Exim & Spam

Alex Villegas

Quality Assurance Representative

Introduction

This presentation will focus on the following subjects:

- **Exim in a Nutshell**
- **Alternatives to Fight SPAM**

As usual, we will take in consideration the **CLI** and **GUI** approaches.

We will touch on a few non supported apps such as ASSP.

What is Exim?

It's acronym was derived from “**Experimental Internet Mailer**” since the outcome of the project was unknown.

Exim is a message transfer agent (**MTA**) developed at the University of Cambridge for use on Unix systems connected to the Internet.

It is freely available under the terms of the
GNU General Public License.

Exim configuration out of the box

- Runs on port 25 (Can be adjusted in WHM)

- Main >> Service Configuration >> Exim Configuration Editor
  - Exim Configuration Editor
  - Exim Advanced Editor

- `/etc/init.d/exim`

  ```
        /scripts/restartsrv_exim
  ```

Where is Exim located?

BINARIES

- /usr/sbin/exim

- /usr/sbin/sendmail* is a wrapper for /usr/sbin/exim

* Note: Must be a setgid wrapper, or will cause messages to be delivered by noon-root users to fail. For example, when a PHP script sends mail while mailtrap is enabled.

Configuration Files

Main configuration file:

- **/etc/exim.conf**

Links to passwd files for virtual mail users:

- **/etc/vmail**

- **/etc/exim.pl**

Querying specific settings from the configuration:

exim -bP variable_name

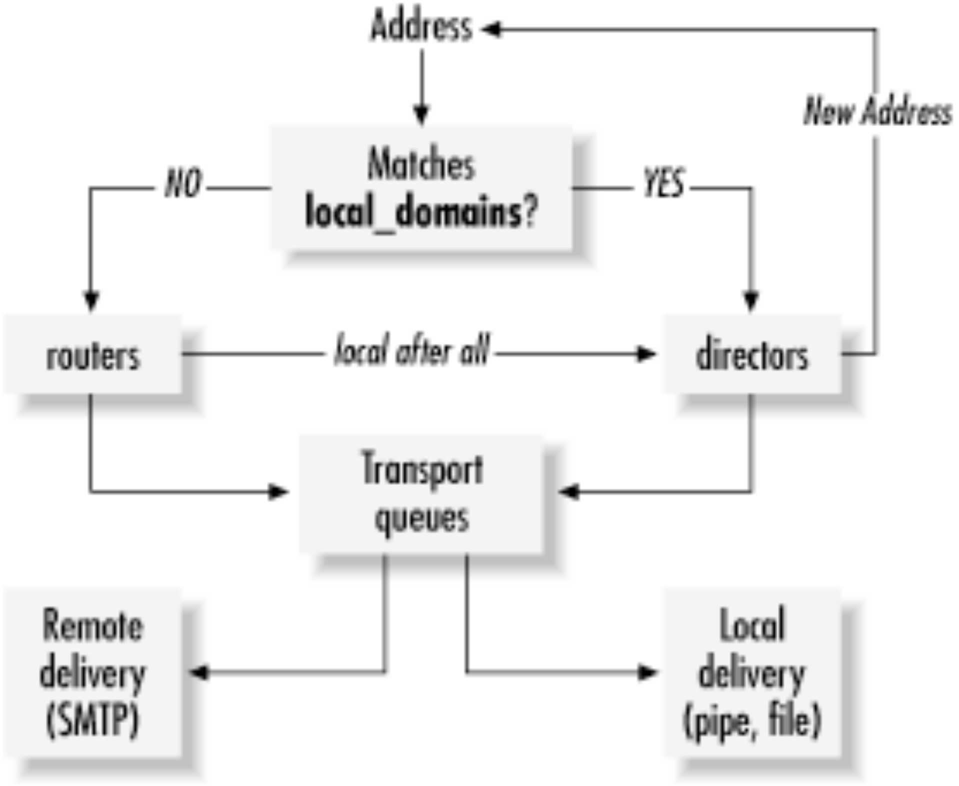
Example: **exim -bP deliver_queue_load_max**

How message delivery works

- Routers
- Transports
- ACLs

http://www.exim.org/exim-html-current/doc/html/spec_html/ch03.html

How message delivery works



Source: http://exim.org/

Routers (1 of 3)

- Routers are used to guide messages to transports, which ultimately handle the delivery of the message
- Routers operate in a linear fashion. They are processed in the order they appear in the exim configuration file.
- You can query available routers by executing:

exim -bP router_list

exim -bP router <router_name>

Example: (exim -bP router localuser)

Routers (2 of 3)

- Routers contain a driver definition, which determines how that driver will behave.

- A router contains conditions which must be met in order for it to accept the message for delivery. Once accepted, the router passes the message off to the defined transport, which handles the actual delivery of the message.

