Le Serveur de communication IceWarp

Quarantaine et Défi

Deep Castle 2 version 13.0

Octobre 2021

Sommaire

Quarantaine et Défi 2

Quarantaine et Défi

Introduction

Ce document indique la configuration à mettre en place pour utiliser la **Quarantaine** et, si besoin, la technique de **Défi** ou "Challenge response" offerte par le module Anti-Spam de serveur IceWarp.

Présentation

La **Quarantaine** est un mécanisme de l'Anti-Spam qui permet de traiter de façon particulière des messages dont on n'est pas certain que ce soit des spams mais sur lesquels il y a un doute.

Les concepts de **Quarantaine** et de **Défi** sont liés dans l'implémentation des techniques Anti-Spam du Serveur IceWarp. Il est cependant possible d'utiliser la Quarantaine sans le Défi.

Le **Défi** 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. Cette technique ne présente toutefois pas que des avantages, il faut l'utiliser avec prudence.

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 :

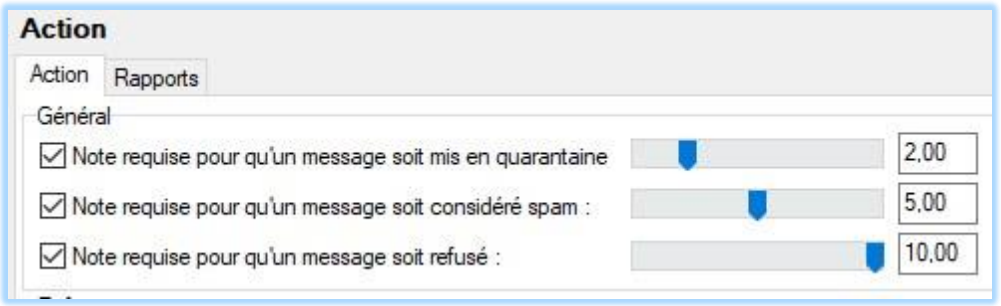
- Un trafic parasite qui encombre le réseau et surcharge le serveur
- Le risque d'être mis en **liste noir** par des serveurs qui détectent ce comportement considéré actuellement comme anormal (bounce back). Voir le site http://www.backscatterer.org/ pour plus d'informations.

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.

Mise en œuvre

Chaque message entrant 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. 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.



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

Seuil de Quarantaine inférieur au seuil de spam

Dans ce cas, tout message dont le score global est :

- Inférieur au seuil de Quarantaine, est considéré comme un message "bon" ou "authentique" 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 ou du destinataire.
- Supérieur au seuil de Spam, est considéré comme "Spam" et traité comme tel

Seuil de Quarantaine égal au seuil de spam

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

Seuil de Quarantaine à zéro

Dans ce cas un message n'est accepté que si son score est strictement égal à zéro. En pratique, seuls les expéditeurs en liste blanche ou authentifiés seront déposés dans la boîte de réception du destinataire.

Le destinataire doit regarder attentivement son dossier Quarantaine ou le rapport de spam pour détecter les messages authentiques qui auraient été mis en quarantaine.

Seuil de Quarantaine supérieur au seuil de spam

Cette configuration est rarement utilisée.

Attention : les messages en quarantaine ne sont **archivés** que lorsqu'ils arrivent dans la boîte de réception du destinataire.

Un utilisateur peut avoir la **Quarantaine validée** ou non dans sa configuration. Si elle n'est pas validée, le seuil de Quarantaine n'est pas traité pour lui et seul le seuil de spam sera effectif.

