Implementazione di un server di posta completo basato su postfix

Alberto Cammozzo mmzz -at- pluto.it

18 maggio 2005

serate a tema PLUTO Padova

Sistema Mail

Mail transfer Agent:
riceve,spedisce e inoltra (forward) la posta fra sistemi diversi, di solito con il protocollo **SMTP** (Simple Mail transfer Protocol)
postfix, sendmail, qmail, exim, nullmailer, ssmtp

Mail delivery agent:

consegna la posta all'interno di un sistema
maildrop, procmail, deliver, sendmail

Mail user agent:

permette all'utente di leggersi la posta
mutt, pine, kmail, mozilla thunderbird...

Sistema mail - II

- **Antivirus:** amavisd, clamav
- **AntiSPAM**: spamassassin, spamcop, spamoracle
- **Analisi dei log**: isoqlog, anteater
- **Grafichetti**: couriergraph, mailgraph
- **Webmail**: squirrelmail, imp4
- **IMAP, POP**: courier, bincimap, cyrus, uw-imapd
- **forwarder/retriever**: perdition, fetchmail, getmail4

Sistema Mail III

- DNS: bind (gestione record MX)
- Firewall e proxy
- Syslog: centralizzare i log della posta, antivirus, per analizzarli

/etc/postfix/main.cf base

- Che nome dominio dare alla **posta in uscita**

```
myorigin = $mydomain
```

- Per quali domini **ricevere**

```
mydestination = $myhostname localhost $mydomain
```

- Da quali intefacce (eth0, eth1, ppp0, ...)

```
inet_interfaces = all
```

- Verso chi inoltrare

```
relay_domains = $mydestination
relay_domains =
```

- Da quali IP

```
mynetworks = 127.0.0.0/8 168.100.189.2/32
```

- Metodo di consegna

```
relayhost =    (default: direct delivery to Internet)
relayhost = $mydomain          (deliver via local mailhub)
relayhost = [mail.$mydomain]   (deliver via local mailhub)
relayhost = [mail.isp.tld]     (deliver via provider mailhub)
```

Esempi: Solo posta locale

```
mynetworks_style = host
relay_domains =
```

Esempi: solo spedizione (null client)

```
myorigin = $mydomain
relayhost = $mydomain
inet_interfaces = 127.0.0.1
local_transport = error:local delivery is disabled
```

Esempi: host PPP

```
relayhost = smtp.ISP.TLD
defer_transports = smtp
disable_dns_lookups = yes
```

E in aggiunta lo script

```
#!/bin/sh
# Start mail deliveries.
/usr/sbin/sendmail -q
# Allow deliveries to start.
sleep 10
# Loop until all messages have been tried at least once.
while mailq | grep '^[^ ]*\*' >/dev/null
do
    sleep 10
done
```

Esempi: rete locale

Client example.com

```
myorigin = $mydomain
mynetworks = 127.0.0.0/8 10.0.0.0/24
relay_domains =
relayhost = $mydomain
```

Server mailhost.example.com

```
myorigin = $mydomain
mydestination = $myhostname localhost.$mydomain localhost \
 $mydomain
mynetworks = 127.0.0.0/8 10.0.0.0/24
relay_domains =
relayhost = [firewall.example.com]
```

DNS:

```
example.com     IN     MX   10 mailhost.example.com.
```

Alias e canonical names

```
alias_maps = hash:/etc/postfix/aliases, hash:/etc/postfix/docenti_facolta
local_recipient_maps = $alias_maps unix:passwd.byname
canonical_maps = hash:/etc/postfix/canonical
```

Ricordarsi di dare il comando
`postalias aliases`

Postfix: che controlli si possono fare?

