



More Email. Less Junkmail.

Spam Filter

The PowerElf II spam filter is designed to reduce unsolicited e-mail, by providing full spam protection for incoming mail going to your server. Each feature can be independently enabled or disabled, so you can customize the filter to suit your needs.

PowerElf II Anti-spam features:

Powerful new anti spam engine (SA 2.63)

The PowerElf spam filter uses the following tactics to determine spam:

- The filter uses a wide range of heuristic tests to identify "unsolicited commercial e-mail".
- Header analysis: spammers will attempt to hide their true identify, by fooling you into thinking they've sent a valid mail, or by making you think you must have subscribed to their mailing list at some stage. The filter will try to spot this pattern.
- Text analysis: spam mails often have a characteristic style, and often include text like disclaimers and CYA text. The spam filter can spot these, too.

Tagging and delete features

Allows you to specify different thresholds for either tagging or deleting spam on the network automatically.

Option to use Global white list/Blacklist

- The **Global White List/Black List** section allows the administrator to add e-mail addresses and domains to a White or Black List.

RBL and bulk mail detection tools

- A common way of detecting spam is by using spam databases (blacklists) that list the addresses of mail servers known (or believed) to send spam. This is done by taking the IP address of the remote mail server, converting it to a domain name, and seeing if that name exists. If the domain tests positive, then the overall spam score is increased. The administrator can set the weight that the RBL tests have on the total overall spam score.
- The Bulk Mail Scanner (DCC) client generates a fuzzy checksum on a mail message and sends that checksum to a DCC server; the server returns counts associated with that checksum. If it comes back with a positive match, then the mail is likely to be bulk mail and the overall spam score is adjusted accordingly.

Continued...

More Email. Less Junkmail.

Ability to auto-delete e-mail with attachments

- E-mail with an attachment type that has been banned can be deleted. The admin can custom create a list of extension to be dropped.(eg. pif, vbs, scr, exe, etc.). The filter drops e-mail before it hits the other filters; thus improving overall performance of the mail server.

Create customized list of Spam keywords

- **Spam Keywords** panel is allows the administrator to specify additional keywords and phrases that the default spam filters are not catching. The admin can then set the weight they want the keywords to have in the overall spam score.

Create customized list of permitted keywords

- This panel is used to specify a list of keywords and phrases that should be allowed through the filter and not tagged as spam. This can ensure that legitimate e-mail does not get tagged as spam. The admin can then set the a weight they want the keywords to have to lower the the overall spam score.

Works with POP3, IMAP, Webmail, Forwarded accounts, and Delegate mail servers

- The spam filter works at the "server" level and not at the mailbox stage. This allows networks whose primary mail server is not on the PowerElf II to still use all the spam filter functionality as long as they have a delegate mail server inside their network. Simply change the MX record to point to the PowerElf II and enter the delegate mail server's IP address.

Administrator can encapsulate tagged (spam) mail if required

- This option will send the tagged message as an attachment, with a spam warning message. This helps prevent the end user from opening potentially dangerous e-mail.

Better integration with virtual domains, and multiple network segments on the PowerElf II

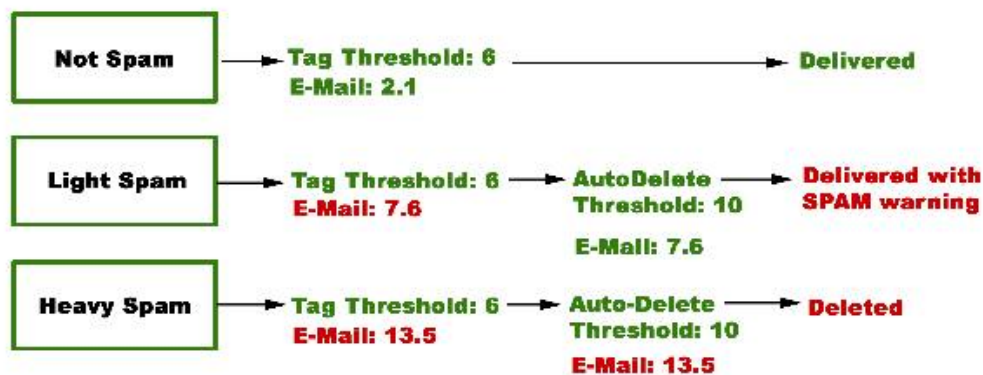
- Outgoing mail from virtual domains are automatically white listed. It does not run network tests on the local network thereby increasing scanning speed.

Designed to work seamlessly with PowerElf Vexira Anti-virus package

- Anti-virus assists the spam filter by eliminating infected email before it hits the spam filter, this increases network efficiency.