Le **journal Anti-Spam** (il est recommandé d'activer le journal Anti Spam à "Détaillé" dans Système -> Journaux -> onglet Services) permet de vérifier l'adéquation des seuils définis. Voici un exemple de message placé en Quarantaine :

```
192.168.10.2 [39EC] 10:42:30 202110081042250048 'bertrand.mennesson@darnis.com
(<SRS0+5fa9292f3aa6d9c9=O4=darnis.com=bertrand.mennesson@darnis.com>)'
'<jean@iwdemo.fr>' 1 score 0,70 reason [SpamAssassin=0,70:(TVD_SPACE_RATIO=0,00,
HTML_MESSAGE=0,00,BAYES_50=0,80,DKIM_VALID=-0,10,SPF_FAIL=0,00,SPF_HELO_NONE=0,00)]
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 le mécanisme 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 soumise au Défi.
- 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 **distribuer 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 (voir l'onglet Quarantaine).

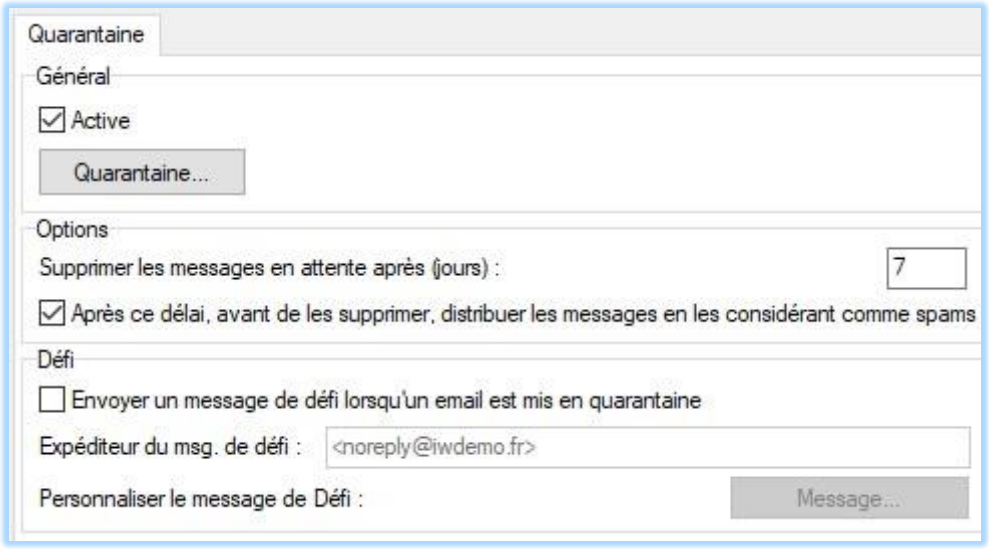
La configuration de la Quarantaine

Activer l'Anti-Spam

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

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 :

Activer l'option Quarantaine au niveau Anti-Spam



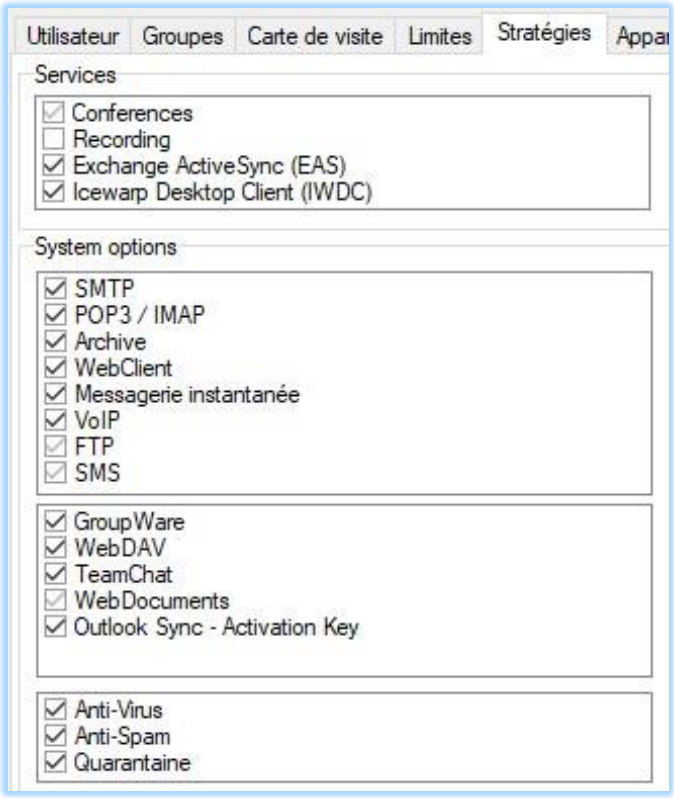
Lorsque l'option est activée et que le dossier n'est pas vide, un dossier Quarantaine apparaît alors dans l'interface du Client Web (et lui uniquement) :

