

Filtrage des connexions avec Exchange 2003

Rédacteur : Eric Drezet
Administrateur réseau
CNRS-CRHEA – 07/2004
Groupe Admin06



But du papier : Filtrer les messages entrants au niveau du serveur Exchange à l'aide d'une black list.

Préalable : Disposer d'un serveur Exchange 2003.

Liens :

Une liste de blocage gratuite sur Internet
<http://www.spamhaus.org/>

Procédure :

En complément des règles de filtrage installées sur les clients Outlook (voir les papiers : Filtrage des spams.pdf, Importation de règles de filtrage.pdf, Modification de règles de filtrage.pdf, Exportation de règles de filtrage.pdf), Exchange 2003 nous permet de mettre en place un système de rejet des mails non sollicités à l'aide d'une black list. Nous en avons choisi une gratuite sur Internet sur spamhaus.org.

Note : Si vous utilisez un fournisseur de listes d'interdiction, lorsque des messages électroniques sont envoyés à votre organisation, la règle de filtrage des connexions contacte la liste d'interdiction du fournisseur et celui-ci recherche l'adresse IP du serveur se connectant. Si l'adresse IP est trouvée dans la liste, le fournisseur de listes d'interdiction retourne une adresse IP indiquant que l'expéditeur est bloqué. Si l'adresse IP de l'expéditeur ne figure pas dans la liste, le fournisseur de listes d'interdiction retourne un message hôte introuvable.

Tout d'abord, lancez le Gestionnaire système Exchange. Dans l'arborescence de gauche, sélectionnez l'objet « Remise des messages » (cf. figure 1).

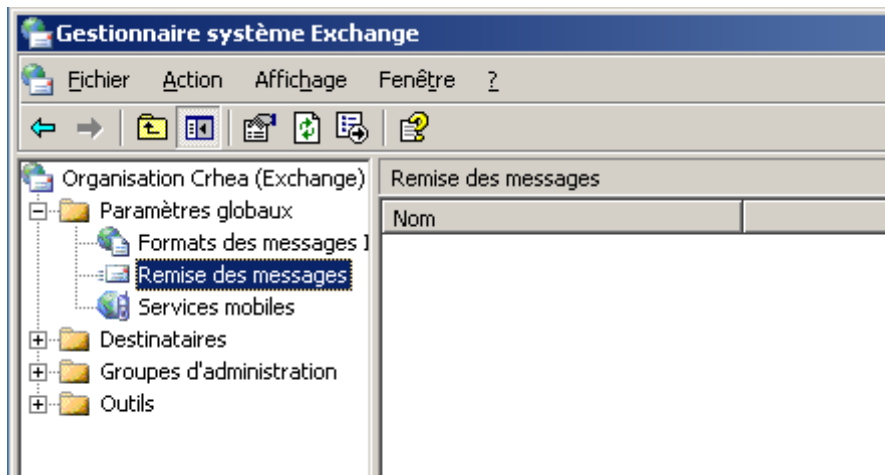


Figure 1 : Remise des messages

Cliquez ensuite sur le bouton droit de la souris et sélectionnez « Propriétés » dans le menu déroulant. La fenêtre « Propriétés de remise des messages » s'affiche (cf. figure 2). Sélectionnez l'onglet « Filtrage des connexions ».

