Tutorial j-chkmail

José-Marcio Martins da Cruz

Ecole des Mines de Paris

Jose-Marcio.Martins@ensmp.fr - http://j-chkmail.ensmp.fr

Plan

- Milters – Kezako ?
- j-chkmail – Kezako ?
- Installation de j-chkmail
- Où sont ... ?
- Les outils en ligne de commande
- Surveillance et contrôle du filtre
- Configuration de j-chkmail
  - Base de données j-policy
  - Variables d'environnement
- Détection des Xfiles

Plan

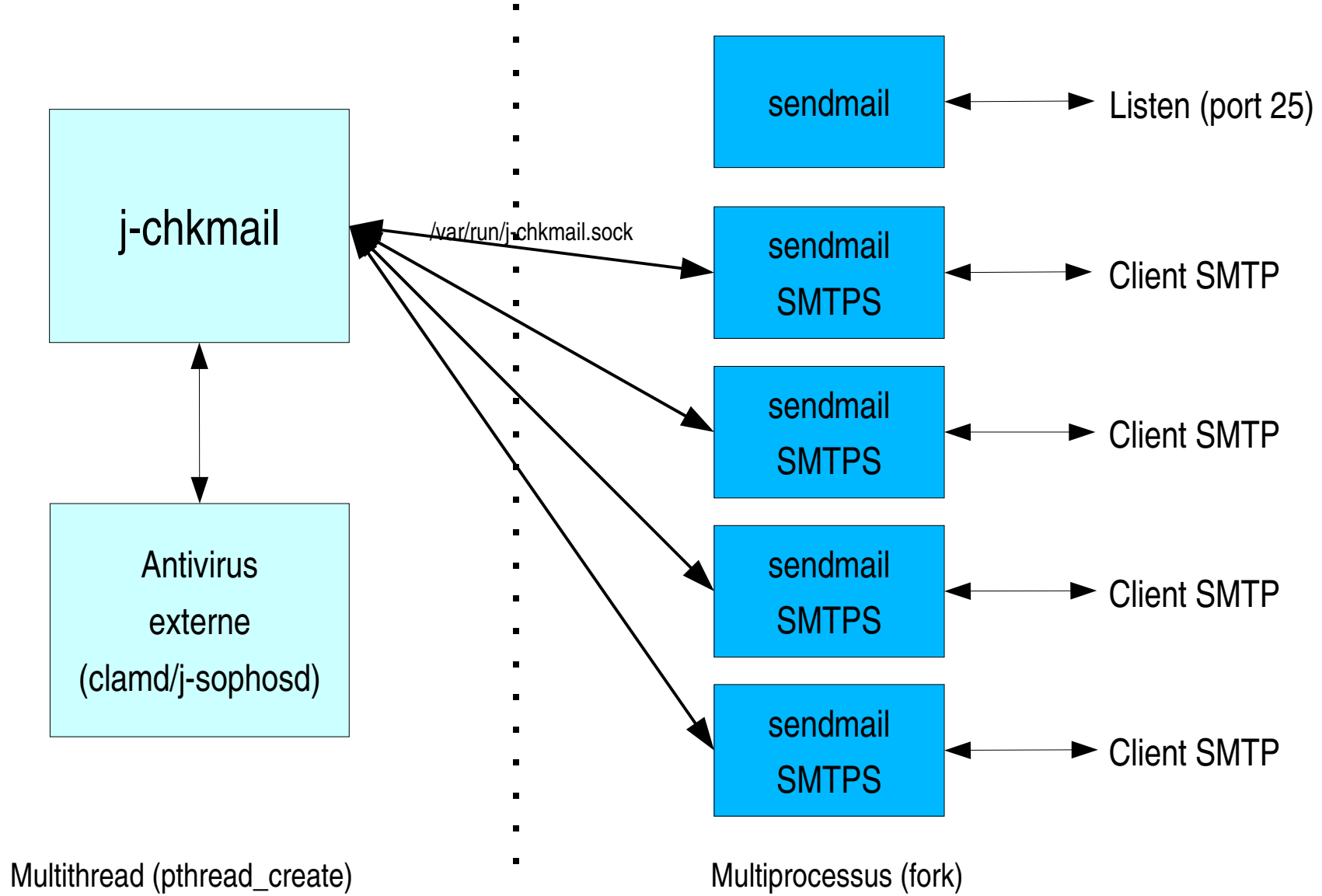
- Interface anti virus
- Filtrage comportemental et de conformité
- Filtrage de contenu – anti SPAM
- Greylisting – en cours
- Autres options de configuration
- Conclusions

Milters – Kezako ?

La bibliothèque libmilter

- Grosso modo : une interface de programmation permettant d'intégrer «en temps réel» un traitement externe dans la chaîne de traitement du protocole SMTP.
- Le filtre fourni des callbacks pour les commandes SMTP *CONNECT, EHLO, MAIL, RCPT, DATA* (8.13 FFR), *EOM* et *QUIT* plus *HEADERS*, *END_OF_HEADERS* et *BODY*.
- Le filtre est un daemon multithreaded qui communique avec sendmail par l'intermédiaire d'une socket UNIX ou INET
- Un milter (mail filter) a besoin de :
  - Sendmail (d'habitude /usr/lib/sendmail ou /usr/sbin/sendmail)
    - *cd sendmail-8.13.4; ./Build; ./Build install*
  - Libmilter (/usr/lib/libmilter.a et /usr/include/libmilter/*)
    - *cd sendmail-8.13.4/libmilter; ./Build; ./Build install*
  - Et le filtre avec ses dépendances

Un milter et sendmail



Libmilter – «pool of workers»

- Avec la libmilter d'origine, chaque connexion SMTP correspond à un thread dans le processus filtre. Ceci est un problème pour des gros serveurs (des centaines de connexions simultanées).
- La plupart du temps, les threads sont inactifs, en attente d'une commande en provenance de sendmail – en fait, de l'ordre de 99 % du temps.
- http://j-chkmail.ensmp.fr/libmilter est une implémentation alternative de la libmilter utilisant un «pool of workers».
- Deux «workers» sont démarrés au départ. Ils ne sont appelés que quand il y a une commande à traiter.

