SPAMfighter SMTP Anti Spam Server

Users Manual

Revised 4/27/2006

1 Table of Contents

2 Terminology

For brevity, the “SPAMfighter SMTP Anti Spam Server” is often referred to as “the Filter” throughout this document.

In addition, “Filter server” refers to the physical server on which the Filter is installed.

3 Technology

3.1 Tunneling and Interception

In contrast to existing anti virus and anti spam mail solutions available today, the SMTP Anti Spam Server is not based on store-and-forward technology. This store-and-forward technology is often referred to as relaying and found in most mail gateway products.

The SMTP Anti Spam Server offers a unique alternative acting as a network proxy inspecting SMTP traffic on-the-fly.

This provides a number of significant advantages over existing solutions:

1. No local mail queues:
   - High performance since there is no need for disk activity
   - Low latency and no delivery delays
   - Reliable - no maintenance and backup needed for queues
2. Recipient address validation is still performed by your existing mail server:
   - No time wasted on setting up and maintaining active mailboxes, etc.
   - No excessive generation of non-delivery reports as seen on most store-and-forward solutions

The high performance characteristics of this technology make it suitable for deployment in large enterprises, hosting centers and Internet Service Providers.

Since there is no local mail queue, the Filter provides no additional protection against failure of the mail server. In that case, the usual rules apply: It is the responsibility of the delivering mail server to queue the mail and retry later. In this fashion no mails are lost but only delayed.

Since the Filter works by inspecting the SMTP traffic before it reaches your mail server, it must be inserted between your internet connection (firewall) and mail server. This is accomplished by setting up a *tunnel* on your Filter server. A tunnel consists of a *local endpoint* (the local IP address and port on the server) and a *remote endpoint* (the IP address and port for SMTP traffic on the mail server).

Once a connection is accepted on the local endpoint the Filter will immediately connect to the mail server and start inspecting/forwarding the traffic. To start accepting connections from the internet, you need to:

1. Set up a forwarding rule in your firewall, sending inbound SMTP connections to the local endpoint
2. Modify the MX record for your domain, point them toward the local endpoint (requires that the local endpoint is an IP address reachable from the internet)

Any number of tunnels can be configured on a single Filter installation, thus a single Filter instance can protect multiple destination servers.

Even though tunneling provides a number of advantages, it may be necessary to address certain security issues before deploying the Filter. Please read chapter 6 “Security Considerations” to fully understand the implications of tunneling.

3.2 Content Classification

The SMTP Anti Spam Server provides a number of different classification mechanisms. Based on the classification of any given email, a number of actions may be performed.

3.2.1 Spam Classification

SPAMfighter ApS employs a collaborative filtering technology in all of its products. The content classification is based on the generation of email signatures which is in turn used in an online voting system.

Based on the votes of the more than 1.200.000 users of the SPAMfighter client software, the database is continuously updated.

For each email the SMTP Anti Spam Server intercepts, it will generate the email signatures and query the voting servers.

3.2.2 Virus Classification

The SMTP Anti Spam Server provides integration with the VIRUSfighter product suite. The virus scanner processes all email parts, compressed archives and nested emails.

The VIRUSfighter scanning engine must be installed on the Filter server – however, it is not necessary to utilize the on-access file system scanner.

A free 30 day trial of the VIRUSfighter product is available from: http://www.virusfighter.com.

3.2.3 Language Classification

The SMTP Anti Spam Server features language classification. A weighted analysis is performed on all plaintext and HTML parts in the message (excluding attachments). The following languages are recognized:

- Arabic
- Chinese
- Danish
- Dutch
- English
- Finnish
- French
- German
- Hebrew
- Italian
- Japanese
- Korean
- Norwegian
- Russian
- Spanish
- Swedish
- Thai

3.3 Policies and Actions

A filtering policy can be defined for each recipient domain and mailbox which determines what action should be taken when an email is classified as spam. Based on the policy one or more of the following actions can be performed:

- Reject the email before it reaches the destination server
- Redirect the email to any number of mailboxes
- Insertion of an email header line for later processing
- Prefixing of the subject header line for later processing
- Store a copy of (dump) the message to the local file system

Policies also contain information about white- and blacklists and the threshold (sensitivity level) for spam detection. It is also possible to create policies which always performs (forces) an action, thus making it possible to create permanent redirects or rejections at the Filter level.

3.4 Standards Conformance

The Filter conforms to these Internet standards:

Document	Title
RFC 2821	Simple Mail Transfer Protocol
RFC 2822	Internet Message Format
RFC 2045	MIME: Multipurpose Internet Mail Extensions
RFC 2046	MIME: Media Types
RFC 2047	MIME: Message Header Extensions for Non-ASCII Text

In addition, the following SMTP Service Extensions are supported:

Document	Title
RFC 1652	SMTP Service Extension: 8 Bit MIME transport
RFC 1870	SMTP Service Extension: Message Size Declaration
RFC 1891	SMTP Service Extension: Delivery Status Notification
RFC 2043	SMTP Service Extension: Enhanced Status Codes
RFC 2554	SMTP Service Extension: Authentication
RFC 2852	SMTP Service Extension: Deliver By
RFC 2920	SMTP Service Extension: Command Pipelining

Unsupported SMTP Service Extensions are suppressed by the Filter.

