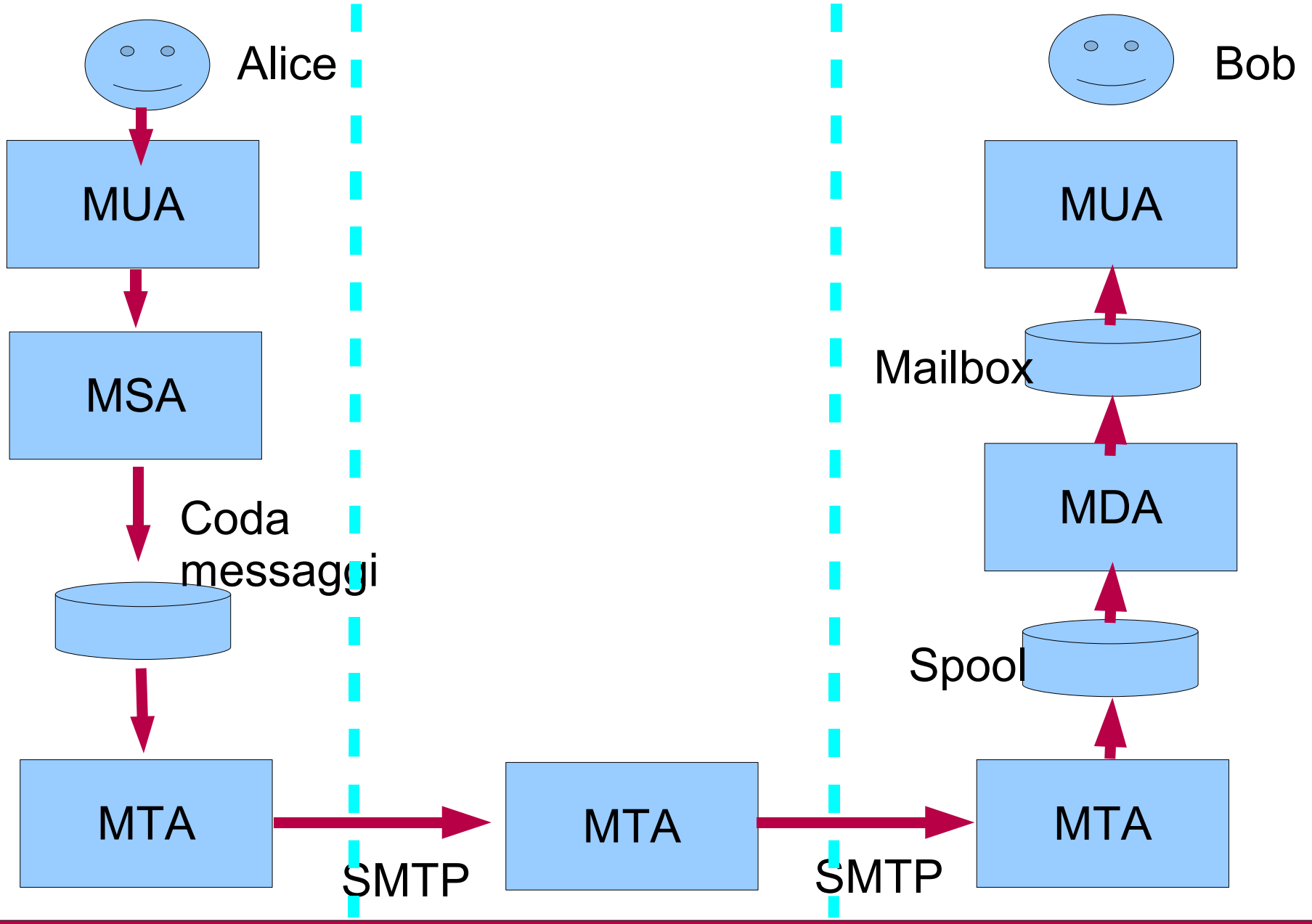
Un sistema di Posta Open Source

Riccardo Lancellotti

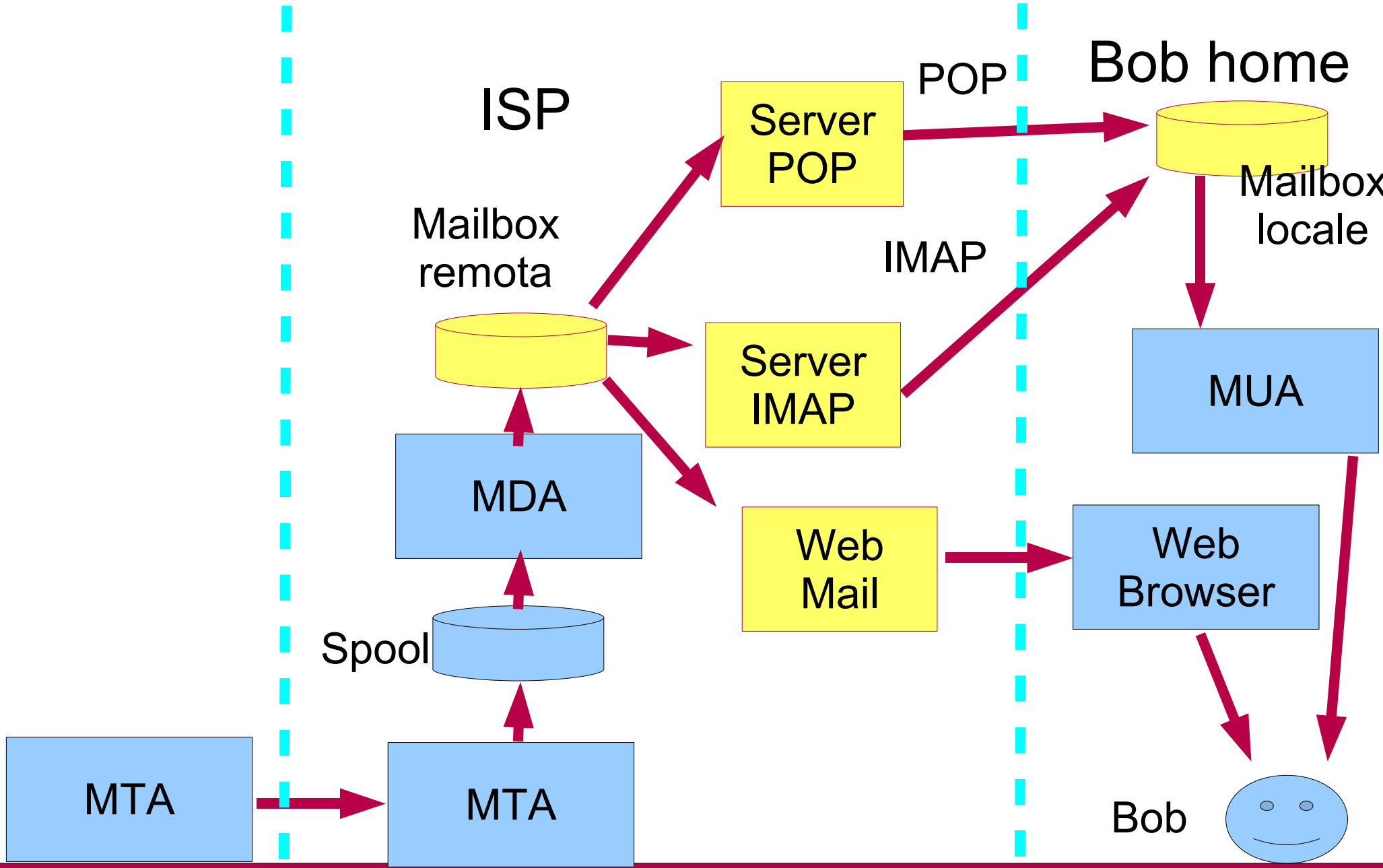
Un sistema di posta (scenario “tradizionale”)



Spiegazione dei componenti

- **MUA= Mail User Agent**
  - Programma usato per comporre e spedire posta
  - E.g., Mozilla Thunderbird, Outlook, Eudora, Evolution...
  - Può essere anche un'applicazione Web (Webmail)
- **MSA= Message Submit Agent**
  - Serve per inoltrare il messaggio al sistema di posta
  - E.g., Sendmail, molti MUA comprendono anche un MSA
- **MTA= Mail Transfer Agent**
  - Gestisce l'invio della posta mediante SMTP
  - E.g., sendmail, exim, qmail
- **MDA=Mail Delivery Agent**
  - Prende i dati dal MTA e li conserva in una mailbox
  - E.g., sendmail, exim, qmail

Un sistema di posta (scenario “con ISP”)



Cambiamenti rispetto a prima

- **Tra il MDA e l'MUA di Bob c'e' uno nuovo strato software**
- **La mailbox viene resa fruibile in remoto mediante appositi server (protocolli POP e IMAP)**
- **Bob usa i server per copiare i contenuti della mailbox remota in locale**

Installazione del sistema di posta

Implementazione di un servizio di posta elettronica

Obiettivi

- **Utilizzare componenti *standard***
- **Valutare livello di sicurezza**

Sistema di base

- **Server SMTP**
- **Server IMAP e/o POP3**
- **Client**
  - Webmail
  - Outlook, Evolution, ...

