



Difesa

Spam-Virus Checking Gateway

Pierpaolo Palazzoli Matteo Valenza 

Grado di difficoltà



In quest'articolo si occuperemo del problema dello spam. La questione ben nota a tutti che usano ogni giorno la posta elettronica. Il problema che irrita ognuno che sta aspettando le notizie importanti e ottiene invece un sacco delle offerte inutili. Spesso con un virus in allegato...

È perfettamente noto a tutti quanto lo spam, in tutte le sue forme, sia un problema ormai estremamente diffuso e fastidioso. Gli strumenti che permettono di arginare questo fenomeno sono numerosissimi e accessibili a chiunque; tipicamente si basano su tecniche di analisi testuale, *blacklist* e modelli statistici

Due strumenti molto potenti che abbiamo a disposizione per contrastare lo spam da una parte e le minacce connesse con i virus dall'altra sono rispettivamente Spamassassin e ClamAV. Bisogna comunque osservare che in molti casi, l'installazione di questi applicativi su un mail server in produzione può rivelarsi piuttosto intrusiva. Un fattore cruciale nella gestione dei sistemi di posta, infatti, è costituito dalla continuità di servizio, di conseguenza è opportuno cercare di limitare gli interventi che possono portare a dei fermi macchina.

Un altro problema a cui si va incontro nella gestione di un mail server riguarda il corretto dimensionamento del sistema, in modo da evitare il rischio di un sovraccarico, con un conseguente degrado delle prestazioni. La causa principale di questo problema è oggi dovuta ai messaggi di posta indesiderati (spam e virus), oltre alle

notevoli risorse assorbite dagli stessi programmi utilizzati per il filtraggio.

Una soluzione a tutti questi problemi si può ottenere introducendo uno *Spam-Virus Checking Gateway* (SVCG), vale a dire un dispositivo dedicato, separato fisicamente dal mail server, demandato alle funzioni di filtraggio e pulizia dei messaggi di posta. Questo dispositivo viene inserito, nella logica di rete nella posizione che occuperebbe un *Gateway*, incaricato di ricevere i messaggi di posta, filtrarli e distribuire i messaggi *sani* ai server incaricati di gestirli.

Dall'articolo imparerai...

- analizzare le problematiche mail,
- configurare un sistema antispam-antivirus,
- personalizzare il sistema in funzione delle proprie esigenze.

Cosa dovresti sapere...

- Configurazione base di un server di posta,
- Basi di Networking,
- Protocolli SMTP e POP3.

In questa configurazione il mail server torna al suo ruolo originale, e non è più necessario nessun intervento sulla sua configurazione per la gestione e manutenzione degli strumenti antivirus/antispam, inoltre l'hardware del sistema potrà essere dimensionato in base ai reali servizi, senza l'esigenza di dover compensare il carico computazionale per il filtraggio della posta indesiderata. Prima di passare alla descrizione della configurazione e dell'inserimento in rete del SVCG, alcuni cenni sulla scelta dell'MTA.

La scelta del pacchetto software da utilizzare non è vincolante, dato che tutti i principali prodotti (Sendmail, Qmail, Postfix, Exim ...) permettono di implementare le funzionalità che verranno di seguito descritte.

L'MTA che verrà descritto in questo articolo è Sendmail. Tale scelta può sembrare discutibile, dato che Sendmail non è certamente il pacchetto più all'avanguardia tra quelli sopra citati, tuttavia presenta dei vantaggi in termini di integrazione con demoni antispam/antivirus. Questa metodologia prende il nome di Militer, e consiste nel ridirezionamento del flusso mail verso dei Socket Unix standard in grado di essere leggibili

da Spamassassin e ClamAV e nel caso specifico di Sendmail è realizzabile in modo estremamente semplice, introducendo poche righe nel file di configurazione (*sendmail.mc*).

Inserimento dell'infrastruttura di RELAY

La prima fase che affrontiamo riguarda l'inserimento dell'SVCG all'interno del contesto di rete già preesistente. Nella Fig. 1 si rappresenta la rete di esempio che verrà di seguito illustrata. Il Mail Gateway va inserito in modo che tutte i messaggi in ingresso siano intercettati prima di poter raggiungere uno dei Mail Server. A questo proposito è necessario che il record MX punti all'indirizzo IP assegnato all' SVCG, o, in alternativa, configurare il router in modo che la porta 25 SMTP venga girata a quest'ultimo che, a sua volta provvederà a consegnare i messaggi processati ai server opportuni. In Sendmail il file di configurazione su cui intervenire a questo scopo è *mailertable* nel Listato 1.

Come si può notare nell'estratto del file di esempio, abbiamo a disposizione gli strumenti per gestire in modo estremamente preciso i flussi di mail, in particolare, nell'esempio, viene detto a Sendmail di ruotare le

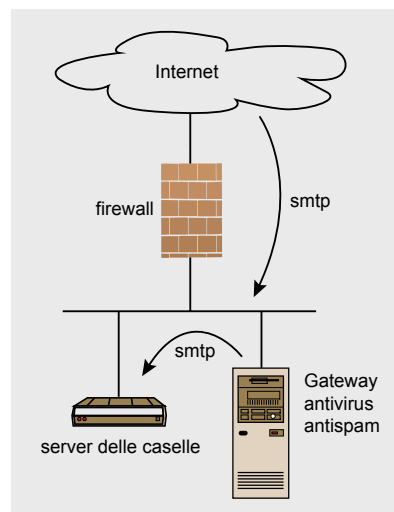


Fig. 1. Lo schema del funzionamento - la rete di esempio

Listato 1. Mailertable, file di configurazione.

```
dominio1.xx esmtp:[192.168.111.25]
dominio2.xx esmtp:[192.168.111.26]
dominio3.xx esmtp:[192.168.111.27]
```

mail dirette al dominio *dominio2.xx* verso l'host 192.168.111.26 con un set di comandi esteso: *esmtp*.

