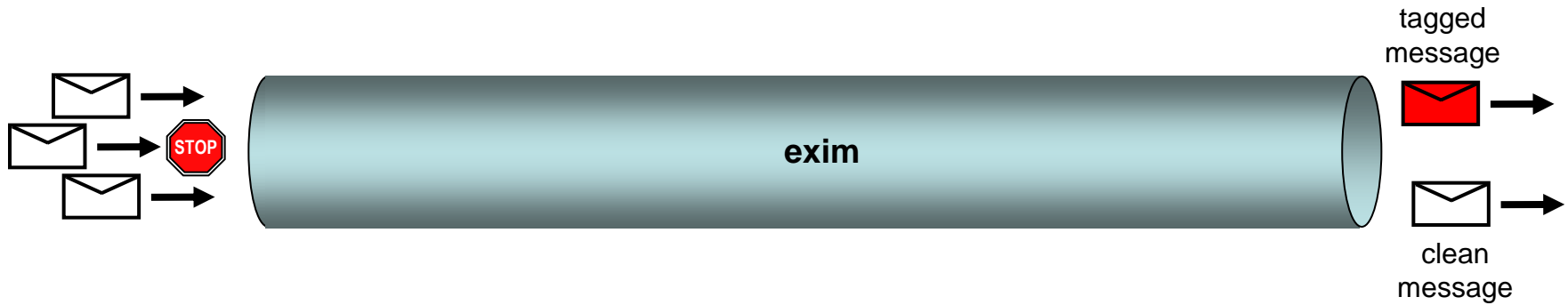


ETH Zürich - Mail Filtering Service

(TERENA 2009)

Mail-Filtering Policy



- Accept or reject messages; do not accept & then silently delete them
- Provide users with a **tag-only** option for spam
- Allow personal **black-listing** & **white-listing** of sender addresses and domains
- Allow use of wildcards in black-listed / white-listed sender domains (*.ru)
- Reject spam messages, unless sender is white-listed or recipient is tag-only
- Reject malware & phishing messages without regard to user preferences

Mail Filtering Environment

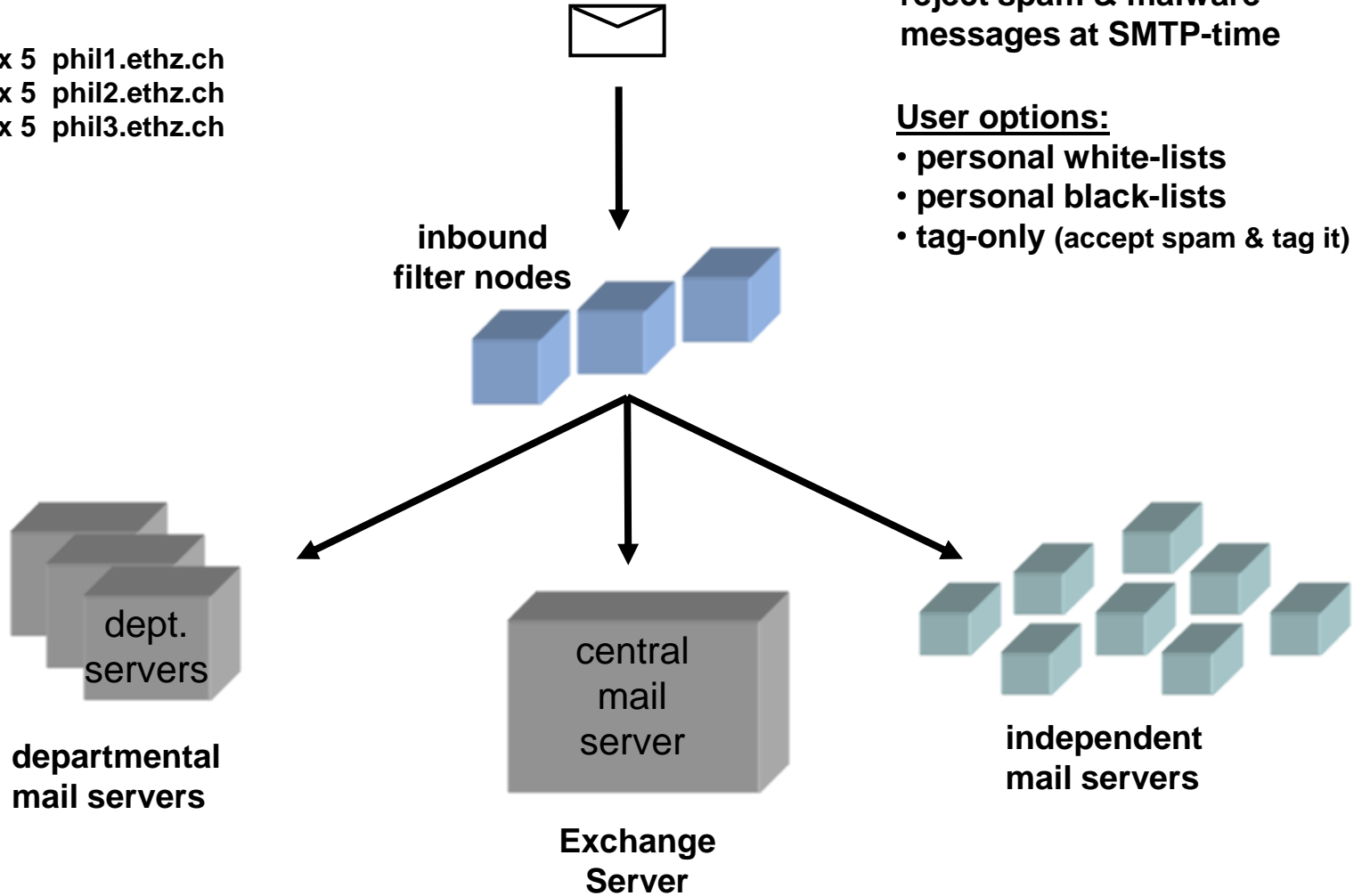


Mail-Filtering Environment (1)

DNS MX records direct a domain's mail to the filter nodes

example:

```
biol.ethz.ch mx 5 phil1.ethz.ch  
biol.ethz.ch mx 5 phil2.ethz.ch  
biol.ethz.ch mx 5 phil3.ethz.ch
```



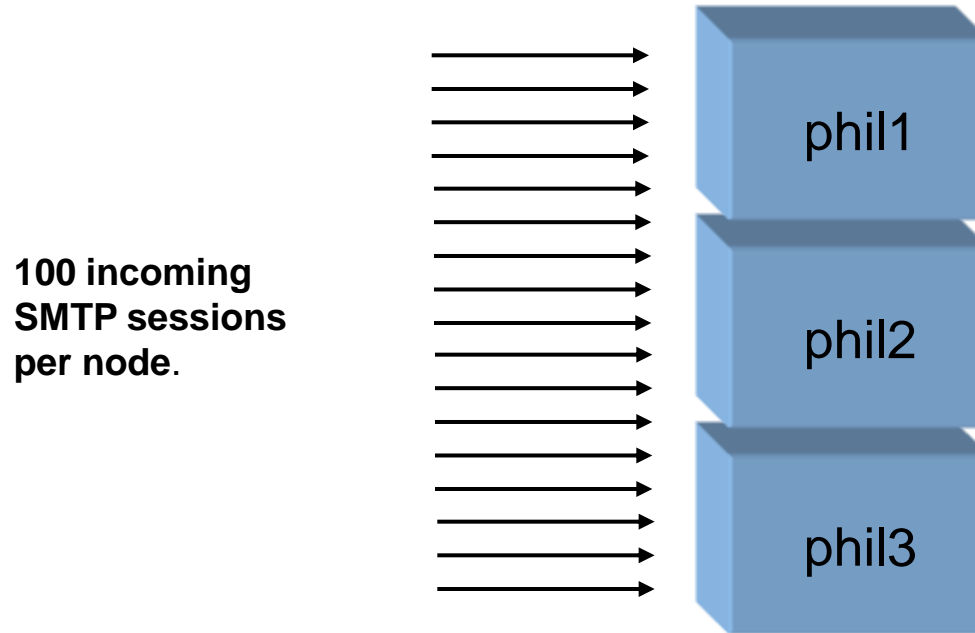
Filtering policy:
reject spam & malware messages at SMTP-time

User options:

- personal white-lists
- personal black-lists
- tag-only (accept spam & tag it)

Mail-Filtering Environment (2)

- filtering provided for 20,000 users
- we process 1.5 to 3.5 million messages per day
- 3 filtering nodes & 1 back-up receiver



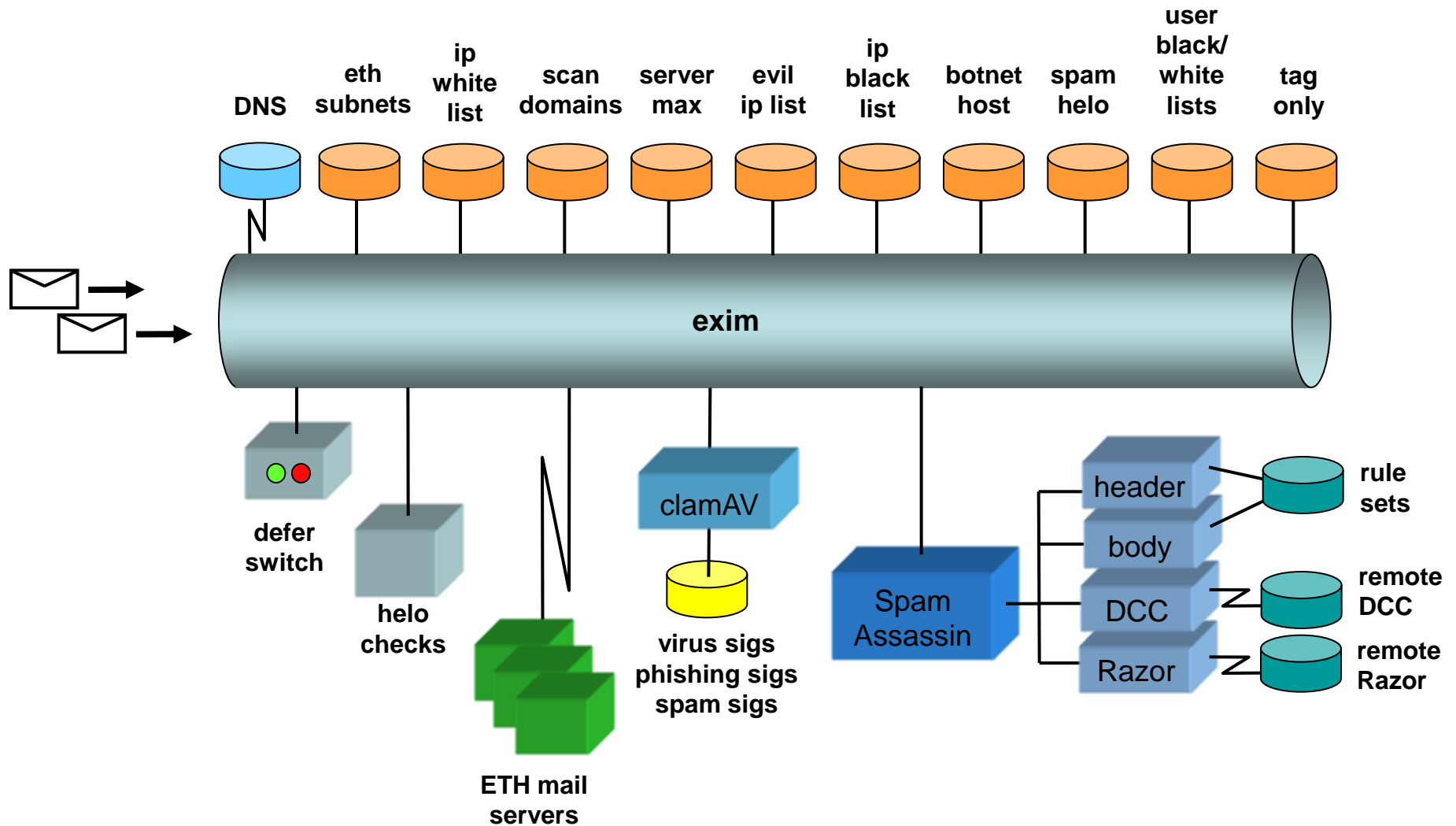
SMTP-time message filtering:

- filtering is done while the SMTP connection is still open
- filtering requires several seconds
- unwanted messages are rejected during the SMTP session, or accepted & tagged

Open-Source Filtering Components

- EXIM mail gateway software
- ClamAV virus/phishing detection network
+ 3rd-party signatures
- SpamAssassin spam content-filtering software
+ SARE & local rule-sets
- DCC mass-mailing detection network
(called from SpamAssassin)
- Razor spam detection network
(called from SpamAssassin)

