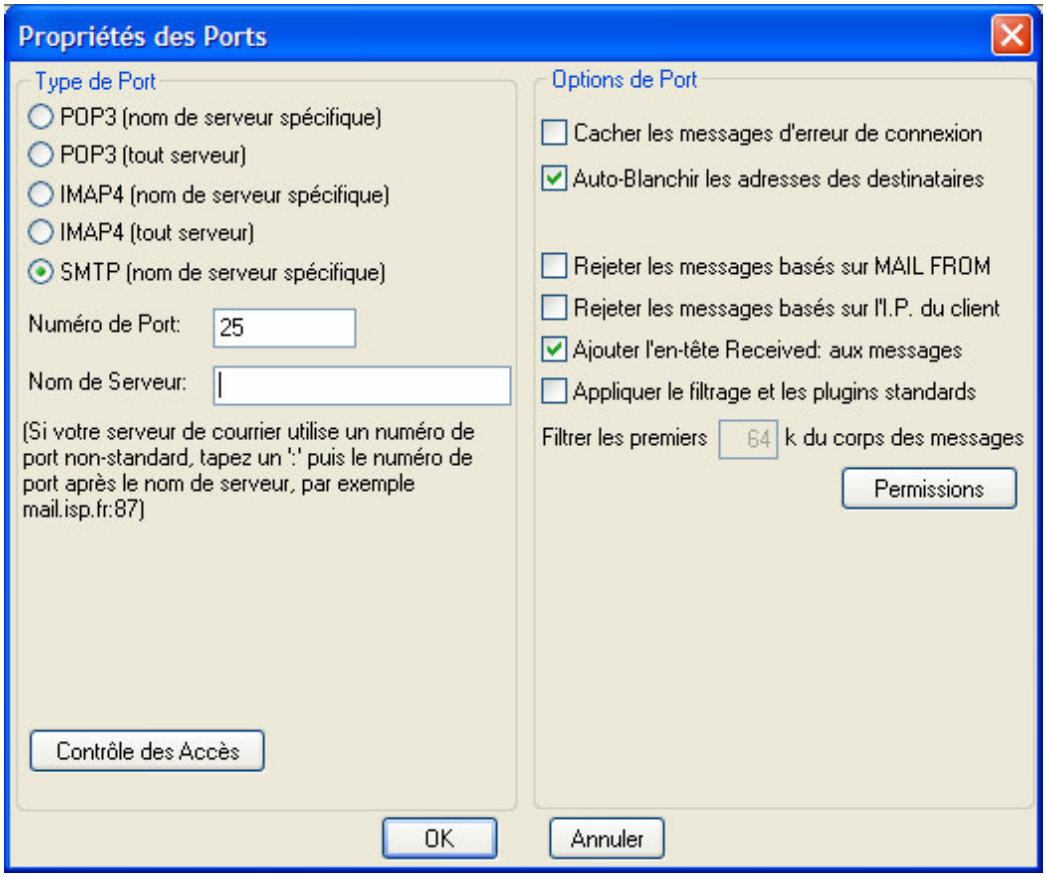
Remplacez cette valeur par : **127.0.0.1**

Allez maintenant à la page **Connections** de SpamPal:



Cliquez sur **Ajouter un port** et changer le type de Port pour **SMTP.**

Changer le **Nom de serveur** pour le **Serveur de courrier sortant (SMTP)** que vous avez noté plus tôt, **smtp.myisp.co.uk**



Maintenant, dès que vous envoyez un email, SpamPal va automatiquement ajouter l'adresse du ou des destinataires à la liste blanche.

Note: Option "Exclusions" de la liste blanche

De temps en temps, un spammer peut utiliser l'adresse de quelqu'un qui est dans votre liste blanche automatique - un collègue ou une autre de vos adresses email, par exemple. D'un coté, vous ne voulez pas ajouter l'adresse de cette personne dans la liste noire parce qu'elle vous envoie beaucoup d'emails légitimes, d'un autre coté, vous ne voulez pas qu'elles finissent dans la liste blanche automatique et court-cuitent les protections anti-spam de SpamPal.

En cliquant sur le panneau **Exclusions**, une fenêtre va apparaître et vous permettre de saisir les adresses de personnes qui ne doivent jamais être ajouter à la liste blanche automatique. Ajouter vos collègues, vos propres adresses, et vous n'aurez plus à vous inquiéter des spammers utilisant ces adresses pour contourner le filtrage de SpamPal. Vous pouvez même ajouter des domaines entiers - *@acme-widgets.com

::Début::

3.4 Créer des filtres ou des règles de messages

Si vous utilisez un serveur **IMAP4**, vous n'avez pas besoin de mettre en place de règle ou de filtre, puisque SpamPal déplace tout message marqué "spam" dans un dossier **inbox.spamtrap** sur votre serveur.

Si vous utilisez un serveur **POP3** et voulez que Outlook Express filtre automatiquement les messages marqués dans une boîte de réception séparée, afin que vous puissiez plus facilement les passer en revue, suivez les étapes suivantes.

Dans le menu **Outils**, **Règles de messages**, sélectionnez **Courrier**; cela va ouvrir une fenêtre présentant la liste de tous les filtres (ou, comme Outlook Express les appelle, des règles) déjà réglés. Cliquez sur **Nouveau** pour en ajouter un.

Normallement, nous devrions créer un filtre pour transférer tout ce qui contient l'entête spécial de SpamPal dans un dossier "spam". Néanmois, comme Outlook Express ne permet pas un tel filtre avancé, nous allons créer une règle qui

détecte tout ce qui contient **`**SPAM**`** dans la ligne de l'objet. SpamPal ajoute ça par défaut à tous les messages dont il pense qu'ils sont du spam. Faites attention à ne pas modifier ce paramètre ou vos règles ne fonctionneraient plus.

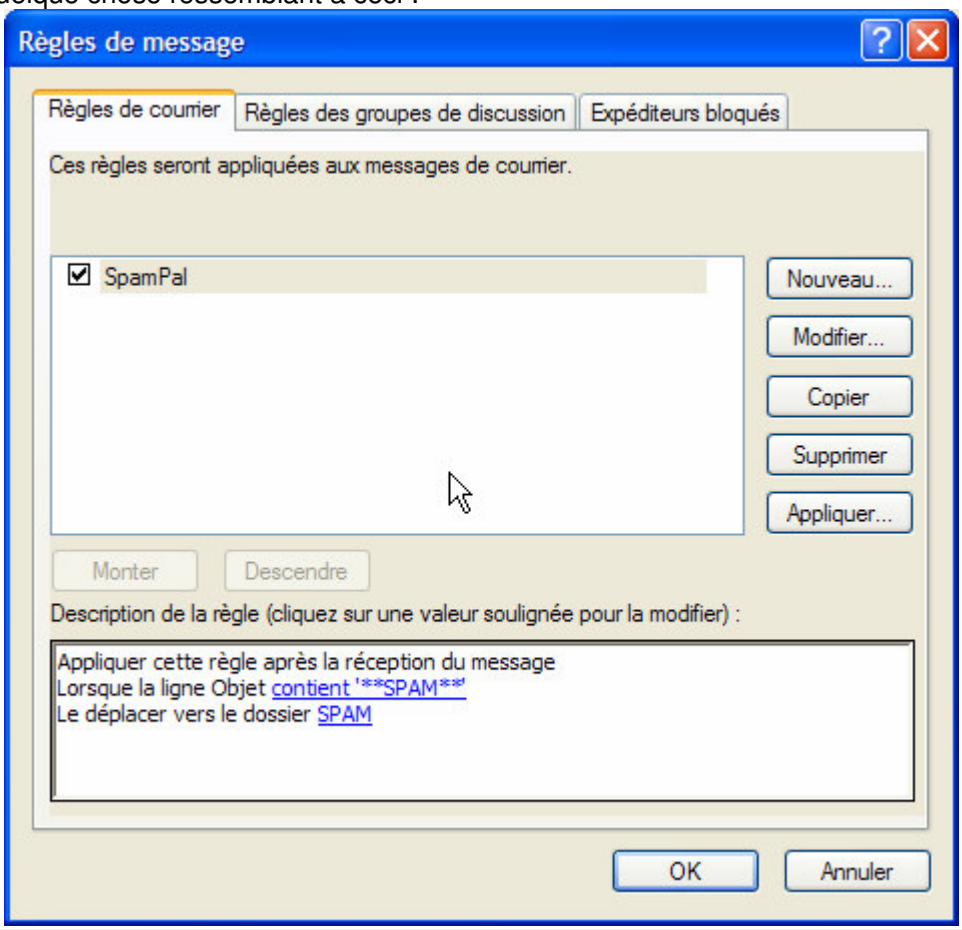
En premier, sélectionnez de filtrer **lorsque la ligne Objet contient des mots spécifiques**, et une action **le déplacer vers le dossier spécifié**. Cliquez maintenant sur la partie bleue **contient des mots spécifiques** dans la partie inférieure; tapez **`**SPAM**`** (sans guillemets) dans le champ du haut de la fenêtre qui apparaît, et cliquez sur **Ajouter à la liste**.

Cliquez sur **OK** pour fermer cette fenêtre, puis cliquez sur la partie bleue **spécifié** et cliquez sur **Nouveau dossier** pour créer un nouveau dossier appelé **Spam Trap** (ou ce que vous voulez).

La description de votre règle devrait être :

Appliquer cette règle après la réception du message
Lorsque la ligne Objet contient '**SPAM**'
Le déplacer vers le dossier SPAM

Vous devriez avoir quelque chose ressemblant à ceci :

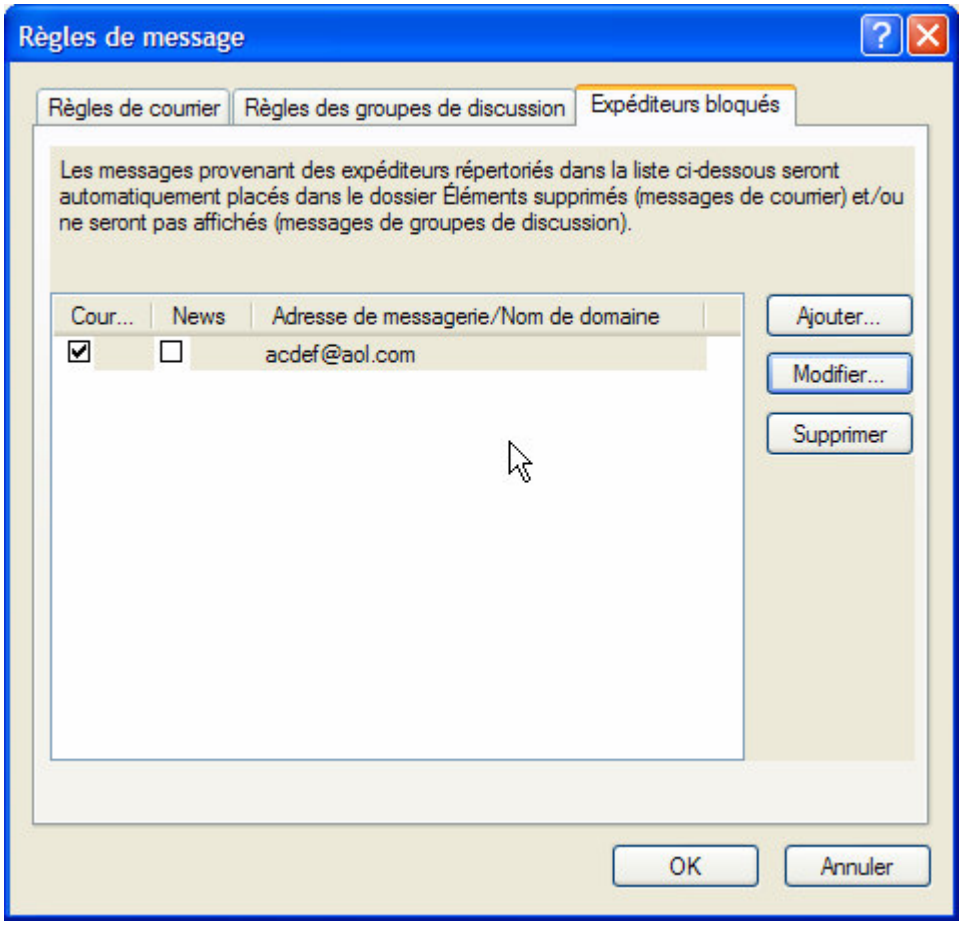


Note 1: Ordre des règles de message

Soyez sûr que votre nouvelle règle pour SpamPal soit la **première** dans la liste, si vous avez beaucoup d'autres règles de message.

Note 2: Expéditeurs bloqués

Si vous avez beaucoup d'expéditeurs bloqués, il vaut mieux les retirer de la liste, parce que SpamPal fait un meilleur travail. Les retirer de la liste va aussi accélérer le traitement du mail.



::Début::

4. Programmes anti-Virus & Firewalls

Des instructions spécifiques pour utiliser une variété de programmes anti-virus avec SpamPal peuvent être trouvées sur la page d'installation principale

Quelques filtres anti-virus ont besoin de se situer entre votre programme email et votre serveur de mail, juste là où se trouve SpamPal. Il n'y a en fait aucune raison qu'ils ne le puissent pas; vous devez juste les mettre en série afin qu'ils puissent récupérer le courrier au travers de SpamPal au lieu de directement, puis votre programme email récupère le courrier à travers le filtre anti-virus.

::Début::

5. Mettre vos amis et contacts en liste blanche

Afin d'accélérer le traitement de vos emails et d'éviter que SpamPal marque les emails de vos amis ou contacts comme spam, c'est une bonne idée à ce point de l'installation de mettre en liste blanche l'adresse de tous vos contacts importants.

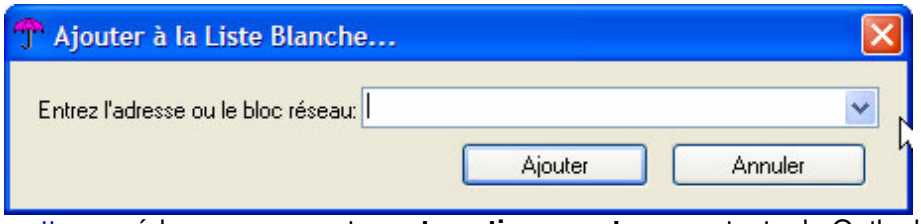
Pour celà, il y a quatre manières de faire :

a) Utiliser la liste blanche automatique **pop3** : cela va ajouter à la liste blanche les adresses dont vous recevez fréquemment du courrier non-spam,
b) Utiliser la liste blanche automatique **smtp** : si configurée en **3.3**, elle ajoute à la liste blanche les adresses auxquelles vous envoyez du courrier,

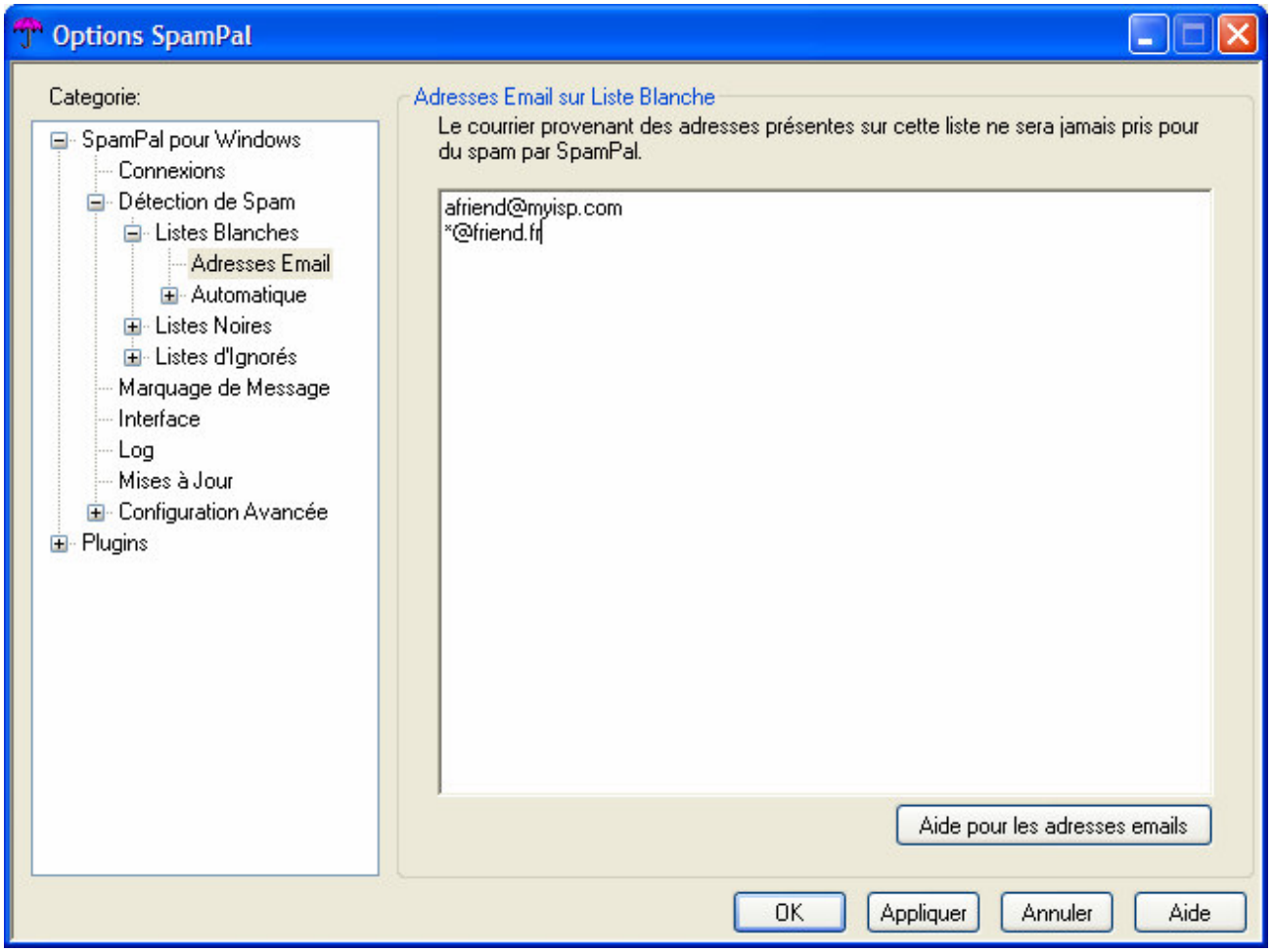
> **Note 1:** Vie privée : liste blanche automatique smtp

Si vous utilisez cette possibilité, spécialement dans un bureau, comme cela va enregistrer toutes les adresses de messages sortants, cela pourrait constituer une atteinte à la vie privée (au Royaume-Uni, vous devez prévenir une personne si vous placez son adresse dans un fichier), ou la constitution d'un fichier (soumis à la loi française "Informatique et libertés")

c) utiliser le menu **Ajouter à la liste blanche** sur l'icône de SpamPal dans la barre des tâches: pour ajouter manuellement à la liste blanche, vous pouvez la taper manuellement, ou la copier :



d) Vous pouvez utiliser cette procédure pour exporter **automatiquement** vos contacts de Outlook Express ou vous pouvez utiliser la page des **adresses email en liste blanche** de SpamPal, pour ajouter manuellement vos adresses email :



Note 2: Entêtes auxquels la liste blanche est comparée

La fonction liste blanche ne regarde que dans certains entêtes de vos emails.

Actuellement, ce sont : **From:**, **Reply-To:**, **Sender:, Mailing-List:** et **Return-Path**:

Au départ, vous remarquerez que l'utilisation de SpamPal rend la récupération du courrier un peu plus longue. C'est parce que SpamPal doit vérifier la présence de chaque adresse dans chaque liste DNSBL (liste noires publiques) pour voir quels emails viennent d'un spammer.

Néanmoins, grâce à sa fonction liste blanche automatique, SpamPal va rapidement apprendre qui vous envoie beaucoup de messages, et va les ajouter à une liste des émetteurs de confiance. Parce qu'ils sont de confiance, SpamPal ne perd pas de temps à les vérifier dans les listes DNSBL. Pour ceux-là, plus vous utilisez SpamPal, plus il deviendra rapide.

Vous pouvez trouver d'autres trucs et astuces pour optimiser SpamPal ici.
Ceci termine l'installation et la configuration de SpamPal.

::Début::

Contenu > Programmes Antivirus

Quelques filtres anti-virus ont besoin de se situer entre votre programme email et votre serveur de mail, juste là où se trouve SpamPal.

Il n'y a en fait aucune raison qu'ils ne le puissent pas; vous devez juste les mettre en série afin qu'ils puissent récupérer le courrier au travers de SpamPal au lieu de directement, puis votre programme email récupère le courrier à travers le filtre anti-virus.

Utiliser SpamPal avec des logiciels anti-virus

- Norton 2002/2003
- Norton 2001

Ces instructions devraient vous permettre de combiner SpamPal avec les fonctions de vérification anti-virus des emails de Norton Antivirus 2002

Commençons...

Configuration de Norton
Grâce à quelques changements effectués par les gens de Symantec, il n'y a aucune configuration additionnelle à effectuer pour utiliser SpamPal avec Norton Antivirus 2002 & 2003.

Installez juste SpamPal normalement et tout devrait fonctionner parfaitement!

Note 1: Time Out

Parfois vous allez lire des entêtes supplémentaires ajoutés à vos emails, comme :

X-Symantec-TimeoutProtection:0
X-Symantec-TimeoutProtection:1

Quand Norton Anti-Virus (et SpamPal) traite un grand message, il doit traiter tout le corps du message (pas seulement les entêtes).

Là où SpamPal envoie un octet de l'entête à la fois au programme email (un signal de maintien de la connexion), Norton voit cela et essaye de générer un entête supplémentaire: X-Symantec-TimeoutProtection:0 Il crée ces entêtes en séquence, changeant le numéro à la fin, comme un moyen de maintenir le flux de données pendant qu'il traite une grosse pièce jointe.

Donc, si vous avez de tels entêtes, cela signifie que l'intervalle de temps entre les paquets de maintien de la connection, est toujours plus long que le réglage timeout de votre programme email, vous devriez essayer de l'augmenter.

Vous pouvez aussi essayer d'aider Norton, en utilisant juste une DNSBL, par exemple SpamCop, et en réglant le délai sur les requêtes DNSBL à une valeur faible, par exemple 10 secondes.

Note 2: Mise à jour depuis NAV 2000

Bien qu'il n'y ait rien de spécial à régler pour Norton 2002, il semble que quelques utilisateurs mettent à jour depuis Norton 2000, sans désinstaller correctement le proxy POP3 de Norton 2000. Ils obtiennent donc une erreur **port indisponible** sans savoir pourquoi.

Le conseil dans ce cas est de vérifier que vous avez désinstallé p**roprement la précédente version de** Norton.

::Début::

Contenu > Antivirus > Norton 2001

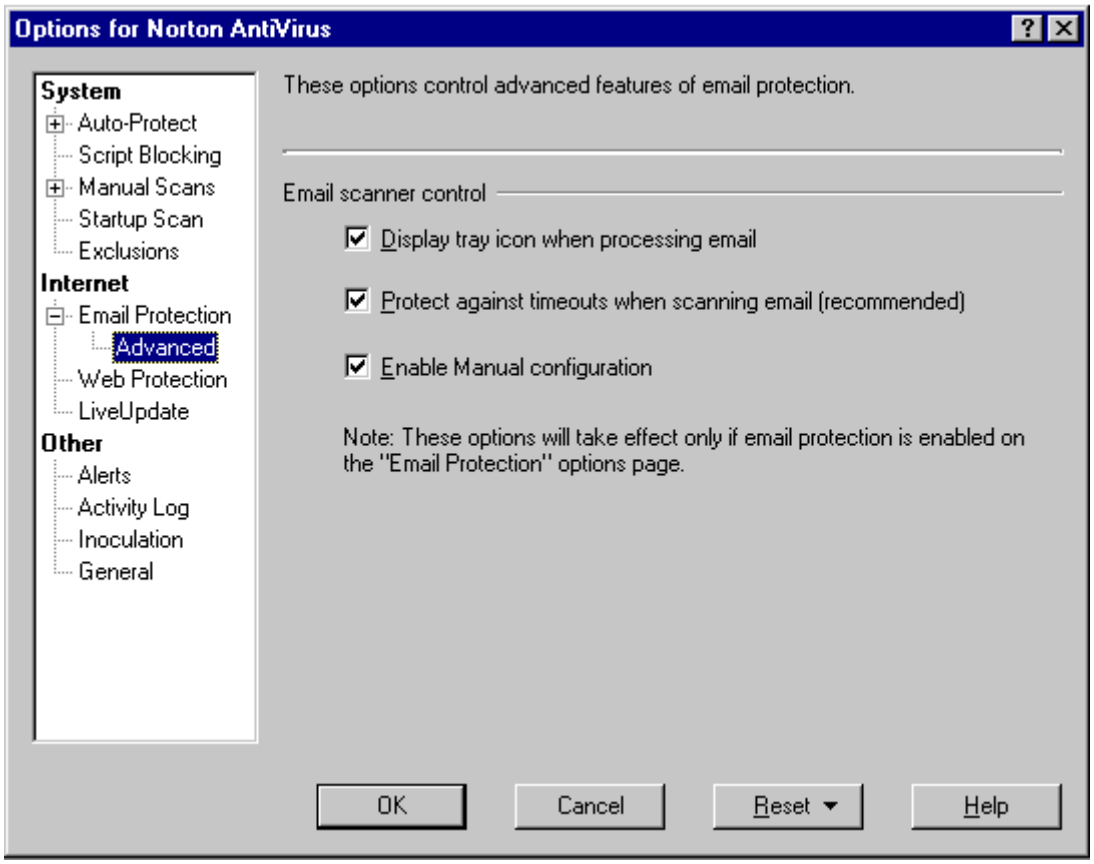
Les instructions suivantes devraient vous permettre d'utiliser en même temps SpamPal et les fonctions de contrôles anti-virus de Norton Antivirus 2001. Elles pourraient aussi s'appliquer à des versions précédentes de f Norton Antivirus.

Les utilisateurs de Norton Antivirus 2002 se rapporteront à cette page.

Commençons...

Configuration de Norton

1. Assurez-vous que Norton Antivirus est installé



Installation de SpamPal

Installez SpamPal normalement, en suivant les instructions spécifiques à votre programme email.

Installation de votre programme email

Configurez dans votre programme email les paramètres de votre compte de la manière suivante :

Utilisateur:
`username/pop.isp.fr  (et non username@pop.isp.fr)`
Serveur POP3:
`127.0.0.1`

Alors ca marche, mais vous n'êtes pas protégé par Norton.

Aller alors dans Norton qui dit que le compte n'est plus protégé, et lui demander alors (par le menu Norton) de le mettre en protection.
A la fin de l'opération, on se retrouve ainsi :

Utilisateur:
`username/pop.free.fr/localhost`
Serveur POP3:
`pop3.norton.antivirus`

Aller dans SPAMPAL options -> Connexions et relever le port que SpamPal a affecté à POP3 tous serveurs, et retourner dans le paramétrage des comptes de messagerie (onglet avancé) et mettre comme numéro de port du serveur de courrier entrant (POP3) le numéro de port relevé précédemment dans SPAMPAL.

Voilà ! les courriers sont alors filtrés successivement (et dans l'ordre) par Norton antivirus, puis par SPAMPAL.

Et... ca marche enfin. Ouf !!!

::Top::

Pour l'utilisation d'un firewall avec SpamPal, vous avez normalement besoin de changer quelques paramètres du firewall, afin de le faire fonctionner normalement.

Ports du Firewall

Si vous utilisez un firewall, il est souvent utile de connaître quels ports SpamPal utilise par défaut:
110 est le port par défaut pour POP3,
143 est le port par défaut pour IMAP4.
25 est le port par défaut pour SMTP

Le port 80 sera utilisé pour la vérification des mises à jour (bien qu'il utilise un proxy HTTP s'il y en a un spécifié dans IE et utilise alors les ports 80/8080/3128).

SpamPal utilise les appels Windows pour émettre les requêtes DNS, ce qui signifie soit des paquets UDP émis sur le port 53, soit des connections TCP sur le port 53.

Si vous avez besoin de connecter SpamPal à d'autres programmes, il est possible d'utiliser les ports 1101, 1102, 1103 sans aucun problème.

Une bonne liste de l'utilisation des ports peut être trouvée ici et un bref résumé dans le glossaire ici.

Contenu > Serveurs locaux de messagerie

SpamPal est conçu comme un filtre personnel de messagerie qui fonctionne sur la même machine que votre programme email.

Néanmoins, SpamPal peut être utilisé sur un réseau local (LAN : local area network) avec un serveur local de messagerie pour fournir une protection contre les spams à plus d'un utilisateur.

SpamPal est écrit pour fonctionner avec les protocoles email standards. Certains services comme AOL, WebTV, Juno et d'autres sites webmail comme Hotmail et Yahoo, utilisent leur propre format propriétaire de messagerie, qui ne respectent pas les standards. Vous ne pouvez pas utiliser directement SpamPal avec ce type de services. Mais en utilisant des logiciels tiers-partie, vous pouvez le faire!

