IT-Security
Firewall & VPN
Managed Services
Secure Server
Spam- & Virenschutz

Electronic Service Center

SpamFix

technical whitepaper

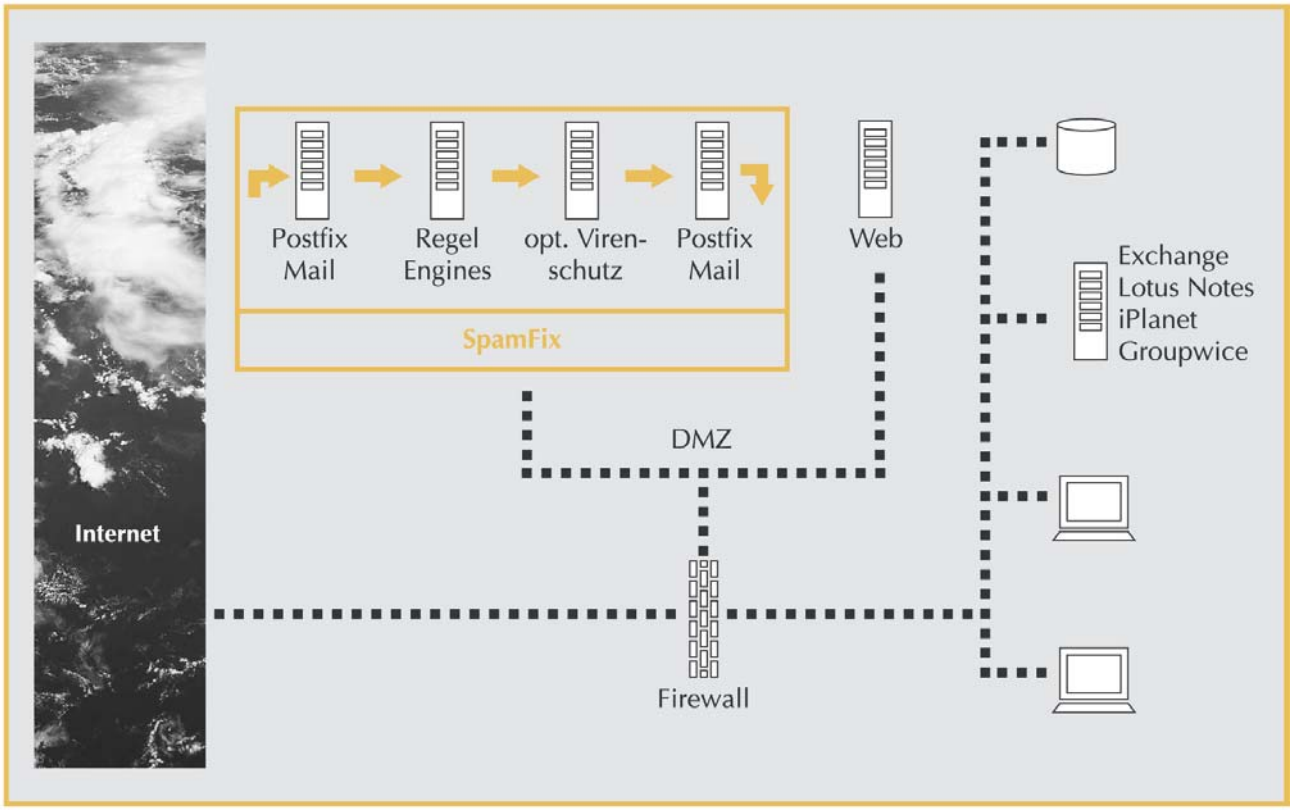
ESC – Electronic Service Center
Schulstr. 13, 06108 Halle (Saale)
Germany
Tel: +49 - 345 - 55844 0
Fax: +49 - 345 - 55844 99
Mail: info@esc.de
Web: www.esc.de

A professional anti-spam solution

Spamfix is an extensive, flexible solution for the recognition and treatment of unwanted e-mail, so-called spam. SpamFix can be adapted to individual and special needs of a particular company or institution, or even specific departments.

