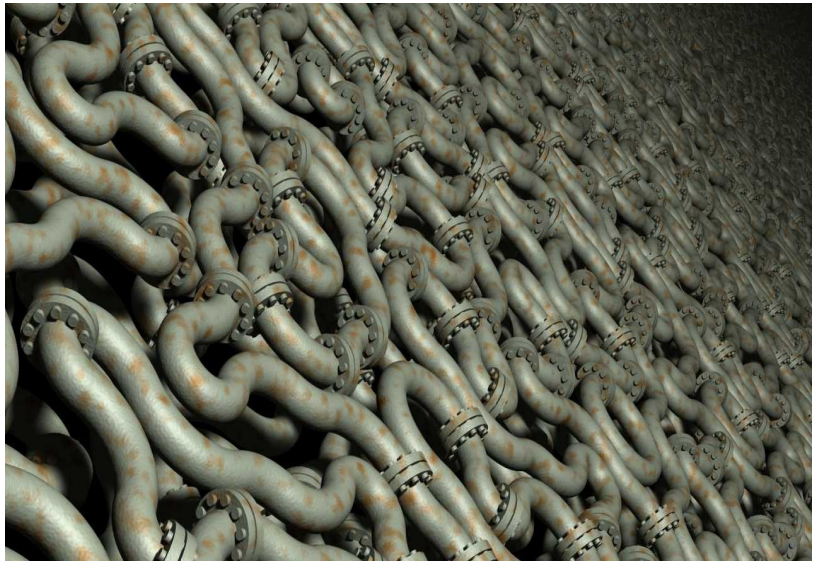

DIY eMail@Home$ tail -f /var/log/mail.log
Feb 3 09:09:29 samchiel postfix/lmtp[26602]: C57A917C0070:
to=<julien@linuxwall.info>, relay=127.0.0.1[127.0.0.1]:5002,
delay=2.6, delays=1.5/0.01/0.04/1.1, dsn=2.6.0, status=sent
(250 2.6.0 <julien@linuxwall.info> Message accepted for delivery)
(N 3 C T 0)
samchiel.linuxwall.i
BELL
IRC: J-V-E
JULIEN
VEHENT
AWEBER
RECOVERY
DISK
4.7GB
120mm

But... I like gmail....

- Privacy concerns...yadda yadda yadda
- 30 years from now, you will want to reread those old emails. Will gmail still exist ?
- This is about Knowledge



← how most people see the Internet

How you do →

Can you host your emails at home ?

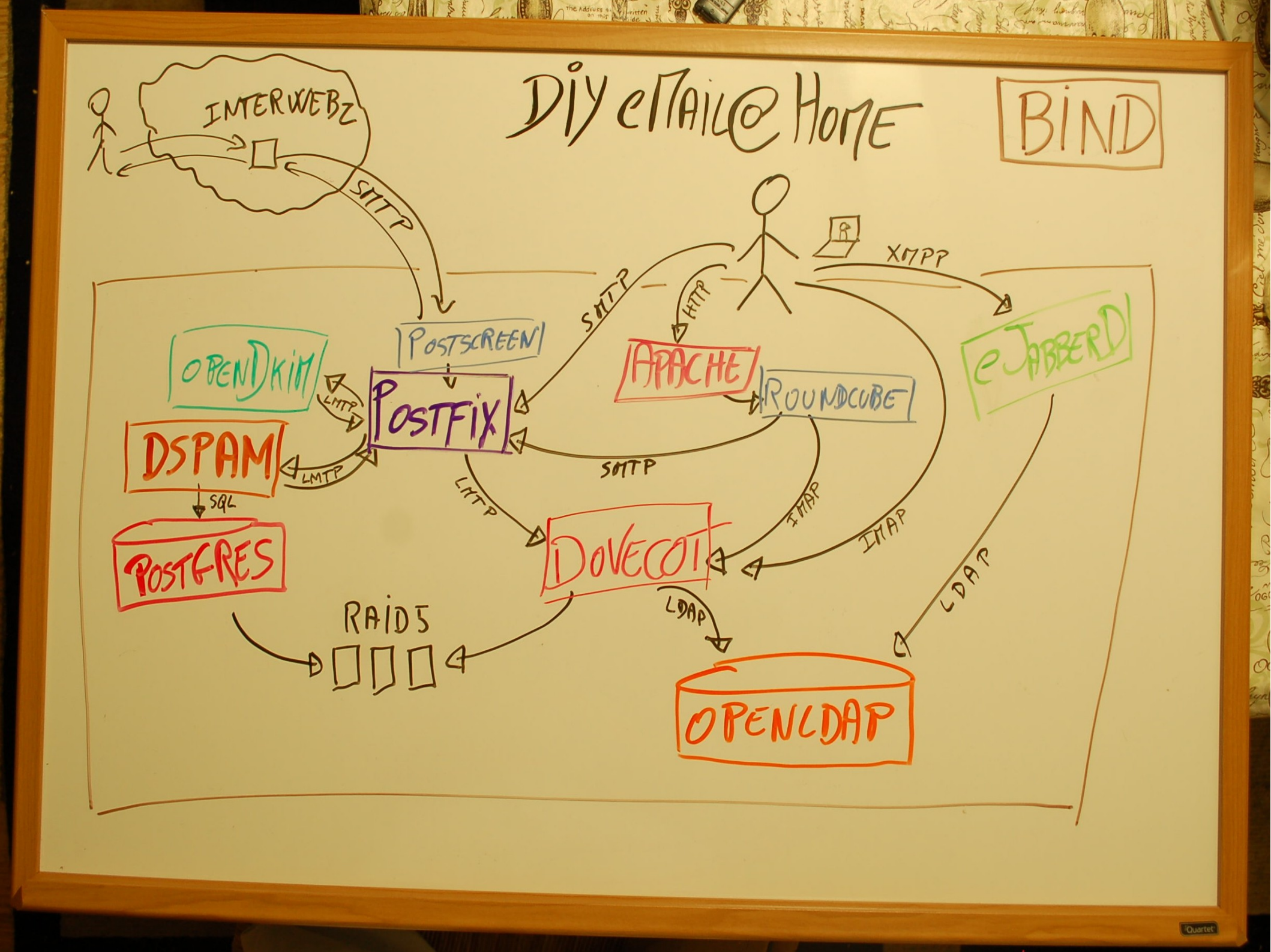
- No.
- At least, not all of it.
- You need backup SMTP & DNS, SMTP relay on a static IP, and a domain name.

