



School of Computer Science & Engineering
Trustworthy Systems Group

Running your own Mail Server

Peter Chubb

`peter.chubb@unsw.edu.au`

16 April 2024



Why Bother?



Why Bother?



 iCloud

Why Bother?



Apple iCloud

Proton Mail

Why Bother?



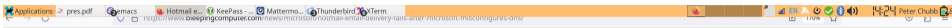
Proton Mail

If you're not paying for a product
You **are** the product

Who chooses which email you see?

Who chooses which email you see?
Who chooses what emails you can
send?

Hotmail example



Hotmail email delivery fails after Microsoft misconfigures DNS

By [Lawrence Abrams](#)

August 18, 2023

11:44 AM

2



Hotmail users worldwide have problems sending emails, with messages flagged as spam or not delivered after

POPULAR STORIES

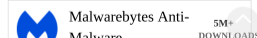


Canada to ban the Flipper Zero to stop surge in car thefts



Microsoft: Outlook clients not syncing over Exchange ActiveSync

LATEST DOWNLOADS



Protonmail example



Government to block ProtonMail after bomb threat: Company responds to India | - Times of India — Mozilla Firefox

Government to block ProtonMail after bomb threat: Company responds to India | - Times of India

https://timesofindia.indiatimes.com/gadgets-news/government-to-block-protonmail-after-bomb-threat-company-responds-.../story.html

EDITION IN DELHI 31°C

THE TIMES OF INDIA [SUBSCRIBE TO TOI](#) [SIGN IN](#) [f](#) [t](#) [v](#) [y](#) [in](#)

Tech Gadgets News AI New Blog Tech News Gadgets Reviews Top Gadgets Slideshows Videos How To Featured **Today's ePaper**

Now Playing After India trip, Priyanka Chopra Jonas resumes work on 'Heads of State' in LA

NEWS / GADGETS NEWS / Govt blocking ProtonMail After Bomb Threat: Can't Directly Answer ...

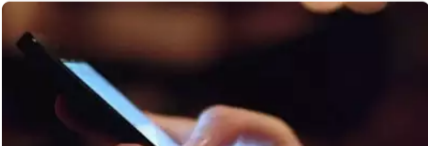
TRENDING Vivo V30 Pro Sundar Pichai OnePlus Nord Ce 4 Garena Free Fire Max Codes Wordle Today Digital Sign

Govt blocking ProtonMail after bomb threat: Can't directly answer to India and other things that the company said

TOI Tech Desk / TIMESOFINDIA.COM / Feb 15, 2024, 12:12 IST

[SHARE](#) [PRINT](#) [AA](#) [FOLLOW US](#)

The IT ministry plans to block ProtonMail at the request of Tamil Nadu police due to a bomb threat. ProtonMail is working with Indian authorities. The decision was taken by the 69A blocking committee and reported by Hindustan Times.



Trending Stories

In Section Entire Website

- Garena Free Fire MAX redeem codes for April 5: Win weapons, diamonds, and other...
- Infosys founder NR Narayana Murthy: Most of you have not experienced hunger. I have ...
- Blinkit to deliver Sony PlayStation 5 Slim to your doorstep in 10-minutes
- Google may be in talks to buy online marketing software company HubSpot in its...
- Amazon still has this 'serious problem' in the US that it 'solved' in India in 2020, claims...

ET Money

Save up to **₹62,400** in taxes & get monthly pension for life

[Invest in NPS on ET Money](#)

Therefore...



- Run own email server
 - Make own mistakes

Therefore...



- Run own email server
 - Make own mistakes
 - Freedom of choice: domain name; email addresses.
 - Privacy guaranteed

Therefore...



- Run own email server
 - Make own mistakes
 - Freedom of choice: domain name; email addresses.
 - Privacy guaranteed — with some caveats
 - Get good logging to detect and fix issues

Therefore...



- Run own email server
 - Make own mistakes
 - Freedom of choice: domain name; email addresses.
 - Privacy guaranteed — with some caveats
 - Get good logging to detect and fix issues
 - At-home storage is cheap

What we want



- Legitimate email generated from our domain(s) to be delivered.