Il est possible de modifier le délai d'attente des messages en quarantaine, 7 jours par défaut.

Il est conseillé de mettre les messages dans les spams après ce délai plutôt que de les supprimer.

Activer l'option Quarantaine au niveau des comptes

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



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

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

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

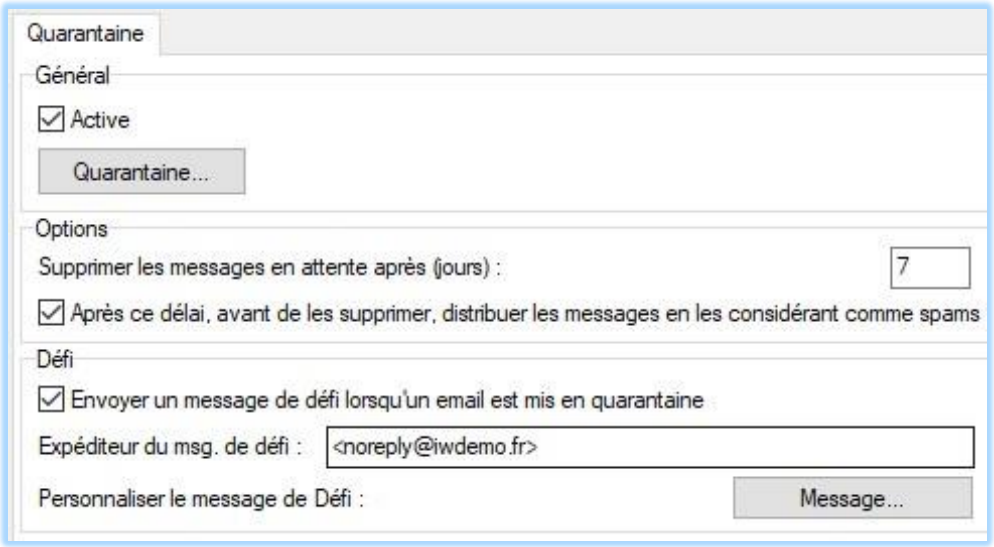
Pour visualiser la Quarantaine (0 = non activée et 1 = activée) :
tool --filter="U_Type=0" get account *@* U_Quarantine

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

Activer le Défi

Si le Défi doit être actif.

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



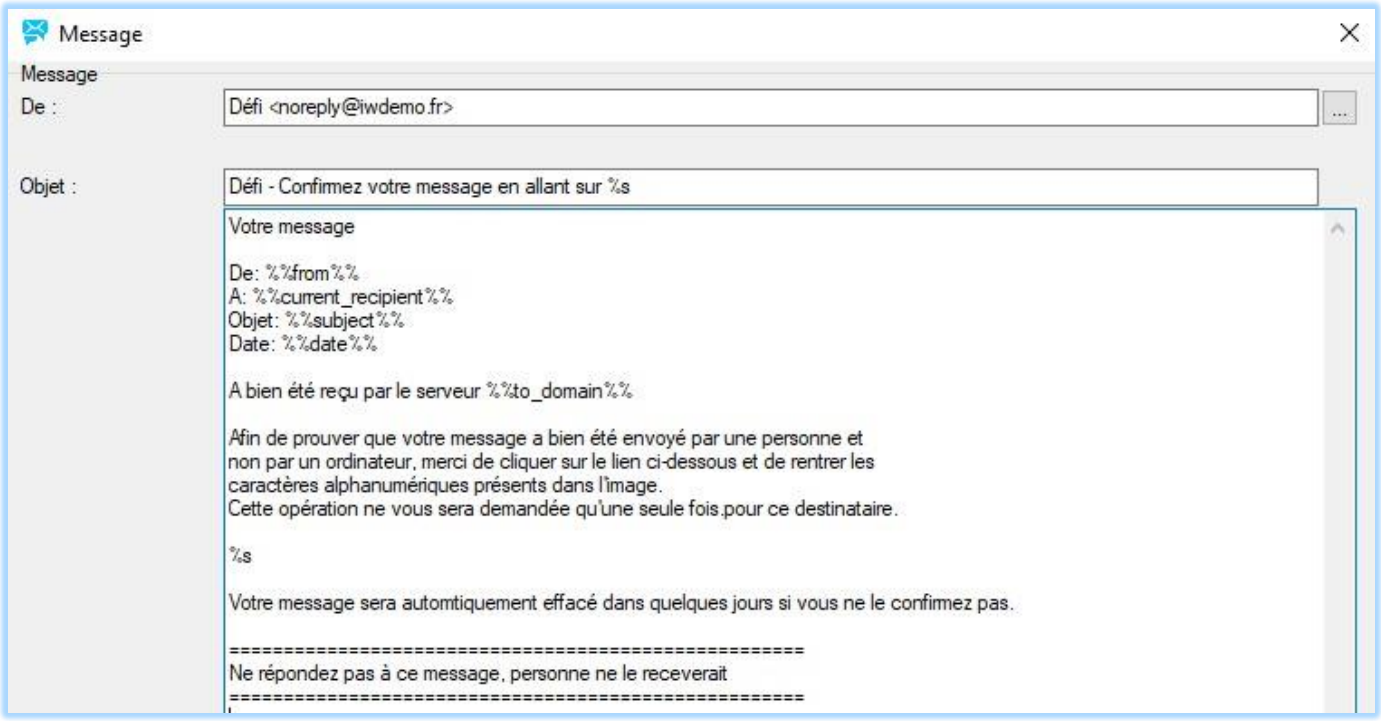
En absence de cette option, le message sera mis en Quarantaine mais l'expéditeur ne sera pas averti de ce fait. Au niveau SMTP, le message est bien reçu par le serveur IceWarp ; donc l'expéditeur a toute raison de croire que son message a été reçu par le destinataire.

Si un compte n'a pas la Quarantaine, il n'aura pas non plus le Défi.

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.

Définir le contenu du message de Défi

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



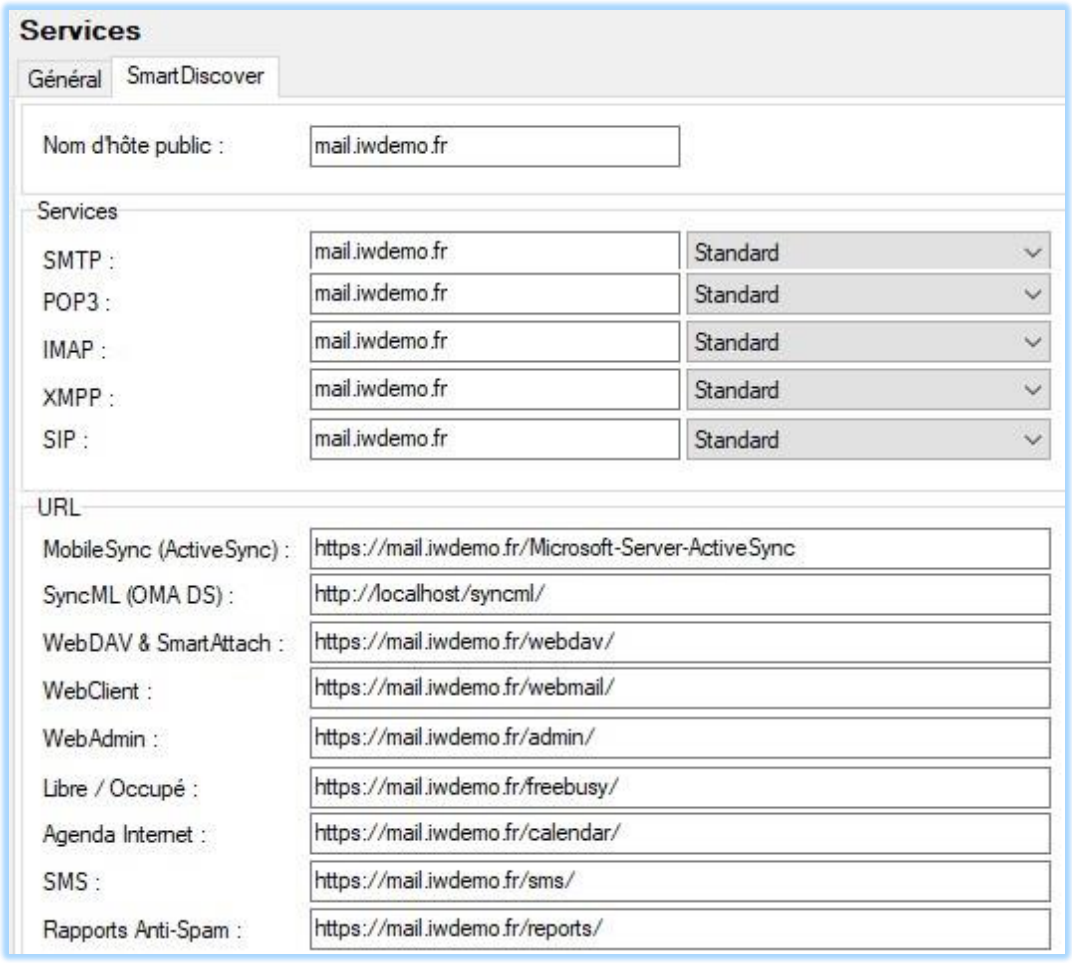