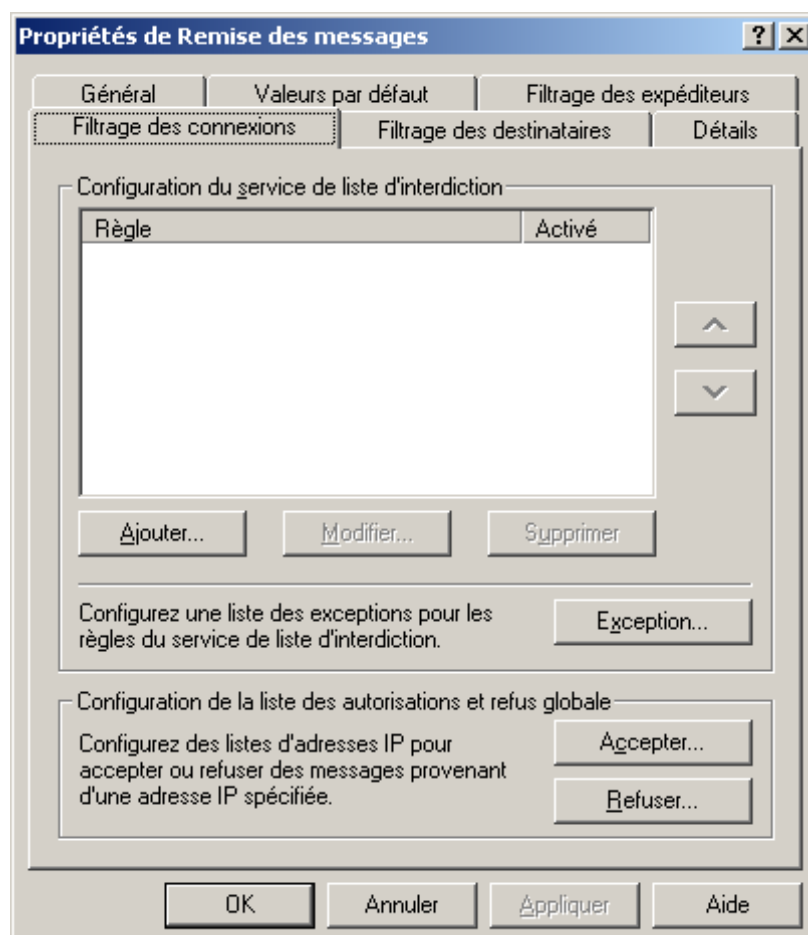


Figure 2 : L'onglet « Filtrage des connexions »

Sous la liste de règles, cliquez sur le bouton « Ajouter... ». La fenêtre « Règle de filtrage de connexion » s'affiche. Dans le champ « Nom affiché », tapez le nom de

vosre règle (SBL+XBLDN dans notre exemple, soit la combinaison des deux règles proposées par l'éditeur pour traquer les spams, les proxies, vers, trojan,...). Dans la zone « Suffixe DNS du fournisseur » tapez l'adresse Internet de la « Spamhaus Block List » (liste noire des sites réputés spammeurs). Cliquez sur le bouton « Renvoyer le code d'état... » pour spécifier la valeur renvoyée selon la règle de filtrage.

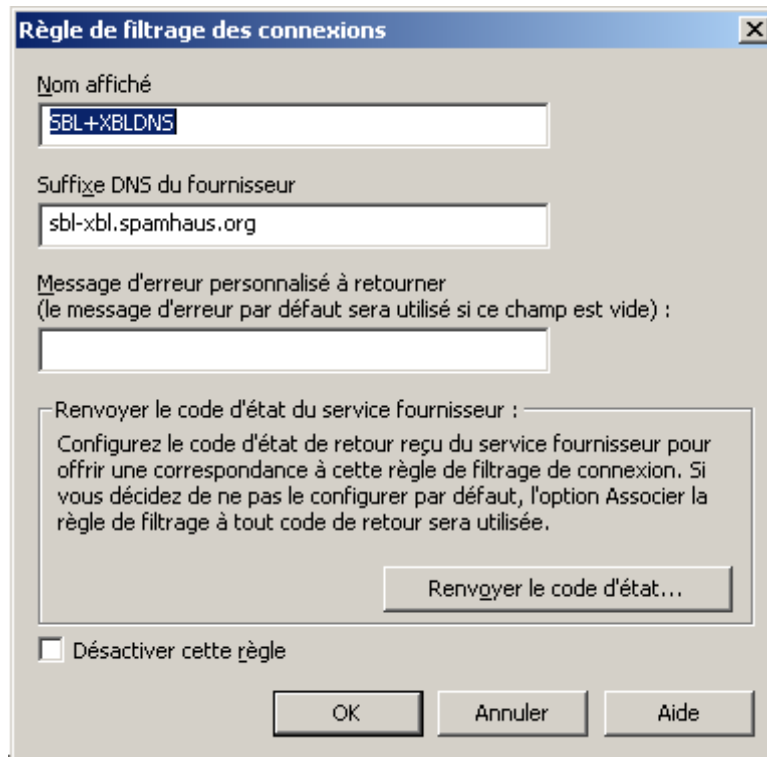


Figure 3 : Définition de la règle de filtrage

Cliquez sur le bouton radio « Associer la règle de filtrage à l'une des réponses suivantes : » et entrez la valeur donnée par le fournisseur de la liste de blocage. Dans notre exemple, les valeurs à saisir vont de 127.0.0.2 à 127.0.0.6 (cf. figure 4).

