Set Up SMTP and IMAP Proxy with HAProxy (Debian, Ubuntu, CentOS)

Last Updated: June 19, 2020 Xiao Guoan (Admin) 3 Comments
Mail Server

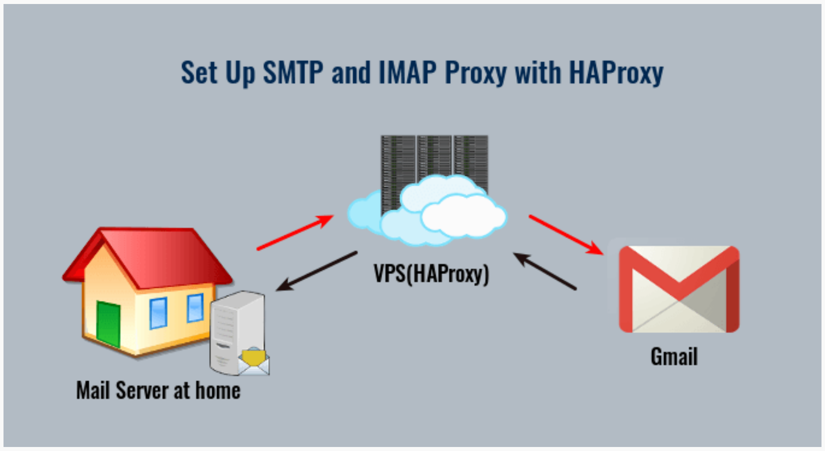
In previous tutorials, we discussed how to set up a mail server from scratch on Linux (Ubuntu version, CentOS/RHEL version), and how to use iRedMail or Modoboa to quickly set up your own mail server without having to manually configure each component of the mail server stack. This tutorial is going to show you how to set up SMTP and IMAP proxy for your mail server with HAProxy.

When Do You Need SMTP and IMAP Proxy?

Some folks run email servers at home, but may have the following problems:

- Port 25 is blocked.
- They don’t have a static IP address.
- They can’t create PTR record.

If port 25 is blocked, you can’t send emails directly to recipients. And if you don’t have static IP address or PTR record, your emails are likely to be rejected or land into the spam folder. If you are in this situation, you can run a VPS (Virtual Private Server) at a data center and use it as a proxy for your mail server. The VPS has a static IP address and you can create PTR record for the IP address. Other email servers would think that the VPS runs your mail service and when you send an email, they would think the email comes from your VPS.



Yes, you can also use SMTP relay services such as Mailjet to solve these problems, but there's a limit on how many emails you can send each day and each month. If you upgrade to a paid account with Mailjet, it costs at least $9.65 each month. The more emails you send, the higher your monthly cost will be. If you run a VPS and set up mail proxy, it costs about $5 per month no matter how many emails you are going to send.

If you run a mail server for lots of people, you might need to set up mail proxy for load balancing and high availability. In this article, I will set up SMTP and IMAP proxy with HAProxy, which is a free, open-source high availability load balancer and proxy server for TCP and HTTP-based applications.

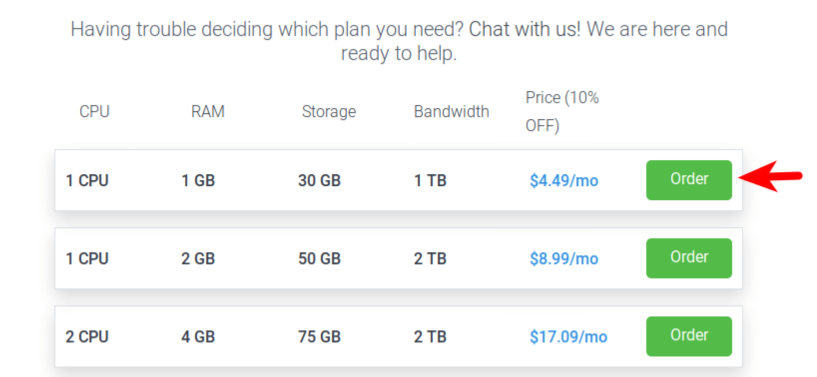
Step 1: Choose the Right VPS for Mail Proxy

You need a VPS that

- allows you to create PTR record
- doesn't block port 25
- allows you to send unlimited emails without restrictions.

