Le Serveur de communication IceWarp

Paramétrage Anti-Spam

Version 12.2

Aout 2019

Sommaire

Paramétrage Anti-Spam 2

Paramétrage Anti-Spam

Introduction

L'objectif de ce document est de décrire le paramétrage à mettre en place pour réduire le nombre de de messages indésirables reçus par les utilisateurs du serveur IceWarp.

IceWarp est livré avec plusieurs techniques permettant de réduire la nuisance des Spams.

Comme nous n'avons aucun contrôle sur l'émission des Spams par les spammeurs, les seules actions possibles du côté du serveur IceWarp (quand il est le serveur destinataire de ces Spams) sont :

- Renforcer la sécurité du serveur SMTP pour empêcher une partie des Spams de rentrer
- Si un Spam est quand-même accepté par le serveur SMTP, avoir des règles pour pouvoir le détecter en tant que Spam et le stocker dans un dossier 'Spam' à part, laissant ainsi la boîte de réception "propre".
- Avoir des bonnes règles Anti-Spam pour que les mails légitimes ne soient pas classés comme Spam (faux positifs).

La suite de ce document explique comment mettre en œuvre cette stratégie.

Ce document ne parle pas des paramétrages qui sont liés plus généralement à la sécurité du serveur (quoi que les deux notions se recoupent parfois) et qui sont décrits dans le document "**Guide de sécurité**" sur http://www.icewarp.fr/downloads/documentation/server/

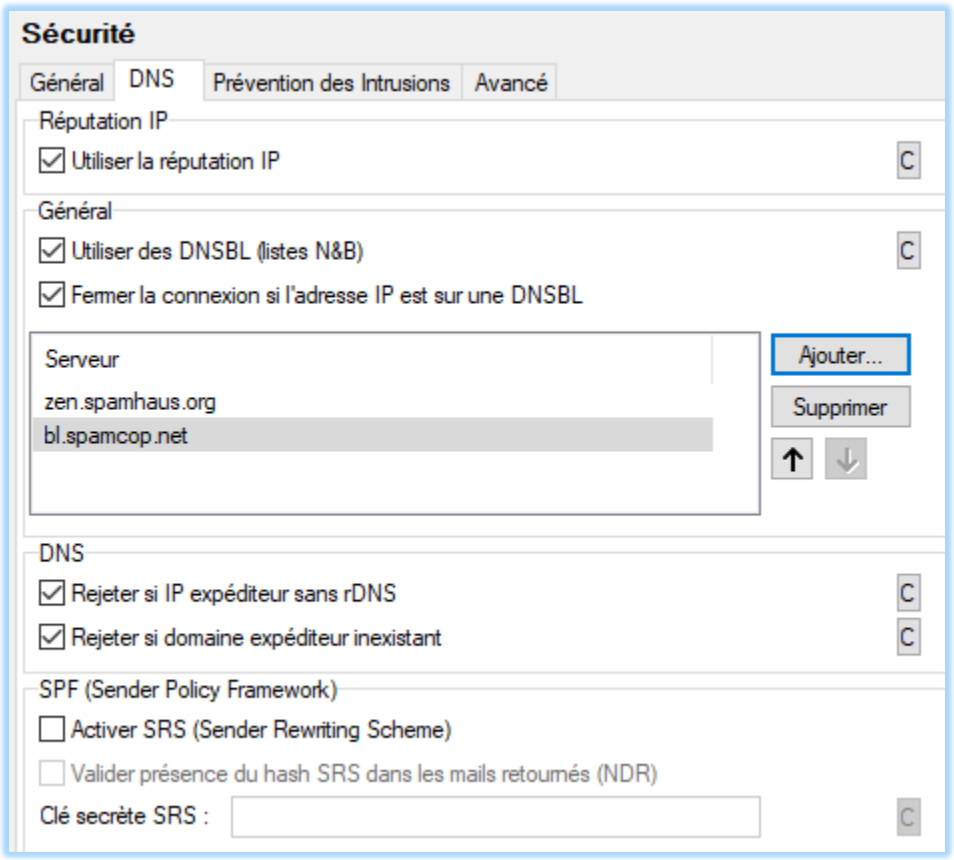
Faire barrage au niveau SMTP

Le paramétrage se fait au niveau du menu Mail -> Sécurité.

Quand ce contrôle détecte une anomalie, le mail est refusé pendant l'échange SMTP. Cela évite ainsi de gaspiller des cycles machine par la suite pour traiter le mail au niveau des moteurs Anti-Spam et Anti-Virus.

Les listes noires de domaines

Aller dans Mail -> Sécurité -> onglet DNS



Réputation IP : ce mécanisme est mis en œuvre par depuis la version 12.1 et il s'appuie sur le composant Anti-Spam Live.

On peut faire appel aux listes noires publiques (**DNSBL**) pour refuser un mail si l'adresse de l'expéditeur se trouve sur l'une de ces listes. Il faut savoir que toutes les listes publiques ne donnent pas toujours les meilleures informations. Les listes présentées dans cet exemple sont fiables et efficaces.

A savoir aussi que ce test nécessite un accès aux URL mentionnées pour chaque mail entrant. Il est donc conseillé de ne pas avoir une liste très longue (3 au plus est un chiffre acceptable).

Généralement les serveurs de vos correspondants légitimes sont bien configurés et ne devraient pas être détectés par ces contrôles dans IceWarp. La liste de contournement (bouton C) permet toutefois de corriger le problème s'il se présentait.

L'option "Rejeter si **l'expéditeur sans rDNS**" permet de n'accepter que des mails venant des domaines qui ont un enregistrement du type PTR. Ce critère est de plus en plus utilisé par les serveurs, il est donc fortement conseillé de créer cet enregistrement sur votre propre serveur.

En revanche, il est conseillé de rejeter le mail si le domaine de l'expéditeur n'existe pas.

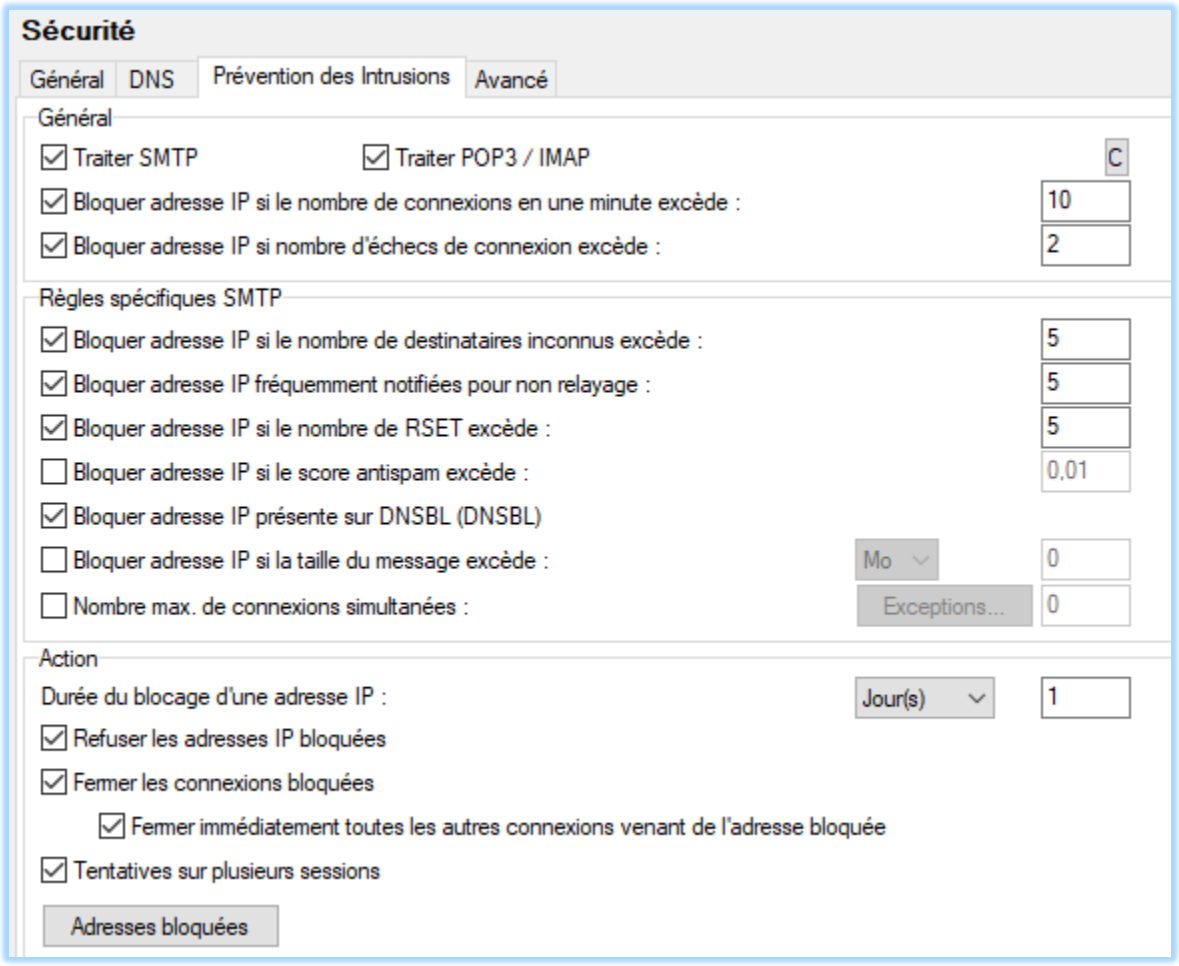
Il est conseillé d'activer SRS si le serveur effectue du relayage. Il s'agit d'un complément à la fonction SPF (http://support.icewarp.fr/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=243)

La Prévention des intrusions

Cette technique permet de détecter les attaques en force et de les bloquer pendant un temps donné.