4 Installation

4.1 Requirements

4.1.1 Environment

The Filter is targeted for installation on the Microsoft Windows platform. Due to the interoperability inherent in the SMTP protocol the product can be deployed effortlessly in a mixed environment.

4.1.2 Operating System

Deployment on Microsoft Windows 2003 Server is *recommended* in performance-critical environments since the Filter will utilize a highly asynchronous communication model introduced in Microsoft Windows 2003 Server. The software is *compatible* with Microsoft Windows 2000 SP3 and later.

The Microsoft .NET 2.0 Framework is required for the Configuration Tool and for exposure of Performance Monitor Data. The installation process will determine if the .NET Framework is missing and will install it accordingly.

4.1.3 Hardware

The full Intel Pentium family of processors (and compatible) is supported. The Filter application is optimized for Pentium 4 and in addition scales linearly in multiprocessor systems.

The memory footprint of the application is approximately 10 megabytes. As the Filter application buffers emails in memory, the actual consumption varies with the number of concurrent SMTP transactions and the size of each message. A good estimate for peak memory consumption in a medium-volume environment is 64 megabytes.

The installation occupies approximately 5 megabytes of disk space (not including any dependencies such as the .NET Framework). A reasonable amount of disk space should be allocated for traffic log files, in most cases a few gigabytes suffice. Please review the “Log Files” chapter below.

4.1.4 Network and Firewall

The Filter application will communicate with the SPAMfighter classification servers to assist in content classification. Periodical usage statistics are also reported back to the SPAMfighter licensing servers. The table below lists the firewall changes that are necessary:

Protocol	Source Address	Port	Destination Address	Port	Direction
TCP	Server Address	Dynamic	smtp.licensing.spamfighter.com	80	Out
UDP	Server Address	Dynamic	servers.backend.spamfighter.com	2409	In / Out

When using a stateful firewall with outbound traffic enabled it is not necessary to perform any changes.

4.2 Deployment Checklist

To successfully deploy the SPAMfighter SMTP Anti Spam Server you need to complete the steps outlined below. Details related to the configuration steps are dealt with in later chapters.

4.2.1 Installation

- Review the "Installation - Requirements" chapter
    - □ Assign an appropriate server
    - □ Modify the firewall configuration as outlined
- Review the "Security Considerations – Relaying" chapter
    - □ Modify the existing mail server setup as outlined
- Download and launch the installation package:
  http://download.spamfighter.com/download/smtp/setup.exe

4.2.2 Configuration

- Create tunnels between the Filter and existing mail servers
- Create or customize the filtering policies
- Create a list of domains to protect and select an appropriate policy for each

4.2.3 Testing

- Start the Filter application in console mode
- Verify that the Filter is configured properly by sending a mix of legitimate and spam mails to the configured domains through the Filter
- Stop the Filter application

4.2.4 Deployment

- Start the Filter application in service mode
- Point the DNS MX records of the domains to the Filter server (or modify the firewall/network appliance configuration to direct traffic through the Filter)

4.3 Contents

The installation process will create the user-defined installation directory and install the following files:

File	Description
Filter.exe	Filter application installed as a Windows Service
Configure.exe	Configuration Tool

The Filter application is installed as a service named "SPAMfighter SMTP Anti Spam Server". You can control the service behavior through the Service Control Manager.

In addition a shortcut folder named Start → Programs → SPAMfighter SMTP Anti Spam Server is created containing these shortcuts:

Shortcut	Description
Configure	Starts the Configuration Tool
Documents → Manual	User Manual
Service → Start	Shorthand to start the Filter application as a service
Service → Stop	Shorthand to stop Filter application if running as a service
Service → Run in Console	Start the Filter application in console mode

Please note that you must stop the service (if running), before starting the application in console mode. Two instances of the application can not run concurrently as the last to start will be unable to bind to the local endpoint(s).

When the Filter application is running in console mode it can be stopped by pressing Ctrl-C.

All configuration data is stored in the Windows Registry, but should only be modified through the Configuration Tool: `HKEY_LOCAL_MACHINE\Software\SPAMfighter Filter Server`.