Configuration de sendmail

- sendmail.mc (jchkmail-v.v/smconfig/milter.mc)

INPUT_MAIL_FILTER(`j-chkmail',`S=local:/var/run/jchkmail/j-chkmail.sock, T=C:2m;S:20s;R:20s;E:5m')

define(`confINPUT_MAIL_FILTERS',`j-chkmail')

define(`confMILTER_LOG_LEVEL',`9')dnl

define(`confMILTER_MACROS_CONNECT', ``j, _, {daemon_name}, {if_name}, {if_addr}, *{client_resolve}*'')

define(`confMILTER_MACROS_HELO', ``{tls_version}, {cipher}, {cipher_bits}, {cert_subject}, {cert_issuer}'')

define(`confMILTER_MACROS_ENVFROM', ``i, {auth_type}, {auth_authen}, {auth_ssf}, {auth_author}, {mail_mailer}, {mail_host}, {mail_addr}'')

define(`confMILTER_MACROS_ENVRCPT', ``{rcpt_mailer},{rcpt_host},{rcpt_addr},*{nrcpts},{nbadrcpts}*'')

define(`confMILTER_MACROS_EOM', ``{msg_id}'')

- sendmail.cf (jchkmail-v.v/smconfig/milter.cf)

O InputMailFilters=j-chkmail

Xj-chkmail, S=local:/var/run/jchkmail/j-chkmail.sock, T=C:2m;S:20s;R:20s;E:5m

O Milter.macros.connect=j, _, {daemon_name}, {if_name}, {if_addr}, *{client_resolve}*

O Milter.macros.helo={tls_version}, {cipher}, {cipher_bits}, {cert_subject}, {cert_issuer}

O Milter.macros.envfrom=i, {auth_type}, {auth_authen}, {auth_ssf}, {auth_author}, {mail_mailer}, {mail_host}, {mail_addr}

O Milter.macros.envrcpt={rcpt_mailer},{rcpt_host},{rcpt_addr},*{nrcpts},{nbadrcpts}*

O Milter.macros.eom={msg_id}

j-chkmail – Kezako ?

j-chkmail – Kezako ?

- Un filtre de messagerie pour sendmail avec la bibliothèque libmilter
  - But : rapidité – environ 60K lignes de code en C
- Anti-virus
  - Filtrage de X-Files (messages avec des fichiers attachés exécutables sous windows)
  - Interface clamd et j-sophosd
  - Interface serveur AV générique (contrib/user-filter)
- Anti-spam
  - Comportement – cadences diverses, spamtraps, harvest, ...
  - Pattern Matching
  - Filtrage URL
  - Filtre heuristique («Oracle»)
  - «Petits checks entre amis»
  - «Greylisting adaptatif» - en cours
- Protection du serveur

Documentation

- Fichier ChangeLog
- FAQ -
  - http://j-chkmail.ensmp.fr/registered/faq - parfois recopiée dans contrib/doc
  - http://j-chkmail.ensmp.fr/registered/faq-fr-1.6 - Contribution de Anne Capdepon
- Documentation Minable 8-(- contrib ???

Version 1.7 ou 1.8 ???

- Les nouveautés de la version 1.7
  - Filtrage d'URL
- Les nouveautés de la version 1.8
  - Base de données j-policy
  - Vérification de l'accessibilité du MX de l'expéditeur (rejet si défini dans j-policy)
  - Filtrage heuristique – seuls les tests dont le taux de faux positif est très bas resteront.
  - Greylisting adaptatif – encore en validation
  - Nettoyage du code

Liens utiles à j-chkmail

- http://j-chkmail.ensmp.fr - URL du site web du filtre
  - http://j-chkmail.ensmp.fr/registered - Partie privée et téléchargement du filtre
  - http://j-chkmail.ensmp.fr/francais-er - Ressources pour la communauté E/R française
- http://j-chkmail.ensmp.fr/j-sophosd - Daemon interface avec lib SAVI – Sophos
- http://j-chkmail.ensmp.fr/libmilter - Version alternative de la libmilter utilisant un «pool of workers»

Installation de j-chkmail

Installation rapide

- La première installation – rapide ... 8-)

```
tar xf jchkmail-1.8-050610.tgz
cd jchkmail-1.8-050610
./configure; make; make install
/usr/sbin/j-chkmail -n > /etc/mail/jchkmail/j-chkmail.cf
# modification des fichiers de configuration dans /etc/mail/jchkmail
/etc/init.d/jchkmail start
```

- Configurer sendmail pour causer avec j-chkmail
  - Noter la socket configurée dans j-chkmail.cf (défaut : *local:/var/run/jchkmail/j-chkmail.sock*)
  - Configurer sendmail pour contacter j-chkmail par l'intermédiaire de cette socket (voir transparents précédents)
  - Relancer sendmail

Installation rapide

- Configurer syslog pour fonctionner avec j-chkmail.
  - Créer un fichier vide /var/log/j-chkmail

    ```
    touch /var/log/j-chkmail
    ```
  - Ajouter la ligne suivante au fichier /etc/syslog.conf, et relancer syslogd

    ```
    local5.*                /var/log/j-chkmail
    ```

    OBS : la séparation entre les champs est constituée de tabulations et non pas de espaces

- En ce point, j-chkmail doit fonctionner en mode surveillance uniquement. Toutes les fonctions de filtrage sont désactivées, par défaut. Mais vous devez voir les lignes de log correspondantes aux connexions et à l'activité de surveillance.