Aller dans Serveur de Messagerie -> Sécurité -> onglet Prévention des Intrusions

Une bonne configuration est :



Chaque administrateur changera ces valeurs en fonction de son expérience.

Généralement les serveurs de vos correspondants légitimes ne devraient pas être détectés par ces contrôles. La liste de contournement (bouton ) permet toutefois de corriger le problème s'il se présentait.

On obtient dans le journal SMTP un message de ce type :

```
197.12.64.220   [0A50] 08:06:35 >>> 421 4.7.1 Intrusion prevention active for
[197.12.64.220][D]
```

[D] signifie que l'IP a été bloquée à cause des listes DNSBL : voir à la fin du document la signification de tous les codes.

Plus de détails sont donnés dans le document Sécurité :

http://www.icewarp.fr/download/guides/IceWarp%20-%20V12%20-%20Guide%20de%20securite.pdf

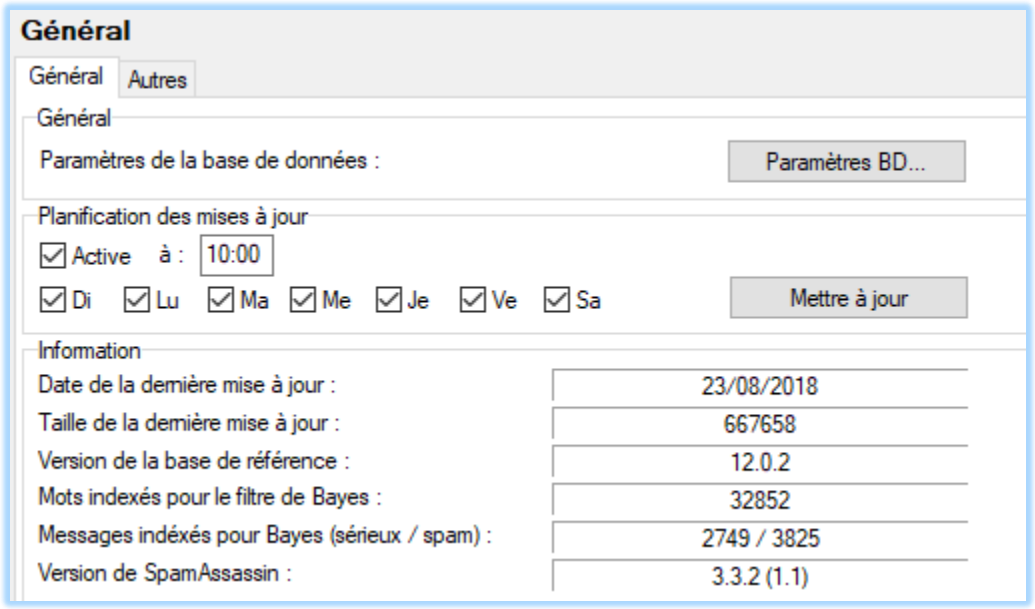
Détection de Spams

Quand un mail est accepté au niveau des échanges SMTP, POP3 ou IMAP, il est contrôlé par les moteurs Anti-Virus et Anti-Spam. En fonction du résultat de ces tests, le mail est soit **Rejeté** ou **Supprimé**, soit mis en **Quarantaine**, soit déposé dans le dossier **Spam**, soit livré dans la **boîte de réception** du (des) destinataires.

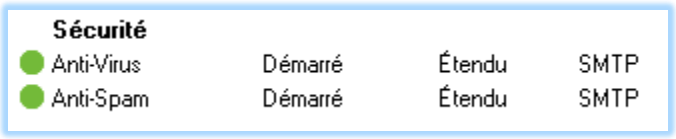
Ci-dessous, une configuration conseillée des différentes options du **menu Anti-Spam**. Comme pour le menu Sécurité, chaque administrateur doit ajuster les différentes valeurs pour mieux correspondre à son installation et à ses besoins.

Général

Onglet Général



Le service Anti-Spam doit être démarré (dans Système -> Services) :



Il est conseillé de laisser le journal Anti-Spam en mode étendu car il n'est pas très volumineux et donne beaucoup d'informations.

Il est possible de valider ou non l'Anti-Spam sur chaque compte (onglet **Stratégies** du compte) en cochant la case correspondante (elle doit être cochée aussi au niveau du domaine) :

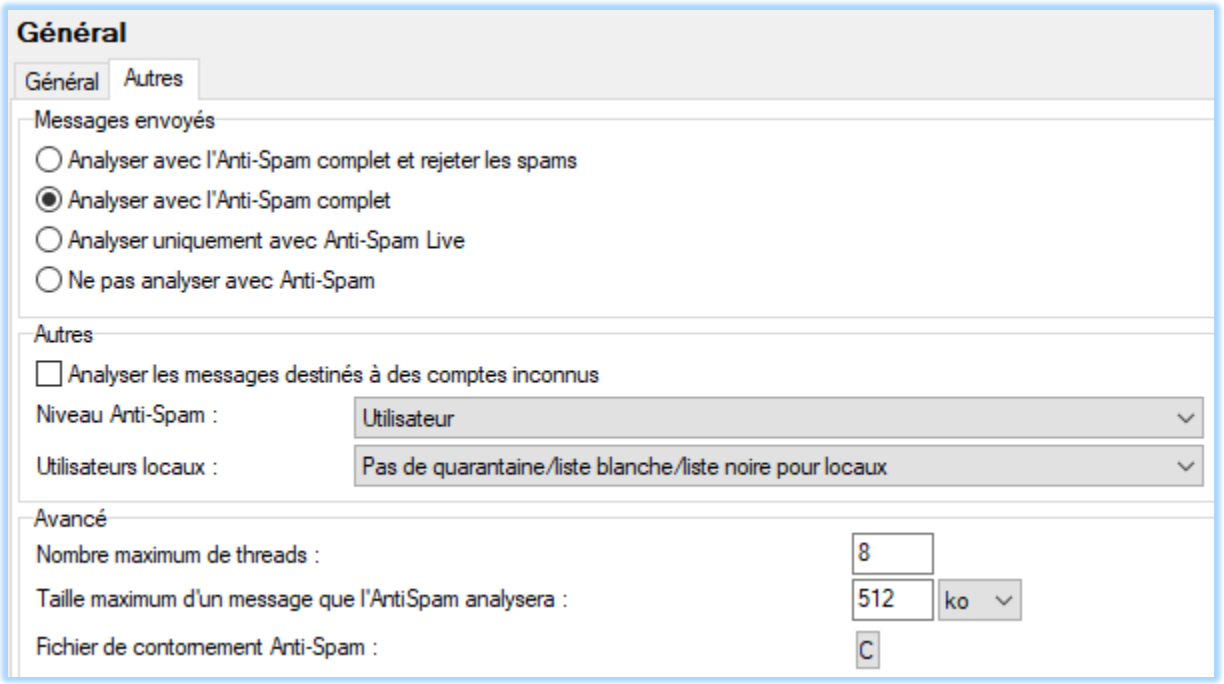
Pour les installations ayant plus de 100 comptes, il est conseillé de stocker les données dans une **base de données** autre que SQLite. Pour plus de détails sur l'installation d'une nouvelle base de données, consulter le document "Guide de Migration vers MySQL" disponible sur http://www.icewarp.fr/downloads/documentation/server/

Programmer une **mise à jour quotidienne** de la base de Spam. La mise à jour peut être activée manuellement en cliquant sur le bouton "Mettre à jour".

L'heure de planification peut être ajustée pour que la mise à jour ait lieu après la mise à jour des serveurs Anti-Spam, c'est-à-dire généralement en début de matinée.

Le module Anti-Spam nécessite une licence pour chaque compte sur lequel il est activé.