What we want



- Legitimate email generated from our domain(s) to be delivered.
- Legitimate email to our domain(s) to be delivered to us

What we want



- Legitimate email generated from our domain(s) to be delivered.
- Legitimate email to our domain(s) to be delivered to us
- Incoming spam to be detected and dealt with as early as possible

What we want

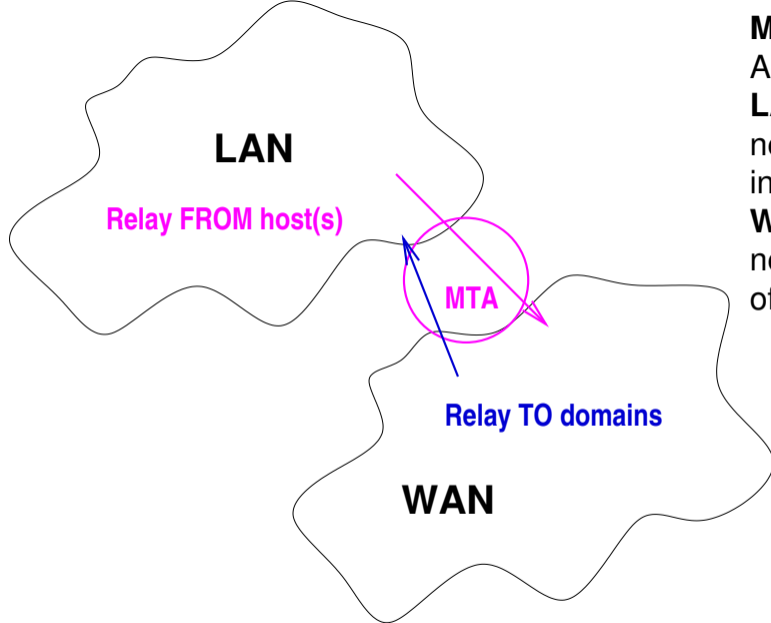


- Legitimate email generated from our domain(s) to be delivered.
- Legitimate email to our domain(s) to be delivered to us
- Incoming spam to be detected and dealt with as early as possible
- Very difficult for spammers to send email via our systems

What we want



- Legitimate email generated from our domain(s) to be delivered.
- Legitimate email to our domain(s) to be delivered to us
- Incoming spam to be detected and dealt with as early as possible
- Very difficult for spammers to send email via our systems
- Very difficult for spammers to pretend to be our domain(s)



MTA: Mail Transfer Agent(s)

LAN: Local area network: your internal addresses

WAN: Wide area network: the rest of the internet



What you need



- on a server that has a DNS A record pointing to it:
- and that has port 25 open to the world
- And a suitable MTA on that server:

```
sudo apt install exim4
```

What you need



- on a server that has a DNS A record pointing to it:
- and that has port 25 open to the world
- And a suitable MTA on that server:

```
sudo apt install exim4  
sudo dpkg-reconfigure exim4-config
```

What you need



- on a server that has a DNS A record pointing to it:
- and that has port 25 open to the world
- And a suitable MTA on that server:

```
sudo apt install exim4
sudo dpkg-reconfigure exim4-config
sudo service exim4 restart
```

What that gives you



- Sending and receiving email
 - using tools like `mutt` or `mailx`

What that gives you



- Sending and receiving email
 - using tools like `mutt` or `mailx`
- *Some* spam protection

What that gives you



- Sending and receiving email
 - using tools like `mutt` or `mailx`
- *Some* spam protection — can be beefed up

What that gives you



- Sending and receiving email
 - using tools like `mutt` or `mailx`
- *Some* spam protection — can be beefed up
- Attacks from wannabe spammers

What that gives you



- Sending and receiving (**internal**) email
 - using tools like `mutt` or `mailx`
- *Some* spam protection — can be beefed up
- Attacks from wannabe spammers

What that gives you



- Sending and receiving **(internal)** email
 - using tools like `mutt` or `mailx`
- *Some* spam protection — can be beefed up
- Attacks from wannabe spammers

30 years ago this worked

spammers

- DNS blacklist: Known spammers

- DNS blacklist: Known spammers
- DNS blacklist: Open Relays

Responses



- DNS blacklist: Known spammers
- DNS blacklist: Open Relays
- DNS blacklist: dynamic IP blocks

- DNS blacklist: Known spammers
- DNS blacklist: Open Relays
- DNS blacklist: dynamic IP blocks
- ISPs block outgoing port 25

- DNS blacklist: Known spammers
- DNS blacklist: Open Relays
- DNS blacklist: dynamic IP blocks
- ISPs block outgoing port 25

Upshot: **Much harder to run own MTA**

SMTP protocol



On port 25:

```
220 mx.example.com ESMTP Exim 4.96 Thu, 14 Mar 2024 15:41:5
```

SMTP protocol



On port 25:

```
220 mx.example.com ESMTP Exim 4.96 Thu, 14 Mar 2024 15:41:5  
HELO example.org
```

