



VISOLVE

OPEN SOURCE SOLUTIONS

## ViMailFilter

---

# Taking Control of your Emails



## Contents

<b>I</b>	<b>Executive Summary.....</b>	<b>2</b>
<b>II</b>	<b>Introduction.....</b>	<b>2</b>
<b>III</b>	<b>Need for Mail Filter.....</b>	<b>2</b>
<b>IV</b>	<b>What to look for in a Mail Filter?.....</b>	<b>3</b>
<b>V</b>	<b>Spam Filtering Techniques.....</b>	<b>3</b>
	Challenge/Response System	
	Heuristic Filters	
	Collaborative Filters	
	Pattern Filters	
	Bayesian Filtering	
<b>VI</b>	<b>ViMailFilter Overview.....</b>	<b>6</b>
<b>VII</b>	<b>Functionality Description.....</b>	<b>6</b>
<b>VIII</b>	<b>Why ViMailFilter?.....</b>	<b>8</b>
<b>IX</b>	<b>Deployment Model.....</b>	<b>9</b>
<b>X</b>	<b>Conclusion.....</b>	<b>10</b>

## I. Executive Summary

Email is one of the most primary communication channels irrespective of the business nature, size and sector. Unfortunately, email is also one of those tools, if not used properly, could bring in irreparable consequences. In addition, enterprises could face legal issues if it fails to establish a proper email filtering strategy as it is directly liable to the use of emails of its employees.

## II. Introduction

Control of Spam and Virus mails is the critical factor in success of most corporate around the globe. A corporate receives thousands of mails everyday hence finding out the legitimate mail and deleting spam mails becomes a tedious and time consuming process. This also reduces the productivity of the employees.

This whitepaper talks about the technical components of a mail filter - its uses, options and advantages. And, more importantly, how this could help in saving an organization's time, increasing employee's productivity and, above all, blocking spam and virus mails.

## III. Need for mail filter

"SPAM" mail is the practice of sending massive amounts of e-mail promotions or advertisements (and scams) to all the people including the ones who have not asked for it. Spam is an unsolicited e-mail on the Internet. Spam floods the inbox and forces the users to spend time and effort purging unwanted mail to just find one legitimate mail.

Spam mail not only floods our inbox it also transmits viruses, adware, malware, spyware and cripples the servers and desktop machines. Spam also eats up a lot of network bandwidth. All these problems can be overcome by using Mailfilter. Hence there comes a need for the Mailfilter software.

MailFilter is used to overcome the challenges faced due to Internet Bandwidth, Performance, Monitoring & Control.

- World Wide Web becomes a global-scale data dissemination system which in turn causes traffic overload at data sources.
- Unwanted email transmitted over the same network again and again, which increases corporate IT spending.
- Unrestricted and unmanaged mails flooding the employee's inbox can lead to dire consequences in the form of wasted time and loss of productivity.
- Unsolicited mails, spam and virus affects the network and reduces the employee productivity.

#### IV. What to look for in a MailFilter?

**Main Features** - The features would be to set up blacklist, white list, grey list and how mail filter works with any mail client.

**Ease of Installation & Setup** - The software should be error free and easy to install. It should provide a user friendly GUI for installation and setup.

**Ease of Use** - The software should be very easy to use and should provide online help options.

**Cost Effectiveness** - MailFilter software should be priced at an affordable rate.

**Customization** - The MailFilter software should be easily customizable and offer levels of filtering.

**Stability** - The Mailfilter software should be compatible with other programs and has to be consistent in performance.

#### V. Spam Filtering Techniques

##### ***Challenge/Response System***

Filters that use a challenge/response system block undesirable emails by forcing the sender to perform a task before their message can be delivered. For instance, if you send an email to someone who's using a challenge/response filter, you'll likely receive an email right back that asks you to visit a Web page and enter the code displayed there into a form. Only after successful completion of this task, your email (and all future emails) will be delivered to the recipient. If you don't complete the challenge after a certain time period, the message is rejected.