Où sont ... ???

Répertoires utilisés par j-chkmail

- /usr/sbin et /usr/bin - exécutables
- /etc/mail/jchkmail - fichiers de configuration
- /var/jchkmail - répertoire de travail
- /var/spool/jchkmail - répertoire de spool
- /etc/init.d/jchkmail - script de démarrage
- /etc/(defaultlsysconfig)/jchkmail - variables d'environnement
- /var/jgreyd - répertoire de travail du daemon greylisting

Le répertoire de configuration

- /etc/mail/jchkmail

```
-rw-r--r--   1 root     other       20813 May 19 22:14 j-chkmail.cf
-rw-r--r--   1 root     other        9045 Jun  1 15:32 j-regex
-rw-r--r--   1 root     other        4030 Jun  3 13:46 j-access
-rw-r--r--   1 root     staff        1067 Feb 28 16:28 j-nets
-rw-r--r--   1 root     other        1639 Apr 26 11:54 j-oradata
-rw-r--r--   1 root     staff         897 Apr 20 17:28 j-xfiles
-rw-r--r--   1 root     other        2290 Apr 19  2004 j-error-msg
-rw-r--r--   1 root     staff        1224 Mar 29 09:54 j-local-users

-rw-r--r--   1 root     other         450 Apr 26 13:02 Makefile
-rw-r--r--   1 root     other         241 Oct 11  2004 get-urlbl

-rw-r--r--   1 root     other    16711680 Jun 10 17:10 j-urlbl.db
-rw-r--r--   1 root     staff    11200150 Jun 10 16:37 j-urlbl.txt

-rw-r--r--   1 root     other       98304 Jun  3 22:22 j-policy.db
-rw-r--r--   1 root     other       61348 Jun  3 22:22 j-policy.txt
```

Le répertoire de travail

- Les fichiers texte – fichiers à retourner

```
-rw-r--r--   1 smmsp    smmsp    2180046 Jun 13 16:55 j-files
-rw-r--r--   1 smmsp    smmsp   85431286 Jun 13 16:56 j-regex
-rw-r--r--   1 smmsp    smmsp       1180 Jun 13 16:56 j-state
-rw-r--r--   1 smmsp    smmsp   10063637 Jun 13 16:55 j-xreport
```

- Les compteurs du filtre

```
-rw-r--r--   1 smmsp    smmsp    6748207 Jun 13 16:53 j-stats
```

- Le historique à court terme

```
-rw-r--r--   1 smmsp    smmsp     720896 Jun 13 16:56 j-bouncedata
-rw-r--r--   1 smmsp    smmsp     720896 Jun 13 16:56 j-bytesdata
-rw-r--r--   1 smmsp    smmsp     720896 Jun 13 16:56 j-conndata
-rw-r--r--   1 smmsp    smmsp     720896 Jun 13 16:56 j-msgsdata
-rw-r--r--   1 smmsp    smmsp     720896 Jun 13 16:56 j-rcptdata
-rw-r--r--   1 smmsp    smmsp     786432 Jun 13 16:56 j-resolvedata
-rw-r--r--   1 smmsp    smmsp     720896 Jun 13 16:56 j-scoredata
-rw-r--r--   1 smmsp    smmsp     720896 Jun 13 16:56 j-svctimedata
-rw-r--r--   1 smmsp    smmsp     720896 Jun 13 16:56 j-xfilesdata
```

- Le historique à moyen terme – taille configurable

```
-rw-r--r--   1 smmsp    smmsp   33554432 Jun 13 16:56 j-history
```

- Les bases greylisting

```
-rw-r--r--   1 smmsp    smmsp   15278080 Jun 13 16:56 j-greypend.db
-rw-r--r--   1 smmsp    smmsp    6733824 Jun 13 16:56 j-greyvalid.db
-rw-r--r--   1 smmsp    smmsp      16384 Mar 29 12:16 j-greywhitelist.db
```

Le répertoire de travail

- /var/jchkmail
  - j-files – fichier simple avec Xfiles detectés

```
1118407320 42A98A97.002 IP=(195.220.252.67) XXX application/zip boulesdenoel.zip
1118407329 42A98AA1.000 IP=(195.220.252.67) XXX application/octet-stream adrianna karembeu.exe
1118407686 42A98C06.001 IP=(193.252.22.30) XXX application/octet-stream instructions.zip
1118408088 42A98D94.000 IP=(200.53.114.34) XXX application/octet-stream document_excel.pif
```

  - j-xreport – description des messages mis en quarantaine

```
42A99331.000.0000  CONN 1118409521 83.195.149.187   ANantes-251-1-14-187.w83-195.abo.wanadoo.fr
42A99331.000.0000  WHY  .xfile
42A99331.000.0000  QUAR 42A99331.000.0000.xfile
42A99331.000.0000  SUBJ Re: document
42A99331.000.0000  FROM <meuhmeuh34@msn.com>
42A99331.000.0000  RCPT <scherer@ensmp.fr>
42A99331.000.0000  SIZE    35749
42A99331.000.0000  FILE XXX application/octet-stream       document.pif
```