SMTP protocol



On port 25:

```
220 mx.example.com ESMTP Exim 4.96 Thu, 14 Mar 2024 15:41:5  
HELO example.org  
250 mx.example.com Hello example.org [93.184.216.34]
```

SMTP protocol



On port 25:

```
220 mx.example.com ESMTP Exim 4.96 Thu, 14 Mar 2024 15:41:5
HELO example.org
250 mx.example.com Hello example.org [93.184.216.34]
MAIL FROM: <user@example.org> ← Envelope FROM address
```

SMTP protocol



On port 25:

```
220 mx.example.com ESMTP Exim 4.96 Thu, 14 Mar 2024 15:41:5
HELO example.org
250 mx.example.com Hello example.org [93.184.216.34]
MAIL FROM: <user@example.org> ← Envelope FROM address
250 OK
```


SMTP protocol



On port 25:

```
220 mx.example.com ESMTP Exim 4.96 Thu, 14 Mar 2024 15:41:5
HELO example.org
250 mx.example.com Hello example.org [93.184.216.34]
MAIL FROM: <user@example.org> † Envelope FROM address
250 OK
RCPT TO: <anotheruser@example.com> † Envelope TO address
```

SMTP protocol



On port 25:

```
220 mx.example.com ESMTP Exim 4.96 Thu, 14 Mar 2024 15:41:5
HELO example.org
250 mx.example.com Hello example.org [93.184.216.34]
MAIL FROM: <user@example.org> † Envelope FROM address
250 OK
RCPT TO: <anotheruser@example.com> † Envelope TO address
250 Accepted
```

SMTP protocol



On port 25:

```
220 mx.example.com ESMTP Exim 4.96 Thu, 14 Mar 2024 15:41:5
HELO example.org
250 mx.example.com Hello example.org [93.184.216.34]
MAIL FROM: <user@example.org> † Envelope FROM address
250 OK
RCPT TO: <anotheruser@example.com> † Envelope TO address
250 Accepted
DATA
```

SMTP protocol



On port 25:

```
220 mx.example.com ESMTP Exim 4.96 Thu, 14 Mar 2024 15:41:5
HELO example.org
250 mx.example.com Hello example.org [93.184.216.34]
MAIL FROM: <user@example.org> † Envelope FROM address
250 OK
RCPT TO: <anotheruser@example.com> † Envelope TO address
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
```

Subject: Get your lovely spam nice and fresh
Date: Thu, 14 Mar 2024 15:02:42 +1100
From: Someone <you@aaa.bbb>
To: Important Person <you@aaa.bbb>
Message-ID: <string-of-characters@aaa.bbb>

Message body here

•

```
Subject: Get your lovely spam nice and fresh
Date: Thu, 14 Mar 2024 15:02:42 +1100
From: Someone <you@aaa.bbb>
To: Important Person <you@aaa.bbb>
Message-ID: <string-of-characters@aaa.bbb>
```

Message body here

.

```
250 OK id=1rkd6Q-00DHzg-2N
```

What we want



Origin	Envelope To	Envelope from	Action	rule
LAN	Anywhere	Our domain	Accept	relay_from_hosts

What we want



Origin	Envelope To	Envelope from	Action	rule
LAN	Anywhere	Our domain	Accept	relay_from_hosts
WAN	Our domain	Anywhere except our Domain	Accept	relay_to_domains local_domains

What we want



Origin	Envelope To	Envelope from	Action	rule
LAN	Anywhere	Our domain	Accept	relay_from_hosts
WAN	Our domain	Anywhere except our Domain	Accept	relay_to_domains local_domains
WAN	Anywhere	Our domain	????	

What we want



Origin	Envelope To	Envelope from	Action	rule
LAN	Anywhere	Our domain	Accept	relay_from_hosts
WAN	Our domain	Anywhere except our Domain	Accept	relay_to_domains local_domains
WAN	Anywhere	Our domain	<i>If Authenticated</i>	allow-authenticated

Reject all others.