5 Configuration

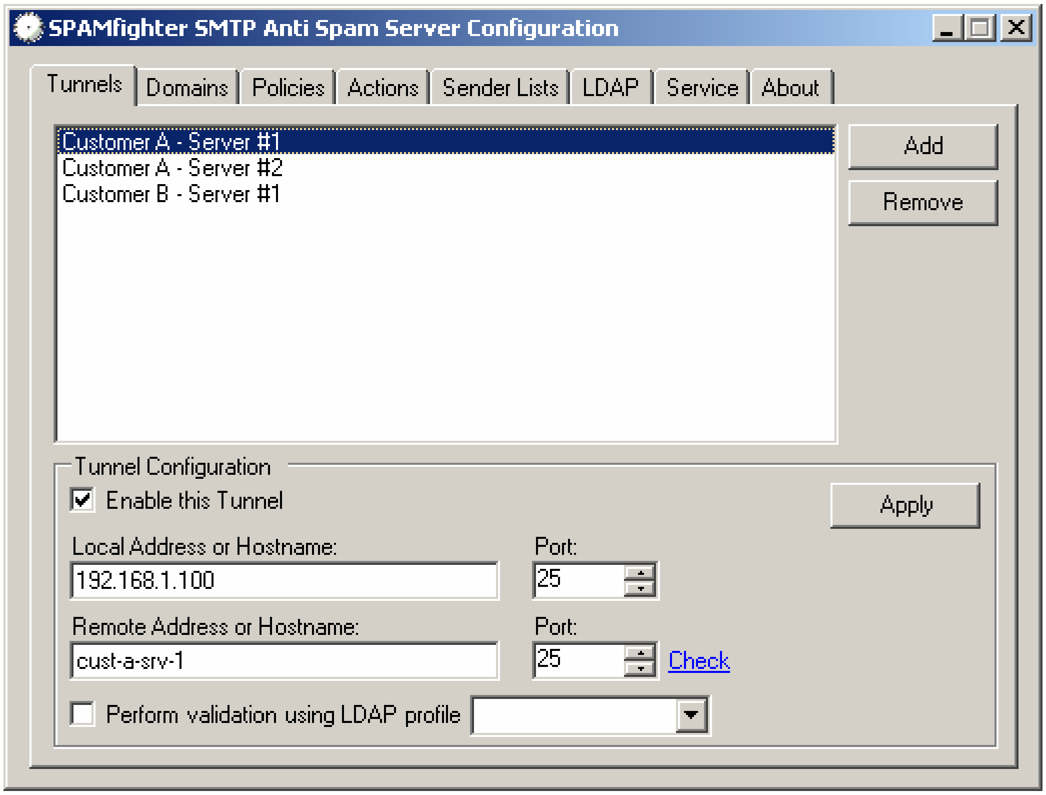
The Configuration Tool is accessible through the SPAMfighter SMTP Anti Spam Server
→ Configure shortcut. It contains a tab for each of the chapters below.

All configuration data can be modified on-the-fly, without restarting the Filter application. If a tunnel is modified or removed, the Filter application will wait until all active tunnel sessions have terminated before applying the changes.

The screenshots included in this document illustrates an installation at a hosting center.

5.1 Tunnels

Since the Filter acts as a proxy it needs information about the destination servers which it is protecting. A tunnel consists of two *endpoints*, the local and remote endpoint:



Customer A - Server #1
Customer A - Server #2
Customer B - Server #1

Tunnel Configuration

☑ Enable this Tunnel

Local Address or Hostname: 192.168.1.100
Port: 25

Remote Address or Hostname: cust-a-srv-1
Port: 25

□ Perform validation using LDAP profile

5.1.1 Local Endpoint

The local endpoint consists of the address and port on which the Filter accepts connections for the tunnel.

The default address is "`0.0.0.0`" which means that the Tunnel will accept connections on any address on the server.

In scenarios where a single Filter installation is protecting multiple destination servers, it is necessary to assign multiple IP addresses to the Filter server: only a single tunnel can listen on any given address/port pair on a server. If it is unfeasible to assign multiple address, non-standard port numbers can be used as discussed below.

The assigned (standard) port number for the SMTP protocol is 25. If the tunnel is accepting connections directly from the Internet, it needs to listen on this port.

It is possible to use a non-standard port number if a firewall capable of port translation is deployed on the network, or the Filter is behind some other kind of network appliance which can be configured to use the non-standard port number.

Using a non-standard port is only recommended if:

1. Another application or tunnel is already listening on the address/port pair and
2. It is not feasible to assign more IP addresses to the server.

5.1.2 Remote Endpoint

Once a connection is accepted on the local endpoint, the remote endpoint information is used to establish the tunnel.

The address or hostname must be specified. The default port number is 25 but can be modified as necessary.

5.1.3 Testing

Once a tunnel has been configured and enabled, the Filter application will start listening on the specified address and port. To verify that the tunnel is working properly, click Start → Run and type:

```
telnet <local-address> <local-port>
```

If the tunnel is working properly you should receive the same SMTP greeting as when executing:

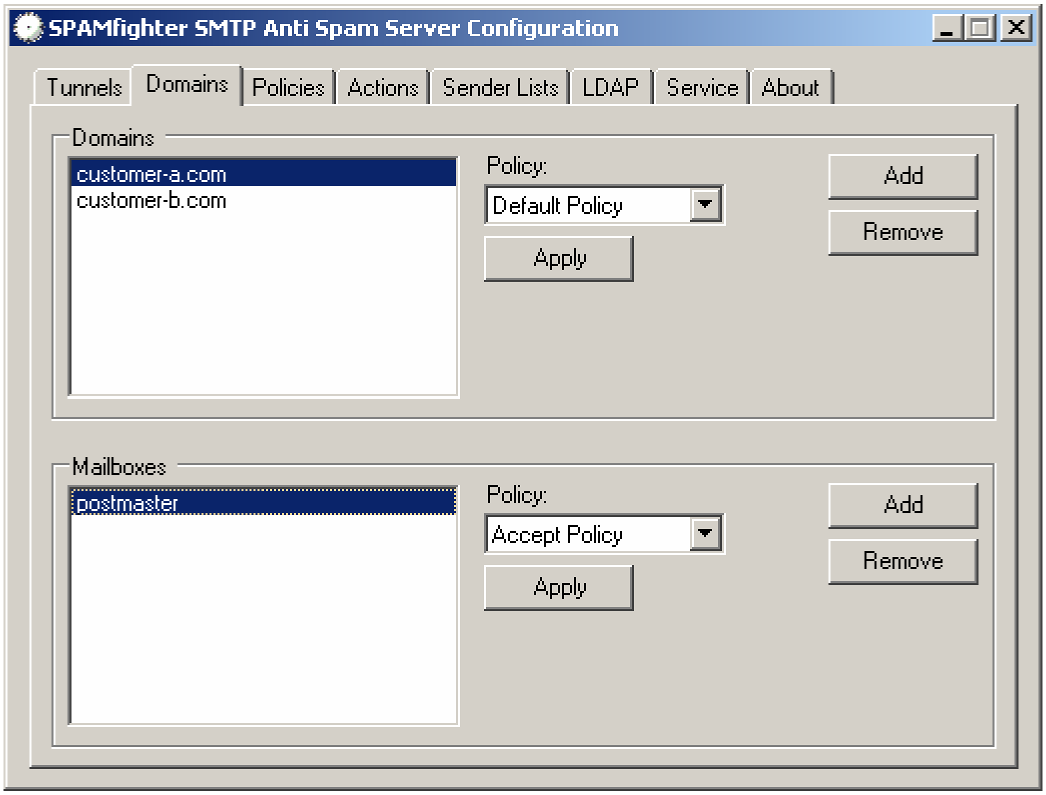
```
telnet <remote-address> <remote-port>
```

If you do not receive a greeting when executing either of the commands, make sure that the SMTP service is running on the destination server.

If you receive a greeting when connecting to the remote endpoint, but not the local endpoint make sure that the Filter application is running. If the Filter application is running but you are still unable to get the greeting, check the Server.log.txt log file in the installation directory for errors.

5.2 Domains and Mailboxes

A filtering policy is defined per domain (or mailbox where required). See the following chapter for information about policies.



Domains

customer-a.com
customer-b.com

Policy: Default Policy

Mailboxes

postmaster

Policy: Accept Policy

Once a policy has been defined for a domain, all mailboxes associated with the domain will automatically inherit it. Exceptions to this inheritance are defined in the Mailboxes list.

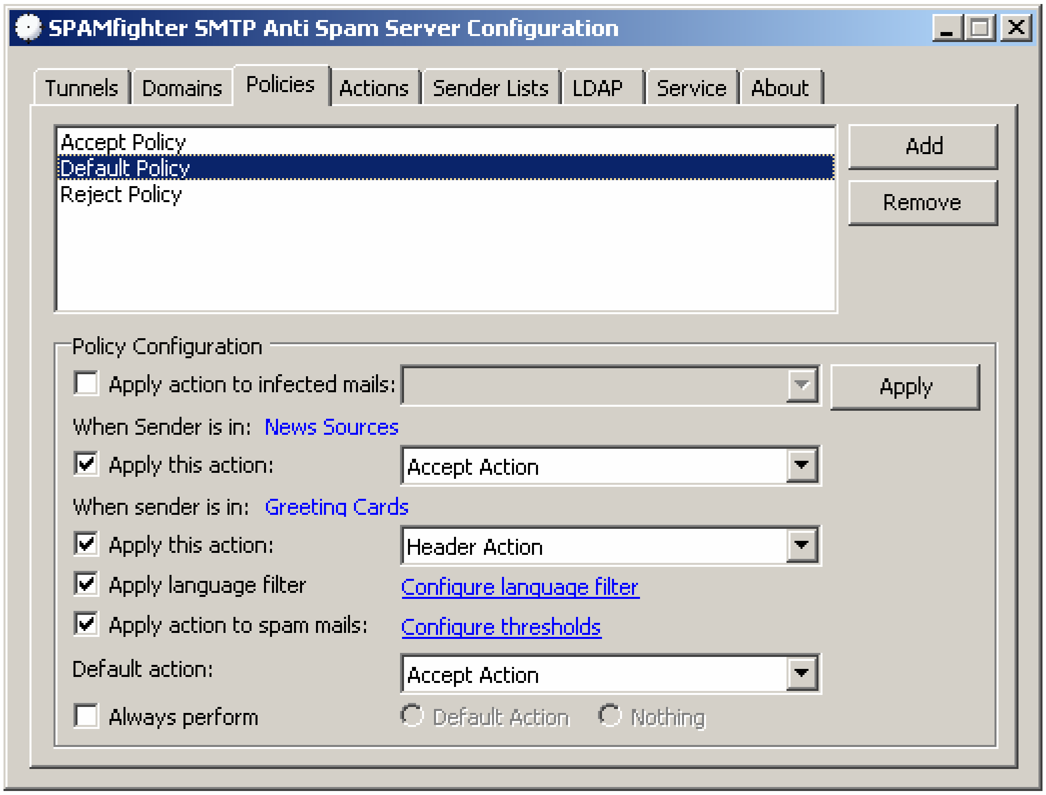
The “`postmaster`” mailbox should always be assigned a policy which delivers all emails.