- il Modulo Smtpd consente il controllo di:
  - **Sender address** checks: sull'indirizzo mittente
  - **Recipient address** checks: sull'indirizzo destinatario
  - **Helo** checks: sulla dichiarazione di HELO
  - **Header** checks: controlli sul contenuto dell'header
- Modulo Cleanup
  - **Body** checks: sul contenuto del corpo del *messaggio*

Controlli: from, helo, recipient

```
#Reject the request when the client sends SMTP commands ahead of time
smtpd_delay_reject = yes
reject_unauth_pipelining = yes

smtpd_sender_restrictions =
    reject_non_fqdn_sender,       #required by the RFC.
    reject_unknown_sender_domain  #MAIL FROM address has no DNS A or MX record

smtpd_helo_required = yes
smtpd_helo_restrictions =
    reject_non_fqdn_hostname
    reject_invalid_hostname       #HELO or EHLO hostname syntax is invalid

smtpd_recipient_restrictions =
        reject_unauth_destination,
        reject_unknown_recipient_domain
```

Controlli su contenuto e header

```
header_checks = regexp:/etc/postfix/header_checks
body_checks = regexp:/etc/postfix/body_checks
```

/etc/postfix/header checks

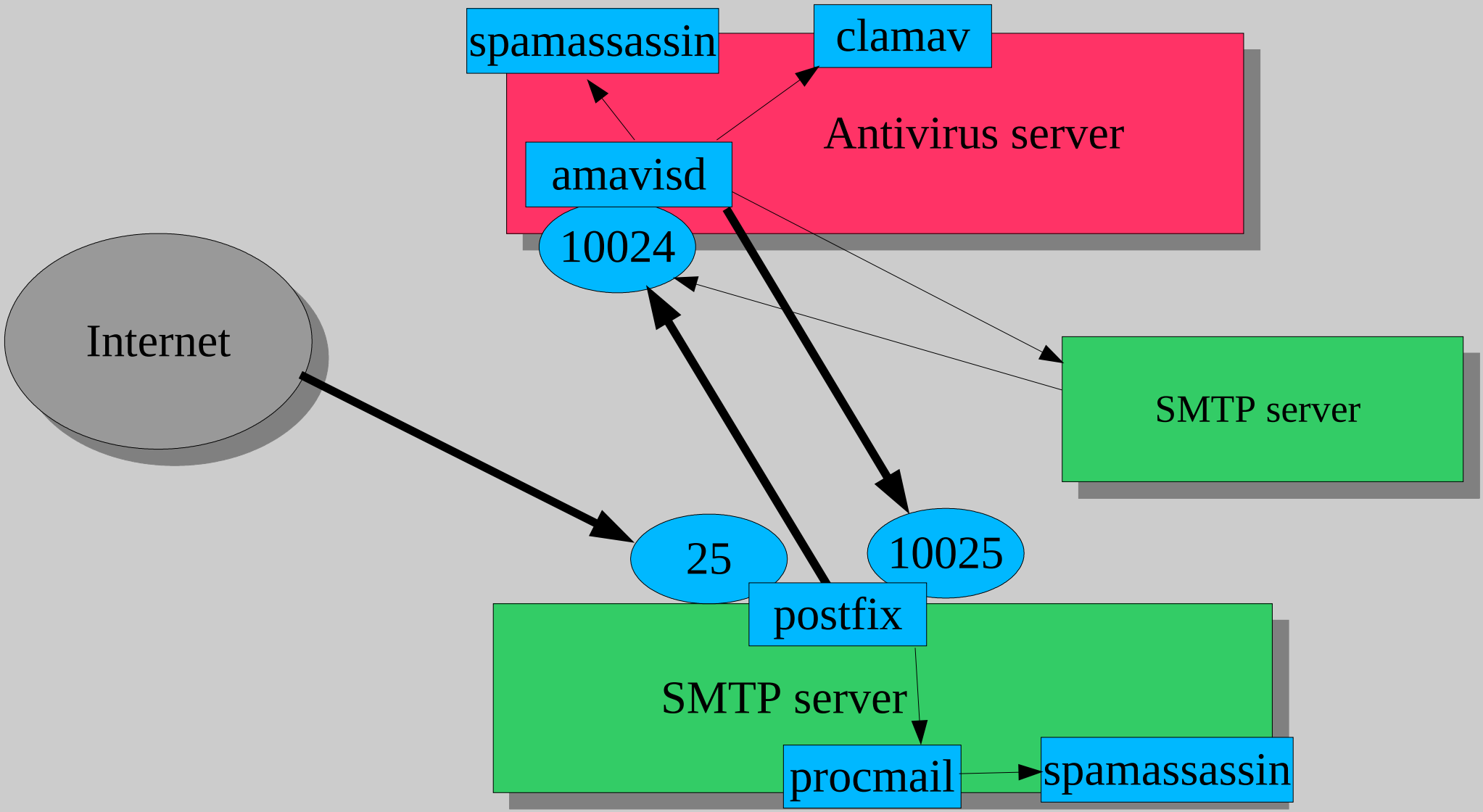
```
#ATTACHMENT
/.+name=.+\.(hta|com|pif|vbs|vbe|js|jse|exe|bat|cmd|vxd|scr|shm|eml|
hlp|spl|swf|shb|vba|dll|reg|ocx|wsf|wsh|lnkr|cpl)"?$/ REJECT
#SUBJECT
/^Subject: retire early.*$/ REJECT
/^Subject: Got Debt? [7xkeh].*/ REJECT
/^Subject: Get Out of Debt NOW! [qcx4l].*/ REJECT
/^Subject: Mens Health Manual\.\.\.\.\.\..*/ REJECT
/^Subject: Vazna informacija! .*/ REJECT
/^Subject: This is what your lover wants.*/ REJECT
#FROM
/^From: "Martina & Laura" <blackgirls@libero.it>/ REJECT
/^From: "Gray" <@msn.com>.*$/ REJECT
/^From: "James" <@msn.com>.*$/ REJECT
/^From: mikeee1029@servicenetbest.com.*$/ REJECT
/^From: beene12981@servicenetbest.com.*$/ REJECT
/^From: "nevio" <nevio111@tin.it>.*$/ REJECT
```