220 mx.example.com ESMTP Exim 4.97 Tue, 02 Apr 2024 13:49:3



220 mx.example.com **ESMTP** Exim 4.97 Tue, 02 Apr 2024 13:49:3

```
220 mx.example.com ESMTTP Exim 4.97 Tue, 02 Apr 2024 13:49:33  
ehlo example.org
```

```
220 mx.example.com ESMTP Exim 4.97 Tue, 02 Apr 2024 13:49:33
ehlo example.org
250-mx.example.com Hello example.org [93.184.216.34]
250-SIZE 52428800
250-8BITMIME
250-PIPELINING
250-PIPECONNECT
250-CHUNKING
250-STARTTLS
250-PRDR
250 HELP
```

```
220 mx.example.com ESMTP Exim 4.97 Tue, 02 Apr 2024 13:49:33
ehlo example.org
250-mx.example.com Hello example.org [93.184.216.34]
250-SIZE 52428800
250-8BITMIME
250-PIPELINING
250-PIPECONNECT
250-CHUNKING
250-STARTTLS
250-PRDR
250 HELP
```

After the TLS handshake



...

After the TLS handshake



...

EHLO gram

After the TLS handshake



...

`EHLO gram`

```
250 mx.example.com Hello example.org [93.184.216.34]
```

```
250-SIZE 52428800
```

```
250-8BITMIME
```

```
250-PIPELINING
```

```
250-PIPECONNECT
```

```
250-AUTH PLAIN
```

```
250-CHUNKING
```

```
250-PRDR
```

```
250 HELP
```

After the TLS handshake



...

EHLO gram

250 mx.example.com Hello example.org [93.184.216.34]

250-SIZE 52428800

250-8BITMIME

250-PIPELINING

250-PIPECONNECT

250-AUTH PLAIN

250-CHUNKING

250-PRDR

250 HELP

exim4 log extract



```
2024-03-29 00:00:28 plain_saslauthd_server authenticator fa
(dynamic-ip-adsl.viettel.vn) [27.72.47.150]:
535 Incorrect authentication data (set_id=user@example.com)
2024-03-29 00:00:52 plain_saslauthd_server authenticator fa
(226-144-19-223-on-nets.com) [223.19.144.226]:
535 Incorrect authentication data (set_id=user)
2024-03-29 00:41:44 plain_saslauthd_server authenticator fa
62.67.50.210.sta.wbroadband.net.au [210.50.67.62]:
535 Incorrect authentication data (set_id=user@example.com)
2024-03-29 00:42:23 plain_saslauthd_server authenticator fa
(host-80-241-253-238.customer.magticom.ge) [2.57.219.2]:
535 Incorrect authentication data (set_id=user)
```

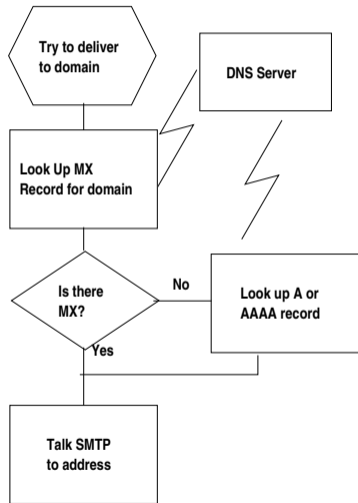
```
2024-03-29 00:00:28 plain_saslauthd_server authenticator fa
(dynamic-ip-adsl.viettel.vn) [27.72.47.150]:
535 Incorrect authentication data (set_id=user@example.com)
2024-03-29 00:00:52 plain_saslauthd_server authenticator fa
(226-144-19-223-on-nets.com) [223.19.144.226]:
535 Incorrect authentication data (set_id=user)
2024-03-29 00:41:44 plain_saslauthd_server authenticator fa
62.67.50.210.sta.wbroadband.net.au [210.50.67.62]:
535 Incorrect authentication data (set_id=user@example.com)
2024-03-29 00:42:23 plain_saslauthd_server authenticator fa
(host-80-241-253-238.customer.magticom.ge) [2.57.219.2]:
535 Incorrect authentication data (set_id=user)
```