The “`*`“ wildcard can be used to define a policy for all other domains than those explicitly specified.

Only a single policy can be active in a SMTP transaction. It is therefore important to limit the number of different policies used across a domain. Please refer to the “Tunneling Details by Example – Policy Selection” chapter for more details on this.

5.3 Policies

A policy contains information about what action to execute when certain criterias are met:



Accept Policy
Default Policy
Reject Policy

Policy Configuration

□ Apply action to infected mails:

When Sender is in: News Sources

☑ Apply this action: Accept Action

When sender is in: Greeting Cards

☑ Apply this action: Header Action

☑ Apply language filter — Configure language filter

☑ Apply action to spam mails: — Configure thresholds

Default action: Accept Action

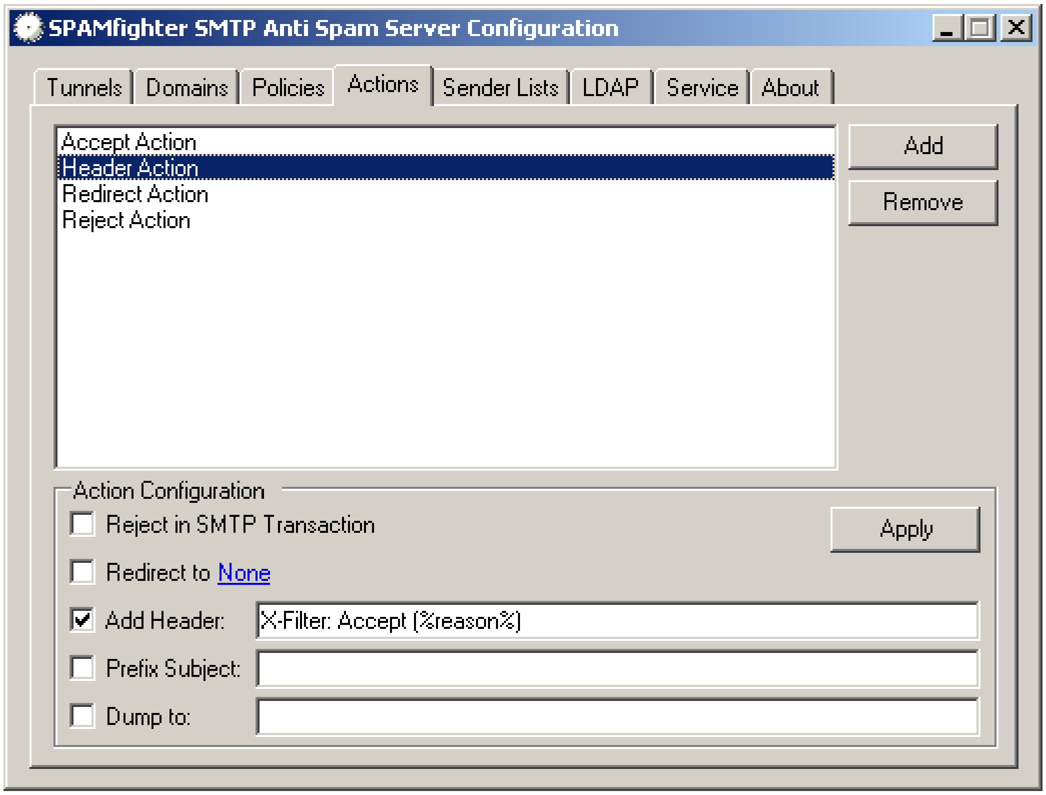
□ Always perform ○ Default Action ○ Nothing

A policy can be configured to always execute the action. This is useful in creating permanent redirects or rejections for certain mailboxes at the filtering level.

Black- and whitelists are also part of the policy: both are made up of sender lists. In this way a number of well-defined lists can be maintained easily and used in different policies.

5.4 Actions

The Filter can be configured to perform a number of actions when triggered by a policy. Policies determine when a given action is executed as described in the previous chapter. A single action can perform multiple operations, i.e. modify the email header and redirect the message.



Accept Action
Header Action
Redirect Action
Reject Action

Action Configuration

☐ Reject in SMTP Transaction

☐ Redirect to None

☑ Add Header: X-Filter: Accept (%reason%)

☐ Prefix Subject:

☐ Dump to:

5.4.1 Reject

Once the action is executed, the Reject operation will issue a SMTP error response to the "DATA" command:

```
    554 Transaction Failed; Rejected by Content Filter
```

Since this will terminate the SMTP transaction, the email will never be forwarded to the destination server. For further details please refer to the "Tunneling Details by Example" chapter below.