/etc/postfix/body_checks

```
/^TV[nopqr]....[AB]..A.A....*AAAA...*AAAA/   REJECT
/^M35[GHIJK].`..`..*````/  REJECT
/^UEsDBAoAAAAAA/ REJECT
```

- Gli allegati base64 iniziano in un dato modo se il file che codificano inizia con una data stringa; e gli eseguibili (anche Windows) iniziano sempre nello stesso modo (prima e seconda riga)
- Anche se sono zippati (terza riga)
- Volendo si può fare lo stesso anche con uuencode, ma non lo usa nessuno.
- Credit: *Hobbit* <hobbit-at-avian-dot-orb>
- Attenzione: qualche falso positivo

Antivirus su antivirus server



Configurazione Postfix

```
#file  /etc/postfix/main.cf
content_filter = smtp-amavis:[avir]:10024

#file /etc/postfix/master.cf
smtp-amavis unix -       -       n       -       2  smtp
        -o smtp_data_done_timeout=1200
        -o smtp_send_xforward_command=yes
        -o disable_dns_lookups=yes

# XX.YYY: LOCAL IP, dirirorno dall'antivirus
# XX.ZZZ: IP host avir sul quale gira l'antivirus
147.162.XX.YYY:10025 inet n - n - - smtpd
        -o content_filter=
        -o local_recipient_maps=
        -o smtpd_helo_restrictions=permit_mynetworks,reject
        -o smtpd_client_restrictions=permit_mynetworks,reject
        -o smtpd_sender_restrictions=
        -o smtpd_recipient_restrictions=permit_mynetworks,reject
        -o mynetworks=147.162.XX.ZZZ/32
```

Configurazione sul server antivirus

installare:

- amavisd-new
- clamav
- clamav-daemon
- clamav-freshclam
- spamassassin

Amavisd ha un file di configurazione infernale: e' uno script PERL /etc/amavisd.conf

Clamav, freshclam e spamassassin si configurano benissimo con debian o con file di configurazione umani in /etc/