A noter l'utilisation de plusieurs **variables système** qui seront remplacées par IceWarp au moment de l'envoi du mail. Ce qui est important, c'est de communiquer l'URL vers laquelle l'expéditeur du message original doit être dirigé pour confirmer son envoi. Cette URL est contenue dans la variable **%s**. 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…). Toutefois il est conseillé de définir le **message le plus simple possible** ayant toutes les chances de passer les barrières anti-spam. Ce message de Défi se retrouve en effet souvent dans les spams de l'expéditeur qui ne confirmera donc jamais son envoi.

Voir les messages reçus ici.

Vérifier l'URL sur laquelle IceWarp génère la page de Défi

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



Ici on a " https://mail.iwdemo.fr/reports/" qu'il faut adapter au nom du serveur.

En cas de système multi domaines, il est possible de personnaliser l'URL par domaine en écrivant :

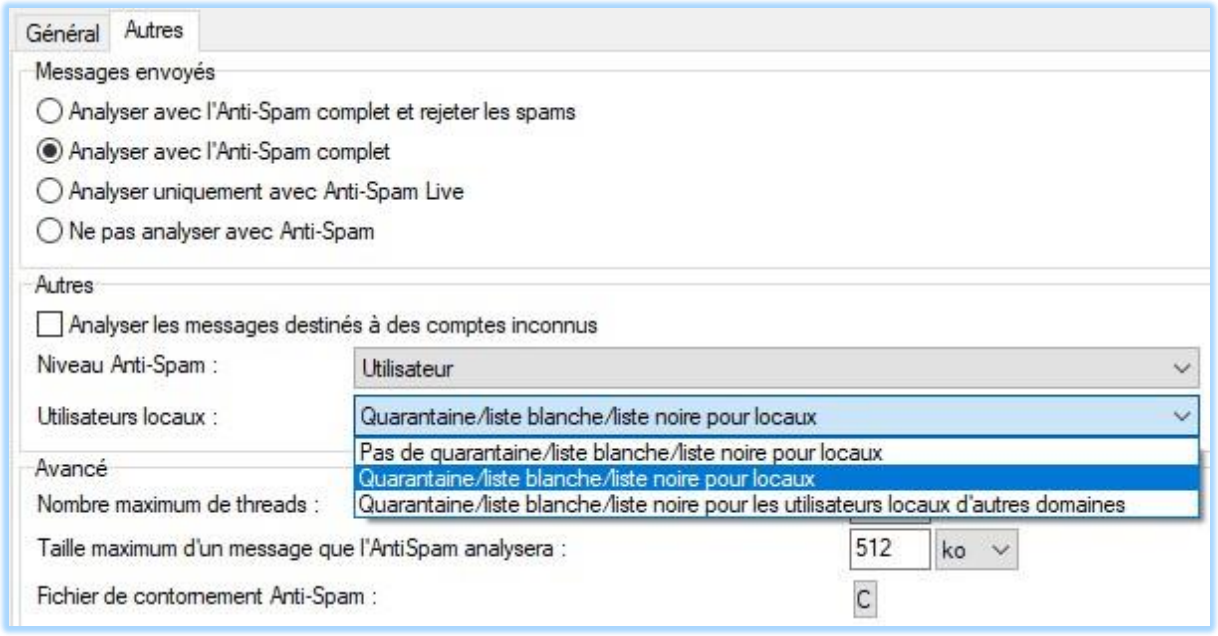
https://mail.%%Recipient_Domain%%/reports/

Il faut toutefois que le nom du serveur soit construit sur le nom du domaine en ajoutant le préfixe "mail."

Il faut toujours utiliser une URL en "https".

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.

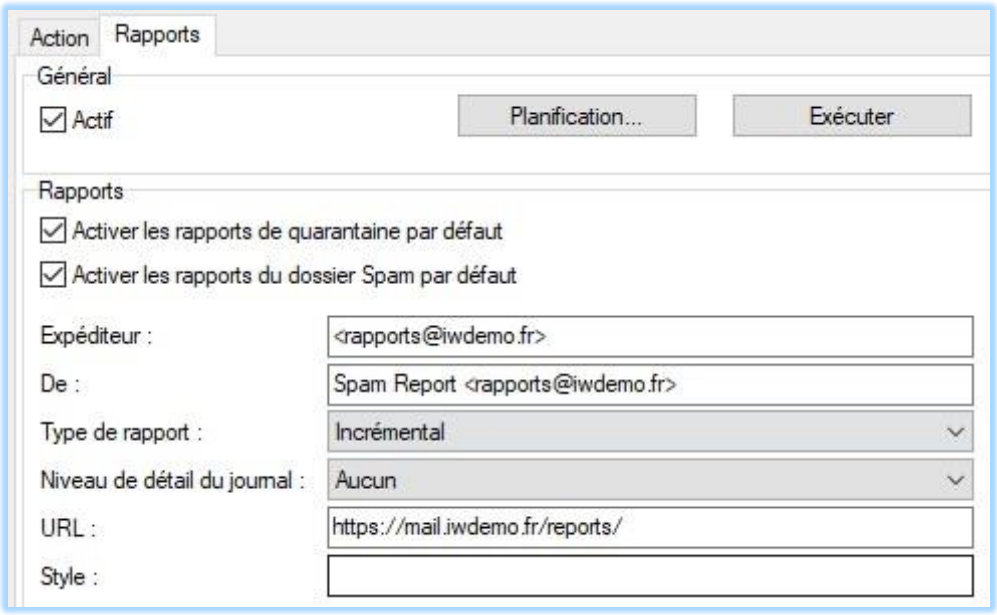


Les différents choix :

