

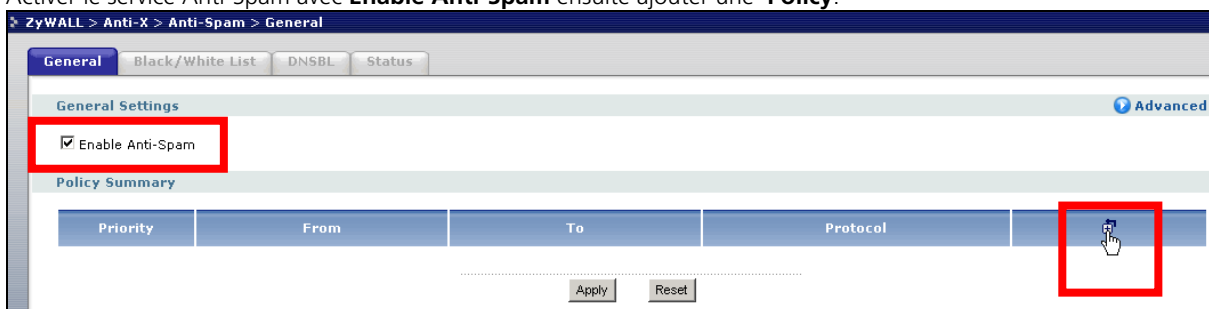
AntiSpam avec le ZyXEL USG 100 et 200

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 "White" listes. Le Service DNSBL Anti-Spam est gratuit, l'achat d'une licence n'est pas nécessaire. Pour plus d'informations sur le DNSBL consultez 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**:

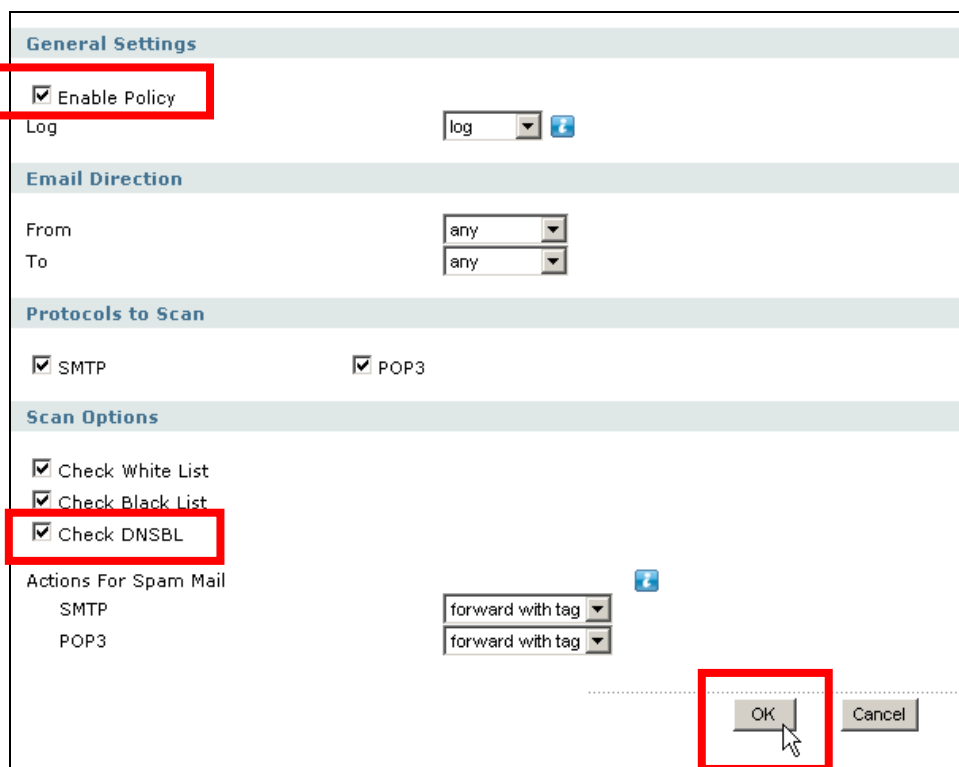
Log: les entrées Spam seront ajoutés dans le Log.

From: Control depuis la Zone (any = toutes les Zones) ou bien choisir une zone (LAN1, WAN1,WLAN, DMZ, ...).

