Effective spam filtering with SPAMfighter SMTP Anti Spam Server and the Microsoft Simple Mail Transfer Protocol (SMTP) service

This whitepaper describes a "best practice" configuration for SMTP Anti Spam Server when used in conjunction with the SMTP service from Microsoft.

Versions this document applies to

- SPAMfighter SMTP Anti Spam Server 2.2.0 and newer
- Microsoft SMTP service shipping with Microsoft Windows Server 2003 and Microsoft Windows XP Professional

Assumptions

- SPAMfighter SMTP Anti Spam Server will be installed on the same computer running Microsoft SMTP service. (If this is not the case, you may still make use of some parts of this document.)
- You have administrative permissions on that computer.
- The computer is using a private, static IP address (not DHCP assigned) and port 25 is being forwarded to it from a public IP address using some router, firewall or gateway device. (If this is not the case, you may still make use of some parts of this document.) You have access to the router's configuration or can have it reconfigured.
- Incoming mail from the internet is received using the SMTP protocol (the default), not downloaded with ETRN or POP3.

Conventions

- When asked to "select" or "activate" a button, menu item or list entry, this can usually be done by either clicking the object using a mouse or other pointing device or by pressing the TAB key until the object in question is highlighted followed by pressing the space bar.
- *Italic text like this paragraph requires special attention.*
- `Text in mono-space font like this paragraph illustrates commands or other text that should be entered into an application.`

Table of Contents

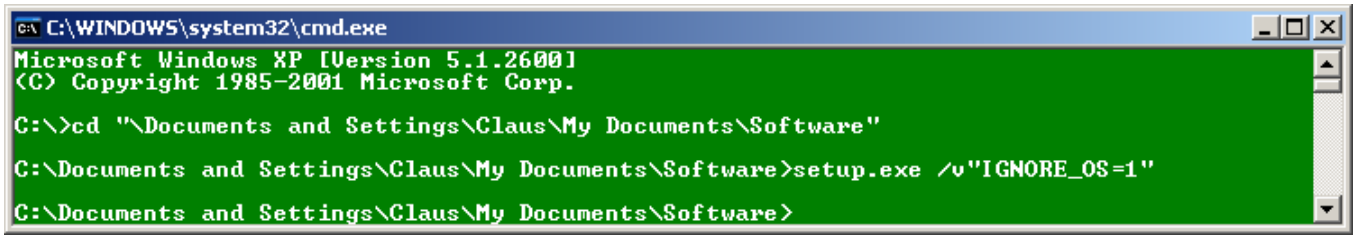
Installing SMTP Anti Spam Server

Installing SMTP Anti Spam Server won't interfere with your current setup. The product does not bind to (listen on) any port until configuration is completed. A reboot is not required by the application itself; however if your computer is missing a Service Pack or the Microsoft .NET Framework 2.0 Runtime, these components might require a reboot.

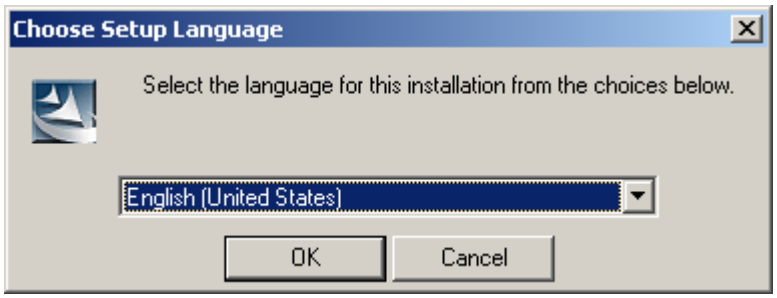
1) Log on to the computer using an Administrator account.

