SERVEUR DE MAIL
&
ANTIVIRUS

Les besoins

- Un serveur de mail robuste
- Limitation de la propagation des virus
- 550 comptes à héberger
- Garder un accès souple et rapide

L ’existant

- Un serveur mono processeur
- Pas d ’alimentation redondante
- Pas de raid
- OS Debian Linux
- Postfix

Nouveau Matériel

- Alimentation redondante
- bi processeurs
- 5 disques en RAID 0+1 avec un spare

Filtrage des mails

- OS Debian Linux Woody
- Postfix (MTA)
- amavisd (en version demon)
- uvscan (Antivirus)
- procmail (MDA) + spamassasin

Intégration

- Postfix supporte deux façons d ’intégrer amavisd
- Lancer deux occurrence de postfix et insérer amavis entre les deux.
- Intégrer amavis comme programme externe chargé de l ’inspection du contenu des pièces attachés aux mails.

Amavis : A Mail Virus Scanner

- Postfix transmet à AMaViS chaque message reçu.
- AMaViS examine le message et fait analyser les documents attachés au message par UvScan
- Le cas échéant AMaViS décompacte les fichiers compressés.

Amavis : A Mail Virus Scanner

- Le message n'est pas transmis à son destinataire.
- L'administrateur est averti par un message contenant
  - L'adresse de l'émetteur
  - Le nom du destinataire
  - Le nom du virus

Amavis : A Mail Virus Scanner

Installation

- Téléchargement et compilation du module amavisd
- Mise en place des différents modules de décompression (arj zip zoo...)
- Ajout dans master.cf des lignes suivantes

```
vscan     unix  -       n       n       -       10      pipe user=vscan
  argv=/usr/sbin/amavis ${sender} ${recipient}
localhost:10025 inet    n       -       n       -       - smtpd -o content_filter=
```

Bench : Amavisd + 3% de virus en entrée smtp (script)

1000 messages sont injectés à postfix sur le port 25 en 9 minutes. Le load est de (6/5/3) et la charge CPU moyenne de 60%. Aucun message ne demeure en queue à la fin de l'injection. Le flux **IN** est de 111 msg/min (2 msg/sec) et le flux **OUT** voisin de 250 msg/min. Les 31 virus sont détectés et mis en quarantaine

Bench: Amavisd + procmail + SAd à blanc

- Amavisd en content filter de postfix + vscan McAfee + procmail + spamd/spamc en .procmailrc
- Le flux est stabilisé en entrée (**IN**) à la même valeur, 250 msg/min. Néanmoins le load est plus élevé (13/13/10) et les flux ne sont pas équilibrés. Les CPUs sont régulièrement à 98% et la charge moyenne monte à 60%. Après coupure du flux entrant (13 minutes), les 2360 messages en queue s'écoulent au rythme **OUT** de 246 msg/min ou 4 msg/sec.

SpamAssassin

- SpamAssassin utilise une méthode de détection qui créé des barèmes pour chaque type de phrases, de techniques des différents spammers. Si le score dépasse le barème général combiné, le mail est modifié et le sujet prend un entête SPAM qu'il devient facile de filtrer.

SpamAssassin

```
SPAM: -------------------- Start SpamAssassin results ---------------------
    -
SPAM: This mail is probably spam.  The original message has been altered
SPAM: so you can recognise or block similar unwanted mail in future.
SPAM: See http://spamassassin.org/tag/ for more details.
SPAM:
SPAM: Content analysis details:   (11.5 hits, 6 required)
SPAM: Hit! (2.5 points)  Cc: contains similar domains at least 10 times
SPAM: Hit! (1.6 points)  Cc: contains similar usernames at least 10 times
SPAM: Hit! (1.0 point)   From: ends in numbers
SPAM: Hit! (0.6 points)  From: does not include a real name
SPAM: Hit! (1.4 points)  Message text disguised using base-64 encoding
SPAM: Hit! (2.0 points)  Forged yahoo.com 'Received:' header found
SPAM: Hit! (2.4 points)  Subject: is empty or missing
SPAM:
SPAM: -------------------- End of SpamAssassin results ---------------------
    -
```

Entête de mail

X-Antivirus: scanned by sophos at u-strasbg.fr

X-Virus-Scanned: by AMaViS snapshot-20010714

X-Spam-Status: No, hits=-100.0 required=6.0

Scanné par le CRC puis par chimie et filtré par SpamAssassin