Configure Postfix for mail forwarding

You can use `postfix` to forward mail from domains that you control the MX records for.

This how-to comes from following the Setup mail forwarding in postfix post.

Take care. Mail servers on port 25 get attacked constantly. A wide open SMTP mail server configuration ***will*** be exploited.

The Postfix documentation is also useful.

Configure DNS records

Go to the AWS Console and create a new ***Hosted Zone*** for the domain.

In Namecheap go to the Domain tab and select ***Custom DNS*** and copy in the nameservers from the AWS record set.

Configure a new A record set for the domain, pointing it to the IP address of the server, e.g. `5.6.7.8`

Configure an MX record set for the domain, in the format `10 my-domain.com` The 10 is the priority of the mail server.

Run the `dig` command to ensure that the `A` and `MX` records are correct:

```
dig <domain> a
dig <domain> mx
```

When everything has propagated correctly, proceed to setting up `postfix`.

Install `postfix`

On the server, run:

```
sudo apt-get install postfix
```

For the default domain name, use `<system>.<domain>`.

Find the location of the `config_directory` with:

```
postconf | grep config_directory
```

Usually this is `/etc/postfix`. First, let's turn off backward compatibility to avoid messages in the log:

```
sudo postconf compatibility_level=2
```

Now edit the main config file:

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

Set `myhostname=<machine>.<domain>`. Then add:

```
virtual_alias_domains = <domain> <my-other-domain>
virtual_alias_maps = hash:/etc/postfix/virtual
```

The `mydestination` parameter specifies what domains this machine will deliver locally, instead of forwarding to another machine. It should contain `mydestination=$myhostname, <machine>, localhost.localdomain, localhost`. That's it.

You can add multiple domains for `virtual_alias_domains` separated by spaces. Now add a `virtual` file with `sudo vi /etc/postfix/virtual` and add:

```
# Emails to be forwarded

admin@<domain> person1@<otherdomain> person2@<otherdomain>
```

NOTE: You can use `@<domain>` to forward ***all*** emails, but ***don't*** because it breaks ***recipient validation***.

Now generate the hash for the `virtual` file:

```
sudo postmap /etc/postfix/virtual
```

And reload `postfix` configuration:

```
sudo systemctl restart postfix
sudo systemctl status postfix
```

Check the log for errors.

Finally, if everything check out, configure the firewall to allow port 25 in:

```
sudo ufw allow smtp
```

Send a test email from another account. You can watch `/var/log/mail.log` to see the email coming in and being processed through the server.

Test Outbound Mail

Go to another machine that is connected to the same network as the Postfix server. Run `telnet`:

```
telnet <mail-server> smtp
Trying 1.2.3.4...
Connected to <mail-server>.
Escape character is '^]'.
220 <mail-server> ESMTP Postfix (Ubuntu)
HELO gmail.com
250 <mail-server>
mail from: yourname@gmail.com
250 2.1.0 Ok
rcpt to: yourname@gmail.com
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Hey, just a test
.
250 2.0.0 Ok: queued as 1BAD34C1104
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

If all is well, you should get an email at `yourname@gmail.com`.

Here is another way to test:

```
mailx -s "Test" -r support@yourdomain.com -aFrom:Support\
<support@yourdomain.com\> yourname@gmail.com < /dev/null
```

PTR Record

Make request to you ISP to add a reverse PTR record.

SPF Record

Use the SPF Wizard to generate an SPF record and add it to the DNS records for the domain.

DKIM Record

Install DKIM tools:

```
sudo apt install opendkim opendkim-tools
```

Add to `/etc/opendkim.conf`:

```
# Commonly-used options; the commented-out versions show the defaults.
#
Canonicalization simple
Mode sv
SubDomains no

# Map AuthorDomains to RSA keys.
#
KeyTable /etc/dkimkeys/rsakeys.table
SigningTable refile:/etc/dkimkeys/signingdomains.table

# Entries from https://www.postfix.io/how-to-configure-opendkim-with-
postfix/
#
AutoRestart yes
AutoRestartRate 10/1M
Background yes
DNSTimeout 5
SignatureAlgorithm rsa-sha256
OversignHeaders From
```

Generate RSA key:

```
cd /etc/dkimkeys/
opendkim-genkey --bits=1024 --selector=key1 --domain=<domain> --append-
domain
```

Rename the files:

```
mv key1.private key1.<domain>.rsa
mv key1.private key1.<domain>.txt
```

Add the `TXT` record given in the `.txt` file to the DNS entry for `<domain>`.

Add to `/etc/dkimkeys/rsakeys.table`:

```
<domain-key> <domain>:key1:/etc/dkimkeys/key1.<domain>.rsa
```

Add to `/etc/dkimkeys/signingdomains.table`:

```
*@<domain> <domain-key>
```

This says that any email from `@<domain>` should be signed with the `<domain-key>` key.

Create a sandboxed DKIM socket:

```
mkdir /var/spool/postfix/opendkim
```

Add `postfix` user to `opendkim` group:

```
sudo adduser postfix opendkim
```

Set file permissions:

```
chown -R opendkim:opendkim /etc/opendkim.conf /etc/dkimkeys
chown -R opendkim:opendkim /var/spool/postfix/opendkim
```

Add to `/etc/postfix`:

```
# OpenDKIM
milter_default_action = accept
milter_protocol = 6
smtpd_milters = unix:opendkim/opendkim.sock
non_smtpd_milters = unix:opendkim/opendkim.sock
```

Restart services:

```
systemctl restart opendkim.service
systemctl restart postfix.service
```

Send test emails and monitors logs.

DMARC

Add this TXT record:

```
"v=DMARC1;p=quarantine;pct=100;rua=mailto:admin@<yourdomain>"
```

You will get daily emails containing XML reports on how your email is being percieved by other email servers.