Onglet Autres



Messages envoyés : Choisir le mode souhaité pour le traitement des messages sortants. Dans une entreprise où le serveur est géré en interne, on peut désactiver le contrôle Anti-Spam pour les messages sortants – l'administrateur connaît ses utilisateurs. Dans le cas des fournisseurs d'accès Internet, il est prudent d'analyser les messages sortants avec Anti-Spam.

Analyser les messages destinés à des **comptes inconnus** : si le serveur contient des domaines de type 'backup' (les comptes inexistants dans le domaine sont redirigés vers un autre serveur désigné), il faut cocher cette case. L'Anti-Spam de IceWarp va ainsi contrôler les mails entrants avant de les transmettre au serveur backup.

Niveau Anti-Spam : Utilisateur - Domaine - Système. Indique en particulier comment sont traités les expéditeurs placés dans les listes blanche ou noire. Si **Utilisateur** est choisi, la mise en liste blanche par un compte ne sera applicable qu'à ce compte, s'il est au niveau **Domaine**, il sera applicable à tous les comptes du domaine et s'il est au niveau **Système**, il sera applicable à tous les comptes du serveur.

Utilisateurs locaux (appartenant au même serveur) : on précise ici si les expéditeurs du serveur doivent être ou non traités par la Quarantaine.
Si l'administrateur connaît tous les utilisateurs de tous les domaines et considère que ses utilisateurs n'envoient pas de Spam, choisir "Pas de Quarantaine pour les utilisateurs locaux".
Si les utilisateurs sont connus uniquement intra-domaine, choisir "Quarantaine pour les utilisateurs locaux d'autres domaines"
Sinon, choisir "Quarantaine pour tous les utilisateurs locaux".

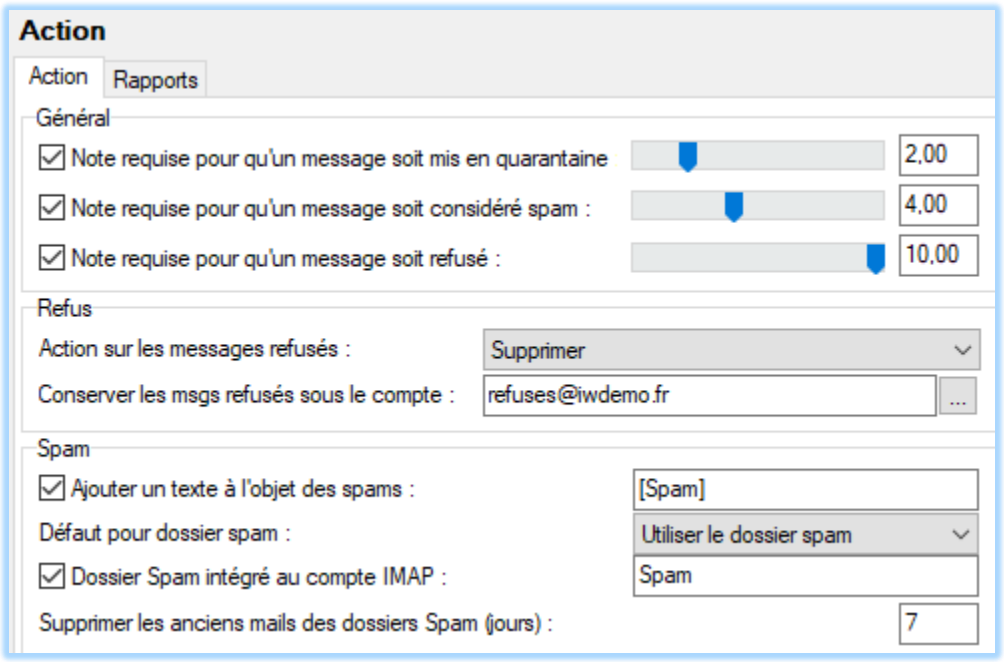
Threads : Il est conseillé de laisser le paramètre 'Pool de threads' à la valeur par défaut : 8

Taille maximum : Le seuil par défaut pour exclure un mail du traitement Anti-Spam étant trop petit, nous utilisons la valeur 512Ko pour ce paramètre. Les Spams étant rarement des mails volumineux, on peut exclure les gros messages, et économiser ainsi des ressources.

Le bouton de **contournement** ouvre un fichier dans lequel on peut inscrire des configurations qui ne seront pas contrôlés par le moteur Anti-Spam. Pour exclure des comptes et des domaines, il vaut mieux utiliser l'option de ces comptes ou domaines (onglet Services) en positionnant le mode d'Accès correctement (cf. onglet Général).

Action

Onglet Action



Toutes les techniques utilisées par le moteur Anti-Spam conduisent finalement à l'attribution d'un **score entre 0 et 10** pour chaque mail analysé.

Dans cette section, l'administrateur définit les actions à entreprendre en fonction du score attribué.

Nous utilisons dans l'exemple ci-dessus la **Quarantaine** pour les messages sur lesquels un doute persiste. Le Défi peut ou non être activé dans ce cas.

Pour les comptes pour lesquels la Quarantaine est activée, un score compris entre 2 et 4 place le mail en Quarantaine.
Un score > 4 place le mail dans le dossier "Spam" (si l'option est cochée).
En surveillant les journaux Anti-Spam sur une période d'une semaine ou deux, l'administrateur doit trouver les bonnes valeurs pour ces seuils.

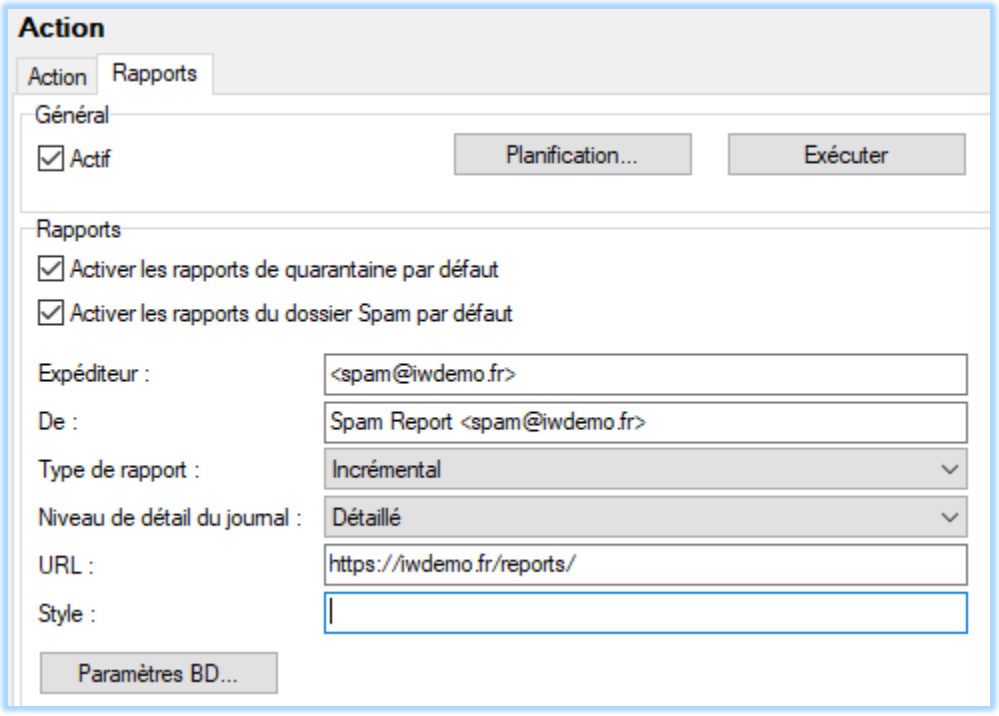
Si un administrateur choisit de **refuser** les mails au-dessus d'un seuil (10 en général), il a la possibilité de programmer la **suppression** pure et simple du mail ou de le **rejeter**. S'il rejette les mails avec un score élevé, l'expéditeur (cad. le spammer) reçoit un message lui signalant ce rejet. Ce qui est fort dommage car dorénavant, il sait que l'adresse email qu'il a trouvé pour envoyer des Spams existe vraiment ! L'autre option est de supprimer de tels mails – avec le risque de supprimer un mail légitime mal classé comme Spam (faux positif). Pour cette raison, il y a la possibilité d'archiver le mail avant sa suppression.

Nous avons choisi de placer les messages dont le score est supérieur à 10 sur un compte spécial de façon à ne pas les perdre. Dans la configuration proposée, chaque mail se trouve quelque part : boîte de réception du destinataire ou des refusés, Spam ou Quarantaine, il n'est jamais supprimé complètement.

Le **marquage** des mails se fait en rajoutant un texte dans l'objet du mail. Les différentes variables système (liste complète dans …/examples/variables.dat.html) peuvent être utilisées pour donner des indicateurs spécifiques au destinataire du mail.