This system works to fight spam because the "challenge" is typically only one that a human can solve. Spammers usually rely on automated mailing programs to send out millions of emails at once, and they rarely check to see what emails come back in response. And even if they did see a challenge message, they aren't likely to respond and risk revealing themselves as a spammer.

However, challenge/response filters might also block email newsletters you subscribe to, as these messages are typically sent by automated programs. Another downside is that some of your organization's constituents may not take the time to complete the challenge or may not understand the challenge email, meaning that their messages will not reach the recipient. And there's always the slight chance that if both the sender and recipient are using challenge/response systems, their anti-spam applications will continue to challenge each other, locking the email in an undeliverable loop.

### ***Heuristic Filters***

Heuristic (or rule-based) filters take things a step beyond simple word-based filters. Rather than blocking messages that contain a suspicious word, heuristic filters take multiple terms found in an email into consideration.

Heuristic filters scan the contents of incoming emails and assigning points to words or phrases. Suspicious words that are commonly found in spam messages, such as "Rolex" or "Viagra," receive higher points, while terms frequently found in normal emails receive lower scores. The filter then adds up all the points and calculates a total score. If the message receives a certain score or higher (determined by the anti-spam application's administrator), the filter identifies it as spam and blocks it. Messages that score lower than the target number are delivered to the user.

Heuristic filters work fast — minimizing email delay — and are quite effective as soon as they have been installed and configured. However, heuristic filters configured to be aggressive may generate false positives if a legitimate contact happens to send an email containing a certain combination of words. Similarly, some savvy spammers might learn which words to avoid including, thereby fooling the heuristic filter into believing they are benign senders.

### ***Collaborative Filters***

Collaborative content filtering takes a community-based approach to fighting spam by collecting input from the millions of email users around the globe. Users of these systems can flag incoming emails as legitimate or spam and these notations are reported to a central database. After a certain number of users mark a particular email as junk, the filter automatically blocks it from reaching the rest of the community's inboxes.

When a collaborative content filtering system involves a large, active user base, it can quickly quell a spam outbreak, sometimes within a matter of minutes. One potential downside to the collaborative-content method is that if a group of spammers mobilize in large numbers and pretend to be legitimate users of the system, they could skew results by falsely labeling spam emails as legitimate messages.

### ***Pattern Filters***

A basic spam filtering technique scans messages for suspicious words or patterns. This technique is effective if the filter is looking for the right word. But spammers, in a bid to outwit these filters, are constantly altering the spelling of key terms or finding new euphemisms for body parts. A good pattern filter would not only catch "prescription," but also to the word "prescr1pt10n" without the user needing to enter that particular combination of letters and numbers.

A good pattern filter should allow you to define your own patterns, and to remove the ones that causes an undue number of false positives for your company. These filters have their role, but their effectiveness directly depends on how frequently they are updated with the latest spam terms. They also can block legitimate mail if a "bad" word is in it. Use pattern filters, but they shouldn't be your first line of defense.

### ***Bayesian Filtering***

Bayesian filters, considered the most advanced form of content-based filtering, employ the laws of mathematical probability to determine which messages are legitimate and which are spam. In order for a Bayesian filter to effectively block spam, the end user must initially "train" it by manually flagging each message as either junk or legitimate. Over time, the filter takes words and phrases found in legitimate emails and adds them to a list; it does the same with terms found in spam.

To determine which incoming messages are classified as spam, the Bayesian filter scans the contents of the email and then compares the text against its two-word lists to calculate the probability that the message is spam. Because a Bayesian filter is constantly building its word list based on the messages that an individual user receives, it theoretically becomes more effective the longer it's used. Bayesian filters can also require more processing power and more time to analyze messages.

Bayesian filters are very powerful and are regarded as one of the most accurate techniques for blocking spam. Among the various types of filtering techniques most reports says that Bayesian filters have shown accuracy of over 99% when the filter has been "well trained".