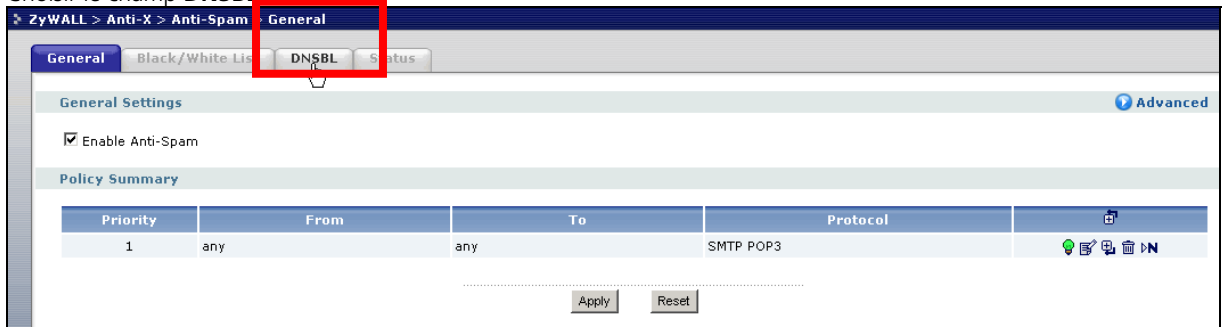
To: Zone de cible (any = tous les zones)) ou bien choisir une zone (LAN1, DMZ, WAN1, WAN2, ...).

Protocols to Scan: Choisir le Protocol qui sera contrôlé (SMTP = Mail envoyé, POP3 = Mail reçus).

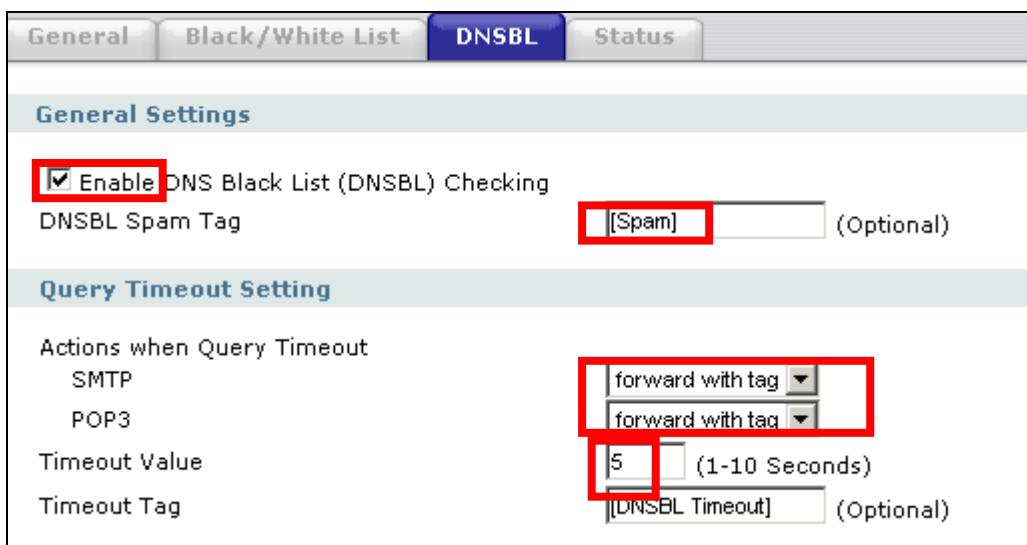
Actions for Spam Mail: les Mails seront retransmises (forward), retransmises avec marquage (forward with tag, ou bien rejetés (drop).



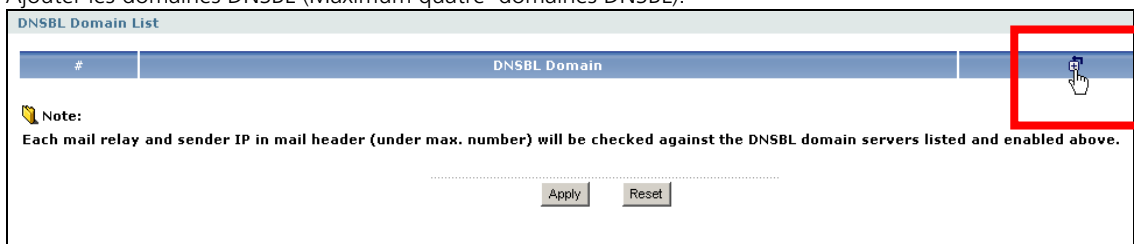
Choisir le champ **DNSBL**:



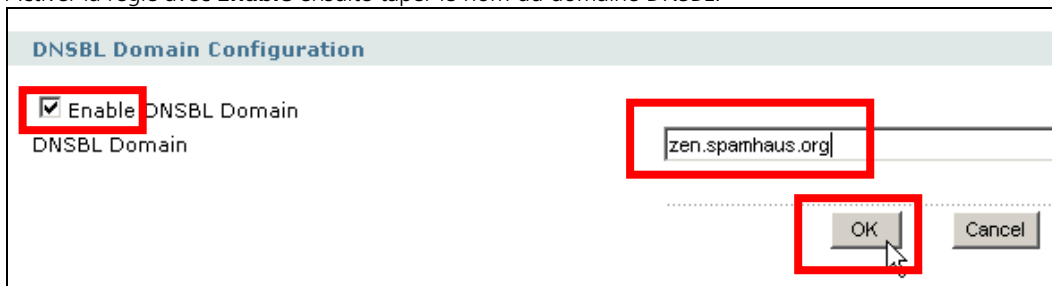
Activer le DNSBL avec **Enable** et éditer si vous le souhaitez le texte de marquage (**DNSBL Spam Tag**) **Actions when Query Timeout** (pas de réponse dans un elapse de temps de x Sekunden): Les Mails avec Spam les Mails seront retransmises (forward), retransmises avec marquage (forward with tag),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



Ajouter les domaines DNSBL (Maximum quatre domaines DNSBL):



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



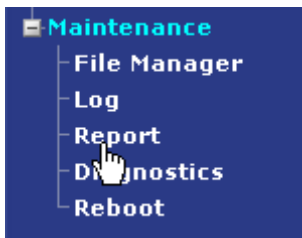
Voici une liste de quatre domaines conseillés par ZyXel vous pouvez placer d'autres domaines en consultant le URL: <http://spamlinks.net/filter-dnsbl-lists.htm>

DNSBL Domain List	
#	
1	zen.spamhaus.org
2	dul.dnsbl.sorbs.net
3	list.dsbl.org
4	combined.njabl.org

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 :

#	DNSBL Domain	Total Queries	Avg. Response Time (sec)	No Response
1	zen.spamhaus.org	0	0.00	0
2	dul.dnsbl.sorbs.net	0	0.00	0
3	list.dsbl.org	0	0.00	0
4	combined.njabl.org	0	0.00	0

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:

Traffic Statistics Session Anti-Virus IDP **Anti-Spam** Email Daily Report

General Settings

Collect Statistics since 2008-05-19 06:20:11 to 2008-05-19 07:04:28

Apply Reset Refresh Flush Data

Email Summary

Total Mails Scanned	269
Clear Mails	214
Spam Mails	55
Spam Mails Detected by Black List	0
Spam Mails Detected by DNSBL	55
DNSBL Timeout	0
When mail session threshold is reached	
Mail Sessions Forwarded	0
Mail Sessions Dropped	0

Statistics

Top Sender By Sender IP

#	Sender IP	Occurrence
1	85.101.73.101	1
2	217.171.129.66	1
3	112.71.118.133	1
4	203.220.83.153	1
5	201.92.246.88	1
6	201.213.156.60	1
7	87.17.240.86	1
8	201.215.145.24	1
9	54.49.151.171	1
10	82.59.56.217	1