- 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**"

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".

C'est une option très utile pour les utilisateurs surtout s'ils n'utilisent pas le Client Web.

Il faut rentrer une planification (au moins 2 fois par jour) et remplir un nom pour l'expéditeur.

Le rapport peut être invalidé pour certains comptes si besoin (onglet Options du compte).

Le traitement des messages en Quarantaine

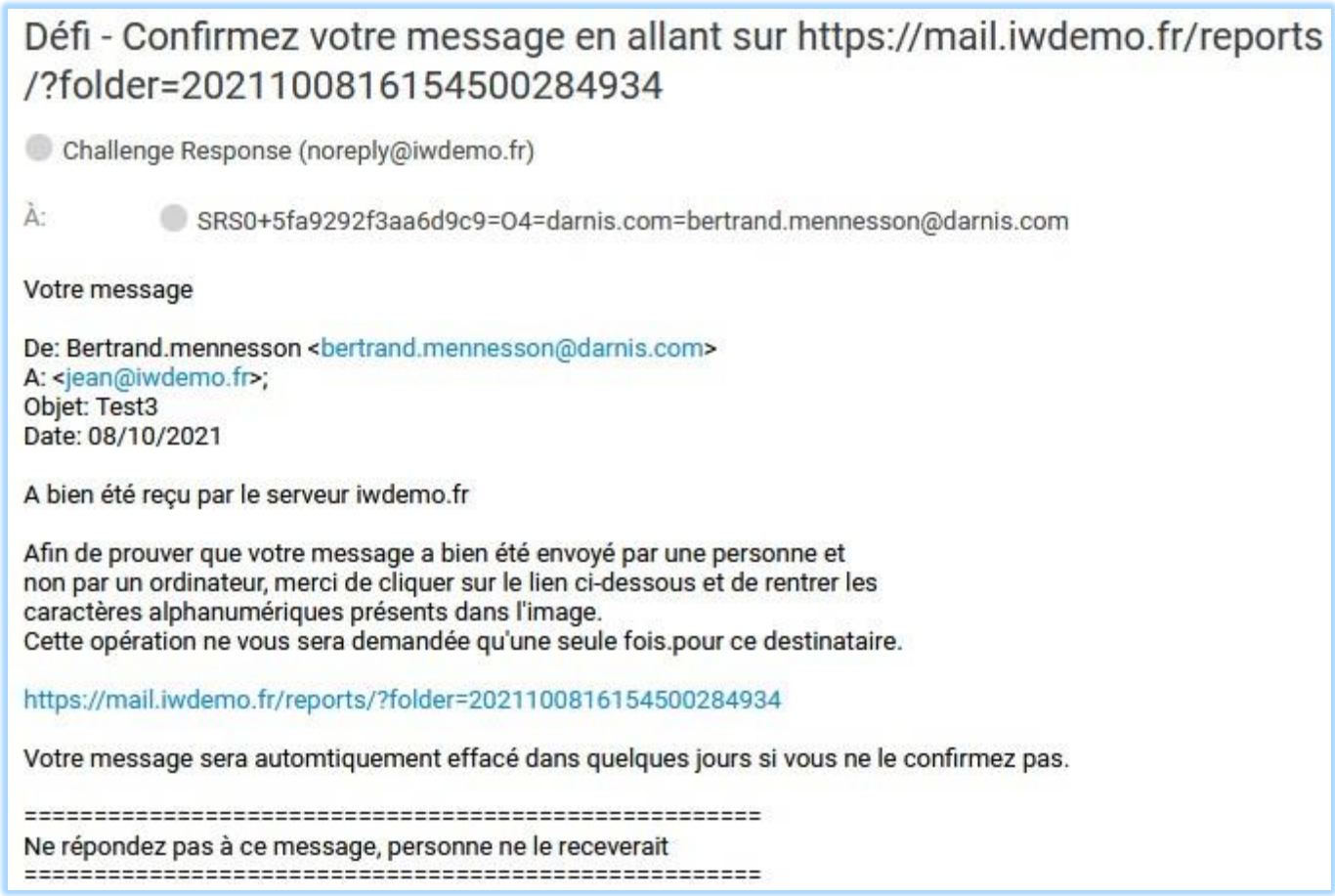
Les messages mis en Quarantaine sont stockés de la façon suivante sur le serveur IceWarp :

- 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 code envoyé pour le 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 :

- 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
- L'option "Envoyer un message de Défi…" était activée
- L'expéditeur reçoit ce message envoyé par le mécanisme de Défi :



Défi - Confirmez votre message en allant sur https://mail.iwdemo.fr/reports/?folder=20211008161545002849 34

Challenge Response (noreply@iwdemo.fr)

À: SRS0+5fa9292f3aa6d9c9=O4=darnis.com=bertrand.mennesson@darnis.com

Votre message

De: Bertrand.mennesson <bertrand.mennesson@darnis.com>
A: <jean@iwdemo.fr>;
Objet: Test3
Date: 08/10/2021

A bien été reçu par le serveur iwdemo.fr