Routers (3 of 3)

```
/etc/localdomains

/etc/remotedomains
```

Transports

- Transports define mechanisms for actually delivering messages. They operate only when referenced from routers.

- The transports section of the configuration starts with:

```
begin transports
```

Transports

- One remote transport and four local transports are defined:

```
remote_smtp:
driver = smtp
```

- This transport is used for delivering messages over SMTP connections. The list of remote hosts comes from the router.

```
local_delivery:
driver = appendfile
file = /var/mail/$local_part
delivery_date_add
envelope_to_add
return_path_add
```

ACLs

Access Control Lists (ACLs) are defined in a separate section of the run time configuration file, headed by “**begin acl**”. Each ACL definition starts with a name, terminated by a colon.

ACLs

Here is a complete ACL section that contains just one very small ACL:

```
      begin acl
      small_acl:
   accept   hosts = one.host.only
```

Note: You can have as many lists as you like in the ACL section, and the order in which they appear does not matter. The lists are self-terminating

ACL Types

acl_not_smtp

ACL for non-SMTP messages

acl_not_smtp_mime

ACL for non-SMTP MIME parts

acl_not_smtp_start

ACL at start of non-SMTP message

acl_smtp_auth

ACL for AUTH

ACL Examples

```
acl_smtp_rcpt = ${if ={25}{$interface_port} \
  {acl_check_rcpt} {acl_check_rcpt_submit} }
```

```
acl_smtp_data = /etc/acls/\
  ${lookup{$sender_host_address}lsearch\
  {/etc/acllist}{$value}{default}}
```

This looks up an ACL file to use on the basis of the host’s IP address, falling back to a default if the lookup fails. If an ACL is successfully read from a file, it is retained in memory for the duration of the Exim process, so that it can be re-used without having to re-read the file.

More info: http://www.exim.org/exim-html-4.67/doc/html/spec_html/ch40.html

Log Files

Exim logs to three locations:

- **/var/log/exim_mainlog**
- **/var/log/exim_paniclog**
- **/var/log/exim_rejectlog**

The Exim Main Log

- The main log records the arrival of each message and each delivery in a single line in each case.

- Message delivery:

```
2002-10-31 08:59:13 16ZCW1-0005MB-00 => marv
  <marv@hitch.fict.example> R=localuser T=local_delivery
2002-10-31 09:00:10 16ZCW1-0005MB-00 =>
  monk@holistic.fict.example R=dnslookup T=remote_smtp
  H=holistic.fict.example [192.168.234.234]
```

The Exim Main Log

- Message delivery failure:

```
1995-12-19 16:20:23 0tRiQz-0002Q5-00 ** jim@trek99.example
  <jim@trek99.example>: unknown mail domain
```

Log Line Flags

- One line is written to the main log for each message received, and for each successful, unsuccessful, and delayed delivery. These lines can readily be picked out by the distinctive two-character flags that immediately follow the timestamp.

Log Line Flags

- The flags are:

<=	message arrival
=>	normal message delivery
->	additional address in same delivery
*>	delivery suppressed by -N
**	delivery failed; address bounced
==	delivery deferred; temporary problem

Increasing the verbosity of the log file

By setting the **log_selector** global option, you can disable some of Exim’s default logging, or you can request additional logging. The value of **log_selector** is made up of names preceded by plus or minus characters.

For example:

```
log_selector = +arguments -retry_defer
```

Increasing the verbosity of the log file

The list of optional log items is in the following table, with the default selection marked by asterisks:

*acl_warn_skipped	skipped warn statement in ACL
address_rewrite	address rewriting
all_parents	all parents in => lines
arguments	command line arguments
*connection_reject	connection rejections
*delay_delivery	immediate delivery delayed

Exigrep

- The **exigrep** utility is a Perl script that searches one or more main log files for entries that match a given pattern. When it finds a match, it extracts all the log entries for the relevant message, not just those that match the pattern.

Exigrep

- The usage is as follows:

```
exigrep [-t<n>] [-l] [-I] [-v] <pattern> [<log file>] ...
```

Example:

```
exigrep '<= .* \[11.22.33.44\] ' /var/log/exim_log
```

The Exim Panic Log

- Generally contains information concerning (not-always) fatal errors to exim. If this file is constantly growing, it's likely indicative of a greater problem.

```
2008-04-28 10:26:51 non-existent configuration file(s): /etc/exim.conf

2008-04-28 10:26:52 Exim configuration error in line 385 of /etc/exim
.conf.buildtest: error in ACL: unknown ACL condition/modifier in "spf = fail"

2008-04-28 10:42:19 1JqJsR-0004JX-Jb User 0 set for local_delivery transport is
    on the never_users list
```