Due to the nature of the reject operation, other operations can never be performed in the same action.

5.4.2 Redirect

The redirect operation is capable of redirecting an email to multiple recipients on multiple domains. Since the redirected message is still delivered directly to the destination server, it must assume responsibility for the delivery and accept emails for the specified domains and mailboxes.

The redirect operation uses a simple yet powerful rewriting engine. The user specifies a set of rewrite patterns, which are processed for each for the original recipients.

The engine supports two variables which are replaced at execution time:

Variable Name	Description
%domain%	The domain part of the recipient email address
%mailbox%	The mailbox part of the recipient email address

If the redirect operation is configured with these rewrite patterns:

```
spam@%domain%
spam.%mailbox%@%domain%
spam@spam-reporting-authority.net
```

And the redirect operation is executed on a SMTP transaction with these recipients:

```
joe@bar.com
honey@n42.net
```

Then the redirect operation will rewrite the recipients to:

```
spam@bar.com
spam@n42.net
spam.joe@bar.com
spam.honey@n42.net
spam@spam-reporting-authority.net
```

The rewrite engine will remove any duplicate addresses generated by the operation. For backwards compatibility the rewrite pattern “address” is translated to “address@%domain%”.

5.4.3 Header Insertion

The specified header field is added to the email header. The variable %reason% will be replaced with a description of why the action was executed. For instance:

%reason%	Description
Spam: <probability>%	Message was classified as spam
Infected: <virus>	Message contained an infected attachment or part
Whitelisted	Sender was whitelisted
Blacklisted	Sender was blacklisted
Neutral	Message was clean

5.4.4 Subject Prefixing

When the action is executed the subject prefix operation simply adds the specified text to the beginning of the subject header. If no subject header exists one is created.

5.4.5 Dump Message

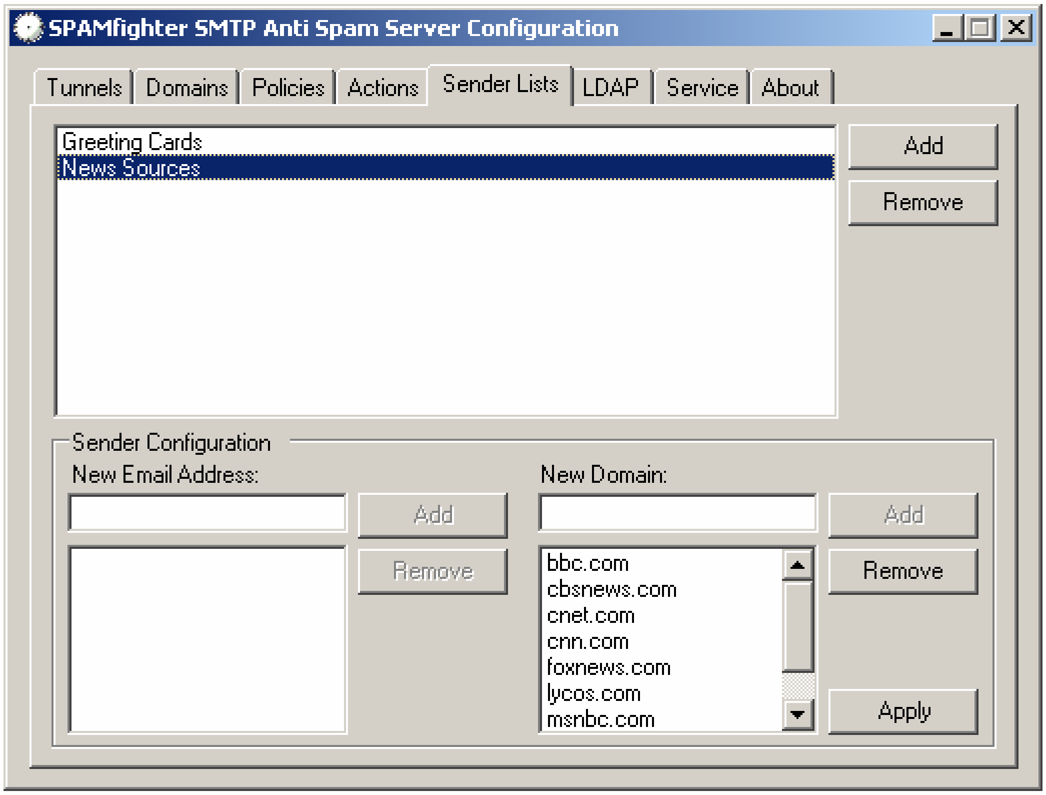
The message will be written to the local file system using a unique file name. The file name will be logged in the tunnel log file.

In the “Dump to:“ field you should enter the directory which you wish to store the dumps in.

5.5 Sender Lists

Each sender list is a user-defined grouping of senders. Good examples of such groupings could be “Newsletters”, “Greeting Cards”, “Business Partners” etc.

A list can contain both domain names as well as email addresses:



Greeting Cards
News Sources

bbc.com
cbsnews.com
cnet.com
cnn.com
foxnews.com
lycos.com
msnbc.com

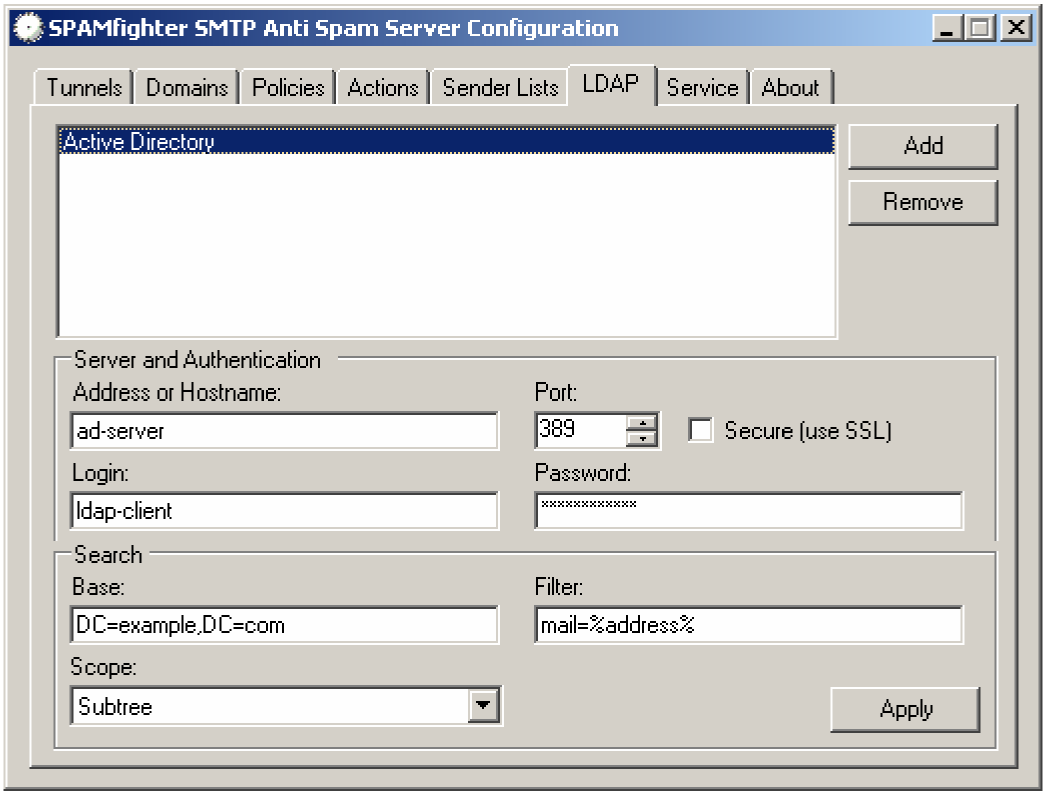
The lists are combined in a policy to form black- and whitelists.

5.6 LDAP Recipient Address Validation

Some destination servers (such as Exchange 5.5, 2000) and antivirus gateways are unable to perform recipient address validation during SMTP transactions. They simply accept the message and generate a Non-Delivery Report (NDR) if they determine that the recipient address is invalid or unknown.

The lack of timely recipient address validation causes wasted server resources and skewed statistics.

Fortunately, an LDAP profile can be associated with a tunnel to provide this validation.



Active Directory

Server and Authentication

Address or Hostname: ad-server

Port: 389

☐ Secure (use SSL)

Login: ldap-client

Password: ************

Search

Base: DC=example,DC=com

Filter: mail=%address%

Scope: Subtree

The search base is typically the distinguished name (DN) form of the domain name. The search filter supports these parameters:

Variable Name	Description
%address%	The full recipient email address
%domain%	The domain part of the recipient email address
%mailbox%	The mailbox part of the recipient email address

6 Security Considerations

6.1 Relaying

Special attention should be paid while deploying the Filter. Due to the tunneling, all traffic originating from the Internet will appear to come from inside the internal network (from the perspective of the destination server). More specifically it will appear to originate from the Filter server.

As such you should make sure that your destination servers do not allow relaying from the Filter server. Failing to do so will enable relaying for any Internet traffic (thus creating an Open Relay).

6.2 Application Level Security

For increased security the Filter application can be configured to impersonate a user account with restricted privileges.

The installation process will configure the Filter application to impersonate the “LocalSystem” account. Follow these steps to use an alternative account:

1. Create a new user account (e.g. “SMTP Anti Spam Server”)
2. Remove any group memberships for the account
3. Give the user account full control over these locations (including siblings):
    a. Registry: HKEY_LOCAL_MACHINE\Software\SPAMfighter
    b. Registry: HKEY_LOCAL_MACHINE\Software\SPAMfighter Filter Server
    c. File System: The Installation Directory chosen during Installation
4. Locate the “SPAMfighter SMTP Anti Spam Server” service in the Service Control Manager. Go to the “Log On” tab and select the newly created user account.

