7 Effective Tips for Blocking Email Spam with Postfix SMTP Server

Last Updated: November 29, 2019 Xiao Guoan (Admin) 27 Comments Mail Server

n this tutorial, I’d like to share with you my 7 tips for blocking email spam with Postfix SMTP server. Over the last two years of running my own email server, I received a lot of spam, most of which came from China. Spam exists because it’s so cheap to send large volume of emails on the Internet. Postfix allows you to block spam before they get into your mailbox, so you can save bandwidth and disk space. This post is the result of my experience in fighting spam.

Note: If you plan to run your own mail server, I recommend using iRedmail, which really simplifies the process of setting up a mail server. It also ships with anti-spam rules. If you prefer to set up a mail server from scratch, then check out my mail server tutorial series.

Characteristics of Spam

Below is what I found about email spam. These spam are easy to block.

1. Their IP addresses don’t have PTR records.
2. The spammer doesn’t provide valid hostname in HELO/EHLO clause.
3. They spoof MAIL FROM address.
4. They generally don’t re-send email after a failed email delivery.

Legitimate email servers should never have these characteristics. So here comes my 7 tips, which will block 90% of spam.

> Fact: Around 93%~95% of emails in the world are rejected at the SMTP gateway, never landed in inbox or spam folder.

PTR record maps an IP address to a domain name. It’s the counterpart to A record. On Linux, you can query the domain name associated with an IP address by executing the following command:

```
host <IP address>
```

For example, the following command returns the hostname of Google’s mail server.

```
host 209.85.217.172
```

Output:

```
172.217.85.209.in-addr.arpa domain name pointer mail-ua0-f172.google.com.
```

Due to the prevalence of spam, many mail servers require that SMTP clients have valid PTR records associated with their IP addresses. Every mail server admin should set PTR record for their SMTP servers. If the SMTP client has a PTR record, you can find a line in Postfix log like below.

```
connect from mail-ua0-f172.google.com[209.85.217.172]
```

If the SMTP client doesn’t have a PTR record, then the hostname will be identified as `unknown`.

```
connect from unknown[120.41.196.220]
```

To filter out emails with no PTR records, open Postfix main configuration file.

```
sudo nano /etc/postfix/main.cf
```

Add the following line in `smtpd_sender_restrictions`. This directive rejects an email if the client IP address has no PTR record.

```
reject_unknown_reverse_client_hostname
```

Example:

```
smtpd_sender_restrictions =
   permit_mynetworks
   permit_sasl_authenticated
   reject_unknown_reverse_client_hostname
```

Save and close the file. Then restart Postfix for the change to take effect.

```
sudo systemctl restart postfix
```

Tip #2: Enable HELO/EHLO Hostname Restrictions in Postfix

Some spammers don't provide a valid HELO/EHLO hostname in the SMTP dialog. They can be non fully qualified domain name, or a domain name doesn't exist or only for internal network. For example, a spammer using a Amazon EC2 instance to send spam is logged on my server as follows:

```
Aug 16 04:21:13 email postfix/smtpd[7070]: connect from ec2-54-237-201-103.compute-1.amazonaws.com[54.237.201.103]
Aug 16 04:21:13 email policyd-spf[7074]: prepend Received-SPF: None (mailfrom) identity=mailfrom; client-ip=54.237.201.103; helo=ip-172-30-0-149.ec2.internal; envelope-from=superdiem@carpaythe.tk; receiver=<UNKNOWN>
```

As you can see, the HELO hostname is `ip-172-30-0-149.ec2.internal` , which is only valid in AWS internal network. It has no valid A record nor MX record.

To enable HELO/EHLO hostname restriction, edit Postfix main configuration file.

```
sudo nano /etc/postfix/main.cf
```

First, add the following line to require the client to provide a HELO/EHLO hostname.

```
smtpd_helo_required = yes
```

Then add the following 3 lines to enable `smtpd_helo_restrictions`.

```
smtpd_helo_restrictions =
    permit_mynetworks
    permit_sasl_authenticated
```

Use the following line to reject clients who provide mailformed HELO/EHLO hostname.

```
reject_invalid_helo_hostname
```

Use the following line to reject non fully qualified HELO/EHLO hostname.

```
reject_non_fqdn_helo_hostname
```

To reject email when the HELO/EHLO hostname has neither DNS A record nor MX record, use

```
reject_unknown_helo_hostname
```

Like this:

```
smtpd_helo_required = yes
smtpd_helo_restrictions =
    permit_mynetworks
    permit_sasl_authenticated
    reject_invalid_helo_hostname
    reject_non_fqdn_helo_hostname
    reject_unknown_helo_hostname
```

Save and close the file. Then reload Postfix.

```
sudo systemctl reload postfix
```

Note that although most legitimate mail servers have valid A record for the HELO/EHLO hostname, occasionally a legitimate mail server doesn't meet this requirement. You need to whitelist them with `check_helo_access`.

```
smtpd_helo_required = yes
smtpd_helo_restrictions =
    permit_mynetworks
    permit_sasl_authenticated
    check_helo_access hash:/etc/postfix/helo_access
    reject_invalid_helo_hostname
    reject_non_fqdn_helo_hostname
    reject_unknown_helo_hostname
```

Then you need to create the `/etc/postfix/helo_access` file.

```
sudo nano /etc/postfix/helo_access
```

Whitelist legitimate mail server's HELO/EHLO hostname like below.

```
optimus-webapi-prod-2.localdomain      OK
va-massmail-02.rakutenmarketing.com    OK
```

It's likely that you don't know which hostnames to whitelist, then simply copy the above two lines, which is the only lines in my `helo_access` file. You can always add more hostnames later. Save and close the file. Then run the following command to create the /etc/postfix/helo_access.db file.

```
sudo postmap /etc/postfix/helo_access
```

And reload Postfix.

```
sudo systemctl reload postfix
```

Tip #3: Reject Email if SMTP Client Hostname doesn't have valid A Record

A legitimate email server should also have a valid A record for its hostname. The IP address returned from A record should match the IP address of email server. To filter out emails from hosts that don't have valid A record, edit Postfix main configuration file.

```
sudo nano /etc/postfix/main.cf
```

Add the following line in `smtpd_sender_restrictions`.

```
reject_unknown_client_hostname
```

Example:

```
smtpd_sender_restrictions =
   permit_mynetworks
   permit_sasl_authenticated
   reject_unknown_reverse_client_hostname
   reject_unknown_client_hostname
```

Save and close the file. Then restart Postfix for the change to take effect.

```
sudo systemctl restart postfix
```

> Note that `reject_unknown_client_hostname` does not require HELO from SMTP client. It will fetch the hostname from PTR record, then check the A record.