Afin de prouver que votre message a bien été envoyé par une personne et non par un ordinateur, merci de cliquer sur le lien ci-dessous et de rentrer les caractères alphanumériques présents dans l'image.
Cette opération ne vous sera demandée qu'une seule fois.pour ce destinataire.

https://mail.iwdemo.fr/reports/?folder=20211008161545002849 34

Votre message sera automtiquement effacé dans quelques jours si vous ne le confirmez pas.

==========
Ne répondez pas à ce message, personne ne le receverait
==========

- L'expéditeur visite la page indiquée dans ce mail. Il voit une page comme celle-ci :

- L'expéditeur entre la chaîne de caractères demandée (majuscules/minuscules non significatifs, blancs non significatifs) et il clique sur le bouton "go"
- Il lui est notifié que sa réponse a été enregistrée
- Le mail est délivré dans la boîte de réception du destinataire
- Le couple (expéditeur, destinataire) est ajouté à la liste blanche

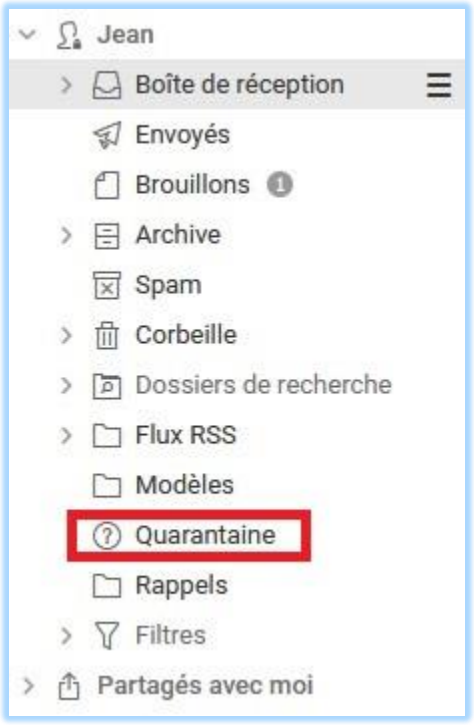
A partir de ce moment, tout mail venant de "l'expéditeur" et envoyé au "destinataire" ne sera jamais considéré comme Spam.

Traitement par le destinataire

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

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 messages en Quarantaine est directement accessible 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.

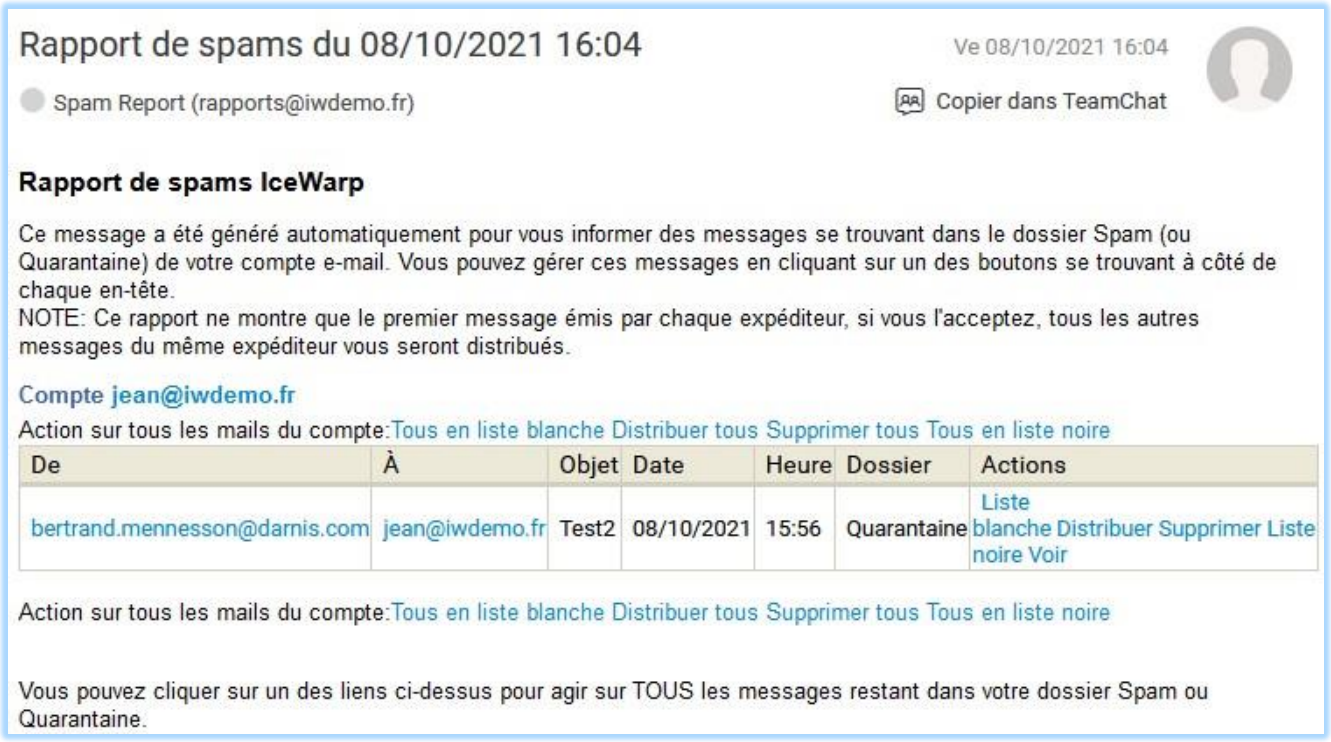
