



# Anti-Spam

**CIPAFILTER's spam filtering system was designed to provide administrators with a simplified and more effective approach to combating spam and junk e-mail. It targets the way spammers operate with some very innovative technology. The result is a tremendous decrease in required management and a "set-and-forget" product that takes care of your spam without blocking legitimate mail.**

**The anti-spam provides the following features and benefits.**

### Virtually eliminates spam

The engine operates using a unique multi-faceted system that focuses on attacking the major operating methods of most spammers, rather than investigating each piece of mail. This method ensures little or no junk mail is delivered to the end user, keeping all your users happy.

### No management or false positives

CIPAFILTER's anti-spam does not require daily management, logs, quarantines, white-list and black-lists, and other management typically associated with anti-spam products. Instead, rest assured that while much of the spam mail is blocked, you will not have to worry about legitimate e-mails not coming through, therefore eliminating management often found in other systems.

### Compatible with any mail server

Because CIPAFILTER operates as a stand-alone mail relay system, capable of forwarding mail to any SMTP mail server located anywhere, it can be used with any e-mail system.

### Phase 1 – Legitimate Mail Server Verification

When the CIPAFILTER receives e-mail for the first time, it will run through a series of tests, attempting to verify if the sending mail server is without a doubt a legitimate mail server. Most legitimate mail servers pass this stage, and if they do, any e-mail sent is immediately passed through to the user without delay. However, 90% of spammers tend to fail this stage because they are not using legitimate mail servers and/or methods of sending spam.

### Phase 2 – CIPAFILTER's Main Defense Mechanism

This phase is very unique to CIPAFILTER, and has been designed based on the initial concept of attacking the operating methods of 90%+ of the spammers. When a message is received for a unique new sender, specific information is recorded to verify the identity

of the sending server and recipient. If CIPAFILTER does not recognize this information, it is recorded, and a standard temporary unavailable message is generated, essentially pretending that we are too busy to accept the message at this time. After approximately 30-45 minutes, the message returns, is recognized, and is passed through to the next phase.

This phase is very effective at blocking 90% of the spam without ever processing it. This is because many of the spammers use illegitimate methods of sending spam that are not RFC and SMTP compliant. They use dictionary attacks, do not queue and retry mail very often, use black-listed mail servers and dynamic/changing IP ranges, do not have valid DNS entries, do not use software that keeps track of who received the mail, and do not honor unsubscribe requests.

See how different we really are!



*"I just wanted to let you know how pleased we are with the spam filter. Users who were daily being bombarded with spam are receiving virtually none!"*  
- Pleasant Valley Schools, IA

*"The anti-spam feature of the CIPAFILTER has been the most popular technology advance for our faculty and staff in a couple of years. As the technology coordinator, the feature is great because I don't have to tweak it; it just works. For our teachers and other employees, CIPAFILTER has reduced the number of spam emails they receive to about zero. While the filtering and web-reporting components work very well, the spam blocking aspect has earned me the most pats on the back from co-workers."*  
- USD 102, KS



# Anti-Spam

*"Our district has complained literally for as long as I have been a tech director about Spam. After just one week we realized just what a gem we had found. We have not had even one complaint so far this school year regarding Spam. This feature alone was far worth the purchase the CIPAFilter"*

- USD 493, KS

*"The CIPAFilter has really cleaned out our spam messages. My own account went from 60-100 e-mails a day to 5-10 important and useful e-mails being received. I would strongly recommend this product to my surrounding IT people for their schools or business. It is easy to administer and really performs."*

- Eastland School District, IL

These spammers do not get through this stage, while legitimate mail passes right on through. Essentially, an actual block of spam is never enforced, meaning CIPAFilter does not have to keep track of all the logging of what it has done with all the mail. It simply cleverly uses built-in SMTP technology to very effectively combat most spammers' methods of sending spam.

### Phase 3 – Message Analysis Stage

This final phase uses many traditional methods of identifying spam, customized to CIPAFilter's advantage and used in combination with the remaining portions of CIPAFilter. This technology is very effective at identifying remaining spam e-mail without over blocking or using quarantines.

Approximately 10% of the spam reaches this phase, and the majority is identified and does not reach the end-user. CIPAFilter calls this stage "Spam Forwarding", and will forward this spam as tagged mail, either to a separate account, or the administrator may customize based on header information, and either delete and/or forward to each user's spam box. Although 100% of the content of this should be spam, any potential false positives would be part of this phase, and can easily be located.

CIPAFilter has a built-in white-list that typically is only used rarely if a domain is encountered that for some reason does not pass through either phase. Other logging is available to identify other issues with the e-mail system other than the filtering. It is also safe for users to unsubscribe to any mail they still receive.

## Installation

It is very important that the Anti-Spam system is installed properly. Although very simple to setup, it is necessary to have proper forward and reverse DNS entries and ensure there are no firewall rules to the CIPAFilter possibly cause issues.

As always, CIPAFilter can be installed in multiple configuration scenarios. It is recommended to use a Public IP address on the interface used to process e-mail, although it will function behind a NAT firewall with limited possible issues.

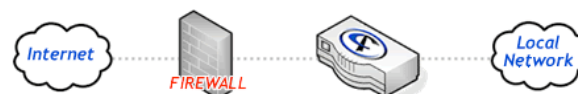
### As Stand-Alone Anti-Spam System



### As Firewall



### As Transparent Bridge



700 16th Ave  
East Moline, IL 61244

1-800-243-3729 ext. 400  
sales@cipafilter.com