- Cost:

  SMTP relay: ~$20/year (dyn.com)

  Domain: ~$15/year (gandi.net)

  Small (atom) server with 2*2.5” drives: ~$250


DIY eMAIL@HOME
BIND
INTERWEBZ
SMTP
POSTSCREEN
OPENDKIM
LMTP
POSTFIX
DSPAM
LMTP
SQL
POSTGRES
RAID5
SMTP
HTTP
APACHE
ROUNDCUBE
SMTP
XMPP
EJABBERD
LMTP
DOVECOT
IMAP
IMAP
LDAP
LDAP
OPENLDAP

Step 1: Sending

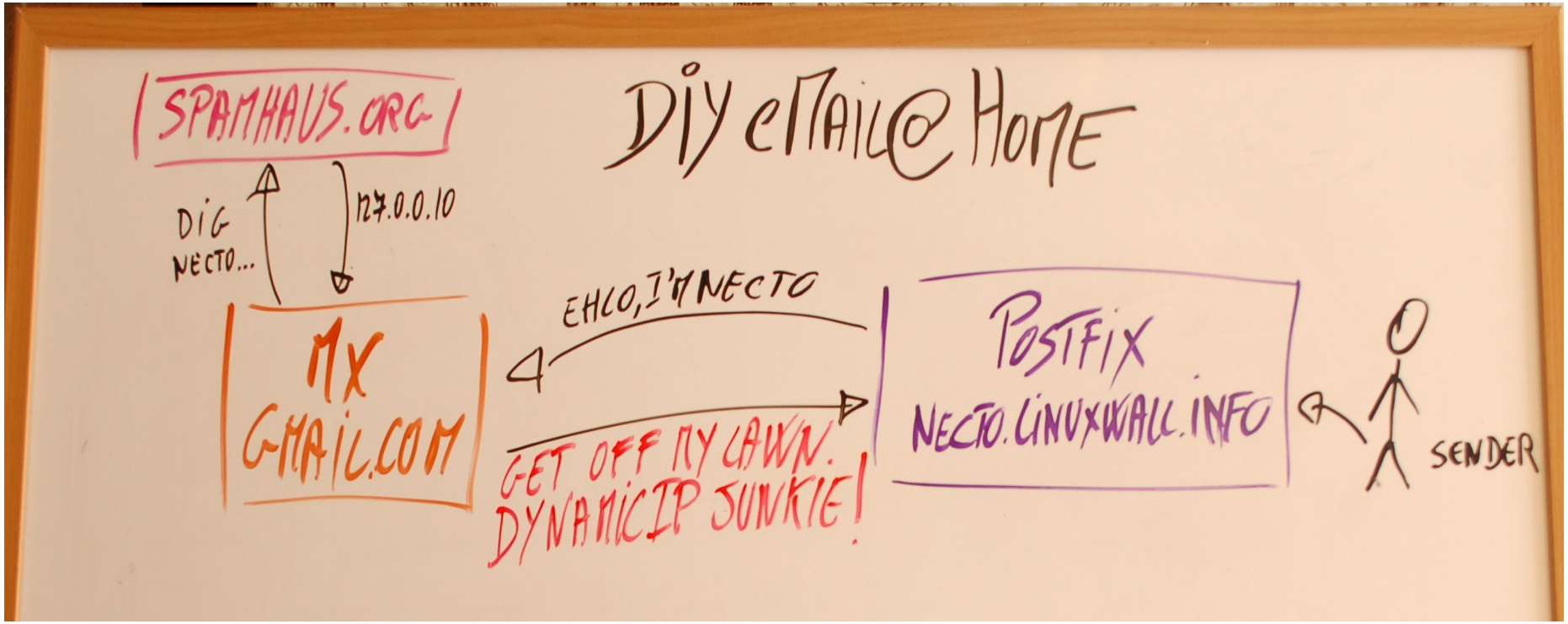
1. apt-get install postfix
2. echo “yiipyy” | mail -s “I can Haz Mail” julien@linuxwall.info
3. Have a beer.

- Sending mail is easy, because postfix handles the DNS resolutions, queuing and sending.
- But most recipients will reject your mail because of your IP reputation.

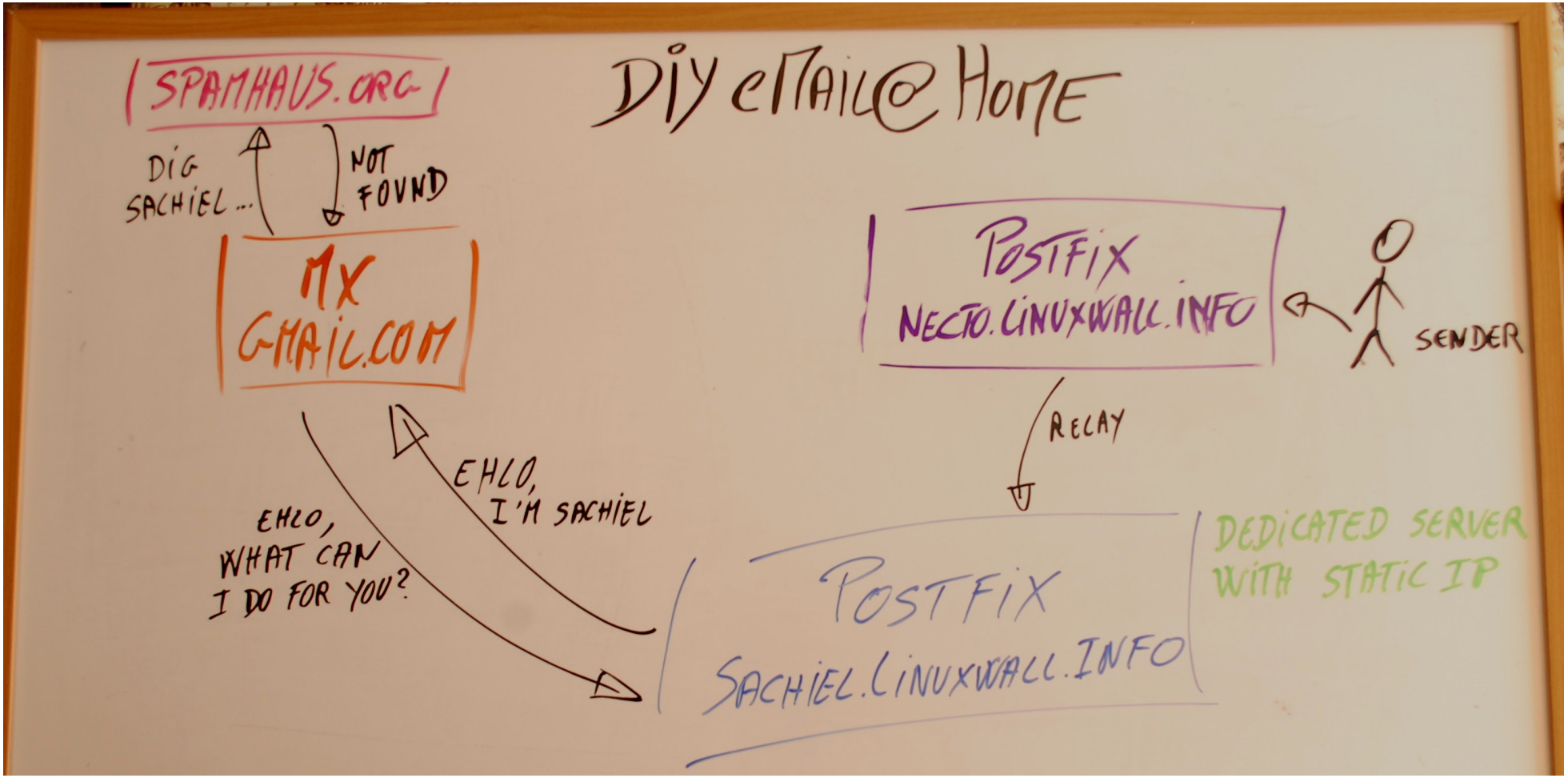
Feb 9 16:55:01 necto postfix/smtp[2538]: 5174341E26: to=<julienv@aweber.com>, relay=mail1.aweber.com[207.106.200.39]:25, delay=0.93, delays=0.09/0/0.68/0.16, dsn=5.0.0, **status=bounced (host mail1.aweber.com[207.106.200.39] said: 550 c-68-80-50-225.hsd1.pa.comcast.net is either part of a dynamic IP range or we have received spam from this domain.** Please see http://www.aweber.com/email-blocked.htm?reason=rdns_id-1002&ip=68.80.50.225 (in reply to RCPT TO command))

How IP Reputation works

- Real-time Blackhole List (RBLs) flag dynamic IPs from residential ISPs
  - $ dig +short 225.50.80.68.zen.spamhaus.org
    - 127.0.0.10
- See http://www.spamhaus.org/faq/section/DNSBL%20Usage#200



Step 1.1 : Sending through a relay

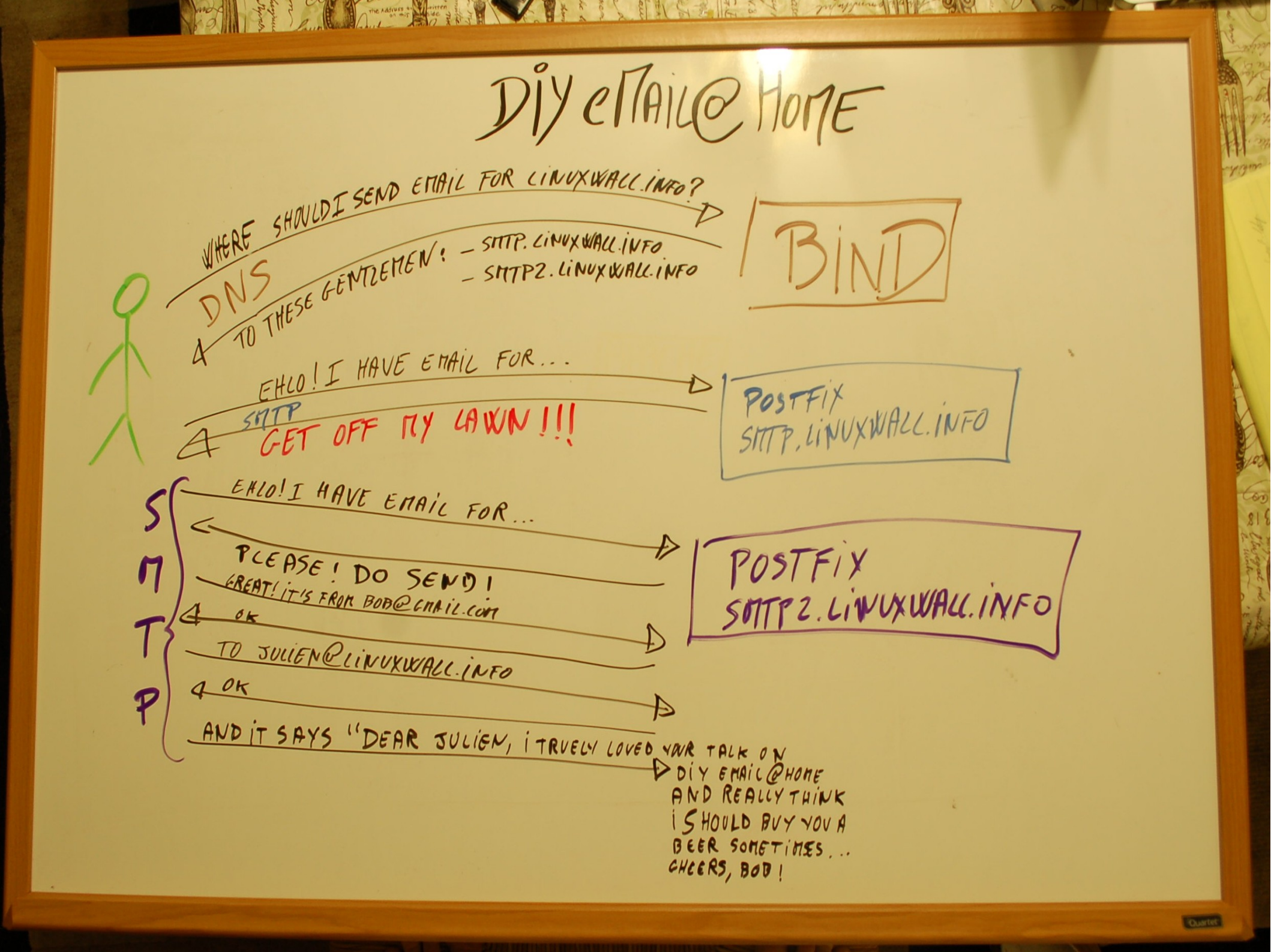


- In `/etc/postfix/main.cf`
  - relayhost = sachiel.linuxwall.info

- Reverse DNS matters:
  - $ dig +short sachiel.linuxwall.info
    - 88.191.125.180
  - $ dig +short -x 88.191.125.180
    - sachiel.linuxwall.info.

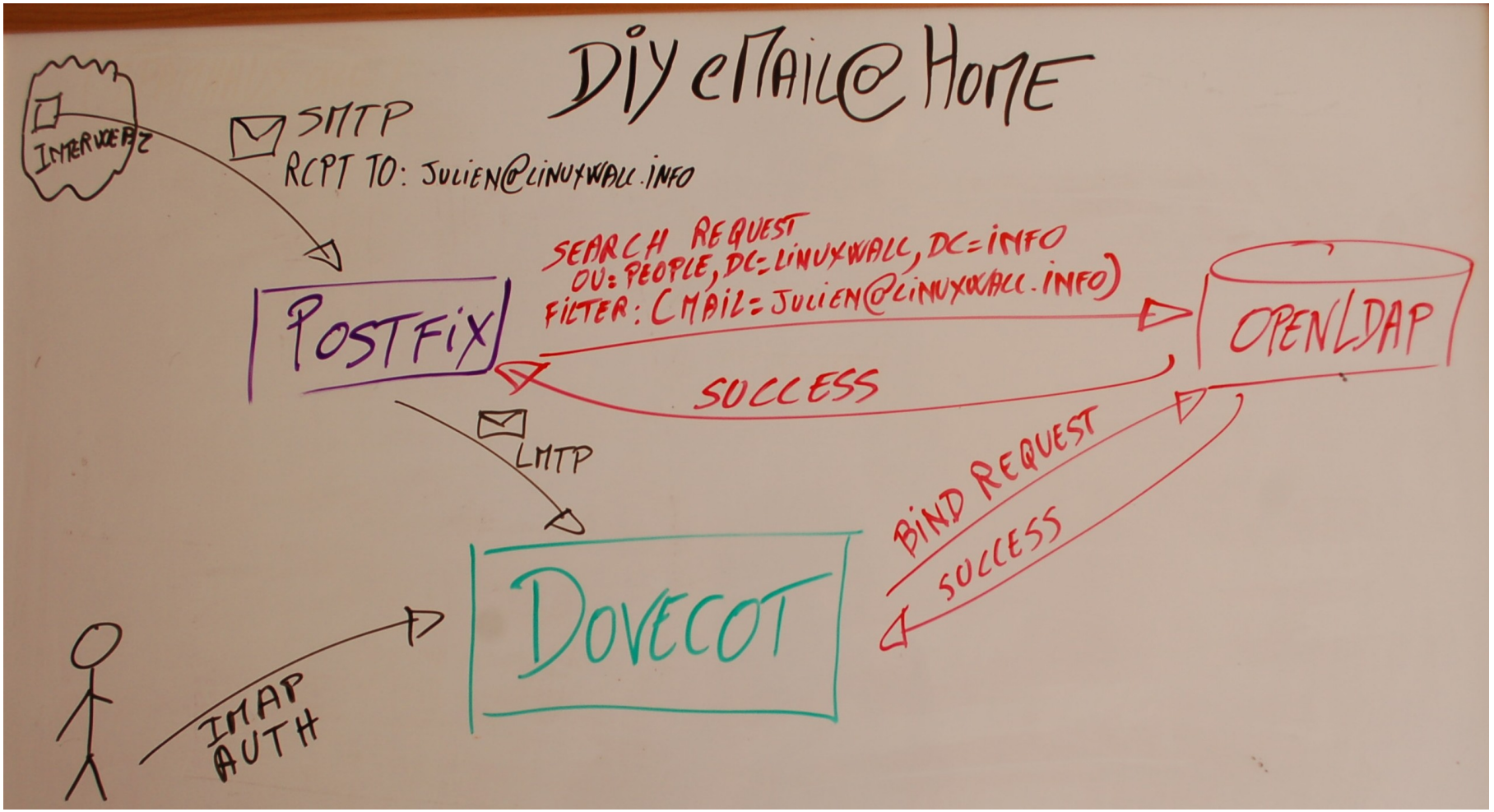
Step 2: Receiving

- Buy a domain
- Declare MX records to point to the public IP(s) of the mail server(s)
- When receiving emails:
  - You don't have to worry about the IP reputation (DNSBL, static vs dynamic IP)
  - You can change the DNS records as you please (just be careful with the TTLs)
  - You may, or may not, receive a lot of spam/bot traffic
  - If your MX is configured as an open relay, you're toast


DIY eMAIL@HOME
WHERE SHOULD I SEND EMAIL FOR LINUXWALL.INFO?
DNS
TO THESE GENTLEMEN: - SMTP.LINUXWALL.INFO
- SMTP2.LINUXWALL.INFO
BIND
EHLO! I HAVE EMAIL FOR...
SMTP
GET OFF MY LAWN!!!
POSTFIX
SMTP.LINUXWALL.INFO
SMTP
EHLO! I HAVE EMAIL FOR...
PLEASE! DO SEND!
GREAT! IT'S FROM BOB@EMAIL.COM
OK
TO JULIEN@LINUXWALL.INFO
OK
AND IT SAYS "DEAR JULIEN, I TRUELY LOVED YOUR TALK ON DIY EMAIL@HOME AND REALLY THINK I SHOULD BUY YOU A BEER SOMETIMES... CHEERS, BOB!
POSTFIX
SMTP2.LINUXWALL.INFO

Step 3: Users mailboxes

- Users are stored in LDAP. Postfix & Dovecot query LDAP for each access.



LDIF user definition

```
dn: cn=Bob Kelso,ou=people,dc=linuxwall,dc=info
uid: bob
uidNumber: 10002
gidNumber: 998
sn: Kelso
cn: Bob Kelso
homeDirectory: /dev/null
objectClass: posixAccount
objectClass: top
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
mail: bob@linuxwall.info
userPassword: {SSHA}MJ.....RR74
```

```
# ldapadd -h 127.0.0.1 -p 389
-D "cn=admin,dc=linuxwall,dc=info"
-W -f /root/bob.ldif
Enter LDAP Password:
adding new entry "cn=Bob
Kelso,ou=people,dc=linuxwall,dc=info"
```

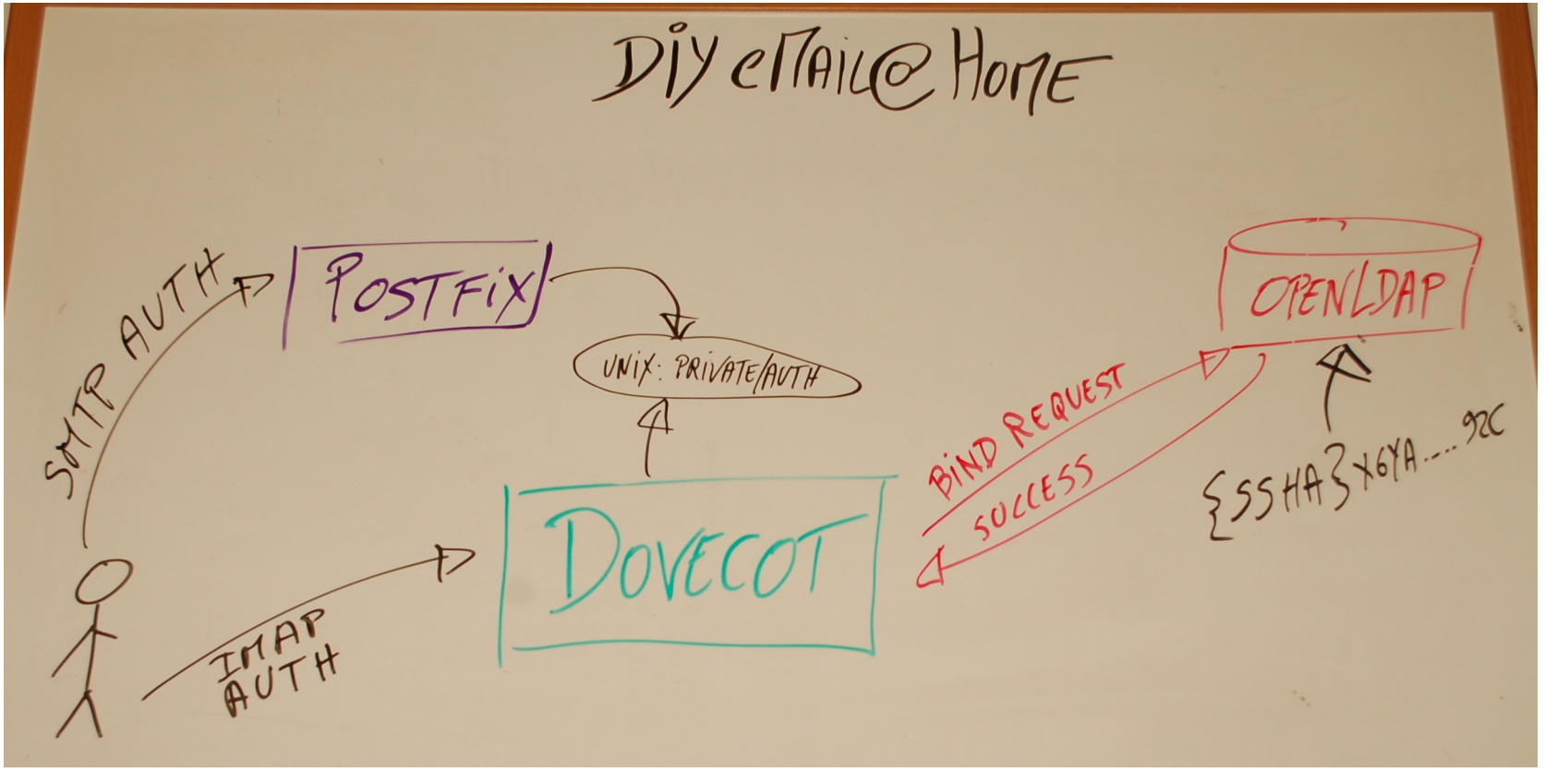
Postfix LDAP lookups

- **For Incoming email only (not local user auth)**

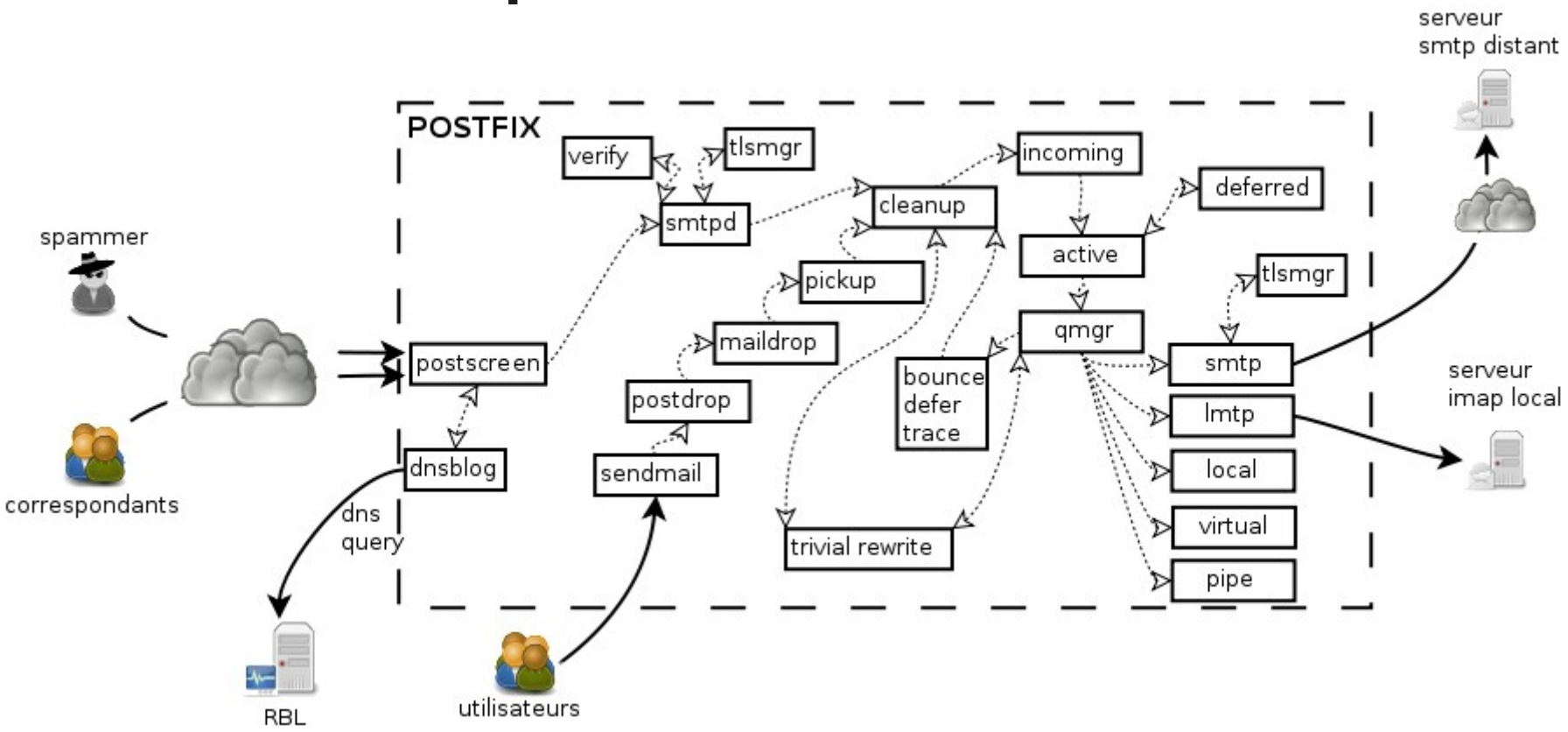
```
# grep ldap /etc/postfix/main.cf
local_recipient_maps = ldap:/etc/postfix/ldap_recipient_map.cf, $alias_maps

# cat /etc/postfix/ldap_recipient_map.cf
server_host = localhost
server_port = 389
search_base = ou=people,dc=linuxwall,dc=info
query_filter = (mail=%s)
result_attribute = mail
```

User Authentication (Postfix & Dovecot)

- LDAP stores hashed passwords (SSHA)
- Dovecot connects to LDAP
- Postfix connects to Dovecot



SPAM !
Step 1: Postscreen



- $ nc 192.168.1.249 25

  220-Welcome. Please wait to be seated

  220 necto.localdomain ESMTP Postfix (Debian/GNU)