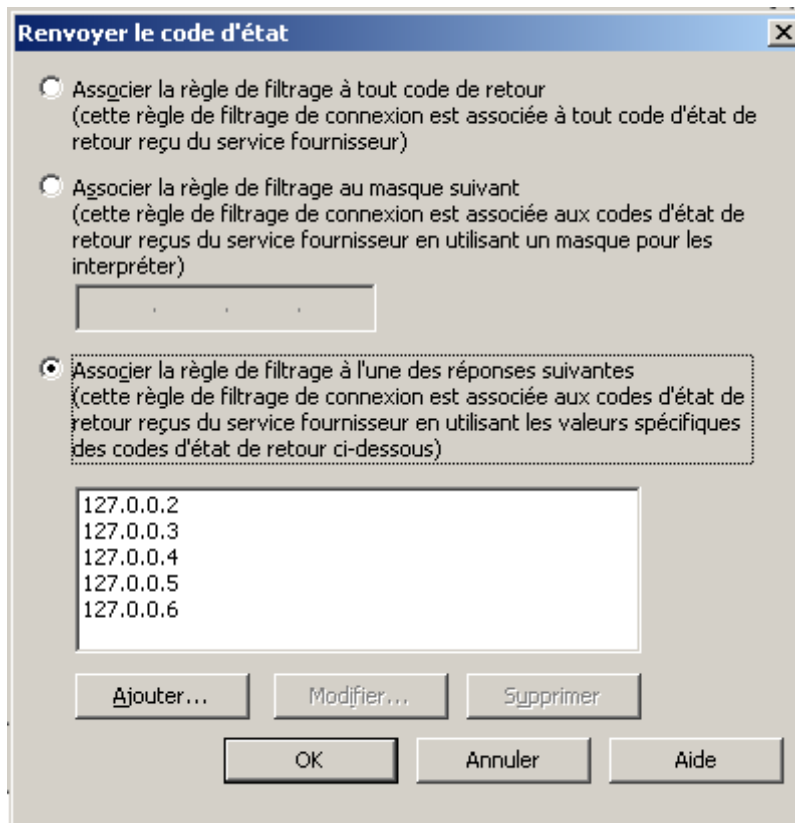


Figure 4 : Saisie de la valeur de retour

Dans la fenêtre « Propriétés de remise des messages », on voit maintenant apparaître le nom de la règle mais la colonne « Activé » affiche « Non ». Pour activer ce filtrage, vous devez sélectionner le serveur virtuel SMTP sur lequel vous voulez appliquer la règle de filtrage (cf. figure 5).

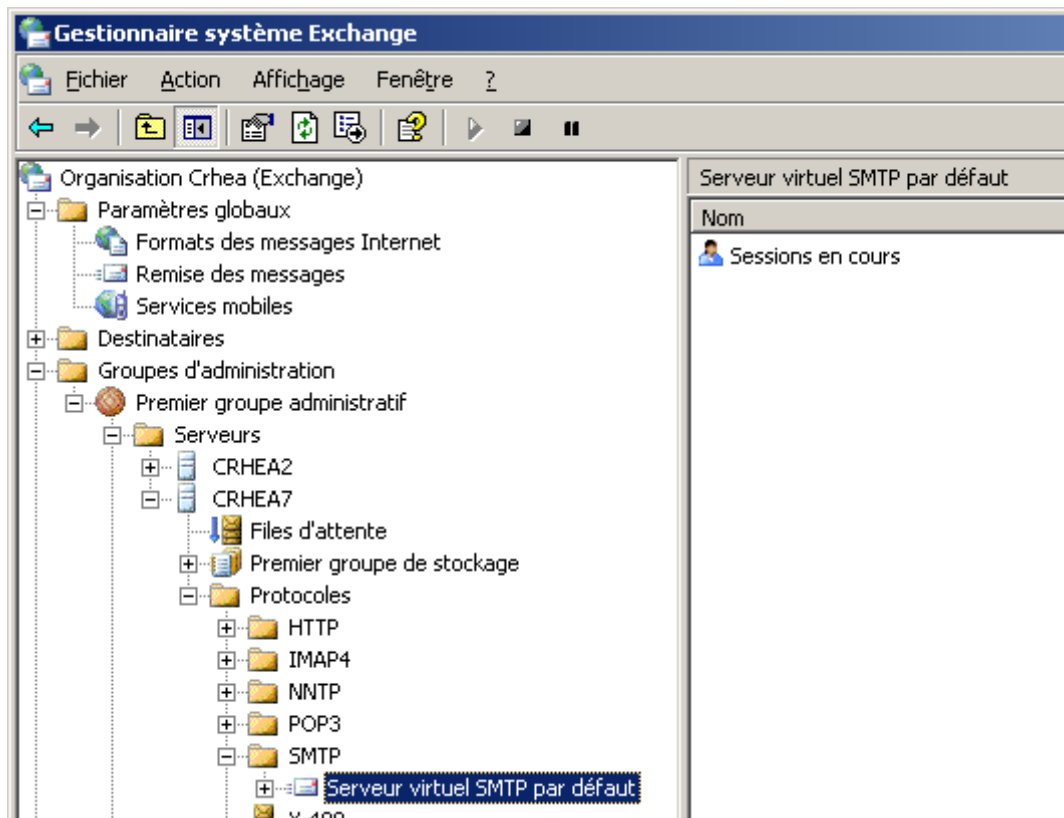


Figure 5 : Sélection du serveur virtuel SMTP

Dans la fenêtre des « Propriétés du serveur virtuel SMTP », cliquez sur le bouton « Options avancées... » (cf. figure 6).