Contenu > Configurations de base

La configuration de SpamPal peut paraître compliquée vu le nombre de paramètres disponibles. Voici par conséquent quelques configurations issues de l'expérience des utilisateurs.

N'hésitez pas à proposer des améliorations ou d'autres configurations de base sur le forum de SpamPal.

Index

1. Configuration pour connexions bas débit

Dans un premier temps, pour Outlook Express, vous écrivez une "règle" du type : - Quand l'en-tête "sujet" contient "**SPAM**", ne pas télécharger. Cette règle ne fonctionnera que si vous n'avez pas modifié le texte ajouté par défaut par SpamPal ("**SPAM**"), si c'est le cas adaptez selon votre texte.

Pour d'autres clients de mail, voyez les options de filtrage disponibles. Certains clients ne permettront pas la suppression directe sur le serveur sans téléchargement de la totalité du message (selon la manière dont ils utilisent le protocole POP3). Mais encore une fois, cela marche parfaitement avec O.E. et beaucoup d'autres logiciels qui utilisent la commande "TOP"!

De temps à autre faire le ménage dans les messages laissés sur le serveur via un accès de type WebMail.

Puis, lorsque vous aurez vérifié que les DNSBL utilisées ne sont pas trop agressives (très peu de messages légitimes marqués à tort), vous pouvez alors remplacer "ne pas télécharger" par "détruire sur le serveur".

Attention : il est risqué de "détruire sur le serveur", les listes noires étant souvent agressives. Faites donc bien attention si vous décidez d'utilisez ce réglage.

::Début::

Contenu > Installation

SpamPal demande un peu de travail lors de l'installation, mais cela ne devrait pas vous prendre plus de dix minutes. Une fois fini, vous n'entendrez plus parler de lui... et du spam.

L'installation comporte sept étapes :

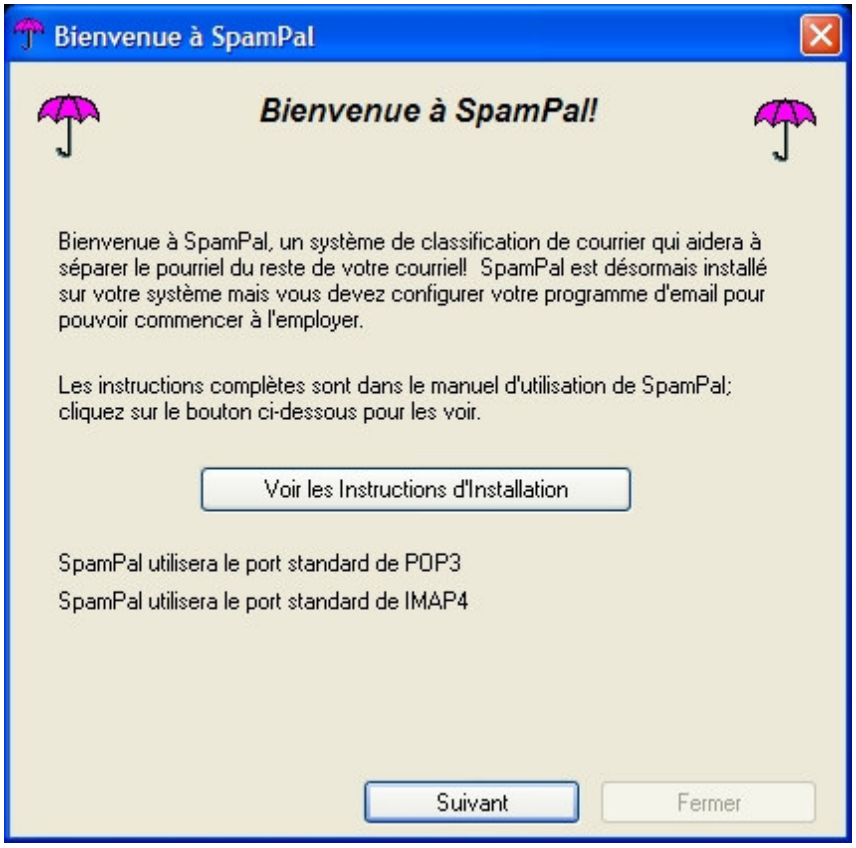
Commençons...

1. Installation de SpamPal

Télécharger SpamPal et lancez l'installation en double-cliquant sur l'icône du programme d'installation de SpamPal (`spampal.exe ou spampal-***.exe`) et suivez les instructions affichées à l'écran. A la fin de l'installation, SpamPal se lance, montrant son icône (un parapluie rose) dans votre barre de tâches.

Si cette installation est une mise à jour, la configuration existante est conservée et le processus est terminé. Sinon, c'est à dire pour une nouvelle installation, suivez les instructions ci-dessous.

La première fois que SpamPal se lance, vous allez voir l'écran de bienvenue suivant:

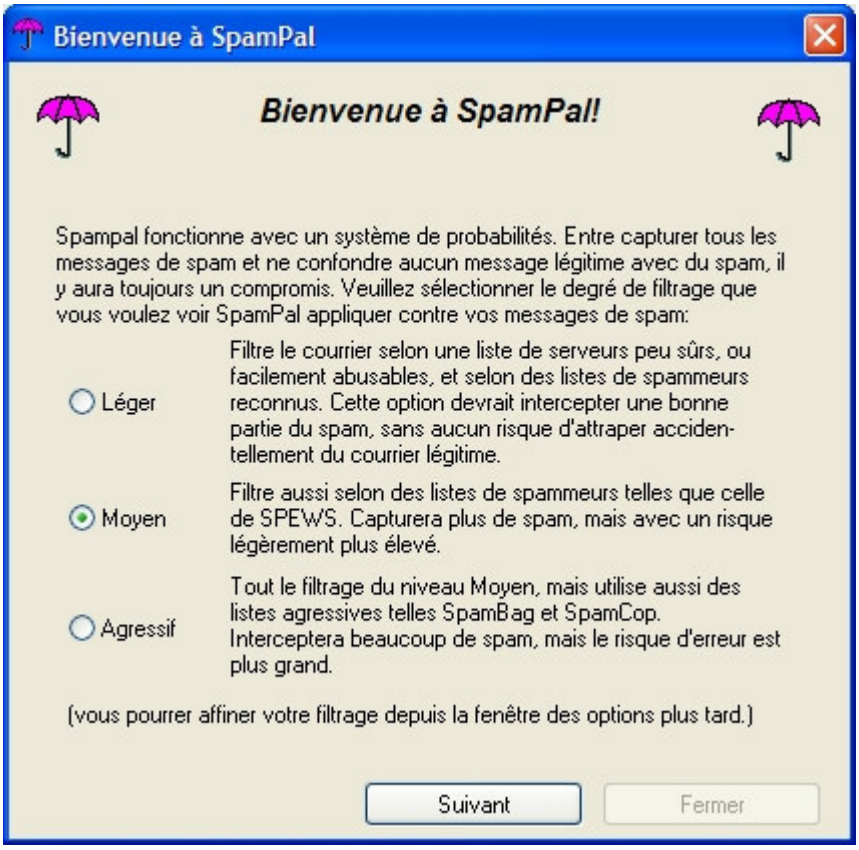


Note 1: Ports Standards

Vous pouvez, ici, avoir un message d'erreur disant que SpamPal ne peut écouter le port POP3 standard. Il ne faut pas s'inquiéter; notez juste le numéro de port que SpamPal vous donne et continuez à suivre ce guide.

Ce message signifie que SpamPal utilise le Port 1110 au lieu du 110. Vous n'avez besoin besoin de le lui dire parce que SpamPal sait déjà qu'il utilise le port 1110. A la place, vous devrez dire à votre programme email (par exemple Outlook Express) d'utiliser le port 1110 au lieu du 110.

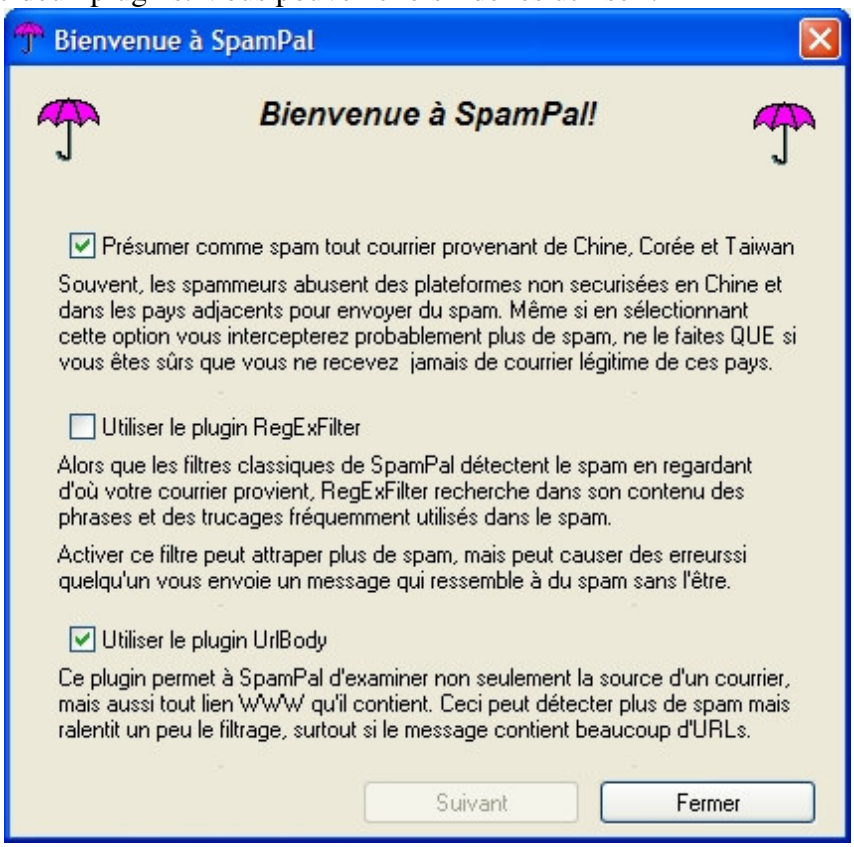
Ensuite, vous devez choisir le niveau de filtrage avec lequel SpamPal va commencer, par défaut, le niveau Moyen est choisi, néanmoins, si vous êtes réellement nerveux, choisissez le niveau Agressif.



Note 2: Stratégie de filtrage

Le niveau que vous choisissez, peut être modifié ensuite, si le niveau choisi ne filtre pas assez ou filtre trop.

L'écran suivant vous invite à considérer comme spam tout courrier provenant de certains pays. Cette version de SpamPal est fournie avec deux plugins. Vous pouvez choisir de les utiliser :



Note 3: Blocage d'un pays tout entier

Si vous appartenez à un groupe international ou recevez beaucoup de mail légitimes de Chine, Corée ou Japon, n'oubliez pas de **décocher** cette option, tous les mails provenant de ces pays seraient marqués comme spam.

Une fois que vous avez mis sur pied une bonne liste blanche, vous pourrez toujours revalider la possibilité de bloquer certains pays.

Une fois que SpamPal est installé, il se lance tout seul et vous devriez voir l'icône en forme de parapluie de SpamPal dans la barre des tâches :

::Début::

2. Configuration de SpamPal

Tout ce dont vous pouvez avoir besoin pour une configuration avancée de SpamPal, se trouve ici.

::Début::

3. Configuration de votre programme email

Maintenant que vous avez réglé SpamPal, vous devez configurer votre programme email, de telle manière que tous les emails soient reçus au travers du proxy POP3 / IMAP4 de SpamPal, et non directement depuis le serveur POP3 de votre fournisseur d'accès.

Vous trouverez ici des instructions spécifiques à votre programme email, cependant, elles sont toutes basées sur les instructions génériques suivantes. Vous devrez changer les deux réglages suivants dans la configuration de votre programme email :

Avant d'utiliser SpamPal	
	Exemple 1
Nom du serveur POP3 entrant: **pop3.yourisp.com**	Nom du serveur POP3 entrant: localhost
Utilisateur: name@surname	Utilisateur:name@surname**@pop3.yourisp.com**
	Example 2
Nom du serveur POP3 entrant: **mail.yourisp.com**	Nom du serveur POP3 entrant: 127.0.0.1
Utilisateur: my_login_name	Utilisateur: my_login_name**@mail.yourisp.com**
	Example 3 (using LAN IP Address)
Nom du serveur POP3 entrant: **192.168.1.1**	Nom du serveur POP3 entrant: 127.0.0.1
Utilisateur: my_login_name	Utilisateur: my_login_name**@192.168.1.1**

Note 1: Noms de serveur
Le "Nom du serveur POP3 entrant", ci-dessus, peut, selon votre programme email aussi être appelé : serveur mail entrant, serveur POP3, Nom d'utilisateur POP3 ou Nom du compte.

Il y a aussi deux façons de préciser le nom du serveur local, qui veulent dire la même chose toutes les deux (mais, avec certains programmes, une seule fonctionne): localhost ou 127.0.0.1

Commencez par localiser ces deux valeurs, puis notez leur valeur. Vous devez ensuite ajouter le **nom du serveur POP3 entrant** au **nom d'utilisateur**, en séparant les deux valeurs par une @.

Note 2: Si le nom du compte comporte déjà un @

Vous pouvez continuer sans problème, SpamPal sait gérer les noms de compte qui contiennent 2 @ sans difficulté.

Note 3:Si le serveur nécessite une authentification (case cochée sous "Serveur de messagerie pour courrier sortant)...

Cliquez sur le bouton Paramètres...**.** situé à coté. Sélectionnez Ouvrir la session en utilisant et entrez votre nom d'utilisateur et mot de passe originaux, c'est à dire, ceux que vous aviez avant de les modifier pour installer SpamPal.

Note 4: Si votre serveur POP3 n'utilise pas le port POP3 par défaut (110)...

Ajoutez le numéro de port au nom du serveur dans la case "Nom du compte" en utilisant ":". Par exemple, si BlueYonder utilisait le port **8090** pour leur serveur POP3, j'aurais un nom d'utilisateur de la forme `jf004d7582@pop3.blueyonder.co.uk:8090`

Note 5: Utilisateurs de Netscape (et tous ceux qui sont basés sur lui)

Vous devriez utiliser un '%' plutôt qu'une '@', c'est à dire : jjf%pop.clara.net.
Les personnes utilisant d'anciens versions d'autres programmes peuvent aussi avoir à utiliser un '%'.

Maintenant changez le **serveur** POP3 pour mettre 127.0.0.1. Si votre programme refuse d'utiliser cette valeur, essayez localhost.

Note 6: Si vous avez eu un message **d'erreur disant que SpamPal ne peut écouter le port POP3 standard**

Vous devrez changer le port que votre programme email va utiliser pour réaliser la connection POP3. La manière de réaliser ce réglage diffère selon les programmes, mais cela devrait être quelque part près de là où vous avez réglé le nom du serveur POP3, peut-être dans un onglet "Avancé"? Changez cette valeur pour mettre celle que vous avez noté plus tôt.

Si vous utilisez plus d'un compte email POP3, répétez cette étape pour chaque compte.

Maintenant, cliquez sur Envoyer/Recevoir dans votre programme email, vous devriez voir l'icone de SpamPal dans la barre des tâches s'animer :

Note 7: Firewalls

Votre programme firewall va probablement vous informer que SpamPal.exe essaye d'accéder à internet, ceci est **tout à fait normal** et vous devriez lui dire d'autoriser Spampal à accéder à internet.

SpamPal va aussi, de temps en temps, accéder à sa propre page de démarrage pour vérifier les mises à jour, encore, votre firewall peut vous avertir à ce propos, là encore, vous devriez lui dire d'autoriser Spampal à accéder à internet.

L'étape quatre ci-dessous traite des réglages nécessaires pour un firewall

::Début::

4. Création de filtres ou de règles de messages

Vous devriez maintenant recevoir normalement des emails. Néanmois, si SpamPal pense qu'un message est un spam, alors la ligne Objet : commencera par ****SPAM**** et un entête supplémentaire sera ajouté à votre message: **X-SpamPal: SPAM**

Note: Example Spam Email

From: i_am_a@spammer.co.uk
To: yourname@yourisp.co.uk
Subject: ****SPAM**** FREE $ FOR YOU !!!
Date: Tue, 24 Jun 2003 13:30:40 +0100
X-SpamPal: SPAM SPCOP xxx.xxx.xxx.xxx

De manière à vous aidez à séparer ce spam de votre courrier normal, vous devriez configurer une règle de message, dans votre programme email, pour déplacer ces messages marqués vers un dossier **spamtrap**.

Commencez par créer ce dossier, vous pouvez l'appeler comme vous le souhaitez, mais, pour les besoins de ce guide, je considère que vous l'avez appelé **spamtrap**. La façon exacte de créer un dossier dépend de votre programme email.

Maintenant créez un nouveau filtre pour déplacer tout courrier entrant pour lequel l'entête **X-SpamPal: contient SPAM** dans le dossier **spamtrap**. Là encore, la manière de créer des filtres dépend de votre programme.

Si votre programme email n'autorise pas le filtrage sur des ent^tes arbitraires, utiliser le filtrage sur les lignes objet contenant **SPAM** aura le même effet.

Pour l'instant, nous avons uniquement donné des instructions générales, qui devraient être suffisantes pour faire travailler SpamPal avec n'importe quel programme email, des instructions spécifiques peuvent être trouvées ici.

::Début::

5. Configuration de programmes anti-Virus & Firewalls

Quelques filtres anti-virus ont besoin de se situer entre votre programme email et votre serveur de mail, juste là où se trouve SpamPal.

Il n'y a en fait aucune raison qu'ils ne le puissent pas; vous devez juste les mettre en série afin qu'ils puissent récupérer le courrier au travers de SpamPal au lieu de directement, puis votre programme email récupère le courrier à travers le filtre anti-virus.

Suivez les pages suivantes pour plus de détail sur la manière de configurer votre logiciel:

Utiliser SpamPal avec un logiciel anti-virus
Utiliser SpamPal avec un firewall

::Début::

6. Ajout de vos amis et contacts en liste blanche

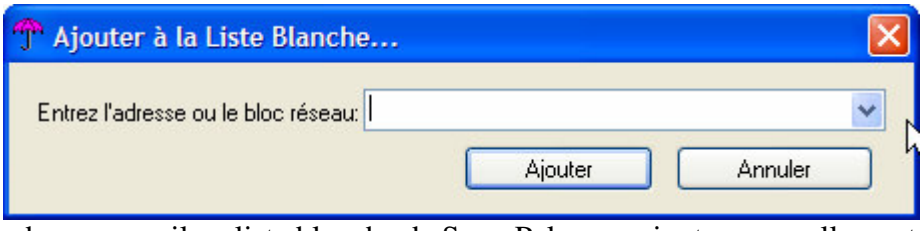
Afin d'accélérer le traitement de vos emails et d'éviter que SpamPal marque les emails de vos amis ou contacts comme spam, c'est une bonne idée à ce point de l'installation de mettre en liste blanche l'adresse de tous vos contacts importants.

Pour cela, il y a quatre manières de faire :

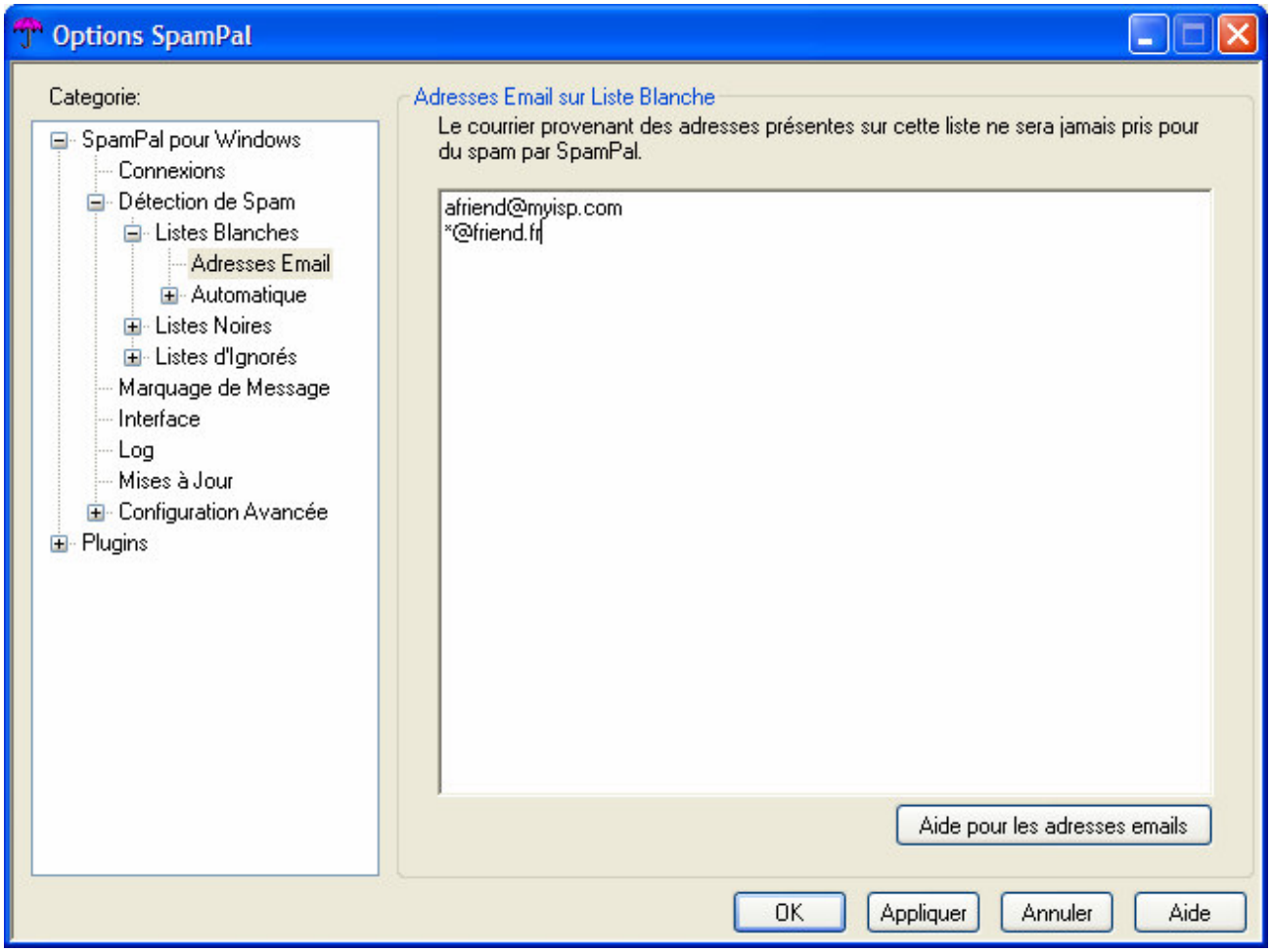
a) Utiliser la liste blanche automatique pop3 : cela va ajouter à la liste blanche les adresses dont vous recevez fréquemment du courrier non-spam,
b) Utiliser la liste blanche automatique smtp : si configurée en 3.3, elle ajoute à la liste blanche les adresses auxquelles vous envoyez du courrier,

Note 1: Vie privée : liste blanche automatique smtp
Si vous utilisez cette possibilité, spécialement dans un bureau, comme cela va enregistrer toutes les adresses de messages sortants, cela pourrait constituer une atteinte à la vie privée (au Royaume-Uni, vous devez prévenir une personne si vous placez son adresse dans un fichier), ou la constitution d'un fichier (soumis à la loi française "Informatique et libertés")

c) utiliser le menu Ajouter à la liste blanche sur l'icône de SpamPal dans la barre des tâches: pour ajouter manuellement à la liste blanche, vous pouvez la taper manuellement, ou la copier :



d) utiliser la page des adresses email en liste blanche de SpamPal, pour ajouter manuellement vos adresses email :



Note 2: Entêtes auxquels la liste blanche est comparée

La fonction liste blanche ne regarde que dans certains entêtes de vos emails.

Actuellement, ce sont : From:, Reply-To:, Sender:, Mailing-List: et Return-Path:

Ceci termine l'installation et la configuration de SpamPal.

::Début::

7. Utilisation des listes noires

S'il vous plait, n'utilisez pas de listes noires massives avec SpamPal, en particulier, pas celles de sites à usage général. Celles-ci sont prévues pour détecter le spam dans des systèmes qui n'utilisent pas les listes noires DNS, les expressions régulières ou d'autres méthodes avancées de détection du spam.

Utiliser une liste noire massive n'est généralement pas utile, puisque les spammers créent généralement leur adresse et n'utilisent jamais la même adresse deux fois. Si vous recevez régulièrement du courrier depuis l même adresse et, pour une raison ou une autre, elle n'est pas signalée dans les listes noires publiques, alors il peut être utile de l'ajouter à votre liste noire personnelle.

Cependant, la plupart des utilisateurs n'ont que quelques adresses dans leur liste noire. Si vous en avez de trop, vous ralentirez SpamPal de façon significative, et vous vous ajoutez du travail sans obtenir de résultat significatif.

Ce raisonnement s'applique aussi aux programmes, comme Outlook et Outlook Express qui offrent la possibilité de

bloquer les émetteurs par adresse email (**appelée Emetteurs bidon/Emetteurs de contenu pour adulte**). Il vaut généralement mieux arrêter d'utiliser ces fonctions et laisser SpamPal faire son travail.

Le premier moyen de réduire le spam avec SpamPal est d'ajuster les listes noires DNS. En utilisant relays.osirusoft.com, Easynet et SpamCop devraient intercepter 90% du spam pour la plupart des utilisateurs. Si vous ne parvenez pas à atteindre ce taux de détection, ou voulez obtenir un taux supérieur, faites-le nous savoir et nous vous ferons des suggestions pour vous aider à augmenter ce succès.

::Début::

Contenu > Utiliser SpamPal

Index

1. Comment démarrer

Par défaut, SpamPal s'installe dans votre répertoire de démarrage et sera toujours présent, dès que Windows sera lancé.

Vous pouvez évidemment l'enlever du répertoire de démarrage, afin de gagner du temps au démarrage de votre PC. Néanmoins, vous ne devez pas oublier de le démarrer, avant de vérifier votre courrier. Sinon, vous aurez des erreurs de connexion au serveur de courrier.

Si vous utilisez une liaison par modem (ligne téléphonique non ADSL), vous pourriez trouver utile un produit comme NetLaunch.)

Au démarrage, SpamPal fait apparaître son icône dans la barre des tâches, sous la forme d'un parapluie rose, qui indique que SpamPal fonctionne :

Chaque fois que vous vérifiez votre courrier, votre programme email va, de façon invisible, utiliser SpamPal (pendant ce processus, vous pourrez voir le parapluie tourner dans l'icône).

Ensuite, les règles ou filtres de votre programme email vont déplacer tout message que SpamPal aura marqué avec ****SPAM****, dans votre dossier **spam**, ce qui gardera votre boite de réception propre!

Bien que SpamPal ne trouve et marque pas **tous** les spams que vous recevez, cependant, vous pouvez estimer qu'il va en attraper au moins 90%, en utilisation normale. Si vous voulez gagner quelques % de plus, vous pouvez installer un des nombreux plugins de SpamPal, qui peuvent être obtenus ici.

De temps en temps, peut-être une fois par semaine, vous devriez vérifier dans votre dossier spamtrap qu'aucun message légitime, un de ceux que vous vouliez recevoir, n'a pas été par erreur aiguillé ici, puis détruire les autres.

SpamPal est très configurable et la plupart des utilisateurs seront satisfaits des réglages par défaut. Si, néanmoins, vous avez besoin de changer ces réglages, vous pouvez adapter SpamPal à vos propres besoins en utilisant la fenêtre Options.

Pour accéder à la fenêtre Options, cliquez droit sur l'icône de SpamPal, et choisissez Options.

::Début::

2. Ajouter vos amis ou contacts en liste blanche

Afin d'accélérer le traitement de vos emails et d'éviter que SpamPal marque les emails de vos amis ou contacts comme spam, c'est une bonne idée à ce point de l'installation de mettre en liste blanche l'adresse de tous vos contacts importants.

Pour cela, il y a quatre manières de faire :

a) Utiliser la liste blanche automatique pop3 : cela va ajouter à la liste blanche les adresses dont vous recevez fréquemment du courrier non-spam,
b) Utiliser la liste blanche automatique smtp : si configurée, elle ajoute à la liste blanche les adresses auxquelles vous envoyez du courrier,

> **Note 1:** liste blanche automatique et marquage **SPAM**
>
> La fonction liste blanche automatique ne va ajouter **que** les adresses qui n'auront **pas** été marquées **SPAM**

> **Note 2: Option "Exclusions" de la liste blanche**

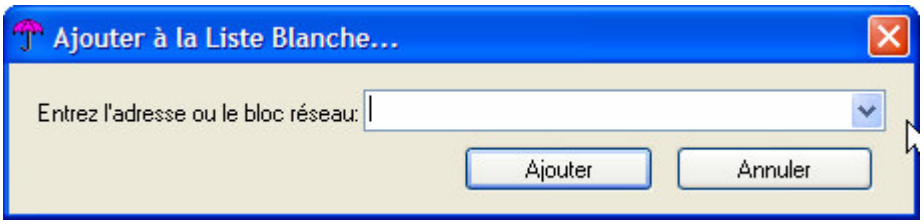
De temps en temps, un spammer peut utiliser l'adresse de quelqu'un qui est dans votre liste blanche automatique - un collègue ou une autre de vos adresses email, par exemple. D'un coté, vous ne voulez pas ajouter l'adresse de cette personne dans la liste noire parce qu'elle vous envoie beaucoup d'emails légitimes, d'un autre coté, vous ne voulez pas qu'elles finissent dans la liste blanche automatique et court-circuitent les protections anti-spam de SpamPal.

