Le Serveur de communication IceWarp

Anti-Spam, Quarantaine et Défi

Version 11

Septembre 2014

Sommaire

Anti-Spam, Quarantaine et Défi

Introduction

Ce document indique la configuration à mettre en place pour utiliser la technique de Défi ou "Challenge response" offerte par le module Anti-Spam de serveur Icewarp.

Nous allons d'abord décrire les principes et concepts, puis nous continuerons avec les étapes de la configuration à créer dans le serveur IceWarp.

Principes

Le **Défi** ou **Challenge Response** (en anglais) est une technique parmi d'autres visant à diminuer le nombre de Spams entrants et qui consiste à demander à l'expéditeur de confirmer manuellement qu'il est bien à l'origine de l'envoi du message.

Puisque les Spams sont (presque) toujours envoyés par des robots, leur envoi ne sera pas confirmé par l'expéditeur. Le nombre des Spams ainsi déposés dans les boîtes aux lettres des utilisateurs est considérablement réduit.

Attention : le mécanisme du Défi est réalisé par l'envoi d'un message à l'expéditeur du message d'origine (adresse du champ From:). Or, les spammeurs placent généralement dans ce champ une adresse factice (**spoofing**) qui n'a rien à voir avec l'émetteur mais qui est empruntée à des domaines existants du réseau internet. Ces derniers vont donc recevoir un message de défi alors qu'ils n'ont rien envoyé.
Cela pose deux problèmes :

- Un trafic parasite qui encombre le réseau et surcharge le serveur
- Le risque d'être mis en **liste noir** par des serveurs qui détectent ce comportement considéré actuellement comme anormal (bounce back); Voir le site http://www.backscatterer.org/ pour plus d'informations.

Il est donc recommandé de filtrer les messages le plus en amont possible du traitement SMTP en utilisant les mécanismes de **prévention des intrusions** et des **listes grises** détaillés en fin de document.

Concept de mise en œuvre

Les concepts de **Quarantaine** et de **Défi** sont liés dans l'implémentation des techniques Anti-Spam du Serveur IceWarp.

Le Défi est une option de la Quarantaine. Il est possible d'utiliser la Quarantaine sans le Défi. Nous supposons par la suite que le mécanisme de Défi est activé.

Chaque mail est analysé avec l'ensemble des techniques Anti-Spam disponibles dans IceWarp. A la fin de ce traitement, un **score global** (entre 0 et 10) est attribué au message. Comme nous le verrons dans la suite, ce score détermine le sort du message.

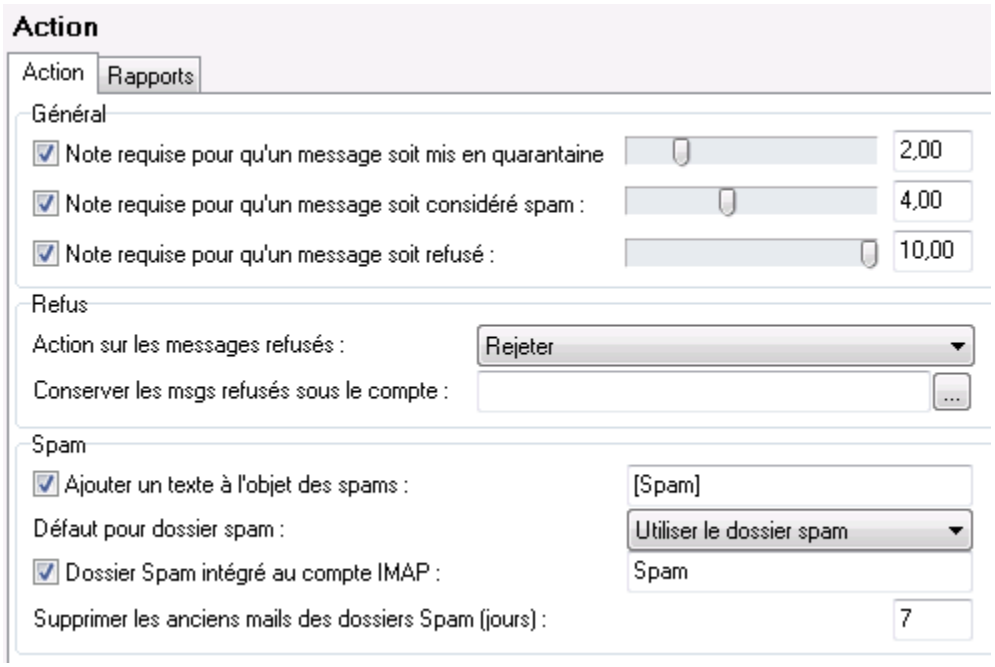
Icewarp permet de gérer trois seuils : un seuil de **Quarantaine**, un seuil de **Spam** et un seuil de **Refus**. Le seuil de Refus est généralement supérieur aux deux autres, nous ne le traiterons pas ici.

Le traitement dépend de la valeur relative des scores Quarantaine et Spam :

1) seuil de Quarantaine < seuil de Spam
   dans ce cas, tout message dont le score global est
   - inférieur au seuil de Quarantaine, est considéré comme un "bon" message et déposé dans la boîte de réception du destinataire
   - entre le seuil de Quarantaine et le seuil de Spam, est considéré comme "suspect" et mis dans une zone de quarantaine en attendant une confirmation de la part de l'expéditeur (il s'agit du mécanisme de Défi)
   - supérieur au seuil de Spam, est considéré comme "Spam" et traité comme tel
2) seuil de Spam < seuil de Quarantaine
   dans ce cas, tout message dont le score global est
   - inférieur au seuil de Spam, est considéré comme un "bon" message et déposé dans la boîte de réception du destinataire
   - entre le seuil de Spam et le seuil de Quarantaine, est considéré comme "Spam" et traité comme tel
   - supérieur au seuil de Quarantaine, est considéré comme "suspect" et mis dans une zone de quarantaine en attendant une confirmation de la part de l'expéditeur (il s'agit du mécanisme de Défi)

Si les deux seuils sont identiques, le traitement effectué au delà du seuil est celui de la Quarantaine.

Tous ces seuils sont réglables dans l'écran suivant obtenu par le menu Anti-Spam -> Général -> onglet Action.



Cet écran contient aussi les traitements à effectuer lorsque le seuil **Spam** est atteint.