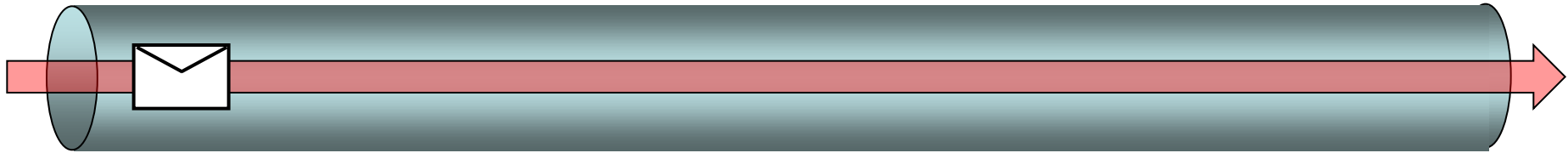
Mail-Filtering Components



An SMTP Session (1)

If connection comes from one of our hosts, then exempt it from spam checks

If sender IP-address cannot be resolved to a host name, then mark it for rcpt-phase rejection



TCP/IP Connection

from 131.111.8.59

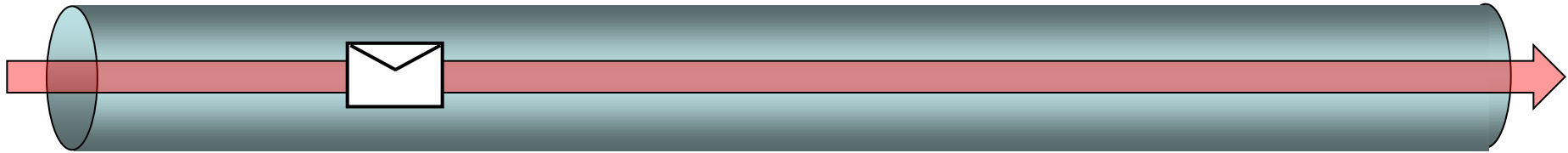
If sender IP is found in a local blacklist, then reject it now or mark it for rcpt-phase rejection

If sender IP is found in a DNS IP blacklist or has a dynamic IP-address, then mark it for rcpt-phase tag/reject

An SMTP Session (2)

If the HELO name does not have correct syntax or the sender said something stupid like **HELO device.local**, then mark it for rcpt-phase tag/reject

If the sender said, **HELO [IP-address]**
& the HELO IP differs from the connecting IP,
or the HELO IP matches my IP-address,
then mark it for rcpt-phase tag/reject



TCP/IP Connection

from 131.111.8.59

EHLO

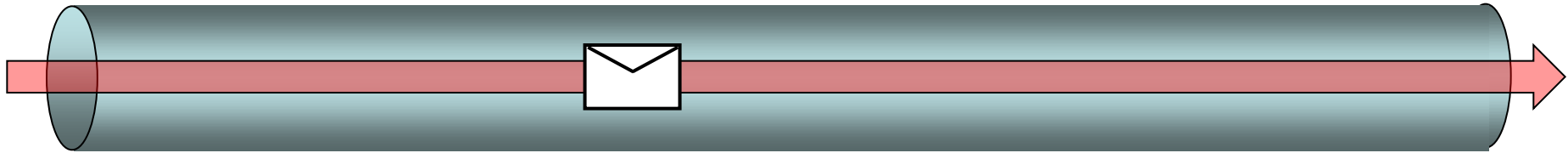
spamcentral.net

If sender host has been identified as a member of a botnet,
then reject it now or mark it for rcpt-phase rejection

If the HELO name does not have corresponding DNS records, or
if the HELO name matches one of my MX records, or
if the HELO name matches my hostname,
if the HELO name matches a spammer HELO,
then mark it for rcpt-phase tag/reject

An SMTP Session (3)