  - j-regex – les “trucs” trouvés dans le contenu des messages

```
1118403458 42A97B82.000 IP=(193.49.22.101) TAG=(REGEX)   1   5 &#[0-9]{1,5};
1118403500 42A97BAB.002 IP=(193.49.22.101) TAG=(REGEX)   1   2 [$][ ]?[0-9]{1,3} [mb]illion
1118403591 42A97C07.000 IP=(195.46.220.211) TAG=(DBURLBL:multi.surbl)   1  20 datenicegirl.com
1118403591 42A97C07.000 IP=(195.46.220.211) TAG=(DBURLBL:multi.surbl)   1  40 pics-4-show.com
```

Le répertoire de travail

-
  - j-stats – les dumps des compteurs internes (pour RRDtool)

```
1118409584 CONN=(10974649) ABRT=(4535743) MSGS=(4787361) KBYTES=(11529215045261564 50) RCPT=
 (13458177) FILES=(1039657) XFILES=(165822) RCPTRATE=(0) THROTTLE=(1754865) OPENCONN=(5768)
 BADRCPT=(101412) SPAMTRAP=(19448) LOCALUSER=(7319) RESFAIL=(23979) RESFORG=(7746) MATCHING=
 (2158372) ORACLE=(2180586) BADMX=(233862)
```

Le répertoire de quarantaine

- /var/spool/jchkmail

```
martins@paris:/var/spool/jchkmail> lt
total 179196
drwxr-x---   2 smmsp    smmsp     289792 Jun 10 15:31 .
-rw-------   1 smmsp    smmsp         50 Jun 10 15:31 42A99600.000.0000
-rw-------   1 smmsp    smmsp     153493 Jun 10 15:27 42A9953C.000.0000.xfile
-rw-------   1 smmsp    smmsp      39893 Jun 10 15:23 42A9943E.000.0000.xfile
-rw-------   1 smmsp    smmsp         58 Jun 10 15:19 42A9930B.000.0000
-rw-------   1 smmsp    smmsp      36050 Jun 10 15:18 42A99331.000.0000.xfile
-rw-------   1 smmsp    smmsp         59 Jun 10 15:17 42A992FC.004.0000
-rw-------   1 smmsp    smmsp         67 Jun 10 15:14 42A99229.002.0000
...
```

Journaux

- syslog (local5 – default) /var/log/milter – utiliser outils spécifiques au système (newsyslog, logadm, ...)
- /var/jchkmail/
  - j-files
  - j-xreport
  - j-regex
  - j-stats
  - j-virus
- Rotation des fichiers de log
  - Outils système pour fichiers générés par syslog (newsyslog, logadm, ...)
  - contrib/scripts/j-rotate pour fichiers enregistrés dans /var/jchkmail

Les outils en ligne de commande

- j-chkmail – le filtre lui-même
- j-printstats – statistiques à partir des informations enregistrées sur disque
- j-ndc – statistiques par connexion au filtre
- j-makemap – manipulation des bases de données
- j-scanfile – scan (X-Files) fichier message format mbox
- j-greyd – daemon greylisting
- contrib/ - scripts non garantis
  - scripts – scripts perl pour manipuler les fichiers de log
  - rrd-jchkmail – scripts perl pour créer des graphiques de suivi d'activité du filtre
  - quarantine-mgmt – des scripts pour gérer la quarantaine (sortie automatique de la quarantaine ???)
- scratch/ - “unsupported trucs” utilisés pour des test. Les deux programmes qui peuvent intéresser sont j-extract-url et j-check-spam

j-chkmail

```
[martins@localhost ~]$ j-chkmail -h
Usage : j-chkmail options
  Joe's j-chkmail v1.8 - Alpha 16 050525
  Compiled on May 25 2005 11:45:49
        -p  : socket
              inet:2000@localhost
              local:/var/sock
        -i  : 2000  (AF_INET)
        -u  : /var/sock (AF_UNIX)
        -d  : inet domain
        -h  : help
        -c  : configuration file
        -l  : log level
        -m  : create configuration file (running conf)
        -n  : create configuration file (default)
        -v  : version / runtime configuration
        -vv : version / compile time configuration
        -x  : compile time X-FILES definition
        -t tablename, where tablename choosen between :
                access | users | networks | classw | regex | rbl | urlbl | oradata | xfiles
```

j-chkmail

- Création d'un fichier de configuration avec les valeurs par défaut
  - j-chkmail -n
- Création d'un fichier de configuration (propre) avec les valeurs actuelles
  - Création d'un nouveau fichier de configuration lors d'une mise à jour
    1. j-chkmail -m > j-chkmail.cf.new
    2. diff /etc/mail/jchkmail/j-chkmail.cf j-chkmail.cf.new > j-chkmail.cf.diff
    3. vi j-chkmail.cf.new
    4. mv j-chkmail.cf.new /etc/mail/jchkmail/j-chkmail.cf
- Comment j-chkmail a interpreté le fichier de configuration

  j-chkmail -v
- Affichage du contenu des tables

  j-chkmail -t access | users | networks | regex | rbl | urlbl | oradata | xfiles

j-makemap

- Manipulation des bases de données j-chkmail
  - Résumé des options : j-makemap -h
- Création d'une base de données

```
j-makemap -b /path/to/fichier.db -m [erase | skip | update] < fichier.txt
```