Modifiche a /etc/amavisd.conf

```
$relayhost_is_client = 1;
# if $relayhost_is_client is true, IP address in
# $notify_method and  $forward_method is dynamically
# overridden with SMTP client peer address

$inet_socket_port = 10024;
# accept SMTP on this local TCP port
# (default is undef, i.e. disabled)

$inet_socket_bind = '147.162.XX.ZZZ';
# limit socket bind to loopback interface
# (default is '127.0.0.1')

@inet_acl = qw( 147.162.XX.YYY 147.162.XX.KKK );
# allow SMTP access only from localhost IP
# (default is qw( 127.0.0.1 ) )
```

/etc/amavisd.conf e spamassassin

```
$sa_tag_level_deflt  = 4.0;
# add spam info headers if at, or above that level

$sa_tag2_level_deflt = 10.0;
# add 'spam detected' headers at that level

$sa_kill_level_deflt = 10;
# triggers spam evasive actions at or above that level

$sa_dsn_cutoff_level = 10;
# spam level beyond which a DSN is not sent

$sa_spam_subject_tag = '***SPAM*** ';
```

Procmail + Spamassassin

$HOME/.procmailrc

```
:0fw: spamassassin.lock
| /usr/bin/spamassassin

:0:
* ^X-Spam-Status: Yes
Mail/SPAM
```

- La prima riga invoca spamassassin
- La seconda archivia automaticamente la mail etichettata come SPAM da spamassassin nel file $HOME/Mail/SPAM

- L'archiviazione automatica può essere attivata quanto non si hanno piu' *falsi positivi* (mail erroneamente etichettata come SPAM)
- Lo può fare l'utente stesso
- L'amministratore deve agire cautamente: se attiva l'archiviazione senza il consenso dell'utente può commettere il reato di *intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche*' (617 quater C.P.: a 1 a 4 anni)

Riassumendo

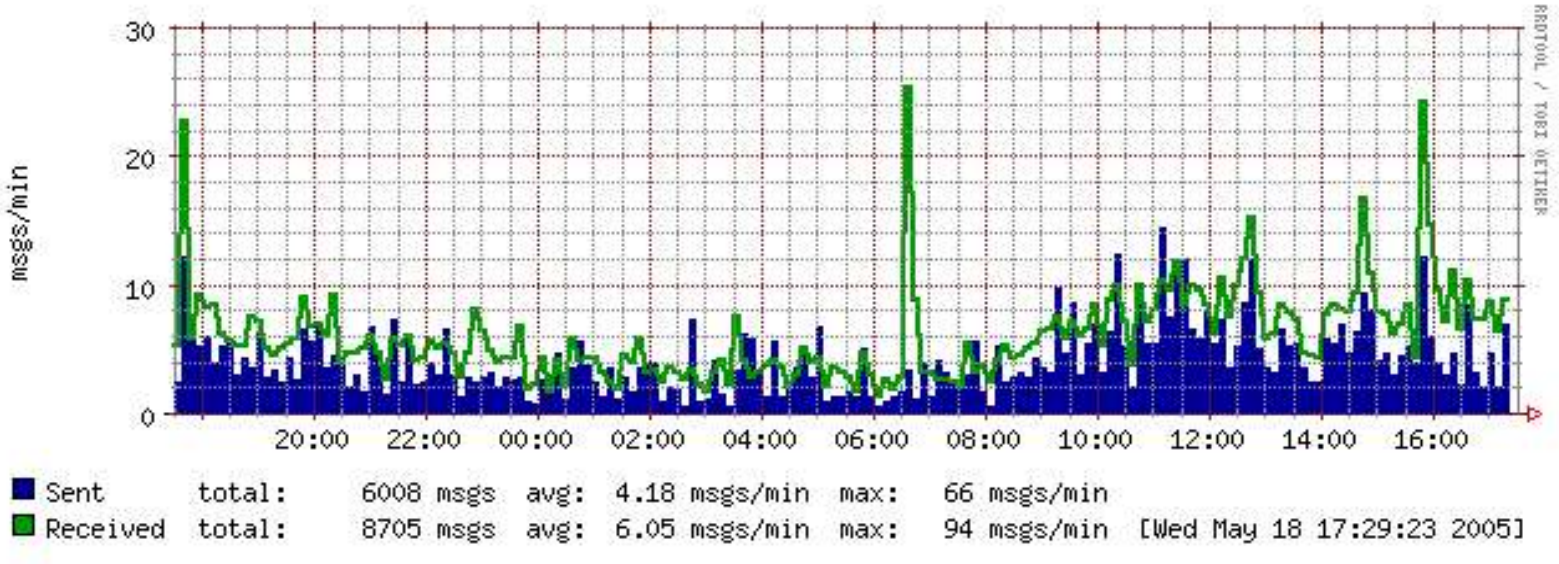
Minimizzare l'intervento di Amavis e dell'antivirus usando pesantemente la tecnica di respingere la mail fasulla.