2) Download the latest version of SMTP Anti Spam Server here:
http://www.spamfighter.com/SMTP_Install.asp

3) *If you are running Windows 2000:*
- Make sure that the computer has Service Pack 3 or later installed. If you are unsure, visit Windows Update and install all critical and recommended updates first by clicking here:
http://windowsupdate.microsoft.com/
- Double-click the downloaded file setup.exe to install SMTP Anti Spam Server.
If you are running Windows Server 2003:
- Double-click the downloaded file (setup.exe) to install SMTP Anti Spam Server.
If you are running Windows XP:
- Open a command prompt and navigate to the download directory using the "cd" command, then enter the following command and press Enter/Return:
`setup.exe /v"IGNORE_OS=1"`

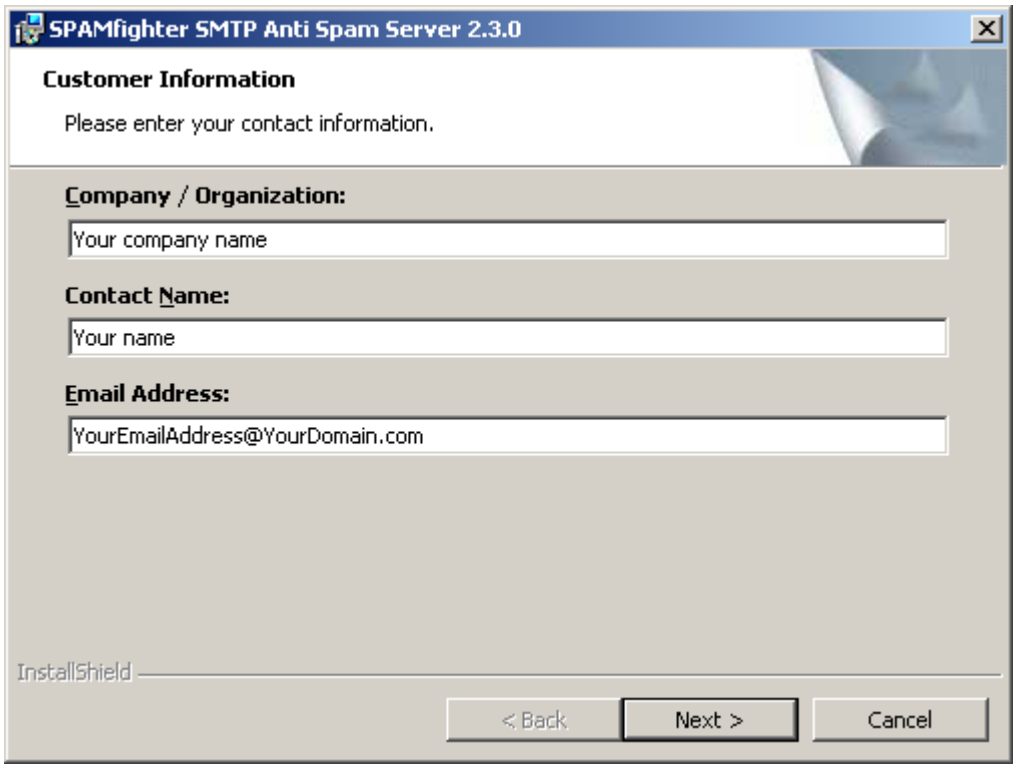


4) Select your preferred language and select "OK":

