From SPAMfighter SMTP Anti Spam Server to SPAMfighter Mail Gateway

This guide will assist you in going from the SPAMfighter SMTP Anti Spam Server to the SPAMfighter Mail Gateway.

It is strongly advised that you read the SPAMfighter Mail Gateway User Manual before reading this guide – do not worry as most of it is pictures and can be skimmed through quickly.

In this guide the SPAMfighter SMTP Anti Spam Server will be referred to as "SMTP filter" and the SPAMfighter Mail Gateway will be referred to as "SMG".

Main differences between the SMTP filter and the SMG:

- The SMTP filter scan the emails as they pass through the filter to the mail server behind whereas the SMG receives the mails, filters them and only if they pass the tests set up will they be forwarded to the mail server behind. This means that the mail server will have much less activity with the SMG then with the SMTP filter.

- With the SMG you need only one IP address for incoming mail traffic, no matter how many mail servers it filters for, whereas with the SMTP filter you would need one for each mail server with its own IP behind the SMTP filter.

- The SMG have quarantine functionality. This meant that incoming emails which are filtered as spam can be saved for a time period, so the users can see and unblock the mail themselves if it has been erroneously blocked as spam.

- You now set up the mailboxes you want filtering for. This guarantees that you only receive mail for mailboxes that you define.

Note:

- If you use the quarantine system in SMG, depending on the amount of spam you receive and how long the SMG is set to save mails classified as spam, the hard disk on which the SMG has been installed on may or may not need to be upgraded with additional space. The SMG compresses all quarantined mails, thereby reducing them significantly in size, and regularly compacts its databases to minimize the space it uses - however as a standard system administrative task, disk space monitoring is suggested on high volume systems.

1. Short description

This is how the installation procedure will go if you follow this guide:

- Installation of the SMG while the SMTP filter is still running.
- Configuration of the SMG.
- Stopping the SMTP filter and making the SMG take over.
- Uninstalling the SMTP filter.

This procedure will give a zero downtime.

2. Installing the SMG

Start by installing the SMG on the server on which the SMTP filter is already running. This is pretty straightforward, but if you are in doubt the process is described in the manual for the SMG.

- During the installation you will be prompted to enter the IP of your mail server. Do not worry if you have more than one mail server as you will be able to enter further mail server addresses once the installation is complete.

3. Configuring the SMG

In this chapter configuration of the SMG will be done by comparing it to the SMTP filter.

To get started open the SMG administration interface using the “Solution Administrator” mode and the SMTP filter configuration menu.

3.1 Routing

Select “Routing” which is found under the “Administration” menu.

3.1.1 Inbound connectors

This is the equivalent of **Local Address or Hostname** on the **Tunnel** tab from the SMTP filter.

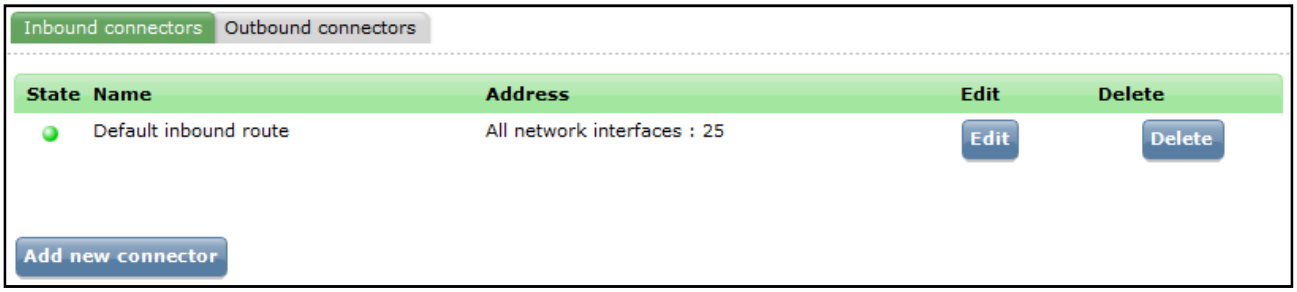

Figure 3.1.1a – Default inbound route

Click “Edit” to choose which IP/port the SMG should listen for inbound emails on.