The Exim Reject Log

- Contains information on messages that were rejected based on policies for RBLS and other ACLs

```
X-AntiAbuse: ID = 80e8a8941009bcd5bf34f4a058c37dc2
R Reply-To: user@yahoo.com
F From: "Dr.Anthony Hobson" <fakebigpimp@excite.com>
MIME-Version: 1.0
X-Sender: fakebigpimp@excite.com
X-Mailer: PHP
Content-Type: text/plain; charset="us-ascii"
Content-Transfer-Encoding: 7bit
I Message-Id: <20070425183915.79B622F669@any.anydomain.com>
Date: Wed, 25 Apr 2007 14:39:15 -0400 (EDT)
2007-04-25 19:39:25 1HgmOi-00028X-Qr H=(wazmzo) [192.168.1.3]
F=<fakebigpimp@excite.com> temporarily rejected after DATA
```

The Exim Queue

- There is just a single collection of messages awaiting delivery, each of which may have several recipients.

- You can list the messages on the queue by running the command:

  exim -bp

- The message-IDs that Exim uses to refer to messages in its queue are mixed-case alpha-numeric, and take the form of: **XXXXXX-YYYYYY-ZZ** Most commands related to managing the queue and logging use these message-ids.

The Exim Queue

- **/var/spool/exim/msglog**

Files contain logging information for each message and are named the same as the **message-id**.

- **/var/spool/exim/input**

Files are named after the message-id, plus a suffix denoting whether it is the **envelope header (-H)** or **message data (-D)**.

Note: These directories may contain further hashed subdirectories to deal with larger mail queues, so don't expect everything to always appear directly in the top /var/spool/exim/input or /var/spool/exim/msglog directories; any searches or greps will need to be **recursive**.

Exim Queue Commands

- `exim -bpc`

Print a count of msgs on the queue

- `exim -bp`

Print a listing oft the msgs on the queue

- `exim -bp | exiqsumm`

Print a summary of messages in the queue

- `exiwhat`

Print what exim is doing

More Info: http://bradthemad.org/tech/notes/exim_cheatsheet.php

Source: http://www.digitalknowhow.com/deals/images/kill_spam.gif

Alternatives to KILL -9 SPAM

Simple – STOP using e-mail

- SpamAssassin
- RBLs
- Boxtrapper
- Account Level Filtering
- SPF
- SRS
- Domain Keys
- DKIM
- ASSP

SpamAssassin/GTUBE

Spam Assassin is an automated mail filter that uses a wide range of heuristic algorithms on mail headers and message body text to identify "SPAM" (unsolicited bulk email).

Once identified, the mail is tagged as "SPAM" for later filtering using the user's desktop mail client.

SpamAssassin on cPanel 11

Exim now runs SpamAssassin scans @ smtp time in ACLS
Previously all mail coming into an account was scanned every time deliver was attempted. This was grossly inefficient.

The side effects of this is that if you have:
* Two domains WITH SEPARATE USERS
* SpamAssassin turned off on the first domain
* SpamAssassin turned on on the second domain
* Mail forwarded to an account on the second domain from the first domain

SpamAssassin on cPanel 11

Any email that was sent to the first domain with be forwarded to the second domain un-scanned as there is no SMTP session between the account as they are local.

Generally you just need to turn SpamAssassin ON for the other domain to solve the problem.

Enabling SpamAssassin

Enabling SpamAssassin globally:
WHM -> Server Configuration -> Tweak Settings

Reinstalling SpamAssassin:
/scripts/realperlinstaller --force Mail::SpamAssassin

For more information, please visit the developer's website: http://www.spamassassin.org/

GTUBE VIDEOS

Ok maybe not.....

GTUBE != YOUTUBE

Source: http://www.pepperspayproductions.org/_borders/watch_videos.gif

Testing SpamAssassin

Testing SpamAssassin (**GTUBE**):
http://spamassassin.apache.org/gtube/

XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE TEST-EMAIL*C.34X

RBLs (Real Time Black List)

A Realtime Black List is a list of IP's that are known to allegedly house spammers on them or be owned by someone who allegedly harbors spammers.
All emails coming from those IP's are blocked immediately.

Examples of RBL's: **SPAMHAUS**, **SPAMCOP**

Boxtrapper

Boxtrapper basically uses the challenge response method to block email.

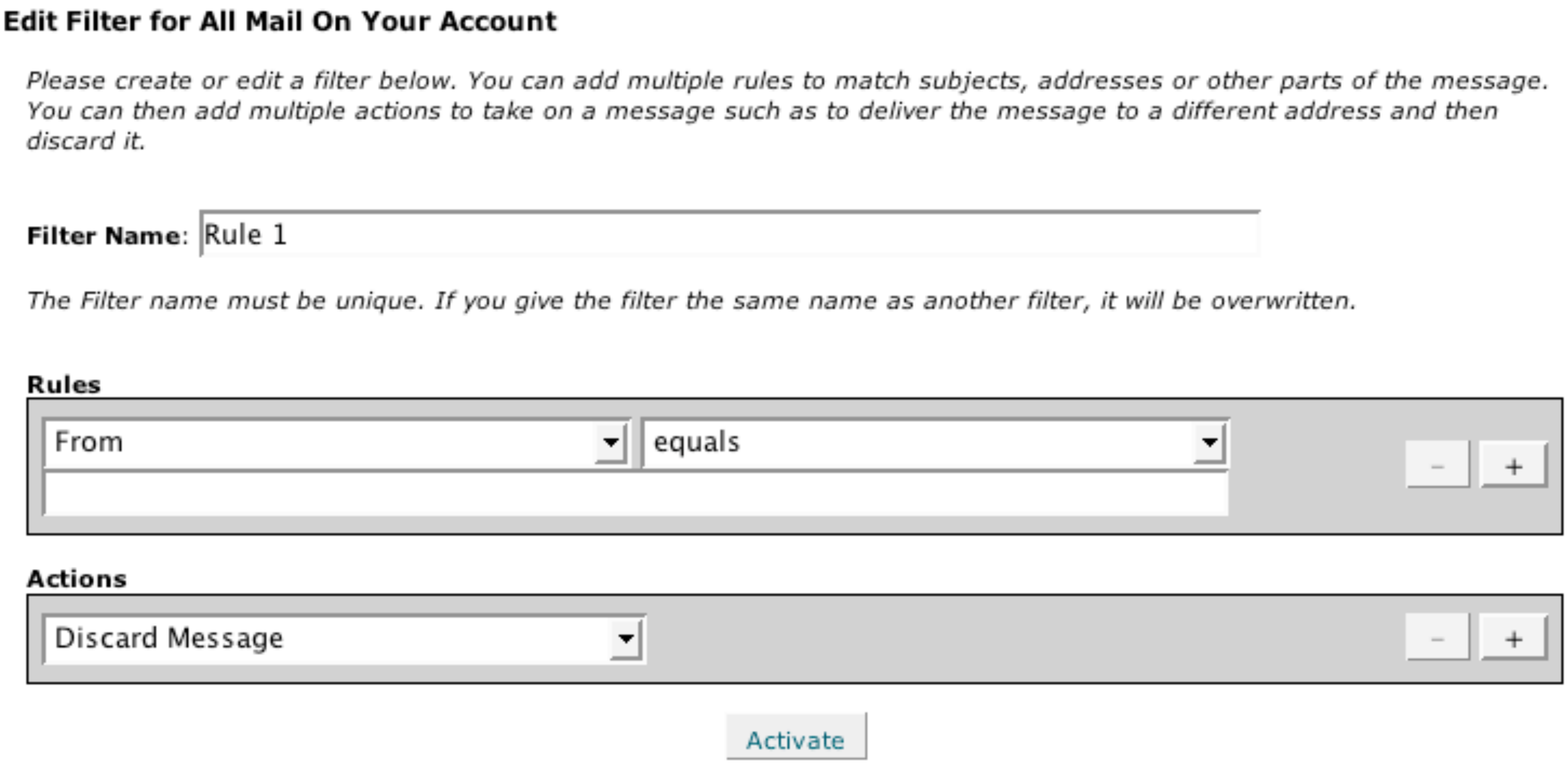
All the e-mail that is not on the user configurable white list is held on a queue waiting for verification.

The mail held on the queue will automatically get a response asking the sender of the address to verify the authenticity of the e-mail by replying to the message without modifying the header.

E-mails with no valid ownership are blocked automatically.

Account Level Filtering

cPanel >> Mail >> Account Level Filtering



Edit Filter for All Mail On Your Account

Please create or edit a filter below. You can add multiple rules to match subjects, addresses or other parts of the message. You can then add multiple actions to take on a message such as to deliver the message to a different address and then discard it.

Filter Name: Rule 1

The Filter name must be unique. If you give the filter the same name as another filter, it will be overwritten.

Rules

From ▾ equals ▾

Actions

Discard Message ▾

Half Time Break

cPanel Skit Alert

“ SPAM Adventures “

Starring:

Matt Dees as “**Spamy**” the alleged Spammer

Eric Ellis as “**Viagry**” the Judge

Todd Shipway as **“Spoofy”** the Plaintiff

Alex Villegas as “**Bulky**” the ISP Dood

SPF

Source: http://papellyy.com/yahoo_site_admin/assets/images/sunburn.33322407_std.jpg

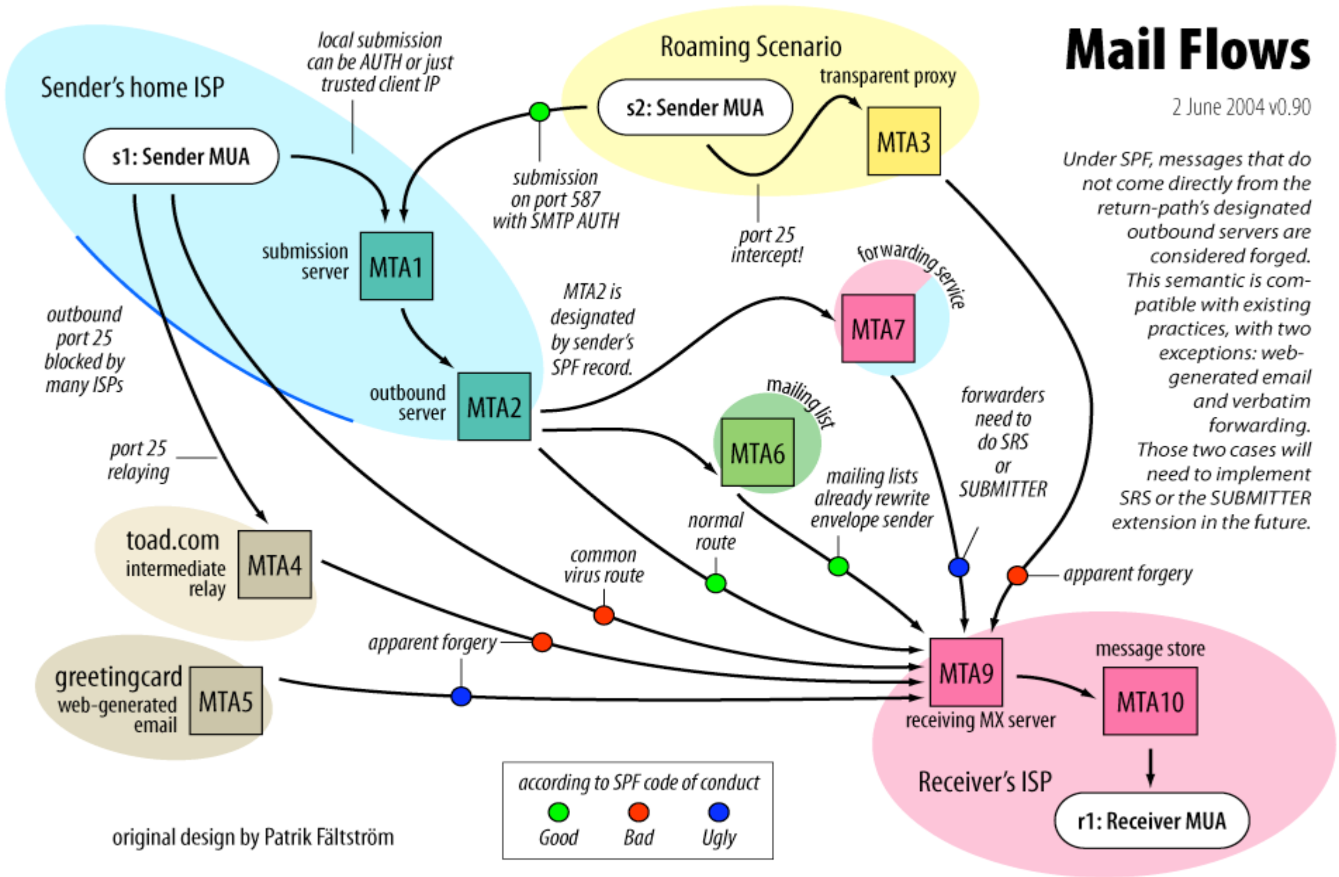
SPF (Sender Policy Framework)

The Sender Policy Framework (SPF) is an open standard specifying a technical method to prevent sender address forgery.

Exim supports SPF. Needs to be activated.

```
deny message = $sender_host_address is not
   allowed to send mail from
$sender_address_domain
    spf = fail
```

SPF (Sender Policy Framework)