How to deliver email

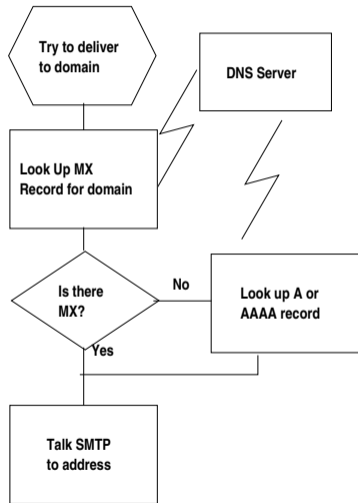


To work out who to deliver general email to

1. Look for an MX record



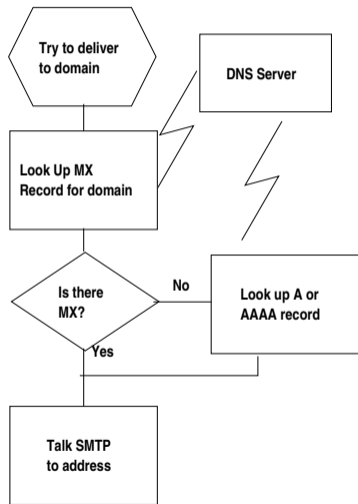
How to deliver email



To work out who to deliver general email to

1. Look for an MX record
2. if there is no MX, attempt AAAA or A

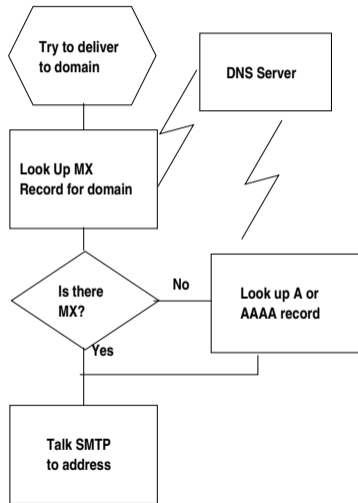
How to deliver email



To work out who to deliver general email to

1. Look for an MX record
2. if there is no MX, attempt AAAA or A
3. Attempt to connect to lowest numbered MX

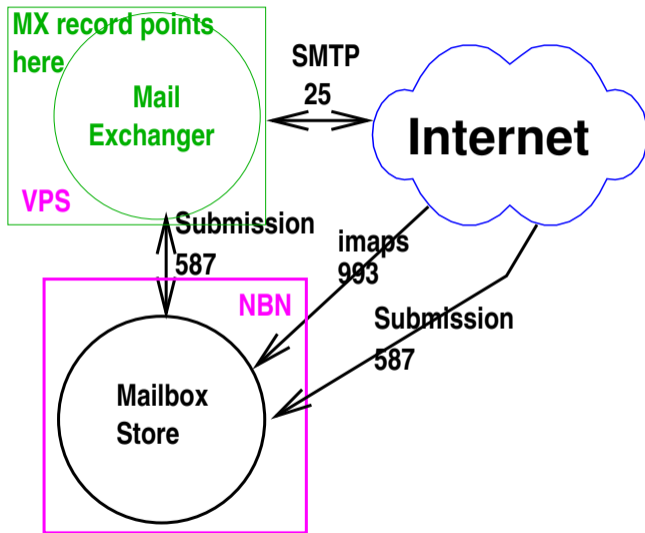
How to deliver email



To work out who to deliver general email to

1. Look for an MX record
2. if there is no MX, attempt AAAA or A
3. Attempt to connect to lowest numbered MX
4. If that fails, use next lowest if any; otherwise back c1 off and try again later.