Rapport de Quarantaine

Comme décrit à précédemment, le destinataire du message 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.

Ce rapport est très utile pour les clients de messagerie autre que le Client Web car ils n'ont pas accès au dossier Quarantaine.



Rapport de spams du 08/10/2021 16:04

Ve 08/10/2021 16:04

Spam Report (rapports@iwdemo.fr)

Copier dans TeamChat

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 à côté de chaque en-tête.
NOTE: Ce rapport ne montre que le premier message émis par chaque expéditeur, si vous l'acceptez, tous les autres messages du même expéditeur vous seront distribués.

Compte jean@iwdemo.fr

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

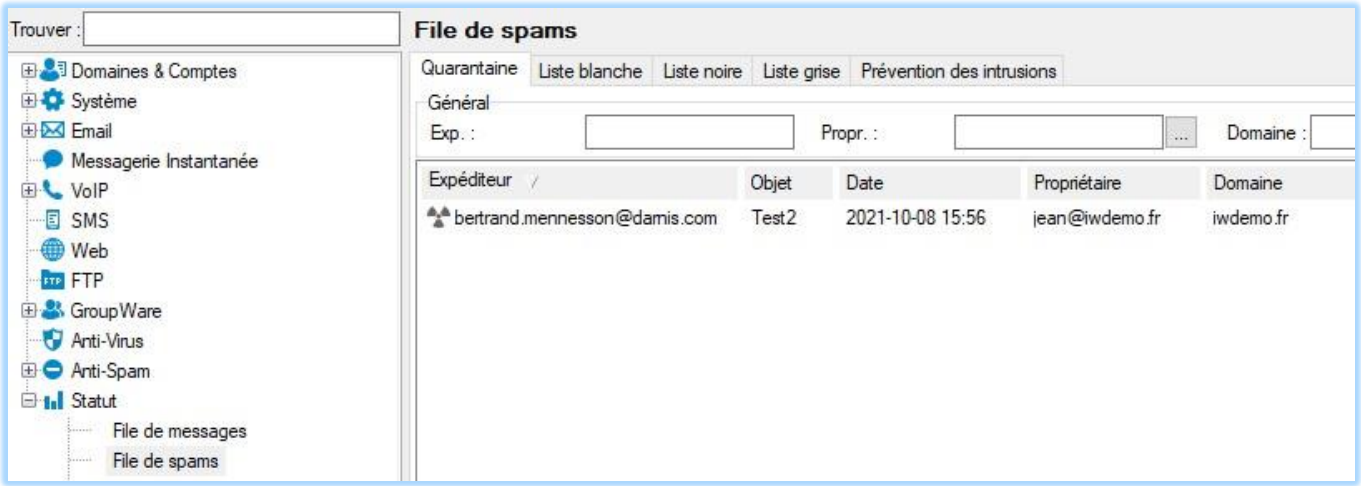
De	À	Objet	Date	Heure	Dossier	Actions
bertrand.mennesson@darnis.com	jean@iwdemo.fr	Test2	08/10/2021	15:56	Quarantaine	Liste blanche Distribuer Supprimer Liste noire Voir

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

Vous pouvez cliquer sur un des liens ci-dessus pour agir sur TOUS les messages restant dans votre dossier Spam ou Quarantaine.

Traitement pas l'administrateur du serveur

La console d'administration de IceWarp (ou la console **WebAdmin**) 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 délivrer (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 Quarantaine).