Implementazione di un servizio di posta elettronica

Possibili componenti aggiuntivi

- **Webmail**
- **Antivirus**
- **Antispam**
- **Autenticazione**
- **Cifratura**
- **Firma digitale dei messaggi**
- **...**

Server SMTP open source

- **Exim**
  Homepage: http://www.exim.org
- **Postfix**
  Homepage: http://www.postfix.org
- **Qmail**
  Homepage: http://www.qmail.org/
- **Sendmail**
  Homepage: http://www.sendmail.org/

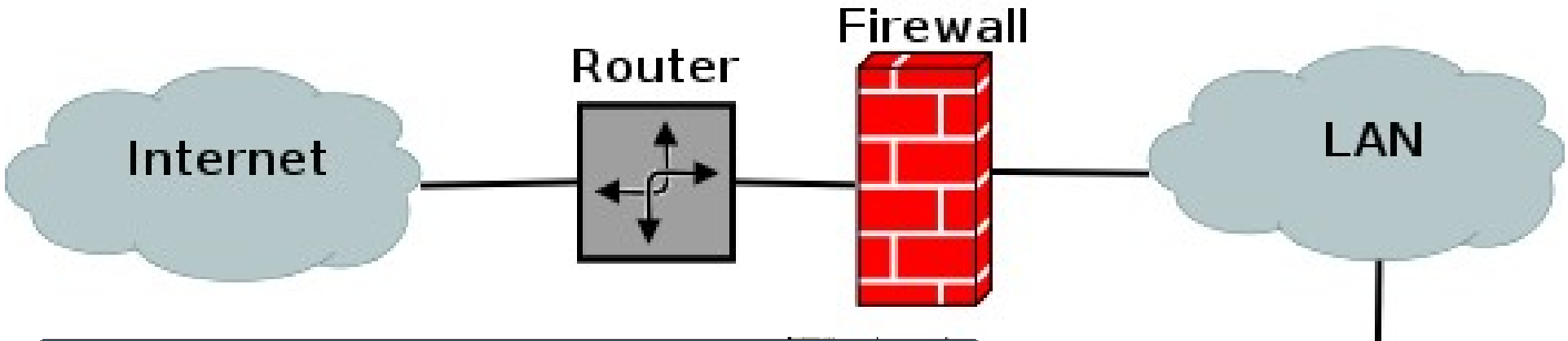
Server SMTP: Exim

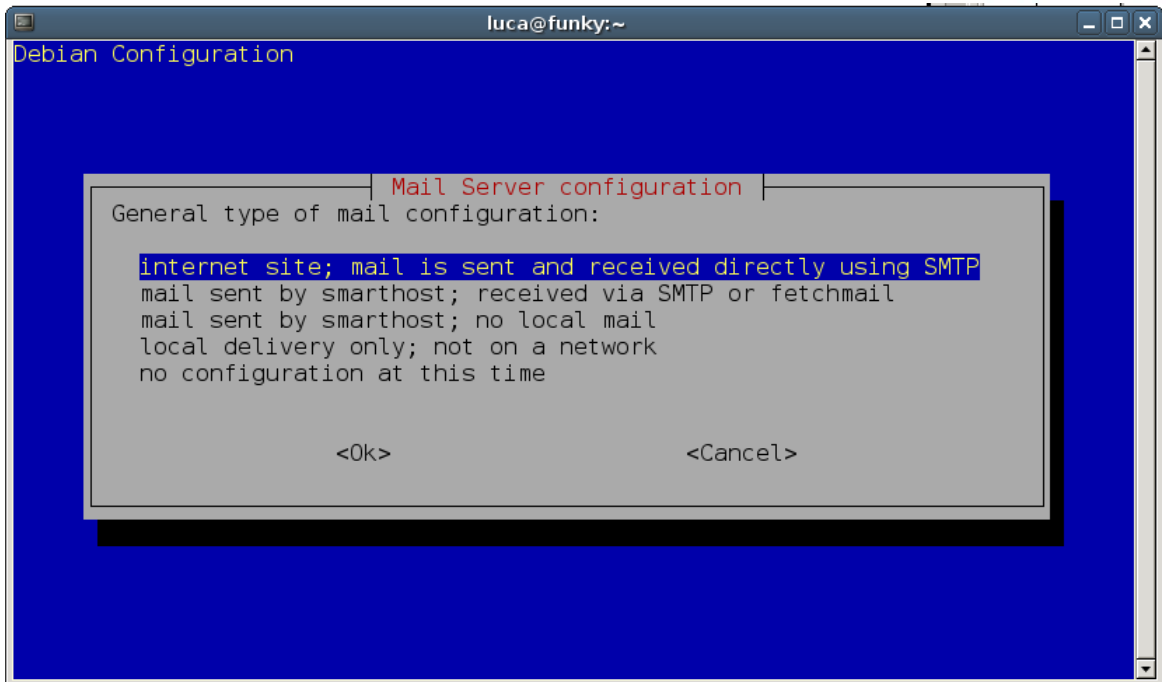
- **SMTP/ESMTP server**
- **MTA pensato per host permanentemente connessi ad Internet (... ma utilizzabile anche dagli altri)**
- **Elevata portabilità:**
  - *nix (sia free che proprietari),
  - Windows (con Cygwin, non nativo)
- **(Relativamente) semplice da installare e configurare**
  - Pacchettizzato per tutte le distribuzioni
  - Un solo file di configurazione monolitico per controllare il demone in tutti i suoi aspetti