- Dump d'une base de données

```
j-makemap -d -b /path/database.db -w 64
j-makemap -d -b /path/database.db -k racine
```

- Comptage du nombre d'enregistrements

```
j-makemap -c -b /path/database.db
j-makemap -c -b /path/database.db -k racine
```

- Duplication d'une base de données

```
j-makemap -d -b oldbase.db | j-makemap -b newbase.db
```

- Ex : mise à jour de la base j-policy.db

```
mv j-policy.db j-policy.db.old
j-makemap -m e -b j-policy.db < j-policy.txt
j-ndc reload databases
```

j-scanfile

- Détection de XFILEs dans un message au format mbox
  - j-scanfile [-v[v[v]] msg msg msg

```
martins@paris:sendmail/virus/exemples> j-scanfile -v W95.Hybris.Gen.1
Loading j-chkmail configuration
Fadings default values
Reading configuration file : /etc/mail/jchkmail/j-chkmail.cf
Reloading configuration tables...
# Loading REGEX table - Using PCRE : YES
*** FILE W95.Hybris.Gen.1 scanned

 ***** (XFILE     ) : attachment application/octet-stream       sexynain.scr
martins@paris:sendmail/virus/exemples>
```

  -

Surveillance et contrôle du filtre

Surveillance du filtre

- Interface en ligne de commande
  - j-printstats – traitement des fichiers de dump périodique
  - j-ndc – connexion au filtre (telnet localhost 2010)
- Scripts de traitement - contrib/scripts
  - j-regex-stat - traite le fichier /var/jchkmail/j-regex
  - j-unwanted - traite le fichier /var/log/milter
  - j-urlbl-stat - traite le fichier /var/jchkmail/j-regex
  - j-xstat.pl - traite le fichier /var/jchkmail/j-files
  - j-handle-xreport - traite le fichier /var/jchkmail/j-xreport (en cours)
- Scripts de traitement – contrib/rrd-jchkmail – necessite installation de RRDTool
  - j-initrrd - pour initialiser une base RRD
  - j-mem2rrd - pour mettre à jour les bases RRD
  - j-dograph - pour créer les graphiques à partir des bases RRD

j-printstats

- Consultation à partir des données enregistrées sur disque
- Les compteurs internes
  - j-printstats -a | -p | -g

```
j-printstats -a
```

- Le historique court
  - j-printstats -t[td] [-m all,conn,rcpt,bounce,msgs,vol,svc] [-l dt]

```
j-printstats -ttd -m conn,rcpt,msgs,vol,svc
```

- Le historique long
  - j-printstats -q [-l dt [s|m|h|d]] [[-v | ip | hostname] | [-m s | e | re | ro | rt | rr | r | x | c | rm | st | rb]]

```
j-printstats -q -l 1d listes.cru.fr
j-printstats -q -l 3h -m rb
```

- Résolution DNS des clients SMTP
  - j-printstats -r[rdc]

```
j-printstats -rrd
```

j-ndc

- Connexion directe sur le filtre (telnet) – le filtre n'attend que 10 sec.
- Commande, modification variables de configuration, consultation statistiques – temps réel
- Exemples :

```
j-ndc help [cmd]
j-ndc version                          - version du filtre
j-ndc stats connopen                   - connexions ouvertes
j-ndc stats scores                     - histogramme des scores
j-ndc reconfig                         - ré chargement de la configuration
j-ndc reload databases                 - réouverture des bases de données
j-ndc reopen logfiles                  - réouverture des fichiers de log
j-ndc setcf XFILES REJECT              - activation détection des XFILES
j-ndc setcf OPEN_CONN_FROM_LOCAL 30    - modification paramètre
...
```

j-ndc - configuration

- Dans /etc/mail/jchkmail/j-chkmail.cf

```
CTRL_CHANNEL_ENABLE          YES
CTRL_SOCKET                  inet:2010@localhost
CTRL_ACCESS                  NONE | ACCESS
```

- Dans /etc/mail/jchkmail/j-access

```
Connect:10.3.5               CTRL_ACCESS_OK
```

- Dans /etc/mail/jchkmail/j-policy.txt

```
CtrlChan:DEFAULT             REJECT
CtrlChan:127.0.0.1           OK
CtrlChan:194.214.168.176     OK
```

- Dans j-ndc

```
my $HOST = "127.0.0.1";
my $PORT = 2010;
```

- Exemple de «stats» que l'on peut faire une fois par jour...

```
HOJE=`date +"%a %e %b %Y"`

/var/log/j-xstat.pl > xfiles.txt

/usr/bin/j-printstats -ttd     > ttd.txt
/usr/bin/j-printstats -q -l 1d > tout.txt
/usr/bin/j-printstats -rrcd    > rrd.txt

./j-regex-stat.pl         /var/jchkmail/j-regex > regex.txt
./j-urlbl-stat            /var/jchkmail/j-regex > urlbl.txt
./j-urlbl-stat -t URLSTR  /var/jchkmail/j-regex > urlstr.txt
./j-urlbl-stat -t URLEXPR /var/jchkmail/j-regex > urlexpr.txt
./j-unwanted /var/log/milter                    > unwanted.txt

/usr/ucb/Mail -s "Statistiques X-FILES $HOJE" martins    < xfiles.txt
/usr/ucb/Mail -s "Stats j-chkmail - URLBL $HOJE" martins < urlbl.txt
```