En cliquant sur le panneau Exclusions, une fenêtre va apparaître et vous permettre de saisir les adresses de personnes qui ne doivent jamais être ajouter à la liste blanche automatique. Ajouter vos collègues, vos propres adresses, et vous n'aurez plus à vous inquiéter des spammeurs utilisant ces adresses pour contourner le filtrage de SpamPal. Vous pouvez même ajouter des domaines entiers - *@acme-widgets.com

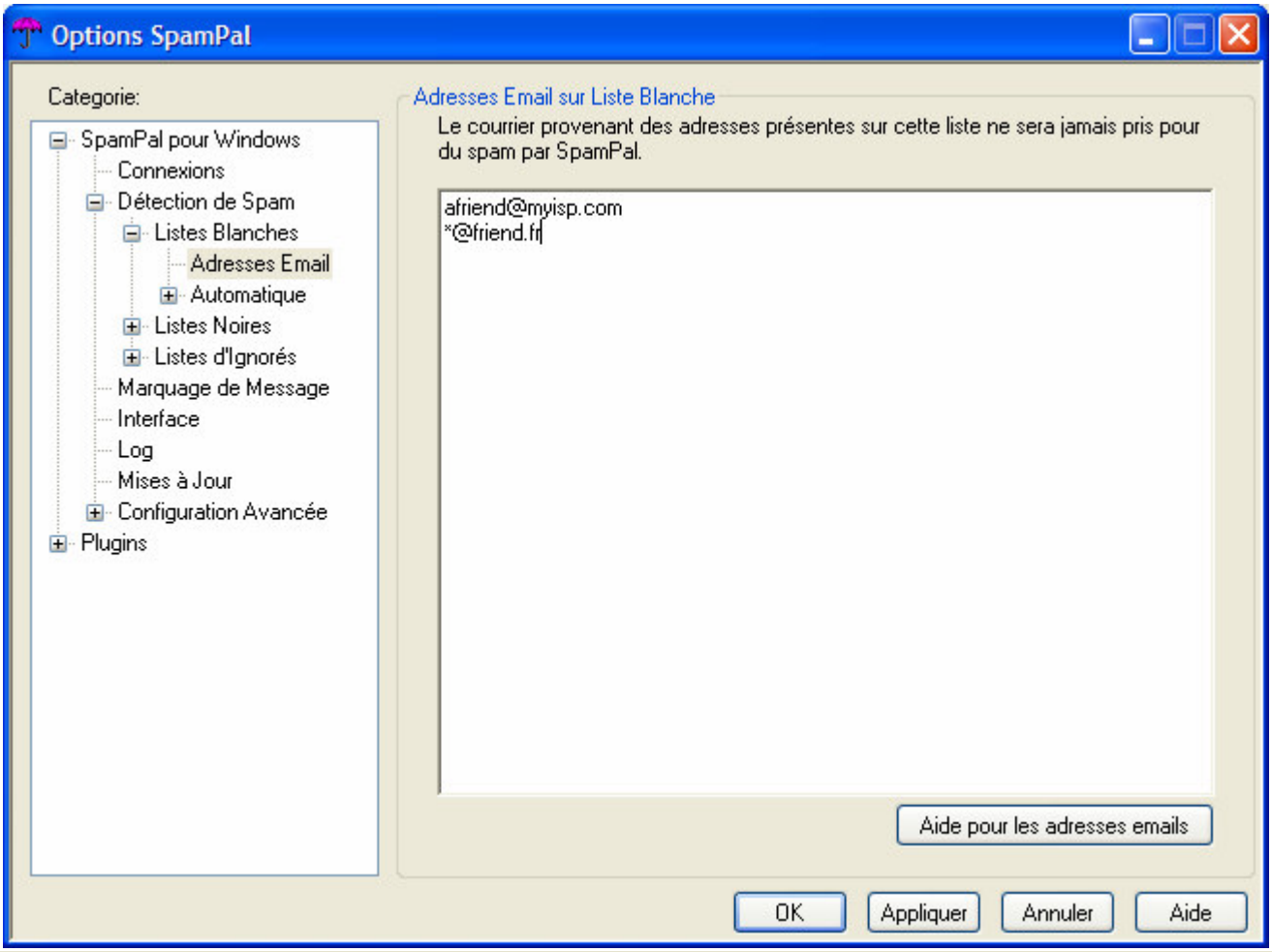
Note 3: Vie privée : liste blanche automatique smtp

Si vous utilisez cette possibilité, spécialement dans un bureau, comme cela va enregistrer toutes les adresses de messages sortants, cela pourrait constituer une atteinte à la vie privée (au Royaume-Uni, vous devez prévenir une personne si vous placez son adresse dans un fichier), ou la constitution d'un fichier (soumis à la loi française "Informatique et libertés")

c) utiliser le menu Ajouter à la liste blanche sur l'icône de SpamPal dans la barre des tâches: pour ajouter manuellement à la liste blanche, vous pouvez la taper manuellement, ou la copier :



d) utiliser la page des adresses email en liste blanche de SpamPal, pour ajouter manuellement vos adresses email :



Note 4: Entêtes auxquels la liste blanche est comparée

La fonction liste blanche ne regarde que dans certains entêtes de vos emails.

Actuellement, ce sont : From:, Reply-To:, Sender:, Mailing-List: et Return-Path:

Au départ, vous remarquerez que SpamPal ralentit un peu la récupération du courrier. C'est parce que SpamPal doit vérifier chaque adresse dans les listes DNSBL (listes noires publiques) pour voir quels emails viennent d'un spammer.

Cependant, grâce à sa fonction liste blanche automatique, SpamPal va rapidement apprendre qui vous envoie du courrier légitime, et les ajouter à une liste de correspondants de confiance. Parce qu'ils sont de confiance, SpamPal ne va pas perdre de temps à effectuer de vérifications dans les listes DNSBL pour ces messages et donc, plus vous utilisez SpamPal, plus rapide il sera.

Vous pouvez trouver plus de trucs et d'astuces pour optimiser SpamPal ici.

::Début::

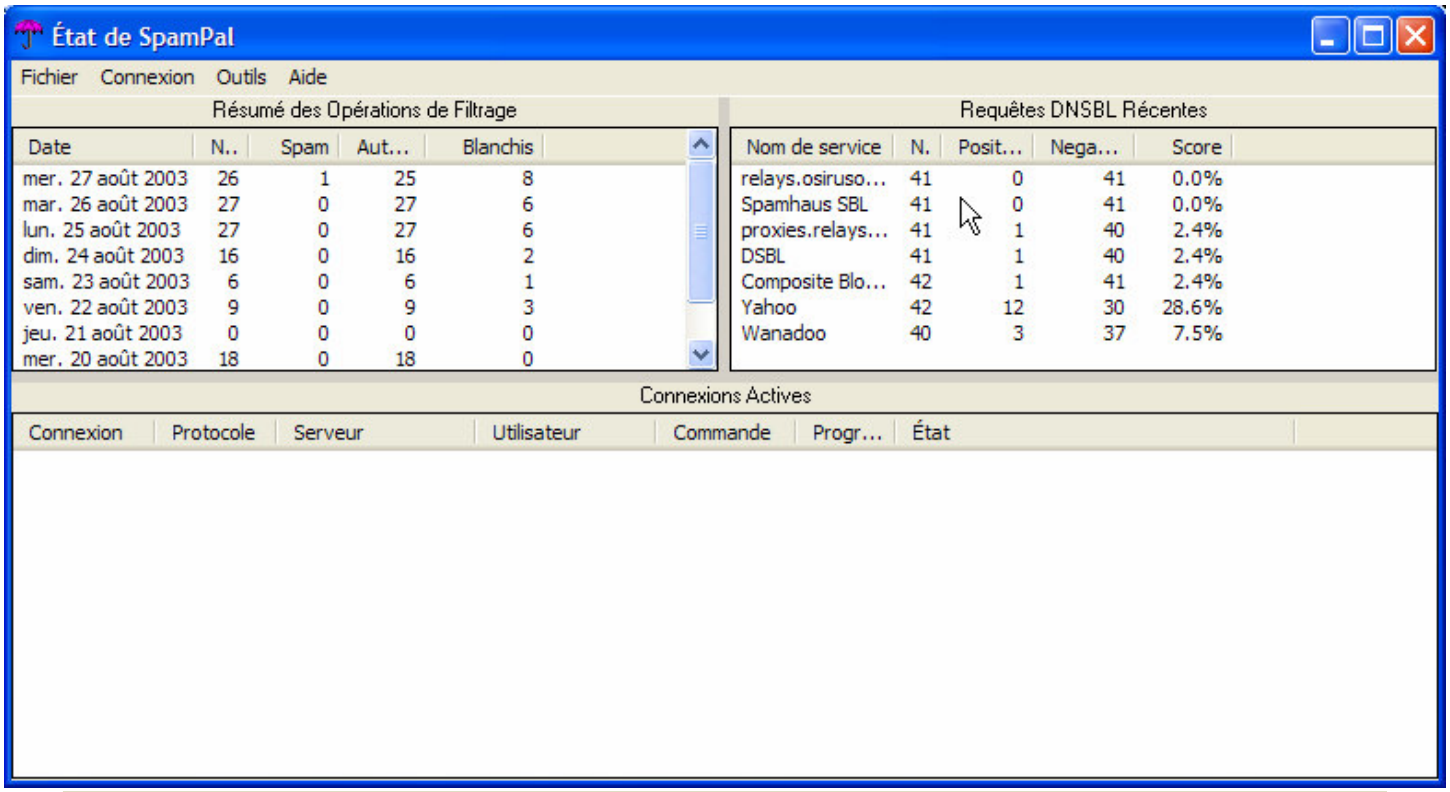
3. La fenêtre État de SpamPal

En utilisant la fenêtre État de SpamPal (cliquez droit sur l'icône de SpamPal dans la barre des taches puis sélectionnez **État**), vous pourrez voir quelles listes DNSBLs vous utilisez et quelle a été leur efficacité au cours des sessions récentes.

Si vous regardez les statistiques de la fenêtre État de SpamPal, vous pourrez voir les taux de détection auquel parviennent les différentes listes DNSBLs que vous avez utilisé dans de récentes requêtes. Vous remarquerez sans doute que certaines listes obtiennent régulièrement des taux importants, 20-50%, et d'autres, des taux plus faibles, voire même aucune détection.

Désélectionner les listes ayant des taux faibles va probablement accélérer la vitesse sans affecter notablement votre capacité de détection des spams.

Par exemple, dans la fenêtre ci-dessous, il semble que Spamhaus-RBL n'a détecté que peu de spam au cours des sessions récentes. Cela pourrait être une bonne idée de désélectionner cette liste, afin d'économiser du temps.



Note

Dans la fenêtre de droite, faites attention au terme "Résumé des opérations de filtrage". Ce n'est pas la même chose que "nombre de messages". Si votre programme email (Outlook Express par exemple) récupère d'abord un aperçu du message avant le message lui-même, cela fait deux opérations de filtrage, et chaque message sera conté deux fois.

::Début::

4. Que dois-je attendre de SpamPal?

Les questions - réponses qui suivent doivent absolument être lues afin de vous assurer que vous obtenez le maximum de SpamPal

Quelle proportion de spam Spampal devrait-il intercepter?

L'objectif est que Spampal intercepte **au moins** 90% du spam, sans intercepter de messages légitimes. Dans la pratique, vous pouvez probablement intercepter sans risque 95% du spam, et quelques personnes indiquent qu'elles parviennent à intercepter 99% ou plus du spam. Néanmoins, plus vous devenez agressif dans votre filtrage des emails, plus vous augmentez le risque d'intercepter par erreur un message légitime. Quelle que soit la qualité de

vos outils anti-spam, il y aura toujours un ou deux spams qui réussiront à passer tout de même sous la barrière. Soyez réalistes dans vos attentes.

Pourquoi ce message n'a-t-il pas été marqué comme spam?

Pour découvrir pourquoi un spam est passé au travers des filtres, vous devez regarder l'entête X-SpamPal du message et découvrir quelles raisons ont conduit à le laisser PASSer. Vous pouvez avoir accidentellement ajouter à votre liste blanche une adresse que vous vouliez ajouter à la liste noire. Il peut aussi ne pas vous donner de raison, indiquant qu'aucune des stratégies que vous aviez choisies ou des listes noires ne l'ont détecté comme spam. Quelqu'en soit la raison, l'entête X-SpamPal est le point de départ à examiner pour améliorer les performances en matière de détection de spam. Visitez cette page pour plus de détails sur les entêtes de SpamPal.

Pourquoi ce message a-t-il été marqué comme spam?

Pour découvrir pourquoi un message est marqué comme spam, vous devez regarder l'entête X-SpamPal du message et découvrir les raisons qu'il indique pour avoir marqué ce message comme SPAM. Vous pouvez avoir accidentellement ajouté à votre liste noire quelqu'un que vous vouliez ajouter à votre liste blanche ou, peut-être, une liste noire publique (DNSBL) que vous avez sélectionnée, semble être trop agressive et bloque trop de messages légitimes (parce que des fournisseurs d'accès amis avec les spammeurs ont aussi des clients qui ne spamment pas!). Quelque soit la raison, l'entête X-SpamPal est la clé pour trouver la solution, aussi visitez cette page pour plus de détails sur les entêtes de SpamPal et leur signification.

Dois-je continuer à ajouter des adresses dans la liste noire?

Non. S'il vous plait, n'utilisez pas de listes noires d'adresses email importante avec SpamPal, particulièrement pas celles de sites à but généraux. Elles sont conçues pour des systèmes de détection de spam qui n'utilisent pas les listes noires DNS, les expressions régulières ou d'autres méthodes avancées de détection du spam.

Utiliser une liste noire importante n'est généralement pas productif, car les spammeurs utilisent généralement une adresse qui n'est pas la leur et n'utilisent jamais la même adresse deux fois. Si vous recevez régulièrement du spam de la même adresse et que, pour une raison ou une autre, il n'est pas détecté par les listes noires publiques, alors et seulement dans ce cas, il peut être utile de l'ajouter à votre liste noire personnelle.

Néanmoins, la plupart des utilisateurs n'ont que quelques adresses dans leur liste noire. Si vous en avez de trop, vous allez ralentir le fonctionnement de SpamPal de façon significative, et vous ajouter beaucoup de travail sans parvenir à quelque chose d'utile.

Ce raisonnement s'applique aussi aux programmes email, comme Outlook et Outlook Express qui offrent la possibilité de bloquer certains émetteurs (**appelés émetteurs de spam**). Il vaut généralement mieux arrêter d'utiliser ces fonctions et laisser SpamPal faire son travail.

Le premier moyen de réduire le spam avec SpamPal est d'ajuster les listes noires DNS. En utilisant relays.osirusoft.com, Easynet et SpamCop devrait intercepter 90% du spam pour la plupart des utilisateurs. Si vous ne parvenez pas à un taux aussi important, ou voulez un taux plus important, faites-le nous savoir et nous pourrons vous faire d'autres suggestions pour vous aider à améliorer ce succès.

Dois-je utiliser toutes les DNSBLs?

Non, vous n'avez besoin que de **trois ou quatre** bonnes DNSBLs pour obtenir de bons résultats. En ajouter plus ne va pas forcément améliorer les choses. Si vous les choisissez toutes, c'est un massacre inutile. C'est aussi une consommation de ressources qui pourraient servir à autre chose. Les personnes qui fournissent ces DNSBLs le font gratuitement et nous aimerions tous que cela le reste.

Certaines DNSBLs fonctionnent mieux que d'autres, et cela dépend aussi de l'endroit où vous vous trouvez dans le monde. Les bonnes listes à but général sont SpamCop, Easynet Blackholes et NJABL. Si vous regardez les statistiques de l'écran État de SpamPal, vous pourrez voir le taux de détection obtenu par chaque liste DNSBL que vous avez utilisé lors des requêtes récentes. Vous remarquerez probablement que certaines DNSBLs donnent régulièrement des scores élevés, 40-50%, et d'autres ont des taux de détection plus faibles, voire même nul. En désélectionnant les listes à taux faible, vous améliorerez probablement la vitesse de traitement sans affecter votre capacité à détecter le spam.

Je ne détecte pas tout le spam : Comment améliorer ma sélection DNSBL?

Vous pourriez regarder à la liste des pays. En ce moment, beaucoup de spam semble transiter par des serveurs situés en Chine. Si vous êtes **absolument certain** que vous ne **recevrez pas de courrier légitime de Chine**, vous pouvez sélectionner ce pays dans la liste noire des pays. Cependant, vous devez faire **très attention** lorsque vous bloquez un pays, par exemple : si vous faites partie d'une entreprise internationale, vous ne voudrez probablement pas utiliser la fonction de blocage par pays!

Une cause plus probable de faible taux de performance des DNSBL est que vous vérifiez votre courrier **trop souvent**. Nous nous sommes aperçu que lorsqu'une vague de spam commence à se répandre, il faut environ 30 minutes pour que les adresses IP coupables commencent à apparaître dans les listes DNSBL. Si vous vérifiez votre courrier à un intervalle d'une minute, vous allez probablement télécharger votre courrier avant que les listes DNSBL aient eu une chance de réagir.

Modifiez les réglages de votre programme email pour ne vérifier et télécharger votre courrier qu'à des intervalles de 30 minutes ou plus, voire même de ne le vérifier que manuellement, et vous devriez alors constater une amélioration de la performance des DNSBL. Malgré ce que pensent souvent certains, le ciel ne vous tombera pas sur la tête si nous ne recevez pas les emails qui vous sont envoyés dans la même minute où on vous l'a envoyé.

Vous devriez aussi vérifier le temps de cache des vérifications DNSBL. La mise en cache améliore la vitesse mais peut mener à des résultats un peu moins performants. A moins que la vitesse ne soit un problème pour votre connexion, les meilleurs résultats seront obtenus lorsque SpamPal est configuré pour se souvenir des **résultats** positifs (Spam) pendant trois jours, et des **résultats négatifs** (courrier légitime) pendant zéro jour zéro heure. Ces réglages peuvent être trouvés dans le panneau "Configuration Avancée" de la fenêtre Options de SpamPal. Sur la même page, vous devriez avoir un temps pour "Terminer les requêtes DNSBL après 10 à 20 secondes de non-réponse", et un maximum de 25 requêtes DNS simultanées devrait être un bon choix pour la plupart des utilisateurs.

Je n'intercepte toujours pas assez de spam: comment puis-je améliorer les performances de SpamPal?

Si vous n'attrapez toujours pas assez de spam, vous feriez mieux d'essayer des stratégies alternatives, pas seulement en s'appuyant sur plus de listes DNSBL. Regardez aux nombreux plugins disponibles.

Il y en a un qui s'appelle URLbody qui vérifie les adresses trouvées dans les messages auprès des listes DNSBL. Bien que les spammeurs puissent déguiser leur adresse email et envoyer le message par des voies très tortueuses, ils auront toujours besoin d'indiquer l'adresse de leur site dans le message qu'ils vous ont envoyé, ce plugin peut être très efficace pour les intercepter.

RegEx va examiner le corps du message pour chercher certaines phrases et autres expressions qui sont de bonnes indications de spam. Il devrait intercepter beaucoup de spam. La majorité des messages spam est en anglais, aussi ceux qui reçoivent couramment des messages dans cette langue peuvent subir des taux de faux positifs assez élevés vu les "motifs" utilisés par RegEx. Néanmoins, la dernière version utilise un système de notation combiné qui devrait fortement améliorer sa sensibilité de discrimination. Certaines personnes ont indiqué avoir des taux de détection bien au-dessus de 90%, uniquement en utilisant RegEx et aucune liste DNSBL du tout.

Le bloqueur MX est utilisé pour détecter les messages qui sont envoyés à partir de serveurs locaux sur les lignes téléphoniques, une tactique commune des spammeurs. Vous pouvez ainsi éliminer beaucoup de spam qui échappe aux listes DNSBLs. Cependant utilisez ce plugin avec précaution puisque l'utilisation d'un serveur local est un moyen normal d'envoyer du courrier : vous pourriez avoir besoin d'ajouter quelques correspondants réguliers à votre liste blanche.

Il y a aussi un plugin "filtre Bayesian" qui prend une approche complètement différente pour détecter le spam, bien que sa nature même indique qu'il est très probable que vous ayez des faux positifs pour commencer et il a absolument besoin d'une période d'apprentissage pour apprendre les caractéristiques de votre courrier.

Pour plus de détails sur les plugins, visitez cette page.

Comme pour les DNSBLs, n'installez pas seulement tous les plugins en une seule fois : c'est inutile. Essayez chaque plugin un par un et cherchez celui ou ceux qui marchent le mieux pour vous.

J'ai plein de vieux spam dans ma boîte de réception que j'ai reçu avant de commencer à utiliser SpamPal, est-ce qu'il peut maintenant les vérifier?

Non. La vérification rétrospective des entêtes de messages ne peut fonctionner car les listes noires sont des objets dynamiques. Elles indiquent quelle est le statut actuel d'une adresse IP, pas celui lorsque vous avez reçu le message.

Pourquoi SpamPal ne renvoi-il pas des messages d'erreur vers le spammeur comme d'autres produits?

La raison habituelle qu'ont les internautes d'aimer les messages d'erreur de transmission (bounce messages) est qu'ils pensent qu'un message d'erreur va indiquer au spammeur que l'adresse n'existe pas et que leur adresse va être retirée des listes et que, dès lors, ils ne recevront plus de spam.

En réalité, les messages d'erreur (bounce messages) sont normalement inutiles parce que :

1. Un spammeur envoie, en quelques minutes, des millions de messages à la fois. Pourquoi devrait-il perdre du temps à supprimer quelques centaines d'adresses qui n'existent pas? Généralement la même adresse est encore spammée la fois suivante (cela ne coûte rien au spammeur, ni en temps, ni en argent, d'envoyer quelques messages de plus). Les retours d'utilisateurs vont uniquement augmenter le trafic sur Internet et cela va finir par coûter à l'utilisateur soit du temps, soit de l'argent, de retourner beaucoup de messages au spammeur.

2. Dans 99.9% des cas, l'adresse de retour est invalide ou n'a rien à voir avec le spammeur réel.

Voici quelques exemple du "monde réel" :-

a) l'émetteur n'existe pas et le message d'erreur ne peut être délivré.

Donc vous retournez encore ce (faux) message d'erreur et, comme la plupart des spammeurs savent reconnaître que cela n'est pas un vrai message d'erreur, vous avez fini par dépenser du temps et de l'argent et VOUS LUI AVEZ CONFIRMÉ QUE L'ADRESSE EXISTE BIEN.

b) l'émetteur (innocent) existe bien et le spammeur a utilisé son adresse pour envoyer le spam.

Les spammeurs utilisent souvent l'adresse email de personnes innocentes (très souvent, ils utilisent l'adresse de personnes qui ont essayé d'arrêter le spammeur par des plaintes). Par conséquent, ces personnes reçoivent des milliers de messages d'erreur réels et d'autres faux envoyés par des logiciels qui vous permettent d'envoyer de faux messages d'erreur.

c) l'émetteur est le spammeur (dans quelques très rares cas).

Le spammeur peut ainsi vérifier que votre compte existe bien (quand il est assez intelligent pour remarquer que votre message d'erreur est faux).

Que dois-je faire avec le spam qui reste malgré tout indétecté? Est-ce un bug de Spampal? Dois-je vous l'envoyer pour que vous puissiez l'étudier?

Non, il y aura toujours quelques spam qui passeront au travers, quelque soient les outils utiliser. Nous vous suggérons de vous inscrire à un compte gratuit de dénonciation de spam auprès de spamcop.net (http://www.spamcop.net), et de leur envoyer le spam. Quand le message a été détecté par plusieurs personnes, il sera ajouté à la DNSBL de SpamCop et les autres utilisateurs de SpamPal pourront bénéficier de votre rapport.

Mais un spam est ENCORE passé au travers, c'est un désastre!

Non. L'objectif n'est pas de détecter tous les messages spam. L'objectif est de vous rendre votre boite de réception et de vous permettre de nettoyer les quelques spam résiduels avec le minimum d'effort. Ne devenez pas obsédé par le spam!

::Début::

5. Vérification de la présence de mises à jour

SpamPal va périodiquement contrôler la présence d'une version plus récente du programme. La mise à jour n'est pas automatique, mais il va vous en informer afin que vous puissiez télécharger la nouvelle version si vous le voulez. Il va aussi vous informer sur la disponibilité de tout nouveau plugin et sur les mises à jour des plugins que vous avez installé.

SpamPal va aussi mettre à jour la liste des listes publiques DNSBL à la même périodicité.
Ainsi, si une des listes que vous utilisez devenait indisponible de façon permanente, il vous le dira eu vous pourrez choisir une autre liste dans la fenêtre Options.

Si une nouvelle version de SpamPal ou d'un plugin est disponible, suivez cette procédure afin que la mise à jour soit aussi rapide et transparent que possible.

::Début::

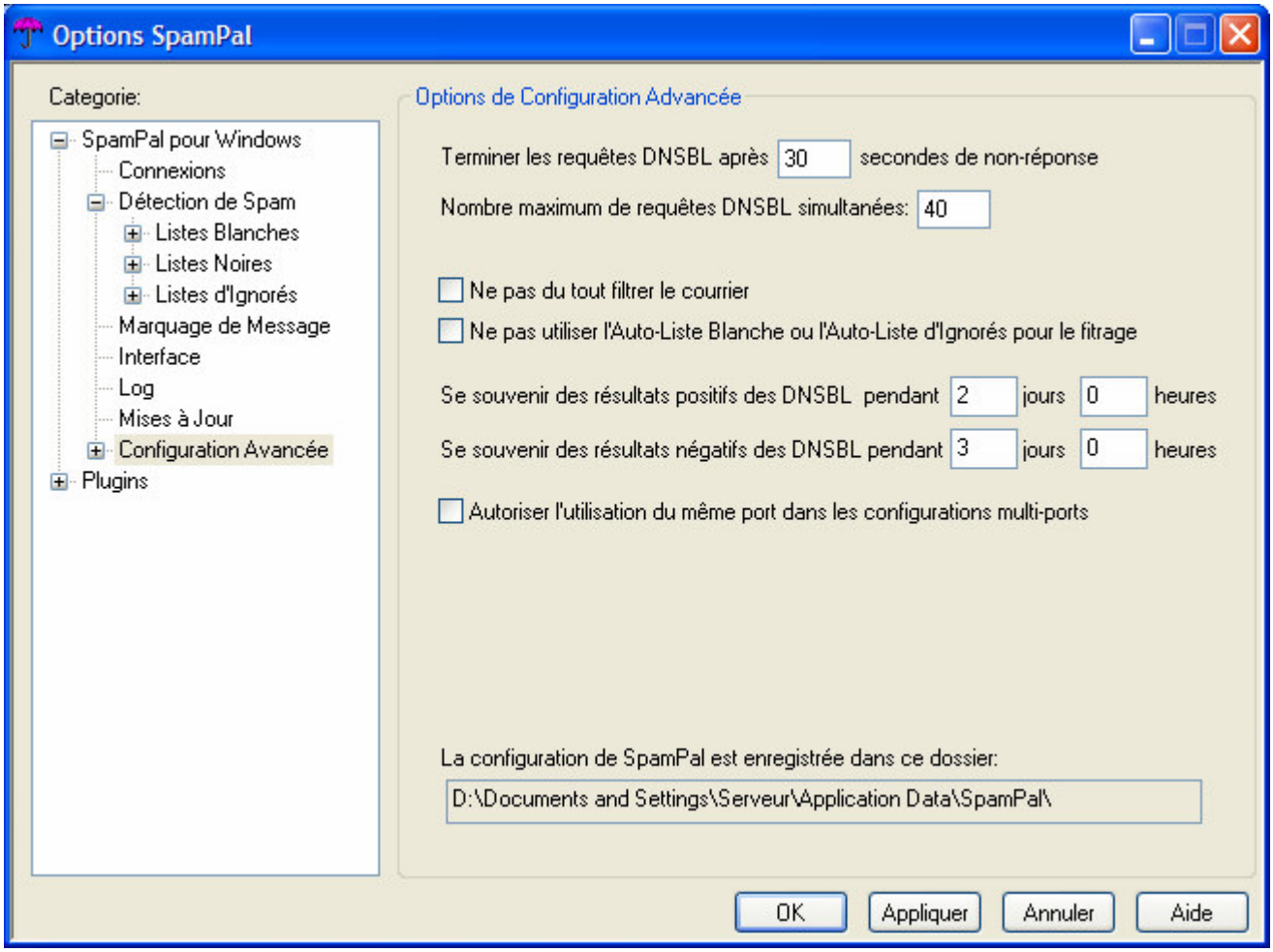
6. Sauvegarde de vous réglages

D'abord, vous devez localiser le répertoire où vos fichiers de configuration Spampal sont enregistrés, ainsi que les réglages des plugins que vous utilisez.