Tip #4: Reject Email If MAIL FROM Domain Has Neither MX Record Nor A Record

The `MAIL FROM` address is also known as `envelope from` address. Some spammers use a non-existent domain in the `MAIL FROM` address. If a domain name has no MX record, Postfix will find the A record of the main domain and send email to that host. If the sender domain has neither MX record nor A record, Postfix can't send email to that domain. So why not reject emails that you can't reply to?

To filter out this kind of spam, edit Postfix main configuration file.

```
sudo nano /etc/postfix/main.cf
```

Add the following line in `smtpd_sender_restrictions`. It will reject email if the domain name of the address supplied with the MAIL FROM command has neither MX record nor A record.

```
reject_unknown_sender_domain
```

Example:

```
smtpd_sender_restrictions =
   permit_mynetworks
   permit_sasl_authenticated
   reject_unknown_sender_domain
   reject_unknown_reverse_client_hostname
   reject_unknown_client_hostname
```

Save and close the file. Then restart Postfix for the change to take effect.

```
sudo systemctl restart postfix
```

Note that I placed this restriction above other `reject` restrictions. From my experience, if it is below other `reject` restrictions, it won't work. (Maybe this only happens on my email server.)

Tip #5: Enable Greylisting in Postfix

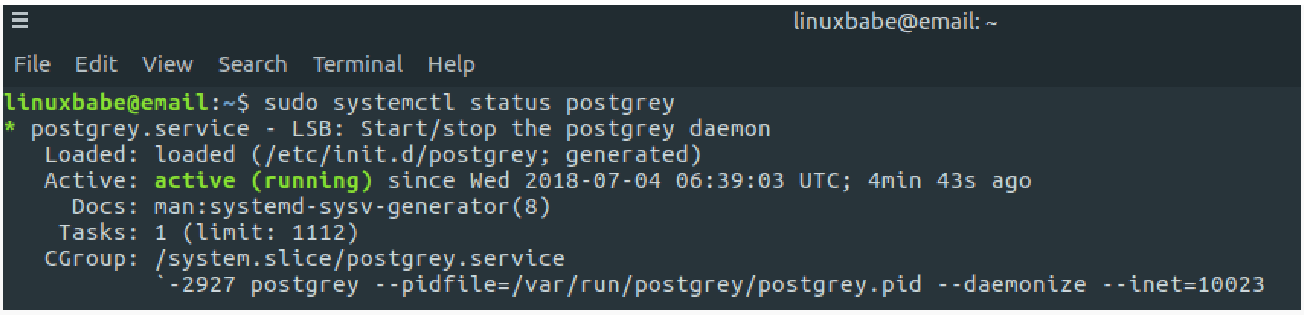
As required by the SMTP protocol, any legitimate SMTP client must be able to re-send email if delivery fails. (By default, Postfix is configured to resend failed emails many times before it informs the sender that the message could not be delivered.) Many spammers usually just send once and would not retry.

`Postgrey` is a greylisting policy server for Postfix. You can install `postgrey` on Ubuntu from the default repository.

```
sudo apt install postgrey
```

It will be automatically started, as shown with:

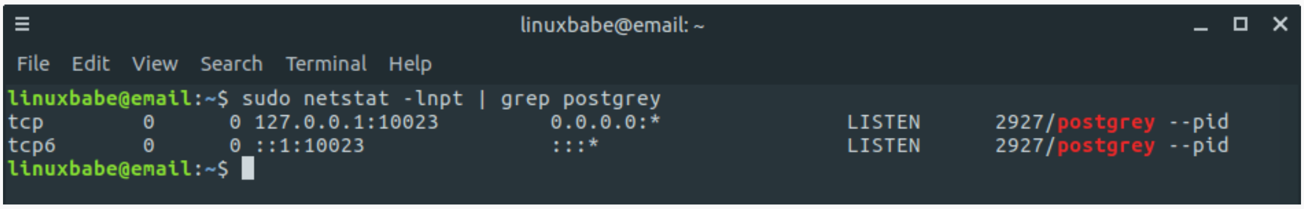
```
sudo systemctl status postgrey
```



```
linuxbabe@email:~$ sudo systemctl status postgrey
* postgrey.service - LSB: Start/stop the postgrey daemon
   Loaded: loaded (/etc/init.d/postgrey; generated)
   Active: active (running) since Wed 2018-07-04 06:39:03 UTC; 4min 43s ago
     Docs: man:systemd-sysv-generator(8)
    Tasks: 1 (limit: 1112)
   CGroup: /system.slice/postgrey.service
           `-2927 postgrey --pidfile=/var/run/postgrey/postgrey.pid --daemonize --inet=10023
```

And it listens on TCP port 10023 on localhost (both IPv4 and IPv6).

```
sudo netstat -lnpt | grep postgrey
```



```
linuxbabe@email:~$ sudo netstat -lnpt | grep postgrey
tcp        0      0 127.0.0.1:10023         0.0.0.0:*               LISTEN      2927/postgrey --pid
tcp6       0      0 ::1:10023               :::*                    LISTEN      2927/postgrey --pid
linuxbabe@email:~$
```

By default, the greylist time is 300 seconds, which means an unknown SMTP client needs to wait 5 minutes before re-sending the email. If that's very long to you, you can change it to 60 seconds or 120 seconds. This can be configured in `/etc/default/postgrey` file.

```
sudo nano /etc/default/postgrey
```

Find the following line.

```
POSTGREY_OPTS="--inet=10023"
```

Change it to

```
POSTGREY_OPTS="--inet=127.0.0.1:10023 --delay=60"
```

Save and close the file. Then restart postgrey for the change to take effect.

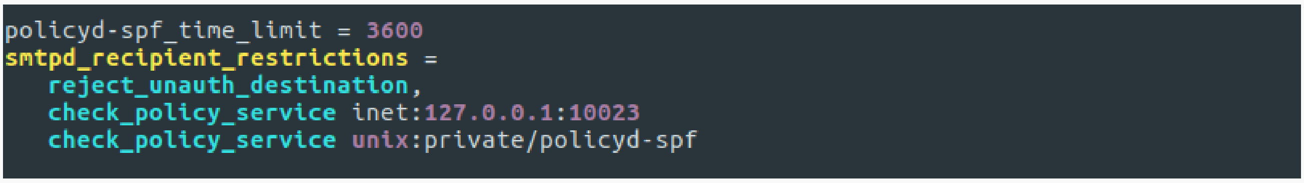
```
sudo systemctl restart postgrey
```

Next, we need to edit Postfix main configuration file to make it use the greylisting policy server.

```
sudo nano /etc/postfix/main.cf
```

Add the following line in `smtpd_recipient_restrictions`.

```
check_policy_service inet:127.0.0.1:10023
```



```
policyd-spf_time_limit = 3600
smtpd_recipient_restrictions =
   reject_unauth_destination,
   check_policy_service inet:127.0.0.1:10023
   check_policy_service unix:private/policyd-spf
```

In case you don't know, the directive `check_policy_service unix:private/policyd-spf` in the above screenshot will make Postfix check SPF record on the sender's domain and you are advised to implement SPF and DKIM on your own domain to improve your email sender score.

Save and close the file. Then restart Postfix.

```
sudo systemctl restart postfix
```

From now on, Postgrey will reject an email if the **sender triplet** (sender IP address, sender email address, recipient email address) is new. The following log message in `/var/log/mail.log` shows a new sender triplet. The action "`greylist`" means this email message was rejected.

```
postgrey[1016]: action=greylist, reason=new, client_name=unknown, client_address=117.90.24.148/32, sender=pnccepjeu@rhknqj.net, recipient=xiao@linuxbabe.com
```

From my experience, Chinese email spammers like to use a fake, weird-looking and randomly generated sender address for every email, so adding these fake email addresses to blacklist won't stop them. On the other hand, they never try re-sending a rejected email with the same sender address, which means greylisting can be very effective at stopping this kind of spam.

Fixing Error

If you see the following error in mail log (`/var/log/mail.log`)

```
warning: connect to 127.0.0.1:10023: Connection refused
warning: problem talking to server 127.0.0.1:10023: Connection
refused
```

The problem is that postgrey is not running. You need to specify 127.0.0.1 as the listening address in `/etc/default/postgrey` file. So change the following line

```
POSTGREY_OPTS="--inet=10023"
```

to

```
POSTGREY_OPTS="--inet=127.0.0.1:10023"
```

Then restart postgrey

```
sudo systemctl restart postgrey
```

Check if it's listening:

```
sudo netstat -lnpt | grep 10023
```

Whitelisting

Greylisting can result in bad experience for the end user, as the user has to wait another several minutes for the email to arrive. To minimize this bad experience, you can create whitelist.

Postgrey ships with two whitelist files (`/etc/postgrey/whitelist_clients` and `/etc/postgrey/whitelist_recipients`). The former contains a list of hostnames and the latter contains a list of recipient addresses.

By default, Google's mail servers are whitelisted. No matter the sender is using a @gmail.com address or other address, as long as the sender is using Google's mail server, Postgrey won't reject the email. The following line in my `/var/log/mail.log` file shows this.

```
postgrey[1032]: action=pass, reason=client whitelist, client_name=mail-yb0-f190.google.com
```

Note: You can also see postgrey logs with this command `sudo journalctl -u postgrey`.

You can add other hostnames in `whitelist_clients` file, like

```
facebook.com
bounce.twitter.com
blogger.com
email.medium.com
```

You can get these hostnames with a tool called `pflogsumm`, which I will discuss later in this article.

Tip #6: Using Public Anti-Spam Blacklists

There are spam emails that are sent from servers that has a valid hostname, valid PTR record and can pass through grey listing. In this case, you can use blacklisting to reject spam. There are many public anti-spam blacklists, also known as DNSBLs (DNS based lists). You can use multiple blacklists to block spam. Go to https://www.debouncer.com and mxtoolbox.com , enter the spammer's domain and IP address to see which blacklists are blocking them, then you can use those blacklists. For example, I found that spammers are blacklisted by one of the following blacklists:

- dbl.spamhaus.org
- zen.spamhaus.org
- multi.uribl.com
- ivmURI
- InvaluementURI

So I can add the following configurations in `/etc/postfix/main.cf` file. Some public blacklisting service requires monthly fee. For now, I'm using the free service of spamhaus.org.

```
smtpd_recipient_restrictions =
   permit_mynetworks,
   permit_sasl_authenticated,
   reject_rhsbl_helo dbl.spamhaus.org,
   reject_rhsbl_reverse_client dbl.spamhaus.org,
   reject_rhsbl_sender dbl.spamhaus.org,
   reject_rbl_client zen.spamhaus.org
```

Where:

- `rhs` stands for right hand side, i.e, the domain name.
- `reject_rhsbl_helo` makes Postfix reject email when the client HELO or EHLO hostname is blacklisted.
- `reject_rhsbl_reverse_client`: reject the email when the unverified reverse client hostname is blacklisted. Postfix will fetch the client hostname from PTR record. If the hostname is blacklisted, reject the email.
- `reject_rhsbl_sender` makes Postfix reject email when the MAIL FROM domain is blacklisted.
- `reject_rbl_client`: This is an IP-based blacklist. When the client IP address is backlisted, reject the email.

Some spammers use Google’s mail server, so `reject_rhsbl_helo` is ineffective, but most of them use their own domain names in the MAIL FROM header, so `reject_rhsbl_sender` will be effective.

Create A Whitelist

Sometimes there are legitimate email servers blacklisted. You can create a whitelist so they won’t be blocked. Create the following file.

```
sudo nano /etc/postfix/rbl_override
```

In this file, whitelist domain names like below.

```
dripemail2.com  OK           //This domain belongs to drip.com

mlsend.com      OK           //This domain belongs to mailerlite email marketing service
```

Save and close the file. Then run the following command to create the `rbl_override.db` file.

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

Edit Postfix main configuration file.

```
sudo nano /etc/postfix/main.cf
```

In `smtpd_recipient_restrictions`, add the following line.

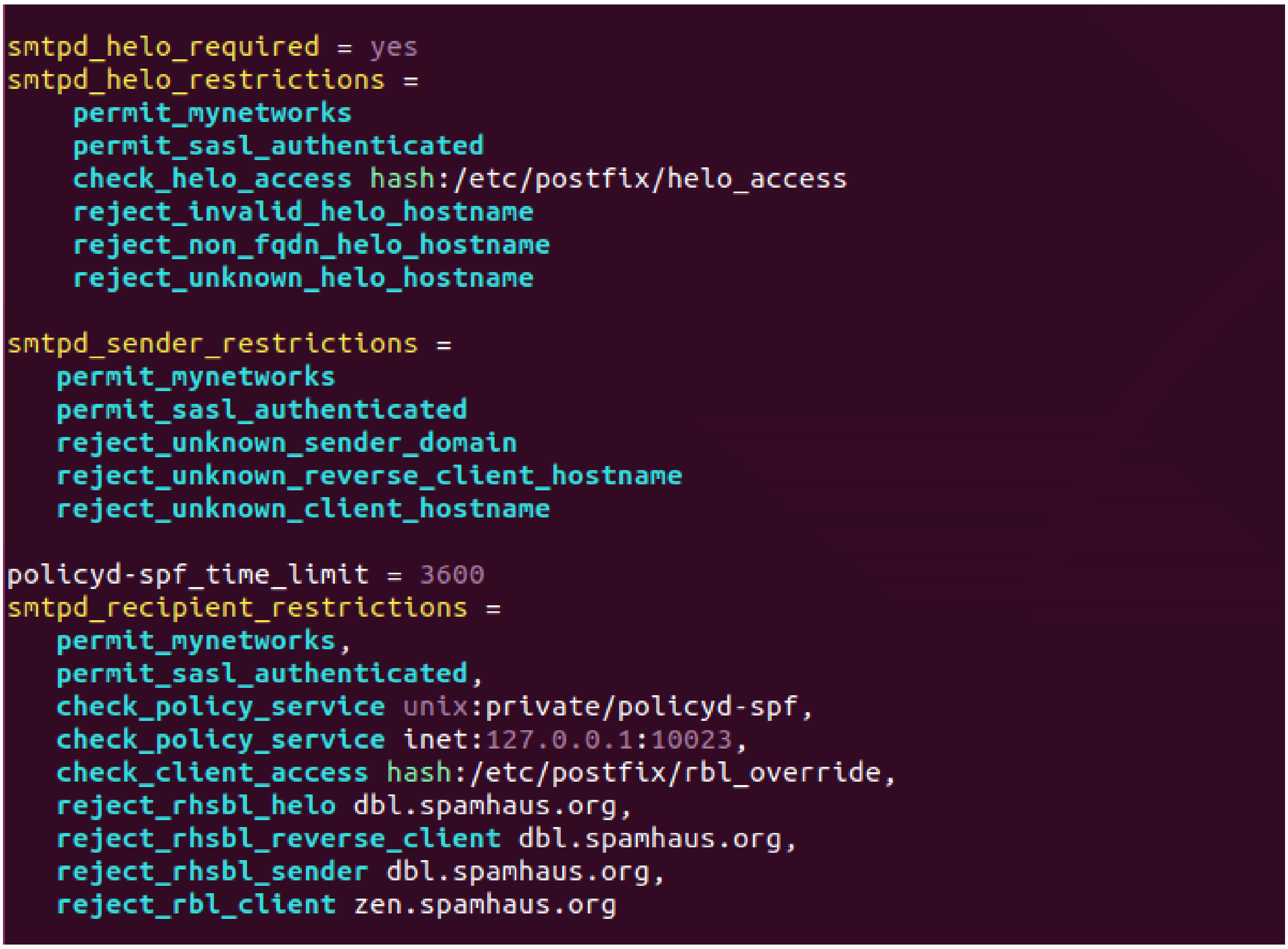
```
check_client_access hash:/etc/postfix/rbl_override,
```

Reload Postfix for the changes to take effect.

```
sudo systemctl reload postfix
```

My Postfix Spam filters

Here’s a screenshot of my Postfix spam filters.



```
smtpd_helo_required = yes
smtpd_helo_restrictions =
    permit_mynetworks
    permit_sasl_authenticated
    check_helo_access hash:/etc/postfix/helo_access
    reject_invalid_helo_hostname
    reject_non_fqdn_helo_hostname
    reject_unknown_helo_hostname

smtpd_sender_restrictions =
   permit_mynetworks
   permit_sasl_authenticated
   reject_unknown_sender_domain
   reject_unknown_reverse_client_hostname
   reject_unknown_client_hostname

policyd-spf_time_limit = 3600
smtpd_recipient_restrictions =
   permit_mynetworks,
   permit_sasl_authenticated,
   check_policy_service unix:private/policyd-spf,
   check_policy_service inet:127.0.0.1:10023,
   check_client_access hash:/etc/postfix/rbl_override,
   reject_rhsbl_helo dbl.spamhaus.org,
   reject_rhsbl_reverse_client dbl.spamhaus.org,
   reject_rhsbl_sender dbl.spamhaus.org,
   reject_rbl_client zen.spamhaus.org
```

You might be wondering why there is no coma in the first two configuration snippets. Well, you can separate values in Postfix configuration file with space, carriage return or coma. If you add coma to one parameter (`smptd_recipient_restrictions` as in the above screenshot), then make sure all remaining values are separated with coma.

Postfix Log Report

`Pflogsumm` is a great tool to create a summary of Postfix logs. Install it on Ubuntu with:

```
sudo apt install pflogsumm
```

Use the following command to generate a report for today.

```
sudo pflogsumm -d today /var/log/mail.log
```

Generate a report for yesterday.

```
sudo pflogsumm -d yesterday /var/log/mail.log
```

If you like to generate a report for this week.

```
sudo pflogsumm /var/log/mail.log
```

To emit “problem” reports (bounces, defers, warnings, rejects) before “normal” stats, use `--problems-first` flag.

```
sudo pflogsumm -d today /var/log/mail.log --problems-first
```

To append the email from address to each listing in the reject report, use `--rej-add-from` flag.

```
sudo pflogsumm -d today /var/log/mail.log --rej-add-from
```

To show the full reason in reject summaries, use `--verbose-msg-detail` flag.

```
sudo pflogsumm -d today /var/log/mail.log --rej-add-from --verbose-msg-detail
```

You can add a cron job to make pflogsumm to send a report to your email address every day.

```
sudo crontab -e
```

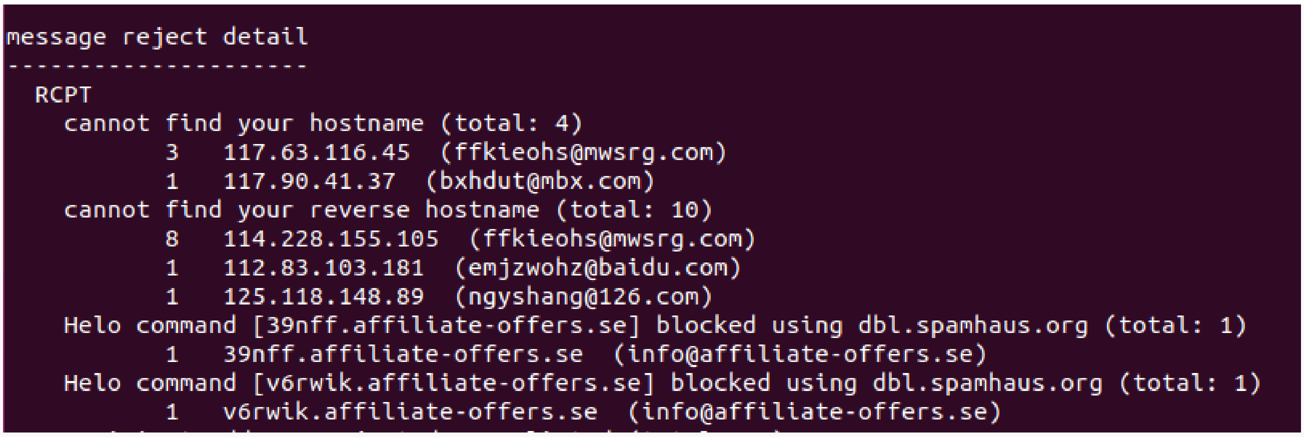
Add the following line, which will generate a report every day at 4:00 AM.

```
0 4 * * * /usr/sbin/pflogsumm -d yesterday /var/log/mail.log --problems-first --rej-add-from --verbose-msg-detail -q
```

To receive the report via email, add the following line above all cron jobs.

```
MAILTO="your-email-address"
```

You should pay attention to the `message reject detail` section, where you can see for what reason those emails are rejected and if there’s any false positives. Greylisting rejections are safe to ignore.



```
message reject detail
---------------------
  RCPT
    cannot find your hostname (total: 4)
           3   117.63.116.45  (ffkieohs@mwsrg.com)
           1   117.90.41.37  (bxhdut@mbx.com)
    cannot find your reverse hostname (total: 10)
           8   114.228.155.105  (ffkieohs@mwsrg.com)
           1   112.83.103.181  (emjzwohz@baidu.com)
           1   125.118.148.89  (ngyshang@126.com)
    Helo command [39nff.affiliate-offers.se] blocked using dbl.spamhaus.org (total: 1)
           1   39nff.affiliate-offers.se  (info@affiliate-offers.se)
    Helo command [v6rwik.affiliate-offers.se] blocked using dbl.spamhaus.org (total: 1)
           1   v6rwik.affiliate-offers.se  (info@affiliate-offers.se)
```

If the MAILTO variable has already been set but you want Postfix log summary sent to a different email address, you can put the following line in your Cron job.

```
0 4 * * * /usr/sbin/pflogsumm -d yesterday /var/log/mail.log --problems-first --rej-add-from --verbose-msg-detail -q | mutt -s "Postfix log summary"  your-email-address
```

The output of `pflogsumm` command is redirected to `mutt`, a command line mail user agent, which will use the output as the email body and send it to the email address you specify at the end. Of course, you need to install mutt on your Linux server.

```
sudo apt install mutt
```

Tip #7: Set Up OpenDMARC to Reject Emails That Fail DMARC Check

DMARC (Domain-based Message Authentication, Reporting and Conformance) is an Internet standard that allows domain owners to prevent their domain names from being used by email spoofers. Please read the following guide.

- Set Up OpenDMARC with Postfix on Ubuntu to Block Email Spoofing/Spam

Don’t be an Open Relay

Mail servers that forward mail on behalf of anyone towards any destination is called open relay. In the beginning, this is a good thing. As time went by, open relays are abused by spammers and now open relays are often blacklisted. The following line in `/etc/postfix/main.cf` file prevents your email server from being an open relay.

```
smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
```

This line tells Postfix to forward email only from clients in trusted networks, from clients that have authenticated with SASL, or to domains that are configured as authorized relay destinations. It should be already in the main configuration file after you install Postfix.

How to Stop SMTP AUTH Flood from Spammers

After some time, the spammer knew that he cannot get through my spam filter. This bad actor started flooding my email server with SMTP AUTH connections. In my `/var/log/mail.log` file, I can find the following messages.

```
Dec 14 09:58:37 email postfix/smtpd[22095]: connect from unknown[117.86.35.119]
Dec 14 09:58:37 email postfix/smtpd[22119]: lost connection after AUTH from unknown[114.232.141.99]
Dec 14 09:58:37 email postfix/smtpd[22119]: disconnect from unknown[114.232.141.99] ehlo=1 auth=0/1 commands=1/2
Dec 14 09:58:37 email postfix/smtpd[22119]: connect from unknown[180.120.191.91]
Dec 14 09:58:38 email postfix/smtpd[22095]: lost connection after AUTH from unknown[117.86.35.119]
Dec 14 09:58:38 email postfix/smtpd[22095]: disconnect from unknown[117.86.35.119] ehlo=1 auth=0/1 commands=1/2
Dec 14 09:58:38 email postfix/smtpd[22119]: lost connection after AUTH from unknown[180.120.191.91]
Dec 14 09:58:38 email postfix/smtpd[22119]: disconnect from unknown[180.120.191.91] ehlo=1 auth=0/1 commands=1/2
Dec 14 09:58:38 email postfix/smtpd[22095]: connect from unknown[49.67.68.34]
Dec 14 09:58:39 email postfix/smtpd[22106]: lost connection after AUTH from unknown[180.120.192.199]
Dec 14 09:58:39 email postfix/smtpd[22106]: disconnect from unknown[180.120.192.199] ehlo=1 auth=0/1 commands=1/2
Dec 14 09:58:39 email postfix/smtpd[22095]: lost connection after AUTH from unknown[49.67.68.34]
Dec 14 09:58:39 email postfix/smtpd[22095]: disconnect from unknown[49.67.68.34] ehlo=1 auth=0/1 commands=1/2
Dec 14 09:58:39 email postfix/smtpd[22119]: connect from unknown[121.226.62.16]
Dec 14 09:58:39 email postfix/smtpd[22119]: lost connection after AUTH from unknown[121.226.62.16]
Dec 14 09:58:39 email postfix/smtpd[22119]: disconnect from unknown[121.226.62.16] ehlo=1 auth=0/1 commands=1/2
Dec 14 09:58:39 email postfix/smtpd[22106]: connect from unknown[58.221.55.21]
Dec 14 09:58:40 email postfix/smtpd[22106]: lost connection after AUTH from unknown[58.221.55.21]
Dec 14 09:58:40 email postfix/smtpd[22106]: disconnect from unknown[58.221.55.21] ehlo=1 auth=0/1 commands=1/2
Dec 14 09:58:47 email postfix/smtpd[22095]: connect from unknown[121.232.65.223]
Dec 14 09:58:47 email postfix/smtpd[22095]: lost connection after AUTH from unknown[121.232.65.223]
Dec 14 09:58:47 email postfix/smtpd[22095]: disconnect from unknown[121.232.65.223] ehlo=1 auth=0/1 commands=1/2
```

To stop this kind of flood attack, you can use fail2ban, which is a set of server and client programs to limit brute force authentication attempts. Install fail2ban from default Ubuntu repository.

```
sudo apt install fail2ban
```

After it’s installed, it will be automatically started, as can be seen with:

```
sudo systemctl status fail2ban
```

The `fail2ban-server` program included in fail2ban monitors log files and issues ban/unban command. By default, it would ban a client’s IP address for 10 minutes if the client failed authentication 5 times. The ban is done by adding iptables firewall rules. You can check iptables rules by running the following command.

```
sudo iptables -L
```

To enable fail2ban on Postifx SMTP AUTH attack, add the following lines in `/etc/fail2ban/jail.local` file. If the file doesn't exist, then create this file.

```
[postfix-flood-attack]
enabled  = true
bantime  = 10m
filter   = postfix-flood-attack
action   = iptables-multiport[name=postfix, port="http,https,smtp,submission,pop3,pop3s,imap,imaps,sieve", protocol=tcp]
logpath  = /var/log/mail.log
```

You can change the bantime to something like `30m` or `12h` to ban the bad actor for longer time. If you would like to whitelist your own IP address, add the following line to tell fail2ban to ignore your IP address. Replace 12.34.56.78 with your own IP address. Multiple IP addresses are separated by spaces.

```
ignoreip = 127.0.0.1/8 ::1 12.34.56.78
```

By default, the allowed max number of failure it 5 times. After 5 failures, the client will be banned. To specify a customized number of failures, add the following line. Change the number to your liking.

```
maxretry = 4
```

Save and close the file. Then create the filter rule file.

```
sudo nano /etc/fail2ban/filter.d/postfix-flood-attack.conf
```

In this file, we specify that if the "lost connection after AUTH from" is found, then ban that IP address.

```
[Definition]
failregex = lost connection after AUTH from (.*)\[<HOST>\]
ignoreregex =
```

Save and close the file. Restart fail2ban the changes to take effect.

```
sudo systemctl restart fail2ban
```

In the fail2ban log file (`/var/log/fail2ban.log`), I can find the message like below, which indicates the IP address 114.223.221.55 has been banned because it failed authentication 5 times.

```
2018-12-14 09:52:15,598 fail2ban.filter [21897]: INFO [postfix-flood-attack] Found 114.223.211.55 - 2018-12-14 09:52:15
2018-12-14 09:52:16,485 fail2ban.filter [21897]: INFO [postfix-flood-attack] Found 114.223.211.55 - 2018-12-14 09:52:16
2018-12-14 09:52:20,864 fail2ban.filter [21897]: INFO [postfix-flood-attack] Found 114.223.211.55 - 2018-12-14 09:52:20
2018-12-14 09:52:21,601 fail2ban.filter [21897]: INFO [postfix-flood-attack] Found 114.223.211.55 - 2018-12-14 09:52:21
2018-12-14 09:52:22,102 fail2ban.filter [21897]: INFO [postfix-flood-attack] Found 114.223.211.55 - 2018-12-14 09:52:22
2018-12-14 09:52:22,544 fail2ban.actions [21897]: NOTICE [postfix-flood-attack] Ban 114.223.211.55
```

I can also check my iptables.

```
sudo iptables -L
```

Output:

```
Chain f2b-postfix (1 references)
target     prot opt source               destination
REJECT     all  --  195.140.231.114.broad.nt.js.dynamic.163data.com.cn  anywhere             reject-with icmp-port-unreachable
RETURN     all  --  anywhere             anywhere
```

This indicates fail2ban has set up a iptables rule that reject connection from `195.140.231.114.broad.nt.js.dynamic.163data.com.cn`, which is a hostname is used by the spammer.

If you would like to manually block an IP address, run the following command. Replace 12.34.56.78 with the IP address you want to block.

```
sudo iptables -I INPUT -s 12.34.56.78 -j DROP
```

If you use UFW (iptables frontend), then run

```
sudo ufw insert 1 deny from 12.34.56.78 to any
```

How To Stop Repeat Senders Who Failed Postfix Check

Some spammers use automated tools to send spam. They ignore the Postfix reject message and continue sending spam. For example, sometimes I can see the following message in Postfix summary report.

```
 504 5.5.2 : Helo command rejected: need fully-qualified hostname; from=<123123@linuxbabe.com> to=<martinlujan997@gmail.com> proto=ESMTP helo= (total: 1)
           1   185.191.228.36
 504 5.5.2 : Helo command rejected: need fully-qualified hostname; from=<123456@linuxbabe.com> to=<martinlujan997@gmail.com> proto=ESMTP helo= (total: 1)
           1   185.191.228.36
 504 5.5.2 : Helo command rejected: need fully-qualified hostname; from=<3vrgfqblaepzfoieznbfntmrpqyix@linuxbabe.com> to=<martinlujan997@gmail.com> proto=ESMTP helo= (total: 1)
           1   185.191.228.36
 504 5.5.2 : Helo command rejected: need fully-qualified hostname; from=<6khdgqr6j@linuxbabe.com> to=<martinlujan997@gmail.com> proto=ESMTP helo= (total: 1)
           1   185.191.228.36
 504 5.5.2 : Helo command rejected: need fully-qualified hostname; from=<a1b2c3d4@linuxbabe.com> to=<martinlujan997@gmail.com> proto=ESMTP helo= (total: 1)
           1   185.191.228.36
 504 5.5.2 : Helo command rejected: need fully-qualified hostna
```

```
me; from=<abuse@linuxbabe.com> to=<martinlujan997@gmail.com> pr
oto=ESMTP helo= (total: 1)
```

This spammer continues sending spam, ignoring the Postfix reject message: `Helo command rejected: need fully-qualified hostname`. To stop this kind of behavior, we can also use Fail2ban by adding the following lines in `/etc/fail2ban/jail.local` file.

```
[postfix]
enabled = true
maxretry = 3
bantime = 1h
filter = postfix
logpath = /var/log/mail.log
```

The `[postfix]` jail will use the builtin filter shipped with Fail2ban (`/etc/fail2ban/filter.d/postfix.conf`). Save and close the file. Then restart Fail2ban.

```
sudo systemctl restart fail2ban
```

Now the spammer will have to wait 1 hour before pounding your mail server again.

Bonus Tip For iRedMail Users

iRedMail automatically configures Postscreen with Postfix. By default, there is a **pregreet test** in Postscreen to detect spam. As you may already know, in SMTP protocol, the receiving SMTP server should always declare its hostname before the sending SMTP server does so. Some spammers violate this rule and declare their hostnames before the receiving SMTP server does.

Sometimes I can see the following lines in `/var/log/mail.log` file, which indicates that this sender declare its hostname first. This spammer just want to pound my mail server with endless connections, but has no intent to send any email. And the EHLO hostname `ylmf-pc` is a clear indication that these connections are originated from compromised home computers. (`ylmf` is an acronym for the defunct Chinese Linux distro: 雨林木风.)

```
PREGREET 14 after 0.22 from [121.226.63.86]:64689: EHLO ylmf-pc
\r\n
PREGREET 14 after 0.24 from [121.232.8.131]:55705: EHLO ylmf-pc
\r\n
PREGREET 14 after 0.24 from [114.232.9.57]:62783: EHLO ylmf-pc
\r\n
```

iRedMail ships with a fail2ban rule to filter this kind of malicious activities. You can see the following line in `/etc/fail2ban/filter.d/postfix.iredmail.conf` file.

```
PREGREET .* from \[<HOST>\]:.* EHLO ylmf-pc
```

But I think the default bantime (1 hour) for this filter to too low. Open the `/etc/fail2ban/jail.local` file and add a custom bantime parameter like below.

```
[postfix-iredmail]
enabled   =  true
max-retry =  1
bantime   =  24h
logpath   =  /var/log/mail.log
```

I set the bantime value to 24 hours because the sender is clearly using compromised home computers. Save and close the file. Restart fail2ban the changes to take effect.

```
sudo systemctl restart fail2ban
```

Next Step

I hope these 7 Postfix anti spam measures helped you block email spam. You may also want to read how to [block spam by checking email header/body in Postfix and SpamAssassin](). As always, if you found this post useful, then [subscribe to our free newsletter]() to get more tips and tricks. Take care ☺