Pour les comptes IMAP (types IMPA ou IMPA & POP3 défini dans l'onglet Options du compte), il est possible de séparer les mails identifiés comme Spam dans un dossier différent de la boîte de réception. Si la troisième option est activée, le dossier contenant les Spams sera intégré aux dossiers IMAP sous le nom indiqué dans le champ prévu. Par défaut, le nom de ce dossier est 'Spam'. Il est conseillé de garder ce nom pour ce dossier.

Onglet Rapports



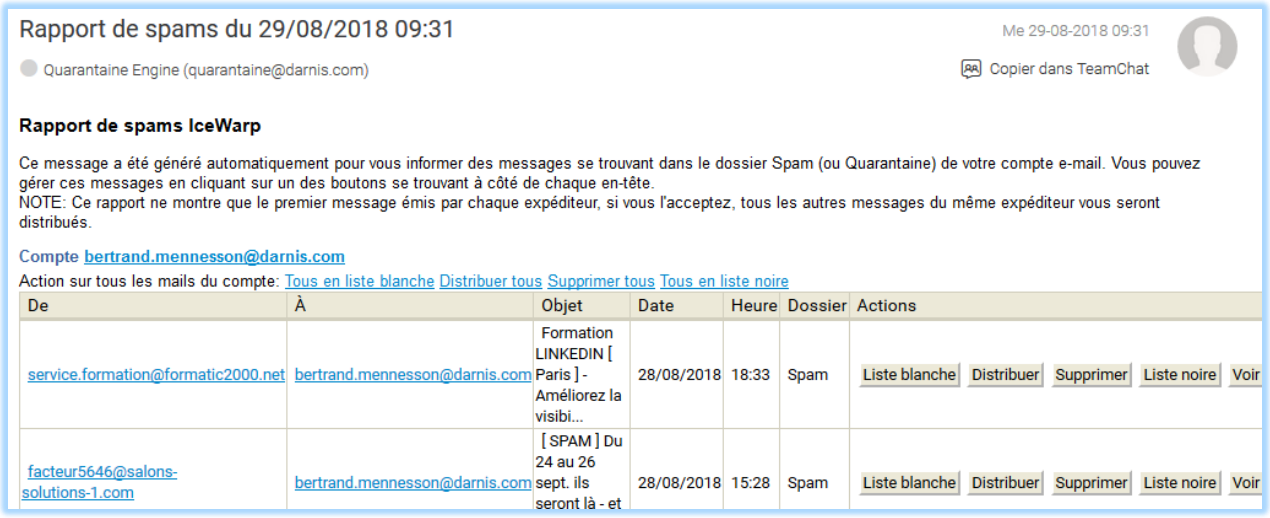
Sur cet écran, on programme l'envoi de la liste des mails en Quarantaine et/ou dans le dossier Spam. Pour recevoir le rapport par mail, en plus de la planification faite sur cet écran, il faut que dans l'onglet "options" de chaque utilisateur concerné, la fonction "Rapports Spam" soit activée (à "défaut", "nouveaux" ou "tous").

Vérifiez que les deux champs "Expéditeur" et "De" contiennent bien des adresses email (le compte n'a pas besoin d'exister).

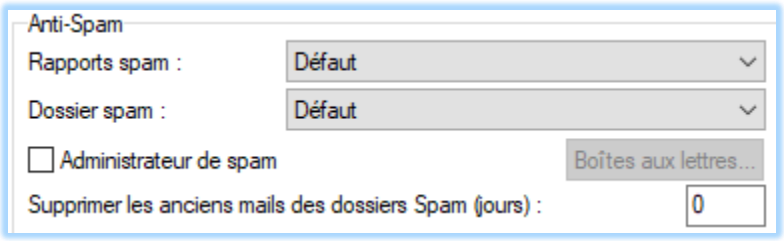
Les utilisateurs du Client Web IceWarp ont la possibilité de voir directement le contenu des dossiers Spam et Quarantaine, cependant cette possibilité n'est pas offerte aux autres clients de messagerie qui doivent alors avoir recours aux rapports de Quarantaine et de Spams pour pouvoir consulter leurs Spams

Le message du rapport est sous forme d'une liste avec les boutons 'hyperliens' qui permettent d'appliquer une action (une fenêtre du navigateur s'ouvre pour indiquer le résultat de l'action) :

- Mettre en liste blanche l'expéditeur
- Distribuer au destinataire
- Supprimer le message
- Mettre l'expéditeur en liste noire
- Voir le contenu du message (texte brut)



Le rapport peut être validé ou non au niveau du compte en allant dans l'onglet Options :



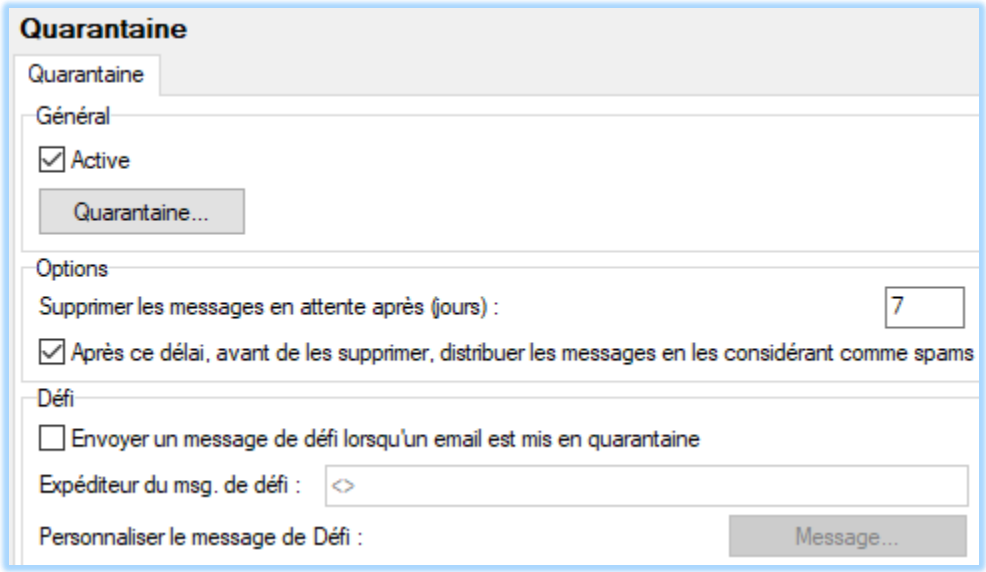
On peut choisir pour les rapports de spam de l'utilisateur :

- Défaut : L'option par défaut du système (définie dans l'onglet Rapports)
- Désactivé : De désactiver les rapports
- Nouveaux : De ne voir que les nouveaux expéditeurs mis en Spam
- Tous : de voir tous les expéditeurs en spam

Cette option est aussi accessible à l'utilisateur par le Client Web dans Options -> onglet Général -> Anti-Spam.

Des informations complémentaires sur les rapports sont donnés dans la FAQ suivante :
http://support.icewarp.fr/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=305

Quarantaine



Les mails placés en Quarantaine peuvent en sortir de trois façons :

- Suite à une action par l'expéditeur (si le mécanisme de Défi est activé),
- par une action du destinataire (au travers du Client Web et/ou le rapport de Quarantaine)
- par une action de l'administrateur (à partir de la console d'administration).

Cependant, les mails non traités après 'X' jours peuvent être supprimés de la Quarantaine (et optionnellement être envoyés au destinataire comme si c'étaient des Spams).