Note:

- It does not matter that the IP/port that you select is already being used by the SMTP filter as the SMTP filter will have first priority over the SMG.
- You only need one **Inbound connector** no matter how many tunnels you have on the SMTP filter. It is the **Outbound connectors**, described next, which will determine where the mail is routed after being filtered.
- If you have multiple tunnels in the SMTP filter then select the IP/port you want the SMG to listen for mail on in the future.

3.1.2 Outbound connectors

This is the equivalent of **Remote Address or Hostname** on the **Tunnel** tab from the SMTP filter as well as the **Domains** part from the **Domains** tab.

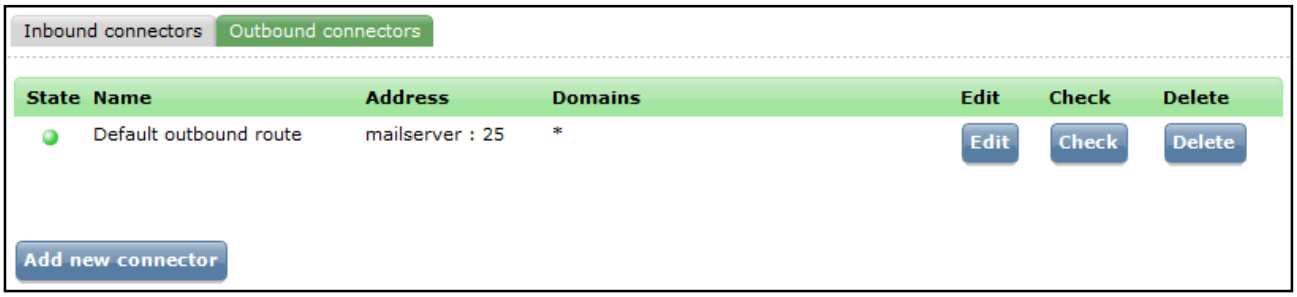

Figure 3.1.2a – Default outbound route

This default outbound connector is set to take care of all domains, hence the * at domains.

Click "Edit" to setup this outbound connector. For each tunnel in the SMTP filter you need to set up one outbound connector in the SMG – click "Add new connector" to add and setup additional connectors.

An example of configuration with 2 mail servers:

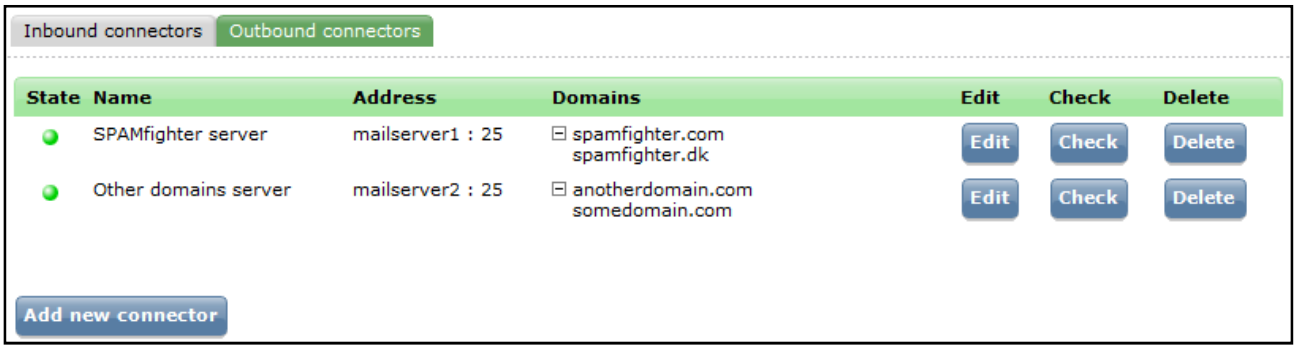

Figure 3.1.2b – Specified outbound routes

If you do not have a catch all domain (*) defined then mails for domains which have not been specified for any of the outbound connectors will be either rejected or quarantined.

3.2 Mailboxes

Select “Mailboxes” under “Configuration”.