La configuration de j-chkmail

Fichiers de configuration

j-chkmail.cf - Fichier principal de configuration

Tables

j-regex - Expressions regulières – Pattern matching
j-access - Accès
j-nets - Réseaux connus – niveau de confiance
j-oradata - Quelques paramètres du filtre heuristique
j-xfiles - Définitions des XFiles

j-error-msg - Contenu des messages de notification

j-local-users - Adresses de destination utilisables dans les réseaux connus

Bases de données

Makefile, get-urlbl – Conversion des bases de données texte -> db

j-urlbl.db - Liste noire d'URLs
j-urlbl.txt

j-policy.db - Base de données policy
j-policy.txt

Classement réseaux (niveau de confiance)

- Classes
  - LOCAL > DOMAIN > FRIEND – configuration
  - AUTH – authentifié
  - KNOWN = LOCAL | DOMAIN | FRIEND | AUTH
  - UNKNOWN – tous les autres
- Configuration
  - /etc/mail/jchkmail/j-nets

```
10/8                        LOCAL
193.49.22.101/32            LOCAL
193.49.22/24                DOMAIN
```

  - /etc/mail/jchkmail/j-policy.txt

```
NetClass:193.49.22          DOMAIN
NetClass:193.49.22.101      LOCAL
```

Pattern Matching

- Fichier /etc/mail/jchkmail/j-regex

```
# OU     POIDS      EXPRESSION
# OU = SUBJECT | HEADERS | BODY | HELO | ANYWHERE

BODY     10  <font [^>]*color=["]?(#[ef]{6,6}|white)["]?[^>]*>
BODY     25  <IMG[^>]{1,160}><BR><IMG[^>]{1,160}><BR><IMG[^>]{1,160}>
BODY     20  http[s]?://[^> *\t\r\n]{1,100}\\*http[s]?://
BODY     10  get.{1,40}(doctorate|university).{1,40}diploma

ANYWHERE 20  WINNING NOTIFICATION
SUBJECT  50 Get.*free

URLEXPR  10  cnn.com/[^ ]{1,20}/africa/
URLEXPR  10  [a-z]+[0-9]{2,5}(biz|drug[s]?|medications|rx|meds|tabs|pill[s]?)\.(biz|us|com)

URLSTR   50  bigbonus-casino.net
```

j-access

```
Connect:KNOWN/From:ensmp.fr                          NO_ORACLE
Connect:KNOWN/From:cma.fr                            NO_ORACLE

# CNRS - CRU
Connect:195.220.94.165                               NO_SPAM_CHECK
Connect:195.220.197.1                                NO_SPAM_CHECK
Connect:195.220.197.22                               NO_SPAM_CHECK
# OSSIR
Connect:195.83.224.3                                 NO_SPAM_CHECK

# amadeus.net - les billets de voyage
Connect:195.27.160.5                                 NO_ORACLE

From:yahoo.com                                       CHECK_DOMAIN_ADDRESS
From:hotmail.com                                     CHECK_DOMAIN_ADDRESS

Connect:UNKNOWN/To:blackhole@paris.ensmp.fr          SPAMTRAP

Connect:194.214.158.176                              CTRL_ACCESS_OK
Connect:194.214.158.200                              CTRL_ACCESS_OK
```

- Ce fichier va peut-être disparaître un jour... remplacé par j-policy.txt

j-oradata

```
# Syntax : TYPE       value
# where TYPE = ( CHARSET | BOUNDARY | MAILER | HTML-TAG )

MAILER       mailing\.[0-9]\.[0-9]\.[0-9]
MAILER       Postmaster BDNMailer
MAILER       [a-z]{1,8}-Mail v[0-9]\.[0-9]\.[0-9]$

CHARSET      ^big5$
CHARSET      ^gb18030$
CHARSET      ^gb2312$

BOUNDARY     ^.{1,14}$
BOUNDARY     ^--=BOUNDARY_[0-9]{9,9}_[a-z]{4,4}_[a-z]{4,4}_[a-z]{4,4}_[a-z]{4,4}$
BOUNDARY     boundary[0-9a-f]{8,8}_related
BOUNDARY     WebTV-Mail-

HTML-TAG     <iframe[^>]*>
HTML-TAG     <script[^>]*>
HTML-TAG     <input[^>]*>
HTML-TAG     <a[^>]+href[^>]+http://[^>]+http://[^>]+>
```

j-policy database

j-policy – contenu

- Valeurs associées à certains paramètres – e.g. Cadence maximale de connexion pour une adresse IP, niveau de confiance d'une classe réseau, ...
- Règles d'accès générales associées soit à un test, soit à une adresse réseau, soit à un expéditeur, soit à un destinataire.

Database policy – logique d'intérrogation

```
query full key
if found return result

extract domain part
if (domain part is IP address)
     query IP address and network addresses
     if found return best matching result
else
     query domains and sub domains
     if found return best matching result
end if

if (key is e-mail)
     query user part
     if found return result
end if

query default value
if found return result else return not found
```

j-policy database – vérification @ email

- E-mail check : *user@sub.domain.com* ou *user@1.2.3.4*
  1. Full check : *Tag:user@sub.domain.com*
  2. Domain check
     - Domain part : *Tag:sub.domain.com*, *Tag:domain.com*, *Tag:com*
     - Network check : *Tag:1.2.3.4*, *Tag:1.2.3*, *Tag:1.2*, *Tag:1*
  3. User part : *Tag:user@*
  4. Valeur par défaut : *Tag:DEFAUT*