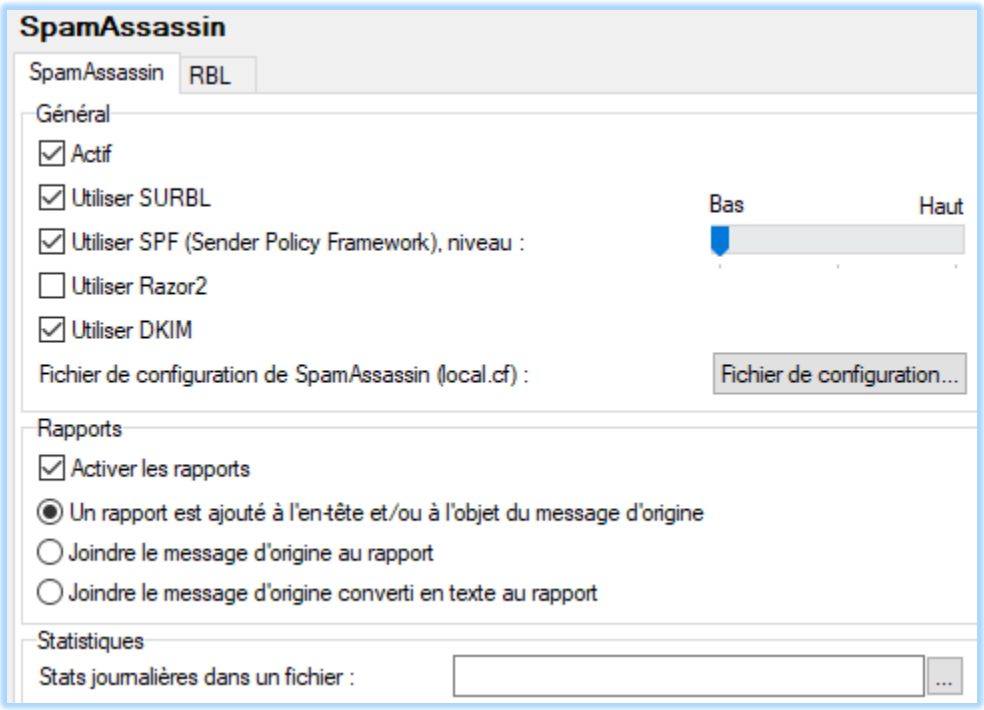
Si l'option "**envoi du message défi**" est cochée, à chaque message placé en Quarantaine et si l'expéditeur est inconnu, un mail est envoyé à l'expéditeur lui demandant de confirmer son envoi.

Pour plus de détails sur le Défi, consulter le document "Guide de configuration du Défi/Challenge response" sur http://www.icewarp.fr/downloads/documentation/server/

Il est possible de valider ou non la quarantaine sur chaque compte (onglet **Stratégies** du compte) en cochant la case correspondante (elle doit être cochée au niveau du domaine) :

SpamAssassin

Onglet SpamAssassin



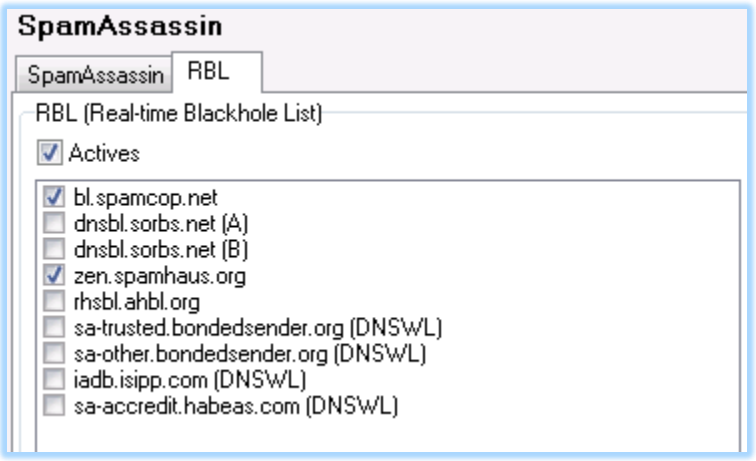
Technique efficace pour la détection des Spams à base de règles.
Ces règles (…/spam/rules) sont mises à jour selon la programmation de l'onglet "Général" (…/spam/spam.db).

Razor2 n'étant pas encore utilisée à une grande échelle, nous ne l'utilisons pas.

Il est intéressant d'activer la fonction "rapports" avec l'option "ajout à l'en-tête". Ainsi, en examinant les en-têtes de chaque mail, on peut avoir les détails sur l'action du moteur Anti-Spam:

```
Subject: RE: [SUPPORT #20]: Export comptes
Date: Mon, 15 Oct 2007 10:58:33 +0200
Message-ID: <000301c80f09$90c48660$b24d9320$@be>
MIME-Version: 1.0
Content-Type: multipart/related;
        boundary="----=_NextPart_000_0004_01C80F1A.544D5660"
X-Mailer: Microsoft Office Outlook 12.0
Thread-Index: AcgMKmOl0WXqoGNQS1qN59kM8edGxAC3oP5Q
Content-Language: fr-be
X-Spam-Status: No, hits=2,79 required=3,00
tests=LOCALPART_IN_SUBJECT,HTML_MESSAGE,BAYES_00,MR_DIFF_MID
version=3.2.1
X-Spam-Level: **
X-Spam-Checker-Version: SpamAssassin 3.2.1 (1.0) on mail.tassigny.darnis.com
```

Onglet RBL



Le rôle de ce menu est le suivant : Si l'adresse IP du serveur d'un mail entrant est sur l'une des listes RBL, le score Spam du mail est augmenté.

Il est important de savoir que cela nécessite de contacter le serveur RBL pour chaque mail analysé. Ainsi, sur un serveur avec une activité importante, ces tests pourront affecter les performances du système. Il est conseillé de ne pas utiliser plus de 2 de ces listes.

Notre conseil est de ne pas activer cette fonction au sein de SpamAssassin si le contrôle est déjà effectué pendant l'échange SMTP (cf. § Sécurité). Ce sont en effet les mêmes serveurs qui sont utilisés.

Anti-Spam Live

Cette fonction est intégrée à l'ensemble anti-Spam depuis la version 12.1.

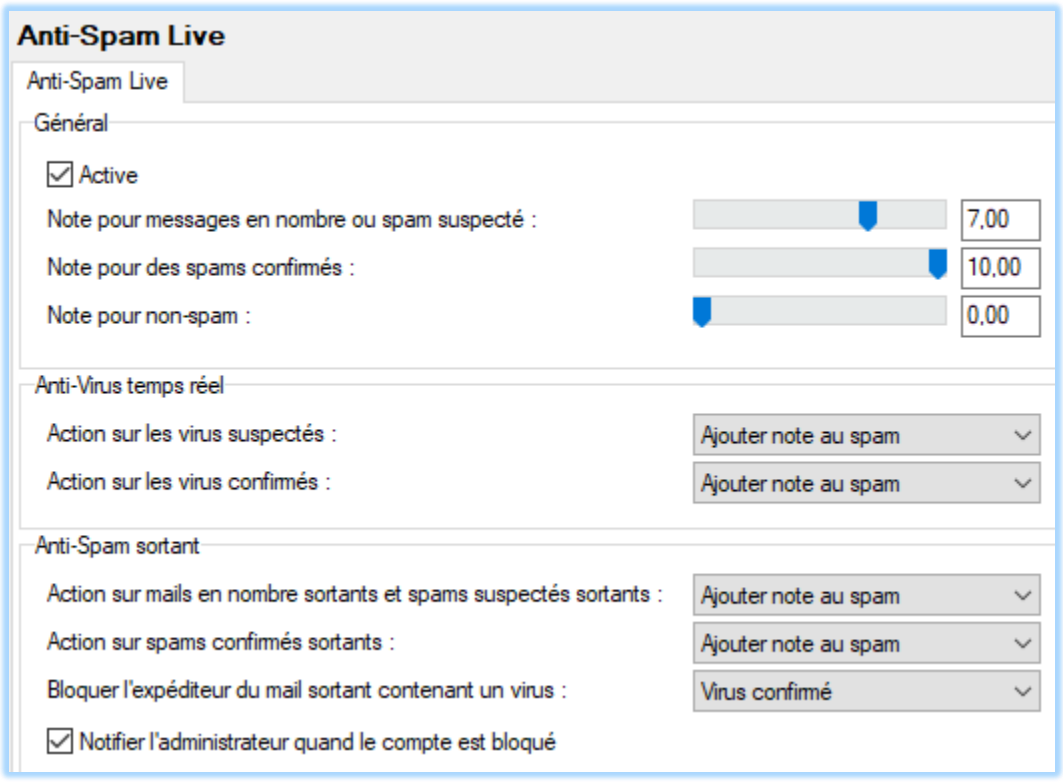
Le système Anti-Spam LIVE (**L**ive **I**dentification and **V**erification **E**ngine) offre une protection temps réelle s'appuyant sur la détection d'une invasion de spam dans le réseau. La technologie LIVE est implémentée comme une couche supplémentaire dans l'Anti Spam en utilisant le service Commtouch RPD (**R**ecurrent **P**attern **D**etection).

Anti Spam Live fait appel à des serveurs externe pour déterminer les risques pour qu'un message soit un spam. Ce serveur n'est consulté que si le message n'a pas été considéré comme Spam par les autres techniques utilisées dans le serveur (sa note est inférieure au seuil Spam).