### VI. ViMailFilter Overview

ViMailFilter is a platform-independent Open Source based Mail Proxy server that provides white-lists and filtering rules to quarantine spam and block virus emails. It is characterized by two key features that are the hallmark of any antispam control product – It stops spam and virus emails before they get to your mail server, and equally importantly, it learns from and adapts to the site's incoming email patterns.

[ViMailFilter = SMTP Proxy + Spam & Virus Filter + Live Reports \(GUI\) + Support](#)

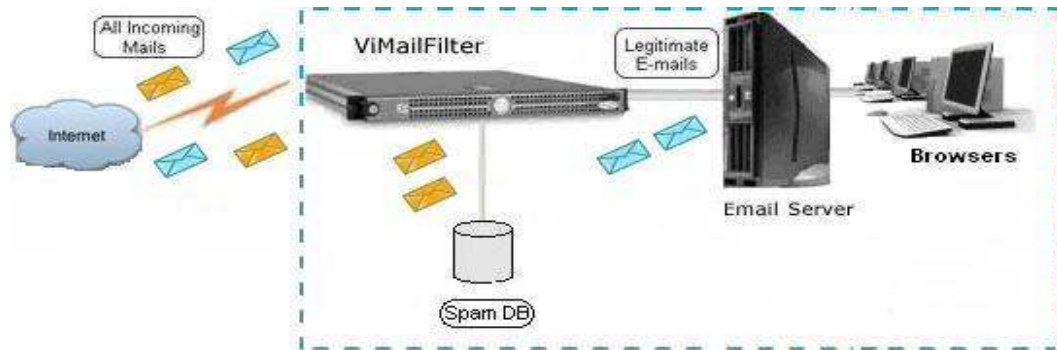
ViMailFilter works with any mail transport, and is easy to manage in an operator-less environment. The more you train your spam DB using correct spam and non-spam mails, the better the product will filter spams.

### VII. Solution and Service

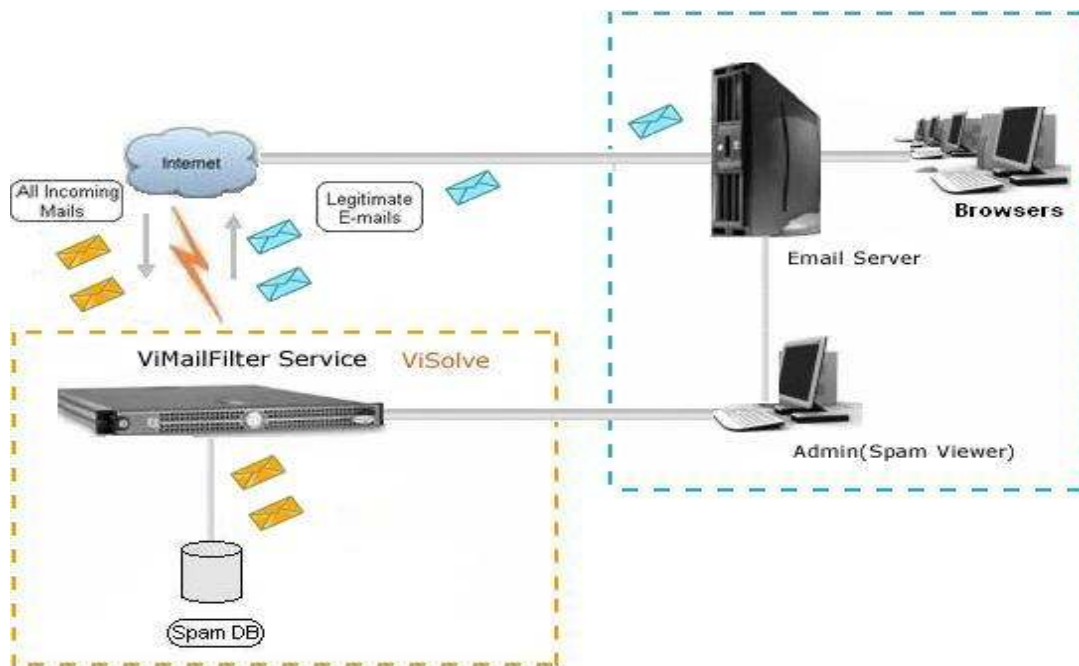
Based on the customer requirements ViMailFilter can be used as a solution or as a service. As a solution ViMailFilter can be deployed at the customer environment i.e., at Client's MailServer or as a service it can be deployed at ViSolve environment ie it can be outsourced from ViSolve's network for continued maintenance.