If you want to use Active Directory then please refer to the chapter **Advanced Administration** from the SPAMfighter Mail Gateway User Manual.

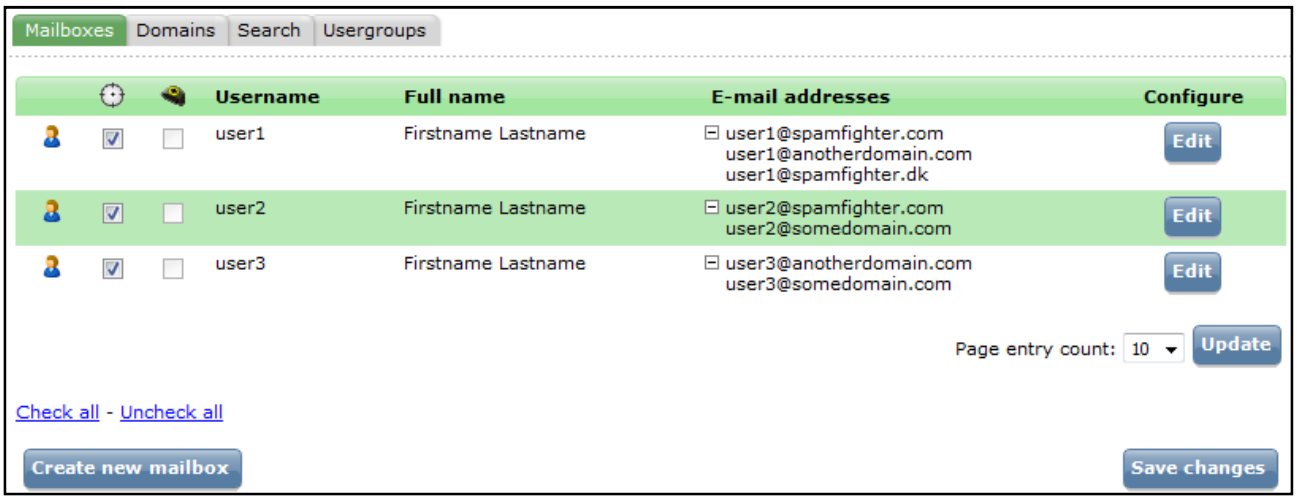

Figure 3.2a – Mailbox list

Here you add the users, their mailboxes and aliases as shown above.

When creating new users their Security rating should normally be set to “Normal user”:

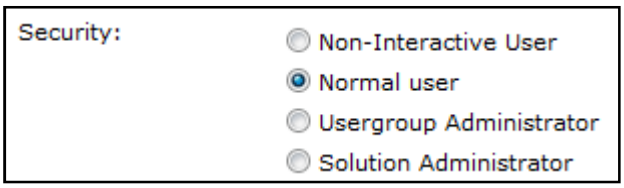

Figure 3.2b – Security rating

This security rating will allow them to pass emails from the quarantine to their mailbox themselves.

Example:

- With the routing specified in Figure 3.1.2b an email arrives for test@test.com – a domain which has not been specified on any of the Outbound connectors. If the mailbox does not exist then the mail will be rejected by the SMG, but if a mailbox exists and there is no outbound route for the domain then the SMG will attempt to deliver the email every minute up to 6 hours and after this time it will be moved to an error folder on the disk. If the latter is the case (that you are missing an Outbound connector to handle a specific domain) you will see the error in Figure 3.2c when you create the mailbox telling you that none of the Outbound connectors has been set up to handle this domain.

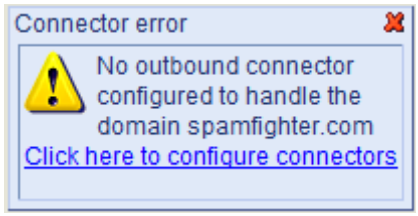

Figure 3.2c – No Outbound connector

3.3 Domains

When finished setting up the mailboxes go to "Domains" found under "Configuration".