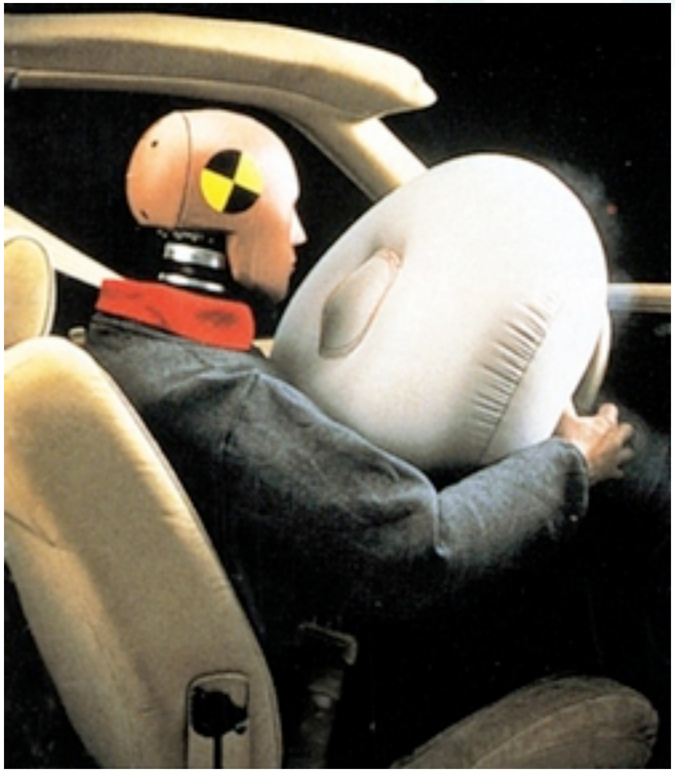

Mail Flows
2 June 2004 v0.90
Sender's home ISP
s1: Sender MUA
local submission can be AUTH or just trusted client IP
submission server
MTA1
outbound server
MTA2
outbound port 25 blocked by many ISPs
port 25 relaying
Roaming Scenario
s2: Sender MUA
transparent proxy
MTA3
submission on port 587 with SMTP AUTH
port 25 intercept!
MTA2 is designated by sender's SPF record.
forwarding service
MTA7
mailing list
MTA6
mailing lists already rewrite envelope sender
forwarders need to do SRS or SUBMITTER
normal route
common virus route
toad.com intermediate relay
MTA4
greetingcard web-generated email
MTA5
apparent forgery
apparent forgery
MTA9
receiving MX server
message store
MTA10
Receiver's ISP
r1: Receiver MUA
according to SPF code of conduct
Good
Bad
Ugly
original design by Patrik Fältström

Under SPF, messages that do not come directly from the return-path's designated outbound servers are considered forged. This semantic is compatible with existing practices, with two exceptions: web-generated email and verbatim forwarding. Those two cases will need to implement SRS or the SUBMITTER extension in the future.

Source: http://old.openspf.org/mailflows-l.png

SRS

Supplementary Restraint System?



http://www.garagelibrary.com/images/airbag.jpg

SRS (Sender Rewriting Scheme)

The SRS (Sender Rewriting Scheme) was developed to solve a problem introduced by SPF for forwarding email. It is a stop-gap measure. Please see this site for details regarding the SRS:

http://spf.pobox.com/srs/

IMPORTANT: It is essential to understand the SRS before using it so that you can make certain you don't introduce security holes in your mail server.

To use SRS, first get the latest version of the libsrs_alt library available from:

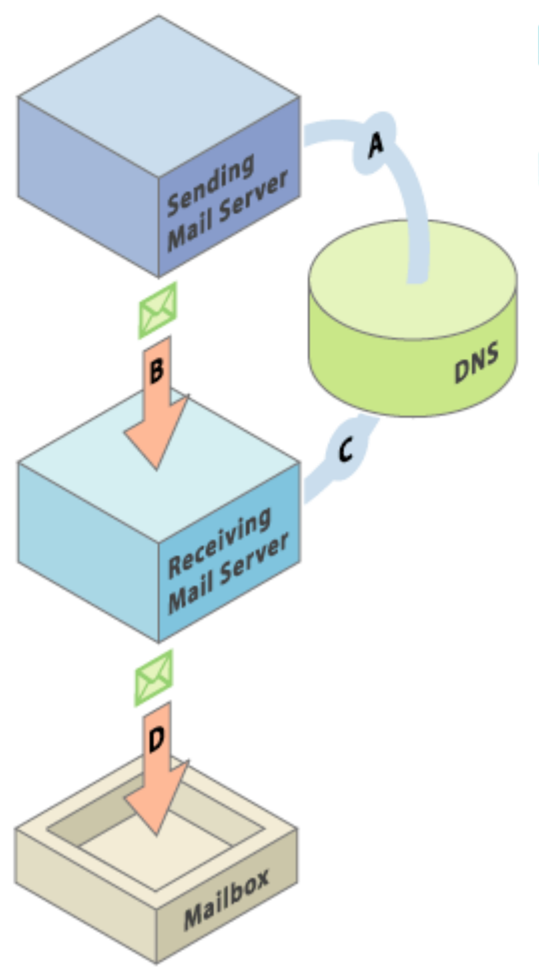
http://srs.mirtol.com/

Domain Keys

DomainKeys is a Yahoo!-proposed system for verifying the domain of an e-mail sender. DomainKeys prevents forged e-mails from claiming to be from a domain it is not coming from.

