

# Spam Firewall

## What is a Spam Firewall?

A spam firewall is a hardware device that sits between your internet firewall and LAN. It is called a "firewall" because it provides data filtering of email packets, and blocks the packets that meet the criteria of "spam". Spam firewalls can also provide anti-virus protection, anti-spyware, anti-spoofing and anti-phishing services, depending on the model you choose. A spam firewall is not designed to protect your network against intruders such as hackers - you will need a regular internet firewall for that.

## How Does a Spam Firewall Appliance Work?

Spam firewalls use a variety of methods for determining what is considered spam and filtering it out. Normally a form of blacklisting is used, which automatically filters out email from known spammy addresses. A whitelist may also be used, which allows the administrator to identify addresses or domains that should never be blocked. Keyword scanning may also be used, allowing the administrator or individual user to block emails containing certain keywords or keyword combinations. A form of message authenticity checking is also normally used to identify valid "from" addresses, check details of the entire SMTP process, or validate legitimate IP addresses. Many spam firewall appliances also use bayesian algorithm filtering, which help the firewall block more spam over time as it "learns" what is considered spam based on message history, user input and other analysis. Incoming message flow filters also look at the number of incoming messages and where they are from, allowing them to quickly spot and stop a sudden barrage of spam emails that have been mass-distributed from the same source. Spam firewalls are very "smart" and good at eliminating the majority of spam email that comes into a network. They are not 100% effective, but many come close.

## Are Spam Firewalls Expensive?

Spam firewall appliances range in price from around \$2000 up to \$20,000 or more, depending on the number of users it needs to protect and features. Many spam firewalls have optional features like antivirus or anti spyware. Spam firewalls need to be kept up to date with the latest data on known spam sites, new algorithms, updated filters, etc... This is normally handled by the firewall manufacturer as an auto-update feature. As with most network appliances, an annual maintenance plan is usually purchased for the purpose of keeping the firewall up to date and performing it's best.

## What About False Positives?

Spam firewall appliances use many sophisticated techniques to identify and block spam, generally with very good success. Because spammers are constantly change their techniques in order to get their junk mail past the latest and greatest spam filtering technologies, spam firewalls must continually monitor patterns and make filtering corrections. Spam firewall manufacturers are also constantly make corrective configuration changes to keep up with the battle against spammers. For this reason, even the best spam firewall is going to filter out "good" mail from time to time. This is called a "false positive", and administrators (and users) must always be on the lookout for this. Most spam firewalls have sensitivity thresholds that can be adjusted by an administrator to help overcome false positives.

A spam firewall appliance is not your typical "set it and forget it" firewall, but the advantage of having such an appliance on your network far outweighs the need for some administrative work. If your organization experiences a lot of spam mail - get a spam firewall and experience the difference!

DJ is a corporate IT Manager and author of the following sites covering information technology topics: Computer Security for Everyone, Save on Phone Service with VoIP, Internet Phone Service - The Future is Here!

Article Source: [http://EzineArticles.com/?expert=Debbie\\_Jacobsen](http://EzineArticles.com/?expert=Debbie_Jacobsen)