ChooseYourRules

Choose the rules you enable

Everyone's spam is different. What rules and plug-ins work for one installation may not work for yours. There can also be significant performance penalties for using some rules.

One way to more about how your installation is working is to check you logs and see what rules are hitting on your spam, and what rules are not. This way you can see which rules are the most productive for your spam. Some scripts to run against your logs are listed at StatsAndAnalyzers

Using scripts such as these to analyze your logs, you can see which rules and plug-ins are working best for your installation. Some installations have chosen to avoid Bayes, DCC, Vipul's Razor and use URI Blacklist tests such as SURBL and URIBL combined with a few custom rules developed in-house and by the SARE Ninjas to save resources. However, what works for another installation may not work for you!

Know your spam.

- Setup a honeypot account, and actually read the spam that arrives there.
- Have users send you complete copies, headers included, of missed spam or tagged ham.
- Analyze your logs as often as you can.
- Learn to write custom rules.

Once you begin to know the spam your system receives, you can begin making educated decisions on rules that will best capture the most spam using the least amount of resources. That equates to faster processing, more messages handled, and happier users.