Chaque administrateur du serveur IceWarp devrait étudier le **journal Anti-Spam** (il est recommandé d'activer le journal Anti Spam à "Détaillé" dans Système -> Journaux -> onglet Services) pour vérifier l'adéquation des seuils définis. Voici un exemple de message placé en quarantaine :

```
127.0.0.1       [0EF8] 13:07:11 TTS42705 '<francois@iwdemo.fr>' '<jean@iwdemo.fr>' 1 score 3,51
reason [SpamAssassin=2,51,Other=1,00:Body=R] action QUARANTINE
```

Un message placé en **Quarantaine** en sortira de quatre façons possibles si le mécanisme de Défi est activé :

- **l'expéditeur confirme son envoi** au travers la méthode de Défi. Dans ce cas, l'adresse email de l'expéditeur est automatiquement inscrite dans la liste blanche du destinataire. Aucun des messages suivants de cet expéditeur à ce destinataire ne sera plus jamais challengé.
- le **destinataire** décide **d'accepter ou de supprimer** le message (par le dossier quarantaine ou le rapport de spam). Il peut aussi décider d'inscrire l'expéditeur dans sa liste blanche/liste noire.
- **l'administrateur** du serveur décide de **délivrer ou de supprimer** le message (par le dossier quarantaine ou le rapport de spam). Il peut aussi décider d'inscrire ce couple (expéditeur, destinataire) dans la liste blanche/liste noire
- à la fin de la **période** (paramétrée) de mise en Quarantaine, le message est supprimé de la file de Quarantaine et optionnellement distribué comme Spam ou supprimé.

La configuration du mécanisme de Défi

Les différentes étapes sont les suivantes.

1. **Activer l'Anti Spam**

Le Défi étant l'une des techniques d'Anti-Spam, ceci est un préalable à la configuration de Défi.

L'anti spam au niveau serveur est activé dans Système -> Services -> onglet Général -> service Anti-Spam (Démarrer/arrêter). Le service doit être précédé d'un rond vert :

L'anti spam doit ensuite être coché au niveau du compte dans l'onglet Stratégies :

Il faut pour cela que la quarantaine soit activée au niveau du domaine.

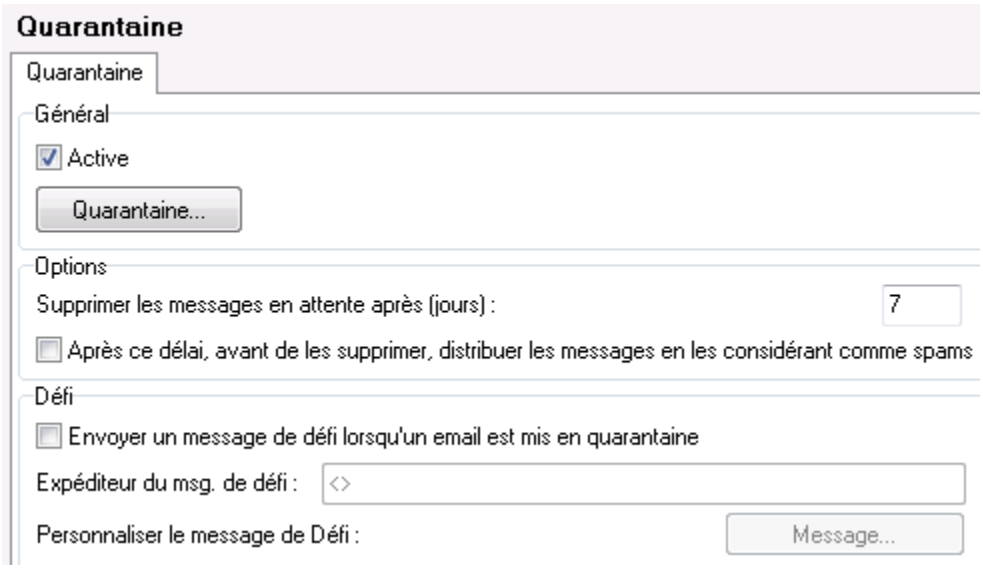
Pour contrôler et modifier la quarantaine sur un grand nombre de compte, il faut utiliser la commande tool dans une invite de commande Windows en se plaçant dans le répertoire principal d'IceWarp :

Pour visualiser la quarantaine (0 = non activée et 1 = activée) :
tool --filter="U_Type=0" get account *@* U_Quarantine

Pour la modifier (0 pour la supprimer) sur tous les comptes utilisateurs du système :
tool --filter="U_Type=0" set account *@* U_Quarantine=0

2. Activer l'option Quarantaine

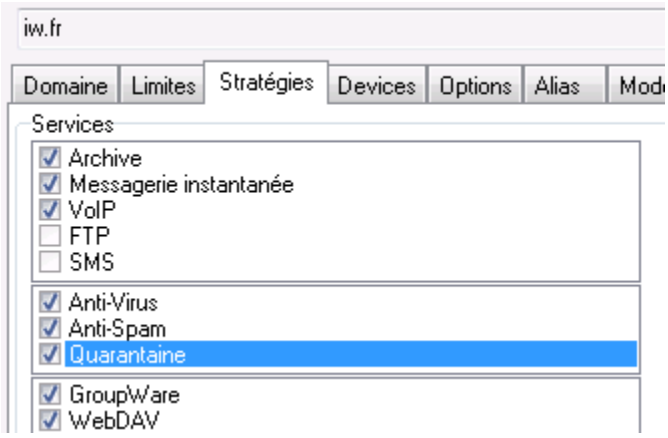
Le Défi étant l'une des options de la quarantaine, ceci est un préalable à la configuration de Défi



3. Indiquer les comptes pour lesquels la Quarantaine est activée.

Les expéditeurs des messages destinés à un compte pour lequel l'option Quarantaine n'est pas activée ne seront jamais challengés.

La quarantaine doit être activée au niveau du compte dans l'onglet Stratégies mais au préalable, il faut l'activer au niveau du domaine :

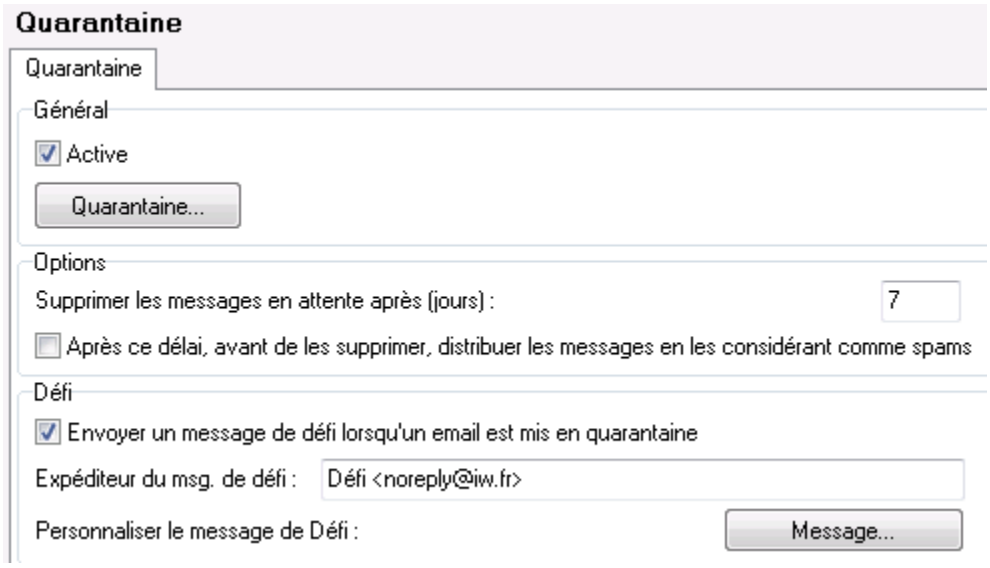


Puis au niveau du compte lui-même :

Il faut prendre soin de décocher l'option pour les comptes dont on ne veut pas qu'ils aient la quarantaine.