Total: 10

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

Statistics

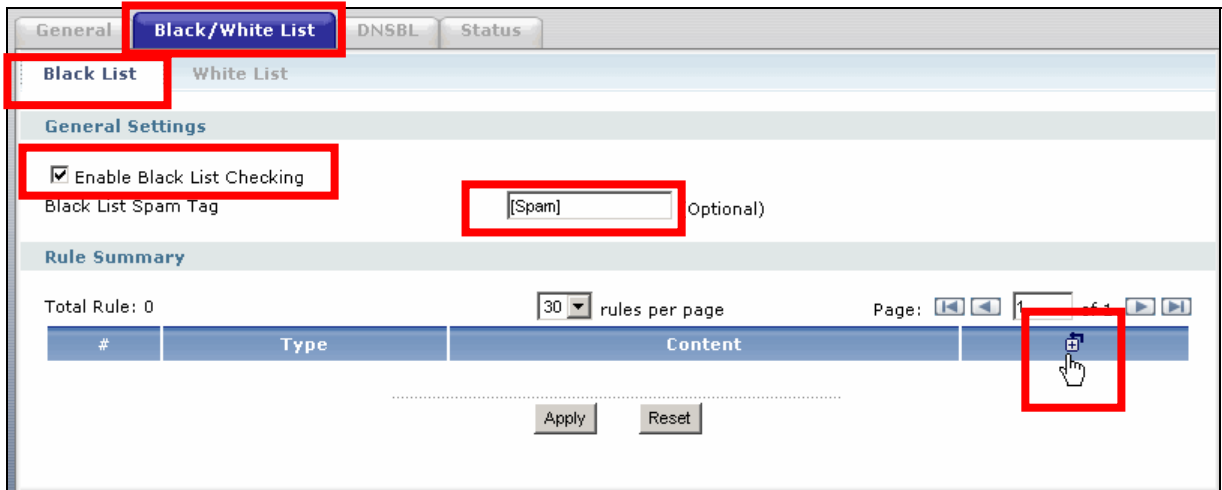
Top Sender By Sender Email Address

#	Sender Email Address	Occurrence
1	2kcaston@optonline.net	1
2	duncsmith2@yahoo.com	1
3	amyawmaxwuaana@ocn.ne.jp	1
4	arousal@heesun.net	1
5	unsophisticated41@yahoo.com.tw	1
6	Ortmannsitsgatr@delphi.com	1
7	uohsnug_1978@Defiancetest.com	1
8	Pognerhpxa@myfirstmail.com	1
9	anwaltgyju@gmx.de	1
10	Olesya-evisages@DIETZEGC.COM	1

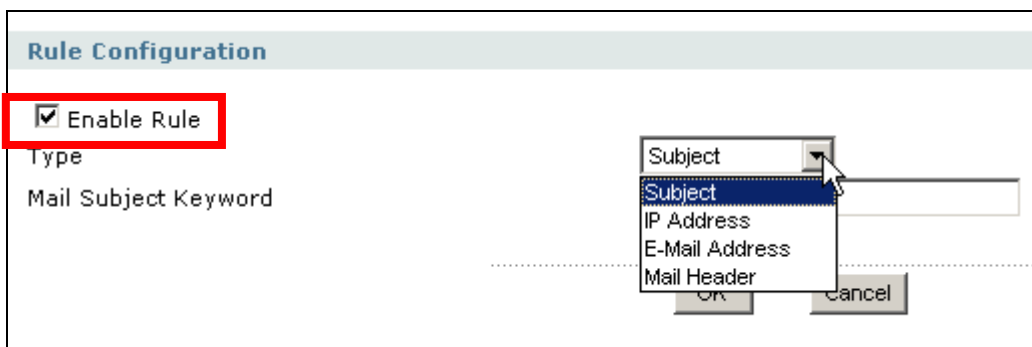
Total: 10

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 souhaitez et pour finir ajouter une règle:

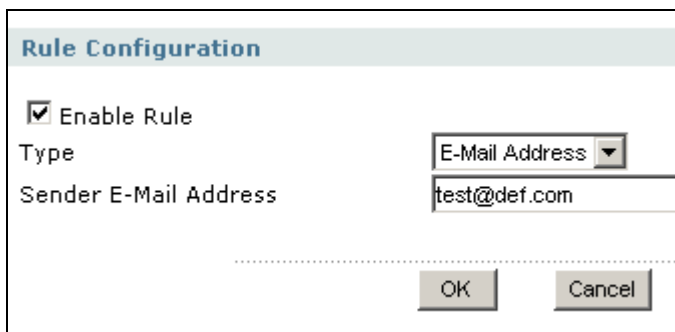


Activer la règle avec **Enable** et choisir une option Keyword (critère) :



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:

Rule Configuration

Enable Rule

Type: E-Mail Address

Sender E-Mail Address:

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:

Black/White List

Black List **White List** DNSBL Status

Enable White List Checking

Rule Summary

Total Rule: 0 30 rules per page Page: 1 of 1

#	Type	Content	
			<input type="button" value="+"/>

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

Rule Configuration

Enable Rule

Type: E-Mail Address

Sender E-Mail Address:

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

Rule Configuration

Enable Rule

Type: Subject

Mail Subject Keyword: