Spam fighting with Postfix

*Using technology to fight a social problem*

Devdas Bhagat
Introduction

Postfix in the anti spam war

"If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology"

– Bruce Schneier
What Postfix can do

- Client IP address or reverse DNS checks.
- Client NS/MX checks.
- HELO/EHLO checks.
- Sender domain checks.
- Sender address checks.
- Recipient checks.
- Simple regular expression checks.
With Additional tools

- Complex multiline checks.
- Customized per recipient policies.
- Antivirus checks.
- SpamAssassin hooks.
What Postfix cannot do

- Bypass the simple regexp checks for specific cases.
- Do complex checks without using external filters.
- Limit the simultaneous number of connections from a single host.
- Stop spam completely.
Postfix configuration variables

- check_client_access
- check_helo_access
- check_sender_access
- check_recipient_access
- header_checks
- mime_header_checks
- body_checks
- content_filter
More configuration variables

- smtpd_helo_required
- strict_rfc821_envelopes
- smtpd_sender_login_maps
- relay_domains
- permit_mx_backup
- permit_mx_backup_networks
- smtpd_delayReject
- reject_non_fqdn_recipient
More configuration variables

- local_recipient_maps
- check_sender_mx_access
- check_sender_ns_access
- reject_unknown_recipient_domain
- reject_unverified_recipient
- reject_unverified_sender
- smtpd_proxy_filter
- check_policy_service
Implementing UBE checks

- **KISS**
- `smtpd_delay_reject = yes` is default
- Put all restrictions in `smtpd_recipient_restrictions` for simplicity
- Order is important. First match wins.
Starting off

- Set mynetworks correctly.
  - mynetworks = 127.0.0.0/8, 192.168.1.0/24

- Set myhostname to a FQDN.
  - myhostname = foo.example.com

- Require a proper SMTP transaction beginning.
  - smtpd_helo_required = yes

- Disable user verification.
  - disable_vrfy_command = yes
Actual restrictions

We start by allowing mail from trusted systems. This is hosts in mynetworks and authenticated users.

```plaintext
smtpd_recipient_restrictions =
  permit_mynetworks
  permit_sasl_authenticated
  reject_unauth_destination
```
Simple tests with data format validation

smtpd_recipient_restrictions =
  reject_invalid_hostname
  reject_non_fqdn_hostname
  reject_non_fqdn_sender
  reject_non_fqdn_recipient
  reject_unknown_sender_domain
  reject_unknown_recipient_domain
  reject_unauth_pipelining
  permit_mynetworks
  permit_sasl_authenticated
  reject_unauth_destination
```plaintext
smtpd_recipient_restrictions =
   reject_invalid_hostname
   reject_unauth_pipelining
   permit_mynetworks
   permit_sasl_authenticated
   reject_unauth_destination
   reject_rbl_client xbl.spamhaus.org
   reject_rhsbl_sender rhsbl.sorbs.net
```
Local access maps

smtpd_recipient_restrictions =
  reject_invalid_hostname : reject_unauth_destination
check_recipient_access hash:/etc/postfix/role-accounts
check_client_access hash:/etc/postfix/allowed-clients
check_client_access hash:/etc/postfix/banned-clients
check_sender_access hash:/etc/postfix/allowed-senders
check_sender_access hash:/etc/postfix/banned-senders
reject_rbl_client xbl.spamhaus.org
$cat /etc/postfix/role-accounts
abuse@ OK
$cat /etc/postfix/banned-clients
comcast.net 554 Too much spam
12 554 Compromised machines.
$cat /etc/postfix/allowed-clients
12.10.54.20 OK
$cat /etc/postfix/allowed-senders
@securityfocus.com OK
$cat /etc/postfix/banned-senders
@indiatimes.com REJECT
Content Filtering

- header_checks = regexp:/etc/postfix/header-regexp
- mime_header_checks = regexp:/etc/postfix/mime-regexp
- body_checks = pcre:/etc/postfix/body-pcre
- content_filter = smtp-amavis:[127.0.0.1]:10024
Simple content filtering

- Header checks check the message headers. Catch fake headers or spam software signatures with this.

- MIME header checks check for attachment and content-type and other MIME headers. These are useful for filtering out on attachments like file.jpg.vbs

- Body checks check the body of the message: Filter for lines with CAN SPAM or US.1618 or "remove me" links.
Complex content filters

Body and header checks have one significant limitation:

These checks are global and cannot be bypassed

- The content_filter is an external program.
- It receives mail on standard input and sends it back to Postfix via standard output.
- Take care to avoid looping.
- Can be very flexible.
- Runs after accepting the mail.
Useful links

- http://www.postfix.org/
- http://www.securitysage.com/
- http://www.ijs.si/software/amavisd/
- http://www.spamassassin.org/
- http://clamav.elektrapro.com/