

CIPAFilter Whitepaper

Anti-Spam

Revised: 2008-06-26

CIPAFilter's spam filtering system was designed to provide administrators with a simplified and more effective approach to combating spam and junk e-mail. The largest benefit is a tremendous decrease in required management, as well as spam e-mails, without blocking legitimate mail.

The anti-spam provides the following features and benefits.

- **Virtually eliminates spam** – The technology uses a unique three-phased system that focuses on attacking the major operating methods of most spammers, in order to decrease more junk e-mail. This method fights spam e-mail to ensure little or no junk mail is delivered to the end user.
- **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 system, capable of relaying 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 most definitely a legitimate mail server. These tests including various DNS-related inquiries, ensuring the sending system is not being used by a spammer. Many 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 - thereby forcing them to pass through the next phase.

Phase 2 – CIPAFilter "Grey-listing" Process

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, specific information is recorded to verify the identity of the sending server and recipient. Essentially, has this person sent you mail before. 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 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. These spammers do not get through this stage, while legitimate mail servers pass 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.

This is hardly ever noticed by users, since only a very small percentage of legitimate mail will get to this phase, and since mail is only delayed once a user would have to know exactly when the person e-mailed them, the first time only, while communicating with a legitimate mail server that isn't configured correctly.

Phase 3 – CIPAFilter “Spam-Assassin” Process

This final phase uses a highly customized version of Spam Assassin (an open-source software packages that uses many traditional methods of identifying spam). The key difference is that CIPAFilter adds new functionality and a customized scoring system, designed to eliminate false positives and further identify spam messages.

Approximately 10% of the spam reaches this phase, and at least 8% 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. It is uncommon. Other logging is available to identify other issues with the e-mail system other than the filtering.

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.

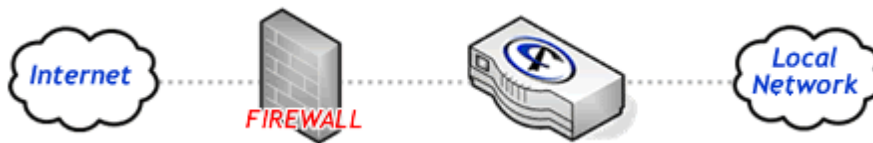
As Stand-Alone Anti-Spam System



As Firewall



As Transparent Bridge



"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 businesses. It is easy to administer and really performs."

- Eastland School District, IL

"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