SpamFix is placed logically as mail-relay between the Internet and the internal mail server and thus is a transparent addition compatible with nearly all mail servers. Spam recognition is based on several procedures combined by various individual evaluations. Common rules from public databases are in use for these procedures as well as relevant up-to-date findings from the SpamFix service team overlooking and controlling numerous SpamFix solutions. These measures can be further extended by rules generated both manually or automatically from the company's or employee's individual e-mail without compromising confidentiality.

SpamFix is a fully integrated solution delivered individually configured and ready-to-use on the chosen hardware. SpamFix operates on Sun Sparc computers with Solaris, as well as on appliance and server systems (Intel, AMD) with a specially hardened Linux configurated according to ESC's regulations for security solutions (Firewalls, VPNs, Viruswalls etc).



Spam recognition using Bayes-Classification

SpamFix combines several classification and discovery methods of which the so-called Bayes-Classification plays a major role. This statistical-heuristic process calculates the probability of an e-mail's contents being wanted or unwanted. It uses previously programmed lists of words as well as word frequencies. Bayes-Classification makes use of data from public databases (findings of the open-source community) as well as data from SpamFix databases in which especially thorough rules for the positive classification of e-mail are constantly updated.
In addition, SpamFix has individual Bayes-Databases which can be extended by manually adding wanted or unwanted e-mails. This training is best conducted through the use of non-recognised spam e-mails (so-called false-negatives) and with e-mails falsely recognised as spam (false-positives).
The Bayes-Classification also learns automatically: if an e-mail exceeds a certain spam threshold, the e-mail is analysed and stored automatically as new spam for the improvement of spam recognition. If an e-mail falls significantly below the given thresholds, it automatically is stored and improves recognition of 'wanted e-mail'.

Spam-Fix Service

The solution is delivered to the customer installed and configured ready-to-use and is integrated in the corporate network. SpamFix is operated at the location of the customer and is administered, monitored and controlled remotely through protected connections by ESC. For this service, we offer various options and reaction times. The continuing care as well as ongoing development of rules and procedures are essential in order to guarantee long-lasting security and constant high spam recognition rates.
Following service options are always included in SpamFix service:

- SpamFix software care: The solution exists in up to four main components and about 30 necessary submodules which are constantly improved. These components are updated on a regular basis.
- Security patches for the operating system: For long-lasting security, the care and updating of the operating system and its necessary components is essential.
- Administration and Configuration: Basic administration service and configuration, such as changes on demand are also included in SpamFix service.
- Learning phase: As detailed above, SpamFix learns automatically from received e-mails. This learning phase is significantly more efficient, when SpamFix is trained manually in the introductory phase with common spam mails and common customers' 'wanted e-mails'. During this phase, individual preferences for alerts and notifications can also be installed.
- Rule improvement and thresholds' adaptation: Within the SpamFix service, we are constantly working on the optimisation of rules and their evaluation in order to increase the recognition rate. These improvements are implemented instantly.
- Spam observation and correlation: The methods of spam senders are getting increasingly smarter. This requires the fastest possible reaction. We are constantly developing and testing new rules and filter methods. As soon as those methods prove to be robust and reliable, they are made available to all SpamFix solutions within our service.

Maximum Reliability and Data Protection

Many anti-spam solutions demand the roundabout way via the server of a service provider. This violates confidentiality since the e-mails are saved, edited and processed out of any realms of control of the customer.
SpamFix is installed at the customer's location in its network and does only transfers analysis data retrieved from e-mails recognised as spam (this data is used by ESC in order to incorporate them in a

central Bayes-Database for further development purposes). All e-mails themselves stay on the local server and thus within customer's control. Even the local data from analysis of 'wanted e-mail' recognition remains at the customer to exclude even the very remote possibility that this data could allow conclusions about the e-mails' contents.
For additional or specific optimisations there is the possibility of deliberately sending extraordinary e-mails to ESC which we can check against rules of the SpamFix solution. So all our customers benefit from findings derived from all spam e-mails received without even remotely violating the confidentiality of our customers' e-mail traffic.

Integration

SpamFix is typically placed directly in a DMZ (demilitarized zone). In order to make quick and seamless integration easier only the standard routing of port 25 to the SpamFix mail relay is changed on the router or gateway. A change of MX entries or similar changes which would demand integration of external devices or services is not necessary. The SpamFix mail relay passes e-mail to the previous mail server after classification.