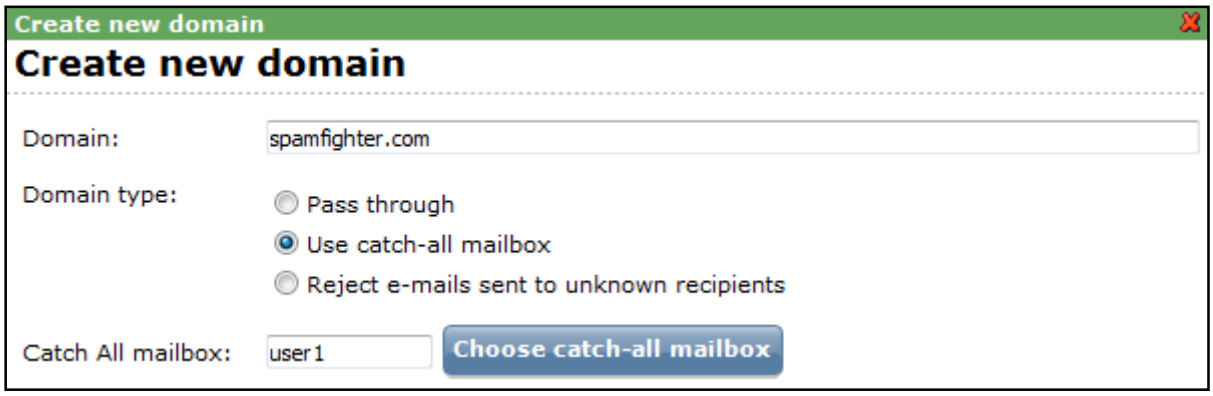

Figure 3.3a – Non-defined mailboxes

You can set up the SMG to handle non-defined mailboxes. "Use catch-all mailbox" means that all mail for non-defined mailboxes will be sent to the primary mailbox for the selected user.

Note:

- If you do not define any rules for non-defined mailboxes then default is that they will be rejected in the SMTP transaction.

3.4 Policies

The “Policies” menu is found as the next point under “Configuration”. The functionality is naturally very much like that found in the SMTP filter.

Just like in the SMTP filter, if you have domains which needs to have different policies (maybe because of different black and white lists for the different domains) then you need to setup different policies here and move the mailboxes to the correct policy.

3.4.1 Filter settings

Starting on the “Filter settings” tab, this is where you assign how your installation should filter incoming emails.

Figure 3.4a – Filter settings

Unlike the SMTP filter in the SMG an email is either considered ham or spam. It is not possible to assign specific actions for an email dependant on which filter blocks it. The reason for this is the quarantine functionality in the SMG which ensures that even emails classified as spam are saved for a time period so the recipient can unblock false positives.

First we have the “**Sender Filter**” (aka. black and white lists). Here you can import any black and white lists you might have in the SMTP filter. To export them from the SMTP filter simply use the tool included in the SMG installation:

- Go to “Start -> All Programs -> SPAMfighter Mail Gateway -> Support -> Tools -> SPAMfighter Script Console”
- Type this into the command prompt: **FilterServerExporter**
- This will open the tool which you can use to place the Sender Lists from the SMTP filter in a folder on the desktop.

The “**Content filter**” which is a completely new feature compared to the SMTP filter. This allows you to filter on attachments.

The “**Community Filter**” is the equivalent of the “Configure thresholds” of the SMTP filter and this is where incoming emails are compared to the database of spam mails which have been blocked by the community of SPAMfighter users. We suggest you use the “Medium” setting to start with.

The “**Language Filter**” is like that in the SMTP filter but just with a nicer interface.

3.4.2 Accept actions

This is the equivalent of configuring the “Accept action” on the Actions tab of the SMTP filter, and this is where you determine what should happen to emails which pass all the filters set up on the “Filter settings” tab.

3.4.3 Block Actions

This is the equivalent of configuring the "Reject action" of the SMTP filter as well as some of the other partly-Reject actions. Because unlike the Reject action of the SMTP filter, which by default blocked the incoming email in the SMTP transaction, you can assign a lot of different actions to emails which are blocked – the most important difference being that they can be put in the quarantine.

3.4.4 Mailboxes

If you have more than one policy, then this is where you get an overview of, and determine, which mailboxes are being filtered by the different policies.