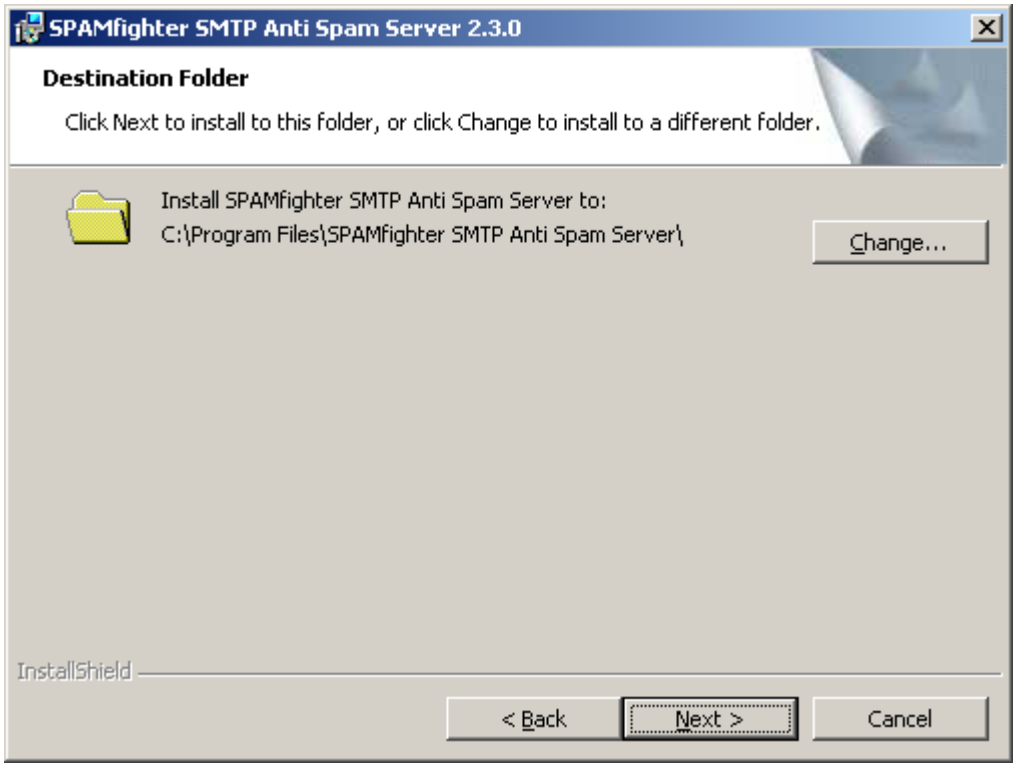


5) When this screen appears, enter your contact details and select "Next". (Are you reinstalling Windows and SMTP Anti Spam Server or moving your existing installation to another server? In this case it is important to enter the exact same details as last time to regain your license(s). If you are unsure, just enter your details

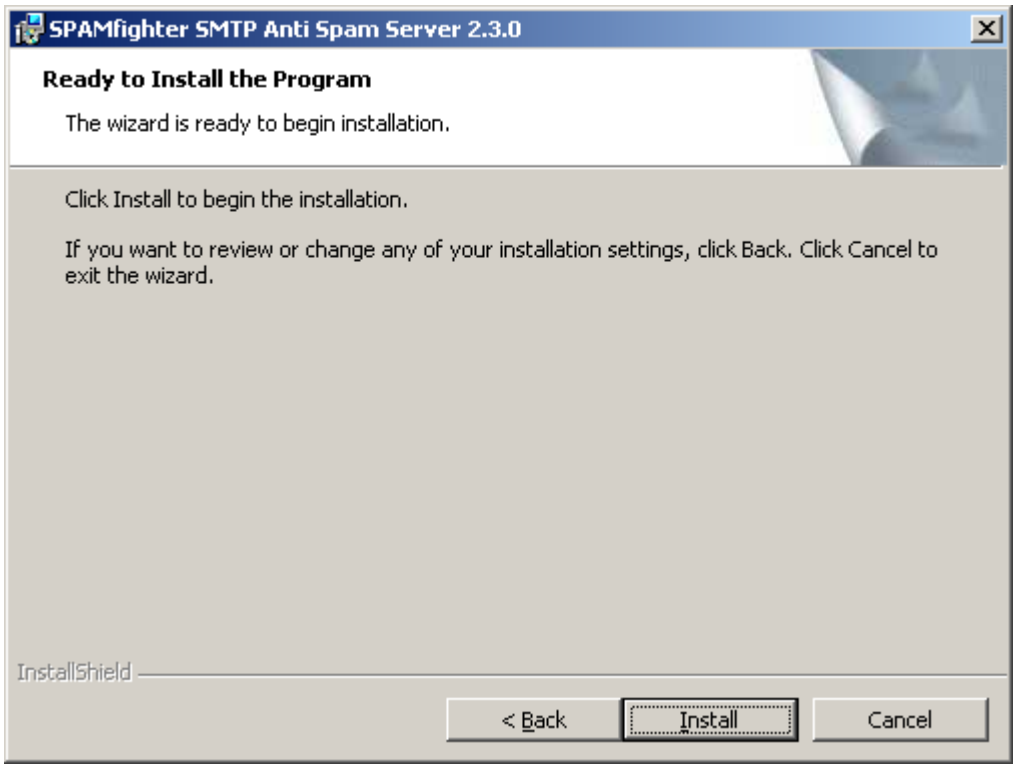
and continue, then contact our support team at smtpsupport@spamfighter.com after the installation.)