La réponse du serveur est sur trois niveaux :

- H : Ce message est sans doute un Spam ou un envoi en nombre
- Y : ce message est très probablement un Spam
- N : ce message n'est pas considéré comme Spam

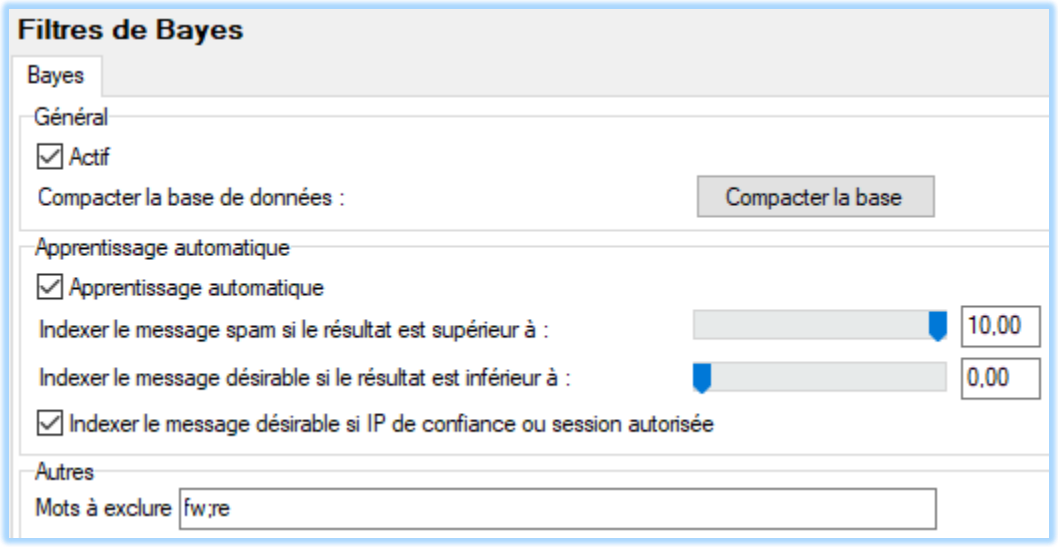
L'écran ci-dessous permet d'affecter une note pour chaque niveau de la réponse :



Anti-virus temps réel permet de d'augmenter la note lorsque la présence d'un virus est suspectée ou confirmée par anti-Spam Live.
Note : Anti-Spam Live ne remplace pas l'anti-virus du serveur. Anti-Spam Live n'est utile que dans les premières minutes de la diffusion d'un nouveau virus.

Anti-Spam sortant permet d'adapter le comportement sur les messages sortants.

Filtres de Bayes



La technique de Bayes compare le contenu des mails à une base de référence et détermine la probabilité que le mail soit un Spam.

Il est conseillé d'utiliser cette technique.

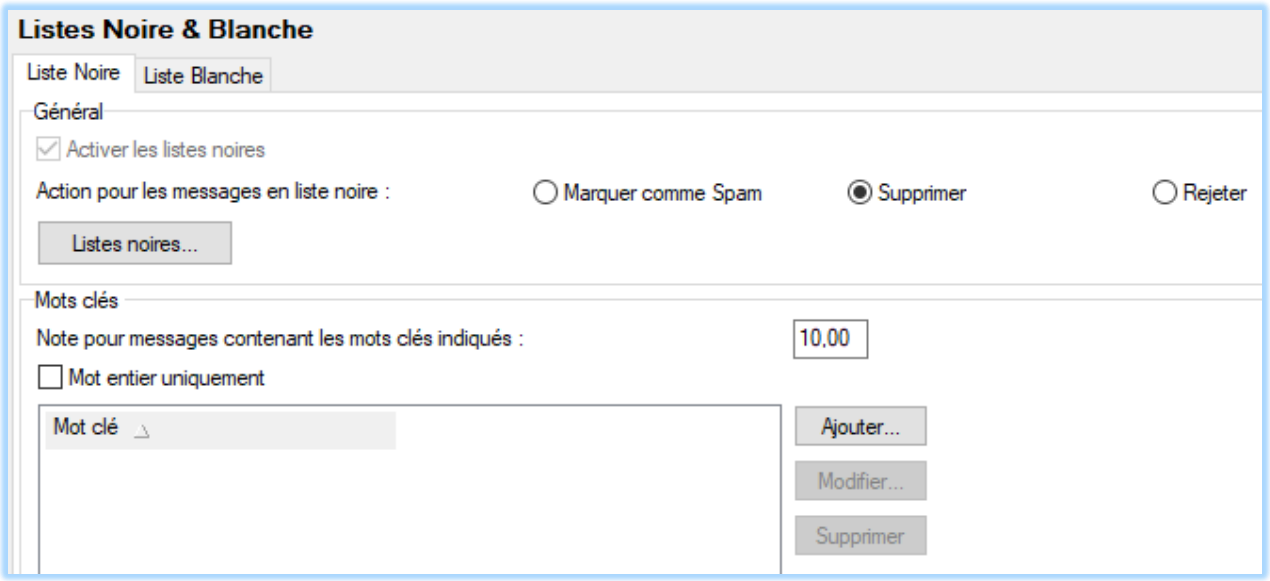
Il existe deux bases consultées par les filtres de Bayes:

- Une base globale mise à jour par IceWarp selon la programmation de l'onglet "Général" (…/spam/spam.db)
- une base propre à l'installation et qui est mise à jour par la méthode d'apprentissage (…/spam/spam.db.usr). L'indexation selon les critères d'apprentissage automatique se fait tous les jours à minuit.

Il est conseillé d'activer l'apprentissage automatique. Selon notre expérience, si le moteur Anti-Spam a affecté un score >10, il est rare que le message ne soit pas un spam → d'où les valeurs que nous utilisons.
De même, en accordant la confiance aux mails venant de serveurs de confiance, on augmente la précision du filtre de Bayes.

Listes noires et blanches

Onglet Liste noire



Note : si la quarantaine est activée, la liste noire est nécessairement activée.

La liste noire permet de forcer un message en Spam en fonction de l'identité de l'expéditeur (l'expéditeur traité est celui qui figure dans le From: de l'entête du message et non celui utilisé pour l'échange SMTP).

L'utilisateur peut mettre un expéditeur "en liste noire" depuis le Client Web ou à partir du rapport de Spam.

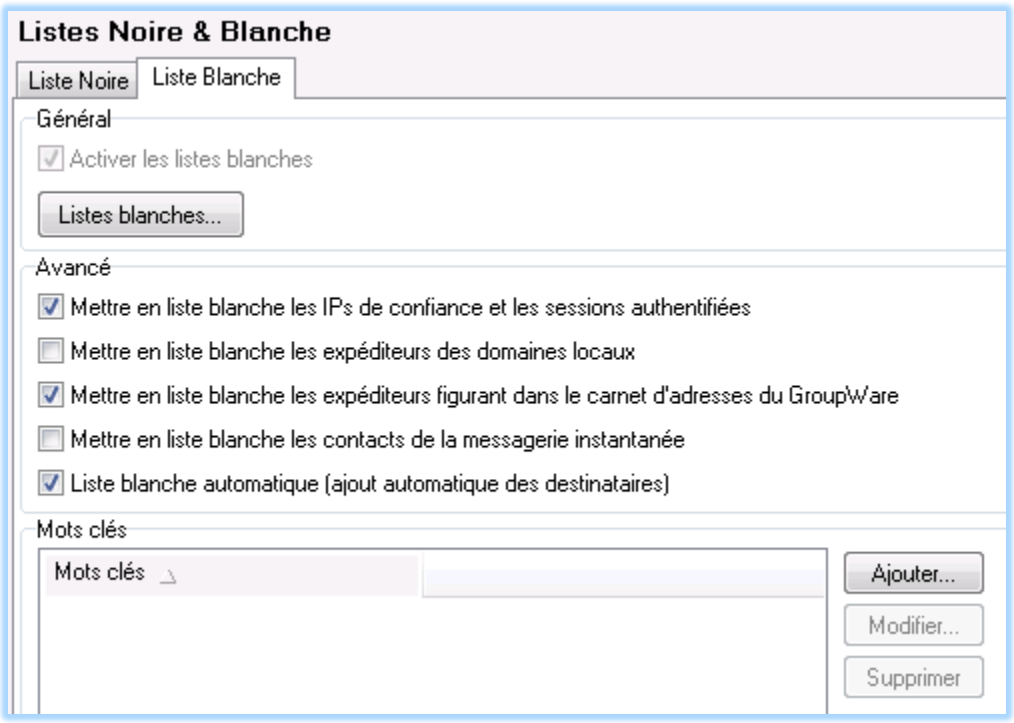
L'administrateur peut aussi mettre des adresses en liste noire à partir du menu Etat -> File de Spams -> onglet Liste noire -> bouton "Ajouter".

Trois possibilités de traitement existent pour un expéditeur en liste noire :

- Marquer comme spam : l'expéditeur continuera à apparaître dans les rapports de spam
- Supprimer : le message est simplement supprimé et n'apparaîtra plus nul part
- Rejeter : un message de rejet est envoyé à l'expéditeur. Cette option est déconseillée pour les Spams.

