

---

Subject: Filter by specific IP

Posted by [tjones](#) on Tue, 18 May 2004 13:32:45 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

With the current rash of viruses blasting around, I find that it would be extremely useful to be able to at least temporarily, block mail by IP by entering it into the blacklist section. Is it possible to do that now?

When I look at the header of a viral email, I can see the originating IP. Using that IP would slow the same repeated virus attacks considerable. If at a later date, they resolve their virus issues and they have a legitimate reason for sending us email. then I would obviously want to be able to easily take them off of the blocked list.

---

---

Subject: Re: Filter by specific IP

Posted by [support](#) on Tue, 18 May 2004 14:03:39 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

> With the current rash of viruses blasting around, I find that  
> it would be extremely useful to be able to at least  
> temporarily, block mail by IP by entering it into the blacklist  
> section. Is it possible to do that now?

>  
> When I look at the header of a viral email, I can see the  
> originating IP. Using that IP would slow the same repeated  
> virus attacks considerable. If at a later date, they resolve  
> their virus issues and they have a legitimate reason for  
> sending us email. then I would obviously want to be able to  
> easily take them off of the blocked list.

The offending IP will probably appear in one of the "Received:" headers. A header rule should get rid of this mail (add this to local.cf in the sa\ruleset subdirectory of your installation with a text editor):

```
header KNOWN_SPAM_IP Received =~ 12.34.56.78
describe KNOWN_SPAM_IP I have every reason to believe this is spam
score KNOWN_SPAM_IP 5.0
```

However, this sort of thing is exactly what RBL lists are for, and you will have a lot of work if you want to maintain your own blacklist this way. Look here for more on the topic of custom rules:

<http://www.exit0.us/index.php>  
<http://wiki.apache.org/spamassassin>

---