Filtrare e buttare lo SPAM piu' grossolano

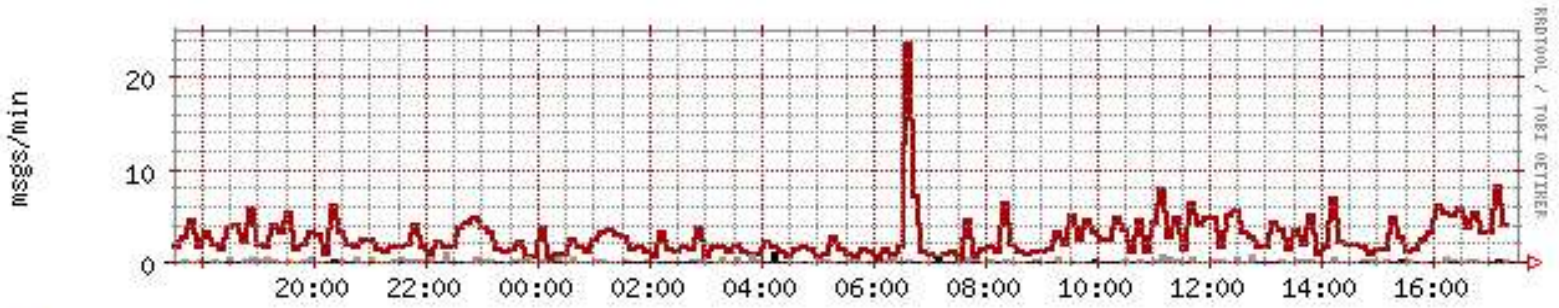
Lasciare all'utente la possibilita' di tarare il proprio filtro antispam a livello fine

mailgraph.cgi

Day Graphs



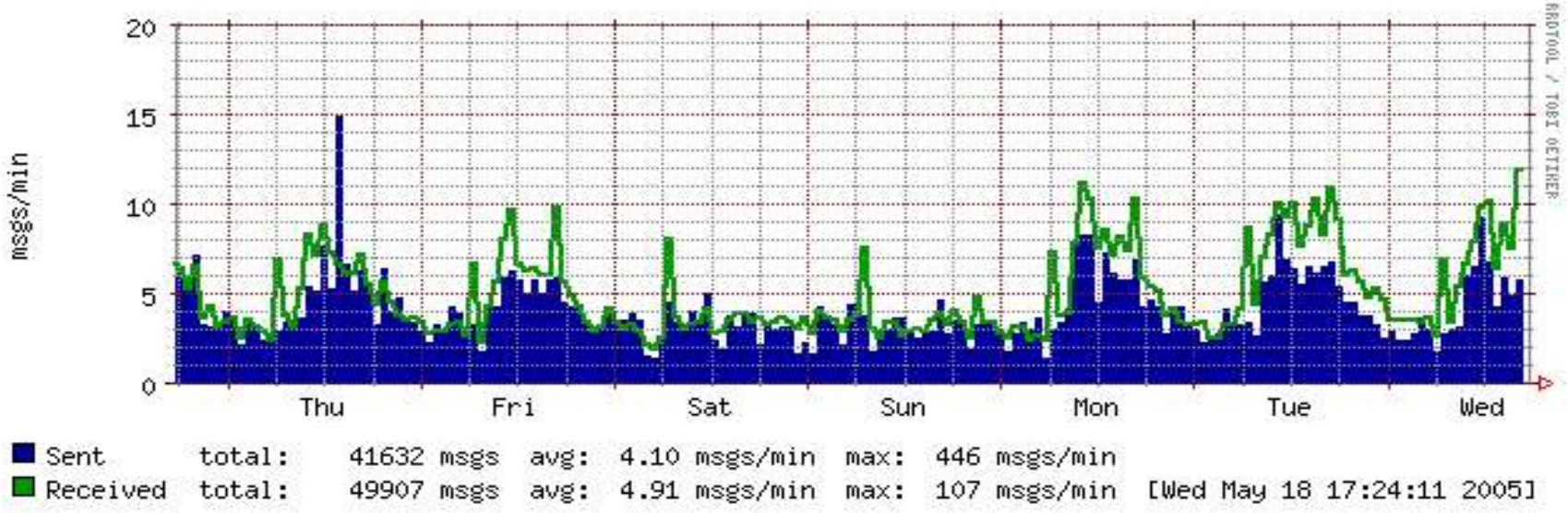
Sent	total:	6008 msgs	avg:	4.18 msgs/min	max:	66 msgs/min	
Received	total:	8705 msgs	avg:	6.05 msgs/min	max:	94 msgs/min	[Wed May 18 17:29:23 2005]