Exim – Installazione e configurazione di base

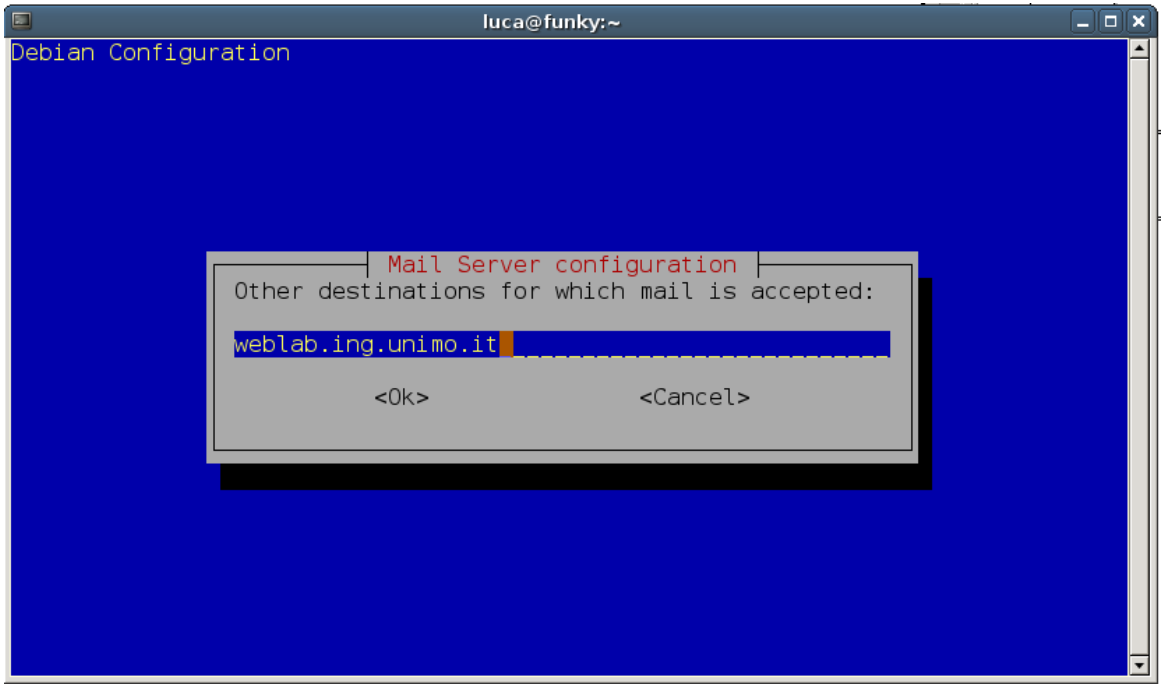
- **Installazione del pacchetto:**
  `$ apt-get update`
  `$ apt-get install exim4`
  (eventualmente installare anche eximon:)
  `$ apt-get install eximon4`
- **Configurazione di base:**
  `$ dpkg-reconfigure exim4-config`
  - tipo di mail-server
  - “caselle postali”? mailbox, maildir, (database)
  - logging? syslog, file
  - …

Exim – Configurazione
Server SMTP per un dominio





Exim – Configurazione
Server SMTP per un dominio



- **Parametro fondamentale: domini per cui il mail server deve accettare posta in ingresso**
- **L'errata configurazione può portare ad un open relay**

Exim – Verifica di funzionamento: invio

```
$ telnet <my_IP> 25
Trying 155.185.54.142...
Connected to tucatuca.ing.unimo.it.
Escape character is '^]'.
220 Knoppix ESMTP Exim 4.63 Mon, 05 Feb 2007 09:44:11 -0500
helo mail
250 Knoppix Hello merlot.ing.unimo.it [155.185.54.157]
mail from:bill@microsoft.com
250 OK
rcpt to: knoppix@weblab.ing.unimo.it
250 Accepted
data
354 Enter message, ending with "." on a line by itself
Subject: prova
Ciao.
.
250 OK id=1HE56P-0001nU-O7
quit
221 Knoppix closing connection
 Connection closed by foreign host.
```

Exim – Verifica di funzionamento: invio

```
$ telnet <my_IP_from_another_IP> 25
Trying 155.185.54.142...
Connected to tucatuca.ing.unimo.it.
Escape character is '^]'.
220 Knoppix ESMTP Exim 4.63 Mon, 05 Feb 2007 09:56:35 -0500
helo mail
250 Knoppix Hello merlot.ing.unimo.it [155.185.54.157]
mail from:bill@microsoft.com
250 OK
rcpt to: ballmer@microsoft.com
550 relay not permitted
quit
221 Knoppix closing connection
Connection closed by foreign host.
```

OK, non è un open relay

Exim – Verifica di funzionamento

- **La configurazione è minimale ... comunque il servizio di posta elettronica (invio/ricezione e-mail) è stato installato ed è funzionante**
- **Mancano gli utenti; due possibilità:**
  - creare un utente di sistema ad ogni utente e-mail
  - Non creare gli utenti di sistema → *virtual domains*
    - DBMail: http://www.dbmail.org/
    - DBMail Administrator: http://library.mobrien.com/dbmailadministrator/
- **Mancano i servizi per la gestione avanzata dei messaggi: protocolli POP3 e/o IMAP**