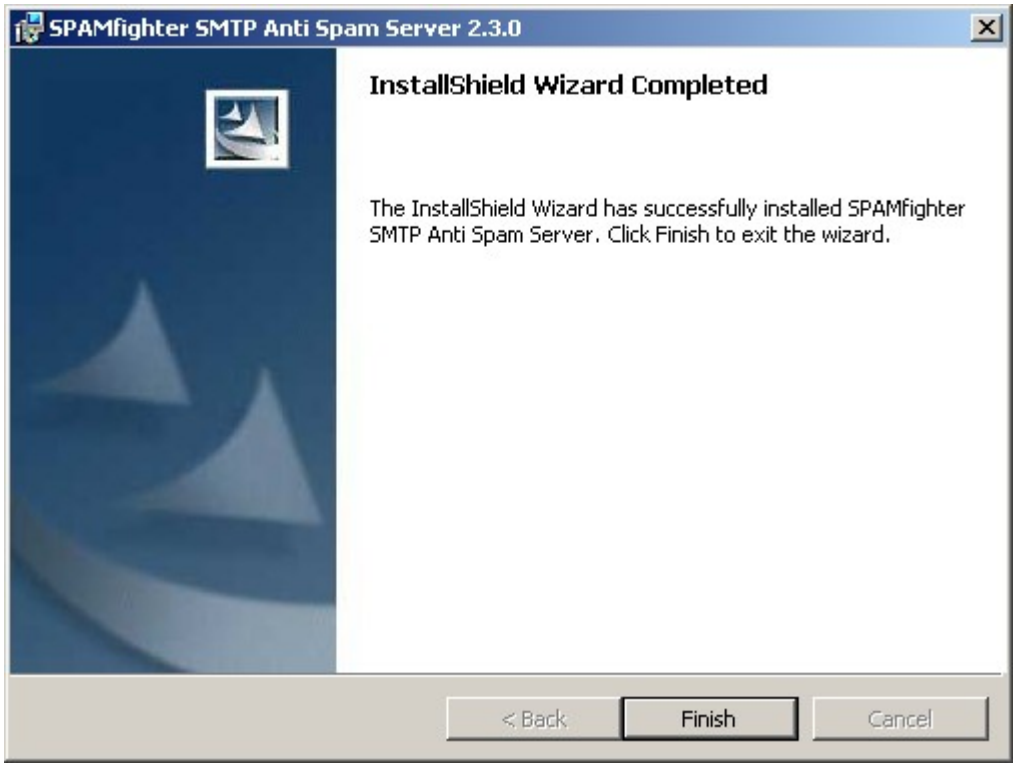
6) Choose the installation directory (it is recommended to install into the pre-entered directory) and select "Next":



7) Select “Install”:



8) Select “Finish” to exit the installation:



Configuring Windows

The following task has to be completed to setup Windows for SMTP Anti Spam Server:

- Add another local IP address for SMTP Anti Spam Server.

Add another local IP address for SMTP Anti Spam Server

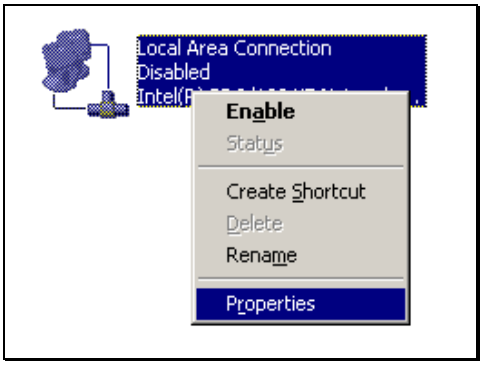
Please note that all numbers and values displayed in the following images are *meant as examples only* and likely need to be adapted to your specific network environment.

1) Select “Start” > “Control panel”.