Ouvrez la fenêtre Options. Sélectionnez maintenant le panneau "Configuration avancée".

Au bas de cet écran, un texte indique où "La configuration de SpamPal est enregistrée dans ce dossier". C'est ce dossier que vous devez sauvegarder.

Utiliser l'explorateur de Windows (ou un programme d'arcives) et sauvegardez tout le dossier.



::Début::

7. Arrêter le filtrage des message par SpamPal

Vous pouvez arrêter le filtrage des messages par SpamPal, sans changer aucun des réglages de votre programme email, en utilisant l'option **Désactiver** du menu "clic droit" de l'icône de la barre des tâches.

Vous pouvez savoir quand SpamPal ne filtre pas les messages quand l'icône devient :

::Début::

Contenu > Configurer SpamPal

Toutes les fonctions de SpamPal sont configurables, mais les réglages par défaut devraient déjà répondre aux besoins de la plupart des utilisateurs. Si, néanmoins, vous avez besoin de changer ses réglages, il vous suffit d'ouvrir la fenêtre **Options** de SpamPal.

Index

::Top::

1. Ouvrir la fenêtre Options

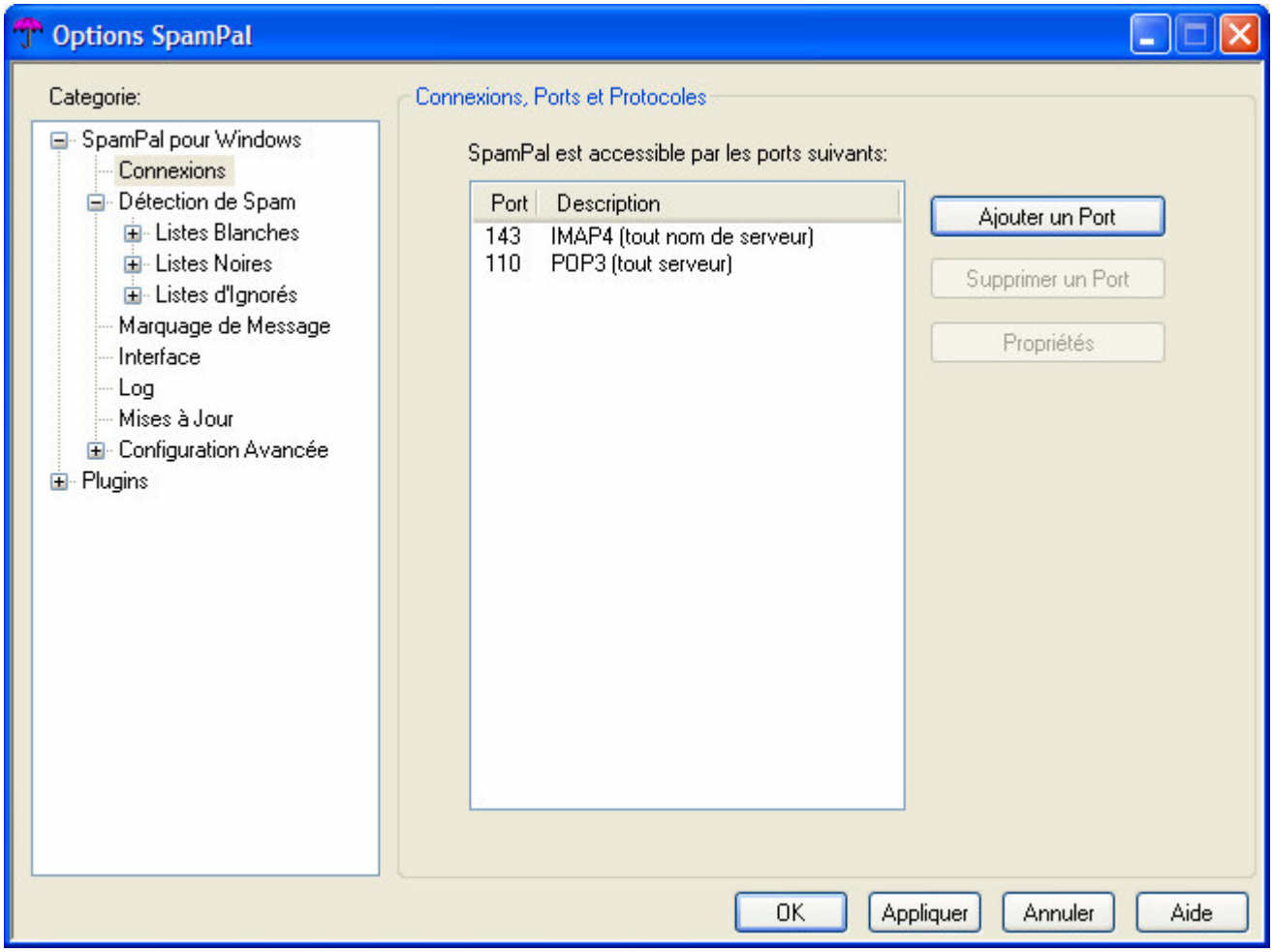
Pour ouvrir la fenêtre Options, cliquez droit sur l'icône en forme de parapluie de SpamPal, située dans la barre des tâches, puis cliquez sur Options.

::Début::

2.1 Connections: Panneau principal

Ce panneau vous permet de contrôler le ou les port(s) que votre programme email utilise pour communiquer avec SpamPal. Vous pouvez normalement laisser les numéros de port, sur les valeurs préréglées par SpamPal et ne pas vous en inquiéter plus.

Les **ports utilisés** par défaut sont 110 (POP3), 143 (IMAP4). Vous pouvez aussi rencontrer le port 25 (SMTP).

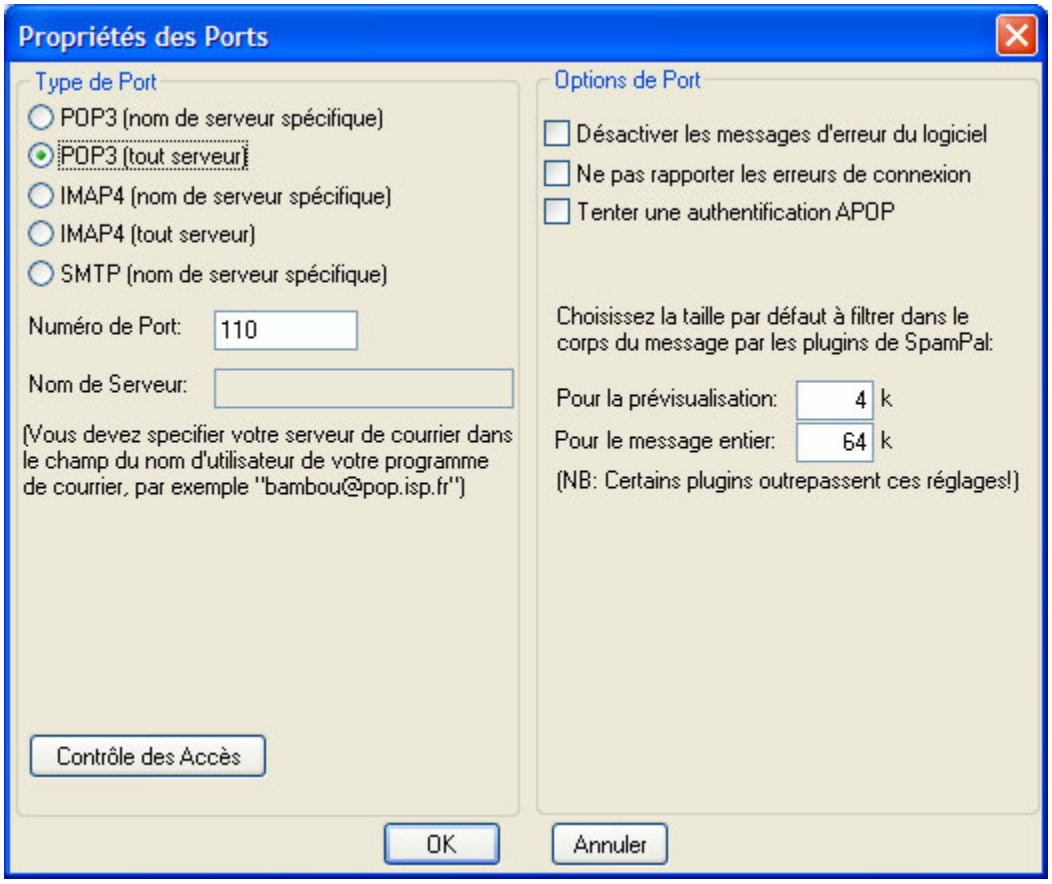


::Top::

2.2. Connections**: Propriétés des Ports : Réglage du proxy POP3 (tout serveur)**

Dans la plupart des cas, vous allez utiliser le proxy POP3 de SpamPal, lors du réglage de SpamPal.

Depuis le panneau principal de Connections (voir ci-dessus), cliquez sur Ajouter un port pour créer un nouveau port (ou sélectionner Propriétés pour modifier les réglages).



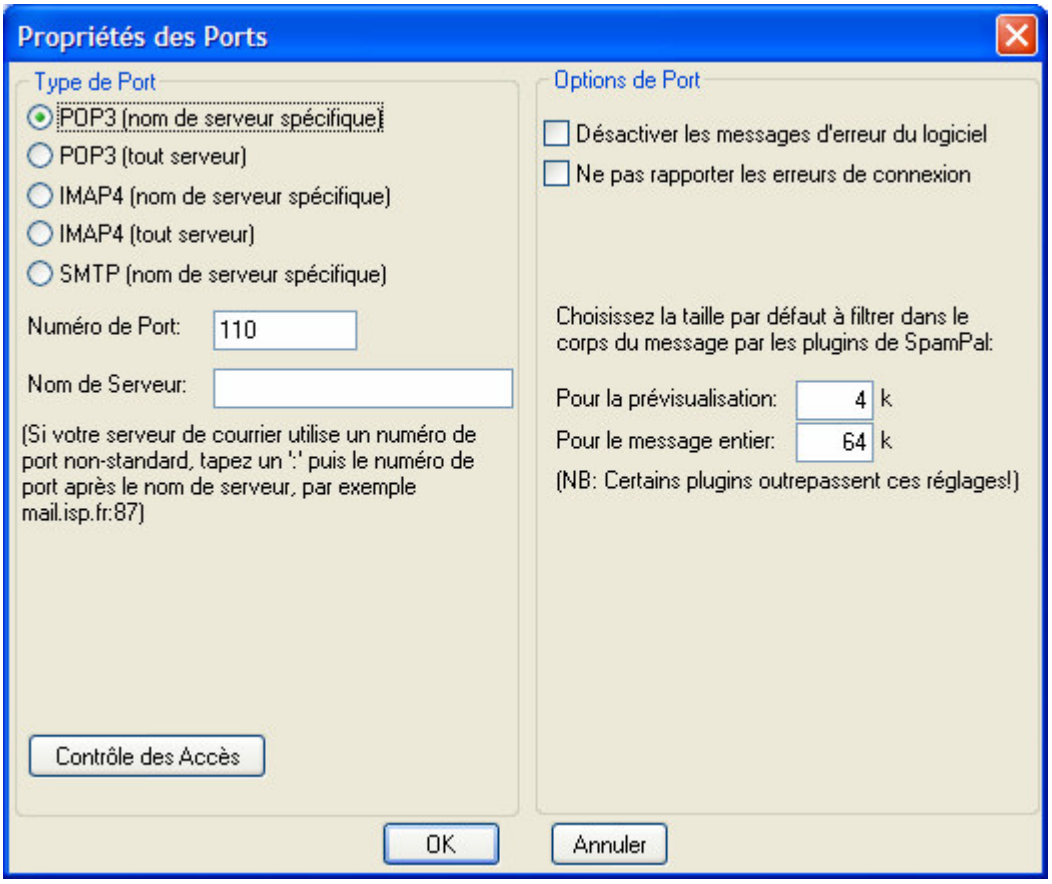
Choisir la taille à filtrer pour la prévisualistion : Il ne sert à rien de filtrer la totalité des gros messages, quand votre programme email ne demande à voir que les entêtes du message. Cela vous permet de préciser combien du corps du messages sera transmis pour filtrage par des plugins comme RegExFilter ou HtmlModify. Une valeur plus faible va rendre SpamPal plus rapide, mais au prix d'un filtrage moins efficace.

Choisir la taille à filtrer pour le message entier : Il n'y a pas besoin de filtrer la totalité des gros messages, cela vous permet donc de préciser quelle taille du corps du message sera transmise pour filtrage aux plugins comme RegExFilter ou HtmlModify. Une valeur plus faible va rendre SpamPal plus rapide, mais au prix d'un filtrage moins efficace.

::Début::

2.3. Connections**: Propriétés des Ports : Réglage du proxy POP3 (nom de serveur spécifique)**

Depuis le panneau principal de Connections, cliquez sur Ajouter un port pour créer un nouveau port (ou sélectionner Propriétés pour modifier les réglages).



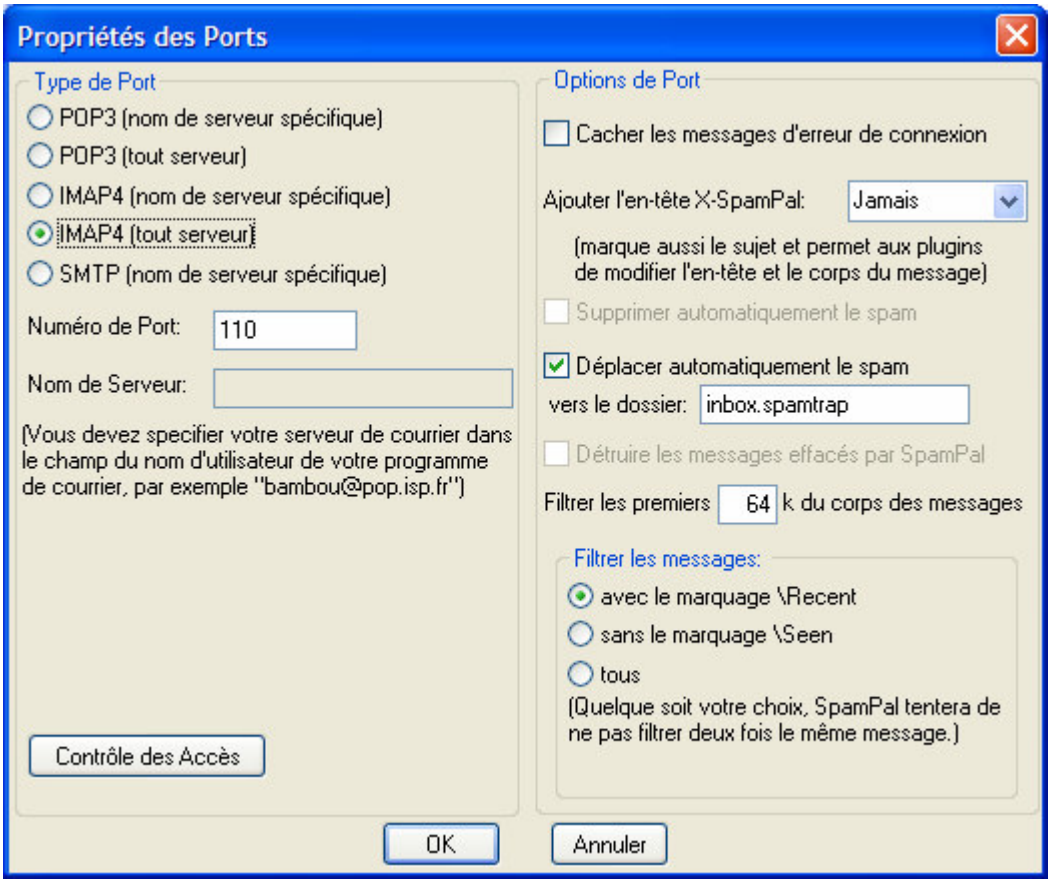
Choisir la taille à filtrer pour la prévisualistion : Il ne sert à rien de filtrer la totalité des gros messages, quand votre programme email ne demande à voir que les entêtes du message. Cela vous permet de préciser combien du corps du messages sera transmis pour filtrage par des plugins comme RegExFilter ou HtmlModify. Une valeur plus faible va rendre SpamPal plus rapide, mais au prix d'un filtrage moins efficace.

Choisir la taille à filtrer pour le message entier : Il n'y a pas besoin de filtrer la totalité des gros messages, cela vous permet donc de préciser quelle taille du corps du message sera transmise pour filtrage aux plugins comme RegExFilter ou HtmlModify. Une valeur plus faible va rendre SpamPal plus rapide, mais au prix d'un filtrage moins efficace.

::Début::

2.4. Connections**: Propriétés des Ports : Réglage du proxy IMAP4 (tout serveur)**

Depuis le panneau principal de Connections, cliquez sur Ajouter un port pour créer un nouveau port (ou sélectionner Propriétés pour modifier les réglages).



Ajouter l'entête X-SpamPal - autoriser SpamPal à modifier l'entête des messages (ou le corps) est très lent en IMAP4, puisque le message complet doit être télécharger par SpamPal, modifié, puis renvoyé vers votre serveur de messagerie. Par conséquent, par défaut, SpamPal n'est pas autorisé à modifier l'entête ou le corps des messages - pas de marque **SPAM** dans le sujet, pas de ligne X-SpamPal: dans l'entête, etc. etc. etc. Vous pouvez autoriser SpamPal à ajouter tout cela à tous les messages ou juste aux messages spam en utilisant cette option.

Supprimer automatiquement le spam - va marquer comme message effacé tout message que SpamPal soupçonne d'être un spam. Par défaut, cette option est désactivée, et je vous recommande fortement de la laisser ainsi jusqu'à ce que vous soyez suffisamment confiant que rien d'important ne sera effacé par erreur, probablement définitivement.

Déplacer automatiquement le spam - L'action par défaut de SpamPal pour un compte IMAP4 est de déplacer le spam dans un autre dossier. Vous pouvez indiquer le nom du dossier ici - s'il n'existe pas, SpamPal va essayer de le créer, et vous donnera un message d'erreur n'il n'y arrive pas.

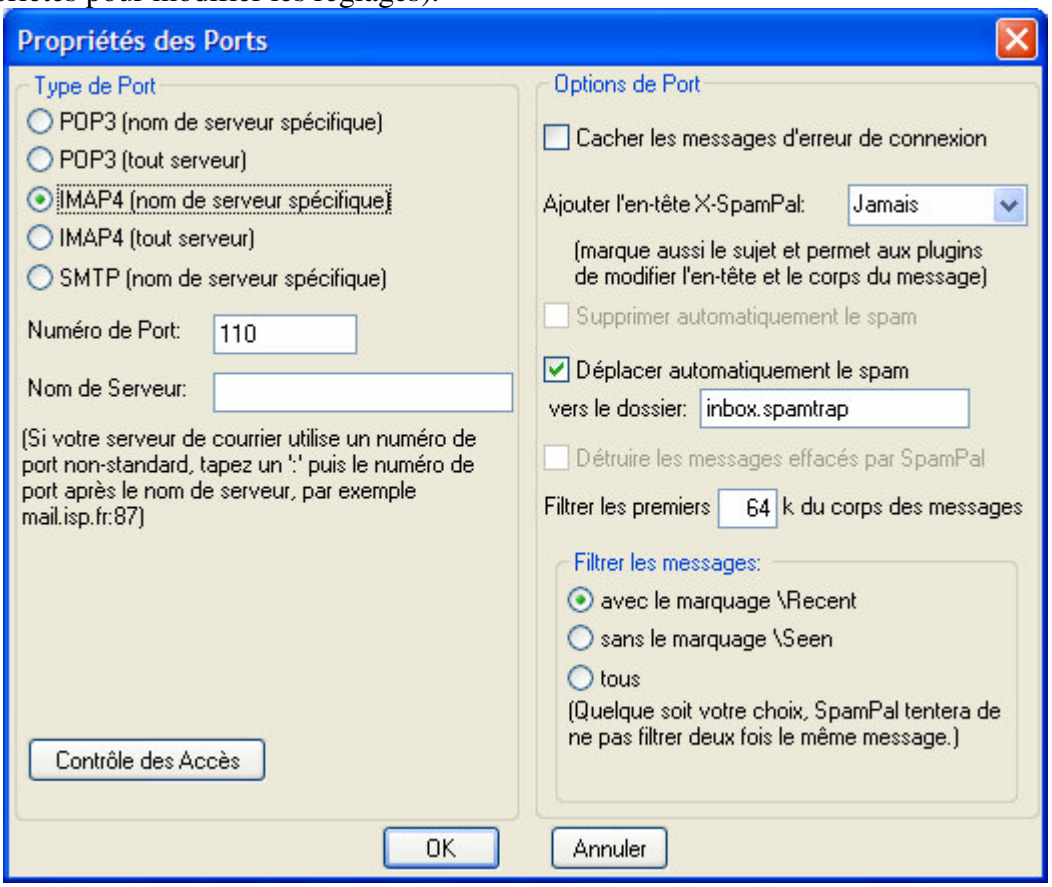
Filtrer les premiers xx k du corps du message : Il n'y a pas besoin de filtrer la totalité des gros messages, cela vous permet donc de préciser quelle taille du corps du message sera transmise pour filtrage aux plugins comme RegExFilter ou HtmlModify. Une valeur plus faible va rendre SpamPal plus rapide, mais au prix d'un filtrage moins efficace.

Filtrer les messages: avec le marquage Recent / sans le marquage Seen flag / tous - ceci est un rélage technique que vous pourrez généralement laisser à sa position originale (avec le marquage Recent). Quelques serveurs IMAP4 semblent ne pas indiquer correctement le marquage Recent, cependant, si SpamPal semble ne pas filtrer tout ou partie de vos messages, essayez de changer ce réglage pour sans marquage Seen, et si cela ne fonctionne toujours pas, indiquez tous.

::Début::

2.5. Connections**: Propriétés des Ports : Réglage du proxy IMAP4 (nom de serveur spécifique)**

Depuis le panneau principal de Connections, cliquez sur Ajouter un port pour créer un nouveau port (ou sélectionner Propriétés pour modifier les réglages).



Ajouter l'entête X-SpamPal - autoriser SpamPal à modifier l'entête des messages (ou le corps) est très lent en IMAP4, puisque le message complet doit être télécharger par SpamPal, modifié, puis renvoyé vers votre serveur de messagerie. Par conséquent, par défaut, SpamPal n'est pas autorisé à modifier l'entête ou le corps des messages - pas de marque **SPAM** dans le sujet, pas de ligne X-SpamPal: dans l'entête, etc. etc. etc. Vous pouvez autoriser SpamPal à ajouter tout cela à tous les messages ou juste aux messages spam en utilisant cette option.

Supprimer automatiquement le spam - va marquer comme message effacé tout message que SpamPal soupçonne d'être un spam. Par défaut, cette option est désactivée, et je vous recommande fortement de la laisser ainsi jusqu'à ce que vous soyez suffisamment confiant que rien d'important ne sera effacé par erreur, probablement définitivement.

Déplacer automatiquement le spam - L'action par défaut de SpamPal pour un compte IMAP4 est de déplacer le spam dans un autre dossier. Vous pouvez indiquer le nom du dossier ici - s'il n'existe pas, SpamPal va essayer de le créer, et vous donnera un message d'erreur n'il n'y arrive pas.

Filtrer les premiers xx k du corps du message : Il n'y a pas besoin de filtrer la totalité des gros messages, cela vous permet donc de préciser quelle taille du corps du message sera transmise pour filtrage aux plugins comme RegExFilter ou HtmlModify. Une valeur plus faible va rendre SpamPal plus rapide, mais au prix d'un filtrage moins efficace.

Filtrer les messages: avec le marquage Recent / sans le marquage Seen flag / tous - ceci est un rélage technique que vous pourrez généralement laisser à sa position originale (avec le marquage Recent). Quelques serveurs IMAP4 semblent ne pas indiquer correctement le marquage Recent, cependant, si SpamPal semble ne pas filtrer tout ou

partie de vos messages, essayez de changer ce réglage pour sans marquage Seen, et si cela ne fonctionne toujours pas, indiquez tous.

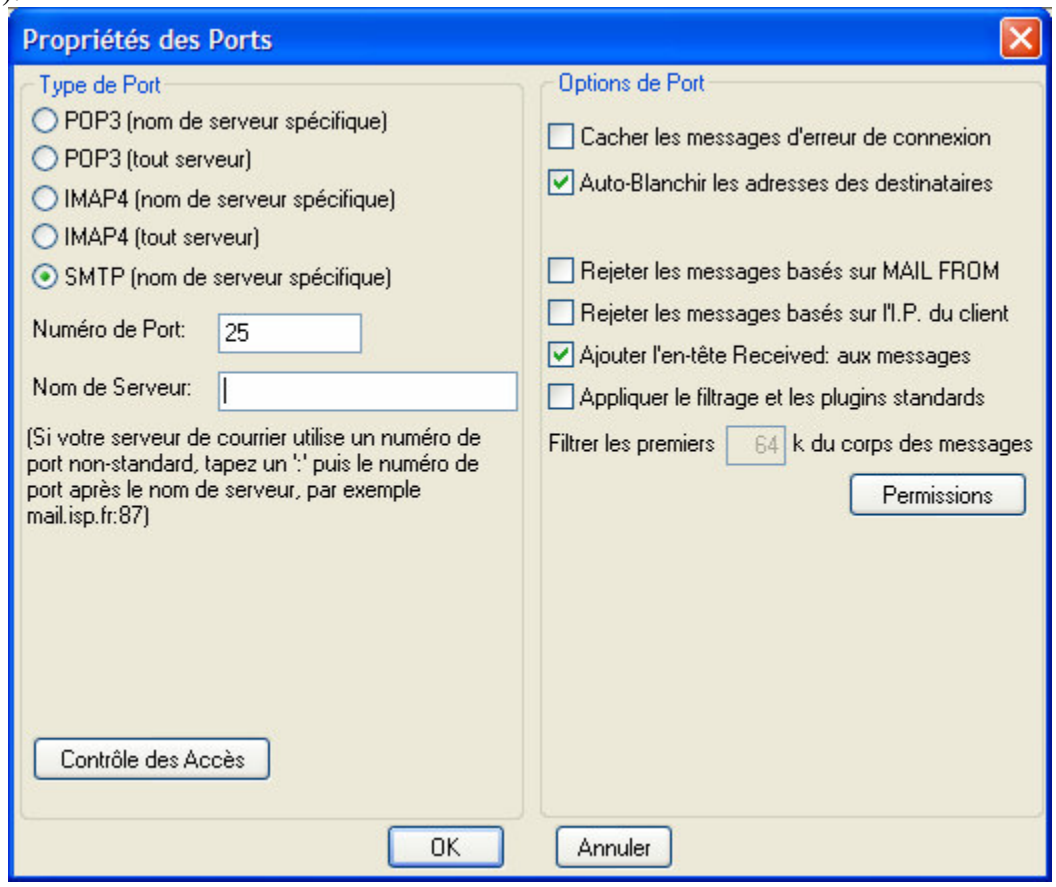
::Début::

2.6. Connections**: Propriétés des Ports : Réglage du proxy SMTP (liste blanche automatique)**

Vous pouvez utiliser la fonction "Liste blanche automatique" de SpamPal pour lui faire apprendre automatiquement à quelles adresses vous envoyez du courrier et les ajouter automatiquement à la liste blanche. Le but est d'accélérer le traitement de votre courrier et d'éviter au courrier venant de vos amis et contacts d'être marqué comme spam.

Depuis le panneau principal de Connections, cliquez sur Ajouter un port pour créer un nouveau port (ou sélectionner Propriétés pour modifier les réglages).

Sélectionnez SMTP (nom de serveur spécifique) dans la partie “Type de port”, et entrez dans la case en dessous le nom de votre serveur SMTP (il doit apparaître dans la configuration de votre programme email comme « nom de serveur sortant »).