Server IMAP open source

- **Courrier**
  http://www.courier-mta.org/imap/
- **Dovecot**
  Homepage: http://www.dovecot.org/
- **Cyrus**
  http://cyrusimap.web.cmu.edu/

Courier imapd – Installazione e configurazione di base

- **Installazione del pacchetto:**

```
$ apt-get update
$ apt-get install courier-imap
$ apt-get install courier-imap-ssl
```

- **Configurazione di base:**
  - /etc/courier/imapd
  - /etc/courier/imapd-ssl
    - /etc/courier/imapd.cnf
    - /usr/lib/courier/mkimapdcert: genera imapd.pem

Webmail

- **Le Webmail open source e gratuite sono svariate**
- **Alcuni esempi:**
  - Squirrelmail
    http://www.squirrelmail.org/
  - Horde
    http://www.horde.org/
  - Sqwebmail - Courier Webmail
    http://www.courier-mta.org/sqwebmail/
  - Openwebmail
    http://www.openwebmail.org/

Webmail

- **La scelta spesso ricade solo sulla grafica ma ...**
- **bisognerebbe considerare le altre applicazioni e protocolli con cui occore integrare la Webmail**
  - IMAP, POP3, SMTP server (SSL o TLS?)
  - LDAP e/o altri servizi di autenticazione
  - Calendari ed Address Book
  - Server Web (HTTP o HTTPS)
  - ...
- **... e naturalmente la sicurezza**

Squirrelmail – Installazione e configurazione di base

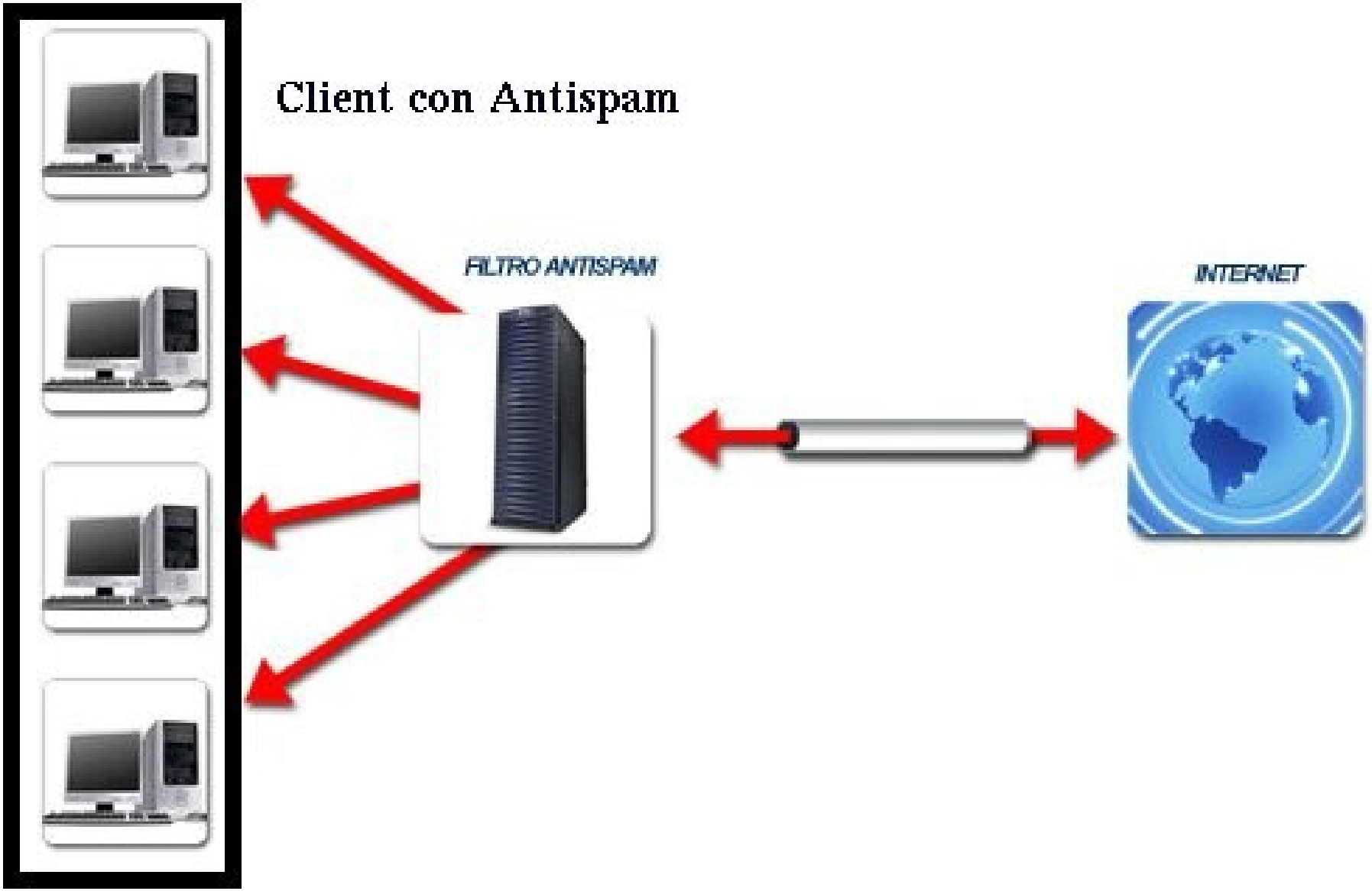
- **Installazione del pacchetto:**
  `$ apt-get install squirrelmail`
- **Configurazione di squirrelmail:**
  `$ /usr/sbin/squirrelmail-configure`
  oppure
  `$ vim /etc/squirrelmail/config.php`
  (Attenzione alla configurazione di SMTPd e IMAPd)
- **Configurazione di apache:**
  - Controllare che mod_rewrite sia abilitato
    `$ ls /etc/apache2/mods-enabled/`
  - Se non lo è ... abilitarlo
    `$ a2enmod rewrite`