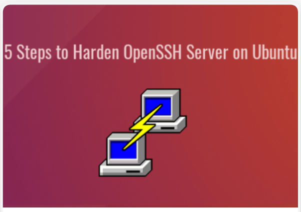
Rate this tutorial

★★★★★ [Total: 28 Average: 4.9]

Linux mail server postfix Spam Filter Ubuntu Ubuntu Server

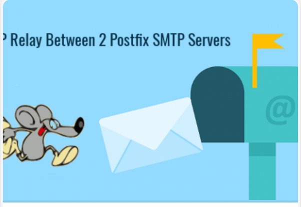
You may also like:

Install Open Web Analytic…



5 Effective Tips to Harden SS…

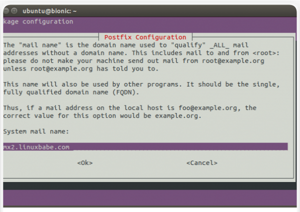
Set up NextCloud…



How to Set Up SMTP Relay…

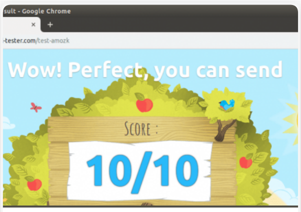
Send Email Using Extern…

Build Your Own Email Server …



```
ubuntu@bionic: ~
kage configuration
                    Postfix Configuration
The "mail name" is the domain name used to "qualify" _ALL_ mail
addresses without a domain name. This includes mail to and from <root>:
please do not make your machine send out mail from root@example.org
unless root@example.org has told you to.

This name will also be used by other programs. It should be the single,
fully qualified domain name (FQDN).

Thus, if a mail address on the local host is foo@example.org, the
correct value for this option would be example.org.

System mail name:

mx2.linuxbabe.com

             <Ok>                        <Cancel>
```

How to Set up a Backup Emai…



How to Set up Postfix SMTP…

⚡ by shareaholic

27 Responses to "7 Effective Tips for Blocking Email Spam with Postfix SMTP Server"

Vladimír 1 year ago Reply

Nice! Thanks for ideas.

Joshua Campbell 12 months ago Reply

Really helpful. I currently pay for web hosting and a mail server but my 3 year contract is ending soon and have been researching methods on hosting this on an easy to deploy Linode instance. Thanks for the spam filter information!!

Mark 11 months ago Reply

For several days I trying to set up and secure mail server. It's probably okay, but I still have questions.
1. GreyList.
In your "How to Easily Set Up a Full-Featured Mail Server on Ubuntu 18.04 with iRedMail" you wrote: "By default, iRedMail has enabled greylisting". What is better: default iRedMail

greylist or Postgrey? If I install Postgrey, should I disable default iRedMail greylist?
2. Fail2ban.
In my version of iRedMail in filter.d/postfix.iredmail.conf file I have something like similar line:

```
"failregex = \[\]: SASL (PLAIN|LOGIN) authentication failed
            lost connection after (AUTH|UNKNOWN|EHLO) from (.*)\
[\]"
```

Is this the same rule or I still should add your [postfix-auth] to my jail.local?
And in my jail.local is only one jail [DEFAULT] – is this correct?

Xiao Guo An (Admin) 11 months ago Reply

If you use iRedMail to set up your mail server, I recommend using the default iRedMail greylisting service and the default Fail2ban jails.

I would use Postgrey and create my custom Fail2ban jails if I set up mail server from scratch.

deibis 10 months ago Reply

Excelente post compa gracias por el aporte.
Aunque actualemtne tengo el siguiente problema:

```
Feb 14 10:20:15 host postfix/smtpd[27908]: connect from 19012112
8161.ip41.static.mediacommerce.com.co[190.121.128.161]
Feb 14 10:20:15 host postfix/smtpd[27877]: Anonymous TLS connect
ion established from unknown[170.210.208.10]: TLSv1 with cipher
DHE-RSA-AES256-SHA (256/256 bits)
Feb 14 10:20:15 host postfix/smtpd[28197]: Anonymous TLS connect
ion established from unknown[190.129.24.236]: TLSv1.2 with ciphe
r ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits)
```

alguna idea de como bloquear esas IP a traves del csf de firewall de centos

kde35 9 months ago Reply

Hi, this is nice, but my postfix server accepts mails from local network (192.168.1.xxx) as well as localhost,
so if I follow one of your first four tips, then it will stop sending mails from local network, am I right?

Xiao Guo An (Admin) 9 months ago Reply

These tips are used to block inbound spam from other SMTP servers. Your own users on the local network and localhost can send emails as usual.

Xiao Guo An (Admin) 9 months ago ↩ Reply

I assume by “accept” you mean outbound emails are **submitted** to Postfix from local network and localhost, which is different than accepting inbound emails from other SMTP servers.

webrunner 9 months ago ↩ Reply

fail2ban-client status
cat /var/log/auth.log | grep ‘Failed password’ – Debian
cat /var/log/secure | grep ‘Failed password’ – Centos

webrunner 9 months ago ↩ Reply

check_policy_service unix:private/policyd-spf – this blocks gmail and other external mailservers, even if maillog show, that gmail is whitelisted.

Xiao Guo An (Admin) 9 months ago ↩ Reply

Sorry if I didn’t explain it well. You need to follow this tutorial to implement SPF checking.

In practice, SPF is more useful when you combine it with DKIM to enforce DMARC record checking to stop spammers impersonating other person’s domain name.

Sunil Kumar 1 month ago ↩ Reply

What if I am using CSF ?

Breen 9 months ago ↩ Reply

I sent email from “http://www.anonymailer.net” and I got this response in maillog
postfix/smtpd[15785]: NOQUEUE: reject: RCPT from unknown[10.230.220.57]: 450 4.7.1 Client host rejected: cannot find your reverse hostname, [10.230.220.57]; from= to= proto=ESMTP helo=

Then, I sent email from my gmail account, I get the same (which is not expected)
postfix/smtpd[15785]: NOQUEUE: reject: RCPT from unknown[10.230.220.56]: 450 4.7.1 Client host rejected: cannot find your reverse hostname, [10.230.220.56]; from=" to= proto=ESMTP helo="

Here is my postfix config:

```
smtpd_helo_required = yes
smtpd_helo_restrictions =
  permit_mynetworks,
  permit_sasl_authenticated,
  reject_invalid_helo_hostname,
  reject_non_fqdn_helo_hostname,
  reject_unknown_helo_hostname
```

```
smtpd_sender_restrictions =
  permit_mynetworks,
  permit_sasl_authenticated,
  reject_unknown_sender_domain,
  reject_unknown_reverse_client_hostname,
  reject_unknown_client_hostname

smtpd_recipient_restrictions =
  permit_mynetworks,
  permit_sasl_authenticated,
  reject_unauth_destination,
  reject_rhsbl_helo dbl.spamhaus.org,
  reject_rhsbl_reverse_client dbl.spamhaus.org,
  reject_rhsbl_sender dbl.spamhaus.org,
  reject_rbl_client zen.spamhaus.org
```

Xiao Guo An (Admin) 9 months ago Reply

10.230.220.56 doesn't seem to be Google's IP address. Every IP address owned by Google has a reverse DNS record.

