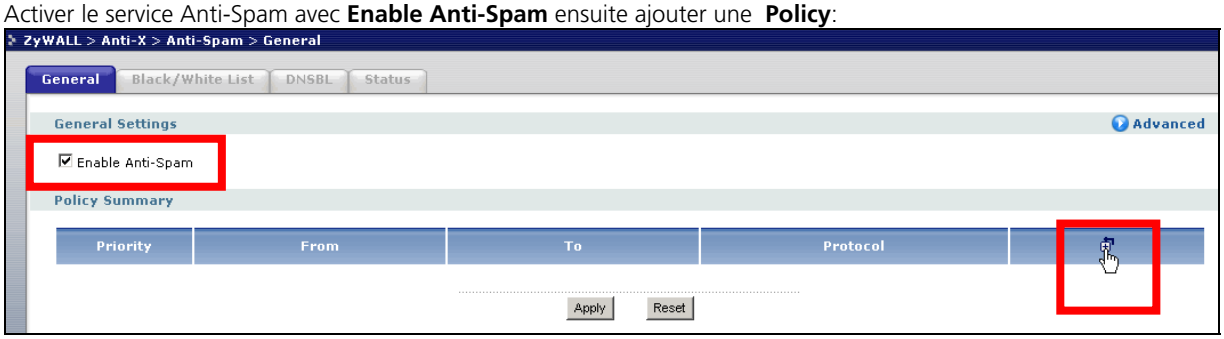
AntiSpam avec le ZyXEL USG 100 et 200

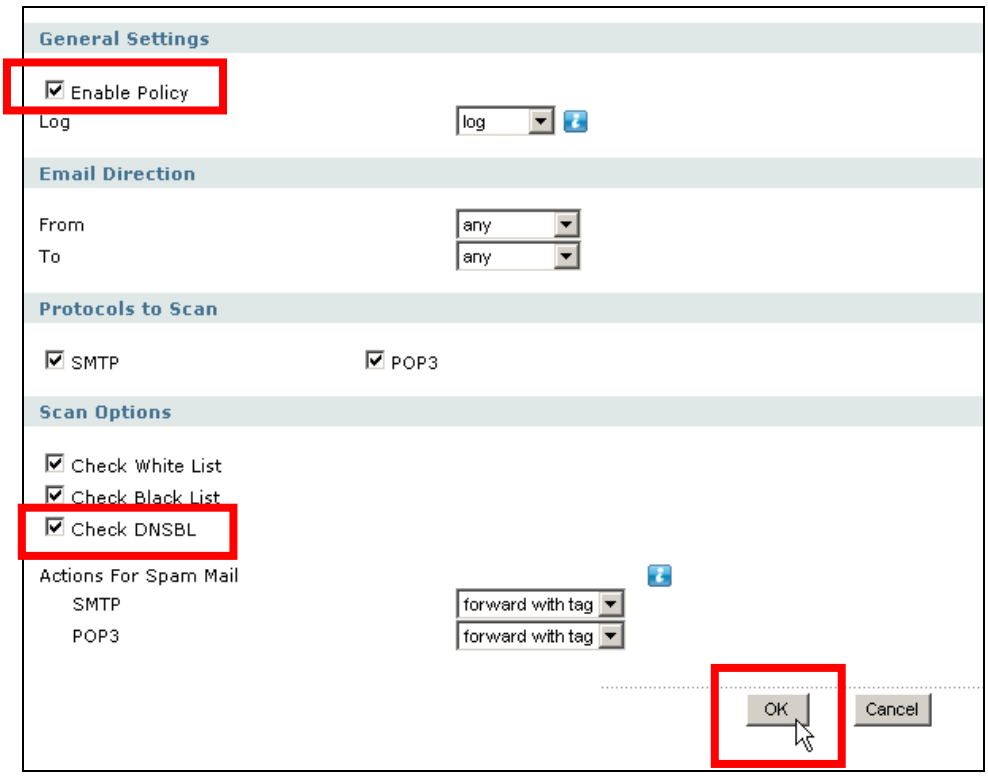
Cet exemple démontre la préparation pour la configuration de la fonction "AntiSpam" du Par-feu USG en utilisant la nouvelle fonction DNSBL (DNS-based Blackhole List) et les entrées manuelles des listes de contrôle "Black" et "Withe" listes. Le Service DNSBL Anti-Spam est gratuit, l'achat d'une licence n'est pas nécessaire. Pour plus d'informations sur le DNSBL consulté le URL: http://en.wikipedia.org/wiki/DNSBL.