Antispam e antivirus

Spam e Antispam

- **L'Unione Europea stima che oltre il 50% dei messaggi di posta elettronica è costituito da mail di spam**
- **Questo comporta notevoli costi per le aziende**
  - La perdita di produttività rappresenta il costo principale dello spam
- **Un altro costo elevato è legato alla banda sprecata**
- **Si tenta di eliminare lo spam in ricezione**
  - Possibili errori: *falsi positivi* e *falsi negativi*

Spam e Antispam



Antispam open source

- **Spamassassin http://spamassassin.apache.org/**
- **Dspam http://dspam.nuclearelephant.com/**
- **Mailwasher http://oss.firetrust.com/home/**
- **SpamPal (per client di posta Windows, open source) http://www.spampal.org/**
- **SpamBayes http://spambayes.cvs.sourceforge.net**

Antispam server-side - Spamassassin

- **È un progetto della Apache Software Foundation**
- **È un mail filter che sfrutta diverse tecniche:**
  - analisi del testo (parole chiave)
  - filtri bayesiani
  - DNSBL (black list)
  - database cooperativi

Filtri bayesiani

- **I primi antispam utilizzavano tecniche di filtraggio basate su liste di parole chiave**
  - Oggi queste tecniche darebbero troppi falsi ed inoltre necessitano di aggiornamenti delle liste continui
- **I filtri bayesiani usano un approccio matematico basato sulla probabilità bayesiana**
  - È basata sul principio che molti eventi sono interdipendenti
  - La probabilità che un evento si verifichi in futuro può essere dedotta dal verificarsi dello stesso nel passato

Database cooperativi

- **Sfruttano digest di messaggi di spam conosciuti**
- **Sono basati su un osservazione semplice: se la stessa e-mail arriva a moltissime persone allora è estremamente probabile che sia spam**
- **Ogni server SMTP può cooperare e/o utilizzare i dati conservati nei database previa iscrizione**
- **Alcuni link:**
  - Razor: http://razor.sourceforge.net/
  - Pyzor: http://pyzor.sourceforge.net/

DNSBL

- **DNS-based blackhole list**
- **Tecnica basata su elenchi di indirizzi IP di mail server, open proxy e ISP sfruttati dagli spammer**
- **Liste sono consultate attraverso query DNS**
- **Aggiornamento garantito dal sistema DNS-like**
- **Alcuni link:**
  - http://www.dsbl.org
  - http://ordb.org
  - http://spamhaus.org

Antispam server-side - Spamassassin

- **Spamassassin NON è un programma per cancellare o instradare verso mail box lo spam, né per inviare *bounce* al mittente a**lla ricezione di posta non gradita
- Ciascun messaggio di posta viene esaminato e, in seguito, viene assegnato un punteggio in base alla probabilità che sia spam
- Sarà compito di altri strumenti software eseguire l'instradamento verso una cartella particolare della posta in base al punteggio assegnato da SA

Antispam server-side - Spamassassin

- Spamassassin controlla sia gli header che i testi delle mail in arrivo attraverso diversi test euristici
- Una volta identificata come spam, la mail può essere marcata per ulteriori azioni da parte dei client di posta
- Generalmente ha una percentuale di successo tra il 95% ed il 100% in base a come viene istruito il filtro bayesiano
- La percentuale di falsi negativi è intorno al 0.9% e quella di falsi positivi è 0.1%

Exim e Spamassassin - Installazione e configurazione

- **Installazione di Spamassassin:**
  ```
  $ apt-get install spamassassin razor
  dcc-client pyzor spamc
  ```
- **È necessario compilare Exim con le opzioni per il content scanning**
- **Utilizzando distribuzioni Debian based il pacchetto da installare è exim4-daemon-heavy:**
  ```
  $ apt-get install exim4-daemon-heavy
  ```

Exim e Spamassassin - Installazione e configurazione

- **Configurazione di spamassassin:**

```
$ cat /etc/spamassassin/local.cf
# This is the right place to customize
# your installation of SpamAssassin.
...
```

- **Configurazione del demone spamd**

```
$ vim /etc/default/spamassassin
```

(impostare "ENABLED=1" ed aggiungere la

```
OPTION "-s /var/log/spamd.log")
$ /etc/init.d/spamassassin restart
```

Exim e Spamassassin - Installazione e configurazione

- **Alcuni esempi di configurazione personalizzata (local.cf):**

```
required_score 4.0
rewrite_header Subject <<<<SPAM>>>>
report_safe 1
score RAZOR2_CHECK 3.5
score PYZOR_CHECK 2.5
score MSGID_DOLLARS_RANDOM 2.0
blacklist_from *@weblab.ing.unimo.it
whitelist_from *@unimore.it
```

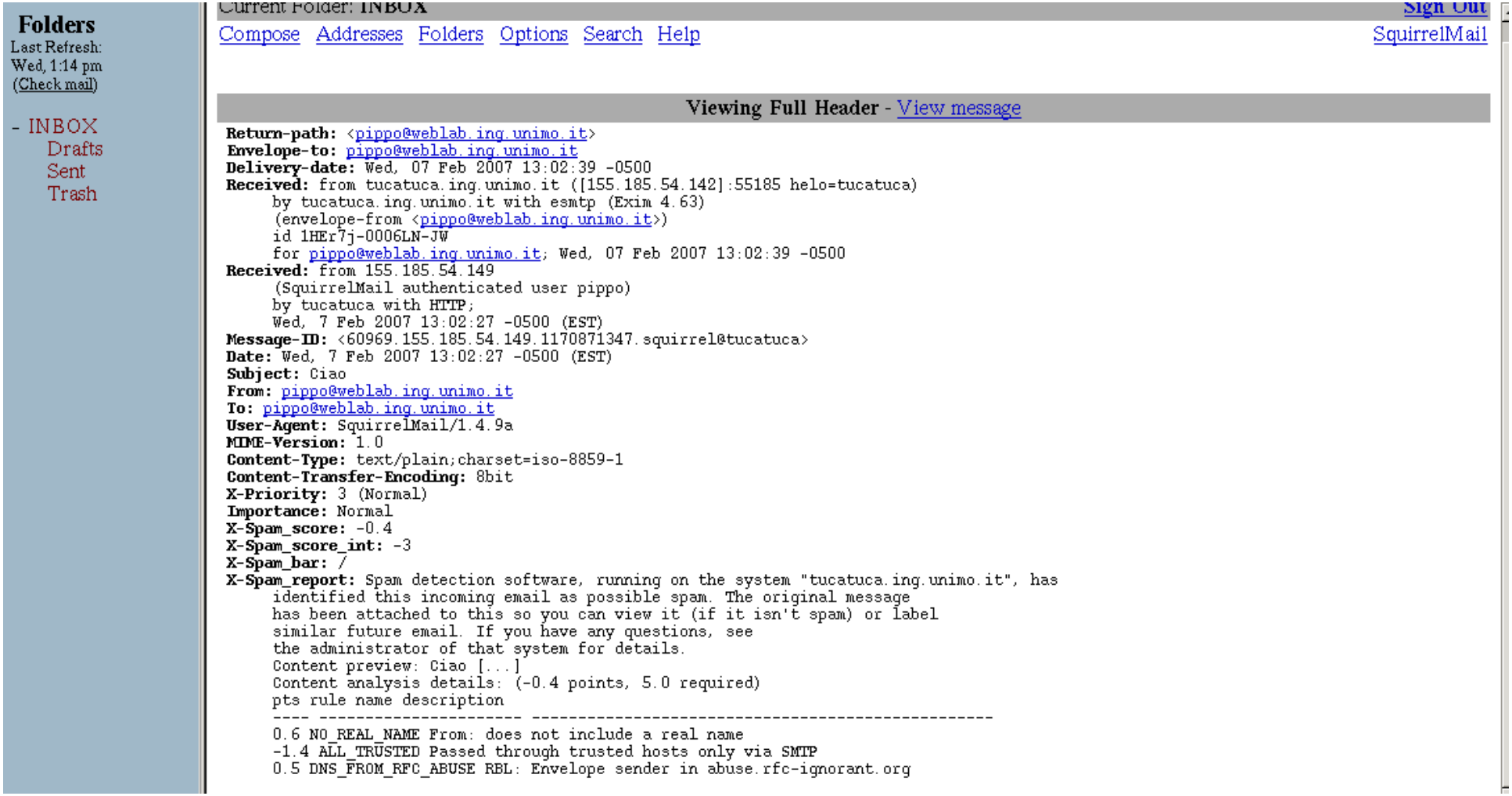
- **Per ulteriori informazioni, vedere la documentazione**

```
$ perldoc Mail::SpamAssassin::Conf
```