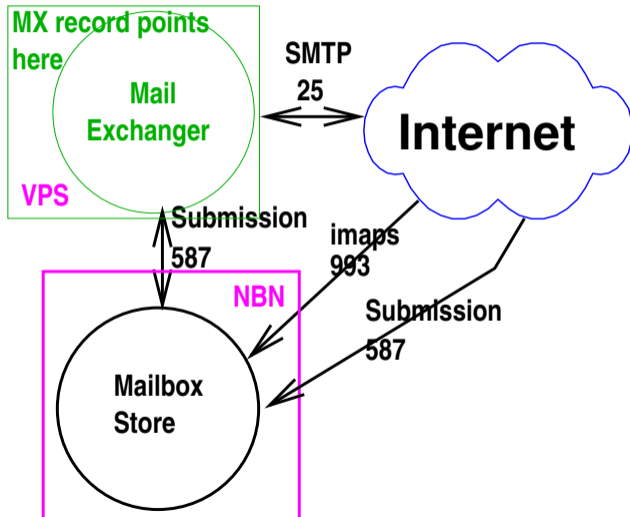
My setup



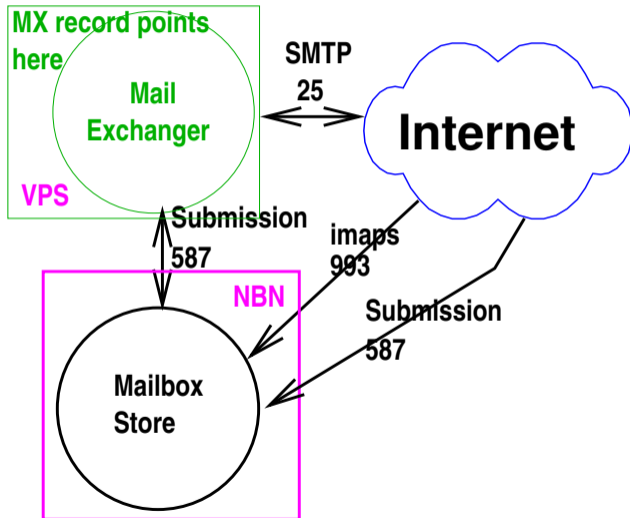
What you need



MX (Mail Exchanger)
For sending email



What you need



MX (Mail Exchanger)

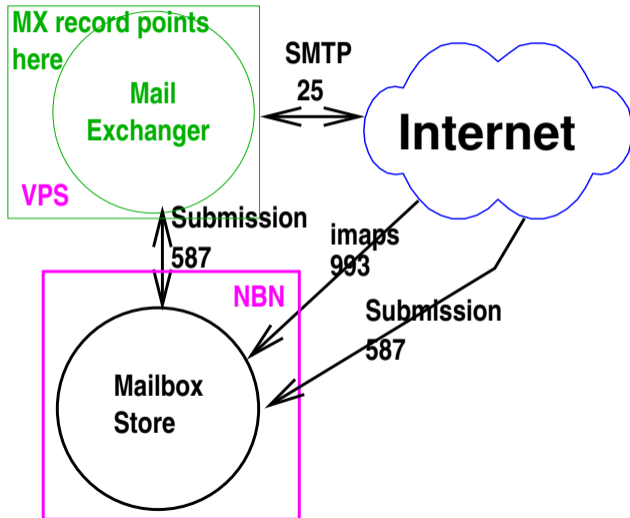
For sending email

- server or VM that's up 24/7
- with ports 587 and 25 open
- and static IPv4 and IPv6 addresses
- and a firewall you control
- \geq 2GB RAM for spamassassin

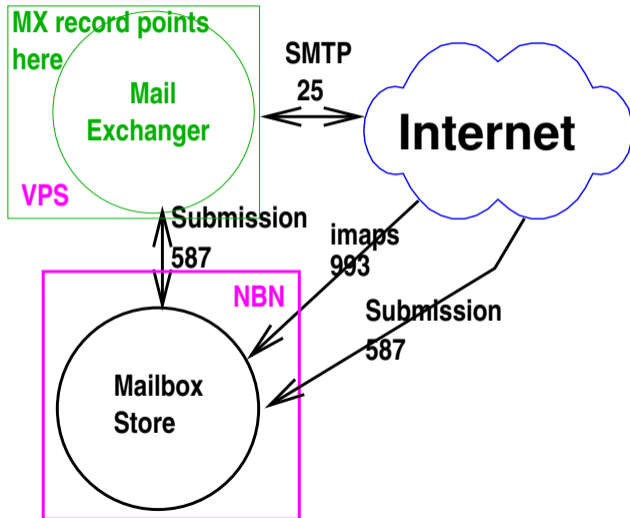
What you need



MX (Mail Exchanger)
For sending email
Around \$100 per year



What you need



Mailbox Store

For reading email

- server or VM that's up 24/7
- With plenty of disc space
- with static (or mostly static) IP address
- Open ports 587 and 993
- \geq 2Gb RAM

MX setup/hardening



- Start with distro config

MX setup/hardening



— Start with distro config — I use Debian with `exim4-daemon-heavy`

MX setup/hardening



- Start with distro config
- Install a spam scanner (e.g., `spamassassin`)

MX setup/hardening



- Start with distro config
- Install a spam scanner (e.g., `spamassassin`)
- Adjust firewall:
 1. Allow **25** — for SMTP
 2. Allow **80** — for *letsencrypt*
 3. Allow **587** — for authenticated ESMTP connections, only from internal MTA — I use IPv6 for this.

- Start with distro config
- Install a spam scanner (e.g., `spamassassin`)
- Adjust firewall:
 1. Allow **25** — for SMTP
 2. Allow **80** — for *letsencrypt*
 3. Allow **587** — for authenticated ESMTP connections, only from internal MTA — I use IPv6 for this.
- Get SSL cert from *letsencrypt*; add deployment hook to install for MTA.