Si le contenu d'un mail contient des **mots** parmi ceux listés sur l'écran des mots clés, le score du mail est incrémenté de la valeur spécifiée.

Onglet Liste Blanche



Note, si la quarantaine est activée, la liste blanche est nécessairement activée.

La liste blanche permet de forcer le moteur Anti-Spam à accepter un message en fonction de l'identité de l'expéditeur (l'expéditeur traité est celui qui figure dans le From: de l'entête du message et non celui utilisé pour l'échange SMTP).

L'utilisateur peut mettre un expéditeur "en liste blanche" depuis le Client Web ou le rapport de Spam.

L'administrateur peut aussi mettre des adresses en liste blanche à partir du menu Etat -> File de Spams -> onglet Liste blanche -> bouton "Ajouter".

Mettre un expéditeur en liste blanche offre la garantie de déposer les mails de cet expéditeur dans la boîte de réception du destinataire.

C'est un moyen très efficace pour diminuer le nombre de messages injustement placés dans les Spams (les "faux positifs") et il est donc vivement conseillé d'utiliser les listes blanches.

Un expéditeur peut être mis en liste blanche pour un utilisateur ou pour tout un domaine.

Les expéditeurs suivants peuvent aussi être considérés optionnellement comme étant en liste blanche:

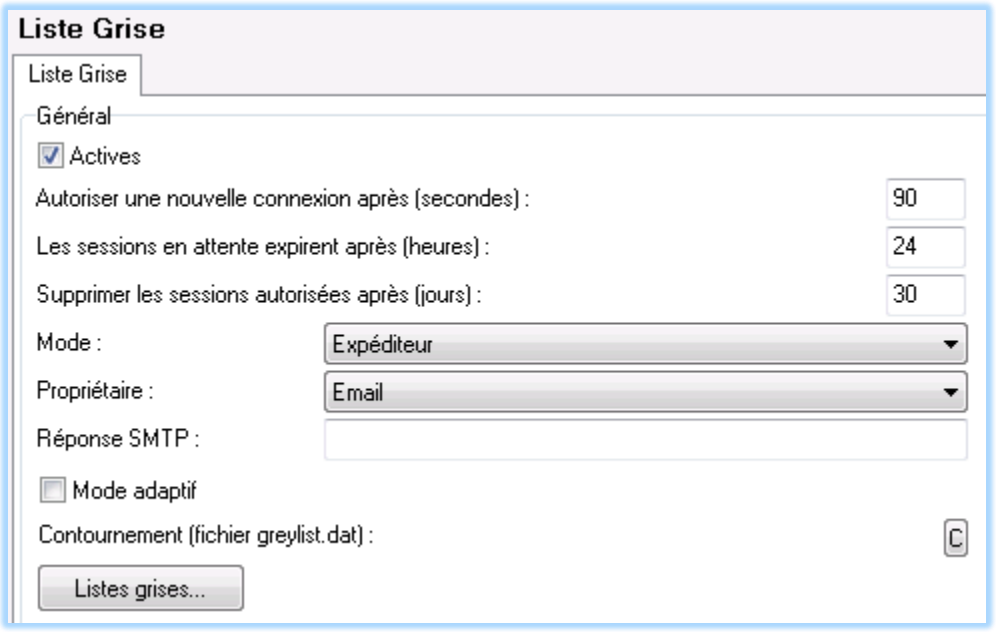
- expéditeurs qui s'authentifient ou qui envoient depuis des adresses de confiance
- utilisateurs du serveur IceWarp (cad. des comptes locaux, à condition qu'ils soient authentifiés)
- contacts du carnet d'adresses
- contacts de la messagerie instantanée

Les destinataires des messages peuvent être optionnellement ajoutés automatiquement à la liste blanche.

Si le contenu d'un mail contient des mots parmi ceux listés sur l'écran des mots clés, l'expéditeur du mail est considéré comme étant en liste blanche.

Note : les listes blanches et noires ne sont pas appliquées si l'expéditeur est local mais la session n'est pas authentifiée et ne provient pas d'un hôte de confiance. Cette option peut toutefois être contournée par l'administrateur (variable *SpamSkipBypassLocalUntrusted)*. Voir plus loin ByPass=H.

Liste grise



Il s'agit d'une technique très efficace qui agit au niveau du protocole avant réception du message.

Quand un mail arrive avec un expéditeur inconnu (de la liste grise) sur le serveur IceWarp, il est systématiquement **refusé** avec un code d'erreur temporaire (4xx) en demandant au serveur émetteur de recommencer. Par exemple :

```
192.168.10.2    [0EB4] 11:37:29 >>> 451 4.7.1 Please try again later
```

Les serveurs de spammeurs le font rarement. Les serveurs correctement configurés renvoient le mail une seconde fois (généralement au bout de 2 minutes) et il est accepté à ce moment (voir Serveur de messagerie -> Général -> onglet Distribution -> bouton "Période entre essais...").

Le mode de traitement conseillé est "Expéditeur". Ainsi, même si le même expéditeur recommence depuis une autre machine, il sera à nouveau mis en liste grise.

Il y a un risque pour que le serveur d'un de vos correspondants ne traite pas le code d'erreur temporaire selon la norme, mais le gain à bloquer de vrais Spams plaide en faveur de l'activation de cette option.

Le bouton de contournement permet d'indiquer des domaines ou des adresses IP qui doivent être exclus de la liste grise.

La liste grise est appliquée selon les mêmes critères que l'Anti-Spam sauf qu'elle n'est pas appliquée sur les IP qui font partie des IP de confiance (voir Serveur de messagerie -> Sécurité -> onglet Général).

Règles d'apprentissage

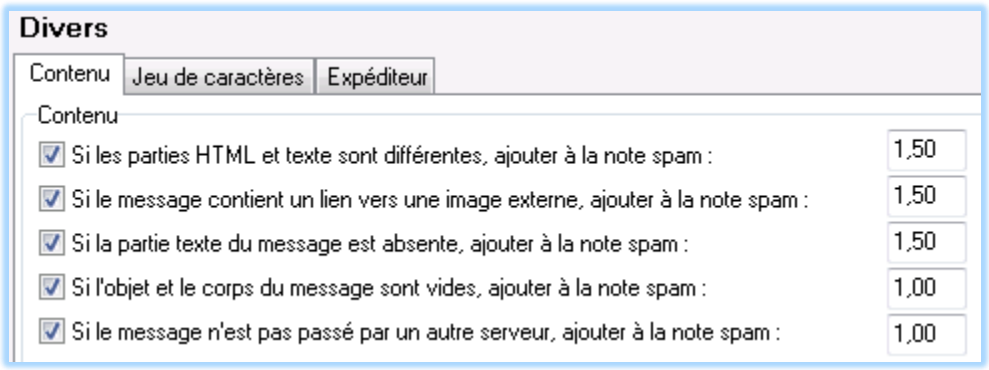
Afin d'augmenter la précision du filtre de Bayes, l'administrateur/l'utilisateur peut déplacer des mails dans des dossiers ou les transférer dans des boîtes aux lettres spécifiques pour que l'indexation (qui a lieu à minuit tous les jours ou avec le bouton "exécuter" de cet écran) analysent ces mails selon les directives.

Cette configuration nécessitant une préparation, elle n'est pas conseillée pour une première approche à l'Anti-Spam de IceWarp.

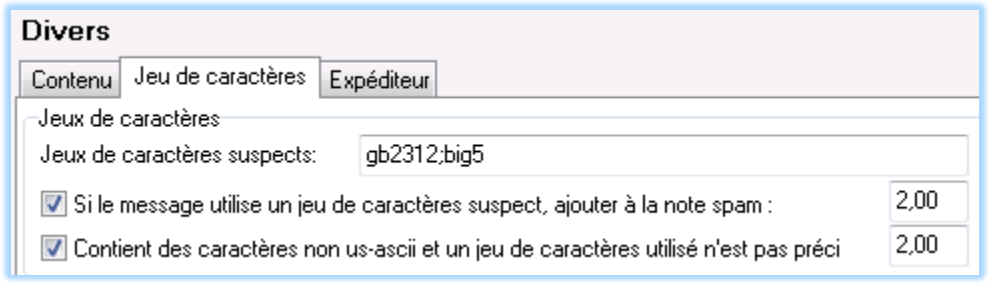
Divers

Dans cette section, l'administrateur donne des valeurs d'incrément au score d'Anti-Spam, chaque fois que la condition est vérifiée. Nous préconisons les valeurs suivantes :

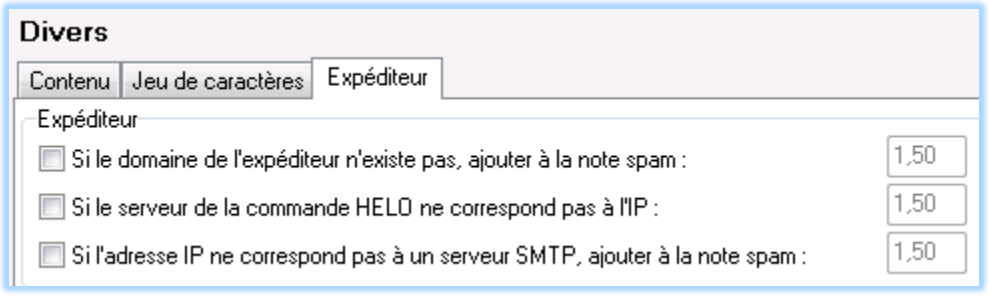
Onglet Contenu



Onglet Jeu de caractères



Onglet Expéditeur



Les deux premiers critères ont déjà été contrôlés dans Mail -> Sécurité -> onglet DNS

Le dernier est assez pénalisant sur la performance et n'est pas toujours un bon critère (certains gros serveurs d'expédition ne font pas la réception de messages).