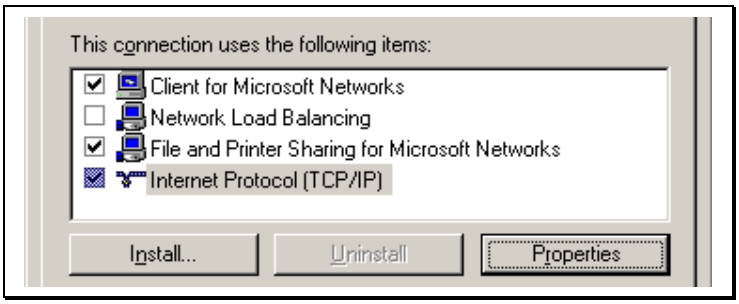
2) If the modern view is displayed, “Switch to classic view” on the upper left.

3) Activate “Network connections”.

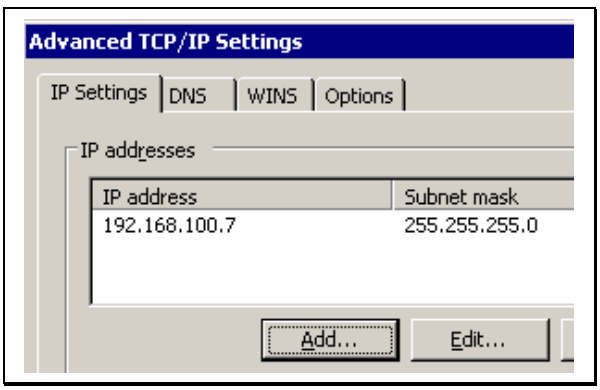
4) Right-click the LAN connection to your router or gateway device and select “Properties”:



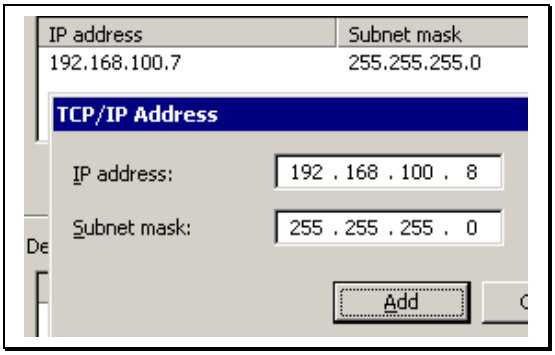
5) Select “Internet Protocol (TCP/IP)” and then “Properties”:



6) Note the existing IP address(es) and select “Add…”:



7) Add a new unoccupied IP address from the same subnet (if you are unsure, consult your network administrator) and click “Add”:



8) Write both IP addresses down – you will need them later.
In the following text we will refer to the example address “192.168.100.8” as the “new IP address” and to the example address “192.168.100.7” as the “old IP address”.

9) Select “OK” three times.

Configuring Microsoft SMTP service

The following tasks have to be completed to setup Microsoft SMTP service for interopability with SMTP Anti Spam Server:

- Unbind Microsoft SMTP service from the newly added IP address.
- Disable relaying access for the newly added IP address.

1) Start Microsoft IIS administration by clicking “Start” > “Run”; enter “inetmgr” and press “OK”.

Unbind Microsoft SMTP service from the newly added IP address

We need to prevent Microsoft SMTP service from listening on the new IP address in order to allow the SMTP Anti Spam Server to use it.

2) Expand the “local computer” icon in the tree on your left hand. Right-click the SMTP service instance (often called “Default SMTP Virtual Server”) and select “Properties”.
3) Click on “Advanced” to the right of the “IP address” dropdown menu.
4) *If the entry “(All Unassigned)” exists in the displayed address list:* select it and click on “Remove”. Then click “Add...”, choose an IP address from the dropdown menu *except the new IP address*, enter “25” in the “TCP port” field, and click “OK”. Repeat this for every IP address *except the new IP address* by clicking “Add...” again, choosing the next IP address from the list, entering “25” in the “TCP port” field, and clicking “OK”.
5) *If the new IP address exists in the displayed address list:* select it and click on “Remove”.
6) The list of IP addresses displayed in the window “Advanced” should now include *at least the old IP address, probably others, but neither the new IP address nor the text “(All Unassigned)”*.
7) Click “OK” to close the “Advanced” window.