j-policy database – vérification @ IP ou domaine

- Ex : *ConnRate* pour *paris.ensmp.fr – 194.214.158.200*
  - @ et réseaux : 194.214.158.200, 194.214.158, 194.214, 194
  - Classe Réseau (NetClass) : 194.214.158.200, 194.214.158, 194.214, 194
    - Si trouvé : ConnRate:CLASS
  - Nom : paris.ensmp.fr, ensmp.fr, fr
  - Classe Réseau (NetClass) : paris.ensmp.fr, ensmp.fr, fr
    - Si trouvé : ConnRate:CLASS
  - Default value: ConnRate:DEFAULT

```
ConnRate:10.3                100
ConnRate:ensmp.fr            110
NetClass:194.214.158.200     MX
NetClass:193.49.22.101       MX
ConnRate:MX                  200
ConnRate:LOCAL               50
ConnRate:DEFAULT             30
```

```
10.3.5.5          ->  100
cep.ensmp.fr      ->  110
194.214.158.200   ->  200
shiva.jussieu.fr  ->  30
```

j-policy database – vérification triplet

- Ex : greylisting
- GreyCheckConnect:ip NO, YES, NO-QUICK, YES-QUICK
  - Si non trouvé, GreyCheckConnect:DEFAULT
- GreyCheckFrom:from NO, YES, NO-QUICK, YES-QUICK
  - Si non trouvé, GreyCheckFrom:DEFAULT
- GreyCheckTo:to NO, YES, NO-QUICK, YES-QUICK
  - Si non trouvé, GreyCheckTo:DEFAULT

```
GreyCheckConnect:DEFAULT                YES
GreyCheckConnect:194.214.158.200        NO-QUICK
GreyCheckConnect:193.49.22.101          NO
GreyCheckFrom:yahoo.fr                  YES
GreyCheckTo:martins@                    YES
GreyCheckTo:martins@cc.ensmp.fr         NO
```

j-policy database – vérification triplet

- En cas de conflit entre plusieurs destinataires (e.g. ContentCheck, XfilesCheck, ...)
  - Option de configuration POLICY_CONFLICT :
    - DEFAULT, ONE_WIN, MAJORITY_WIN

j-policy – tags reconnus

- Tags reconnus :

```
NetClass
CtrlChan
BadMX
ConnRate
ConnOpen
RcptRate
SpamTrap

   GreyCheck    (Connect | From | To)
   Quarantine   (Connect | From | To)
*  ContentCheck (Connect | From | To)
*  XfilesCheck  (Connect | From | To)
*  VirusCheck   (Connect | From | To)
** Notify
** IntranetRcpt

*  Très bientôt
** Un peu plus tard
```

Variables d'environnement

Variables d'environnement reconnues

- A mettre dans le fichier /etc/default/jchkmail ou /etc/sysconfig/jchkmail :
  - JCHKMAIL_SOCKET=»inet:2000@localhost»
  - DB_CACHE_SIZE=4M
  - DESIGNATED_QUARANTINE=yes
  - FILE_EXT=»exe pif com scr»
  - HIGH_LOAD_AUTO_RESTART=98
  - PERIODIC_AUTO_RESTART=24h
  - JCHKMAIL_LOG_LEVEL=10
  - MILTER_LOG_LEVEL=9

Détection des XFiles

Définition XFILES

- Vérification de la définition par défaut des XFILES

```
[martins@localhost]$ j-chkmail -v | grep EXT
  603 FILE_EXT                              (null)
    FILE NAME EXTENSIONS :
    -  EXT    : ade   adp   app   bas   bat   bin   btm   chm   cmd
    -  EXT    : com   cpl   csh   dll   drv   exe   fxp   hlp   hta
    -  EXT    : inf   ini   ins   isp   js    jse   ksh   lnk   mdb
    -  EXT    : mde   mdt   mdw   msc   msi   msp   mst   ops   pcd
    -  EXT    : pif   prg   reg   scr   sct   shb   shs   sys   url
    -  EXT    : vb    vbe   vbs   vxd   wsc   wsf   wsh
[martins@localhost]$
[martins@localhost]$ j-chkmail -x
```

- Modification (version 1.8) dans fichier *aux/xfiles.def*
- *Fichier /etc/mail/jchkmail/j-chkmail.cf*
  - Option FILE_EXT : si non null, remplace hardcoded definition

    ```
    FILE_EXT          exe pif exe com
    ```

  - Option FILE_REGEX : nom de fichier correspondant à expression régulière

    ```
    FILE_REGEX        \.xls\.pif$
    ```

Définition XFILES

- Fichier /etc/mail/jchkmail/j-xfiles

```
# configuration par défaut
ALL                    DEFAULT
# fichiers zip dont le type MIME n'est pas «x-zip-compressed»
!x-zip-compressed      \.zip$
# les fichiers zip dont le nom est plus court que 15 caractères
ALL                    ^.{0,15}\.zip$
ALL;size=0,250000      \.zip$
# fichiers codés aux format TNEF ou CLSID (spécifiques Microsoft)
ALL                    TNEF
ALL                    CLSID
# les vulnérabilités RFC2046
message/partial        DEFAULT
message/external       ALL
```