Le journal Anti-Spam

Il est conseillé de valider le **journal Anti-Spam** au niveau détaillé dans Système -> Services -> Anti-Spam.

La consultation du journal Anti-Spam permet de comprendre comment un mail particulier a été traité. Voici quelques exemples et explications.

Exemple de message accepté par le serveur

```
157.55.234.76   [0A50] 10:57:41 201409101057410771 '<xxx@yyy.com>'
'<vineeta.darnis@darnis.com>' 1 score 0,00 reason [Bypass=W] action NONE
```

on trouve comme informations :

- **157.55.234.76** - L'adresse IP de l'expéditeur
- **[0A50]** - Le numéro du thread que l'on retrouve dans le journal SMTP ou POP3 suivant l'origine du message.
- **10:57:41** - L'heure du traitement
- **201409101057410771** - L'identité du message que l'on retrouve aussi dans le journal SMTP
- **'<xxx@yyy.com>'** - L'expéditeur
- **'<vineeta.darnis@darnis.com>'** - Le destinataire
- **1** - Le nombre de messages traités simultanément (ils sont parfois regroupés)
- **score 0,00** - le score obtenu
- **reason [Bypass=W]** - les critères qui ont conduit à la note et à la décision finale (voir détails ci-après).
- **action NONE** - l'action exécutée peut être :
    - NONE (placé dans la boîte de réception du destinataire),
    - SPAM (placé en Spam),
    - QUARANTINE (quarantaine),
    - REJECT (rejeté, un message est renvoyé à l'expéditeur),
    - DELETE (simplement supprimé).

Exemple de message placé en Spam

```
178.33.139.123  [0A50] 07:18:58 201409100718460115
'<protection@m92.visuh.info>(<marc@m92.visuh.info>)' '<info@darnis.com>' 1
score 10,00 reason
[SpamAssassin=9,68,Bayes=100,00%,Other=1,50:Body=E,Bypass=J] action SPAM
```

L'expéditeur est de la forme suivante : '<protection@m92.visuh.info>(<marc@m92.visuh.info>)'

- **marc@m92.visuh.info** est l'adresse utilisée dans l'échange SMTP (MAIL FROM:)
- **protection@m92.visuh.info** est l'adresse du From: contenue dans l'entête du message (celle que voit le destinataire et qui sera mise en liste blanche ou noire si le destinataire décide de mettre le message en liste blanche ou noire).

Ce message a été mis en spam à cause de la note obtenue (10) supérieure au seuil des Spams.

Exemple de message supprimé

```
192.168.0.66    [0B28] 22:45:56 20140909224553391O
'<root@localhost.localdomain>' '<vineeta.darnis@darnis.com>' 1 score 9,30
reason [SpamAssassin=5,80,Bayes=99,89%,Other=3,50:ContentFilter=Sauvegarde
Actitime,Sender] action DELETE
```

Ce message a été supprimé à cause du filtre de contenu " Sauvegarde Actitime"

Explications sur les raisons du traitement

Les raisons du traitement sont placées entre crochets, on y trouve les critères suivants :

- **AntiVirus** - c'est le module anti-virus qui demande le rejet ou la suppression du message
- **Blacklist** - l'expéditeur est en liste noire
- **Bypass** - les raisons sont résumées dans le tableau ci-dessous
- **Other** - suivi d'une note et des précisions suivantes : **Body**, **Charset**, **Sender** - qui dépendent des options contenues dans Anti-Spam -> Divers -> Onglets **Contenu**, **Jeu de caractères**, **Expéditeur** (voir plus de détails dans les tableaux ci-dessous pour Body et Charset)
- **Bayes** - pourcentage attribué par les Filtres de Bayes (note incluse dans SpamAssassin)
- **SpamAssassin**, - note attribuée par SpamAssassin
- **Rules** - action entreprise par une règle dont le nom est donné
- **ContentFilter** - action entreprise par un filtre de contenu dont le nom est donné
- **Live** - résultat du test par Anti-Spam Live (voir ci-dessous)

La **note globale** indiquée après le mot **score** est la somme de la note SpamAssassin et de la note Other (elle est limitée à 10).

Code des raisons des traitements

Voici les tableaux des codes utilisés dans le journal Anti-Spam pour indiquer les critères qui ont été détectés. Il y a un tableau pour : Body, Charset, ByPass et Live puis un tableau pour les codes de la prévention des intrusions.

Code pour Body

Code	**Raison**
P	Le bloc HTML et le bloc texte ne coïncident pas
E	Contient des images externes
N	Pas de bloc texte
I	Image incluse
B	Pas de corps et pas d'objet dans le message
R	Pas de serveur intermédiaire
S	Le message contient un script
F	Note Spam attribuée par un filtre
K	Note Spam attribuée par un mot en liste noire
X	Le message ne peut pas être placé en quarantaine (par exemple base Anti-Spam inaccessible)

Code pour Charset

Code	**Raison**
F	Jeu de caractères interdit
M	Jeu de caractères non défini

Code pour ByPass

Code	**Raison du contournement**

B	Un contournement a été défini dans le fichier des contournements de l'Anti-Spam.
G	L'expéditeur se trouve dans un des carnets d'adresses du GroupWare *
H	Les listes blanche et noire ne sont pas vérifiées si le serveur d'envoi dit que l'expéditeur est local même si la session n'est pas authentifiée ni ne vient d'un serveur de confiance. Le message est ensuite traité normalement et les autres règles sont appliquées. Ce comportement ne peut être modifié qu'en utilisant la console API et en modifiant la variable ***c_as_spamskipbypasslocaluntrusted*** qui est à faux par défaut. Cette option évite qu'un spammeur puisse faire passer des messages en empruntant une adresse locale pour le From:
K	Des mots ont été trouvés dans la liste blanche des mots clés *
L	License non valide
M	Le compte n'a pas l'option Anti-Spam validée (onglet Stratégies du compte)
O	Message sortant (cf. Anti-Spam -> Général -> onglet Autres)
Q	Expéditeur d'un domaine local *
R	L'expéditeur est un contact de la messagerie instantanée *
S	Le message dépasse la taille limite (cf. Anti-Spam -> Général -> onglet Autres)
T	La session est authentifiée ou l'adresse IP de l'expéditeur est en liste de confiance *
U	Si : - Les rapports de Spam ou de Quarantaine sont validés, - La connexion SMTP provient du serveur local ou d'un serveur faisant partie de l'ensemble Equilibrage de Charge - L'expéditeur est identique à celui spécifié dans le champ Expéditeur du menu Anti-Spam -> Action -> onglet Rapports Alors la connexion est acceptée et ByPass=U est indiqué.
W	L'expéditeur est en liste blanche ou une règle a accepté le message
X	Le message n'a pas pu être mis en quarantaine (La quarantaine n'est pas activée)
J	Le compte n'a pas la quarantaine validée (onglet Stratégies du compte)
Z	L'option "Pas de quarantaine/liste blanche/liste noire pour locaux" est sélectionnée (cf. Anti-Spam -> Général -> onglet Autres)

* Pour activer/désactiver ces options, aller dans Anti-Spam -> Listes noire et blanche -> Liste blanche

Code pour Anti-Spam Live

Code	Raison
Y	Ce message est considéré par Anti-Spam Live comme étant très probablement un Spam
H	Ce message est très probablement un envoi en nombre
N	Ce message est considéré comme authentique

Codes pour la Prévention des Intrusions

C	Filtre de contenu
I	trop de connexions par minute
M	message trop gros
R	trop de commandes RSET
D	IP listée sur DNSBL
A	envoi à un compte bloqué
P	trop de destinataires inconnus
Y	relayage
S	score de spam trop important
U	blocage manuel par la console
L	trop de tentatives de connexion ayant échoué