Exim is a DomainKey aware MTA.
Yahoo Domain Keys Documentation:
http://antispam.yahoo.com/domainkeys

Domain Keys



Source: http://www.notebooknews.co.uk/2000/graphics/dkeys.gif

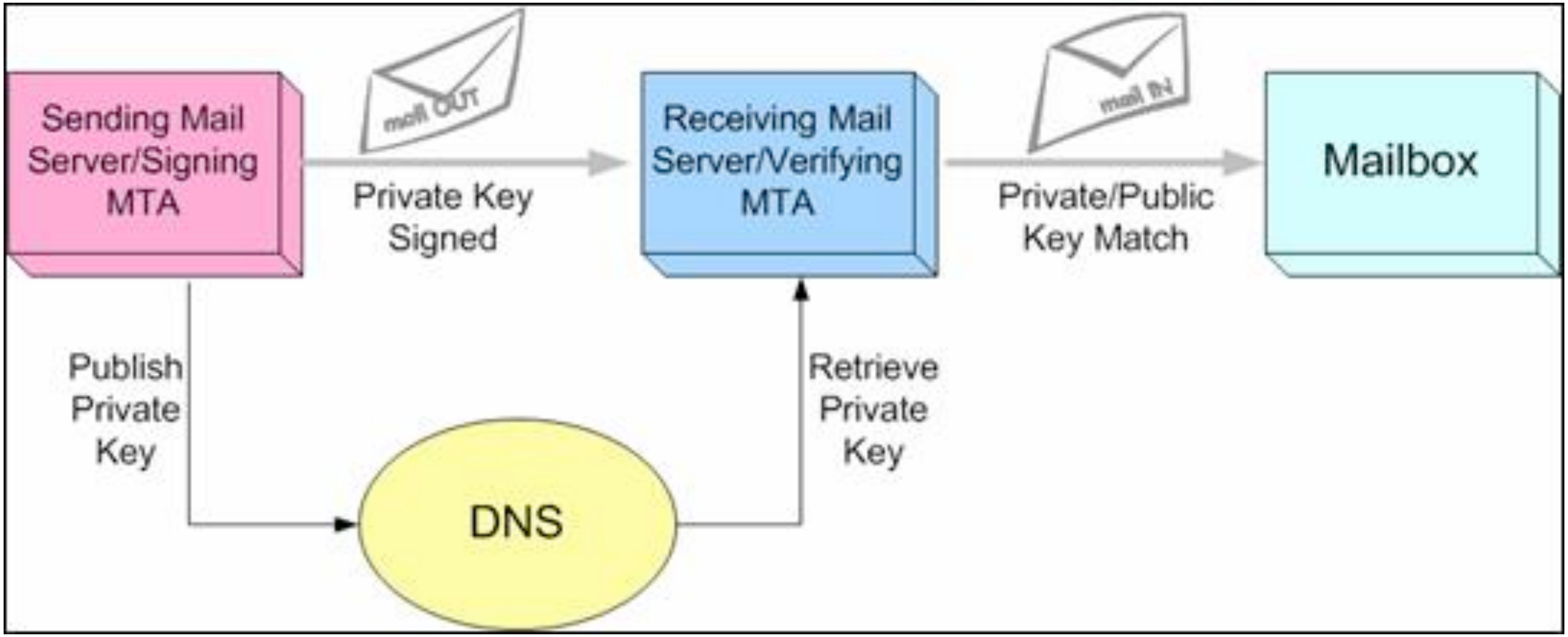
DKIM (DomainKeys Identified Mail)

DomainKeys Identified Mail (DKIM) lets an organization take responsibility for a message while it is in transit. The organization is a handler of the message, either as its originator or as an intermediary.

Their reputation is the basis for evaluating whether to trust the message for delivery. Technically DKIM provides a method for validating a domain name identity that is associated with a message through cryptographic authentication.

http://www.dkim.org/

DKIM



Source: http://www.axigen.com/usr/images/article/Antispam%20Practices/clip_image003.jpg

ASSP (Anti-Spam-SMTP-Proxy)

Features:

- Ability to block or subject-line tag e-mail against a multitude of spam types
- Fully transparent Training Mode for implementation testing
- Bayesian Analysis
- Automatic Bayesian corpus training
- Automatic Whitelisting
- Redlist to control what addresses can and can not be added to the Whitelist
- Allow spam to bypass certain filters per recipient
- RegEx based filters
- Penalty Box (PB) trapping of misbehaving IP addresses
- DNSBL (DNS-based Block List), aka RBL

http://assp.sourceforge.net

ASSP (Anti-Spam-SMTP-Proxy)

Features:

- SPF (aka Sender Policy Framework)
- SRS fix-up (aka Sender Rewriting Scheme)
- Delaying (aka Greylisting)
- Sender & recipient validation
- Multi-level attachment blocking
- Honeypot e-mail address trapping
- Multiple RFC validation mechanisms
- Low maintenance once setup
- Analysis interface to determine exactly why a message was blocked
- Ability to send copies of all spam to specified address

http://www.asspsmtp.org/wiki/Welcome

ASSP (Anti-Spam-SMTP-Proxy)

Benefits:

- Simple Integration with existing environment
- Highly customizable filtering mechanisms
- ASSP does not generate e-mail or backscatter. (except for administrative/ internal spam/notspam report confirmation messages)
- Runs on FreeBSD, Linux, OS X, Windows, and many others

Who is it not for?