Le sort du message dépend de l'option "**Après ce délai, avant de les supprimer, distribuer les messages en les considérant comme Spam**" :

- 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.

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 du Défi 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.

Prévention des Défis factices

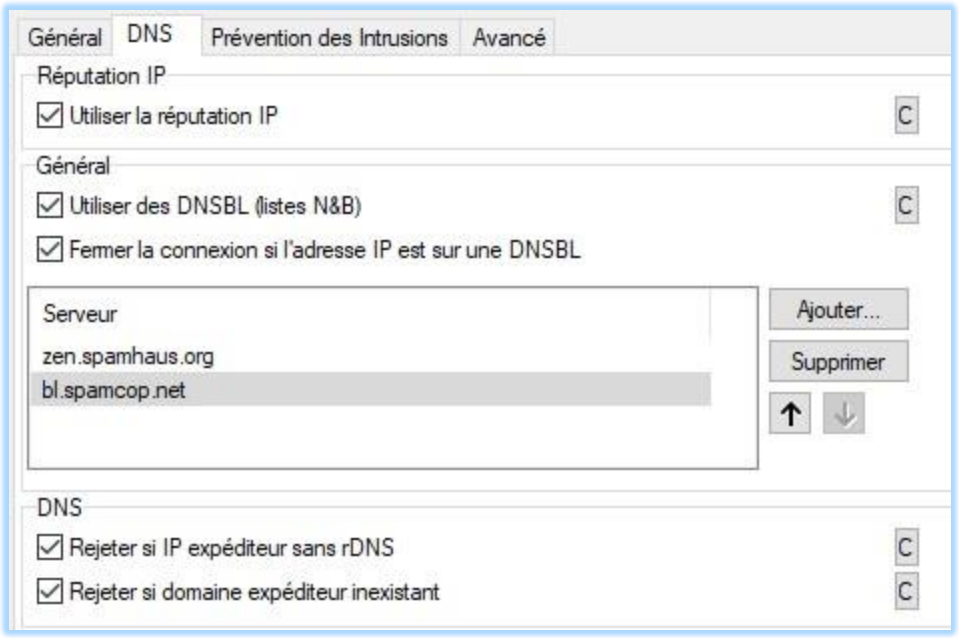
Comme indiqué au début de ce document, le mécanisme de Défi peut être considéré comme nocif pour le réseau Internet car il envoie un message à tous les expéditeurs présumés (From:) sans être certain qu'ils sont les vrais expéditeurs.

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.

Pour plus détails, consulter le Guide de Sécurité.

Les listes noires des DNS

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

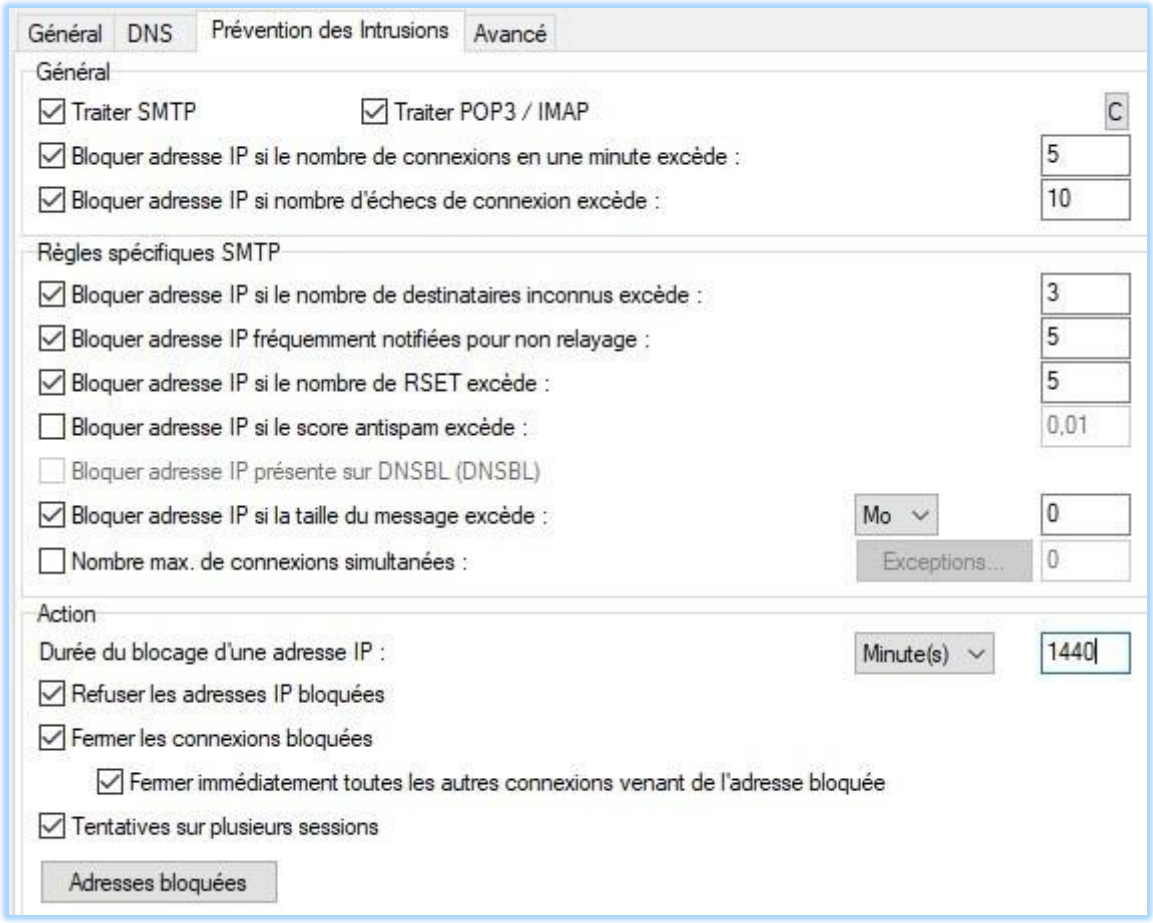


Ce mécanisme est très efficace, il fait appel à des serveurs externes qui listent les émetteurs de messages douteux (zen.spamhaus.org...).

Il peut être contourné ponctuellement (bouton C)

La Prévention des intrusions

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

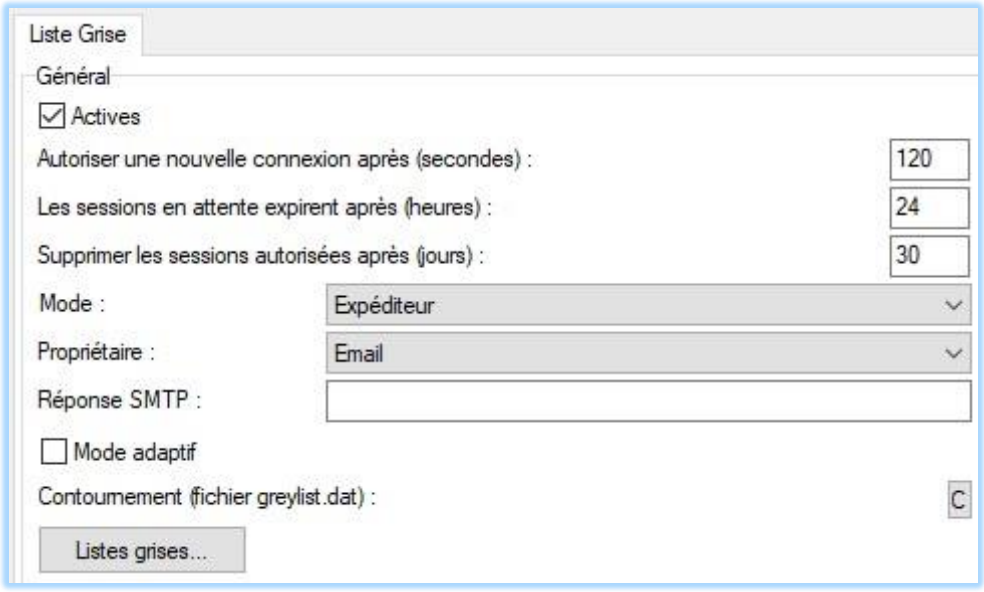


Ce mécanisme détecte certains comportements anormaux et bloque les adresses IP correspondantes.

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)