Note 1: Port SMTP

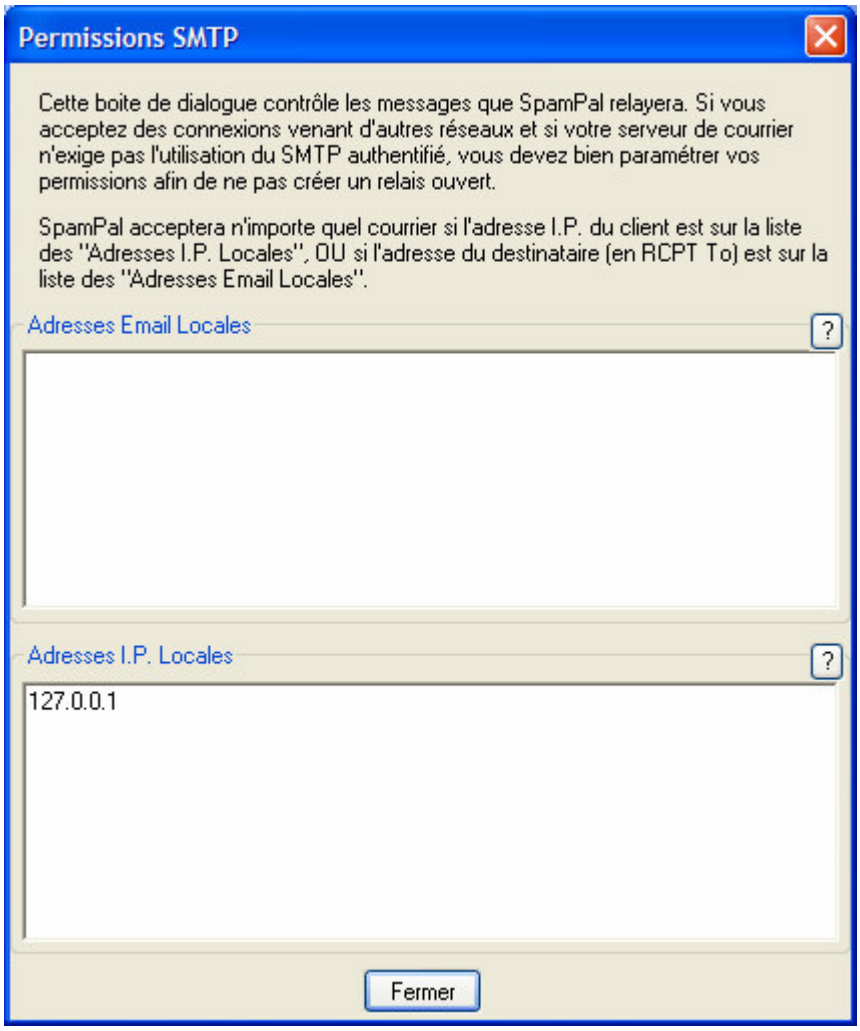
Vérifiez que le port local est bien réglé à 25.

Maintenant, allez dans la configuration de votre programme email ou les réglages des comptes, trouvez le réglage du **serveur** SMTP ou serveur de courrier sortant, et changez-le pour localhost. Essayez de vous envoyer un message pour vérifier si ça fonctionne.

Maintenant, dès que vous enverrez un message à quiconque, son adresse sera ajoutée à la liste blanche automatique, il n'y a donc plus de danger que sa réponse soit marquée comme spam.

> **Note 2:** Option Exclusions de liste blanche automatique
>
> Si vous vous envoyez souvent des messages, ajoutez votre propre adresse à la liste d'exclusion. En effet, certains spammeurs modifient les entêtes des messages afin qu'ils semblent venir de vous-même.

Les options sur la droite du dialogue de propriété des ports peuvent être ignorées, à moins que vous ne laissiez SpamPal écouter d'autres adresses IP que 127.0.0.1. Dans ce cas, vous aurez besoin de cliquer sur le bouton Permissions et d'ajouter ces adresses I.P. à la liste des **adresses IP locales**.



> **Note 3:** Adresses IP SMTP
>
> Faire fonctionner la fonction SMTP de SpamPal sur une autre adresse IP que 127.0.0.1 est **très dangereux**, puisque cela signifie que votre système peut alors être utilisé par les spammeurs comme relais ouvert.

SpamPal peut aussi être utilisé pour filtrer le spam au niveau du **serveur SMTP**.

En principe, vous avez juste besoin de déplacer votre ancien relais SMTP vers un autre port ou une autre machine, installer SpamPal à sa place, créer un port SMTP (nom de serveur spécifique) dans les options de SpamPal, utilisant le port 25 (celui qu'utilisait votre ancien relais SMTP) et d'entrer le nom du nouvel emplacement de votre serveur réel dans le champ **Nom de serveur**.

Modifiez les options sur la droite (l'option Appliquer les options et réglages standards ne fera que marquer les messages spam; l'option Rejeter les messages basés sur l'IP du client rejettera les emails provenant d'une adresse IP apparissant dans une liste DNSBL ou en liste noire.

Vous devrez aussi cliquer sur le dialogue Permissions et entrez toutes les adresses email locales. SpamPal rejettera tous les messages dont le champ RCPT TO: n'apparît pas dans cette liste. (Vous pouvez utiliser le caractère générique "*" si vous voulez, mais soyez prudent!) Si cette version de SpamPal est aussi utilisée par vos propres utilisateurs pour filtrer les messages sortants, entrez vos **adresses IP locales** dans la fenêtre correspondante; la restriction sur le champ RCPT TO: ne s'applique pas aux connections depuis ces adresses IP.

Il est probablement plus sûr d'installer SpamPal comme un **relais interne de messagerie**, avec un serveur de messagerie traitant les connections extérieures. Cependant, vous perdez la possibilité de rejeter le courrier basé sur l'adresse IP du client si vous faites ainsi. Les filtres standards de SpamPal devraient néanmoins fonctionner correctement.

::Début::

3. Détection de spam : Liste blanche

3.1. Détection de spam : Liste blanche : Adresses Email

Les listes blanches sont très importantes pour s'assurer que le courrier que vous envoient vos correspondants réguliers et les listes de diffusion passent au travers. Un élément d'une liste blanche est une balle en or. Quoi qu'en dise n'importe quelle liste noire, si une adresse est en liste blanche, le courrier ne sera pas marqué comme spam.

La liste blanche est l'inverse des listes noires. Elle en a le format - une adresse email par ligne, le caractère indiquant une ligne de commentaire.

Vous pouvez aussi utiliser des astérisques (*) comme caractère générique, de façon à laisser passer tout le courrier venant d'une adresse email (ou d'un domaine) et, désormais, le courrier ne sera jamais marqué comme spam par SpamPal. C'est très utile si vous avez un ami qui utilise un fournisseur d'accès qui apparaît dans une liste DNSBL - vous n'avez qu'à l'ajouter à votre liste blanche et son courrier ne finira plus dans votre corbeille à spam!

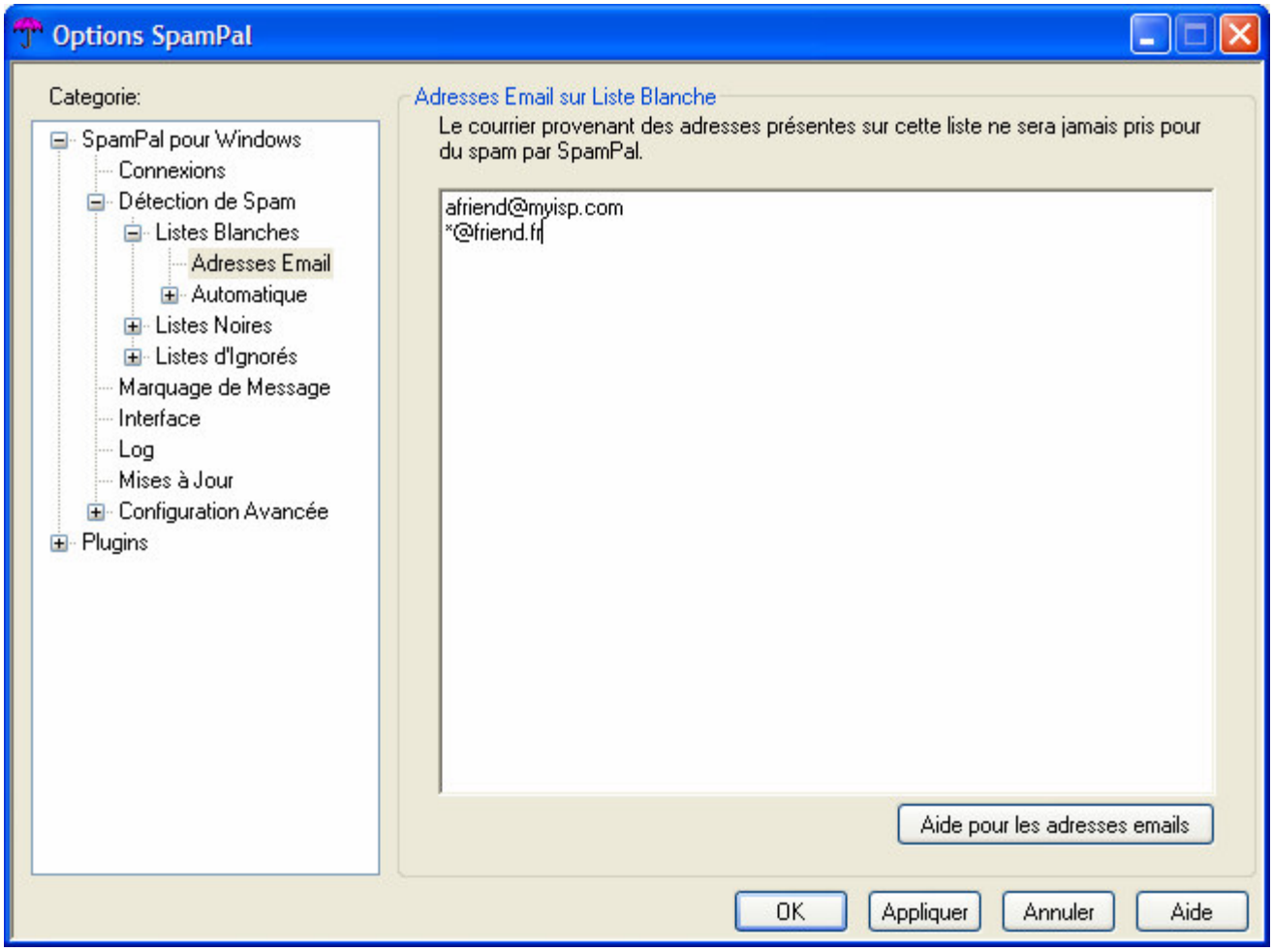
Par exemple, vous pouvez décider que James Farmer, qui est un chic type, ne vous enverra jamais de spam et, donc, vous décidez d'ajouter à votre liste blanche les lignes suivantes :

James Farmer ne va jamais m'envoyer de spam
jjf@spampal.twinlobber.org.uk

Ou, d'un autre coté, vous pouvez penser "je connais beaucoup de personnes utilisant Hotmail et ils ne m'envoient jamais de spam". Ajoutez alors :

Hotmail = personnes très gentilles!
*@hotmail.com

Les adresses de la liste blanche sont prioritaires sur celles apparaissant dans une liste noire. Ceci signifie qie vous pouvez (par exemple) mettre *@hotmail.com dans votre liste noire et ajouter ensuite à votre liste blanche l'adresse de vos connaissances qui utilisent hotmail.com.



Note: Entêtes auwquels la liste blanche est compatée

La fonction liste blanche ne regarde que les adresses email apparaissant dans les entêtes suivantes des messages reçus:
Actuellement, ces entêtes sont : From:, Reply-To:, Sender:, Mailing-List: et Return-Path:

::Début::

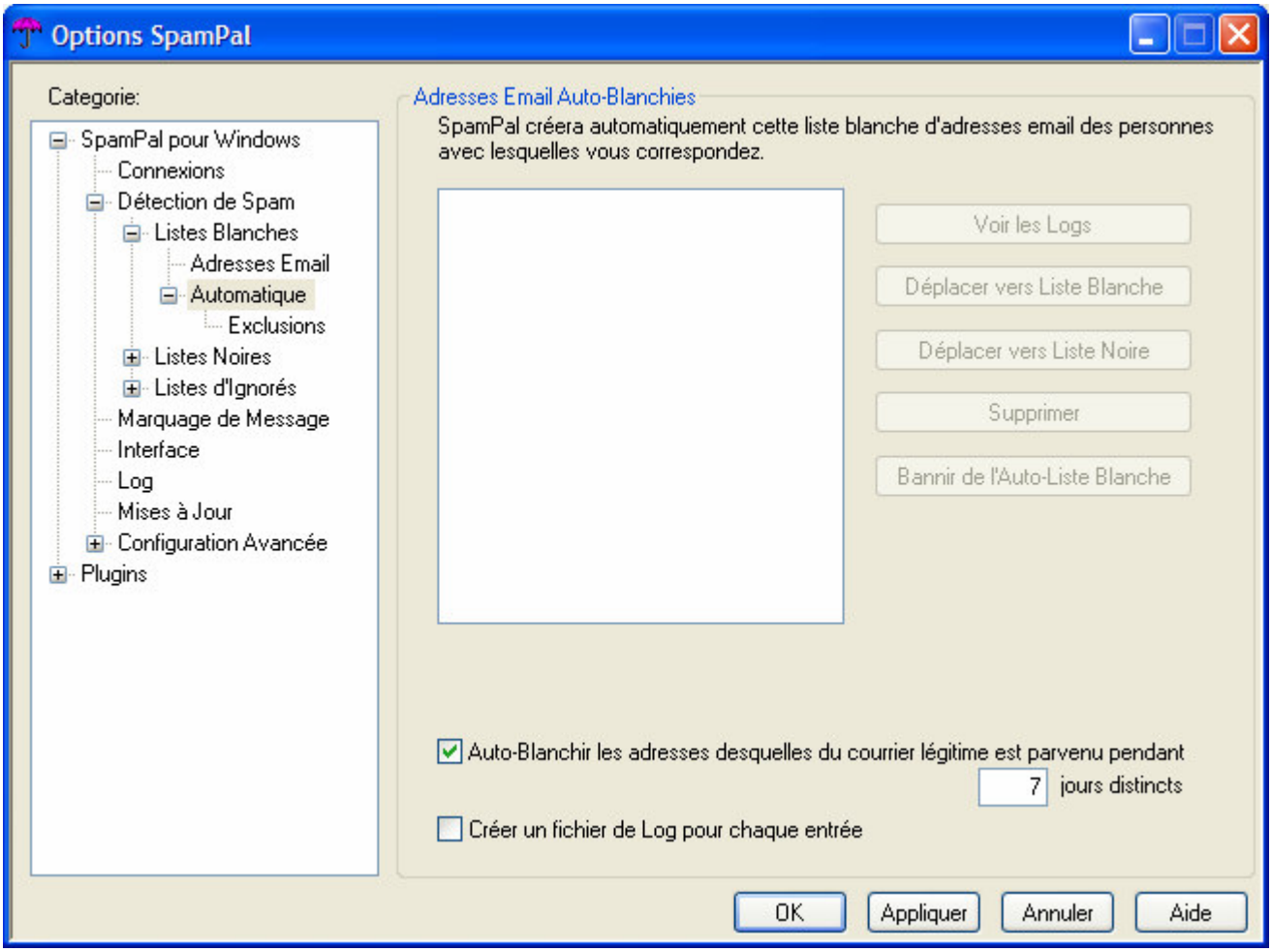
3.2. Détection de spam : Liste blanche : Automatique

La liste blanche normale est très pratique, mais vous devez encore perdre du temps à lui ajouter des adresses. Ne serait-ce pas génial si SpamPal le faisait à votre place? Eh bien, grâce à la liste blanche automatique, SpamPal le peut!

Les adresses email sont ajoutées à votre liste blanche automatique dès lors que vous en avez reçu des messages pendant plus d'un certain nombre de jours. Vous pouvez alors être certain que les gens avec lesquels vous correspondez régulièrement ne finiront pas dans votre corbeille à spam.

C'est généralement une bonne idée de valider la case à cocher Créer un fichier log pour chaque adresse, afin de savoir sur quelles bases l'adresse a été ajoutée.

A partir de l'écran principal (voir ci-dessous), vous pouvez aussi déplacer vos adresses de la liste blanche automatique vers votre liste blanche (pour faire les choses plus claires), vers votre liste noire ou même les bannir de la liste blanche automatique.



Note 1: Liste blanche automatique et message **SPAM**

La fonction liste blanche automatique ne traite **que** les messages qui n'ont **pas** été marqués **SPAM**

Note 2: Option "Exclusions" de la liste blanche

De temps en temps, il arrive qu'un spammeur utilise l'adresse de quelqu'un qui apparait dans votre liste blanche automatique -par exemple, un collègue, l'administrateur de votre réseau ou même une autre de vos adresses. Si vous ne voulez pas mettre cette personne en liste noire parce qu'ils vous envoient du courrier légitime, vous ne voulez pas non plus qu'ils finissent dans votre liste blanche automatique et contournent les vérifications de SpamPal.

Pour cela, sélectionner une adresse de la liste et cliquez sur **Bannir de l'auto liste blanche**. Cette adresse sera enlevée de la liste blanche automatique et ne pourra jamais y revenir.

Note 3: Vie privée : liste blanche automatique smtp

Si vous utilisez cette possibilité, spécialement dans un bureau, comme cela va enregistrer toutes les adresses de messages sortants, cela pourrait constituer une atteinte à la vie privée (au Royaume-Uni, vous devez prévenir une personne si vous placez son adresse dans un fichier), ou la constitution d'un fichier (soumis à la loi française "Informatique et libertés").

::Début::

3.3. Détection de spam : Liste blanche : Automatique : Exclusions

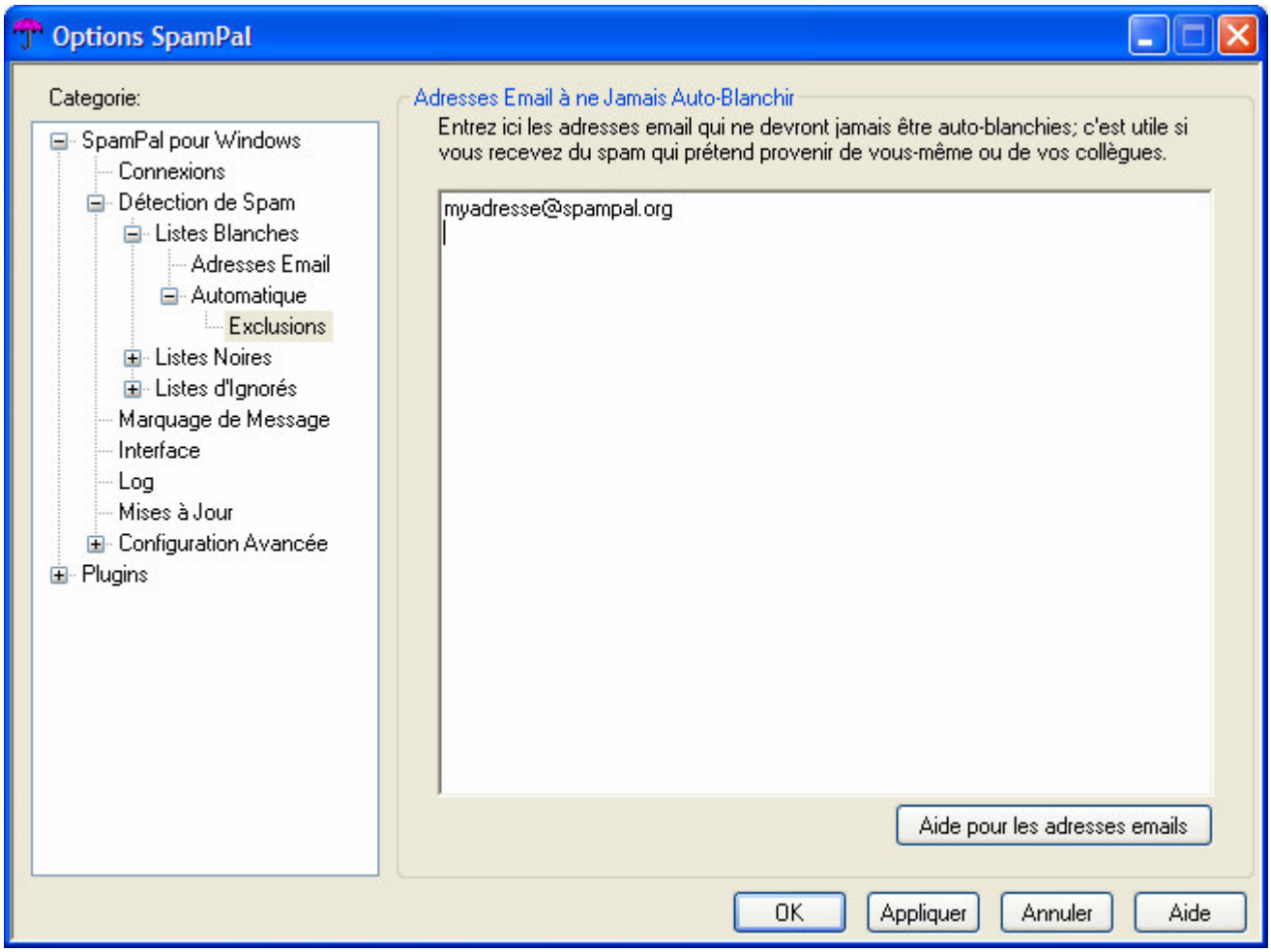
De temps en temps, il arrive qu'un spammeur utilise l'adresse de quelqu'un qui apparait dans votre liste blanche automatique -par exemple, un collègue, l'administrateur de votre réseau ou même une autre de vos adresses.

Si vous ne voulez pas mettre cette personne en liste noire parce qu'ils vous envoient du courrier légitime, vous ne voulez pas non plus qu'ils finissent dans votre liste blanche automatique et contournent les vérifications de SpamPal.

Dans ce panneau, vous pouvez ajouter les adresses des personnes qui ne devront jamais être ajouter à la liste blanche automatique.

Ajoutez vos adresses ici et vous n'aurez plus à vous inquiéter des spammeurs qui masqueront leurs adresses pour contourner les filtres de SpamPal.

Vous pouvez même ajouter votre domaine complet : *@acme-widgets.com.



::Début::

3.4. Spam-Detection: Blacklists: Public blacklists (DNSBLs)

SpamPal works by checking your mail against a number of DNSBL lists which list parts of the Internet that facilitate spamming. This pane allows you to choose which DNSBL lists you want to check your mail against.

The right-hand area lists the available DNSBL lists; those with a tick beside them are the ones you are currently using.

Click on a list, to toggle whether you are using it or not.

Sometimes one DNSBL list incorporates all the data from another; in these cases, if the first DNSBL service is selected then the second will be grayed out in the list.

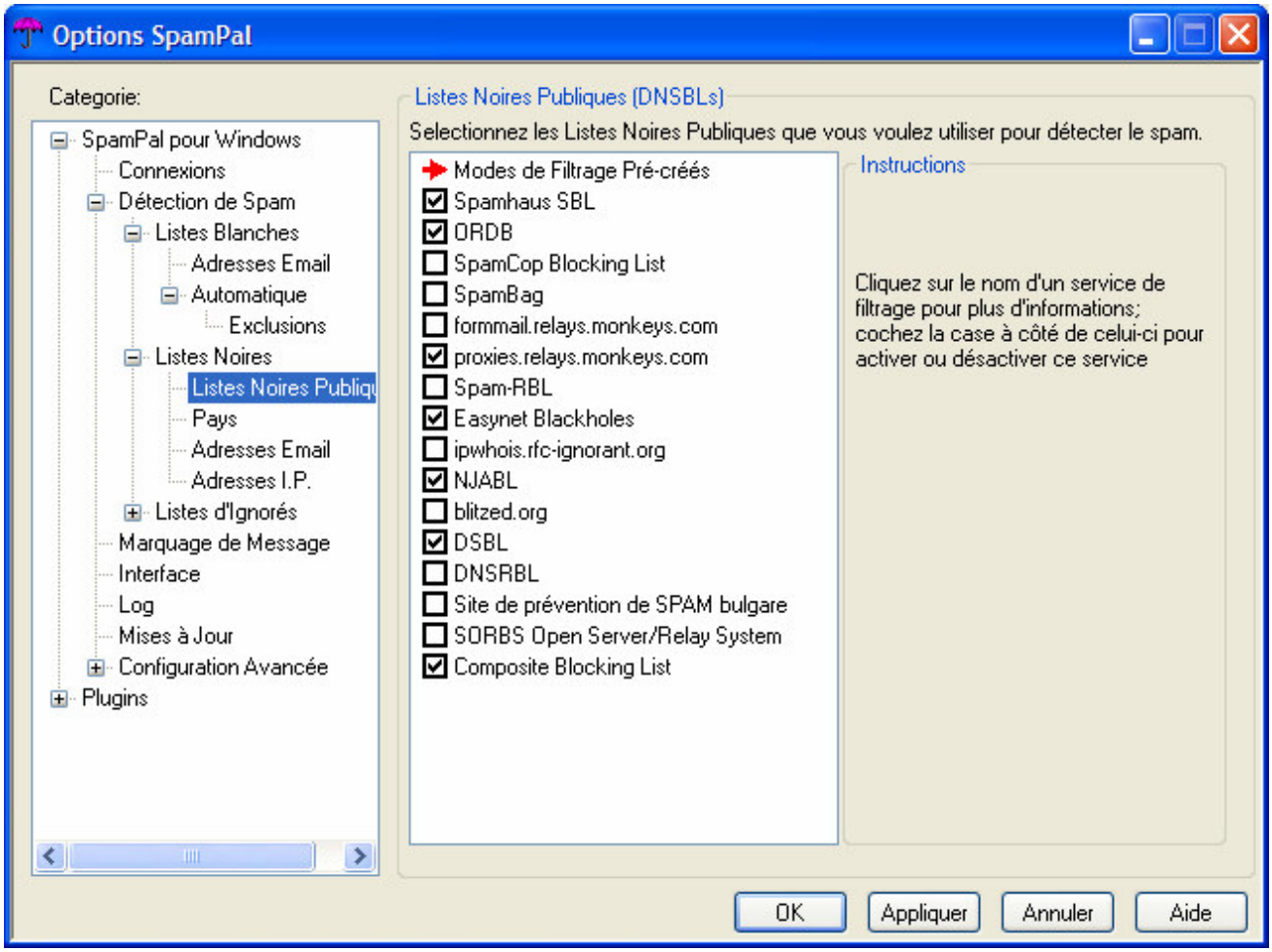
As the mouse pointer moves over a list, information about it appears to the right; the list name, website (click on it to go to that website), and a short description.

Each list also has a Header Code, which is used to identify the list in the X-SpamPal: header, for example: X-SpamPal: SPCOP

It's usually best to see if changes to your DNSBL choices can find spam rather than blacklisting individual entries, as Spammers are continually changing address, so it's not very productive to blacklist them.

You can copy and past IP addresses here to see which blacklists would have caught each IP address in the header. Start with the first Received line and work your way through the rest of them.

See here for more information on how to Optimise your DNSBL selection.



Different lists will have different characteristics. A couple of the more popular DNSBL services will have been selected by default, but feel free to experiment with other lists.

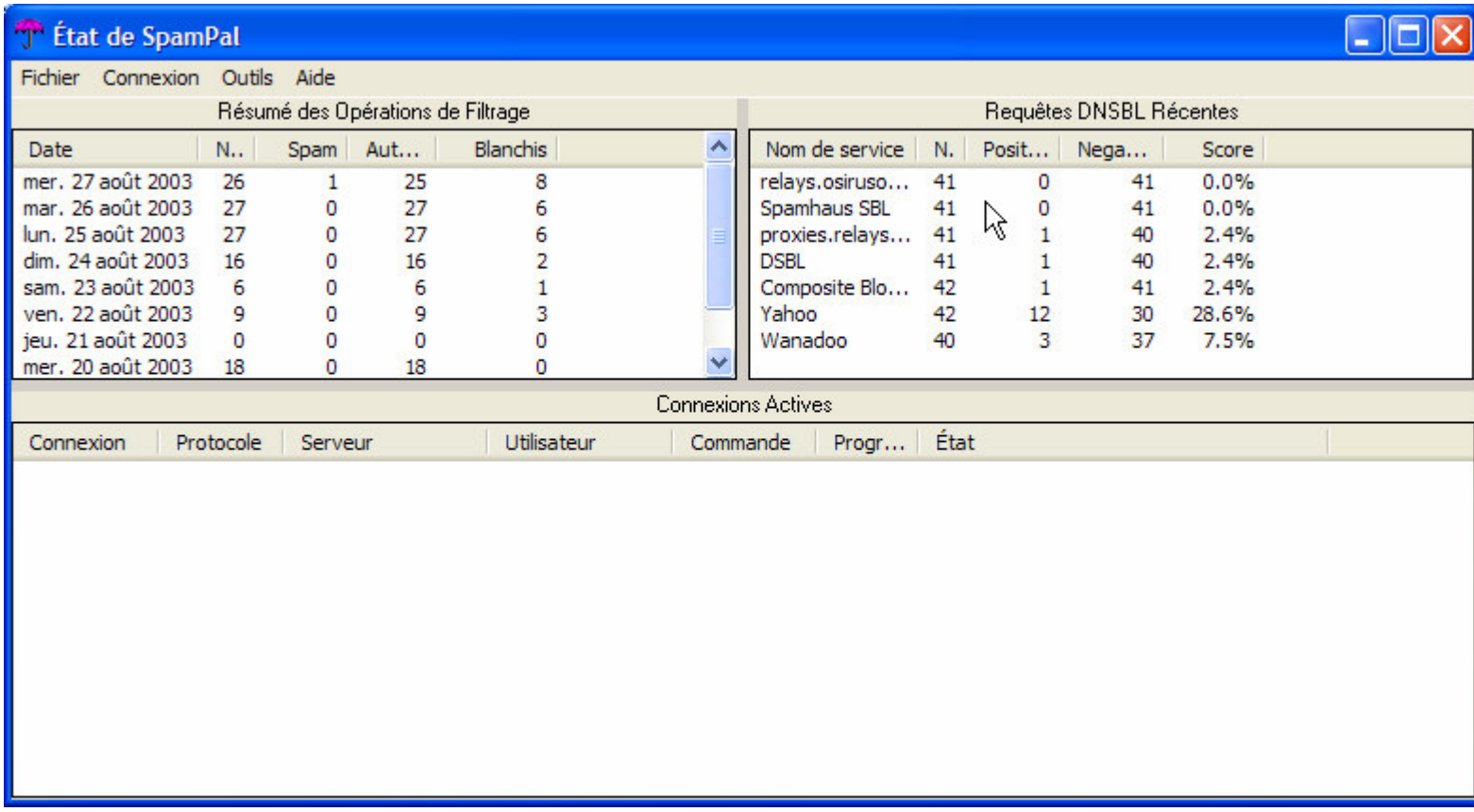
If a list seems to aggressive and blocks too much legitimate email (because spam-friendly providers may well have non-spamming customers too!), you can just deselect it from the list. You can see which DNSBL marked you email as spam, by looking at the headers of your email message, see this page for more details about SpamPal headers.