Exim e Spamassassin - Installazione e configurazione

- **Configurazione di exim**
  `$ vim exim4.conf.template` **(decommentare la l'opzione `spamd_address` e la parte relativa allo spam di `acl_check_data`)**
  `$ update-exim4.conf`
  `$ /etc/init.d/exim4 restart`

Spamassassin ed Exim – Verifica di funzionamento



Approccio agli antivirus

- **Due approcci alla lotta ai virus:**
  - Single-Vendor
  - Multi-Vendor
- **La maggior parte dei produttori di antivirus commerciali è iscritta al CARO (Computer Antivirus Research Organisation)**
  - condivisione dei sorgenti e delle informazioni
- **Talvolta l'approccio Multi-Vendor è obbligato: supporto per tutte le piattaforme utilizzate**

e-mail Antivirus

- **Quando filtrare la posta elettronica?**
  - Ricezione/invio
    - SMTP
  - Lettura
    - POP3
    - IMAP
- **Antivirus Open Source**
  - Clamav
    http://www.clamav.net
  - OpenAntiVirus
    http://www.openantivirus.org

Clam antivirus

- **Antivirus open source e free**
- **http://www.clamav.net/**
- **Utilizzato da diverse applicazioni come motore antivirus. Tre modalità operative:**
  - libclamav
  - clamscan
  - clamd - clamdscan
- **Update automatico delle rules → freashclam**
- **on-access scanning (Linux e FreeBSD) → clamuko**
- **No clean dei file infetti (solo delete o quarantine)**

Alcune soluzioni basate su ClamAV

- **HTTP**
  - HAVP - http://www.server-side.de/
  - Squid clamav redirector - http://squidclam.sourceforge.net/
  - Dansguardian - http://dansguardian.org/
  - Safesquid - http://dansguardian.org/
    - Standard subscription 50.00$

Alcune soluzioni basate su ClamAV

- **SMTP**
  - Amavisd-new - http://www.ijs.si/software/amavisd/
  - Clamsmtp - http://memberwebs.com/nielsen/software/clamsmtp/
  - Protea AV per Lotus Domino - http://www.proteatools.com/buynow/
    - ClamAV version, Unlimited time, upto 50 user → 99$

Alcune soluzioni basate su ClamAV

- **IMAP**
  - imapproxy - http://www.imapproxy.org/
  - imapfilter - http://imapfilter.hellug.gr
- **POP3**
  - p3scan - http://p3scan.sf.net/
  - pop3.proxy -
  - ClamMail - http://www.bransoft.com/clammail/en/features.html
    “POP3 proxy for small network allow sharing single Internet connection”

ClamAV ed Exim – Installazione e configurazione

- **È necessario compilare Exim con le opzioni per il content scanning**
- **Utilizzando distribuzioni Debian based il pacchetto da installare è exim4-daemon-heavy:**

```
$ apt-get install exim4-daemon-heavy
```

- **Installazione di ClamAV:**

```
$ apt-get install clamav-daemon
$ apt-get install clamav-freshclam
```

ClamAV ed Exim – Installazione e configurazione

- **Controllare che in `/etc/clamav/clamd.conf` sia presente la seguente voce:**
  `AllowSupplementaryGroups`
- **L'utente clamav deve appartenere al gruppo dell'utente con cui gira Exim**
  ```
  $ usermod -G Debian-exim clamav
  ```
- **(Se non esiste,) creare la directory in cui Exim mette le e-mail da analizzare**
  ```
  $ mkdir /var/spool/exim4/scan
  $ chown -R Debian-exim: /var/spool/exim4/scan
  $ chmod -R 750 /var/spool/exim4/scan
  ```

ClamAV ed Exim – Installazione e configurazione

- **Nel file `/etc/exim4/exim4.conf.template` ci sono da configurare due cose:**
  `av_scanner` **(la socket; deve esesre la stessa che è indicata nel file di configurazione di ClamAV)**
  e
  `acl_check_data`
- **Dopo aver modificato il file**

```
$ /etc/init.d/exim4 stop
$ update-exim4.conf
$ /etc/init.d/exim4 start
```

ClamAV ed Exim – Installazione e configurazione

- **Esempio 1**

```
deny
 demime = *
 malware = *
 message = Malware detected ($malware_name).
```

- **Esempio 2**

```
warn
  message = Subject: ****VIRUS DETECTED**** $h_Subject \n\
            X-Virus-Report: Malware detected ($malware_name)
  malware = *
  demime  = *
```

- **La prima configurazione impedisce la ricezione di messaggi contenenti virus mentre la seconda modifica il Suject e inserisce un tag X-Virus-Report negli header**

ClamAV ed Exim – Verifica di funzionamento

Un sistema di Posta Open Source

Riccardo Lancellotti

Green

Blue

Black