How to Configure the Spam Filter Service

https://campus.barracuda.com/doc/73719348/

This article provides instructions on how to configure the SPAM Filter service. It also provides an overview of the service settings.

Before You Begin

Before configuring the SPAM Filter service, verify that it is properly created. For more information, see How to Configure Services.

Configure the SPAM Filter Service Settings

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > SPAM-Filter > SPAM Filter Settings**.
2. Click **Lock**.
3. In the **Spamfilter Settings** section, configure the spam filter settings. For more information see **Spamfilter Settings** section below..
4. Click **Send Changes** and **Activate**.

Configure Advanced Network Settings

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > SPAM-Filter > SPAM Filter Settings**.
2. In the left menu, select **Advanced Network Settings**.
3. Click **Lock**.
4. Edit the following settings:

Setting	Description
Listening Port	The listening port for the SPAM Filter service.
IPs allowed to Connect (ACL)	In this table, add the IP addresses of the clients that are allowed to connect to the SPAM Filter service. By default, *127.0.0.1* is included in this table. It specifies the internal loopback interface of the Barracuda CloudGen Firewall. This interface must be used when the mail gateway and spam filter reside on the same system.

5. Click **Send Changes** and **Activate**.

Spamfilter Settings

Setting	Description
Text To Insert Into Subject	The text that is placed in the subject of an email that is classified as spam. If this field is left empty, the subject of the email is not altered.
SPAM Mail Modification	Specifies how spam emails are modified. You can select the following options: • *only_add_tags (default)* – Adds SPAM tags into the mail header but does not alter the mail body. • *as_attachment* – Adds a verbose SPAM report into the mail body and appends the actual email as attachment. • *as_attachment_text* – Adds a verbose SPAM report into the mail body and appends the actual email as a text attachment.
Report Language	The language in which the SPAM report is written when it is added to the mail body (default: *English*). The report content is generated by SpamAssassin and cannot be customized. Note that report translations are not yet available completely for all configurable languages.
Threshold	A mail is classified as SPAM when its score exceeds the configured threshold. Increasing the threshold will increase the amount of SPAM missed, but will reduce the risk of false positives (default: *5*, medium: *7.5*, high: *10*, max.: *100*).
Maximum Children	The maximum number of concurrent spam filter servers. When the limit is reached, spam filtering is put on hold until a server is available.
Enable HA Sync	To synchronize spam filtering between an HA pair, select *yes*. The synchronization starts at 4:20 am. To schedule the synchronization at a different time, select *no* and create a cronjob for the required time interval (phionrcscleanup). Enter the following line for the cronjob: */opt/phion/modules/server/spamfilter/bin/hacron.sh SERVER SERVICE.* During the HA synchronization, the spam filter is deactivated.
WHITE AND BLACKLISTS	To edit the whitelists and blacklists, click **Set** or **Edit**. In the following tables, add the email addresses or domains of senders and recipients: • **Whitelist From** – List of senders whose mail should never be tagged as spam (regardless of an email's score). • **Whitelist To** – List of recipients whose mail should never be tagged as spam (regardless of an email's score). • **Blacklist From** – List of senders whose mail should always be tagged as spam. The whitelist is processed before the blacklist. As a result, you can block a domain while also allowing specific senders from it.

ONLINE TESTS	To specify the spam-tracking databases to be used by the SPAM filter service, click **Set** or **Edit**. You can select the following settings: • **Use DCC** – The Distributed Checksum Clearinghouse (DCC) does not list domain names or IP addresses but detects bulk mail messages by creating checksums. These checksums include values that are constant across common variations in bulk messages, including personalization. To use DCC, you must also enable Internet access on UDP port 6277. For more detailed information on DCC, see www.rhyolite.com/anti-spam/doc. • **Use Razor V2** – Razor detects spam by analyzing statistical and randomized signatures that spot mutating spam content. To use Razor V2, you must also enable Internet access on TCP port 2703. • **Use Pyzor** – Pyzor detects spam by calculating digests of email parts and comparing these with other recipient's emails. To use Pyzor, you must also enable Internet access on TCP port 80 and UDP port 24441. Pyzor uses a server list at http://pyzor.sourceforge.net/cgi-bin/inform-servers-0-3-x. If it cannot reach this list it uses its internal default server list. • **Skip RBL-Tests** – The Real-time Blackhole List (RBL) contains server IP addresses that are responsible for spam or are known to be hijacked for spamming. When this option is selected, the IP search in this list is deactivated. • **Use Black List Tests** – Checks for domain names in emails and compares these names against online blacklists, in order to detect messages sent by spammers. By enabling DNS blocklists (DNSBL) the SPAM Filter service uses external servers to verify if specific IP addresses or URIs have already been used by spammers. The usage policy of the external service surbl.org guarantees free use for organizations that have fewer than 1,000 users or scan fewer than 250,000 messages per day. If your organization exceeds either the number of email users or number of messages per day, do not enable DNSBL checks. To disable this function create a rule in section **RULES**, parameter **Rules**, with this contents: score URIBL_BLACK 0.
RULES	To configure rules that manually override specific testing sequences, click **Set** or **Edit**. To disable a given test set (such as one that is known to deliver incorrect results), set its score to *0*. For a complete list of available rules, see http://spamassassin.apache.org.
TRAINING OPTIONS	For more information, see How to Improve Spam Filtering.

Next Step

Continue with How to Improve Spam Filtering.