4. Indiquer à IceWarp qu'un message de Défi doit être envoyé à l'expéditeur

Ceci s'effectue en cochant l'option "Envoyer un message de défi lorsqu'un email est mis en quarantaine" :

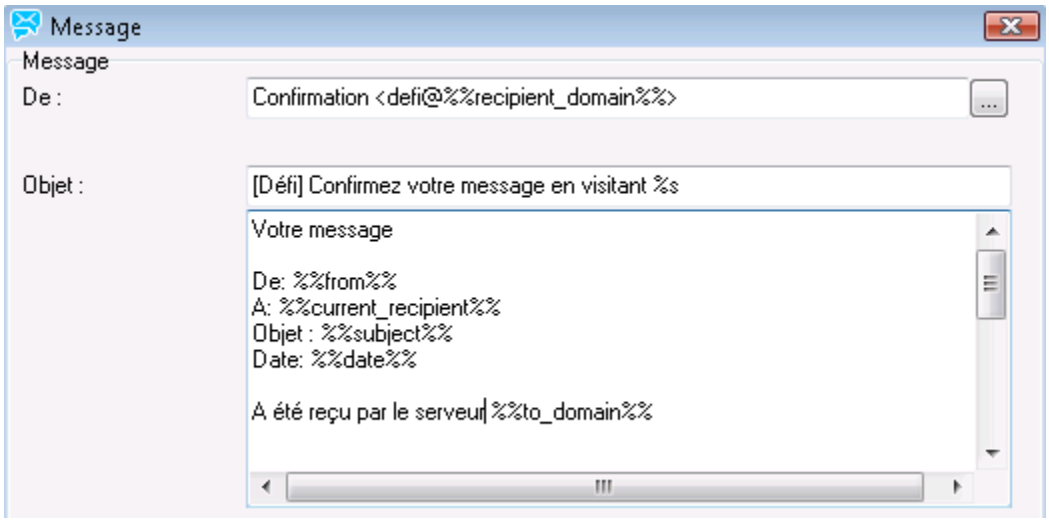


En absence de cette option, le message sera mis en Quarantaine mais l'expéditeur ne sera pas averti de ce fait. Au niveau SMTP, le message est bien reçu par le serveur IceWarp; donc l'expéditeur a toute raison de croire que son message a été reçu par le destinataire.

L'expéditeur de ce message ("Défi <noreply@iwdemo.fr>")est volontairement positionné à un compte non existant sur votre serveur. Le nom utilisé est significatif pour indiquer qu'il n'est pas nécessaire de répondre à ce message.

5. Définir le contenu du message

Le **contenu** du message peut être modifié par le bouton "Message..." de l'écran précédent :



La variable **%%recipient_domain%%** est remplacée par IceWarp par le nom de domaine du compte à qui le message initial était destiné. Le paramétrage de Défi étant commun à tout le serveur, l'utilisation de cette variable fournit un service personnalisé pour chaque domaine du serveur IceWarp.

Ce qui est important, c'est de communiquer l'URL vers laquelle l'expéditeur du message original doit être dirigé pour confirmer son envoi. Cette URL est contenue dans la variable **%s**. Ainsi, il est impératif de mettre cette chaîne "%s" au moins une fois dans l'objet et/ou texte du message automatique de Défi.

Le texte du message peut être en html (couleurs, polices, images…). Un exemple de texte complet est présenté ici (à personnaliser par chaque administrateur).

```
<html>

<head>
<meta http-equiv=Content-Type content="text/html; charset=utf-8">
</head>

<body>
Votre message
<br>
De: <b>%%Sender_Email%%</b>
<br>
A: <b>%%Current_Recipient%%</b>
<br>
Objet: <b>%%subject%%</b>
<br>
Date: <b>%%date%%</b>
<br>
<br>
a été reçu par le serveur de messagerie du domaine %%recipient_domain%%.
<br>
<br>
Afin d'acheminer le message que vous venez d'envoyer, merci de suivre la procédure ci-dessous.
<br>
<br>
<FONT COLOR="#FF0000"> VOTRE MESSAGE NE SERA REMIS QU'APRES CETTE CONFIRMATION !</FONT>
<br>
```

```
<br>
Vous devez consulter la page Web suivante :
<p><a href="%s">%s</a></p>

Une série de lettres et de chiffres va s'afficher sur une grille. Vous devez recopier ces caractères dans le
champ situé en dessous et valider (bouton "GO").
<br>
Cette opération ne vous sera demandée qu'une seule fois, vos messages seront ensuite automatiquement
acceptés par notre anti-spam.
<br>
<br>
Merci.
<br>
Administrateur de messagerie
<br>
<p class=MsoNormal><font size=2 face=Arial><span style='font-size:10.0pt;
font-family:Arial'><img
src="https://mail.iwdemo.fr/reports/%%recipient_domain%%/domainlogo.gif"></span></font></p>
</body>

</html>
```

A noter l'utilisation de plusieurs variables système qui seront remplacées par IceWarp au moment de l'envoi du mail. Si des images sont utilisées comme ci-dessus, il faut placer les fichiers correspondants dans le répertoire "…\html\reports\<nom du domaine>\"

L'expéditeur original reçoit un message comme celui-ci :

[Défi] Confirmez votre message en visitant http://192.168.0.229/reports /?folder=201008111201180025008 5

Confirmation <Challenge@iwdemo.fr> [+]

À: francois@iwdemo.fr [+]

Votre message
De: **francois@iwdemo.fr**
A: **jean@iwdemo.fr**
Objet: **test Défi**
Date: **11/08/2010**

a été reçu par le serveur de messagerie du domaine iwdemo.fr.

Afin d'acheminer le message que vous venez d'envoyer, merci de suivre la procédure ci-dessous.

VOTRE MESSAGE NE SERA REMIS QU'APRES CETTE CONFIRMATION !