# Taking Control of your Emails

The image shows ViMailFilter as a solution – Deployed at Customer Environment



The image shows ViMailFilter as a service – Deployed at ViSolve Environment



### VIII. Functionality Description

ViMailFilter can be configured easily based on whitelist, blacklist, Redlist and Greylist. The users can specify and categorize their mails based on their preferences. Customized policies like allowing/blocking any particular user can also be done using ViMailFilter.

ViMailFilter filters incoming Mails based on IP, Domain, Email ID and content. Therefore, customers have the choice to choose their preferred filtering method. ViMailFilter has a unique Content based filtering feature which can filter mails based on subject, Regular expression, Keywords, attachments etc. Spammers often send spam in the form of attachments so this can be avoided very easily using ViMailFilter. ViMailFilter can be configured based on the users needs. Hence ViMailFilter offers rule customization and over riding rules of whitelists and blacklists is also possible.

ViMailFilter uses Bayesian Filtering technique and hence there is a need to train the DB to obtain efficient results. Most of the organizations would like to know the count on the number of spam being blocked and hence ViMailFilter offers graphical reports through which the manager / lead of the team can view the email received for their respective team, the number of mails blocked as spam etc.

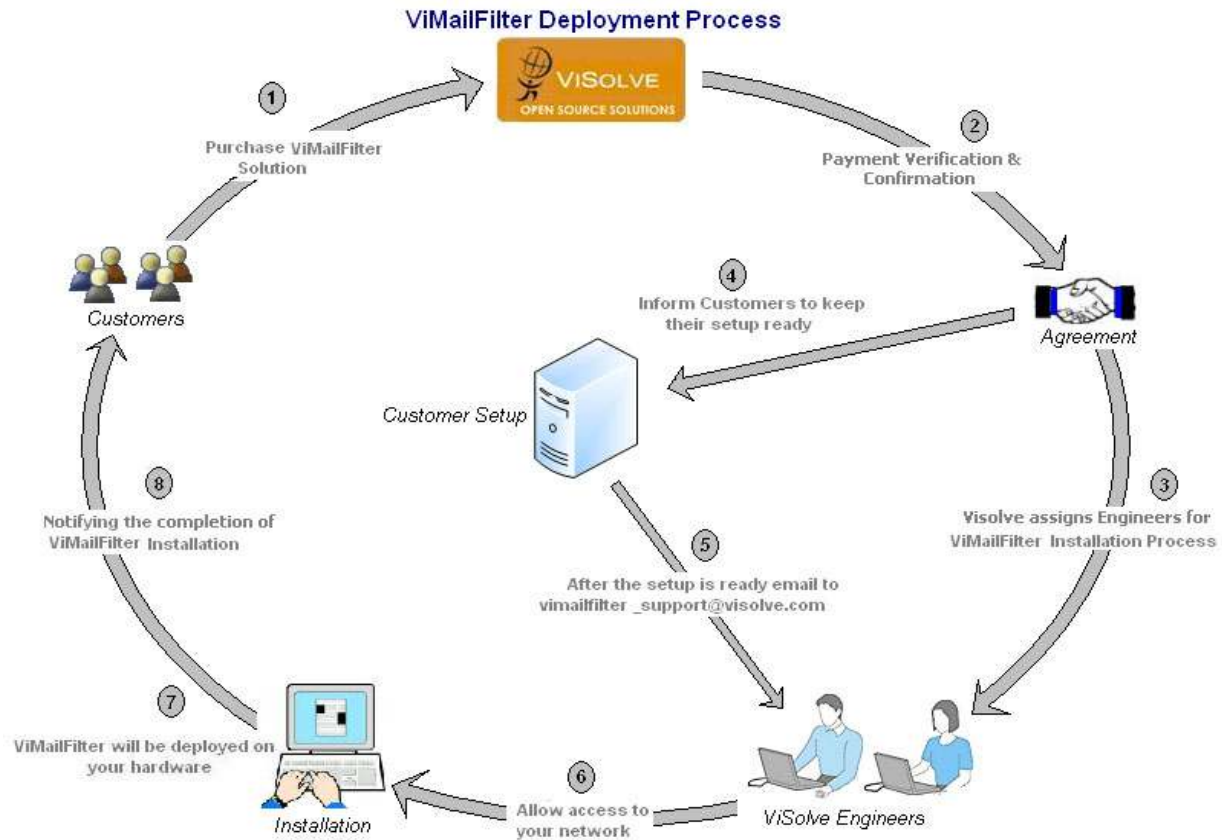
ViMailFilter has automatic update of spam and virus database. ViMailFilter can be easily deployable in any Linux platform. These are few of the standout functionalities of ViMailFilter.