If the sender domain does not exist,
then reject the connection now



TCP/IP Connection

from 131.111.8.59

EHLO

spamcentral.net

MAIL FROM:

spammer@spam.net

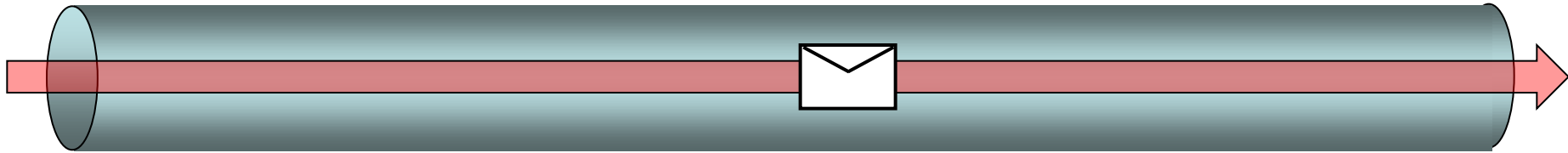
SIZE=381

An SMTP Session (4)

If the recipient address does not exist,
then reject the recipient address

If the **MAIL FROM SIZE** parameter indicates that the
message is too big for the recipient's mail server,
then reject the recipient address

If the recipient has blacklisted this sender then
reject the recipient address



TCP/IP Connection

from 131.111.8.59

EHLO

spamcentral.net

MAIL FROM:

spammer@spam.net

SIZE=381

RCPT TO:

tom@ethz.ch

If the recipient has white-listed this sender , or has selected
the tag-only option, then skip the spam checks

If the recipient uses default spam-handling then reject the
recipient address, if the message has been marked

If this is a multi-recipient message, & the current recipient's
spam preference differs from that of the 1st recipient, then
temporarily reject this recipient address

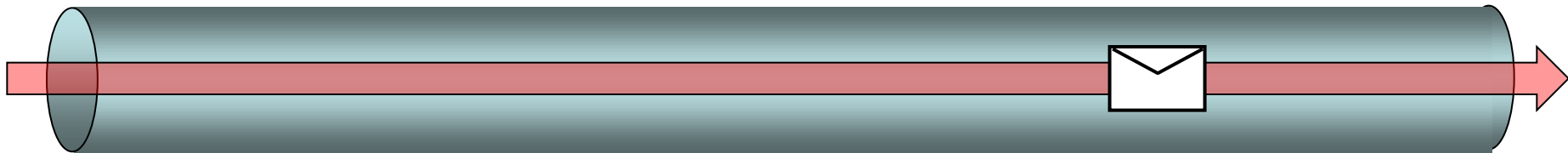


An SMTP Session (5)

If the message is bigger than 30 MB,
then reject the message

If the message content matches a ClamAV
malware signature, then reject the message

If the message content matches a ClamAV spam
signature, then tag or reject the message



TCP/IP Connection

from 131.111.8.59

EHLO

spamcentral.net

MAIL FROM:

spammer@spam.net

SIZE=381

RCPT TO:

tom@ethz.ch

DATA

Subject: A Hot deal!
From: admin@ethz.ch
Date: 08/30/2007 16:00
To: santaclaus@northpole.net
Received: from mail1.pole.net [83.4.6.232]

The PRGN stock price is about to soar!
Buy it now to get in on the HOT DEAL!

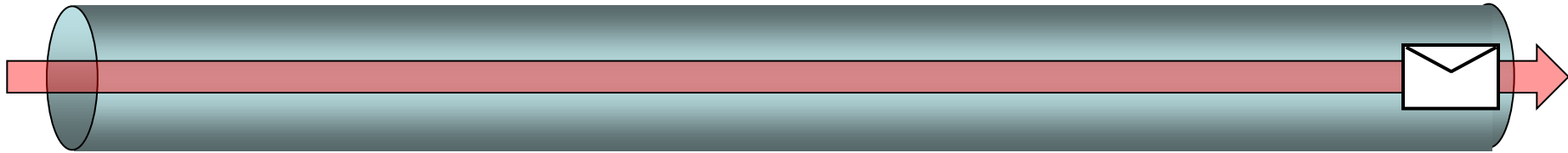
.

If SpamAssassin thinks that the message is spam,
then tag or reject the message



An SMTP Session (6)

Accept & deliver
tagged, clean &
white-listed
messages



TCP/IP Connection

from 131.111.8.59

EHLO

spamcentral.net

MAIL FROM:

spammer@spam.net

SIZE=381

RCPT TO:

tom@ethz.ch

DATA

Subject: A Hot deal!
From: admin@ethz.ch
Date: 08/30/2007 16:00
To: santaclaus@northpole.net
Received: from mail1.pole.net [83.4.6.232]

The PRGN stock price is about to soar!
Buy it now to get in on the HOT DEAL!

.

QUIT

accept &
deliver



End