By using the SpamPal Status page (right click on the Systray Umbrella and select Status), you'll be able to see which of DNSBLs you are using and how effective they have been during a recent session.

If you look at the statistics on SpamPal's status screen, it will show you the hit rates being achieved by the various DNSBLs you are using for recent queries. You will probably notice that some of the DNSBLs regularly give high numbers, 20-50%, and others may be very low, or even zero hits.

Deselecting the ones with low hit rates, will probably improve speed, without affecting your spam detection capability.

For example, in the screen below, it looks like Spam-RBL has caught little spam in this session and therefore, may be a good idea to deselect this from your list of DNSBLs (public blacklists), in order to save time.



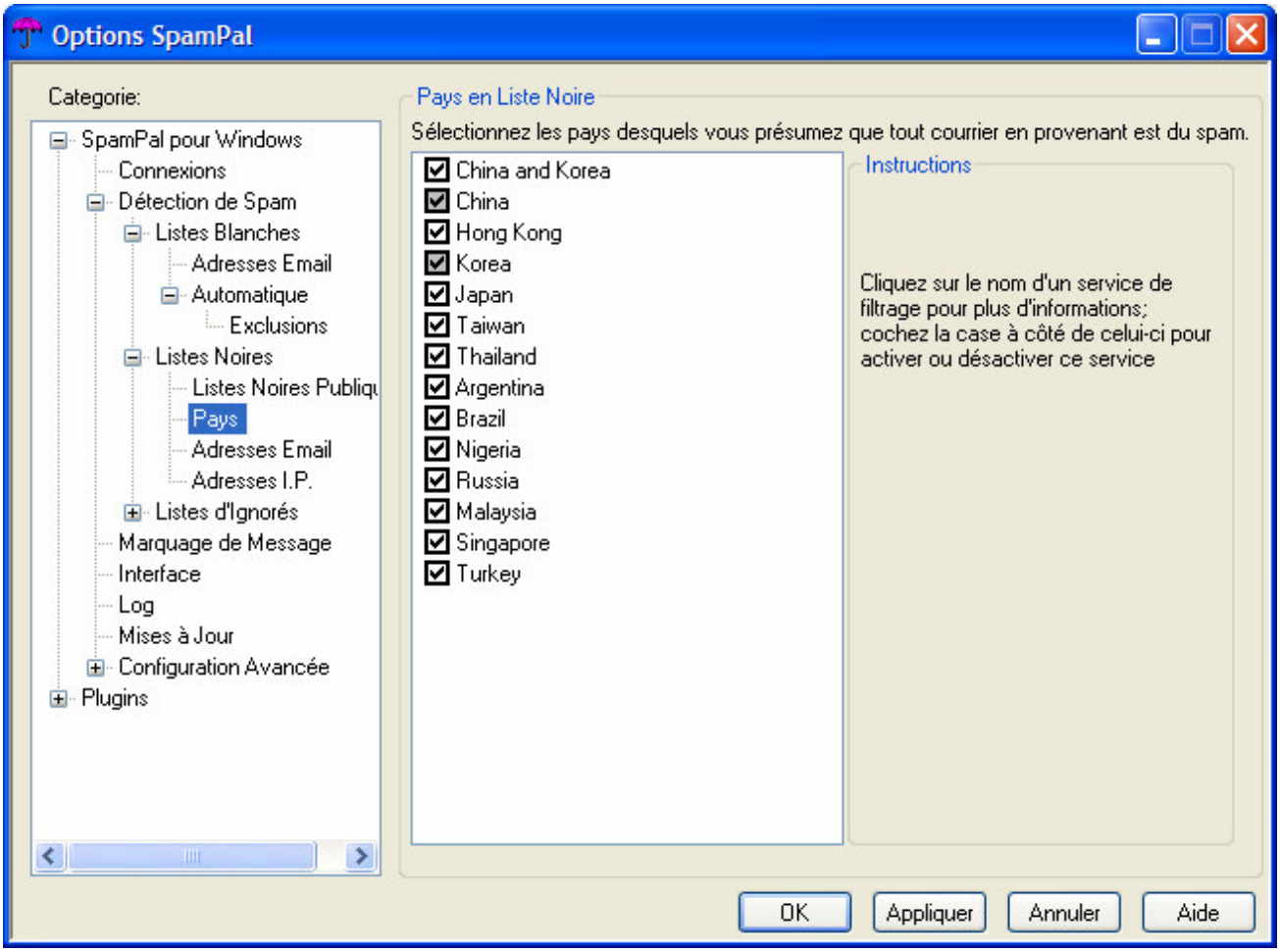
::Top::

3.5. Spam-Detection: Blacklists: Countries

If you are receiving a lot of spam from certain Countries, you can in this pane, select the Countries which you want to be blocked by SpamPal.

At the time of writing, a lot of spam seems to be routed through open relays in China. If you are absolutely sure that you never receive legitimate email from China, you could select this country in the countries blacklist.

However, you need to exercise great consideration when blocking by country, for example, if you're running a global business, you certainly don't want to be using the blocking by county feature!



::Top::

3.6. Spam-Detection: Blacklists: Email-Addresses

If you're getting lots of spam with the same email address in the From line, you can use the Blacklist to have it automatically tagged by SpamPal.

Basically, the blacklist comprises of a list email address, one per line, which will mean that all email from one of those addresses will be tagged as spam.

Blank lines are allowed in the blacklist, and you can add comments by starting them with a '#', so you can document what you put in your blacklist, e.g.: #

#Porn spammer keeps emailing me
sexygirl@bigpornspammer.com
sexygirl2@bigpornspammer.com
sexyboy@bigpornspammer.com

Chain letter pyramid scheme spammer
really_stupid_idiot@aol.com

You can also use an asterix * as a wildcard, which allows you to stop email with a given ISP in the From: line.

For example:

All I get from Hotmail is spam, so let's block it all!
*@hotmail.com

And I don't know anyone with sexy in their email address
sexy

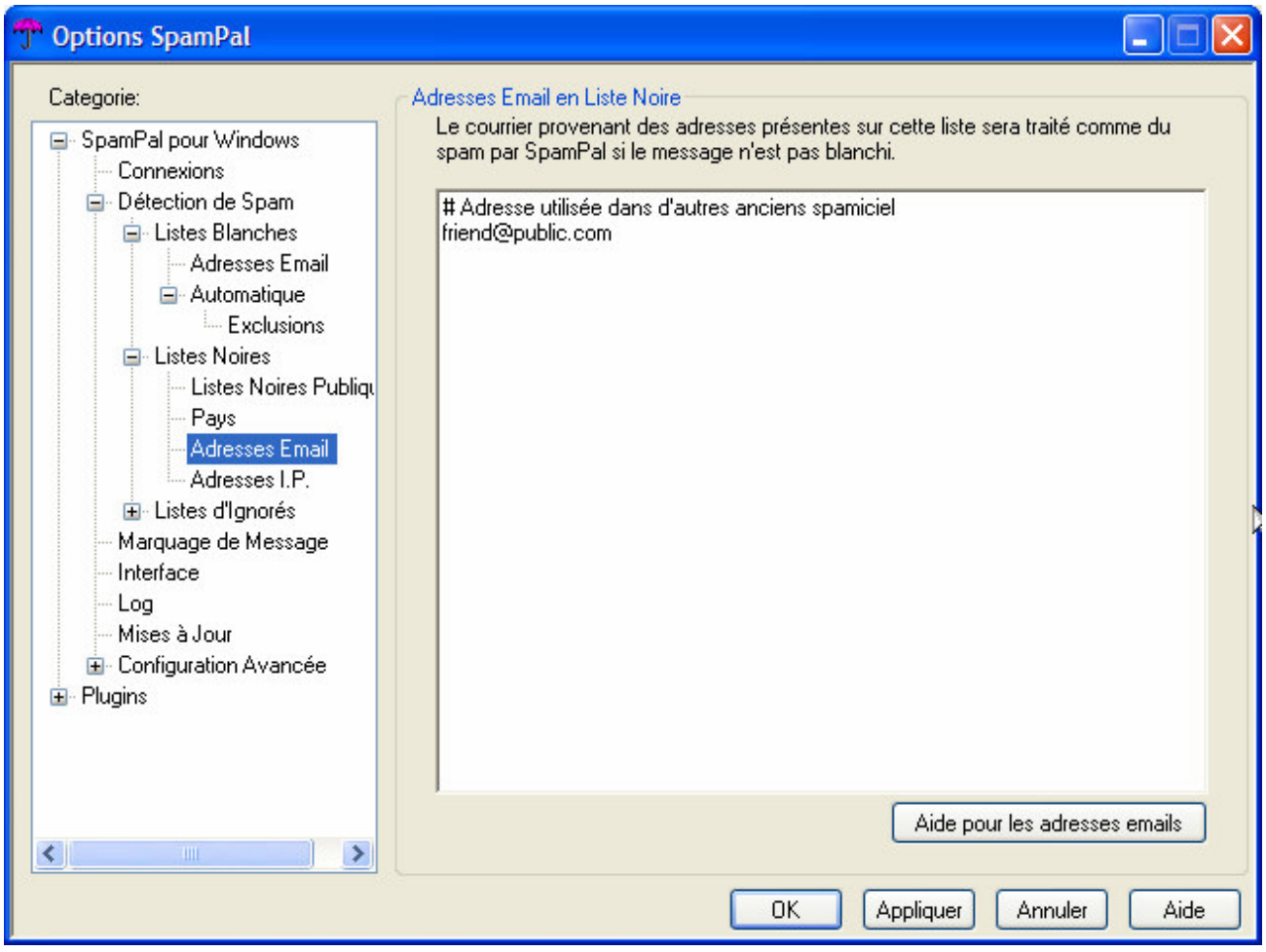
Note: Blacklist use

It's generally best not to do this for normal spam, relying on the DNSBLs or plugins to catch that.

Blacklists are more appropriate for individuals or companies who are bothering you but aren't generic spammers.

Remember also that the From: line in email messages, can easily be forged, so blacklisting the addresses of all the spams you receive, is largely a waste of time

Some email programs, such as Outlook have a Junk Mail facility which will blacklist email address, it's normally a good idea to disable this feature (which will give you a small speed boost) and just use SpamPal to do the work.

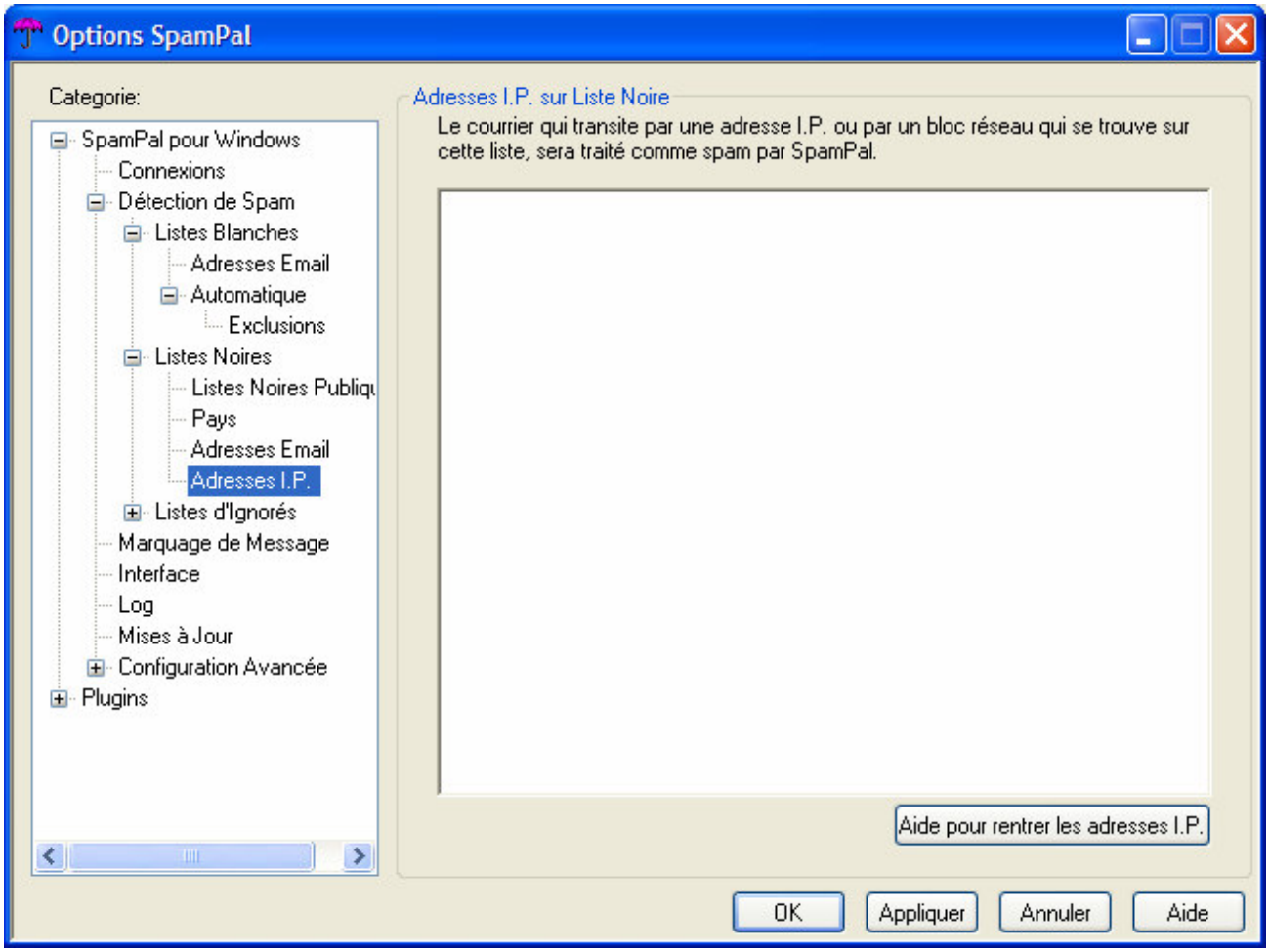


::Top::

3.7 Spam-Detection: Blacklists: I.P. Addresses

This is similar to the normal blacklist, except it works on I.P. addresses and netblocks rather than email addresses.

Like the DNSBL lists, any email from one of the machines on the advanced blacklist will be tagged as spam.



Note: how to specify address ranges

Wildcards (e.g.. 127.0.0.*) aren't permitted in netblock specifications.

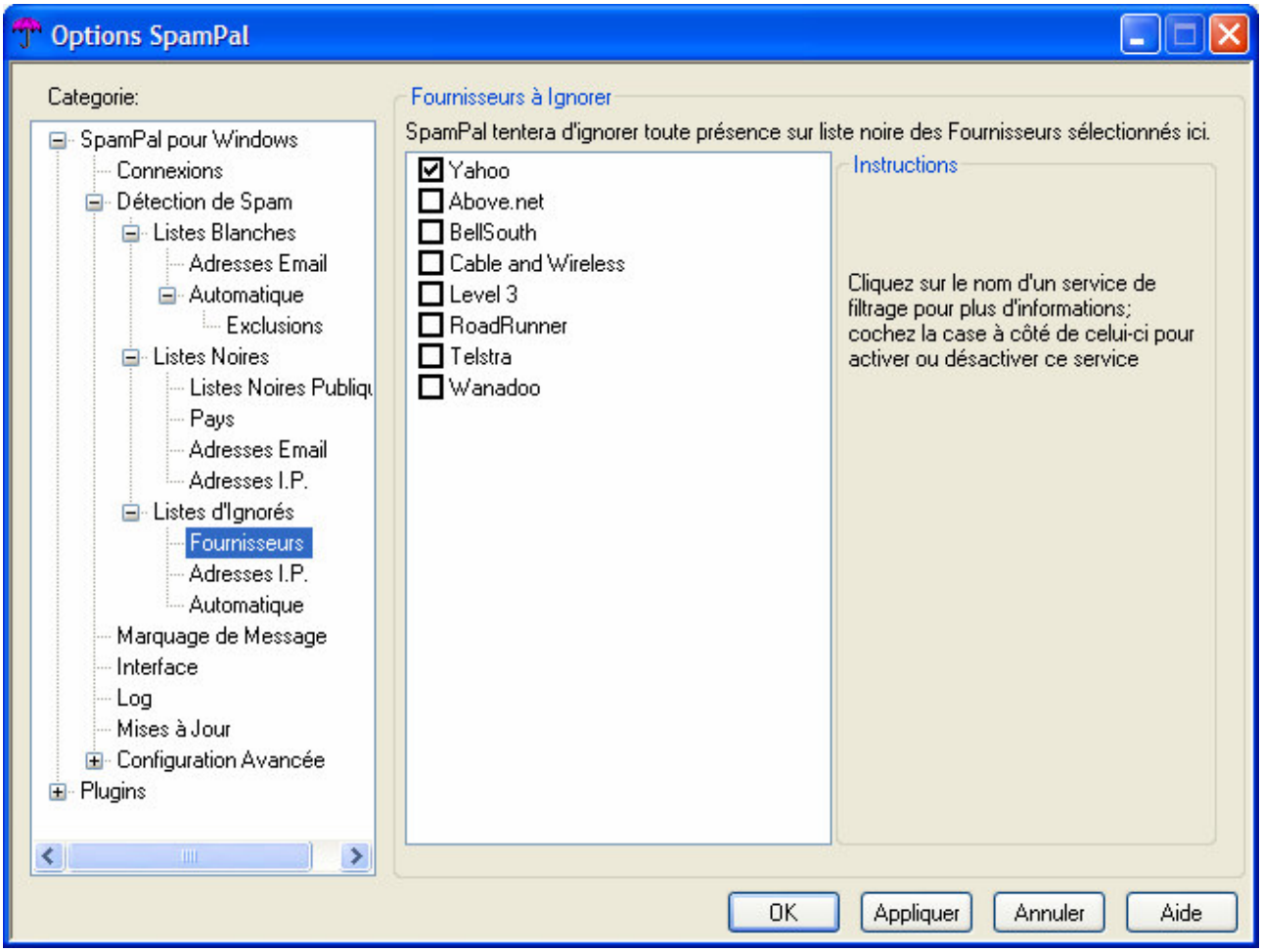
If you want to specify a range, either use the start and end addresses, e.g.: 127.0.0.0-127.0.0.255 or use the network prefix notation, e.g.: 127.0.0.0/24

::Top::

3.8. Spam-Detection: Ignore-Lists: Providers

Unfortunately, some aggressive DNSBL's might place a whole provider on one of it's blacklists.

This is a list of common providers, which if ticked, won't be checked to see if they are spammers against those DNSBL's

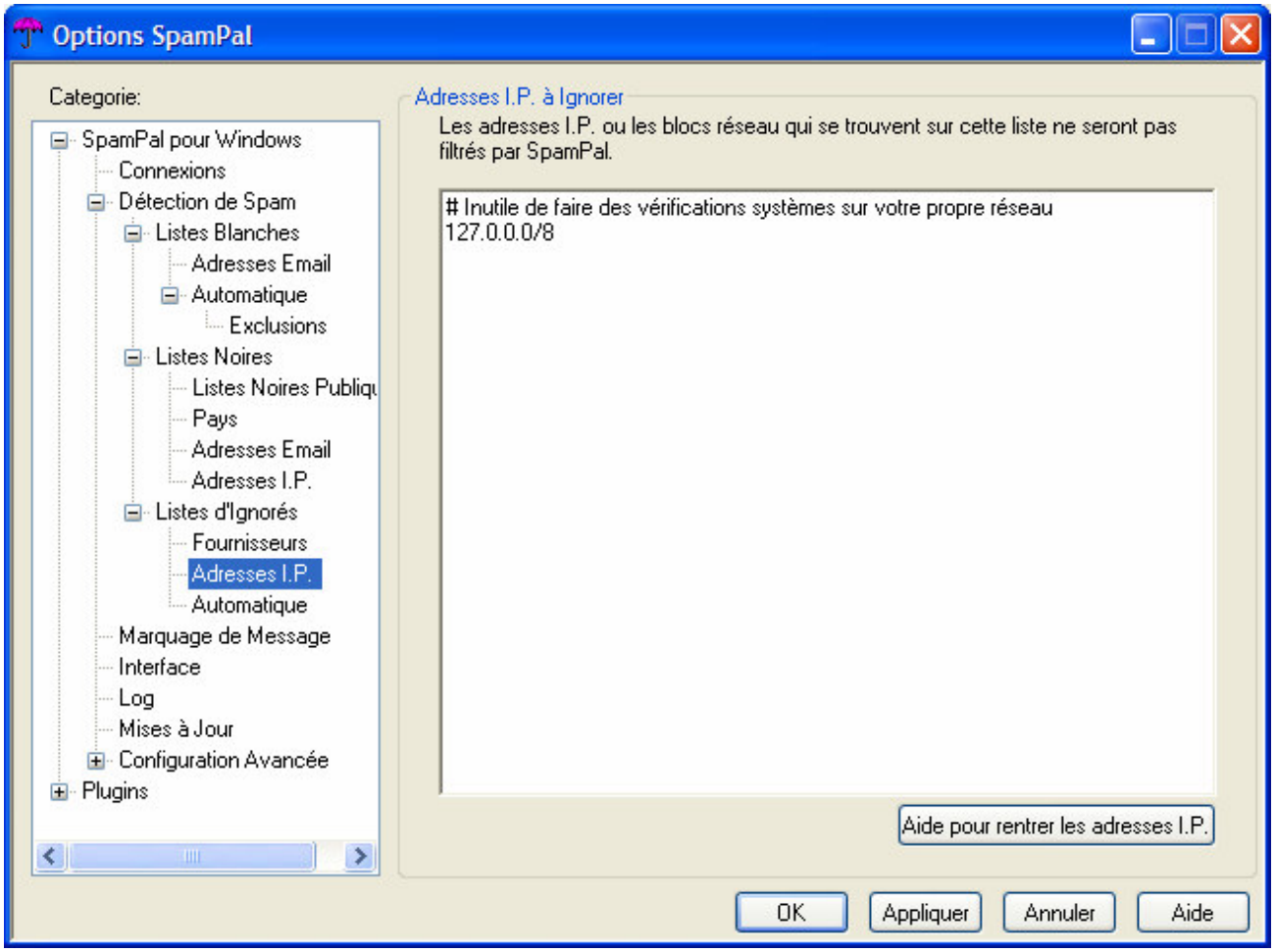


::Top::

3.9. Spam-Detection: Ignore-Lists: I.P. Addresses

This is a list of server IP addresses or ranges which won't be checked to see if they are spammers. For speed and safety you should add all of the mail servers of your own ISP, possibly taken from Received lines of mail you send to yourself, to this list.

Servers are ignored but just mentioning one of these IP addresses won't prevent a mail from being marked as spam, if another IP address in the headers, is that of a spammer.



Note 1: how to specify address ranges

Wildcards (e.g.. 127.0.0.*) aren't permitted in netblock specifications.

If you want to specify a range, either use the start and end addresses, e.g.: 127.0.0.0-127.0.0.255 or use the network prefix notation, e.g.: 127.0.0.0/24

Note 2: Example email marked as spam - but shouldn't have been

If you have an email that for some reason, you cannot whitelist by email address (or by using one of the plugins),
you can add the IP address(s) of the server(s) it uses to the ignore list, so that it's IP address(s) aren't checked against the DNSBL's (public blacklists)

Example:

Return-Path: <asasas@mail.cicg.com>
Received: from mail.cicg.com ([216.88.68.110]) by mail3-lx.icom.com (8.12.9/8.12.5) with ESMTP id h6EN50DD032210
for <me@myisp.com>; Mon, 14 Jul 2003 19:05:01 -0400
Message-Id: <200307142305.h6EN50DD032210@mail3-lx.icom.com>
Received: from mail.cicg.com (77.44.d858.cidr.airmail.net [216.88.68.119])
by mail.cicg.com (Post.Office MTA v3.5.3 release 223 ID# 0-58581U100L2S100V35) with ESMTP id com
for <me@myisp.com>; Mon, 14 Jul 2003 18:06:39 -0500

Content-type: text/plain
Date: Mon, 14 Jul 2003 18:03:55 -0500
From: ADB
Subject: **SPAM** WebRep Alert from AIR-C in MAIN
To: me@myisp.com
X-UIDL: Tc9!!T`'!=*E!>M!
X-SpamPal: SPAM DSBL 216.88.68.110

Add 216.88.68.110 and 216.88.68.119 to the Ignore List, which will stop this email being checked

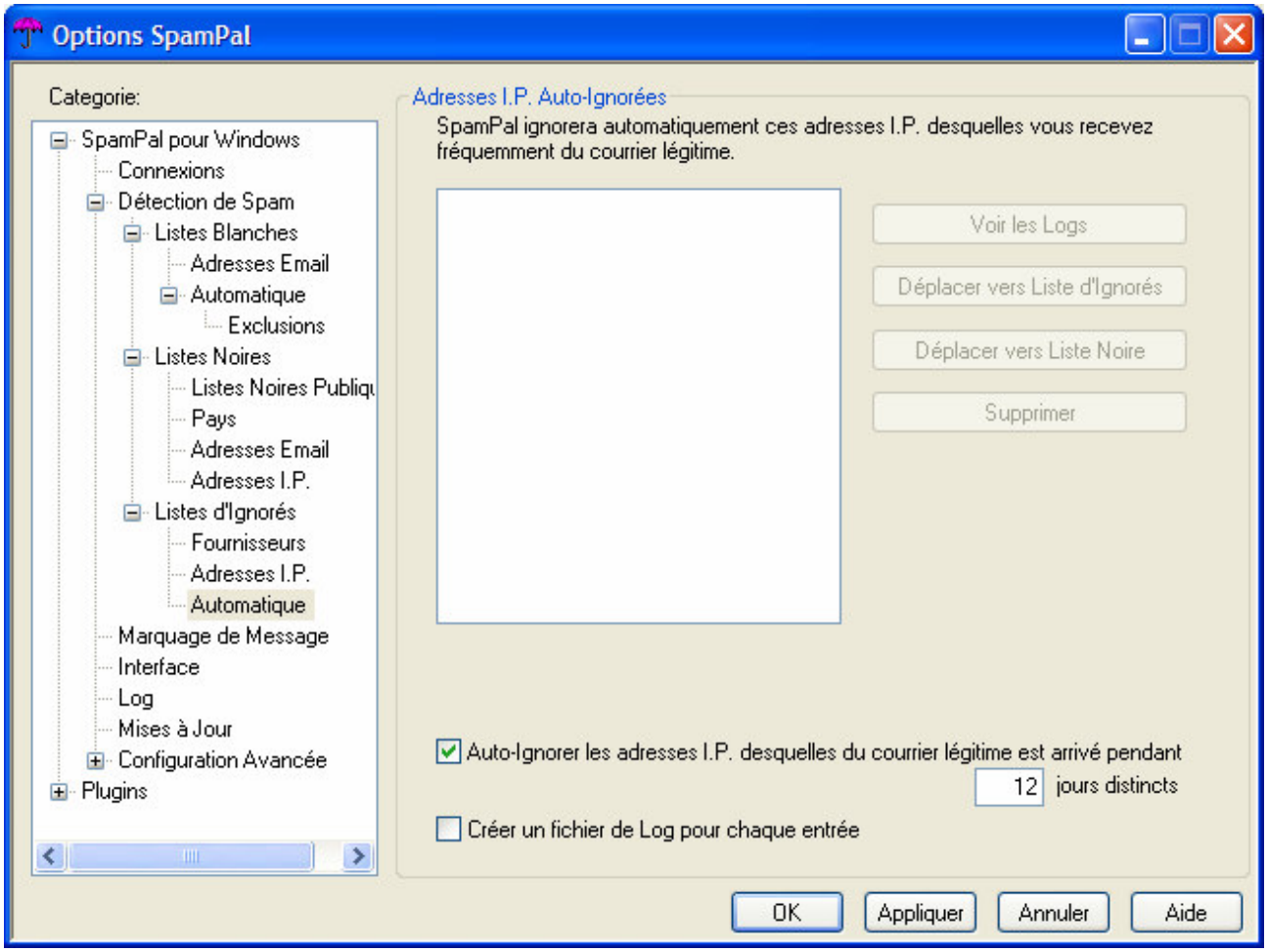
::Top::

3.10. Spam-Detection: Ignore-Lists: Automatic

This is an automatic list of server IP addresses (or ranges) from which you have received email over several days, which won't be checked to see if they are spammers,

For speed and safety the mail servers of your own ISP, possibly taken from Received lines of mail you send to yourself, will normally be addess to this list

Even though you ISP's mail servers will end up being placed on the ignored list, other IP addresses in the headers from a spammer, won't prevent a mail from being marked as spam



::Top::

4. Message-Tagging

The tagging screen controls how SpamPal marks mail subject lines and headers. It defaults to marking the Subject line with **SPAM** and adding the **X-SpamPal: SPAM** header line, after other headers.

You use the Subject line tagging in your email program's message rules, telling your email program, to move all spam messages to a special spam trap folder and/or to delete it automatically for you.

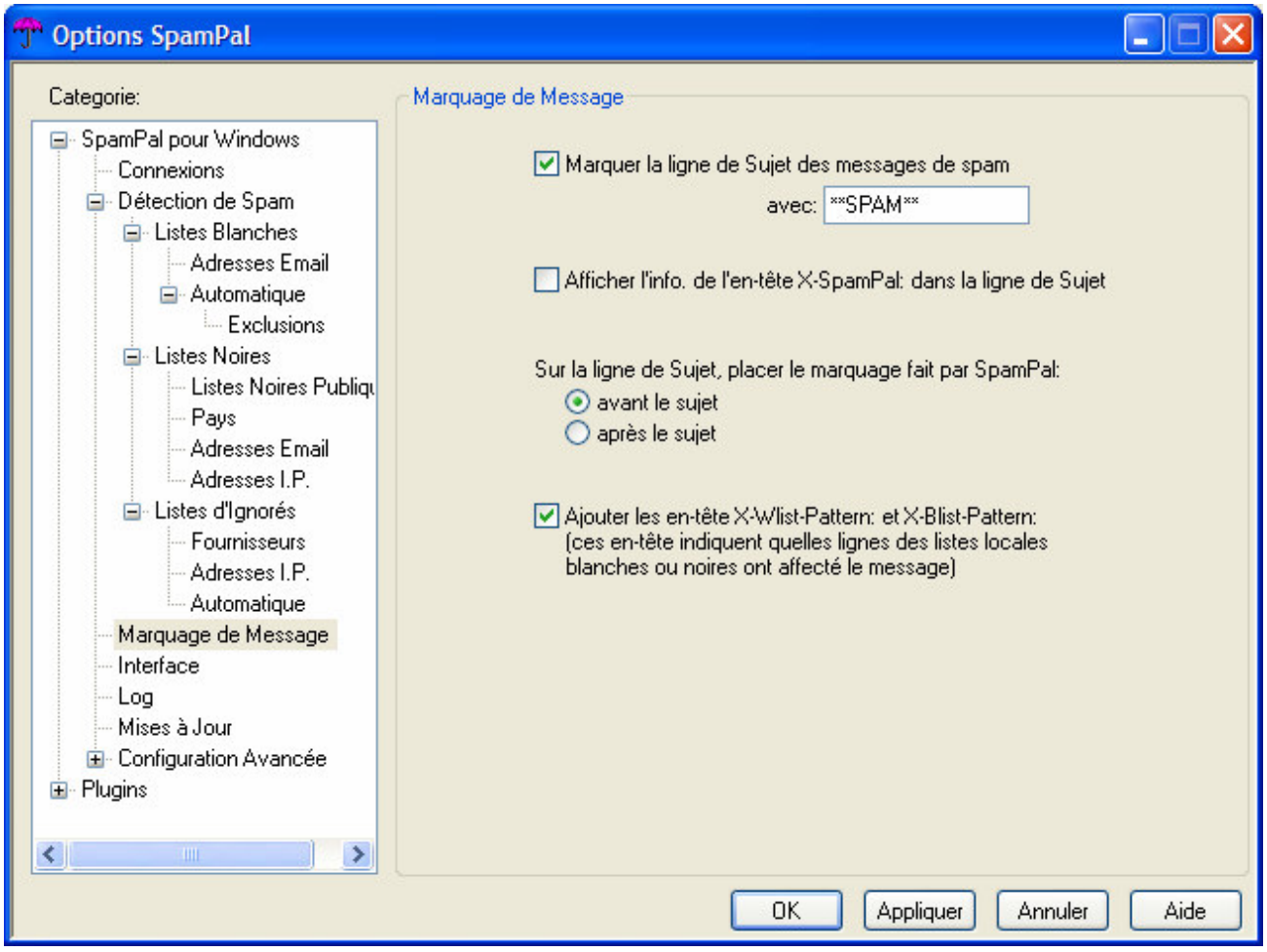
By default, SpamPal will add two items, to any messages that it thinks might be spam:

The **X-SpamPal: SPAM** header;
The string ****SPAM**** to the start of the subject line

Using the options in this pane, you can disable the second of these tags, or change it to some other string of letters, for example: [SPAM]

Alternatively, you could choose to mark the subject lines with a duplicate of the X-SpamPal: header, by ticking the Display X-SpamPal: header information in subject lines box. This will change the format of your subject lines will, to be something like this:

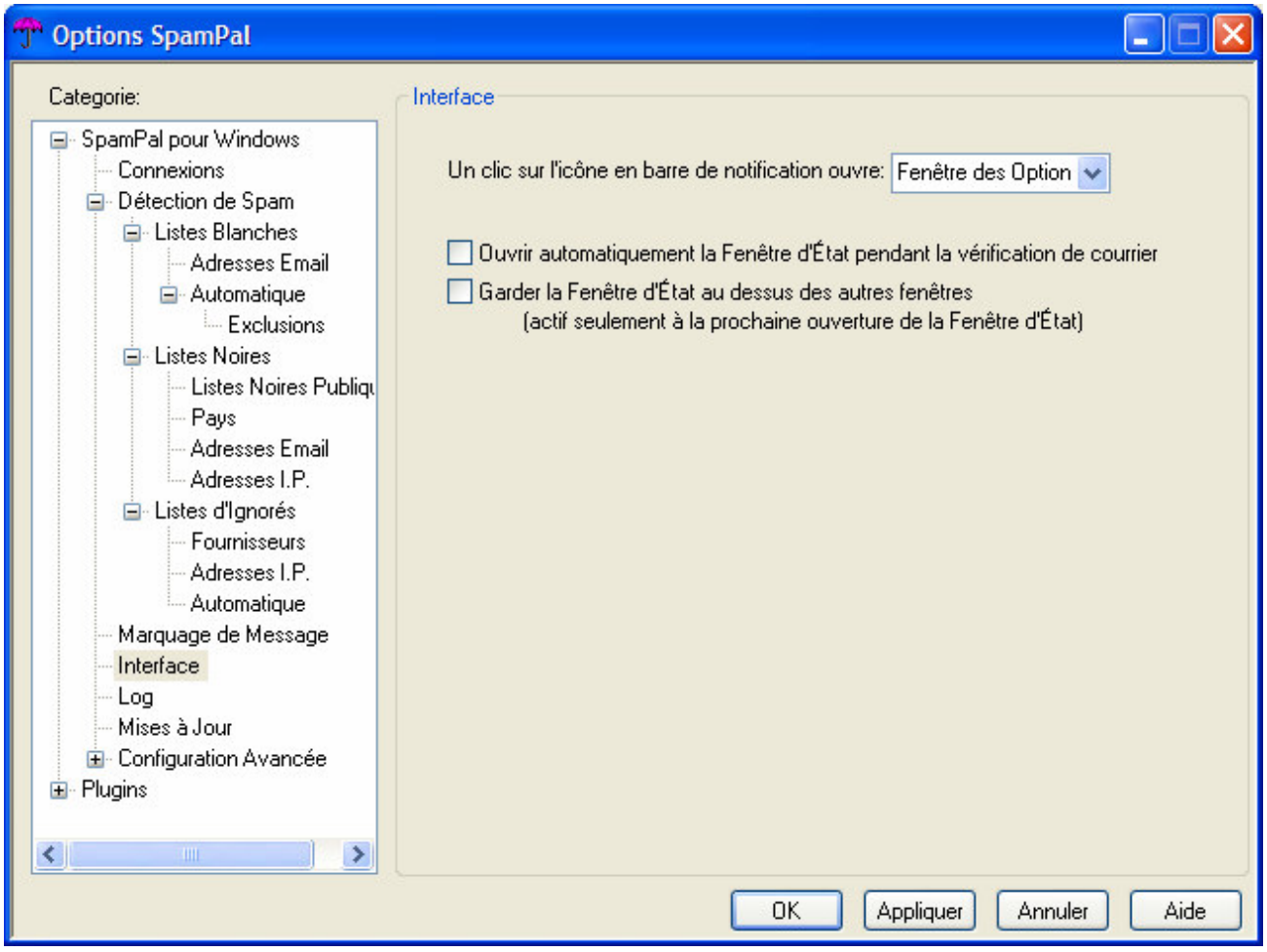
Subject: **SPAM** **SPAM OSIRU 207.218.164.32** Checking Out!



::Top::

5. Interface

Using this pane you can modify how SpamPal's User Interface works; for example, you can change which window appears when you click on the tray icon with the left mouse button, or make the status window appear automatically whilst SpamPal is active (usually while checking your emails)

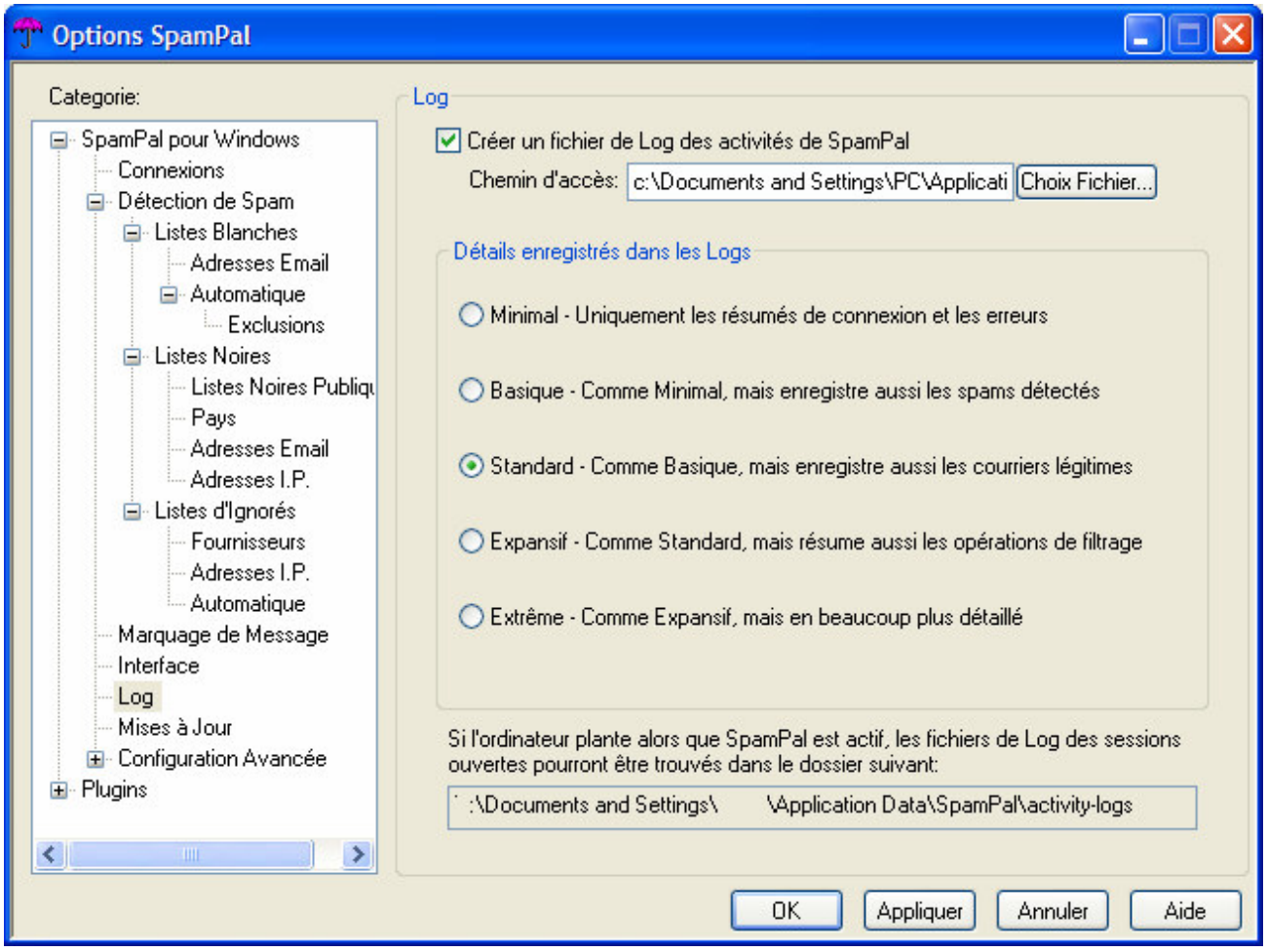


::Top::

6. Logging

This enables you to create a log file of what happens while your email program, SpamPal and your ISP's server all talk to each other, in the process of checking your mail for spam.

The main aim of this screen, is to help SpamPal Support find any problems you may be having, while all the email processing takes place and therefore help fix future versions of SpamPal.



::Top::

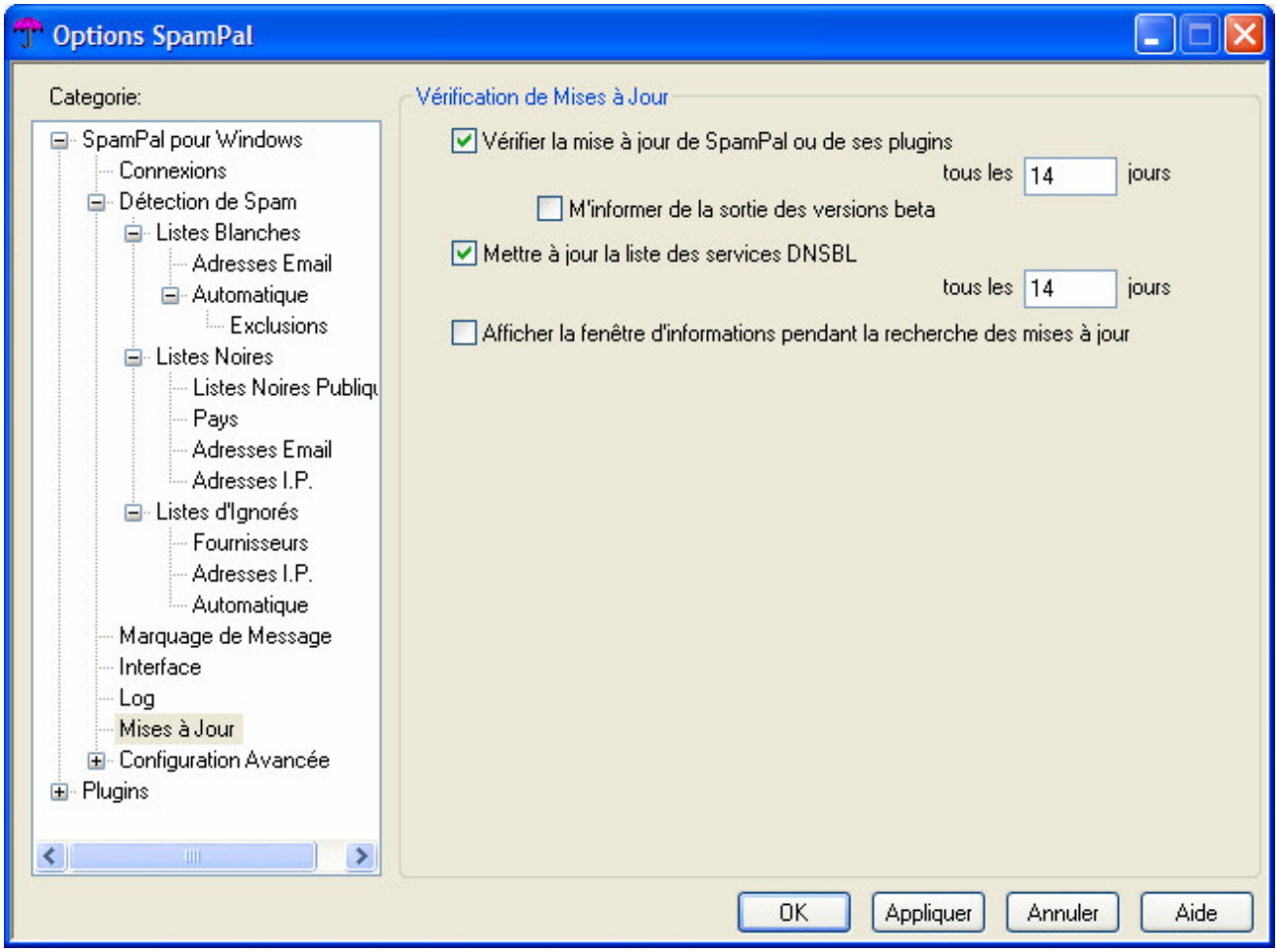
7. Updates

Every so often, SpamPal will check back with the SpamPal website to see if there's a new version of the program available, and to download an updated list of DNSBL services.

This pane also allows you to control this process, by specifying how often each check takes place, and whether you'd like a window to open to inform you when they're happening.

You don't have to check for updates every day, so the default settings shown here, should be fine for most people. If you really have to, you can manually check for updates.

The update process is explained in more detail here.



::Top::

8. Advanced

This panel enables you to alter various advanced options (although most users will not need to change anything in this panel)
DNSBL Queries time out after; DNSBL services are sometimes overloaded with requests, and can be rather slow. To prevent your mail checking from becoming prohibitively sluggish, SpamPal will time-out (stop waiting for) DNSBL queries after 20 seconds.

You can use this option to change this interval; lengthen it if you're seeing the X-SpamPal: PASS TIME-OUT header a lot and don't mind your email checking taking longer; shorten it if checking your mail seems to take forever and you don't mind a few extra spams not getting filtered into your spamtrap folder.

Maximum simultaneous DNSBL queries; allows you to set how many DNSBL queries SpamPal should make at the same time. If you use lots of DNSBL lists and/or check lots of mailboxes simultaneously, increasing this figure can result in a performance increase.

Don't filter mail at all; allows you to disable all of SpamPal's spamfiltering features. This options is also available from the systray

Don't filter mail using auto-whitelist or auto-ignorelist; disables filtering of mail against the automatic whitelists. Note that email & I.P. addresses will still be added to the automatic whitelists, it's just that they won't have any

affect. It effectively turns the automatic whitelists into lists of seen email and I.P. addresses that are candidates to be moved to the whitelist after due consideration.

Remember positive (spam) DNSBL results & Remember negative (non-spam) DNSBL results; allows you to control for how many days SpamPal should cache the results of queries to DNSBL services. The higher each of these are set, the quicker your mail will be fetched, but at increased risk of SpamPal using out-of-date information and making more mistakes.

Allow multiple port setting to share a single port number; This allows you to effectively have to sets of port configurations using a single port number; when a connection comes in, SpamPal will use the following criteria to choose between them:

- If the connection is coming from an I.P. address that is only on the access control list of one of the port settings, those settings are used.
- If the connection is coming from 127.0.0.1, then SpamPal will get the real I.P. address of your machine and perform the first test again.
- If SpamPal still can't decide which port settings to use, it will prompt the user to choose between them. The user can choose to have their selection remembered until SpamPal restarts, or to choose again for each incoming connection to this port.

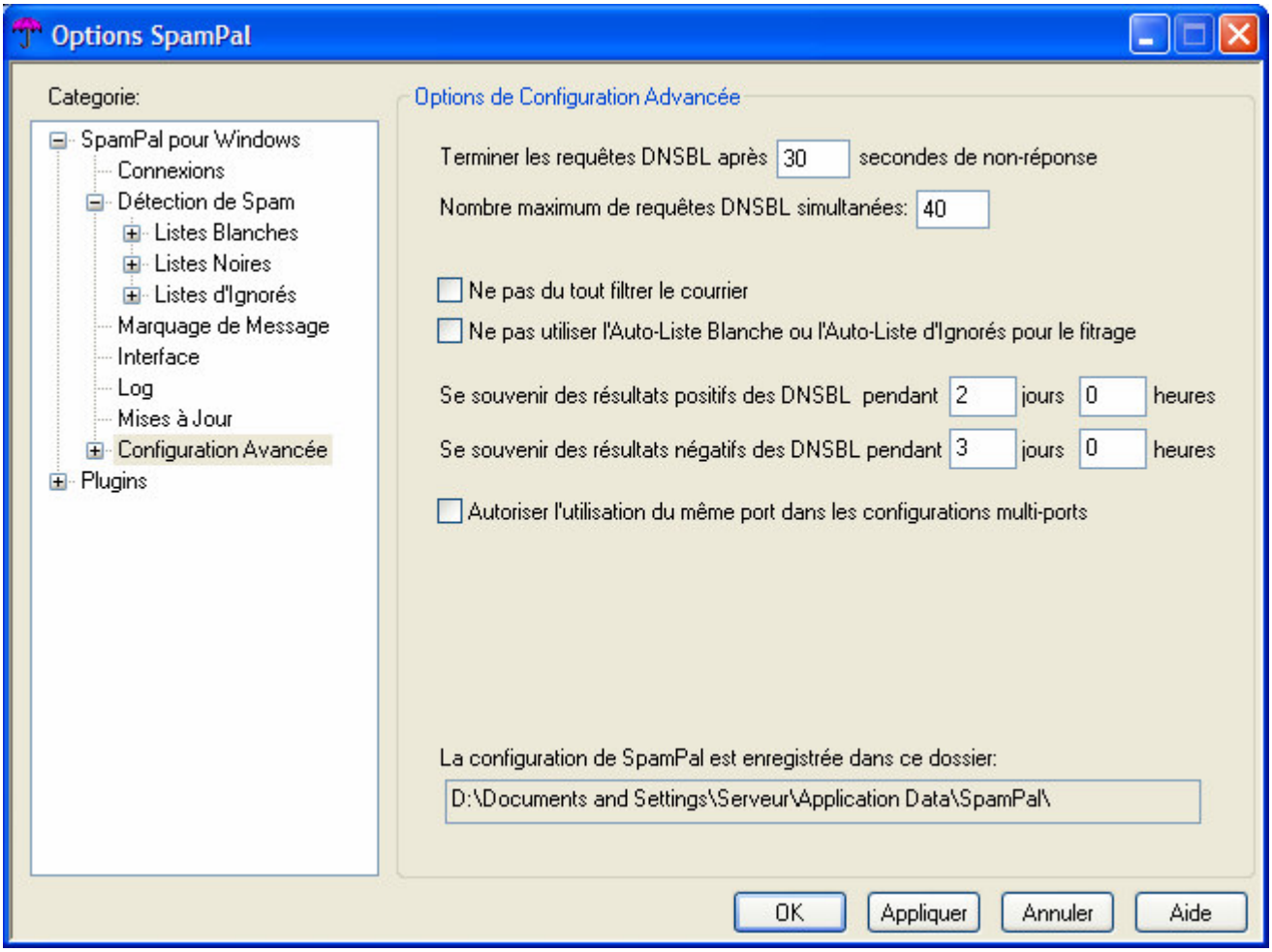
How could this be useful? Well, let's take the example of SpamPal's SMTP proxy. Let's say you use two ISPs, example.com and lapmaps.com. You want to use the SMTP server of whichever ISP you happen to be dialled into. You could add a setting for both mail.example.com and smtp.lapmaps.com to the ports list in SpamPal, make both settings use port 25, and then when you want to send mail SpamPal will prompt you to choose which you want to use.

Is this a security risk?

The access control lists determine what I.P. addresses are allowed to connect to SpamPal. However, as long as SpamPal is configured to listen on 127.0.0.1 (click on IP Configuration in the Advanced options pane), only the local machine will be able to connect to SpamPal regardless of what you put in the access control lists. So, while SpamPal is listening on 127.0.0.1, this is not a security risk.

Spampal's configuration is stored in this folder; This is the directory:

- where SpamPal stores it's own configuration files and also of it's plugins.
- that needs to be backed up, if you are thinking of reinstalling your operating system.



Note: some speed tips

- You can also tune the number of connections SpamPal makes; go to the advanced settings and increase the Maximum Simultaneous DNSBL queries to **50** (if you are on broadband/cable/adsl)
- Don't set the caching times too low

::Top::

8.1. Advanced: Lan Configuration

SpamPal is designed as a personal mail filter that will run on same local machine as your email client. It contains many features that specifically tailored to this way of working.

However, some people have expressed a wish to run SpamPal as a service for a local network. Although this isn't advised, it is now possible.

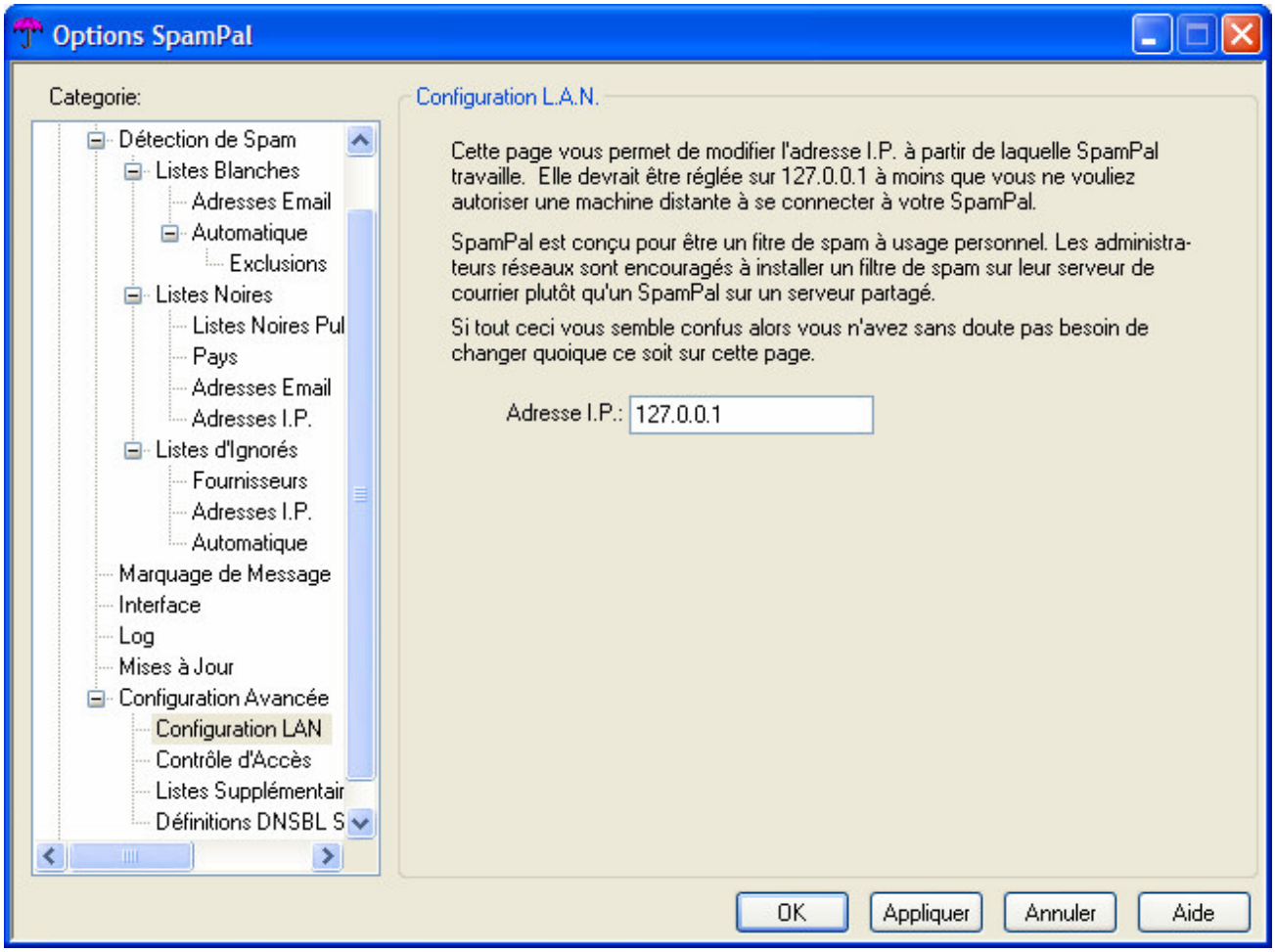
But before doing it, please consider:

- SpamPal has a GUI, and pops up error boxes in various circumstances.
- The auto-whitelist has privacy implications if SpamPal has more than one user.
- Tagging mail on retrieval (which SpamPal does) is not the most efficient way of doing it. A far better solution is to tag mail when it is received by your mailserver. If you're at the stage of running SpamPal on a local network, you probably have a mailserver; investigate the spamfilters that can be installed on it.

If after reading this you still want to be able to connect to SpamPal from a remote machine, here's what to do.

Go SpamPal's Options pane and then select the Lan Configuration pane.

Change the I.P. address setting from 127.0.0.1 to the I.P. address of the machine on which SpamPal is running. Now, go to 8.2 (Access Control) for the next step.