Menu **Anti-X / Anti-Spam**:

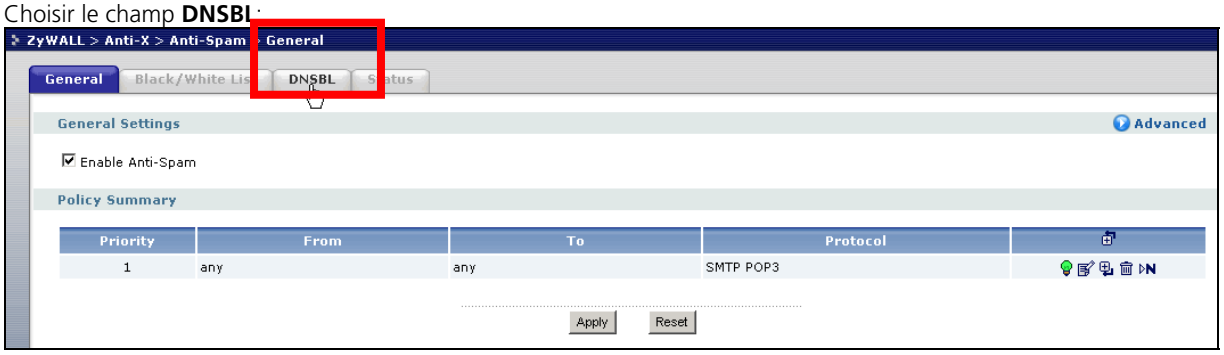
Activer le service Anti-Spam avec **Enable Anti-Spam** ensuite ajouter une **Policy**:



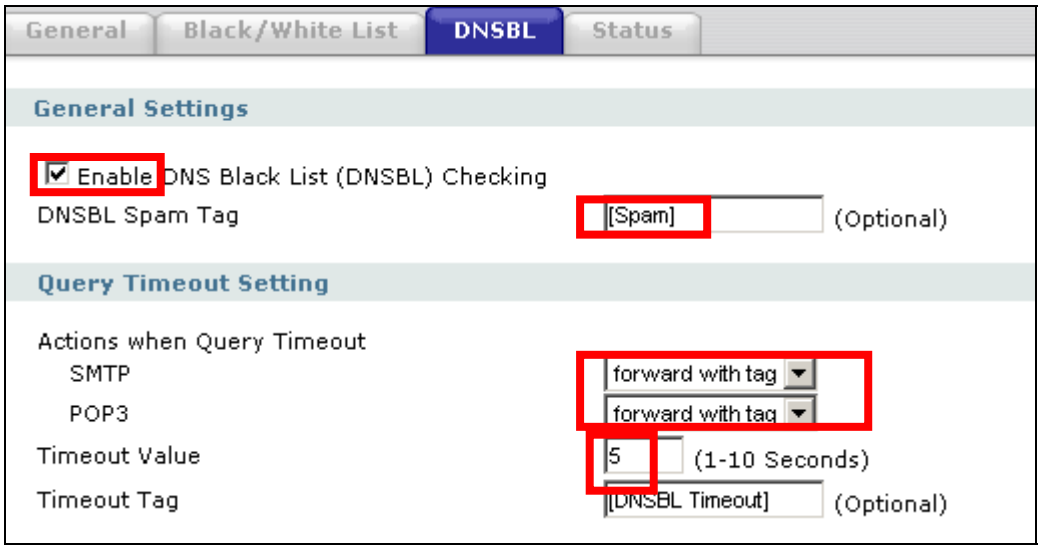
Activer la Policy avec **Enable Policy:**
Log: les entrées Spam seront ajoutés dans le Log.
From: Control depuis la Zone (any = toutes les Zones) ou bien choisir une zone (LAN1, WAN1,WLAN, DMZ, ...).
To: Zone de cible (any = touts les zones)) ou bien choisir une zone (LAN1, DMZ, WAN1, WAN2, ...).
Protocols to Scan: Choisir le Protocol qui sera contrôlé (SMTP = Mail envoyé, POP3 = Mail reçus).
Actions for Spam Mail: les Mails seront retransmises (forward), retransmises avec marquage (forward with tag, ou bien rejetés (drop).



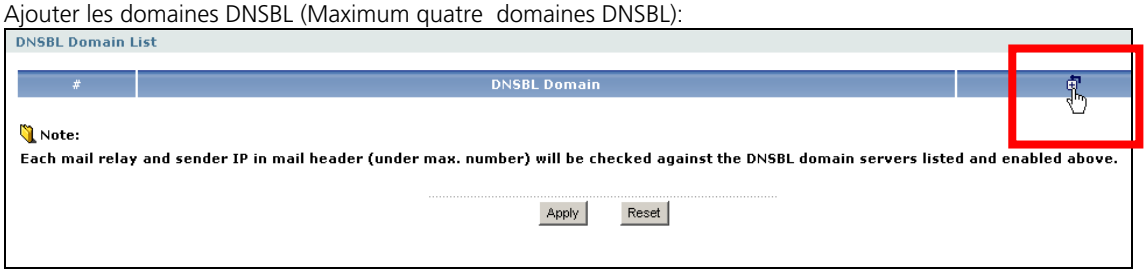
Choisir le champ **DNSBL**:



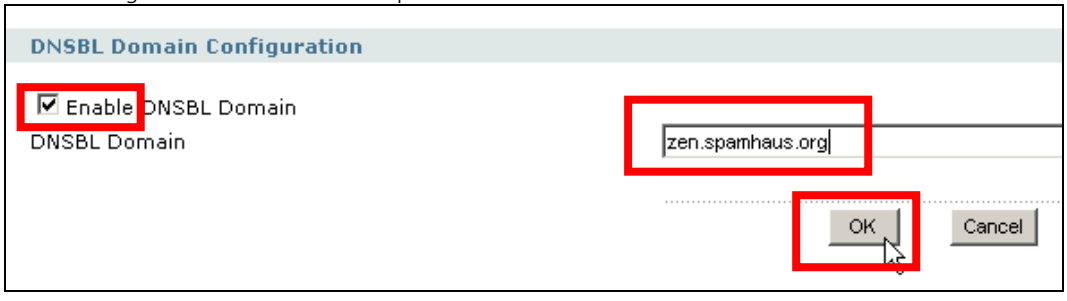
Activer le DNSBL avec **Enable** et éditer si vous le souhaité le texte de marquage (**DNSBL Spam Tag**) **Actions when Query Timeout** (pas de réponse dans un elapse de temps de x Sekunden): Les Mails avec Spam les Mails seront retransmises (forward), retransmises avec marquage (forward with tag, ou bien rejetés (drop). Timeout (default est de 5 secondes) éditer ce temps si vous le souhaité:



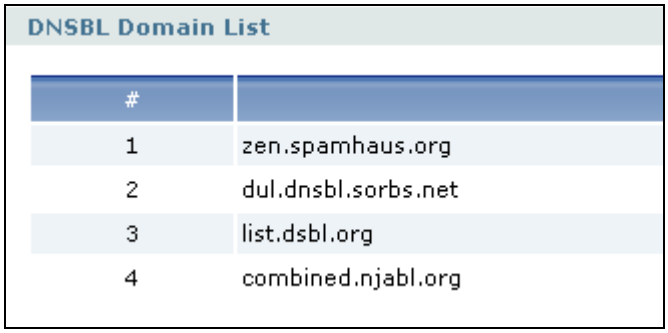
Ajouter les domaines DNSBL (Maximum quatre domaines DNSBL):



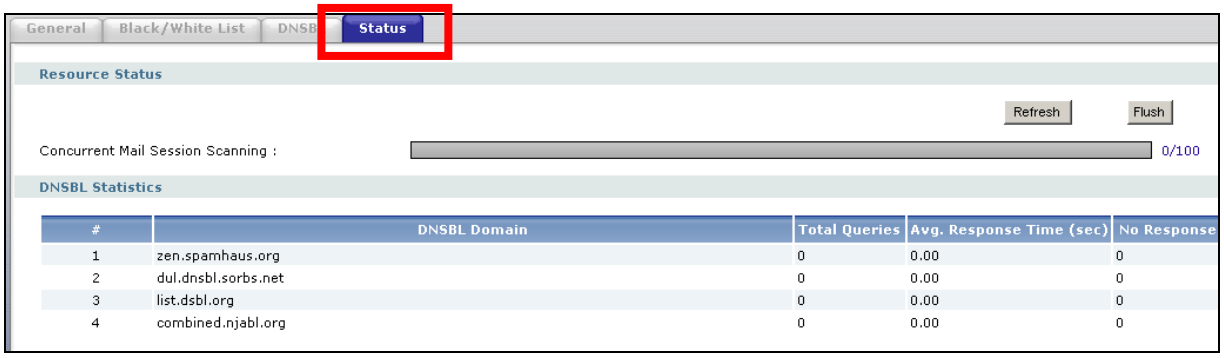
Activer la règle avec **Enable** ensuite taper le nom du domaine DNSBL:



Voici une liste de quatre domaines conseillés par Zyxel vous pouvez placer d'autre domaines en consultant le URL: http://spamlinks.net/filter-dnsbl-lists.htm



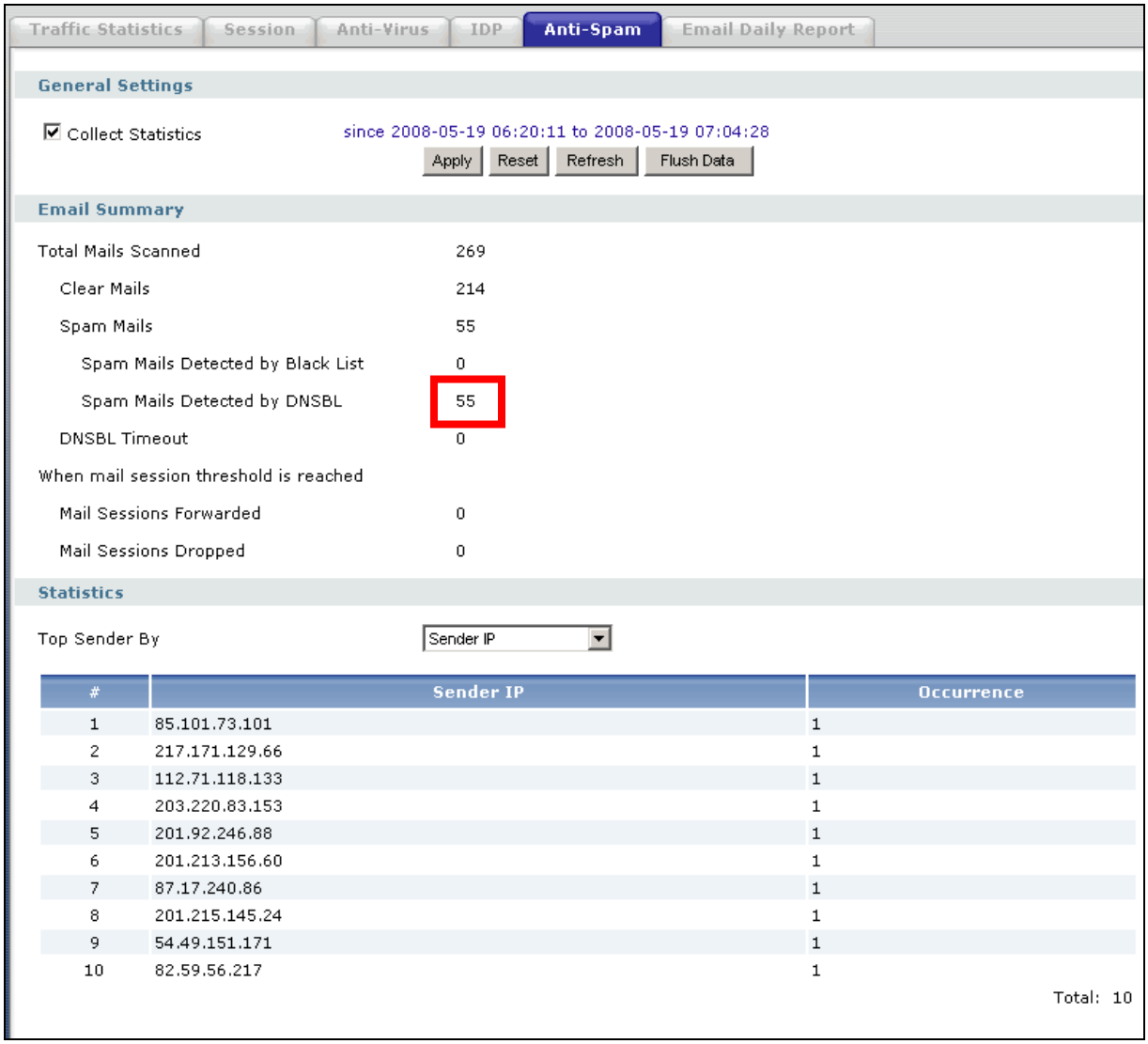
Via le **Status** vous pouvez consulter les demandes vers les domaines, le temps de réponse et les timeout de chaque domaine, de cette manière vous pouvez décider si un domaine ne convient pas à votre localité :