Jack 9 months ago Reply

Hi, thanks for your post. Let me say my IMHO:
Guys, don't use greylisting in your postfix config. Because of different implementation many mail servers can attempt second connection through very long time instead of your server advised. Your mail can be delayed for a long time, it's not good idea for 21 century ☺

Xiao Guo An (Admin) 9 months ago Reply

That's true if you receive emails from many different domains.

Alan 6 months ago Reply

These seem quite sensible. When I implemented the HELO checks, however, I started to get emails to my local Postmanster account with subject lines like

```
Postfix SMTP server: errors from rrcs-162-155-179-211.central.bi
z.rr.com[162.155.179.211]
```

I assume these are notifying me of rejected messages. How can I suppress these notification emails?

Xiao Guo An (Admin) 6 months ago Reply

Postfix by default does not report rejected messages. Getting this kind of email probably means there's something wrong with your mail server. Usually you can see the reason at the bottom of the email.

Nikolay 🕘 5 months ago ↩ Reply

for what version of postfix is this?

I find lots of options different from my own. I use bit old version –

mail_version = 2.10.1

but this is what I get with CentOS 7. Should I consider upgrade?

Xiao Guo An (Admin) 🕘 5 months ago ↩ Reply

Postfix 3.x on Debian/Ubuntu.

There are several options that are different in Postfix 2.x. You can find the equivalent in Postfix documentation.

Pauli 🕘 4 months ago ↩ Reply

I made it a bit different.

I scheduled download of spammers list IP addresses from https://lists.blocklist.de/lists/mail.txt and new addresses I add to previously downloaded lists. So the list get bigger every day.

When in the list is more then 20 addresses in one range then I block the entire range eg. 176.221.42.0/24.

Example of postfix_blocklist_de file:

```
176.221.42.0/24          REJECT Your IP range is spam added by postfix_blocklist_de since 2019-08-15
```

Postfix conf main.cf:

```
smtpd_recipient_restrictions =
    check_client_access cidr:/root/firewall/postfix_blocklist_de.list
```

I made some whois checking that I do not block IPs registered to well known brands/partners and countries.

I also made whitelisting feature. Since I made this, we eliminated 99.99% of spam.
Of course I filtered from log all blocked addresses to check if there is some false blocking and in two months is no regular email blocked.

Sorry for the English, but certainly you have a clue what have I done ☺

Peet Verstraten 2 months ago Reply

These tips helped me perfectly to block spammers and SMTP AUTH requests from our Zentyal email server. Thanks a lot !

Fernando 1 month ago Reply

Hello,

My server is sending spam emails with my Postfix.

How can that be done? What happened here? Did the get the root password?

Thanks

> Sunil Kumar 1 month ago Reply
>
> I too looking for same.

Matteo 1 week ago Reply

Thanks for your advice, they helped me a lot!
Just a question: pflogsumm configured as you say it sends me a summary email but graylisting warning lines are also included, can they be omitted in some way?

> Xiao Guoan (Admin) 1 week ago Reply
>
> Perhaps you can pipe the pflogsumm report to `sed`, which deletes the lines that contain the word “greylisting”. Of course you need to know how to use the `sed` editor.
>
> > Matteo 1 week ago Reply
> >
> > Yes! I’ve used the command
> >
> > ```
> > sed '/Greylisted/,+1 d'
> > ```
> >
> > to remove the lines containing the word “Greylisted” and the line directly after it.
> > thanks!

Leave a Comment

- Comments with links are moderated by admin before published.
- Your email address will not be published.
- Use **<pre> ... </pre>** HTML tag to quote the output from your terminal/console.
- Please use the community (https://community.linuxbabe.com) for questions unrelated to this article.
- I don't have time to answer every question. Making a donation would incentivize me to spend more time answering questions.

Name

Email

☑ Receive notification via e-mail when someone replies to my comment.

Post Commen

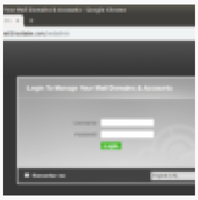
Search ... Search

Select Language ▼

Powered by Google Translate

SaferVPN – 81% OFF

Featured Tutorials



How to Easily Set Up a Full-Featured Mail Server on Ubuntu 18.04 with iRedMail

How to Quickly Set up a Mail Server on Ubuntu 18.04 with Modoboa

ubuntu 18.04 nextcloud nginx

Install NextCloud on Ubuntu

18.04 with Nginx (LEMP Stack)

How to Easily Set up a Full-Fledged Mail Server on Ubuntu 16.04 with iRedMail

atomic wallet linux

How to Install and Use Atomic Wallet on Linux

quickly set up mail server centos 7 modoboa

How to Quickly Set Up a Mail Server on CentOS 7 with Modoboa

install systemback on ubuntu 18.04

How to Install Systemback on Ubuntu 18.04 and Ubuntu 18.10, 16.04

osm tile server ubuntu 18.04 install

How to Set Up OpenStreetMap Tile Server on Ubuntu 18.04

How to Easily Create RAM Disk on Debian, Ubuntu, Linux Mint, CentOS

quickly set up mail server

Quickly Set Up a Mail

debian 9 modoboa

Server on Debian 9 Stretch with Modoboa

pCloud 65% Off Cloud Storage

Follow us

Claim Your $50 Hosting Credit

Recent Posts

How to Install and Use Atomic Wallet on Linux
Linux Terminal and Console Explained For Dummies
Install Roundcube Webmail on Ubuntu 18.04 with Apache/Nginx
How to Stop Your Emails Being Marked as Spam
How To Use SaferVPN on Linux – 81% Off

Search ... Search

Recent Ratings

Vote **5** from **anonymous** on **2 Ways to Upgrade Ubuntu 18.04/18.10 To Ubuntu 19.04 (GUI & Terminal)**
Vote **5** from **anonymous** on **2 Ways to Upgrade From Ubuntu 16.04/17.04 to Ubuntu 17.10 (Graphical & Terminal)**
Vote **5** from **anonymous** on **Linux Terminal and Console Explained For Dummies**
Vote **5** from **anonymous** on **Linux Terminal and Console Explained For Dummies**
Vote **5** from **anonymous** on **How to Install Systemback on Ubuntu 18.04 and Ubuntu 18.10, 16.04**

Home HTML Sitemap Contact Me Donation Privacy Policy Terms & Conditions
Disclaimer Affiliate Disclosure