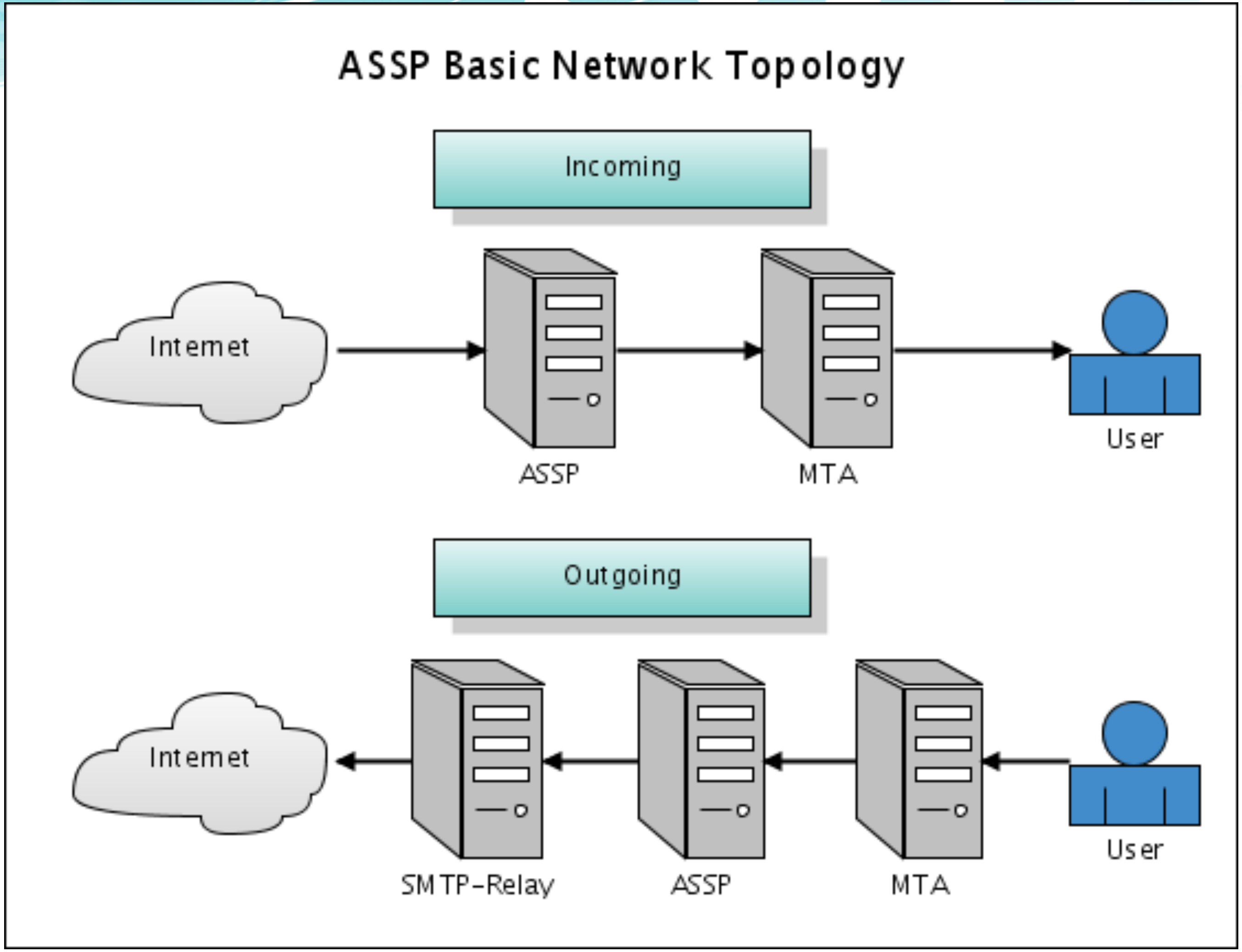
- Individual clients. ASSP must be installed and configured to filter in-front of an SMTP server.
- Domains which receive mail indirectly. Fetchmail for example.

What it is not

- An SMTP server. ASSP is proxy between your SMTP server, and SMTP clients (other public SMTP server and your local clients).

http://www.asspsmtp.org/wiki/Welcome

ASSP E-mail Flow



Source: http://www.asspsmtp.org/wiki/images/thumb/d/db/ASSP_-_Network_topology_-_Basic.png/400px-ASSP_-_Network_topology_-_Basic.png

Geek Brainstorm

Share your EXIM/SPAM Knowledge

Please feel to share any knowledge, suggestions, tips & tricks.

The floor is yours!

Source: http://www.steveshardwoodfloors.com/images/woodFloorLg.jpg

Q & A

Source: http://thumbs.dreamstime.com/
thumb_27/11303812072So19e.jpg