Not all VPS providers meet the above 3 requirements. For example, DigitalOcean blocks port 25 and it would not unblock port 25. If you use Vultr VPS, then port 25 is blocked by default. They can unblock it if you open a support ticket, but they may block it again at any time if they decide your email sending activity is not allowed. Vultr actually may re-block it if you use their servers to send newsletters.

I run my mail server on hostwinds, and I always recommend it when setting up mail server. An entry-level VPS is enough to run mail proxy, so you can choose the $4.49/month unmanaged Linux VPS plan. You can choose any Linux distro for your VPS, but I recommend you to use Debian, Ubuntu, or CentOS.



Having trouble deciding which plan you need? Chat with us! We are here and ready to help.

CPU	RAM	Storage	Bandwidth	Price (10% OFF)	
1 CPU	1 GB	30 GB	1 TB	$4.49/mo	Order
1 CPU	2 GB	50 GB	2 TB	$8.99/mo	Order
2 CPU	4 GB	75 GB	2 TB	$17.09/mo	Order

Once you created an account, Hostwinds will send you an email with the server SSH login details. To log into your server, you use an SSH client. If you are using Linux or macOS on your computer, then simply open up a terminal window and run the following command to log into your server. Replace 12.34.56.78 with the IP address of your VPS.

```
ssh root@12.34.56.78
```

You will be asked to enter the password. If you are using Windows, please read the following article on how to use SSH client.

- 3 Ways to Use SSH on Windows to Log Into Linux Server

Step 2: Set Up VPN Server on Your VPS

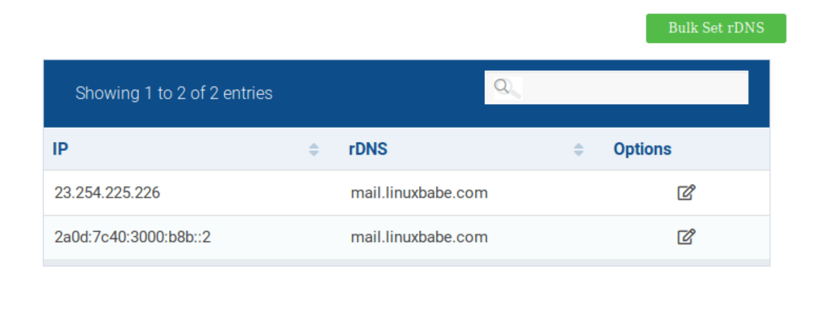
If you have a dynamic IP address at your home, then you need to set up a VPN server on your VPS, so your VPS will be able to communicate with your mail server without being interrupted due to the change of IP address. The VPN server can also help you bypass port 25 blocking.

You can set up WireGuard VPN on your VPS by following one of the tutorials below. Why do I choose WireGuard instead of other VPN protocols like OpenVPN? Because WireGuard allows you to assign static private IP addresses to VPN clients.

- Set Up Your Own WireGuard VPN Server on Ubuntu
- Set Up Your Own WireGuard VPN Server on Debian
- Set Up Your Own WireGuard VPN Server on CentOS

When following the instructions in the above articles, your VPS is the VPN server and your mail server is the VPN client. The VPS will become the default gateway for your mail server and all outbound traffic on your mail server will be tunneled through VPN, so receiving SMTP servers (Gmail, Hotmail, Yahoo Mail, etc) will think your emails come from the VPS.

You should set a PTR record, aka reverse DNS record, for your VPS. To edit the PTR record for Hostwinds VPS, log into Hostwinds client area, select `Domains` -> `Manage rDNS`, Then you can edit the reverse DNS record for both IPv4 and IPv6 addresses.



Showing 1 to 2 of 2 entries

IP	rDNS	Options
23.254.225.226	mail.linuxbabe.com	✎
2a0d:7c40:3000:b8b::2	mail.linuxbabe.com	✎

Step 3: Open Ports in Firewall and Set Up Permissions

The VPS needs to open port 25, 587, 465, 143 and 993 in the firewall. Run the following commands to open these ports.

Debian/Ubuntu:

```
sudo ufw allow 25,587,465,143,993/tcp
```

CentOS:

```
sudo firewall-cmd --permanent --add-service={smtp,smtp-submission,smtps,imap,imaps}

sudo systemctl reload firewalld
```

The mail server needs to open various ports to the VPS. Run the following command.

Debian/Ubuntu:

```
sudo ufw insert 1 allow in from 10.10.10.0/24
```

CentOS:

```
sudo firewall-cmd --permanent --add-rich-rule='rule family="ipv4" source address="10.10.10.0/24" accept'

sudo systemctl reload firewalld
```

`10.10.10.0/24` is the private IP range created by the VPN server, so the VPS can access all ports on the mail server.

Configure SELinux on CentOS

Later in this tutorial, HAProxy on the VPS needs to bind to various email ports like 25, 587, 465, 143 and 993, but is prevented from doing so by SELinux. If you use CentOS on the VPS, you need to run the following command to allow HAProxy to bind to these ports.

```
sudo setsebool -P haproxy_connect_any 1
```

Step 4: Set Up SMTP Proxy to Receive Email

Now you need to set up SMTP proxy so that other mail servers can send emails to your own mail server via the VPS. SSH into your VPS and install HAProxy.

Debian/Ubuntu

```
sudo apt install haproxy
```

CentOS

```
sudo dnf install haproxy
```

Then edit the HAProxy main configuration file.

```
sudo nano /etc/haproxy/haproxy.cfg
```

Add the following lines at the end of the file. Replace `12.34.56.78` with the public IP address of your VPS.

Replace `10.10.10.101` with the private IP address of your mail server, which is assigned by your VPN server.

```
frontend ft_smtp
      bind 12.34.56.78:25
      mode tcp
      timeout client 1m
      log global
      option tcplog
      default_backend bk_smtp

backend bk_smtp
      mode tcp
      log global
      option tcplog
      timeout server 1m
      timeout connect 7s
      server postfix 10.10.10.101:252
5 send-proxy
```

The above configuration will make HAProxy listen on port 25 and pass SMTP connections to port 2525 of your mail server. Save and close the file. Restart HAProxy.

```
sudo systemctl restart haproxy
```

And enable auto-start at boot time.

```
sudo systemctl enable haproxy
```

To use HAProxy as a reverse proxy for the Postfix SMTP server, you need to enable Postscreen in Postfix. SSH into your mail server and edit the Postfix master configuration file.

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

Add the following lines at the beginning of this file. Replace `10.10.10.101` with the private IP address of your mail server assigned by VPN server. This will enable Postscreen on port 2525 and it can accept HAProxy connections from your VPS. Postfix is able to obtain the original IP address of SMTP client from HAProxy.

```
10.10.10.101:2525      inet  n
 -       -       -       1       post
screen
  -o postscreen_upstream_proxy_protoc
ol=haproxy
  -o postscreen_cache_map=btree:$data
_directory/postscreen_2525_cache
  -o syslog_name=postfix/2525
```

Then uncomment the following 3 lines. (**Note:** If you use iRedMail or Moboboa to run your mail server, then the following 3 lines are uncommented by default.)

```
smtpd     pass  -       -       y
-       -       smtpd
dnsblog   unix  -       -       y
-       0       dnsblog
tlsproxy  unix  -       -       y
-       0       tlsproxy
```

Where:

- The first line will make Postscreen pass SMTP connection to `smtpd` daemon.
- The dnsblog (DNS Blacklist Logger) service enables logging of DNS blacklist checks.
- The tlsproxy service enables STARTTLS support for postscreen, so remote SMTP clients can establish

encrypted connection when Postscreen is enabled.

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

```
sudo systemctl restart postfix
```

Now add a new MX record for your domain name like below, and your mail server is able to receive emails via the VPS.

```
Record Type    Name      Mail Server             Priority

MX             @         hostname-of-your-VPS    0
```

Don’t forget to add A record for the hostname of your VPS.

Step 5: Set Up Submission Proxy

Your users can submit outgoing emails to your mail server without proxy, but what if you want your users to be able to submit outgoing emails through the VPS? You need to set up proxy for the Postfix submission service.

Edit the HAProxy main configuration file on your VPS.

```
sudo nano /etc/haproxy/haproxy.cfg
```

Add the following lines at the end of the file. Replace `12.34.56.78` with the public IP address of your VPS. Replace `10.10.10.101` with the private IP address of your mail server, which is assigned by your VPN server.

```
frontend ft_submission
      bind 12.34.56.78:587
      mode tcp
      timeout client 1m
      log global
      option tcplog
      default_backend bk_submission

backend bk_submission
      mode tcp
      log global
      option tcplog
      timeout server 1m
      timeout connect 7s
      server postfix 10.10.10.101:105
87 send-proxy

frontend ft_submissions
      bind 12.34.56.78:465
      mode tcp
      timeout client 1m
      log global
      option tcplog
      default_backend bk_submissions

backend bk_submissions
      mode tcp
      log global
      option tcplog
      timeout server 1m
      timeout connect 7s
      server postfix 10.10.10.101:104
65 send-proxy
```

There are commonly two ports that can accept email submissions from authenticated users: 587 and 465. So in the above configuration, we defined two front ends in HAProxy listening on port 587 and 465. They will pass connections to port 10587 and 10465 of your mail server, respectively.

Save and close the file. Restart HAProxy.

```
sudo systemctl restart haproxy
```

Then edit Postfix master configuration file on your mail server.

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

Add the following lines at the end of this file. Replace `10.10.10.101` with the private IP address of your mail server, which is assigned by your VPN server. Please allow at least one whitespace (tab or spacebar) before `-o`. In postfix configurations, a preceding whitespace character means that this line is continuation of the previous line. However, you should not add space before or after the equal sign (`=`).

```
10.10.10.101:10587     inet     n
 -    y    -    -    smtpd
  -o syslog_name=postfix/10587
  -o smtpd_tls_security_level=encrypt
  -o smtpd_tls_wrappermode=no
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_relay_restrictions=permit_
sasl_authenticated,reject
  -o smtpd_recipient_restrictions=per
mit_mynetworks,permit_sasl_authentica
ted,reject
  -o smtpd_sasl_type=dovecot
  -o smtpd_sasl_path=private/auth
  -o smtpd_upstream_proxy_protocol=ha
proxy

10.10.10.101:10465     inet   n
```

```
 -       y       -       -       smtpd
  -o syslog_name=postfix/10465
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_recipient_restrictions=permit_mynetworks,permit_sasl_authenticated,reject
  -o smtpd_sasl_type=dovecot
  -o smtpd_sasl_path=private/auth
  -o smtpd_upstream_proxy_protocol=haproxy
```

In the above configuration, we enabled two submission services listening on port 10587 and 10465, and they support the `haproxy` protocol, so they will be able to accept connections from HAProxy. Save and close the file. Restart Postfix for the change to take effect.

```
sudo systemctl restart postfix
```

Step 6: Set Up IMAP Proxy

We also want users to be able to log into the IMAP server via the VPS, so we need to set up IMAP proxy.

Edit the HAProxy main configuration file on your VPS.

```
sudo nano /etc/haproxy/haproxy.cfg
```

Add the following lines at the end of the file. Replace `12.34.56.78` with the public IP address of your VPS. Replace `10.10.10.101` with the private IP address of your mail server, which is assigned by your VPN server.

```
frontend ft_imap
    bind 12.34.56.78:143
    mode tcp
    default_backend bk_imap

backend bk_imap
    mode tcp
    balance leastconn
    stick store-request src
    stick-table type ip size 200k expire 30m
    server imap1 10.10.10.101:1109 send-proxy-v2

frontend ft_imaps
    bind 12.34.56.78:993
    mode tcp
    default_backend bk_imaps

backend bk_imaps
    mode tcp
    balance leastconn
    stick store-request src
    stick-table type ip size 200k expire 30m
    server imaps1 10.10.10.101:10993 send-proxy-v2
```

There are two ports for the IMAP service: 143 and 993. Port 143 can use STARTTLS and port 993 uses implicit TLS, so in the above configuration, we added two front ends in HAproxy listening on port 143 and 993. They will pass connections to port 1109 and 10993 of your mail server, respectively. Save and close the file. Restart HAProxy.

```
sudo systemctl restart haproxy
```

Edit Dovecot configuration file on your mail server.

```
sudo nano /etc/dovecot/conf.d/10-master.conf
```

Add HAProxy support for IMAP and IMAPS like below.

```
service imap-login {
  inet_listener imap {
    port = 143
  }
  inet_listener imaps {
    port = 993
    ssl = yes
  }

  inet_listener imap_haproxy {
    port = 1109
    haproxy = yes
  }
  inet_listener imaps_haproxy {
    port = 10993
    ssl = yes
    haproxy = yes
  }
}
```

In the above configuration, we enabled two IMAP services: `imap_haproxy` and `imaps_haproxy`, listening on port 1109 and 10193, respectively. They support the `haproxy` protocol, so they will be able to accept connections from HAProxy. Save and close the file.

Then we need to add trusted proxy hosts in Dovecot. Edit the Dovecot main configuration file.

```
sudo nano /etc/dovecot/dovecot.conf
```

Add the following two lines at the end of this file. Replace `10.10.10.1` with the private IP address of your VPN server.

```
haproxy_trusted_networks = 10.10.10.1
haproxy_timeout = 3s
```

Save and close the file. Restart Dovecot for the change to take effect.

```
sudo systemctl restart dovecot
```

Now you should be able to log into the IMAP server and submit outgoing emails via the VPS.

Final Thoughts

Notice that we enabled proxy support for Postfix and Dovecot by adding more listening ports (2525, 10587, 10465, 1109, 10993). We didn’t enable proxy support for existing ports (25, 587, 465, 143 and 993), because if we do, then Postfix and Dovecot will accept connections from HAProxy only and deny connection from other IP addresses, including localhost. This can prevent your webmail or web application running on the mail server to use `127.0.0.1:25` to send emails, and prevent the webmail client from fetching emails from Dovecot. You will probably see the following error when this happens.

```
host mail.example.com refused to talk
to me: 421 4.3.2 No system resources
```

And your Postfix SMTP server would log the following message in the mail log.

```
postfix/postscreen[1479]: warning: haproxy read: time limit exceeded
```

Configure HAProxy Automatic Restart

I found the `haproxy.service` on CentOS/RHEL can fail to start at boot time. The error is as follows.

```
Starting frontend ft_smtp: cannot bind socket [23.254.225.226:25]
```

If I manually start the service, it works, which is confusing to me. To solve this issue, we can edit the `haproxy.service` to make it automatically restart on failure. To override the default systemd service configuration, we create a separate directory.

```
sudo mkdir -p /etc/systemd/system/haproxy.service.d/
```

Then create a file.

```
sudo nano /etc/systemd/system/haproxy.service.d/restart.conf
```

Add the following lines in the file.

```
[Service]
Restart=always
RestartSec=5s
```

Save and close the file. Then reload systemd.

```
sudo systemctl daemon-reload
```

Postfix/Dovecot Automatic Restart

It’s also recommended to configure Postfix and Dovecot on the mail server to automatically restart on failure.

Postfix

Create a separate directory.

```
sudo mkdir -p /etc/systemd/system/postfix.service.d/
```

Then create a file.

```
sudo nano /etc/systemd/system/postfix.service.d/restart.conf
```

Add the following lines in the file. Note that on Debian/Ubuntu, the `postfix.service` is an `oneshot` service, which doesn’t allow `Restart=always`.

```
[Service]
Restart=on-failure
RestartSec=5s
```

Save and close the file. Then reload systemd.

```
sudo systemctl daemon-reload
```

Dovecot

Create a separate directory.

```
sudo mkdir -p /etc/systemd/system/dovecot.service.d/
```

Then create a file.

```
sudo nano /etc/systemd/system/dovecot.service.d/restart.conf
```

Add the following lines in the file.

```
[Service]
Restart=always
RestartSec=5s
```

Save and close the file. Then reload systemd.

```
sudo systemctl daemon-reload
```

IP Blacklist Removal

What if the IP address of your VPS is blacklisted by a particular email service provider? You can read the following article to learn how to get your IP address removed from blacklists.

- Mail Server IP Blacklist Removal Tips to Improve Email Deliverability

I hope this tutorial helped you set up SMTP and IMAP proxy. 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: 3 Average: 5]

HAproxy Linux Server