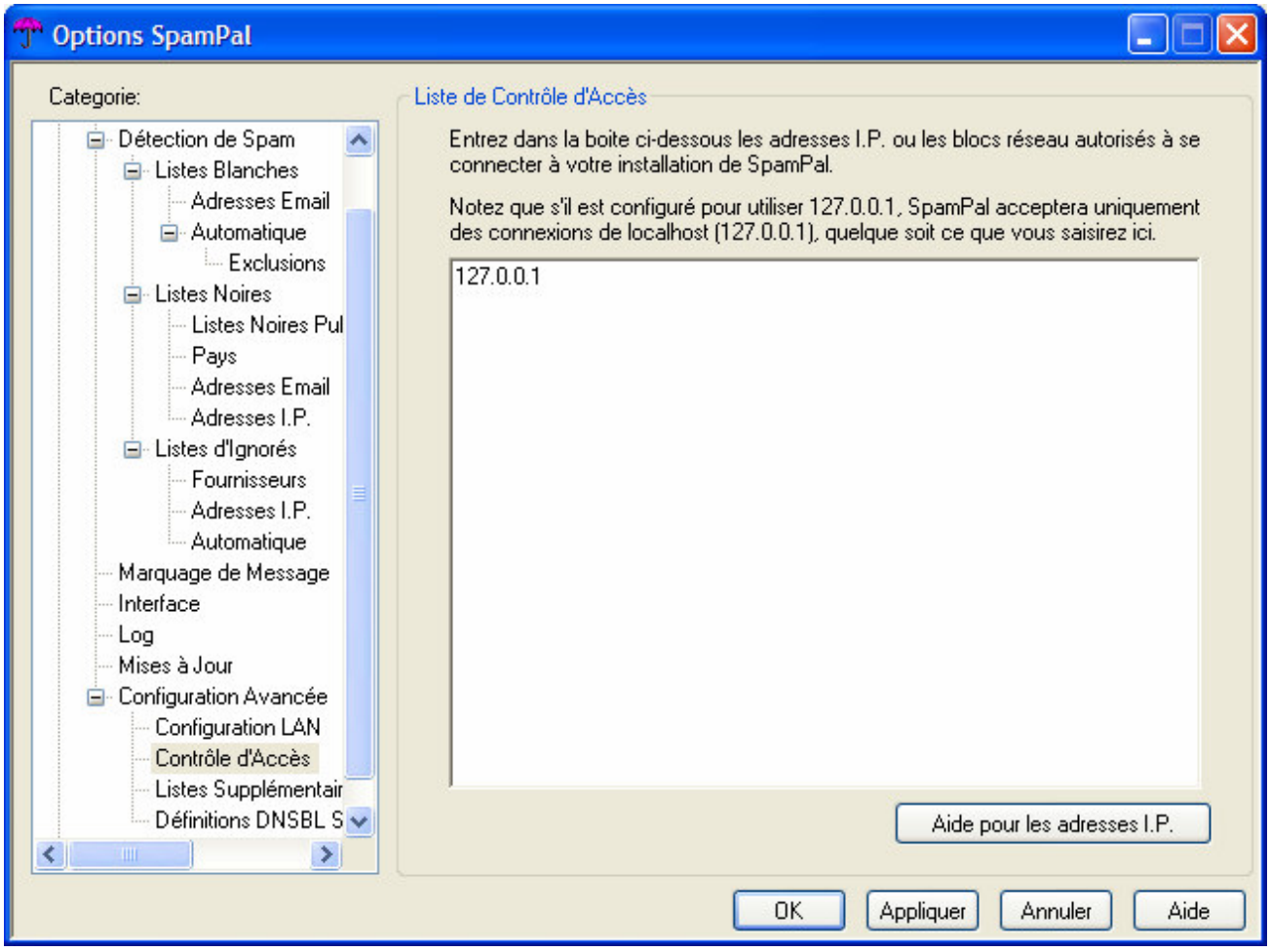


::Top::

8.2 Advanced: Access Control

Following on from the 8.1 (Lan Configuration) instructions, type the I.P. addresses of the machines that will be permitted to connect to SpamPal, one on each line.

You can specify a range of I.P. addresses using either the network prefix notation (e.g. 127.0.0.1/24) or by giving the start and end of the range (e.g. 127.0.0.1-127.255.255.255).



Note: IP Addresses - Remote Access

When you enter the IP address, be very careful when you do this - you don't want to accidentally allow external
machines to connect to SpamPal!!!

::Top::

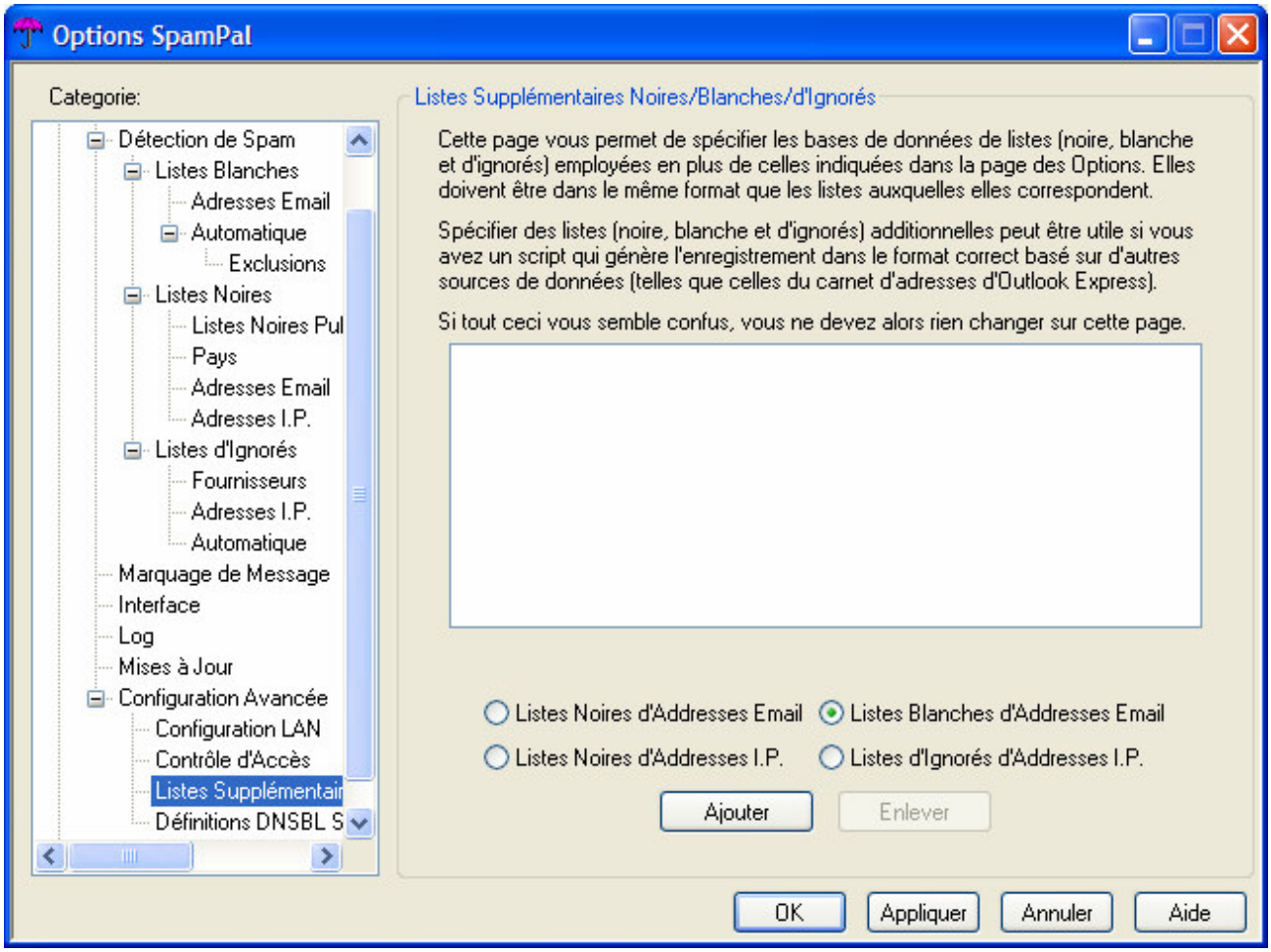
8.3 Advanced: Extra Black/White/Ignore Lists

This pane can be used to a add the filename and location of a text file, which contains a list of email address (or IP addresses) to whitelist, blacklist or ignorelist.

The advantage of using this feature over the normal whitelist, is that it's easy to keep things organised neatly by topic and it also makes it easy to update them at different times.

For example:

C:\spampal\friends.txt - could contain all your friends that you want to whitelist
C:\spampal\work.txt - could contain your work contacts that you want to whitelist

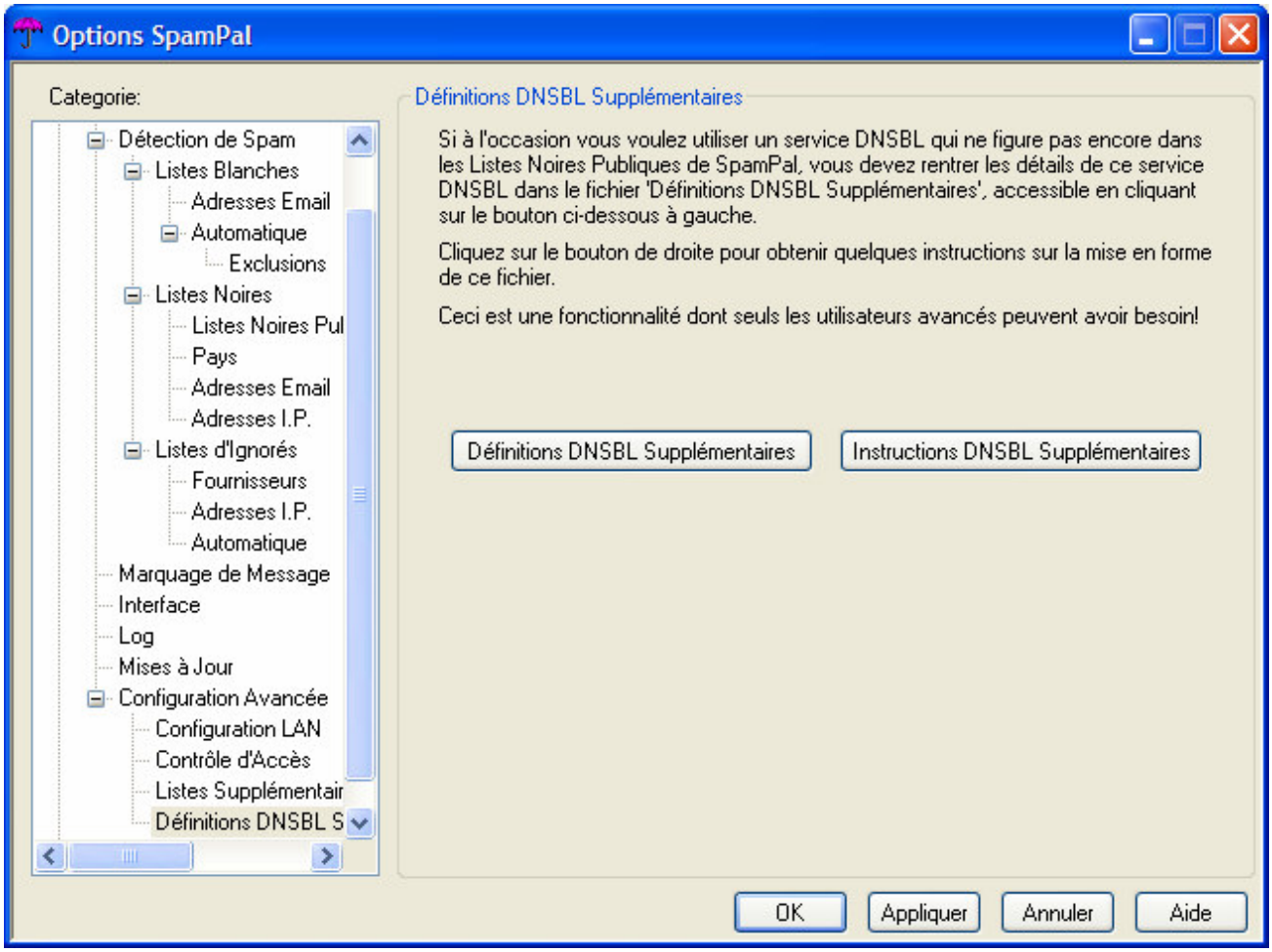


::Top::

8.4 Advanced: Extra DNSBL Definitions

In this pane, you can add an extra DNSBL service, that isn't currently listed in SpamPal's normal blacklist/ignorelists pane.

In order to add a new DNSBL, you must first click on the Extra DNSBL Definitions button (see screen below)



Windows notepad should now open the extra_dnsbl.txt file, located in your spampal directory. In this file, you will see an example of what information is needed to enable you to add an extra dnsbl.

For example, the Composite Blocking List is a quite good dnsbl; to add this to your public blacklists (dnsbl), cut and paste the following, onto the end of your extra_dnsbl.txt file:
LIST CBL
NAME Composite Blocking List
WEBSITE http://cbl.abuseat.org/
ZONE cbl.abuseat.org
DESCRIPTION The CBL takes its source data from very large spamtraps, and only lists IPs exhibiting characteristics which are specific to open proxies of various sorts
Save it, click OK to dismiss the SpamPal options window then open it again - CBL should now be listed with the other blacklists.

However, you will now need to enable this extra CBL dnsbl by going into SpamPal's Spam Dection: Blacklist: Public Blacklist pane, finding the CBL dnsbl entry and ticking the enable box.

Now, when you check your status screen, you should start to see results from your new CBL dnsbl

::Top::

9. Plugins

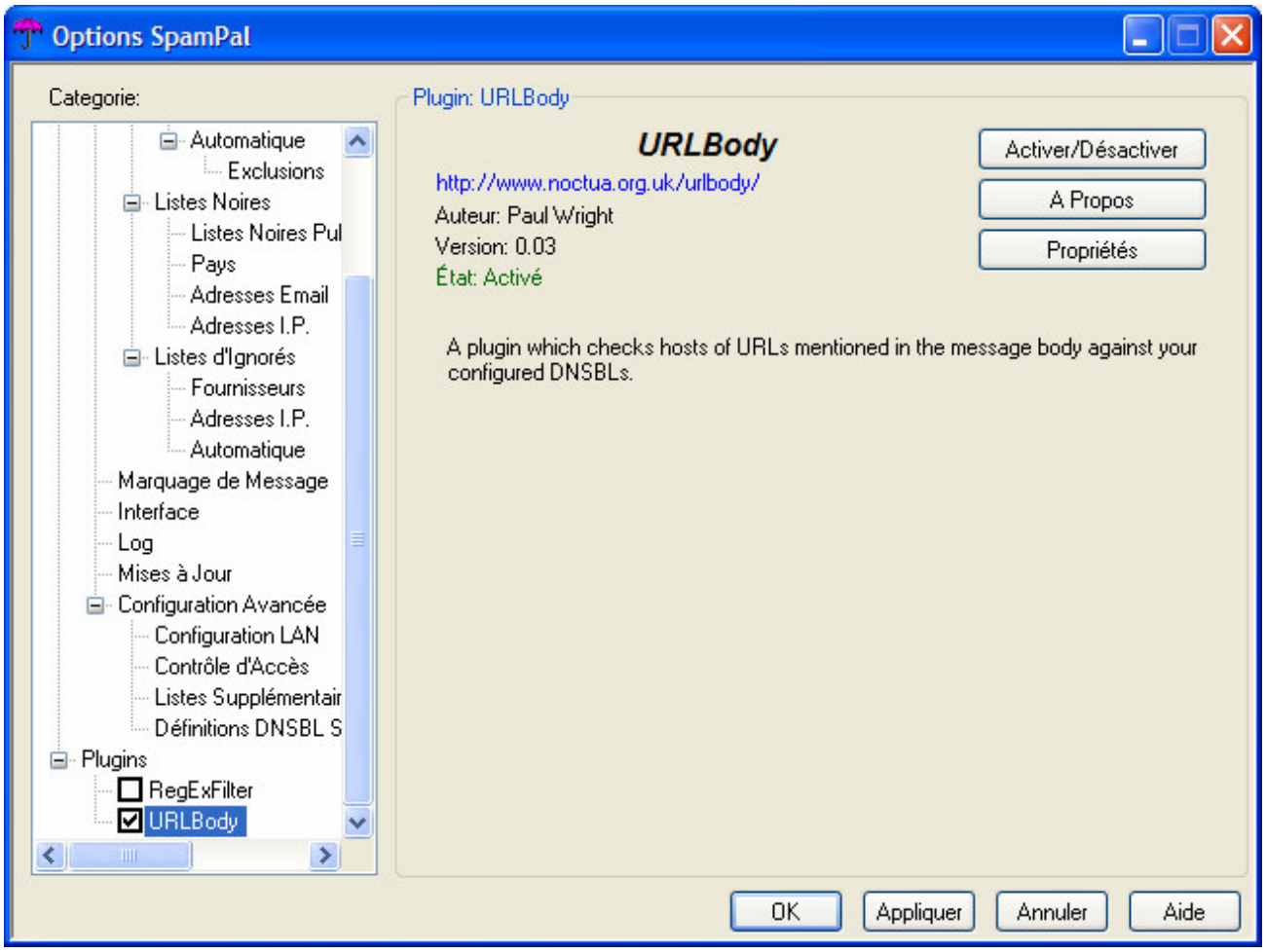
You can add extra spam-filtering capabilities to SpamPal by installing Plugins.

Plugins are the second key to how SpamPal filters out the spam. SpamPal has a powerful plugin

interface and documentation to allow others to add extra features to SpamPal. Plugins are available for Bayesian filtering, regular expression filtering, censoring web bugs, logging, spam quarantining, extra DNSBL blocking functions and more.

You can obtain plugins from the SpamPal website; install them in the plugins directory within the SpamPal installation and they will appear on this pane, but you will have to click on them and then click on Enable/Disable to enable them before they will work.

Try the core DNSBL filtering before adding plugins - the DNSBLs are very effective and may be all you need.



::Top::

10. Command Line options

Although SpamPal has a graphical user interface, it does have a few useful command line options...

::Top::

10.1 Command Line options: Configuration Directories

SpamPal stores its configuration files in the user profile, or failing that in it's own installation directory.

Advanced users who wish to alter this can do so by specifying an alternative directory on the command-line, using the -configdir switch.

For example:

SpamPal.exe -configdir c:\my_spampal_configdir (If the specified directory does not exist, it will be created)

This will mean that all SpamPal and Plugin data will now be stored in the c:\my_spampal_configdir directory, which has two advantages:

a) It's easy to backup (see here)

b) as this can be a common directory, it means that more that one user can share the SpamPal settings, for example, on a windows XP system, that is using it's multi-user logon feature.

::Top::

10.2 Command Line options: Multiple Instances

Normally, you can only run one copy SpamPal at a time. If for some reason you want to run multiple copies of SpamPal on the same machine (for e.g., if you want to listen on two different ports with a different configuration on each), you should add -allow_multiple_instances yes, to the command-line

e.g.:

SpamPal.exe -allow_multiple_instances yes

If you only want to run one version of SpamPal, but don't want to see an error message if you should try to run a second (e.g. if you're starting it from a batch file that may get run multiple times), you can use the option -suppress_multiple_instances_warning yes,

ie:

SpamPal.exe -suppress_multiple_instances_warning yes

Obviously, combining these two command-line options would make no sense at all.

::Top::

10.3 Command Line options: Tray Icon

SpamPal will put a small icon in the system tray to allow you to access its configuration options.

If you don't often use this icon and you don't want it cluttering up your tray, use the command-line option -trayicon none,

e.g.:

SpamPal.exe -trayicon none

Of course, if you do this then to access SpamPal's configuration, you will have to; exit it from the task manager and restart it - without this option on the command-line.

::Top::

Contenu > Glossaire

Voici quelques termes que vous pouvez rencontrer dans le manuel ou sur les forums.

Terme	Description
UCE	Terme anglais "Unsolicited Commercial Email" (message commercial non sollicité), ou spam
DNSBL (DNS Blacklist) Liste noire DNS	Il s'agit d'un type de filtre basé sur l'adresse internet de la connexion entrante de messagerie. Pour faire simple, la connexion commence par un "bonjour" (HELLO) arrivant depuis un autre serveur de messagerie. Le filtre DNSBL est conçu pour rechercher et comparer l'adresse de provenance du message à la liste disponible en ligne des adresses indésirables. Cette liste se trouve dans un serveur DNS, à une zone ou un domaine spécifique. Si l'adresse de provenance est en liste noire, (c'est à dire si cette adresse est trouvée sur le serveur DNS) la connexion est refusée. Ceci arrive très tôt dans l'échange de message avec le serveur SMTP (Simple Mail Transport Protocol). La DNSBL (aussi connue sous le terme RBL ou "Real-time Blackhole List" : liste trou noir temps réel) consiste en une zone d'adresses IP sur un serveur DNS particulier ou une hiérarchie de serveurs. Ces données sont basées sur les plaintes, sur des vérifications automatiques, des statistiques, des informations provenant des bases de propriétés des domaines internet (WHOIS), etc.
Relais ouvert	Par définition, un relais ouvert permet à quiconque, de n'importe où, d'envoyer des messages par l'intermédiaire d'un serveur de messagerie, ce qui cause la majorité des cas de spam. Votre serveur de messagerie a été piraté. C'est une tactique fréquente des spammers commerciaux qui essaient d'utiliser le serveur d'un tiers pour cacher la source de leurs messages ou contourner le blocage de leur compte.
Scam Nigérian 419	Ainsi appelé parce qu'il viole la section 419 du code criminel Nigérian. Ces scam viennent souvent, pas toujours, du Nigéria (dernièrement, on en découvert venant d'Irak). Le scam, c'est lorsque vous recevez un message signé par un officiel du Nigéria ou d'un autre état d'Afrique, qui vous dit que quelqu'un a besoin de transférer une grosse somme d'argent hors du pays et que vous avez été retenu pour les y aider. En dédommagement de votre aide, vous toucherez une commission très importante. Tout ce que vous avez à faire est de payer une sorte d'avance ou de taxe de transfert, voire de leur donner votre numéro de compte afin qu'ils puissent y virer l'argent.

Entêtes	Les entêtes sont les blocs de lignes d'information qui apparaissent au début d'un message ou d'une news. Les entêtes identifient l'émetteur et le destinataire du message, le chemin pris par le message pour aller de l'un à l'autre. Les entêtes peuvent aider à identifier l'origine réelle d'un spam.
Relayer	L'acte de transférer un message (comme un email ou un news) d'un serveur de messagerie à un autre.
Opt-In	C'est la méthode de choix de réception des messages de publicité. Dans cette méthode, l'utilisateur doit expressément exprimer son choix de recevoir des messages. L'Opt-in est considéré comme le seul moyen légitime du marketting par email. C'est la méthode prônée par l'Europe.
Opt-Out	Dans la méthode Opt-out, l'utilisateur est inscrit comme destinataire de messages publicitaires a son insu ou sans sa permission Il peut cependant demander à être retirer de la liste. Méthode qui fait la part belle aux spammers et retenue par les USA.
POP3	POP3 : abréviation de Post Office Protocol - protocole utilisé pour la délivrance des messages sur Internet.
IMAP	IMAP : abréviation de Internet Message Access Protocol. C'est un moyen de gérer les messages sur un serveur distant, similaire au protocole POP3.
SMTP	Abréviation de Simple Mail Transfer Protocol. C'est le protocole le plus répandu pour le transfert des messages entre serveurs.
Serveur PROXY	Un serveur proxy est un serveur qui agit comme intermédiaire entre l'ordinateur de l'utilisateur et Internet

Port	Nom habituel	Utilisation	Description
25	smtp	serveur SMTP	Transfert de message de l'utilisateur vers un serveur ou entre serveurs
110	pop, pop3	serveur POP	Permet à l'utilisateur de récupérer son courrier sur un serveur distant
143	imap	serveur IMAP	Permet à l'utilisateur de récupérer et de gérer son courrier sur un serveur distant
465	smtps	protocole wsmtp via TLS|SSL	SMTP via SSL connexion cryptée (messagerie sécurisée)
993	imaps, simap	IMAP via SSL	IMAP via SSL connexion cryptée (messagerie sécurisée)
995	pop3s, pops, spop	POP via SSL	POP via SSL connexion cryptée (messagerie sécurisée)

Contenu > Messages d'erreur

Voici quelques messages d'erreur que vous pouvez rencontrer en utilisant SpamPal :

Message d'erreur	Causes et solutions
a. Le programme Email n'arrête pas de demander le mot de passe b. Il y a un problème de connexion à votre serveur de courrier c. Mauvais nom de serveur d. Incapable de résoudre le nom du serveur e. Votre nom d'utilisateur est incorrect f. Mot de passe incorrect	(Réponses aux messages d'erreur a. à f.) La cause la plus probable de cette erreur est que vous avez entré une mauvaise configuration dans votre client email. D'habitude, c'est parce que vous avez indiqué votre adresse email normal dans le champ Nom d'utilisateur au lieu de userid@pop3servername. Cela ressemble beaucoup mais ce n'est absolument pas la même chose. Une autre erreur commune est une erreur de frappe dans l'orthographe. Vous pouvez aussi obtenir cette erreur si vous avez indiqué le mauvais type de **connexion** POP3 dans le réglage de votre programme email. Pour SpamPal, allez dans Options, Connections. Si le port POP3 est configuré à POP3 (tout serveur), votre programme email doit être configuré avec un nom d'utilisateur user@pop.server.name et un nom de serveur de 127.0.0.1 ou localhost. C'est la configuration recommandée de SpamPal. Néanmoins, si vous avez utilisé ces paramètres mais avez configuré SpamPal en POP3 (un seul serveur), vous aurez une des erreurs ci-dessus. Si les causes précédentes n'expliquent pas le problème, c'est probablement le même problème que l'erreur 10053.
Pas de serveur	Si vous essayez d'accéder au mauvais port de votre machine, vous obtiendrez cette erreur, C'est à dire, si les ports entrant et / ou sortant de client email ne sont pas bien configurés. Normallement, le c**ourrier entrant** POP3 passe par le port 110 et le **courrier sortant** par le port 25.

Erreur 11001	Dans votre programme email, vous avez probablement mal entré le nom du serveur. localhost s"écrit en un seul mot qui doit être tapé tel quel. Si localhost ne fonctionne pas, essayez à la place 127.0.0.1.
Erreur 10053: Le logiciel a provoqué la perte de connexion	La cause la plus probable est que votre firewall empêche SpamPal d'accéder à Internet. Vous devez avoir manqu" ou sauté le message lorsque vous avez installé ou mis à jour SpamPal. Vérifiez les réglages de votre firewall afin de vous assurer que SpamPal peut accéder librement à Internet. Vous pouvez aussi rencontrer ce problème avec certains antivirus. Essayez de désactiver l'antivirus pour quelques instants et regardez si SpamPal peut se connecter à Internet.
Erreur 10061: Connexion refusée	Vous obtiendrez ce message si vous vous connectez à SpamPal sur le mauvais port. Le port utilisé par défaut par SpamPal pour le proxy POP3 est le port 110 . Si, pour une raison ou une autre, il ne peut utiliser le port 110, il va essayer de trouver un autre port disponible, généralement 1110. Vous avez dû avoir un message d'erreur à ce propos lorsque vous avez démarré SpamPal. Pour savoir quel port SpamPal utilise, ouvrez SpamPal, Options, Connections. Si SpamPal n'utilise pas le port 110, vous pourrez voir lequel est utilisé, et devrez décider si vous voulez le changer. Votre accès à Internet peut être bloqué. Vérifiez que vous pouvez y accéder en essayant d'accéder à des sites que vous n'avez pas visité auparavant, en utilisant Google et en allant sur des sites au hasard). Vous pouvez aussi avoir besoin de réinitialiser votre liaison, voire de rebooter votre PC. Si vous avez cliqué le choix Authentification APOP, vous pouvez rencontrer ce problème. (Un utilisateur a rapporté ce problème mais je n'ai pu le reproduire). Dans votre programme email, vérifiez la valeur

entrée dans l'adresse du serveur POP3. Si vous avez une valeur invalide, 127.1.1.1 au lieu de 127.0.0.1 par exemple, vous obtiendrez une erreur 10061. Si vous utilisez localhost, essayez de le remplacer par 127.0.0.1 au cas où un autre programme aurait changé votre référence localhost par défaut.

Si vous n'accédez à SpamPal que localement, vérifiez que l'adresse IP indiquée dans Options, Configuration Avancée, Configuration LAN est bien 127.0.0.1 .

Si vous accédez à SpamPal à travers un réseau local (LAN), vérifiez que l'adresse IP indiquée dans Options, Configuration Avancée, Configuration LAN est bien celle de la machine sur laquelle fonctionne SpamPal et que les adresses de toutes les machines autorisées à utiliser SpamPal, sont indiquées dans **Contrôle d'accès**.

Si vous avez cliqué l'option dans Outlook qui indique **Ce serveur nécessite une connexion sécurisée**, vous aurez cette erreur. Pour des connexions sécurisées, vous devez utiliser Stunnel ou un autre programme similaire.