4. Switching to the SMG

Once you are done configuring the SMG follow the guide below which describes your situation.

4.1 If you have only one tunnel in the SMTP filter

Open the SMTP filter Configuration tool and select the Service tab:

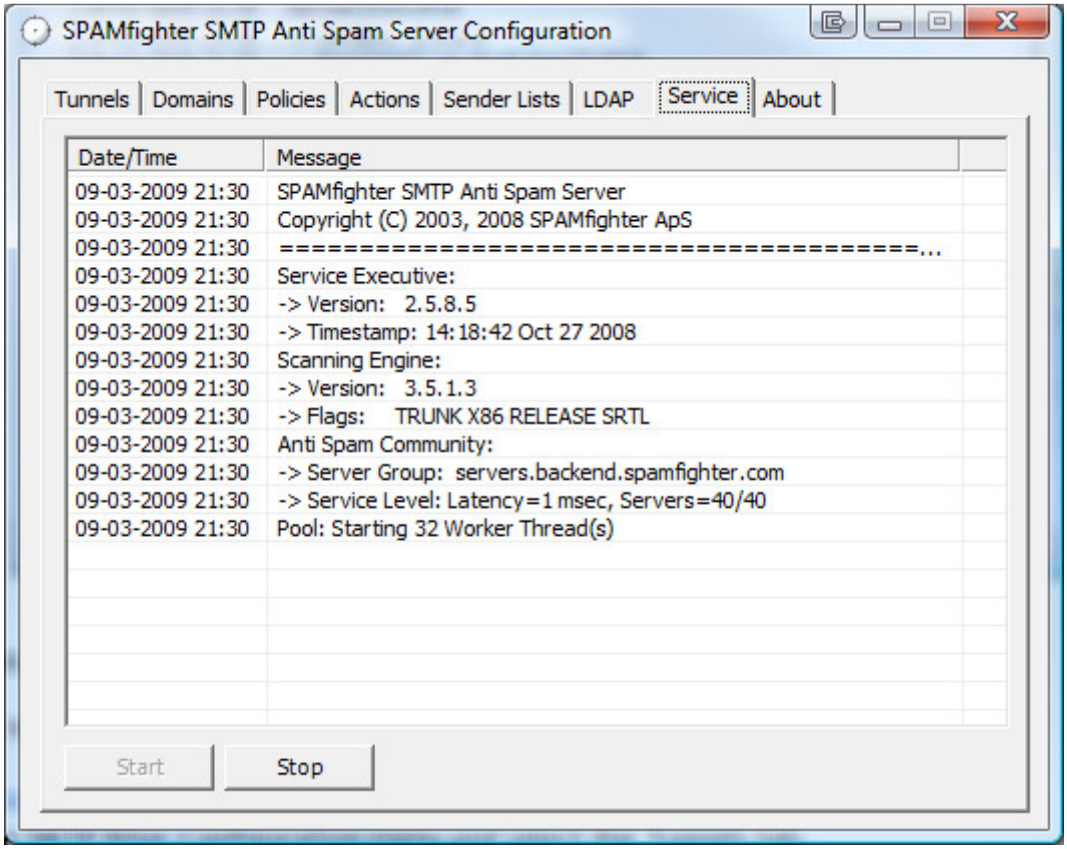

Figure 4.1a – SMTP filter Service configuration tab

Simply stop the service by clicking "Stop" and the SMG will take over.

You are now ready to uninstall the SMTP filter – skip to chapter 5.

4.2 If you have more than one tunnel in the SMTP filter

Open the SMTP filter Configuration menu and select the Tunnels tab.