Vous devez consulter la page Web suivante:

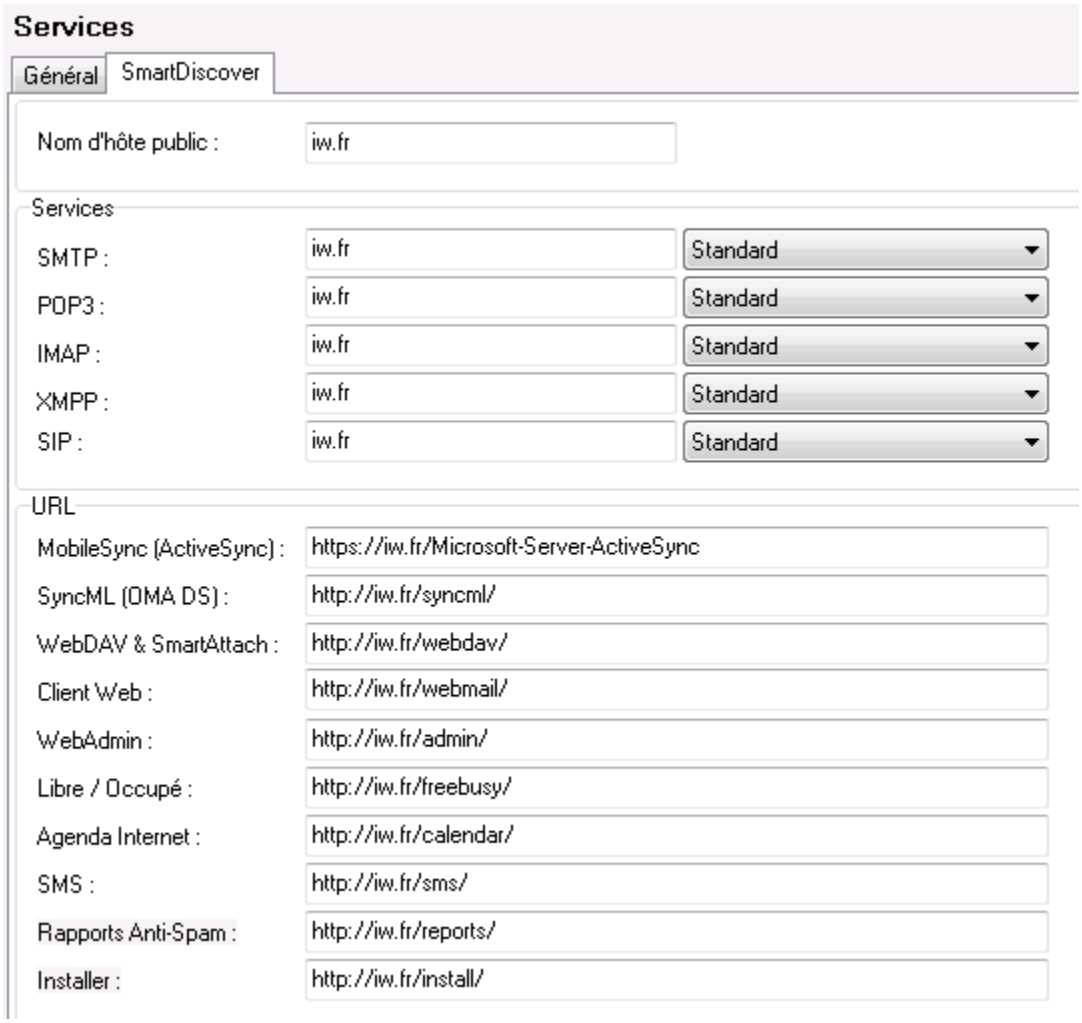
http://192.168.0.229/reports/?folder=20100811120118002500 85

Une série de lettres et de chiffres va s'afficher sur une grille. Vous devez recopier ces caractères dans le champ situé en dessous et valider (bouton "GO").
Cette opération ne vous sera demandée qu'une seule fois, vos messages seront ensuite automatiquement acceptés par notre anti-spam.

Merci.
Administrateur de messagerie

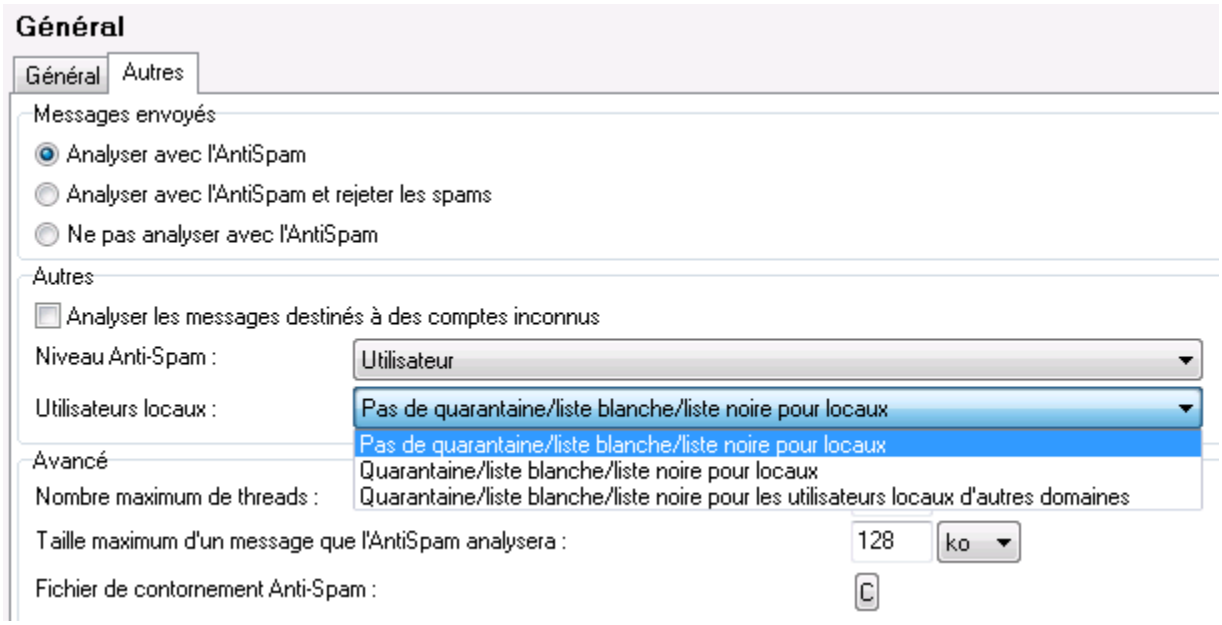
6. Vérifier l'URL sur laquelle IceWarp génère automatiquement une page de challenge

On trouve cette URL dans le menu Système -> Services -> onglet SmartDiscover -> Rapports Anti-Spam :



7. **Définir la stratégie à adopter pour les utilisateurs locaux**

Cette option permet de définir les actions à effectuer vis à vis des autres utilisateurs du serveur.

