By Falko Timme
Published: 2008-06-10 12:07

How To Whitelist Hosts/IP Addresses In Postfix

Version 1.0
Author: Falko Timme <ft [at] falkotimme [dot] com>
Last edited 06/06/2008

If you are administrating a mail server and use blacklists to block spam (like in this article: **How To Block Spam Before It Enters The Server (Postfix)**), you probably know this problem: from time to time your customers complain that they cannot receive emails from certain freemailers. Most often this happens because a freemailer was abused to send out spam and therefore got blacklisted. This short guide shows how you can whitelist such a mail server in Postfix to make your customers happy again.

I do not issue any guarantee that this will work for you!

If a blacklisted server tries to send mail to your server, you should find something like this in your mail log:

```
SMTP error from remote mail server after RCPT TO:<bla@example.com>: host mail.example.com [4.3.2.1]: 554 5.7.1 Service unavailable; Client host [1.2.3.4] blocked using dnsbl.sorbs.net; Currently Sending Spam See: http://www.sorbs.net/lookup.shtml?1.2.3.4
```

In this example, the mail server `1.2.3.4` is blacklisted and therefore blocked.

To whitelist that server, create the file `/etc/postfix/rbl_override` where you list all IP addresses or host names (one per line!) that you want to whitelist:

```
vi /etc/postfix/rbl_override
```

```
1.2.3.4 OK
1.2.3.5 OK
mail.freemailer.tld OK
```

After you've created/modified that file, you must run

```
postmap /etc/postfix/rbl_override
```

Next open */etc/postfix/main.cf* and search for the *smtpd_recipient_restrictions* parameter. Add *check_client_access hash:/etc/postfix/rbl_override* to that parameter, after *reject_unauth_destination*, but before the first blacklist.

So if *smtpd_recipient_restrictions* looks like this now...

```
vi /etc/postfix/main.cf
```

```
[...]
smtpd_recipient_restrictions = reject_invalid_hostname,
                        reject_unauth_pipelining,
                        permit_mynetworks,
                        permit_sasl_authenticated,
                        reject_unauth_destination,
                        reject_rbl_client multi.uribl.com,
                        reject_rbl_client dsn.rfc-ignorant.org,
                        reject_rbl_client dul.dnsbl.sorbs.net,
                        reject_rbl_client list.dsbl.org,
                        reject_rbl_client sbl-xbl.spamhaus.org,
                        reject_rbl_client bl.spamcop.net,
                        reject_rbl_client dnsbl.sorbs.net,
                        reject_rbl_client cbl.abuseat.org,
```

```
                reject_rbl_client ix.dnsbl.manitu.net,
                reject_rbl_client combined.rbl.msrbl.net,
                reject_rbl_client rabl.nuclearelephant.com,
                permit
[...]
```

... modify it so that it looks as follows:

```
[...]
smtpd_recipient_restrictions = reject_invalid_hostname,
                reject_unauth_pipelining,
                permit_mynetworks,
                permit_sasl_authenticated,
                reject_unauth_destination,
                check_client_access hash:/etc/postfix/rbl_override,
                reject_rbl_client multi.uribl.com,
                reject_rbl_client dsn.rfc-ignorant.org,
                reject_rbl_client dul.dnsbl.sorbs.net,
                reject_rbl_client list.dsbl.org,
                reject_rbl_client sbl-xbl.spamhaus.org,
                reject_rbl_client bl.spamcop.net,
                reject_rbl_client dnsbl.sorbs.net,
                reject_rbl_client cbl.abuseat.org,
                reject_rbl_client ix.dnsbl.manitu.net,
                reject_rbl_client combined.rbl.msrbl.net,
                reject_rbl_client rabl.nuclearelephant.com,
                permit
[...]
```

That's it! Restart Postfix, and you're done:

```
/etc/init.d/postfix restart
```

Links

- Postfix: **http://www.postfix.org**