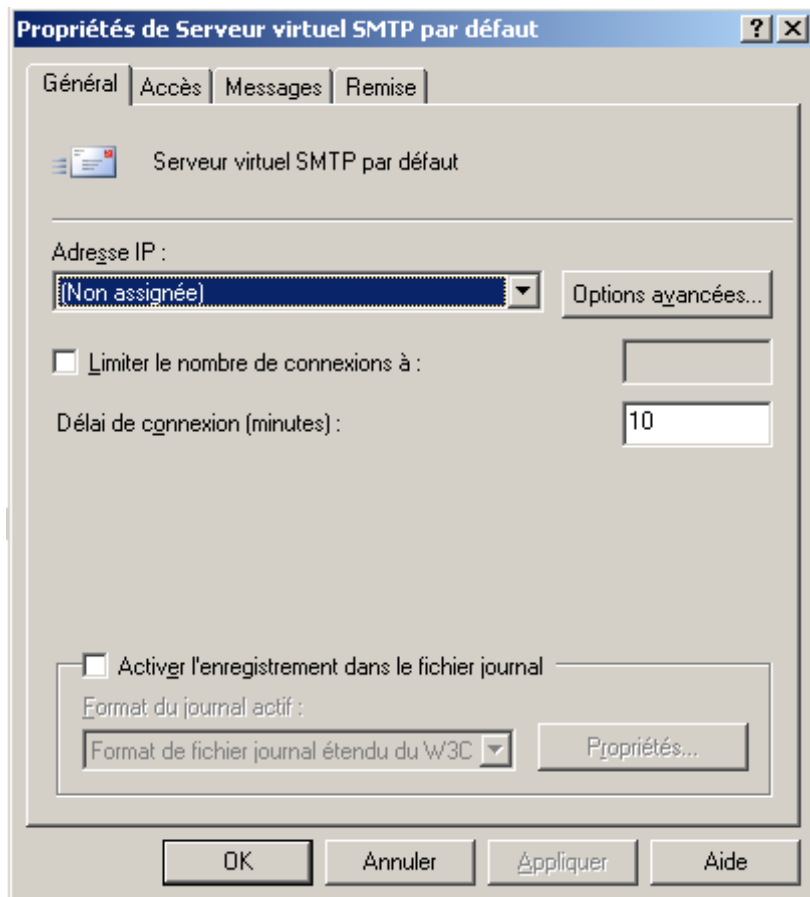


Figure 6 : Modification des options avancées

Cliquez dans la case à cocher « Appliquer le filtre de connexion » (cf. figure 7).

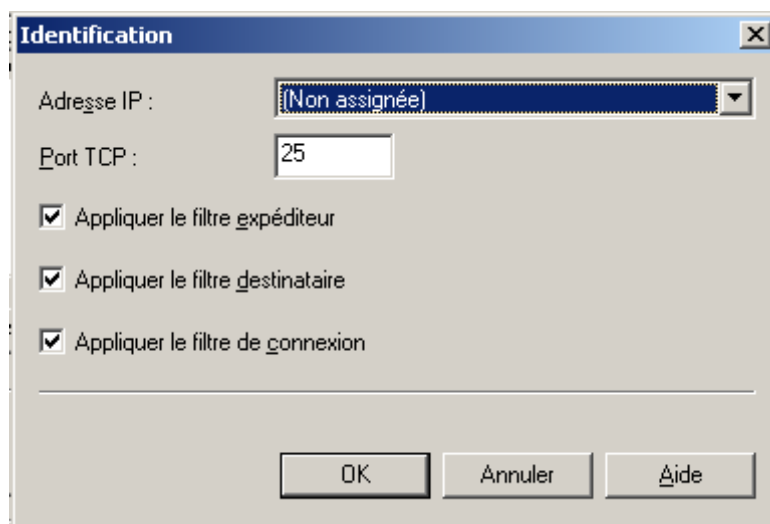


Figure 7 : Application du filtre de connexion

Dans la fenêtre « Propriétés de remise des messages », on voit maintenant en face du nom de la règle, la colonne « Activé » affiche « Non ».