7 Monitoring and Statistics

7.1 Performance Monitor

The Filter application exposes Performance Monitor Data in an object named “SPAMfighter SMTP Anti Spam Server”. A number of real-time counters are available.

7.2 Log Files

Once the Filter application is run for the first time (either in console mode or as a service) a server log file named “Server.log.txt” is created in the installation directory.

In addition a subdirectory named “`Logs`” is created. This directory will contain traffic logs for each tunnel, each named “`tunnel-name.log.txt`”. This is referred to as the “live” log for a tunnel. Live log files are locked when the Filter application is running but allows read-only access.

Once a live log file exceeds 128 megabytes in size it will be archived as “`tunnel-name.timestamp.log.txt`”, and a fresh live log file will be created. The archive log file lock is released by the Filter application thus allowing the file to be moved to alternate storage (for backup purposes etc.).

7.3 Statistics

All domain and mailbox statistics are stored in the registry and reported back to a central licensing system.

All statistics are available through a web interface. You’ll receive an email containing a link to the system once the installation has completed.

It is possible to give external users access to the statistics (or parts of the statistics). Thus, in a hosting center setup, customers can get access to their own statistics.

8 Tunneling Details by Example

In the example below the Filter accepts mail for domains “`bar.com`” and “`n42.net`”. The Filter is configured with different policies for the two domains.

Notice the distinction between the “filtering policy” (enforced by the Filter) and the “delivery policy” (enforced by the destination server).

8.1.1 Initiation

The session is initiated once the client (originating server) connects to the Filter. The Filter will then establish a tunnel between the client and the destination server by connecting to the server and acting as a proxy:

Direction	Data	Description
Client → Filter		Client connects to Filter
Filter → Server		Filter establishes Tunnel
Client ← Filter ← Server	220 bar.com Ready	
Client → Filter → Server	EHLO foo.com	
Client ← Filter ← Server	250-bar.com Hello 250-8BITMIME 250-PIPELINING 250 HELP	

8.1.2 Policy Selection

The Filter will determine the filtering policy of a transaction by using the recipient addresses. These addresses are validated by the server before the filtering policy is locked:

Direction	Data	Description
Client → Filter → Server	MAIL FROM: <joe@foo.com>	
Client ← Filter ← Server	250 OK	Filter locks sender
Client → Filter	RCPT TO: <smith@bar.com>	Filter resolves filtering policy
Filter → Server	RCPT TO: <smith@bar.com>	Server checks delivery policy
Client ← Filter ← Server	250 OK	Filter locks filtering policy

Only a single filtering policy can be active for any given transaction. The Filter will detect a policy conflict and respond with a temporary error, causing the client to retry later:

Direction	Data	Description
Client → Filter	RCPT TO: <jane@n42.net>	Filter resolves filtering policy
Client ← Filter	451 Policy Conflict	Filter detects a policy conflict

The server is still responsible for performing recipient address validation. Hence the Filter does not need to know about each mailbox attached to a domain:

Direction	Data	Description
Client → Filter	RCPT TO: <john@bar.com>	Filter resolves filtering policy
Filter → Server	RCPT TO: <john@bar.com>	Server checks delivery policy
Client ← Filter ← Server	550 Unknown User	Server detects a delivery conflict

8.1.3 Data Interception

The Filter will buffer the message data to delay its delivery to the server. The message data will only be delivered to the server if the transaction passes the filtering policy:

Direction	Data	Description
Client → Filter	DATA	
Client ← Filter	354 Go Ahead	
Client → Filter	<Message Data>	Filter buffers the message data

During interception the Filter will issue periodic "NOOP" commands to the server to keep the session from timing out.

8.1.4 Policy Enforcement

If the transaction is accepted it is forwarded to the Server:

Direction	Data	Description
Filter → Server	DATA	
Filter ← Server	354 Go Ahead	
Filter → Server	<Message Data>	
Client ← Filter ← Server	250 Message Saved	Server accepted message data

If the transaction is rejected by the filtering policy a policy action will be enforced. One such action might be to modify the message header and still forward it to the server.

An action might also be configured to reject the message:

Direction	Data	Description
Client ← Filter	554 Content Rejected	

Or redirect the message to a predefined mailbox, in this instance <spam@bar.com>:

Direction	Data	Description
Filter → Server	RSET	Reset transaction
Filter ← Server	250 OK	
Filter → Server	MAIL FROM: <joe@foo.com>	
Filter ← Server	250 OK	
Filter → Server	RCPT TO: <spam@bar.com>	Server checks delivery policy
Filter ← Server	250 OK	
Filter → Server	DATA	
Filter ← Server	354 Go Ahead	
Filter → Server	<Message Data>	
Client ← Filter ← Server	250 Message Saved	Server accepted message data

8.1.5 Termination

Direction	Data	Description
Client → Filter → Server	QUIT	
Client ← Filter ← Server	220 Bye	