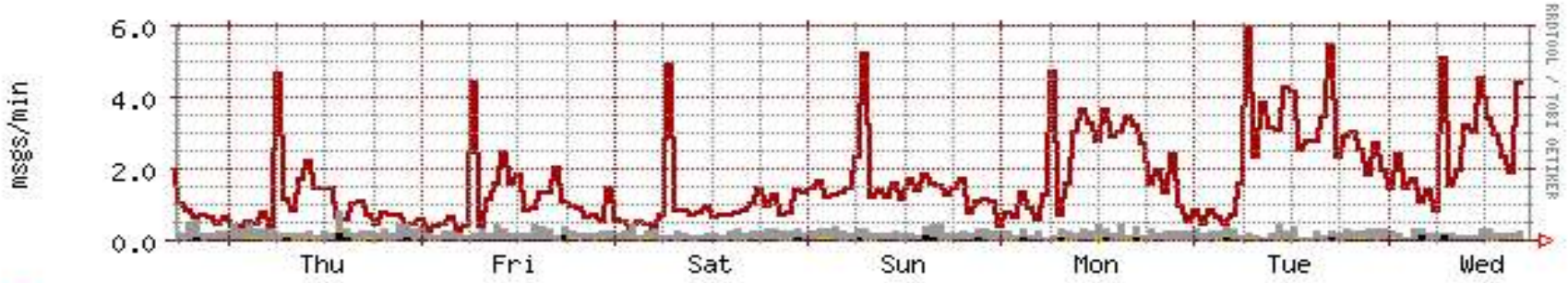
Rejected	total:	3622 msgs	avg:	2.52 msgs/min	max:	61 msgs/min	
Bounced	total:	69 msgs	avg:	0.05 msgs/min	max:	9 msgs/min	
Viruses	total:	26 msgs	avg:	0.02 msgs/min	max:	2 msgs/min	
Spam	total:	233 msgs	avg:	0.16 msgs/min	max:	5 msgs/min	[Wed May 18 17:29:24 2005]

mailgraph.cgi

Week Graphs



Sent	total:	41632 msgs	avg:	4.10 msgs/min	max:	446 msgs/min	
Received	total:	49907 msgs	avg:	4.91 msgs/min	max:	107 msgs/min	[Wed May 18 17:24:11 2005]



Rejected	total:	16158 msgs	avg:	1.59 msgs/min	max:	67 msgs/min	
Bounced	total:	466 msgs	avg:	0.05 msgs/min	max:	13 msgs/min	
Viruses	total:	167 msgs	avg:	0.02 msgs/min	max:	6 msgs/min	
Spam	total:	1920 msgs	avg:	0.19 msgs/min	max:	21 msgs/min	[Wed May 18 17:24:12 2005]

Fine