### IX. ViMailFilter Advantages?

- ViMailFilter can be deployed either as a solution or as a hosted service
- Saves your time and bandwidth by blocking "Spam / Virus" mails at connection level.
- Easily deployable in few minutes ie you provide the hardware and we deploy the solution.
- Co-existence with your existing mail server.
- Automatically updates "Spam/Virus" database.
- Provides browser based administration with live and historical customized reports.
- Allows the user to plug and play with your existing network environment.

## X. Deployment Model?

ViMailFilter deployment process has been depicted in the below image.



The various steps involved in the deployment process are

**Step 1 :** Customers purchases ViMailFilter solution.

**Step 2 :** Customer receives a confirmation email from ViSolve once the order has been processed.

**Step 3 :** ViSolve assigns consultant/engineer for the installation process of ViMailFilter.

## Taking Control of your Emails

**Step 4 :** ViSolve informs customers to keep their setup ready. The list of required software components are given in the Install/Conf ViMailFilter document.

**Step 5 :** 'Email' and "IM" will be the primary modes of communication. After the setup is ready the customer emails their IM id to [vicemailfilter\\_support@visolve.com](mailto:vicemailfilter_support@visolve.com). The assigned ViSolve consultant/engineer will also be in touch with the customer via other means (telephone, fax) as necessary.

**Step 6 :** Once the deployment base has been setup, customer provide us with a web-access document which should contain the physical and logical network diagram of the current (and the proposed) setup. This is to enable our support engineers to meet the customer needs and to provide a customized solution. Then the customer allows us to access their network to install and configure ViMailFilter.

**Step 7 :** ViMailFilter will be deployed on your hardware.

**Step 8 :** ViSolve engineers will email you once the installation is completed.

### XI. Conclusion

Spammers use various spamming tricks and are trying to bypass anti-spam techniques by changing the methods they used to send spam. Its best for coporates to protect themselves with a mail filtering solution that uses advanced spam blocking technique. Hence by using an advanced MailFilter solution would provide a solution to spam and thereby save time, increase the productivity and safeguard the network resources of the organization.

### About ViSolve

ViSolve is a software consulting and support organization focused on providing value-added solutions largely through open source products and technologies. We deliver scalable and cost-effective solutions/services in **Networking and Security, Internet Caching (Squid), Databases (MySQL) and Web Applications (JBoss)** with immediate and measurable business values.

Our knowledge and experience in a variety of platforms and technologies combined with our strong understanding of business processes enables us to implement comprehensive solutions/services you need to achieve your goals. ViSolve is committed to helping you get the most from your IT investments by offering 7x24 commercial support and services to your business. Our Source initiative will be an advantage to boost up your market potential.