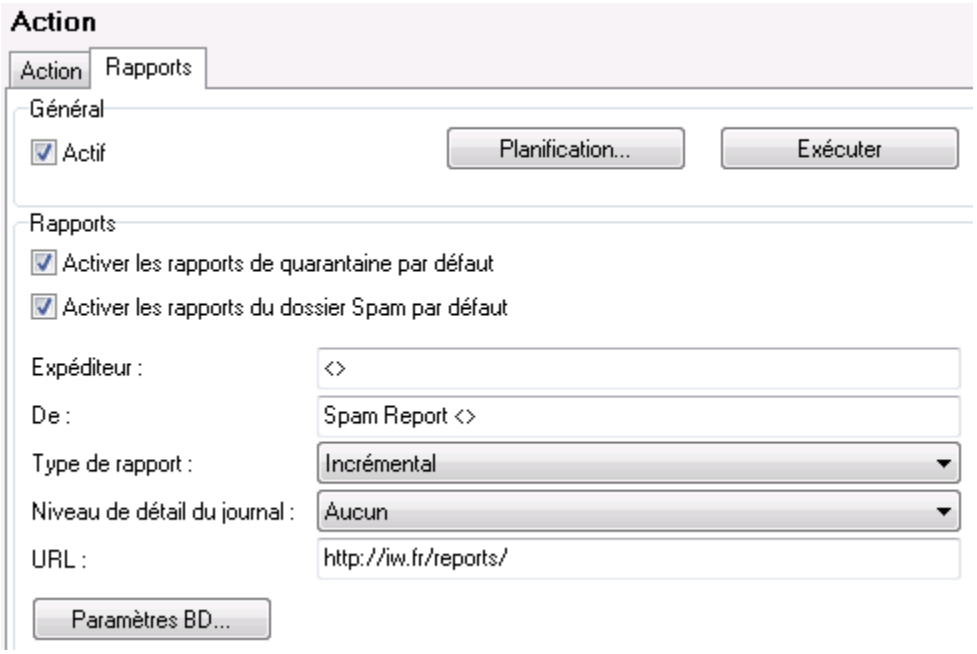


Les différents choix :

- Vous n'avez qu'un domaine sur le serveur IceWarp et vous considérez que tous les comptes de ce domaine sont des comptes connus et qu'il n'est pas nécessaire de leur demander confirmation : utiliser "**Pas de Quarantaine/liste blanche/liste noire pour locaux**"
- Vous avez plusieurs domaines sur le serveur IceWarp et vous pouvez faire confiance aux utilisateurs du même domaine que vous mais pas à ceux d'autres domaines : utiliser "**Quarantaine/liste blanche/liste noire pour locaux d'autres domaines**"
- Vous avez un ou plusieurs domaines sur le serveur IceWarp et vous ne pouvez faire confiance à aucun des comptes de ce(s) domaine(s) : utiliser " **Quarantaine/liste blanche/liste noire pour locaux**"

8. Utilisation des rapports

Cette option permet de faire envoyer un rapport au destinataire pour lui indiquer la mise en Quarantaine des messages qui lui étaient destinés :



Il faut cocher l'option "Activer les rapports de Quarantaine par défaut".

9. Personnalisation de la page affichée à l'URL de Défi

Le contenu de la page affichée quand l'expéditeur visite l'URL de défi, est défini dans le fichier suivant: "…\html\reports\lang\rf\lang.xml".

L'administrateur peut éditer ce fichier pour personnaliser le texte.

Attention : Si les chaînes contenues dans ce fichier contiennent des textes avec des caractères accentués, il faut sauvegarder ce fichier en mode 'UTF-8'.

Le traitement des messages en quarantaine

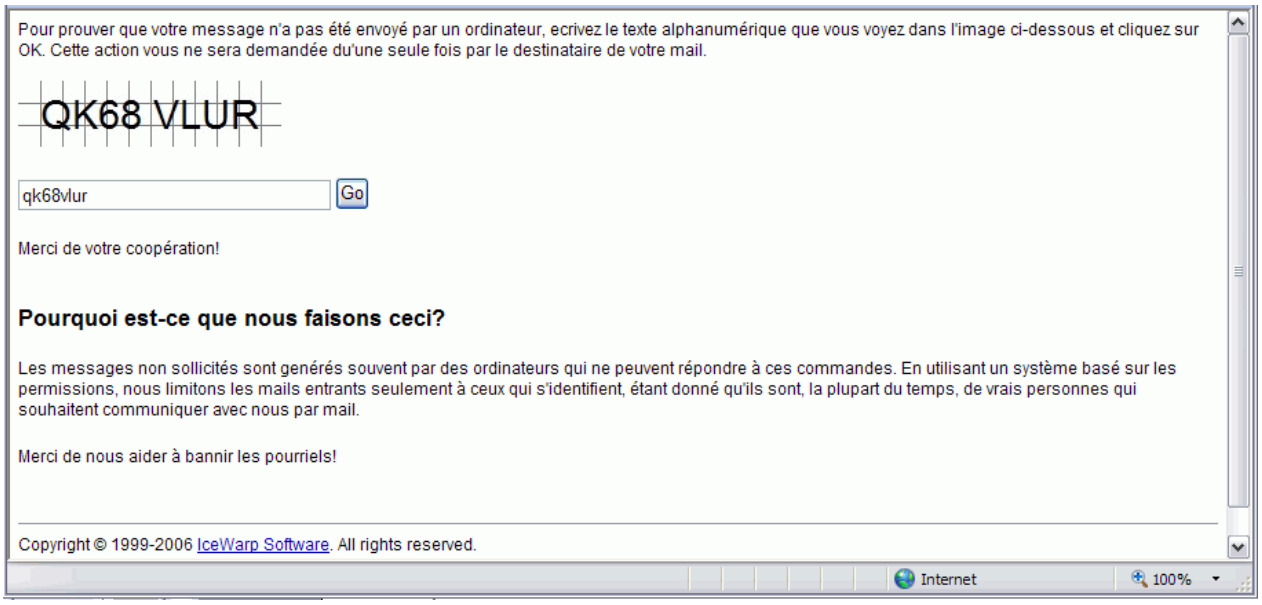
Les mails mis en Quarantaine sont stockés de la façon suivante sur le serveur IceWarp:

- Une ligne est inscrite dans la table "Senders" de la base de données Anti-Spam indiquant l'expéditeur, le destinataire, la date, l'heure, l'objet du mail, le mot envoyé pour Défi, le dossier de stockage.
- Le mail lui-même est stocké dans le répertoire :
  ...\mail\<domaine>\<compte>\~spam\~quarantine\

Confirmation par l'expéditeur

Voici la séquence de traitement vue de l'expéditeur du message original :