MX setup/hardening



- Disallow AUTH except from port 587.

```
plain_server:  
    driver = plaintext  
...  
    server_advertise_condition = ${if  
        and{  
            {eq{587}{$received_port}}  
            {eq{$tls_cipher}{}}  
        }{}}{*}}
```

MX setup/hardening



Send email for your domains to your internal MX.

MX setup/hardening



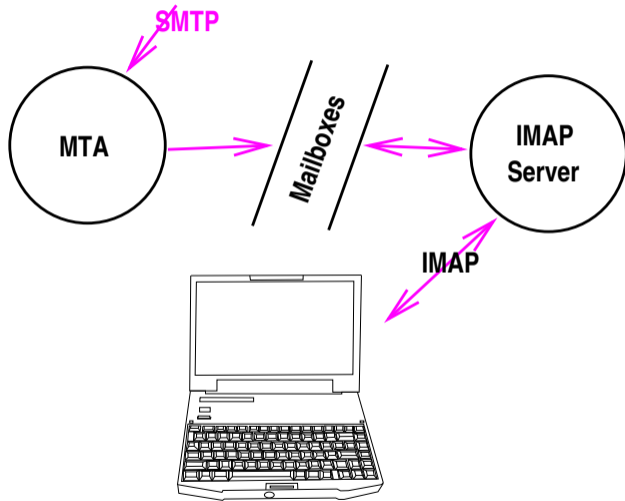
Send email for your domains to your internal MX.
Use authenticated delivery for this (on port 587).
(On exim: use the `hubbed_hosts` mechanism)

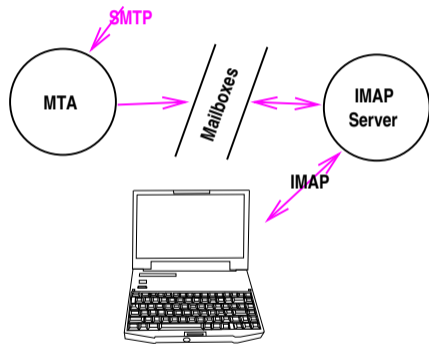
Mail storage setup/hardening



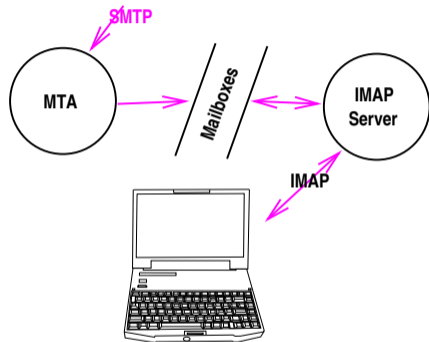
- Set up as *smarthost* system with local delivery.
- Make it relay for all your local networks (don't forget IPv6!)
- Smarthost is your external server
- Set to listen on ports 587 and 25
- Firewall allow 587 inwards and outwards.
- Use `saslauthd` to authenticate
- Use `fail2ban` to drop brute-force passwd attacks
- Run password cracker locally

User Agent





- Most MUAs talk IMAP protocol
- Need IMAP server. Most popular are:
 - dovecot — very full featured
 - Courier-imap — small footprint
 - ...heaps of others



- Coordinate mail storage between MTA and IMAP servers
- Can be:
 - Traditional Mailbox — single file
 - MailDir — Directory with files per message
 - MailDB
- Can use IMAP server as local delivery agent (LDA)

- Need good passwords

- Need good passwords — run passwd cracker regularly

- Need good passwords — run passwd cracker regularly
- Use SSL: letsencrypt is good enough
 - allow port 80 (HTTP) for ACME challenge(or run webserver on same host)
 - Add deploy hook to give certs to exim4 and dovecot

Spammers can pretend to be from your domain!

- Add SPF (Sender Policy Framework) DNS TXT record

```
"v=spf1 mx ~all"
```

- Check SPF for incoming email.

```
CHECK_RCPT_SPF=true
```

in exim4 configuration.

Spammers can pretend to be from your domain!

- Add SPF (Sender Policy Framework) DNS TXT record

```
"v=spf1 mx ~all"
```

- Check SPF for incoming email.

```
CHECK_RCPT_SPF=true
```

in exim4 configuration.

- This breaks email forwarding:

Spammers can pretend to be from your domain!

- Add SPF (Sender Policy Framework) DNS TXT record

```
"v=spf1 mx ~all"
```

- Check SPF for incoming email.

```
CHECK_RCPT_SPF=true
```

in exim4 configuration.