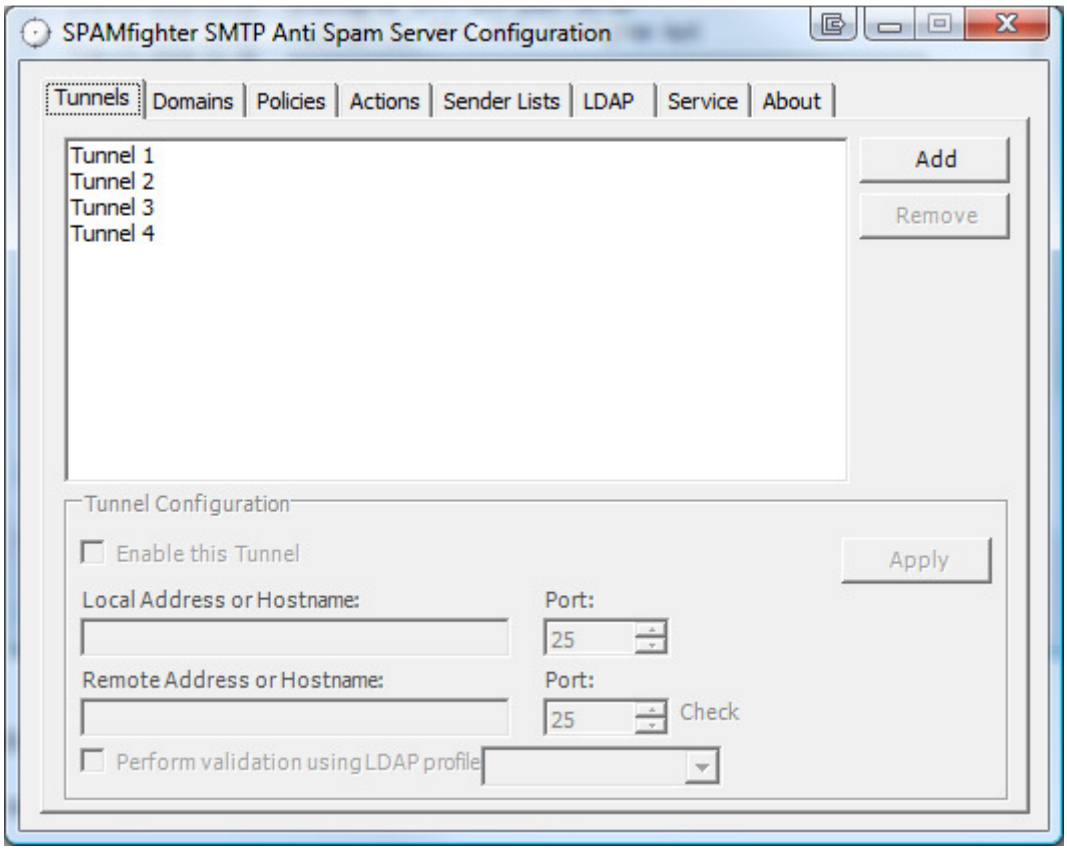

Figure 4.2a – SMTP filter Tunnels configuration tab

Now locate the tunnel which has the IP/port that was assigned as the Inbound connector for the SMG as “Local Address or Hostname” in the SMTP filter. Remove the check mark in “Enable this Tunnel” and click “Apply”. This will move filtering of emails that was normally running on that IP/port to the SMG.

Next you have to configure your network or the MX Records which is pointing emails for the various domains to the various tunnels on the SMTP filter to the IP/port which was specified as the Inbound connector for the SMG in chapter 3.1.1.

4.2.1 Reconfiguring Network

If you are doing this by configuring your network the changes should be instantaneous and you can proceed to chapter 5.

4.2.2 Changing MX Records

If you are doing this by changing MX Records we recommend that you start by creating Inbound connectors for each tunnel in the SMTP filter and leave them running until the change has mitigated to all DNS's.

Note:

- This can take up to a couple of days, so leave the Inbound connectors for 5 days to be on the safe side before you delete them again.

Once this has been done you can continue to chapter 5.

5. Uninstalling the SMTP filter

If you have not done so already, start by stopping the SMTP filter as described in chapter 4.1. This will let the SMG take over instantly.

Now uninstall the SMTP filter.

6. After

There is nothing else to do but sit back and enjoy the new features of the SMG. We are sure you will be happy with it.

If you should have any questions please do not hesitate to contact us.

SPAMfighter technical support
Email: smgsupport@spamfighter.com
Telephone: (+45) 7022 1551

SPAMfighter sales
Email: sales@spamfighter.com
Telephone: (+45) 7022 1551