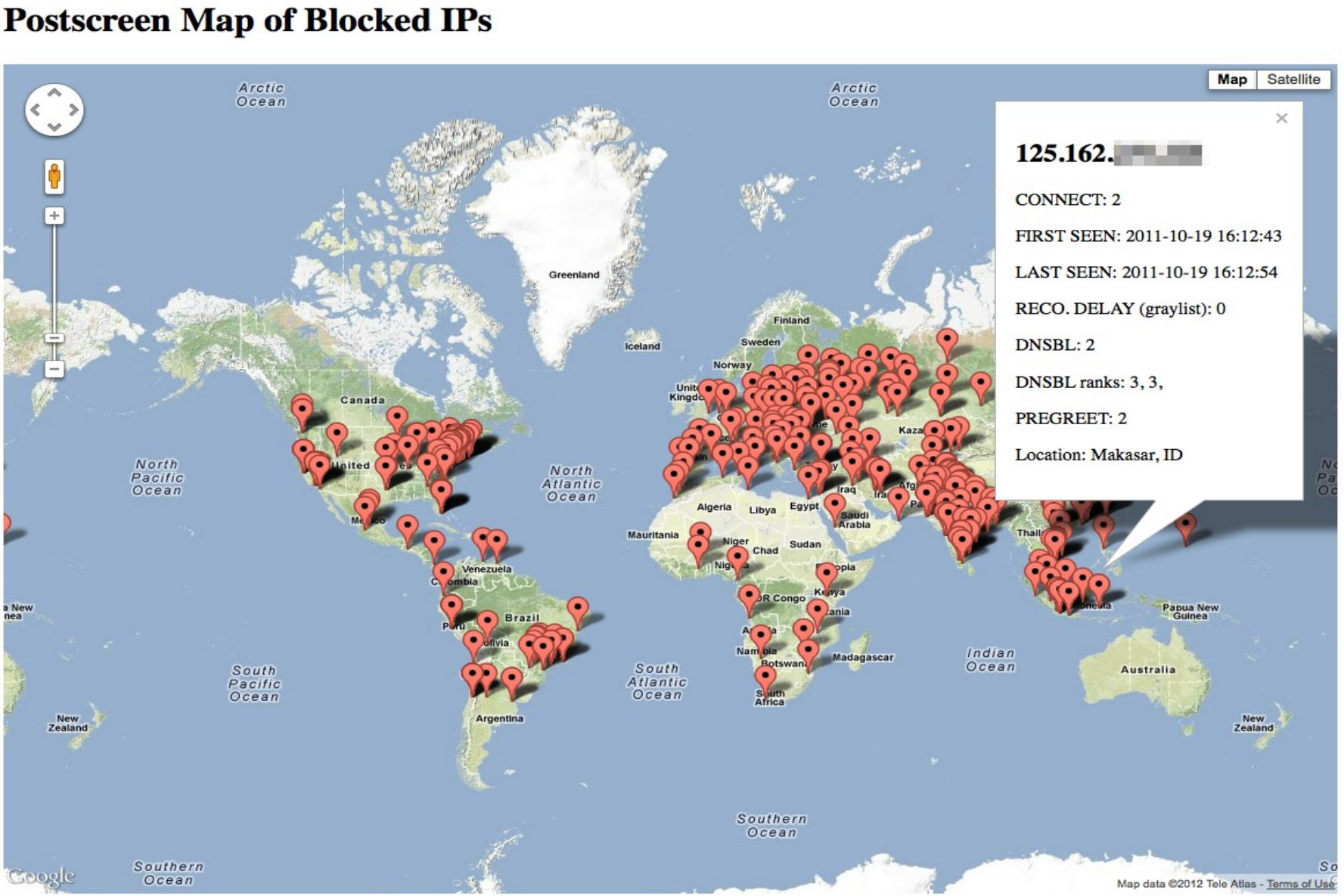
Postscreen enforces clean SMTP

and blocks everything else, such as bots

```
# Postcreen configuration
postscreen_access_list = cidr:/etc/postfix/postscreen_access.cidr
postscreen_blacklist_action = enforce

postscreen_dnsbl_sites =
    zen.spamhaus.org*3
    dnsbl.njabl.org*2
    bl.spameatingmonkey.net*2
    dnsbl.ahbl.org
    bl.spamcop.net
    dnsbl.sorbs.net
postscreen_dnsbl_threshold = 3
postscreen_dnsbl_action = enforce

postscreen_greet_banner = Bienvenue et merci
d'attendre qu'on vous assigne une place
postscreen_greet_action = enforce
postscreen_pipelining_enable = yes
postscreen_pipelining_action = enforce
postscreen_non_smtp_command_enable = yes
postscreen_non_smtp_command_action = enforce
postscreen_bare_newline_enable = yes
postscreen_bare_newline_action = enforce
```

Plenty of logs, to generate maps from

https://github.com/jvehent/Postscreen-Stats



generated using Postscreen-Stats by Julien Vehent

SPAM !
Step 2: DSPAM

http://wiki.linuxwall.info/doku.php/en:ressources:dossiers:dspam

- Breaks down emails into tokens, and assigns a spam probability to each token

  “Heute Abend war ich mit meiner Freundin im Kino und habe viel gelacht”

TOKEN: ‘mit’ CRC: 5158417007107899392

TOKEN: ‘ich+mit’ CRC: 5158416839735805488

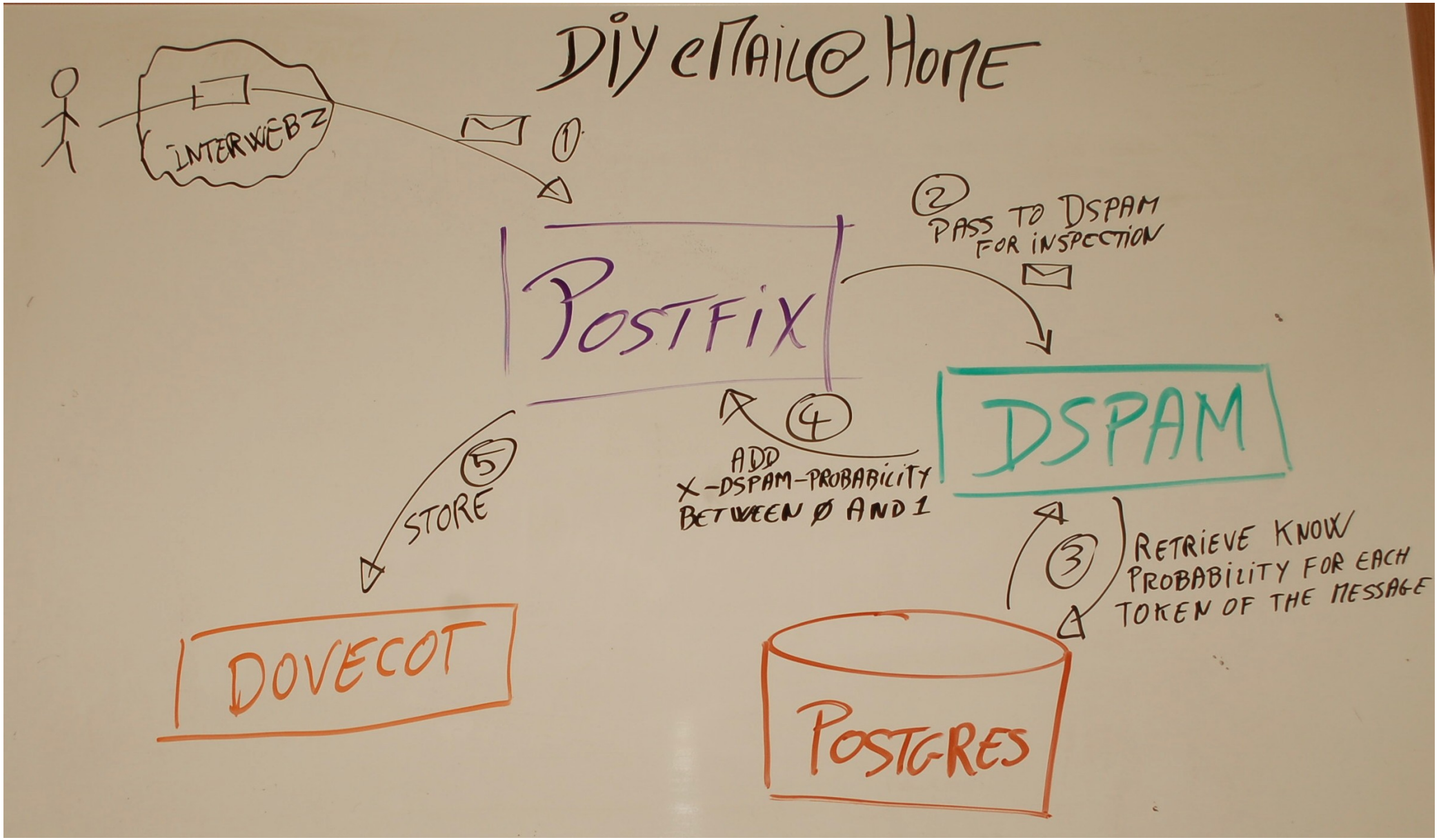
TOKEN: ‘war+#+mit’ CRC: 157078174934358472 27

TOKEN: ‘war+ich+mit’ CRC: 690533613960537 8569

TOKEN: ‘Abend+#+#+mit’ CRC: 548265207421969 3289

TOKEN: ‘Abend+#+ich+mit’ CRC: 200645400382372 1484

DSPAM doesn't accept or drop it simply calculates a probability



DSPAM doesn't accept or drop it simply calculates a probability

X-DSPAM-Result: Spam

X-DSPAM-Processed: Fri Feb 8 15:08:25 2013

X-DSPAM-Confidence: 0.9984

X-DSPAM-Improbability: 1 in 64201 chance of being ham

X-DSPAM-Probability: 1.0000

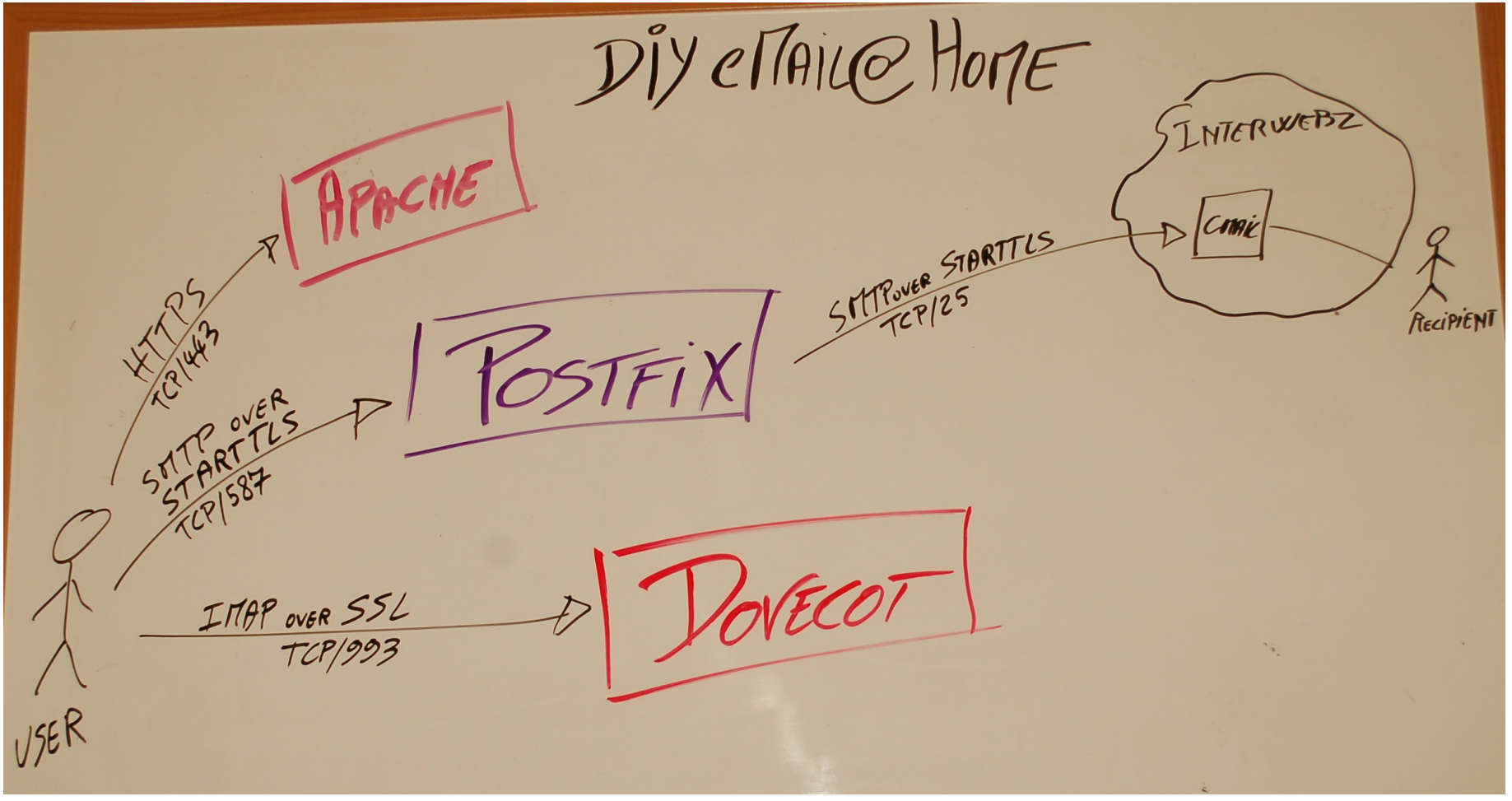
X-DSPAM-Signature: 51155b39130198027420682

X-DSPAM-Factors: 15,

com+ATTENDEE, 0.99872, SEQUENCE+0, 0.99872, RSVP+TRUE, 0.99872, BEGIN+#+DTSTART, 0.99867, VCALENDAR+PRODID, 0.99867, BEGIN+#+PRODID, 0.99867, TRUE+mailto, 0.99862, X+#+CDO, 0.99862, X+#+#+INTENDEDSTATUS, 0.99862, mailto+#+#+#+ATTENDEE, 0.99862, RSVP+#+mailto, 0.99862, MICROSOFT+#+INTENDEDSTATUS, 0.99862, X+MICROSOFT, 0.99862, CDO+INTENDEDSTATUS, 0.99862,**TRUE+#+#+#+com, 0.99862**

Security: SSL/TLS everywhere

- STARTTLS upgrades an existing TCP connections to SSL
- Most MX support it, inbound and outbound



Security: SSL/TLS everywhere

```
# STARTTLS client options
smtp_use_tls = yes
smtp_tls_note_starttls_offer = yes
smtp_tls_loglevel = 1

# TLS server options
smtpd_tls_security_level = may
smtpd_tls_auth_only = yes
smtpd_tls_key_file = /etc/postfix/certs/smtp.key
smtpd_tls_cert_file = /etc/postfix/certs/smtp.pem
smtpd_tls_CAfile = /etc/postfix/certs/ca.crt
smtpd_tls_mandatory_protocols = !SSLv2
smtpd_tls_mandatory_ciphers = high
smtpd_tls_mandatory_exclude_ciphers = aNULL, MD5
```

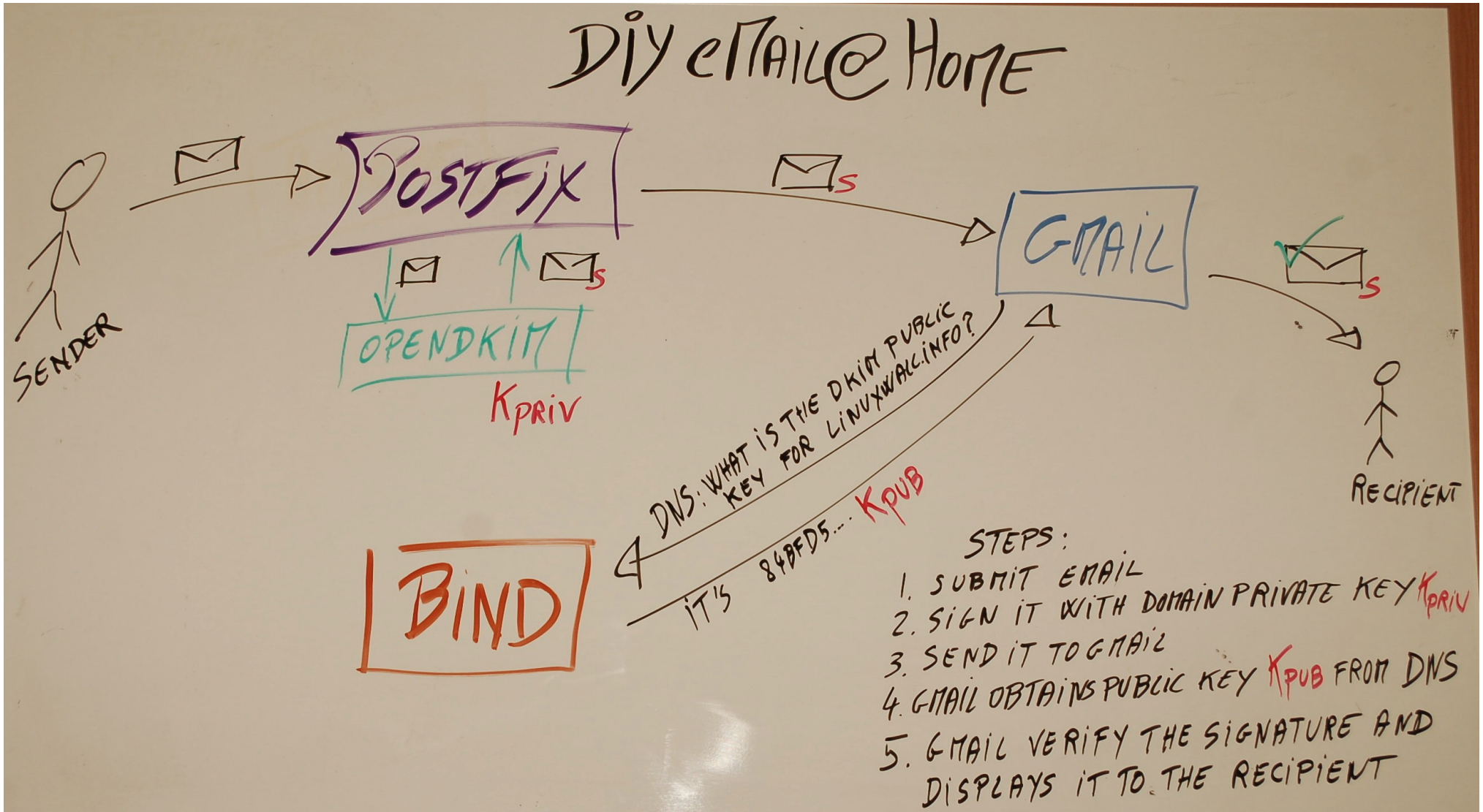
Security: DKIM

http://wiki.linuxwall.info/doku.php/en:ressources:dossiers:postfix:dkimproxy

DKIM-Signature: v=1; a=rsa-sha256;c=relaxed/relaxed;d=gmail.com;s=gamma;

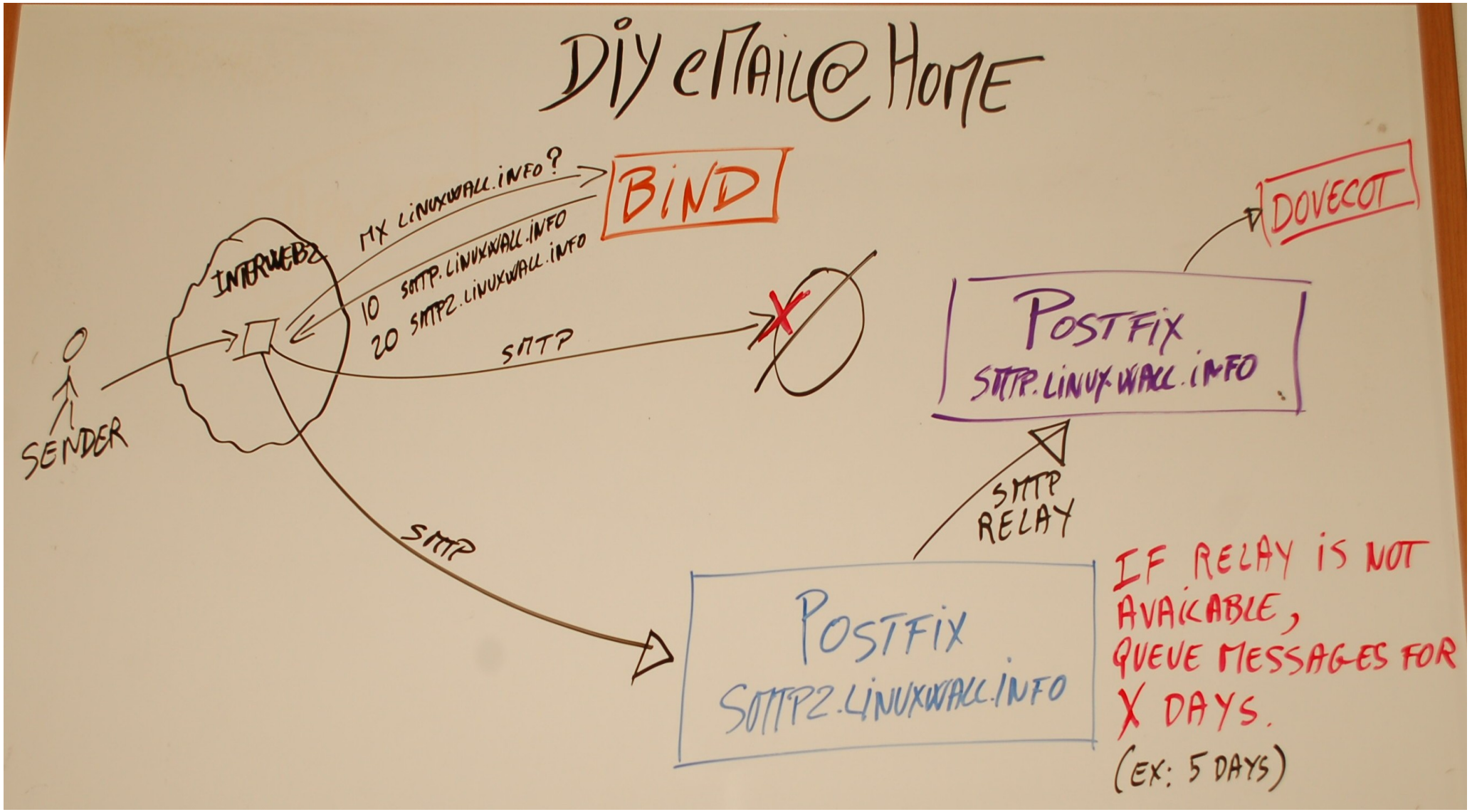
h=domainkey-signature:mime-version:received:date:message-id:subject:from:to:

content-type;bh=+h+GzK7.....=



Surviving outages with a backup MX

```
# postconf -v maximal_queue_lifetime
maximal_queue_lifetime = 5d
```



Configuration is documented at

http://wiki.linuxwall.info/doku.php/en:ressources:dossiers:nectux