Il file così modificato va ricompilato in *.db* con il seguente comando:

```
makemap hash mailertable.db
< mailertable
```

Generato il file, è necessario che sendmail lo legga in fase di elaborazione della mail. È sufficiente aggiungere nel file di configurazione *sendmail.mc* la riga:

```
FEATURE(`mailertable', `hash
-o /etc/mail/mailertable.db')dn1
```

Nella Figura 1, possiamo osservare una rappresentazione della tipologia di rete descritta. Lo SVCG è il primo a ricevere la connessione SMTP, quindi la mail viene presa in carico dal suo MTA e può essere processata da parte di qualsiasi demone integrabile a Sendmail. Nel nostro caso i demoni in questione sono Clamav e Spamassassin che tramite i pacchetti clamav-milter e spamass-milter possono essere integrati nativamente.

Listato 2. Clamav-milter options, file di configurazione

```
--config-file=/etc/clamd.conf
--max-children=25
--force-scan
--quiet
--dont-log-clean
--noreject
--external
-obl local:/var/run/clamav/clamd.sock
CLAMAV_USER='clamav'
```

Cenni sugli autori

Il Progetto Snortattack come si legge nel sito è un SUG (Snort User Group) è finalizzato alla stesura di documentazione per l'installazione e configurazione di Snort. Inoltre scrive script per automatizzare l'installazione di Snort in modalità inline. Alla base del progetto esiste un concetto univoco: "Comunicazione Informazione Conoscenza", per tutti quindi, la possibilità di attingere, aggiungere e condividere tutto ciò che viene pubblicato. Snortattack.org, risultato della fusione di conoscenze e collaborazione tra Matteo e Pierpaolo. Compare in internet circa sei mesi fa ma nasce nella mente del Team circa due anni orsono. Punto di forza sono guide e script per l'installazione di Snort in Italiano e Inglese, forum e mailinglist.



Preparazione e Dimensionamento dello SVCG

È fondamentale la corretta scelta dell'hardware sul quale verrà installa-

to Linux. La scelta della distribuzione è soggettiva; tutti i pacchetti necessari sono disponibili sia in formato pacchettizzato per Debian e Fedora, che in formato sorgente.

La macchina deve avere un corretto dimensionamento soprattutto dal punto di vista della RAM. Una stima approssimativa, ma comunque attendibile richiede 1 GB ogni

Listato 3. Piccola parte Sendmail.mc, file di configurazione

```
define(`confMILTER_MACROS_CONNECT', `b, j, _, {daemon_name}, {if_name}, {if_addr}')dnl

INPUT_MAIL_FILTER(`clamav', `S=local:/var/run/clamav/clamd.sock, F=T=S:4m;R:4m')dnl

INPUT_MAIL_FILTER(`spamassassin', `S=local:/var/run/spamass-milter/spamass-milter.sock, F=T=C:15m;S:4m;R:4m;E:10m')dnl

define(`confINPUT_MAIL_FILTERS', `spamassassin,clamav')dnl
```

Listato 4. Sendmail.mc completo, file di configurazione

```
include(`/usr/share/sendmail-cf/m4/cf.m4')
VERSIONID(`linux ')dnl
OSTYPE(`linux')
define(`confDEF_USER_ID', `8:12')dnl
undefine(`UUCP_RELAY')dnl
undefine(`BITNET_RELAY')dnl
dnl define(`confAUTO_REBUILD')dnl Parametro per auto rigenerare il Sendmail.cf
define(`confTO_CONNECT', `1m')dnl
define(`confTRY_NULL_MX_LIST', true)dnl
define(`confDONT_PROBE_INTERFACES', true)dnl
define(`PROCMAIL_MAILER_PATH', `/usr/bin/procmail')dnl
define(`ALIAS_FILE', `/etc/aliases')dnl
define(`STATUS_FILE', `/etc/mail/statistics')dnl Scrittura su un file di testo delle statistiche dell'MTA
define(`UUCP_MAILER_MAX', `2000000')dnl
define(`confUSERDB_SPEC', `/etc/mail/userdb.db')dnl
define(`confPRIVACY_FLAGS', `authwarnings,novrfy,noexpn,restrictqrun')dnl
define(`confTO_IDENT', `0s')dnl Velocità 0 secondi nel rispondere sulla porta 25 SMTP
define(`confTO_QUEUEWARN', `4h')dnl Ore di coda dopo le quali mandare un warning
define(`confTO_QUEUERETURN', `3d')dnl Giorni massimi di coda
define(`confMAX_DAEMON_CHILDREN', `60')dnl Massimo dei processi figli
define(`confMAX_CONNECTION_RATE_THROTTLE', `20')dnl
define(`confMAX_MESSAGE_SIZE', `2000000')dnl Massima dimensione processabile di mail in byte
FEATURE(`no_default_msa', `dnl')dnl
FEATURE(`smrsh', `/usr/sbin/smrsh')dnl
FEATURE(`mailertable', `hash -o /etc/mail/mailertable.db')dnl Lettura del file di routing mail
FEATURE(`virtusertable', `hash -o /etc/mail/virtusertable.db')dnl
FEATURE(redirect)dnl
FEATURE(always_add_domain)dnl
FEATURE(use_cw_file)dnl
FEATURE(relay_entire_domain)dnl
FEATURE(use_ct_file)dnl
FEATURE(`access_db', `hash -o /etc/mail/access.db')dnl Lettura del file di relay
FEATURE(local_procmail, `', `procmail -t -Y -a $h -d $u')dnl
FEATURE(`blacklist_recipients')dnl
FEATURE(`use_cw_file')dnl
EXPOSED_USER(`root')dnl
FEATURE(`accept_unresolvable_domains')dnl
MAILER(smtp)dnl
MAILER(procmail)dnl
Cwlocalhost.localdomain
define(`confSEPARATE_PROC', `True')dnl
define(`confDEF_USER_ID', `8:12')dnl
define(`confMILTER_MACROS_CONNECT', `b, j, _, {daemon_name}, {if_name}, {if_addr}')dnl
INPUT_MAIL_FILTER(`clamav', `S=local:/var/run/clamav/clamd.sock, F=T=S:4m;R:4m')dnl
INPUT_MAIL_FILTER(`spamassassin', `S=local:/var/run/spamass-milter/spamass-milter.sock, F=T=C:15m;S:4m;R:4m;E:10m')dnl
define(`confINPUT_MAIL_FILTERS', `spamassassin,clamav')dnl Connessione ai milter
```