- This breaks email forwarding: implement Sender Rewriting Scheme (SRS) to fix
- Checks Envelope From address, not header From address

- DKIM (Domain Key Identified Mail): sign outgoing emails.
 - Body
 - Also From, To, CC, Subject
 - This checks From Headers.
 - Public key in DNS

Preventing Spoofing



- DKIM (Domain Key Identified Mail): sign outgoing emails.
 - Body
 - Also From, To, CC, Subject
 - This checks From Headers.
 - Public key in DNS
- Allows recipients to check email integrity.
- This can break mailing lists

- DKIM (Domain Key Identified Mail): sign outgoing emails.
 - Body
 - Also From, To, CC, Subject
 - This checks From Headers.
 - Public key in DNS
- Allows recipients to check email integrity.
- This can break mailing lists
- Unsigned emails can still be spoofed.

Tell recipients what to do if SPF or DKIM fail

```
_dmarc.example.com "v=DMARC1; p=drop"
```

- If SPF fails or DKIM fails, drop message.
- If message not DKIM signed, drop the message
- if Envelope From doesn't match From address, mark as spam.

Tell recipients what to do if SPF or DKIM fail

```
_dmarc.example.com "v=DMARC1; p=drop"
```

- If SPF fails or DKIM fails, drop message.
- If message not DKIM signed, drop the message
- if Envelope From doesn't match From address, mark as spam.

Can break mailing lists and email forwarders

Tell recipients what to do if SPF or DKIM fail

```
_dmarc.example.com "v=DMARC1; p=drop"
```

- If SPF fails or DKIM fails, drop message.
- If message not DKIM signed, drop the message
- if Envelope From doesn't match From address, mark as spam.

Can break mailing lists and email forwarders

Can ask for failure reports using `rua=` and `ruf=`.

Other policies (`none`, `quarantine`) also possible.

(See <https://dmarc.org>)

Broken implementations

Broken implementations

```
$ host -t txt _dmarc.gmail.com
_dmarc.gmail.com descriptive text "v=DMARC1; p=none;
    sp=quarantine; rua=mailto:mailauth-reports@google.com"
```

Even Google doesn't apply DMARC.

Broken implementations

```
$ host -t txt _dmarc.gmail.com
_dmarc.gmail.com descriptive text "v=DMARC1; p=none;
    sp=quarantine; rua=mailto:mailauth-reports@google.com"
```

Even Google doesn't apply DMARC.

Things to do with your Mail Server



- Throw away addresses

Things to do with your Mail Server



- Throw away addresses— delete when abused

Things to do with your Mail Server



- Throw away addresses— delete when abused
- Provide hostmaster/webmaster/abuse addresses for your domains

Things to do with your Mail Server



- Throw away addresses— delete when abused
- Provide hostmaster/webmaster/abuse addresses for your domains
- Share with family and friends

Things to do with your Mail Server



- Throw away addresses— delete when abused
- Provide hostmaster/webmaster/abuse addresses for your domains
- Share with family and friends — Family interest email lists

Things to do with your Mail Server



- Throw away addresses— delete when abused
- Provide hostmaster/webmaster/abuse addresses for your domains
- Share with family and friends — Family interest email lists
- **Enjoy the freedom**

Summary



- Spammers make our life harder
- It's still not that hard to run a mail server

- Spammers make our life harder
- It's still not that hard to run a mail server

Take Control
Give it a go.

Resources



<https://dmarc.org> — DMARC explanation

<https://www.dmarcly.com/blog/>

[how-to-set-up-sender-policy-framework-spf-the-complete-guide](#)
– Guide to SPF

<https://mikepultz.com/2010/02/using-dkim-in-exim/> DKIM
in Exim

<https://easydmarc.com/blog/>

[how-to-configure-dkim-opendkim-with-postfix/](#) DKIM in
Postfix

https://www.andrewferrier.com/my-work/spamassassin_tips/

Tips
for Spamassassin setup

<https://dmarcly.com/tools/> Tools for generating _dmarc and SPF
TXT records and for checking yours.

<https://mxtoolbox.com/SuperTool.aspx> Tools for solving Email issues

https://exim.org/exim-html-current/doc/html/spec_html/ch-dkim_spf_srs_and_dmarc.html Exim4 official docs

<https://linux.goeszen.com/>

[configuring-exim4-with-spamassassin-and-sa-exim-on-debian-a.html](#) Integrating Spamassassin into Debian Exim