Optional: Virus Protection

ESC has successfully integrated protection against viruses, worms, trojan horses and other 'pests' for years. Especially the product TrendMicro Interscan VirusWall has been operated with very positive results. For this product as well as other security services, ESC offers very comprehensive and reliable managed services.
TrendMicros Interscan VirusWall can optionally be integrated directely into the SpamFix solution and it can be serviced, monitored and controlled by ESC as part of the continuous SpamFix service.
SpamFix itself, however, also offers the integration of almost all virus scannes available. For particular security relevant applications, SpamFix can also incorporate multiple virus scanners on demand to check e-mail traffic at a very high standard.

Platforms:

- Sparc server from Sun Microsystems with Solaris
- Linux server from Sun Microsystems with Linux (security-hardened)
- Appliance platforms from ESC (Intel, AMD) with Linux (security-hardened)
- ESC server (Intel, AMD) with Linux (security-hardened)
- For very high demands load balancers (such as Alteon) or round-robin-DNS can be installed to distribute load and increase availability and security

Constant observation of hardware and procedures as well as instant reaction to disturbances and their correction is part of ESC's Managed Services for hardware and operating system.

Product Characteristics

- **Quality assurance**: E-mails are not deleted, but labelled as spam and users can automatically filter or sort them with common mail clients and thus also regularly check if necessary.
- **Filters**: E-mails classified as spam can be directly refused. The sender can be sent a reply which can contain further explanations as an option.
- **Plausibility**: E-mails sent to non-existent recipients can be directly refused at the external mail-relay, avoiding so-called 'bounce' e-mails.
- **Checking**: E-mails can be checked for RFC-conformity and can be refused directly. Limited and strictly RFC-conforming SMTP avoids not permitted or unwanted access, such as relay hijacking and misuse. E-mails from unknown or non-existent sender domains can be refused directly.
- **Performance**: SpamFix is based on high performance scaleable server processes for the efficient incorporation of all components as well as one or more virus scanners.
- **Further functions and options**: All known processing options for e-mail, such as alias, distribution lists, virtual domains, mailer tables etc are possible with SpamFix or can be optionally installed in addition to the already existing functions.

Technical Basis and Procedures

- **Security**: All processes run in a secure Unix-Chroot environment. SSL-authentification for SMTP is possible. High-level protection against buffer overflow and similar attacks by use of the Perl programming language.
- **Checks and Evaluations**: A number of sample comparisons and heuristic tests for the entire e-mail. Every rule assigns points that are added up for each e-mail to determine its final classification grade. From a specific threshold at the customer's choice , the e-mail is classed as spam.
- **Bayes-Classification**: Heuristic probability analysis for spam and wanted e-mail based on previous, latter, and present mail analysis.
- **Auto learning**: The Bayes-Databases are automatically trained with the content of e-mails which were classified at very high or very low threshold levels.
- **Blacklists and databases**: Blacklists of unsecured mail relays (e.g. from mail-abuse.org or ordb.org) or external databases with spam signatures (e.g. razor or DCC) can be included in spam evaluation and then are checked automatically.
- **Whitelists and auto whitelisting**: Whitelists with known senders can be generated manually or automatically using classifications with very high probability.
- **Extendable**: All rules, evaluations and thresholds as well as all notifications etc are easily editable and extendable.

Flow Chart

This flow chart clarifies the procedure of mail processing within the individual components of the SpamFix solution. Each e-mail is received by the external postfix mail transfer agent (MTA) from the Internet and already there undergoes a series of plausibility checks. Only with clearance is it passed on to the Amavisd-New daemon process.

Amavisd-New comprises the results of e-mail classification by databases supporting rules for content evaluation and checks every e-mail with a series of complex tests for spam or 'wanted e-mail'. If sender or recipient are found in the white- or blacklists or if an e-mail exceeds a particular size no further evaluation is made at this point.

After processing by Amavisd-New, the e-mail can be passed on to local or external virus scanners (e.g. TrendMicro VirusWall). The last step is again the postfix MTA which sends the e-mail to the internal company mail server or users and may retain e-mail in a mail queue if necessary.

In addition to technical administration and continious component care, ESC works constantly on development and optimisation of rules and procedures within the SpamFix service.