150 domini di 20 caselle ognuno. Per una corretta gestione di grossi banchi di Ram è più performante la scelta di un processore a 64 bit. Lo spazio disco può essere contenuto (30 GB) nel caso si scelga una configurazione RAID (RAID 1 per avere vantaggi in velocità di scrittura).

Per evitare che i servizi utilizzino le risorse in modo non corretto è necessario reperire ulteriori informazioni relativamente al traffico di messaggi che la macchina dovrà gestire. In particolare è opportuno conoscere, oltre al numero di domini e di caselle di posta, il numero di sessioni TCP

contemporanee, il numero di mail in transito al giorno, il traffico sulla scheda di rete del server. Se tali informazioni non sono disponibili in fase di installazione, potranno essere raccolte in seguito (potrebbe essere utile installare un demone per il protocollo snmp) e affinare di conseguenza la configurazione. Prerequisito indispensabile è che Sendmail abbia il supporto ai milter.

I pacchetti spamass-milter e clamav-milter sono degli eseguibili configurabili sia da linea di comando che da file di configurazione, se inclusi nei file init come nel Listato 2.

In questo esempio è stata operata la scelta di usare il milter appoggiandosi al motore antivirus di clamav. Quest'opzione è attivata dal parametro `--external`. In alternativa è possibile utilizzare le libclamav direttamente.

Ora che il sistema è configurato in modo tale che clamav prenda in carico le email, bisogna definire verso quale socket vanno indirizzate. Un parametro da non sottovalutare è costituito dal numero massimo di processi figli: se non dimensionato correttamente potrebbe arrivare a causare un *crash* dell'applicazione.

Per quanto riguarda invece spamass-milter, utilizziamo l'opzione `-m` che permette di non modificare il messaggio e `-r` per definire il livello di spam per il quale le mail vanno direttamente cestinate.

```
spamass-milter -p /path/to/socket -P
/path/to/pidfile -m -r 5
```

A questo punto sorge un problema: nell'eventualità in cui uno dei due milter dovesse andare in *crash*, il flusso di email si bloccherebbe. Per evitare questo disservizio esiste un programma di nome *milter_watch* in grado di monitorare lo stato dei milter e lanciare un comando per ripristinare il servizio.

```
milter_watch -q local:/var/milter.sock
&& /etc/init.d/milter restart
```

Una volta configurati i milter possiamo inserire in *Sendmail.mc* le righe del Listato 3, per comunicare a Sen-

Listato 5. Local.cf, file di configurazione

```
required_hits 5.0
defang_mime 1
report_header 1
ok_languages all
ok_locales all
use_hashcash 1
auto_learn 1
use_bayes 1
bayes_auto_learn 1
use_auto_whitelist 0
bayes_auto_learn_threshold_nonspam 0.2
bayes_auto_learn_threshold_spam 8.0
pyzor_options --homedir /etc/mail/spamassassin
```

Listato 6. Clamav.conf, file di configurazione

```
LogFile /var/log/clamav/clamd.log
LogFileUnlock
LogFileMaxSize 0
LogTime
LogSyslog
PidFile /var/run/clamav/clamd.pid
TemporaryDirectory /var/tmp
DatabaseDirectory /var/lib/clamav
LocalSocket /var/run/clamav/clamav.sock
FixStaleSocket
MaxConnectionQueueLength 30
MaxThreads 30
ReadTimeout 300
IdleTimeout 15
User clamav
ScanMail
MailFollowURLs
ScanArchive
ScanRAR
ArchiveMaxFileSize 25M
ArchiveMaxFiles 1500
```

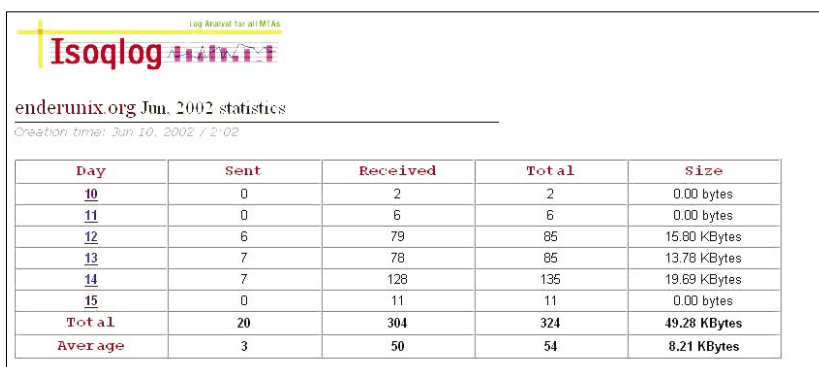


Fig. 2. Le statistiche

Listato 7a. *Mrtg.conf*, file di configurazione

```
# $Id: mrtg.cfg,v 1.2 2000/11/27 19:16:30 rowan Exp $
#####
# Mail server stats
#
# gather statistics on the local machine
# count bytes transferred instead of messages
#
workdir: /var/www/html/mrtg/
LoadMIBs: /usr/share/snmp/mibs/UCD-SNMP-MIB.txt,/usr/share/snmp/mibs/TCP-
        MIB.txt

Target[syn.mail]: `/usr/bin/mrtg-mailstats`
Options[syn.mail]: nopercent,noinfo,perhour
Background[syn.mail]: #738AA6
WithPeak[syn.mail]: my
Title[syn.mail]: (Nome host) Mail processed - messages per hour
PageTop[syn.mail]: <h1>(Nome host) Mail processed - messages
per hour</h1>
MaxBytes[syn.mail]: 10000000
YLegend[syn.mail]: msgs/h
ShortLegend[syn.mail]: msgs/h
LegendI[syn.mail]: &nbsp;Mail in:
LegendO[syn.mail]: &nbsp;Mail out:
Legend1[syn.mail]: Mail processed per hour, input messages
Legend2[syn.mail]: Mail processed per hour, output messages
# CPU Monitoring
# (Scaled so that the sum of all three values doesn't exceed 100)
Target[server.cpu]:ssCpuRawUser.0&ssCpuRawUser.0:community@localhost +
ssCpuRawSystem.0&ssCpuRawSystem.0:community@localhost +
ssCpuRawNice.0&ssCpuRawNice.0:community@localhost
Title[server.cpu]:Server CPU Load
MaxBytes[server.cpu]: 100
ShortLegend[server.cpu]: %
YLegend[server.cpu]: CPU Utilization
Legend1[server.cpu]: Current CPU percentage load
LegendI[server.cpu]: Used
LegendO[server.cpu]:
Options[server.cpu]: growright,nopercent
Unscaled[server.cpu]: ymwd

# Memory Monitoring (Total Versus Available Memory)
Target[server.memory]:memAvailReal.0&memTotalReal.0:community@localhost
Title[server.memory]: Free Memory
PageTop[server.memory]: <H1>Free Memory</H1>
MaxBytes[server.memory]: 100000000000
ShortLegend[server.memory]: B
YLegend[server.memory]: Bytes
LegendI[server.memory]: Free
LegendO[server.memory]: Total
Legend1[server.memory]: Free memory, not including swap, in bytes
Legend2[server.memory]: Total memory
Options[server.memory]: gauge,growright,nopercent
kMG[server.memory]: k,M,G,T,P,X
# Memory Monitoring (Percentage usage)
Title[server.mempercent]: Percentage Free Memory
PageTop[server.mempercent]:<H1>Percentage Free Memory</H1>
Target[server.mempercent]:(
memAvailReal.0&memAvailReal.0:community@localhost ) * 100 / (
memTotalReal.0&memTotalReal.0:community@localhost )
options[server.mempercent]: growright,gauge,transparent,nopercent
Unscaled[server.mempercent]: ymwd
MaxBytes[server.mempercent]: 100
YLegend[server.mempercent]: Memory %
```

dmail dove reperirli. I path dei socket devono essere necessariamente gli stessi definiti nelle opzioni di esecuzione dei due milter.

Una regola da prevedere dopo l'inserimento di qualsiasi riga nel *sendmail.mc* è la ri-esecuzione dell'*m4* per la creazione del file *sendmail.cf*. Nelle versioni più recenti di Sendmail viene fatta ad ogni riavvio del demone.

Personalizzazione dei file di configurazione

I file di configurazione da impostare con maggior attenzione sono di sicuro: *local.cf* (spamasassin), *clamav.conf* e *Sendmail.mc*. Questi tre file permettono di decidere se effettuare il tagging o procedere all'eliminazione delle email processate.

Iniziando da *Sendmail.mc* (Listato 4) si spiegheranno alcuni dei parametri più significativi per ottenere le maggiori *performance* e la massima precisione nell'individuazione delle email indesiderate.

Quando si personalizza il file di configurazione di Sendmail è bene privilegiare la velocità di elaborazione, al fine di rendere per quanto possibile trasparente la presenza del SVCG. Uno dei parametri che incide maggiormente sulla velocità di elaborazione sia per quanto riguarda ClamAV, sia Spamasassin è la massima dimensione del messaggio. Nell'esempio si è fatto riferimento ad un valore di 20 MB.

Il file di configurazione principale per spamasassin è *local.cf*, che si trova tipicamente in */etc/mail/spamasassin/* (Listato 5) ed è caratterizzato da delle direttive basate su valori booleani. Il livello di soglia è definito come la sommatoria dei riscontri testuali avvenuti sulla email in esame. Il valore deve essere pesato da un parametro di check. È possibile attivare filtri baesiani, pyzor, hashash, blacklist e molto altro. L'analisi bayesiana è indispensabile per avere un riscontro quasi immediato su cambiamenti repentini di flussi email. Importante configurare correttamente anche autolearn per renderlo efficace: l'utilizzo di soglie troppo lontane o troppo vicine al required hits porterebbe a dei falsi negativi o falsi positivi.

Il principio di funzionamento *hashcash* sarà spiegato successivamente.

L'analisi è effettuata su tutte le lingue e i locale. Mai sottovalutare le opzioni di esecuzione di spamassas-

sin che incidono in modo sostanziale sulla RAM utilizzata:

```
spamd -d -c -m50 -H -r /var/run/
spamd.pid
```

Listato 7b. *Mrtg.conf*, file di configurazione

```
ShortLegend[server.mempercent]: Percent
LegendI[server.mempercent]: Free
LegendO[server.mempercent]: Free
Legend1[server.mempercent]: Percentage Free Memory
Legend2[server.mempercent]: Percentage Free Memory

# New TCP Connection Monitoring (per minute)
Target[server.newconns]:tcpPassiveOpens.0&tcpActiveOpens.0:
                        community@localhost
Title[server.newconns]: Newly Created TCP Connections
PageTop[server.newconns]: <H1>New TCP Connections</H1>
MaxBytes[server.newconns]: 10000000000
ShortLegend[server.newconns]: c/s
YLegend[server.newconns]: Conns / Min
LegendI[server.newconns]: In
LegendO[server.newconns]: Out
Legend1[server.newconns]: New inbound connections
Legend2[server.newconns]: New outbound connections
Options[server.newconns]: growright,nopercent,perminute

# Established TCP Connections
Target[server.estabcons]:tcpCurrEstab.0&tcpCurrEstab.0:community@localhost
Title[server.estabcons]: Currently Established TCP Connections
PageTop[server.estabcons]: <H1>Established TCP Connections</H1>
MaxBytes[server.estabcons]: 10000000000
ShortLegend[server.estabcons]:
YLegend[server.estabcons]: Connections
LegendI[server.estabcons]: In
LegendO[server.estabcons]:
Legend1[server.estabcons]: Established connections
Legend2[server.estabcons]:
Options[server.estabcons]: growright,nopercent,gauge
```

Il valore dopo il parametro *-m* definisce il numero massimo di processi contemporanei.

Il file di configurazione del clamav è *clamav.conf*, reperibile tipicamente in */etc/*. Contiene note direttive cruciali, il path del socket è una di queste: deve essere assolutamente diverso da quello dichiarato da *clamav-milter*.

La dimensione massima di un archivio e il numero massimo dei file per archivio sono dei valori da ponderare correttamente in funzione della ram del sistema. Come anticipato, nel nostro esempio si ipotizzano 2 GB di RAM (25 MB con 1500 file).

All'interno dei file descritti in precedenza esistono dei parametri che non configurati correttamente possono compromettere le prestazioni in modo sostanziale.

Di seguito uno schema con i parametri più importanti da utilizzare per un'applicazione come quella trattata.

Sendmail.mc: `define('confTO_QUEUEUERETURN', `3d')dnl` incide molto sulla lunghezza della coda.

Spamassassin: `spamd -m50` ... incide molto sulla RAM.

Clamav-milter: `--max-children=25` incide sulla velocità di processo in funzione della CPU del server.

Clamav.conf: `MaxThreads 30` numero massimo di threads :RAM e CPU.

Questi parametri per essere configurati opportunamente devono essere integrati da sistemi di monitoraggio. La maggior parte di questi sistemi si basano sul protocollo SNMP, quindi è necessario configurare e installare sull'antispam antivirus gateway il pacchetto *net-snmp*.

Un ottimo e largamente conosciuto programma di monitoraggio è mrtg, che offre anche il vantaggio di poter accettare come sorgente oltre a snmp, anche il file statistics (tramite il pacchetto *mrtg-mailstats*) di sendmail.

Nei listati successivi sono presentati i file per mrtg che permettono

Mail Statistics for the ISG.EE Mail Server

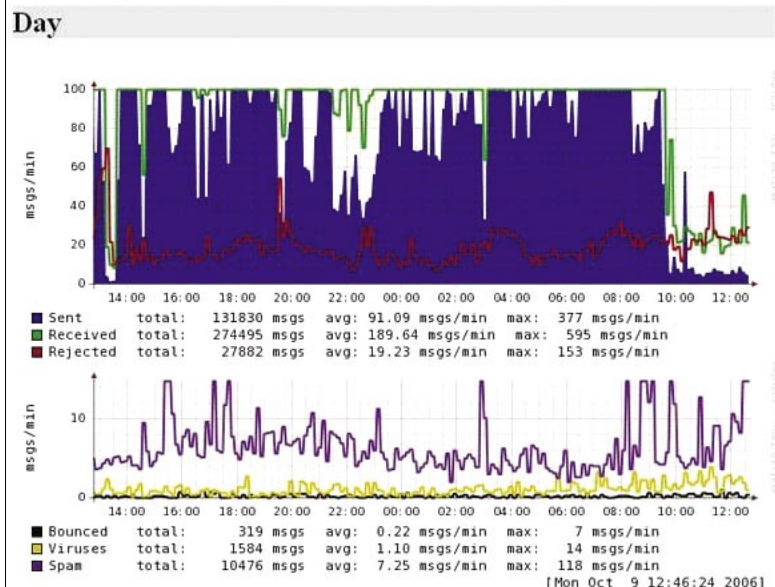


Fig. 3a. Le statistiche delle mail per l'ISG.EE Mail Server: giorno

Listato 8a. Local.cf seconda parte, file di configurazione

```
score AS_SEEN_ON 0.393 0.320 0.613 0.613
score BAD_CREDIT 1.161 1.161 0.817 0.817
score BANG_GUAR 0.297 0.297 0.254 0.254
score BANG_MORE 0.287 0.287 0.294 0.294
score BAYES_00 0 0 -1.665 -1.665 Pesi baesiani
score BAYES_05 0 0 -0.925 -0.925 Pesi baesiani
score BAYES_20 0 0 -0.730 -0.730 Pesi baesiani
score BAYES_40 0 0 -0.276 -0.276 Pesi baesiani
score BAYES_50 0 0 1.724 1.724 Pesi baesiani
score BAYES_60 0 0 4.02 4.02 Pesi baesiani
```

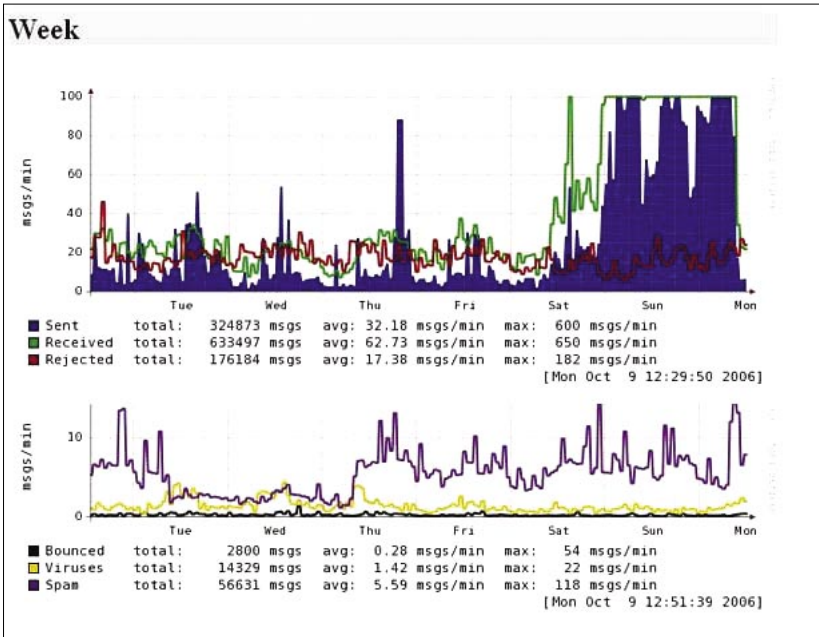


Fig. 3b. Le statistiche delle mail per l'ISG.EE Mail Server: settimana

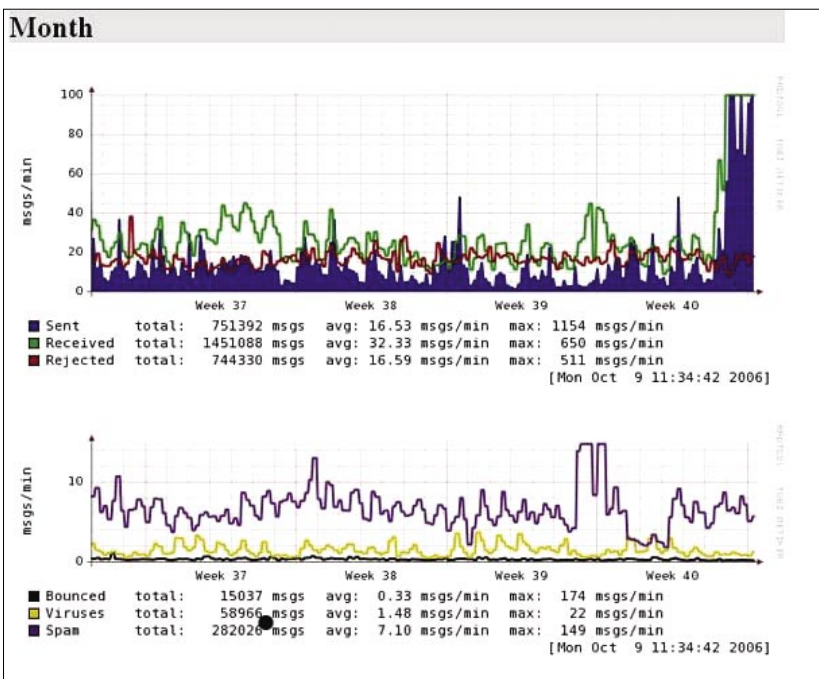


Fig. 3c. Le statistiche delle mail per l'ISG.EE Mail Server: mese

di visualizzare statistiche sul numero di messaggi ogni ora e sulle connessioni contemporanee.

Il file di configurazione è necessario per reperire informazioni sull'utilizzo delle risorse del server, quindi poter aggiustare i parametri.

Leggendo i file di configurazione si può osservare che i parametri monitorati sono quelli tipici di un server di posta.

Altri strumenti di monitoraggio utili sono: Isoqlog e Mailgraph.

Questi strumenti sono specifici per server di posta. Nelle Figure 3, 4 e 5 sono riportati alcuni screenshot. Il primo esempio visualizza i dati di transito mail organizzato per domini e temporalmente. Il secondo pacchetto visualizza graficamente, tramite rrdtool, il passaggio di messaggi divisi in: mail, spam e virus.

Anche questi componenti vanno configurati in base all'MTA che si utilizza.

I file di configurazione principali per ogni pacchetto sono : *isoqlog.conf*, *isoqlog.domains* per *isoqlog*. Per mailgraph è sufficiente eseguire `/usr/bin/perl -w /root/mailgraph-1.12/mailgraph.pl -l /var/log/maillog`.

Il frontend Isoqlog è formato da pagine in PHP, mentre mailgraph è un cgi.

Taratura dei Livelli di soglia

In questa fase si può procedere, innanzitutto, alla configurazione dei filtri bayesiani. I file di configurazione sono:

```
use_bayes 1
bayes_auto_learn 1
use_auto_whitelist 0
bayes_auto_learn_threshold
_nonspam 0.2
bayes_auto_learn_threshold
_spam 8.0
```

La funzionalità di auto-learn deve essere impostata con un limite inferiore e uno superiore: il sistema acquisisce esperienza su come classificare lo spam.

Spamassassin oltre alle funzionalità standard da la possibilità di personalizzare il file di configurazione con funzioni molto avanzate. Nella sezione

del listato, è possibile notare come si possano modificare i pesi dell'analisi dei contenuti, ciò permette di orientare il filtro verso la tipologia di spam da cui si è maggiormente afflitti.

Queste scelte influiscono pesantemente nel calcolo bayesiano,

per cui il meccanismo dei pesi va gestito con attenzioni: tutto deve essere visto in funzione del limite configurato in spamass-milter, che è quel valore oltre il quale vengono cancellate automaticamente le mail.

Listato 8b. Local.cf seconda parte, file di configurazione

```
score BAYES_80 0 0 4.32 4.32 Pesi baesiani
score BAYES_95 0 0 4.98 4.98 Pesi baesiani
score BAYES_99 0 0 5.54 5.54 Pesi baesiani
score BEST_PORN 0.566 0.263 0.263 0.263
score BLANK_LINES_80_90 0.046 0.046 0.216 0.216
score BODY_ENHANCEMENT 0.151 0.481 2.500 2.500
score BODY_ENHANCEMENT2 0.814 0.845 3.000 3.000
score CUM_SHOT 4.000 4.000 4.000 4.000
score DEAR_FRIEND 0.542 0.766 1.288 1.288
score DIET_1 0.671 0.365 0.274 0.274
score DISGUISE_PORN 1.490 1.835 0.798 0.798
score DNS_FROM_RFC_ABUSE 0 0.374 0 0.374
score DRUGS_ANXIETY 2.823 0.205 0.205 0.205
score DRUGS_ANXIETY_EREC 0.024 0.038 0.524 0.538
score DRUGS_DIET 0.771 0.415 0.771 0.415
score DRUGS_DIET_OBFU 2.345 2.345 2.704 2.748
score DRUGS_ERECTILE 1.250 1.250 2.250 2.250
score DRUGS_ERECTILE_OBFU 2.090 2.090 3.390 3.390
score DRUGS_MANYKINDS 0.031 2.734 0.031 2.734
score DRUGS_MUSCLE 0.001 0.169 0.001 0.169
score DRUGS_PAIN 2.871 2.871 1.358 1.358
score DRUGS_SLEEP 0.320 0.107 0.053 0.053
score FREE_PORN 0.794 0.794 1.937 1.937
score FROM_ENDS_IN_NUMS 0.177 0.516 0.517 0.517
score FROM_HAS_MIXED_NUMS 0.107 0.298 0.024 0.024
score FROM_NONSENDING_DOMAIN 1.486 1.486 1.678 1.678
score FROM_STARTS_WITH_NUMS 1.218 1.492 1.441 1.441
score GUARANTEED_100_PERCENT 0.615 0.435 0.669 0.669
score GUARANTEED_STUFF 0.100 0.238 0.403 0.403
score HARDCORE_PORN 1.520 1.520 1.850 1.850
score LIVE_PORN 0.040 0.360 1.000 1.000
score MIME_QP_LONG_LINE 0 0.000 0.105 0.105
score MISSING_MIMEOLE 0.068 0 0 0.100
score MORTGAGE_BEST 0.948 0.923 4.000 4.000
score MORTGAGE_PITCH 0.297 0 3.465 3.465
score MORTGAGE_RATES 0 0.689 0.700 0.700
score NIGERIAN_BODY2 2.400 0.489 2.400 2.400
score NIGERIAN_BODY3 1.395 1.931 2.273 2.273
score NIGERIAN_SUBJECT1 0 0 0.270 0.270
score NO_REAL_NAME 0.124 0.178 0.336 0.336
score NONSECURED_CREDIT 0 0 1.074 1.074
score ONLINE_PHARMACY 2.730 0 2.895 2.895
score OPTING_OUT_CAPS 0.067 0.026 0.483 0.483
score ORDER_REPORT 0 0 1.230 1.230
score PORN_16 0.907 0.462 1.305 1.305
score PORN_CEBELBRITY 0.675 1.569 1.569 1.569
score PORN_URL_SEX 5.865 5.427 5.817 5.817
score PORN_URL_SLUT 1.941 2.022 2.022 2.022
score RCVD_ILLEGAL_IP 1.335 1.370 1.588 1.588
score SOMETHING_FOR_ADULTS 1.433 1.513 1.614 1.614
score SUBJECT_DRUG_GAP_C 1.993 1.917 2.501 2.501
score SUBJECT_DRUG_GAP_VIA 2.659 1.770 3.158 3.158
score SUBJ_AS_SEEN 0.995 1.691 1.214 1.214
score SUBJ_BUY 0.565 0.490 0.414 0.414
score SUBJ_YOUR_OWN 0.872 1.294 1.371 1.371
```

REKLAMA



La tecnologia *HashCash* permette di legittimare le email che non sono spam. Maggiore è il *valore* del francobollo inserito nell'header, maggiore è il tempo di elaborazione che è stato impiegato per inviare il messaggio che quindi, verosimilmente, non sarà spam: uno spammer, tipicamente, invia un numero elevato di messaggi in tempi brevi.

Per abilitare questa funzionalità è sufficiente inserire nel file *local.cf*:

```
use _hashcash 1.
```

Tutte queste opzioni concorrono nella sommatoria del punteggio assegnato ad una mail. Il punteggio, come spiegato, permette a spamass-milter di decidere quali mail debbano essere eliminate automaticamente. Nella prima fase però deve essere fatto un *popolamento baesiano*, che significa che il sistema deve auto istruirsi per un certo periodo di tempo.

Può essere utilizzato *isoqlog* per quantificare il numero di mail transitate, perciò raggiunto un numero proporzionale al numero domini configurati (tipicamente 1000 per dominio) si può attivare in spamass-milter l'eliminazione diretta delle mail. Di sicuro è possibile incorrere sia in falsi positivi che falsi negativi. Per risolverli immediatamente è possibile utilizzare le direttive *whitelist* e *blacklist*, che identificano immediatamente se la mail proveniente o destinata ad un indirizzo o dominio è spam (*black*) o no (*white*).

Ecco le direttive da inserire nel file di configurazione: *whitelist_from good@example.com blacklist_from bad@example.com*

L'indirizzo da *good@example.com* verrà sempre accettato e *bad@example.com* sarà sempre eliminato.

Conclusioni

Per combattere la posta indesiderata è necessario oltre che la tecnica, l'analisi. Bisogna imparare ad analizzare i report dati dagli strumenti di monitoraggio. Questo vi farà capire quanto sia importante dimensionare bene tutti i parametri.

Vi consiglio di aprire un account su domini comuni, in modo da avere idea di che tipo di spam circola.

Questo esempio di approccio allo spam è solo un esempio, esistono centinaia di soluzioni: open source

e commerciali. Quello che conta è il tecnico che amministra l'antispam antivirus gateway. ●

Listato 8c. Local.cf seconda parte, file di configurazione

```
score TO_NO_USER 0.332 0.116 1.615 1.615
score WORK_AT_HOME 0 0 0.325 0.325
score MICROSOFT_EXECUTABLE 2.100
score DATE_IN_FUTURE_03_06 0.1
score DATE_IN_FUTURE_06_12 0.2
score DATE_IN_FUTURE_12_24 0.3
score DATE_IN_FUTURE_24_48 0.4
score DATE_IN_FUTURE_48_96 1.0
score DATE_IN_PAST_03_06 0.1
score DATE_IN_PAST_06_12 0.2
score DATE_IN_PAST_12_24 0.3
score DATE_IN_PAST_24_48 0.4
score DATE_IN_PAST_48_96 1.0
score BIZ_TLD 1.000 1.000 1.000 0.800
score BigEvilList_RX 2.500 3.200 3 1.400
score MORTGAGE_PITCH 2.500 3.200 0 1.400
score MORTGAGE_BEST 2.500 3.200 0 1.400
score SAVE_UP_TO 1.000 1.000 1 1
score SAVINGS 0.990 0.990 0.990 0.990
score SAVE_THOUSANDS 3.800 3.000 1.400 3.400
score BANG_GUARANTEE 2.100 2.100 1.800 1.800
score BANG_BOSS 2.100 2.100 1.800 1.800
score BANG_MONEY 2.100 2.100 1.800 1.800
score URI_OFFERS 2.800 2.800 2.400 2.400
score SUB_FREE_OFFER 1.800 2.000 1.400 2.400
score DRUGS_ERECTILE 2.400 2.800 3.400 3.400
score DRUGS_ANXIETY 2.400 2.800 3.400 3.400
score DRUGS_SLEEP 2.400 2.800 3.400 3.400
score DRUGS_DEPRESSION 2.400 2.800 3.400 3.400
score CASHCASHCASH 2.400 2.800 3.400 3.400
score ORDER_NOW 2.400 2.800 3.400 3.400
score LIMITED_TIME_ONLY 1.800 2.000 3.400 3.400
score AP_CONSUMMATE 0.900 0.800 1.200 1.500
score BAD_CREDIT 2.400 0.800 1.000 0.800
score CLICK_BELOW 3.000 3.000 3.000 3.000
score REMOVE_PAGE 1.500 1.500 1.500 1.500
score FREE_CONSULTATION 3.100 2.400 1.000 1.400
score FORGED_HOTMAIL_RCVD 2.800 2.800 2.600 2.600
score FORGED_HOTMAIL_RCVD2 2.800 2.800 2.600 2.600
score FORGED_YAHOO_RCVD 2.800 2.800 2.600 2.600
score FORGED_YAHOO_RCVD_SMTP 2.800 2.800 2.600 2.600
score NO_REAL_NAME 0.800 0.800 0.600 0.600
score UNPARSEABLE_RELAY 3.800 3.000 1.400 3.400
score URIBL_JP_SURBL 3.800 3.000 1.400 3.400
score USER_IN_WHITELIST_TO -50.000 -50.000 -50.000 -50.000
```

In rete

- <http://www.sendmail.org/>
- <http://savannah.nongnu.org/projects/spamass-milt/>
- <http://www.clamav.net/doc/0.80/html/node19.html>
- <http://www.clamav.net/>
- <http://spamassassin.apache.org/>
- <http://people.ee.ethz.ch/~dws/software/mailgraph/>
- <http://oss.oetiker.ch/mrtg/>
- <http://www.enderunix.org/isoqlog/>
- <http://www.hashcash.org/>
- http://en.wikipedia.org/wiki/Bayesian_filter