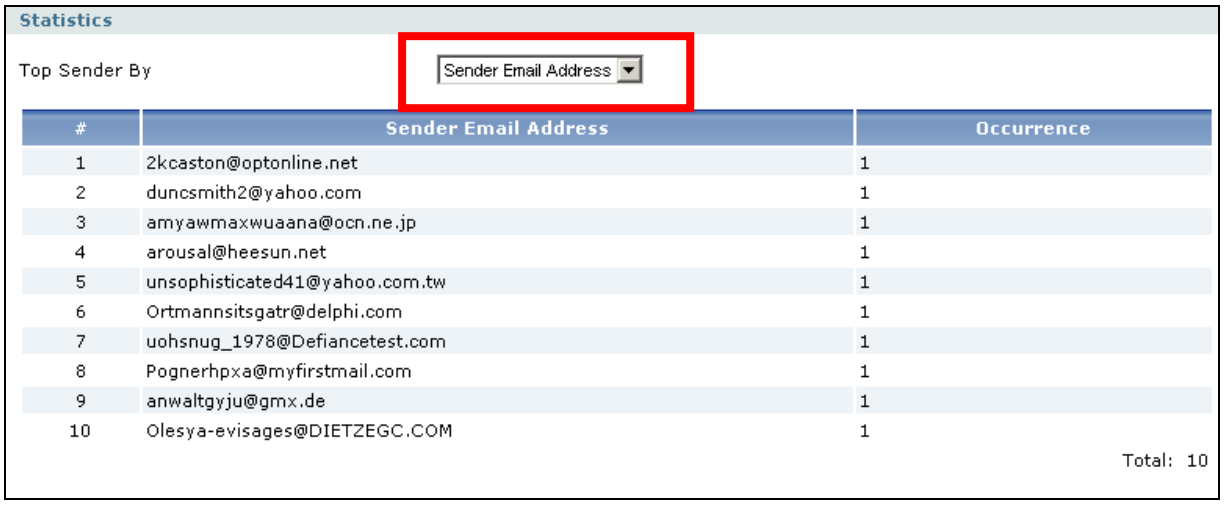
Activer le Report pour la Fonction Anti-Spam par le menu **Maintenance / Report:**

Choisir le champ **Anti-Spam**. Activer la coche **Collect Statistics** puis cliquer sur **Apply** afin de sauvegarder la configuration:

Exemple d'une statistique Anti-Spam, ici l'USG a détecté 55 Spam Mails:

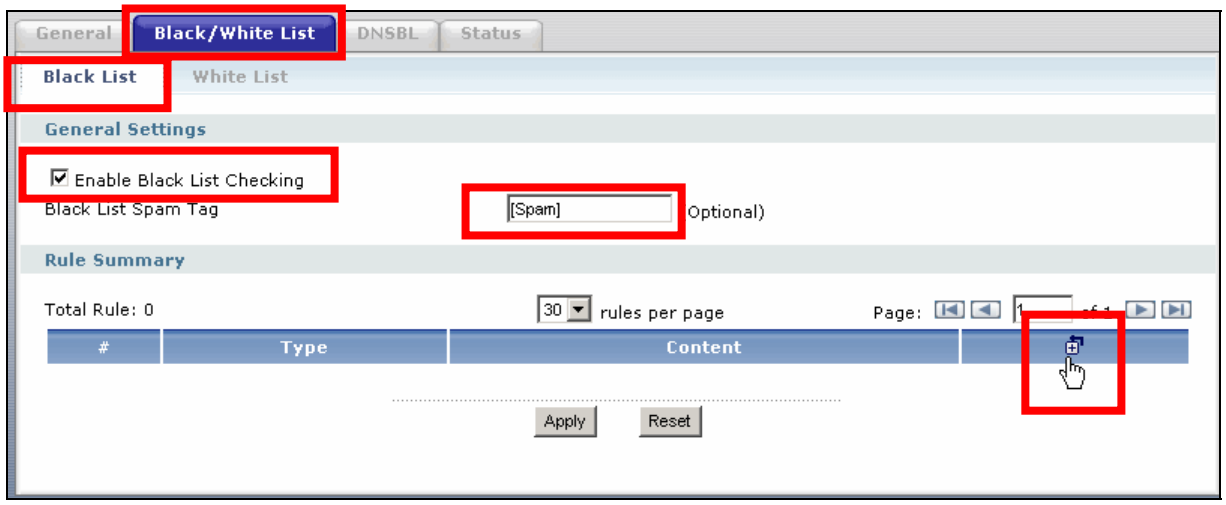


Indications des **Sender Email Address** au lieu des **Sender IP** est aussi possible:

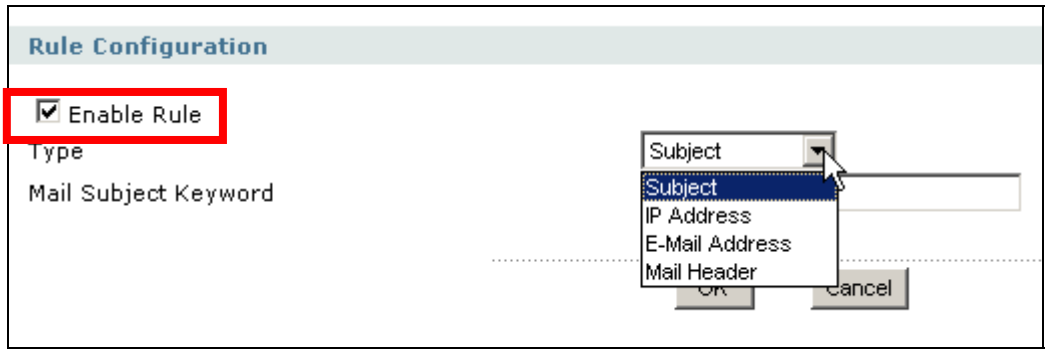


Via la fonction **Black List** les Mails avec un certain critère (Subjekt, IP Adresse, E-mal, Domaine, Header) seront marqués comme SPAM.

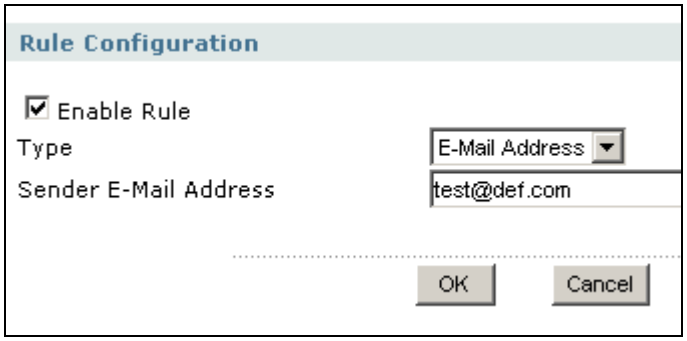
Choisir le champ **Black/White List** ensuite le champ **Black List,** activer la fonction avec **Enable**, changer la définition du marquage (Black List Spam Tag) si vous le souhaité et pour finir ajouter une règle:



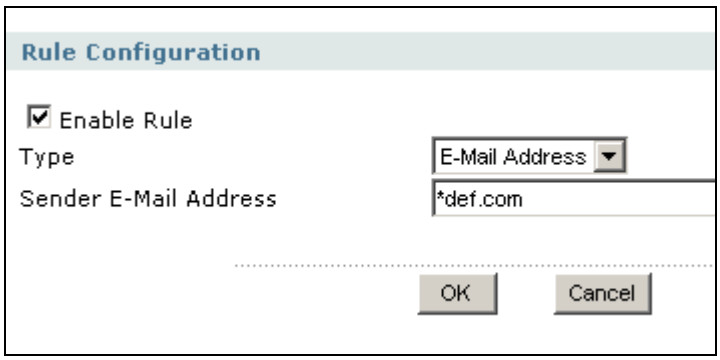
Activer la règle avec **Enable** et choisir une option Keyword (critère) :



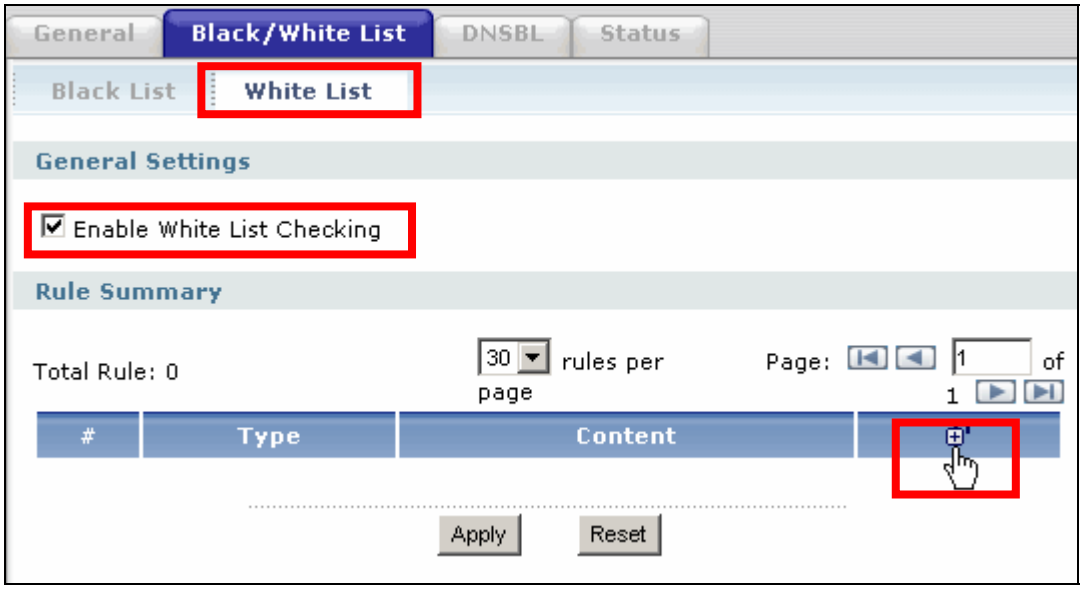
Activer la règle avec **Enable**.
Par exemple le Type E-Mail Adresse l'adresse est **test@def.com**, toutes les Mails de cet envoyeur seront marqués comme SPAM:



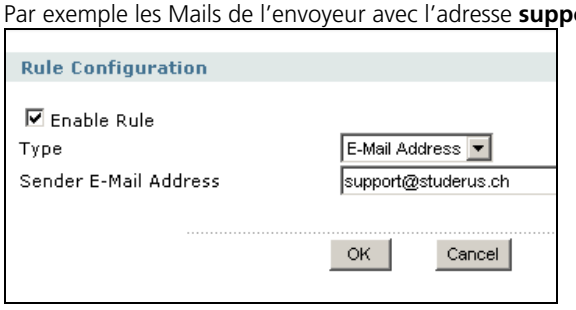
Ou bien toutes les Mails du domaine **def.com** seront aussi marqués comme SPAM:



White List, au contraire de la Black List les Mails avec un certain critère ne seront pas marqués comme SPAM, utiliser cette fonction pour les Mails désignés comme **false/positive** Mails qui seront reconnus comme SPAM:



Par exemple les Mails de l'envoyeur avec l'adresse **support@studerus.ch** ne seront pas marqués comme SPAM:



Ou toutes les Mails avec le sujet **zyxel:**