Spam levels and thresholds

The spam filter works by assigning each mail message that passes through the filter a number. The number given to each piece of mail is determined by a set of rules that the spam filter uses to determine the spam characteristics of each message.



The diagram above shows how mail is treated as it goes through the filter. An e-mail message with a number below the threshold is allowed through and messages above are tagged or deleted, depending on their spam number.

Continued...

More Email. Less Junkmail.

Additional features of the PowerElf II spam filter:

Auto-Update for anti spam software

- The PowerElf II offers an auto-update mechanism for downloading latest engine updates, as well as new rules, as they are made available.

Optional aggressive rule sets

- Smarter, more aggressive anti-drug rules to detect obfuscated drug words (eg. Vi%agra).
- Includes rules known to be from spammers (eg. freevitamins, freedvds,xmas4cheap.net).
- New rules can look for obfuscated words hidden in the e-mail (eg. g.eta go^od dea@! at h\$ome.).
- Includes a search for spamware mistakes that spam software sometimes includes.(eg. %RANDOM_WORD)
- The aggressive rules for your PowerElf II can be downloaded for free from the PowerElf II auto-update system.

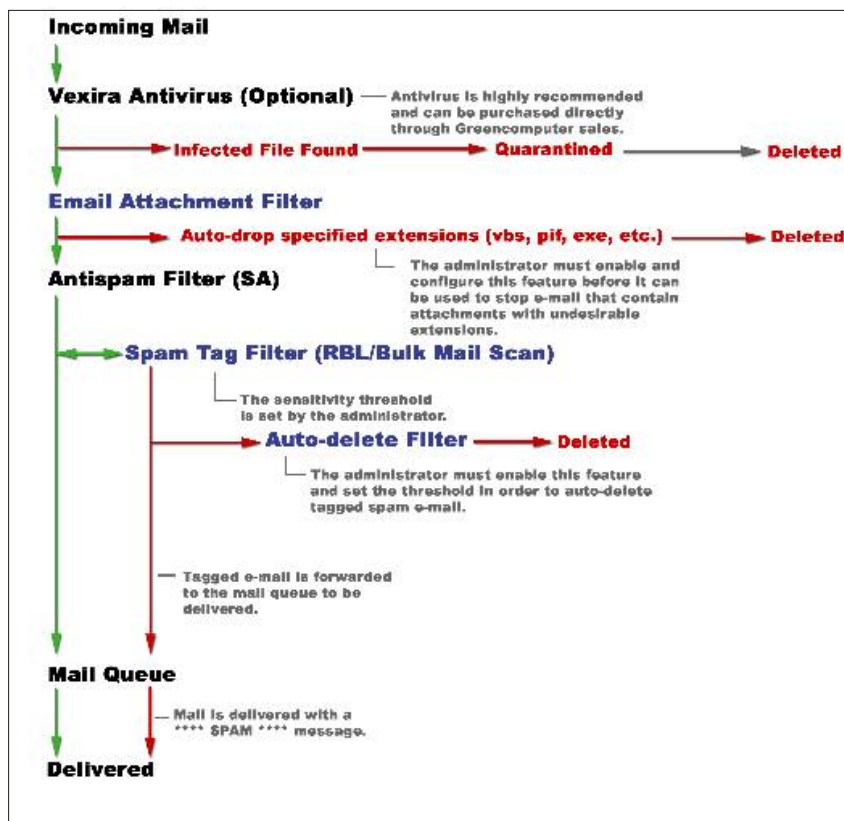
PowerElf II mail delivery process

The PowerElf uses several different techniques to help stop spam at its entry point, long before it has a chance to travel to the end-user's mailbox. Instead of relying on a single mechanism to handle mail, the PowerElf II cleverly uses multiple methods to route and sort e-mail. These techniques improve performance and accuracy.

The mail server receives the mail and puts it through the antivirus scanner (optional) to ensure that the mail passing through does not contain a virus.

It is then passed through the e-mail attachment filter to scan for executable attachments that are undesirable. The administrator can configure and enable this feature for all types of attachments, including non-executable content, such as mp3, jpg, gif, and mpg. This can help increase productivity and save bandwidth.

The Antispam engine receives the e-mail at this point and uses heuristics to scan the content of the message. If the aggressive rule set is enabled the mail will be scanned with those rules as well. The mail will also be checked against a list of key words, if the admin has enabled this feature and entered a list of spam and accepted words or phrases.



If enabled by the administrator, it will also perform an RBL (Real-time Blackhole List) scan as well as a Bulk mail check. A "spam-rating" number will be assigned to the e-mail. If it is higher than the threshold set by the administrator, it will be tagged as spam. If the Auto-Delete is enabled and the threshold is set, the server will determine whether to delete the spam or let it pass through.

Tagged e-mail and non-spam will be delivered to the recipient.