- L'expéditeur a envoyé un mail sur un compte pour lequel l'option Quarantaine était activée
- Le score affecté au mail déclenche sa mise en Quarantaine (cf. § concept)
- L'option "Envoyer un message de défi…" a été activée (cf. étape 4)
- L'expéditeur reçoit le mail envoyé par le moteur Défi (cf. étape 5)
- L'expéditeur visite la page indiquée dans ce mail. Il verra une page comme ceci:



- L'expéditeur entre la chaîne de caractères demandée (majuscules/minuscules non significatifs, blancs non significatifs) et il clique sur le bouton "Go"
- Il est notifié que sa réponse a été enregistrée
- Côté serveur IceWarp,
  - Le mail est délivré dans la boîte de réception du destinataire

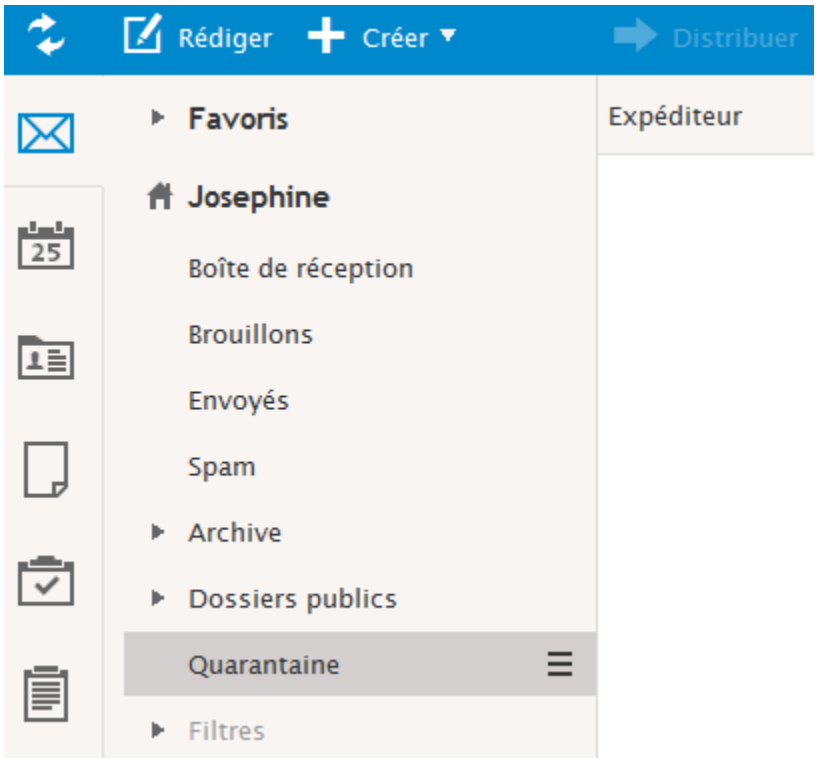
  - Le couple (expéditeur, destinataire) est ajouté à la liste blanche
- A partir de ce moment, tout mail venant de "l'expéditeur" et envoyé au "destinataire" ne sera jamais considéré comme Spam.

Traitement par le destinataire

Le destinataire a deux façons de visualiser la liste de ses messages en Quarantaine et prendre une action souhaitée.

Dossier Quarantaine

Cette option n'est offerte qu'aux utilisateurs du Client Web dont le compte est de type IMAP ou IMAP & POP3, le dossier de leurs mails en Quarantaine est directement accessible en sans paramétrage spécifique :



A partir de cette interface, l'utilisateur peut choisir pour chaque message entre :

- **distribuer** le mail (sans ajouter l'expéditeur à la liste blanche)
- mettre l'expéditeur en **liste blanche**, le mail lui est remis
- mettre l'expéditeur en **liste noire** et le mail ne lui est pas remis
- **supprimer** le mail (sans ajouter l'expéditeur à la liste noire)

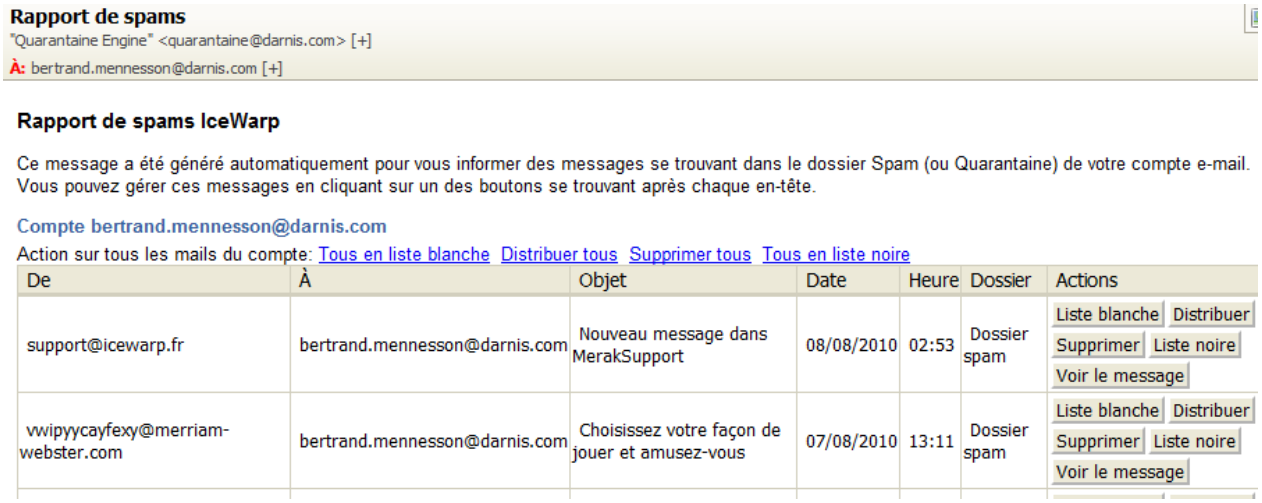
Il peut faire des actions en bloc en sélectionnant plusieurs messages à la fois.

Rapport de Quarantaine

Comme décrit à l'étape 8, le destinataire du mail original peut choisir de recevoir un rapport de ses mails en Quarantaine.

Grâce aux hyperliens contenus dans le mail de rapport, le destinataire peut effectuer les mêmes actions qu'au travers de son dossier Quarantaine

Il peut faire des actions en bloc en sélectionnant plusieurs messages à la fois.



Rapport de spams
"Quarantaine Engine" <quarantaine@darnis.com> [+]
À: bertrand.mennesson@darnis.com [+]

Rapport de spams IceWarp

Ce message a été généré automatiquement pour vous informer des messages se trouvant dans le dossier Spam (ou Quarantaine) de votre compte e-mail. Vous pouvez gérer ces messages en cliquant sur un des boutons se trouvant après chaque en-tête.

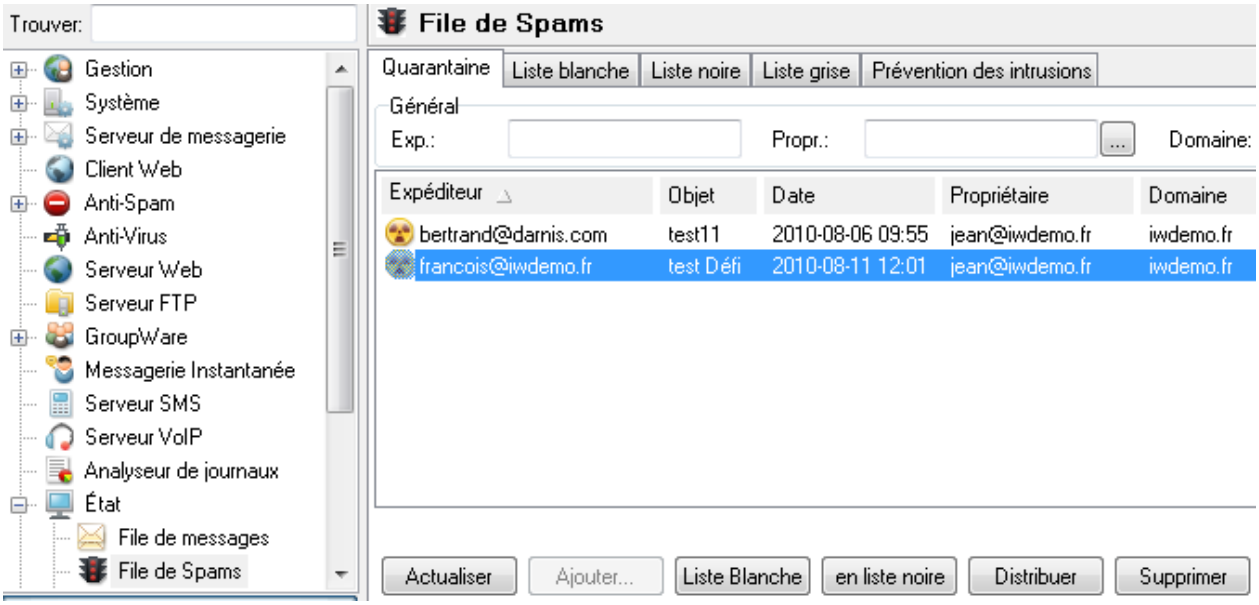
Compte bertrand.mennesson@darnis.com

Action sur tous les mails du compte: Tous en liste blanche Distribuer tous Supprimer tous Tous en liste noire

De	À	Objet	Date	Heure	Dossier	Actions
support@icewarp.fr	bertrand.mennesson@darnis.com	Nouveau message dans MerakSupport	08/08/2010	02:53	Dossier spam	Liste blanche Distribuer Supprimer Liste noire Voir le message
vwipyycayfexy@merriam-webster.com	bertrand.mennesson@darnis.com	Choisissez votre façon de jouer et amusez-vous	07/08/2010	13:11	Dossier spam	Liste blanche Distribuer Supprimer Liste noire Voir le message

Traitement pas l'administrateur du serveur

La console d'administration de IceWarp (ou la console Web admin) qui est accessible aux administrateurs d'IceWarp permet de visualiser la file des messages en Quarantaine (Etat -> File de Spams -> onglet Quarantaine).



Sur cette interface, il peut livrer (bouton 'Distribuer') les messages en Quarantaine (sans les ajouter en liste blanche), mettre les messages en liste blanche (cela a aussi pour effet de délivrer ces messages), mettre les messages en liste noire ou les supprimer.

Traitement automatique après un lapse de temps

Si aucune action n'est appliquée à un message en Quarantaine, ni par l'expéditeur, ni par le destinataire, ni par l'administrateur, au bout du nombre de jours configuré dans l'option "Supprimer les messages en attente après (jours)", le mail est supprimé du dossier de Quarantaine (cf. écran de l'étape 2)

Le sort du message dépend de l'option "**Après ce délai, avant de les supprimer, distribuer les messages en les considérant comme Spam**" (cf. écran de l'étape 2) :

- si elle est cochée, les messages sont sortis de la Quarantaine et livrés au destinataire dans sa boîte Spam
- Si elle n'est pas cochée, les messages sont sortis de la Quarantaine et supprimés du serveur.

Si l'expéditeur visite la page URL après que le délai soit expiré et donc le message retiré de la file de Quarantaine, il recevra un message d'erreur approprié (voir les textes dans le fichier "…\html\reports\lang\fr\lang.xml").

Il est conseillé de positionner la variable "destruction des messages en attente après (jours)" à une valeur raisonnable pour que les trois acteurs aient le temps de prendre l'action appropriée.

Le premier acteur (l'expéditeur, le destinataire, l'administrateur) à traiter le mail termine la mise en Quarantaine de ce mail. Si l'expéditeur visite la page URL après qu'un traitement ait été effectué par le destinataire ou par l'administrateur ou après le temps maximum, il recevra un message d'erreur approprié (voir les textes dans le fichier "…IceWarp\html\challenge\lang\en\lang.xml").

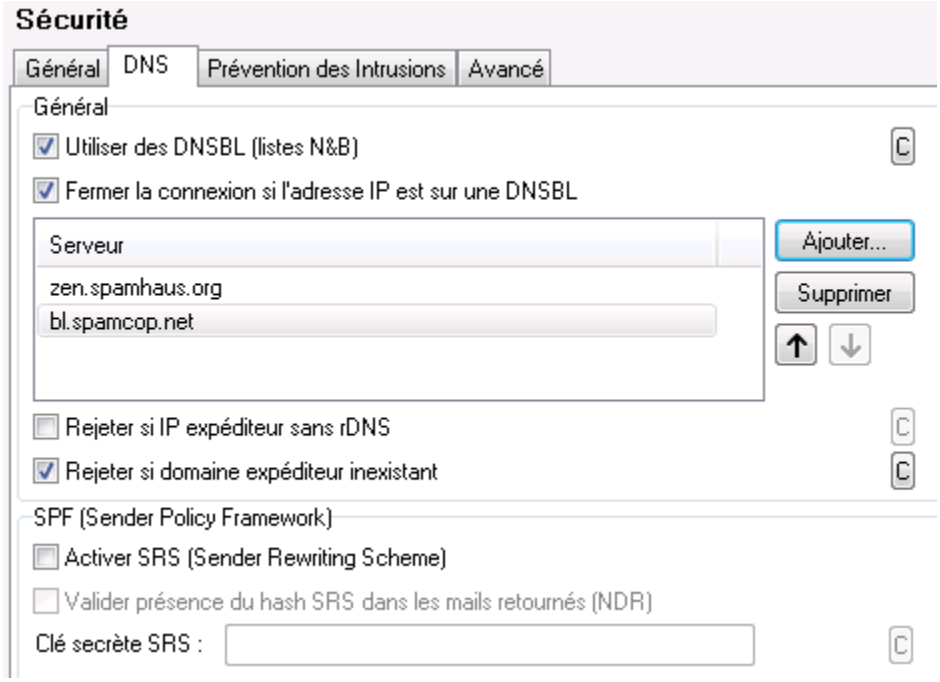
Prévention des Défis factices

Comme indiqué au début de ce document, le mécanisme de Défi peut être considéré comme nocif pour le réseau Internet car il envoie un message à tous les expéditeurs présumés (From:) sans être certain qu'ils sont les vrais expéditeurs.

La seule solution pour s'affranchir de ce problème est d'éliminer le plus possible de messages avant le traitement Anti-Spam proprement dit. Il existe plusieurs mécanismes sur le serveur IceWarp qui agissent au niveau du protocole SMTP, nous allons les indiquer et donner une configuration typique.

Les listes noires des DNS

Aller dans Serveur de messagerie -> Sécurité -> onglet DNS

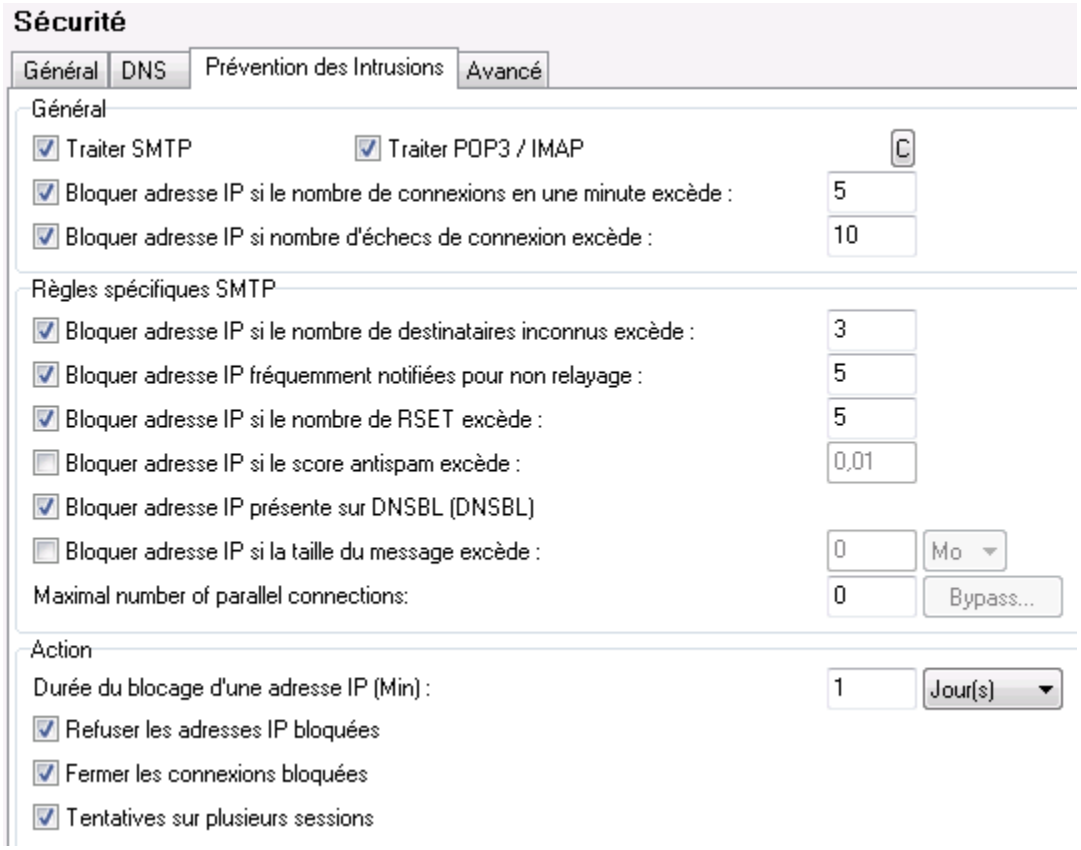


Ce mécanisme est très efficace, il fait appel à des serveurs externes qui listes les émetteurs de messages douteux (zen.spamhaus.org...).

Il peut être contourné ponctuellement (bouton C)

La Prévention des intrusions

Aller dans Serveur de messagerie -> Sécurité -> onglet Prévention des intrusions

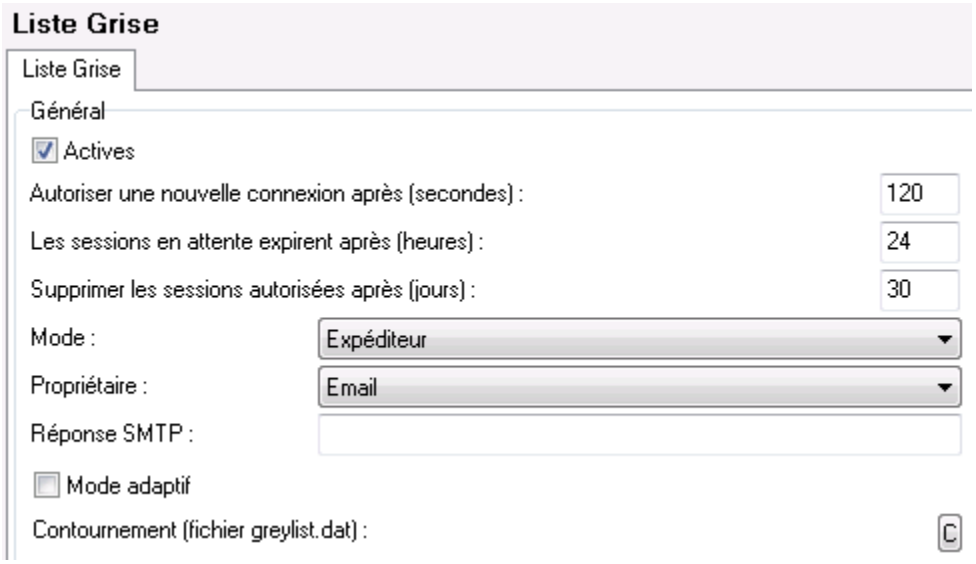


Ce mécanisme détecte certains comportements anormaux et bloque les adresses IP correspondantes.

Il peut être contourné ponctuellement (bouton C)

Les listes grises

Aller dans Anti-Spam -> Liste Grise



Ce mécanisme oblige tout nouvel expéditeur (non déjà référencé dans le serveur) à réémettre sa demande après un délai de 120 secondes (modifiable).

Ce délai incite beaucoup de spammeurs à renoncer alors que les émetteurs authentiques effectuent cette réémission conformément aux règles du protocole SMTP.

Il peut être contourné ponctuellement (bouton C)