Disable relaying access for the newly added IP address

The relaying list in Microsoft SMTP service determines which computers may use your connection to send e-mail to external domains. By default Microsoft SMTP service won’t relay e-mails for unauthenticated users; however you might have changed this setting previously in order to simplify client configuration. *Because the IP address used by SMTP Anti Spam Server represents external, unauthenticated clients, it is extremely important to disable relaying access from the new IP address.*

8) Select the ”Access” tab in the SMTP service properties window, then click on the ”Relay...” button.
9) *If the field ”Only the list below” is checked:* Make sure the list of IP addresses in this window does *not* include the new IP address. If it does, modify the list so that it excludes the new IP address explicitly.
10) *If the field ”All except the list below” is checked:* Make sure the list of IP addresses in this window *includes* the new IP address. If it does not, click on ”Add...”, enter the new IP address in the topmost field, then click on ”OK”.
11) *Important:* if you have external users (users which send mail to internet addresses through this SMTP server from outside the office, e. g. at home or on the road), make sure the checkbox ”Allow all computers which successfully authenticate to relay, regardless of the list above.” is checked. If it wasn't checked before you might have to instruct those users to enable authentication for sending mails in their e-mail applications. *This*

does not apply to internal users (in the office) nor those who already send mails authenticated or via external SMTP servers, i.e. those provided by their internet providers or phone companies.

12) Click ”OK” in the ”Relay Restrictions” window, then again ”OK” in the SMTP service properties window.

Configuring SMTP Anti Spam Server

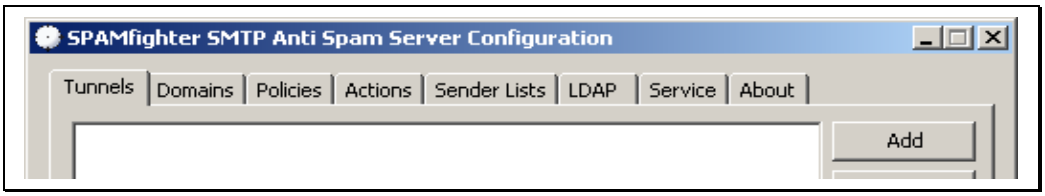
The following tasks have to be completed to setup SMTP Anti Spam Server for interopability with Microsoft SMTP service:

- Establish a tunnel between the new and old IP address.
- Decide on a policy for spam handling.
- Apply the policy to domains.

1) Start the SMTP Anti Spam Server configuration utility by choosing “Start” > “All programs” > “SPAMfighter SMTP Anti Spam Server” > “Configure Anti Spam Server”.

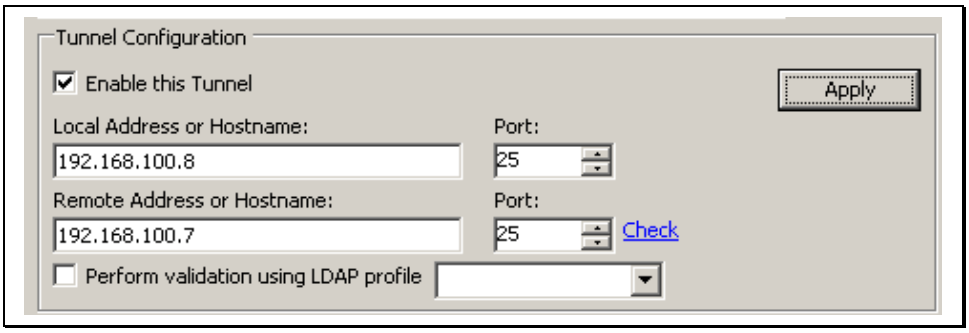
Establish a tunnel between the new and old IP address

2) On the “Tunnels” pane, select “Add” to create a new tunnel:

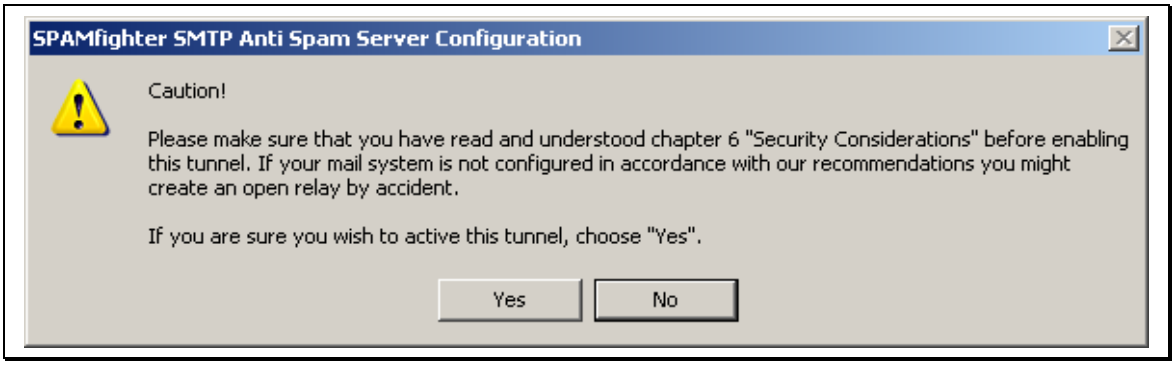


3) Select the “New tunnel” that appeared in the list.

4) For “Local Address or Hostname”, enter the new IP address you added to the server previously.
For “Remote Address or Hostname”, enter the old IP address used by Microsoft SMTP service.
Put a checkmark in the “Enable this Tunnel” box and activate the “Apply” button:



5) If you receive a security warning, confirm it by selecting “Yes”:



Decide on a policy for spam handling

SMTP Anti Spam Server enables different scenarios depending on the control you and your users require over filtered spam mails. Among the possible spam handling actions are:

- Reject delivery (the default)
- Redirect them to a collection mailbox
- Deliver them to the intended recipient and:
    - Insert “SPAM” or other text in the subject
    - Insert a header line in the mail

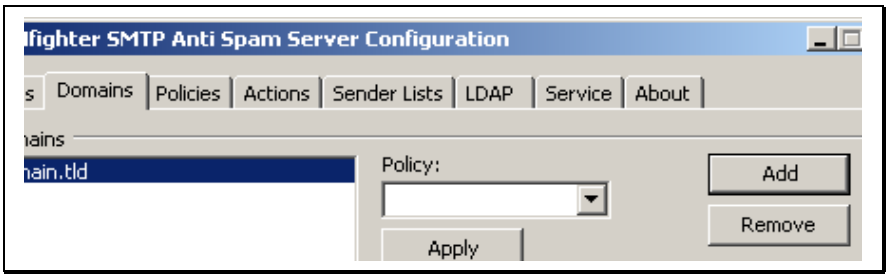
  for further sorting in the mail server or mail application.

These “actions” can be applied to one or more “policies” that in turn can be applied to one or more domains and/or recipients.

In the following steps we will apply the “Default policy”, which is a basic policy configured to reject mails with a high spam probability. For more information on configuring actions, policies and other advanced features of SMTP Anti Spam Server please refer to the manual included with your installation or available for separate download here.

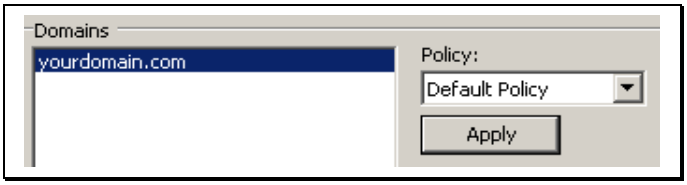
Apply the policy to domains

6) On the “Domains” pane, select “Add” to add your first domain:



7) Double-click (or select and press F2) the new domain “domain.tld” added to the list, rename it to your real domain name and press Enter:

8) With the domain still selected, choose the “Default Policy” from the dropdown and activate the “Apply” button:



After having verified that the setup is working you might want to customize your policy and spam handling actions further. Please refer to the manual included with your installation or available for separate download here for further instructions at that time.

Configuring your router, firewall or gateway device

The last step will be to configure your router, so incoming mail from the internet is sent through the tunnel before being delivered to your Microsoft SMTP service.

How to do this depends on the hard- and software to use. Usually you would change the port forwarding setting for port 25 (SMTP) from the old IP address to the new one (following our example, you would change 192.168.100.7 to 192.168.100.8 in the router's port forwarding configuration). If in doubt, please ask your network administrator or consult the manuals included with your hard- or software.