- Vérification de l'interprétation du fichier j-xfiles
  - j-chkmail -t xfiles

Configuration Détection des XFiles

```
# XFILES
#     What to do with X-files ? (OK, REJECT, NOTIFY, DISCARD)
#     VALUES :  OK  REJECT  NOTIFY  DISCARD  X-HEADER
XFILES                    OK

# FILE_EXT
#     X-files filename extensions
FILE_EXT          exe pif com

# FILE_REGEX
#     Regular expressions matching X-files filename
FILE_REGEX        \.xls\.pif$

# XFILE_SAVE_MSG
#     Shall quarantine messages containing X-Files ?
#     VALUES :  NO  YES
XFILE_SAVE_MSG             YES

# XFILE_SUBJECT_TAG
#     Tag to be inserted on Subject
XFILE_SUBJECT_TAG
```

Notification virus et X-Files

- Dans j-chkmail.cf

```
# NOTIFY_SENDER
#     Send warn message to sender
#     VALUES :  NO  YES
NOTIFY_SENDER              NO

# NOTIFY_RCPT
#     Send warn message to recipient
#     VALUES :  NO  YES
NOTIFY_RCPT                YES

# J_SENDER
#     Identity of sender of replacement warning message
#     VALUES :  SENDER  OTHER
J_SENDER                   SENDER

# J_SUBJECT
#     Subject of replacement warning message
#     VALUES :  SUBJECT  OTHER
J_SUBJECT                  SUBJECT
```

- Définir message de notification dans j-error-msg

Interface anti-virus

Interface antivirus

- Daemon externe
  - Utilisation daemon clamd
  - Utilisation daemon j-sophosd (http://j-chkmail.ensmp/fr/j-sophosd)
  - Utilisation d'un daemon générique (contrib/user-filter) – script Perl permettant d'utiliser presque n'importe lequel antivirus.
- Intégration à j-chkmail d'une bibliothèque antivirus – que des inconvénients. Les principaux sont le besoin de recompiler et réinstaller j-chkmail à chaque nouvelle version de la bibliothèque et la difficulté de débogage
  - ClamAV (`./configure --with-clamav=PATH`)
  - Sophos SAVI (`./configure --with-sophos=PATH`)
- Gestion avancée de la quarantaine plus le fichier de log j-xreport, par un programme externe. A faire – contrib ???

Interface scanneur anti-virus

```
# SCANNER_ACTION
#     VALUES :  OK  REJECT  NOTIFY  DISCARD  X-HEADER
SCANNER_ACTION              OK

# SCANNER_SOCK
#     Communication socket between j-chkmail and external scanner
#  Syntax : inet:PORT@HOSTNAME | local:SOCKET_PATH
SCANNER_SOCK                inet:2002@localhost

# SCANNER_PROTOCOL
#     Protocol
#     VALUES :  INTERNAL  CLAMAV
SCANNER_PROTOCOL            CLAMAV

# SCANNER_TIMEOUT
#     Timeout waiting for the scanner answer
SCANNER_TIMEOUT             15

# SCANNER_MAX_MSG_SIZE
#     Max message size to pass to scanner
SCANNER_MAX_MSG_SIZE        100000

# SCANNER_SAVE
#     Shall messages be quarantined ???
#     VALUES :  NO  YES
SCANNER_SAVE                YES
```

Utilisation bibliothèque integrée

- ClamAV

```
#     libclamav - from ClamAV - VALUES :  OK  REJECT  NOTIFY  DISCARD  X-HEADER
CLAMAV_ACTION              OK

#     ClamAV database directory
CLAMAV_DBDIR               /opt/clamav/db

#     Quarantine ClamAV detected virus - VALUES :  NO  YES
CLAMAV_SAVE                YES

#     Max Filesize to scan (0 = no limit)
CLAMAV_MAXSIZE             0
```

- Sophos

```
#     libsavi - from Sophos - VALUES :  OK  REJECT  NOTIFY  DISCARD  X-HEADER
SOPHOS_ACTION              OK

#     Quarantine Sophos detected virus - VALUES :  NO  YES
SOPHOS_SAVE                YES

#     Max Filesize to scan (0 = no limit)
SOPHOS_MAXSIZE             0
```

Filtrage comportementale et de conformité

Contrôle de Cadence

- Limitation du nombre de connexions ou destinataires sur une fenêtre de 10 min
- Configuration :
  - Activation dans le fichier j-chkmail.cf

```
CHECK_THROTTLE                  NO
CHECK_THROTTLE_CONN             NO
CHECK_THROTTLE_RCPT             NO
OBS : CHECK_THROTTLE = CHECK_THROTTLE_CONN | CHECK_THROTTLE_RCPT
```

  - Définition des limites dans j-chkmail.cf

```
CONN_THROTTLE_FROM_DOMAIN      200
CONN_THROTTLE_FROM_LOCAL       300
CONN_THROTTLE_FROM_FRIEND      100
CONN_THROTTLE_FROM_UNKNOWN      10

RCPT_THROTTLE_FROM_DOMAIN      200
RCPT_THROTTLE_FROM_LOCAL       300
RCPT_THROTTLE_FROM_FRIEND      100
RCPT_THROTTLE_FROM_UNKNOWN      25
```

Contrôle de cadence

- Définition des limites dans j-policy.txt

```
ConnRate:194.214.158        100
NetClass:194.214.158        FRIEND
ConnRate:FRIEND             50
ConnRate:ensmp.fr           30

NetClass:10.3.5             DEPMATH
ConnRate:DEPMATH            40

RcptRate:194.214.158        100
NetClass:194.214.158        FRIEND
RcptRate:FRIEND             50
RcptRate:ensmp.fr           30

NetClass:10.3.5             DEPMATH
RcptRate:DEPMATH            40
```

Contrôle de Cadence

- Mettre dans les classes LOCAL et DOMAIN les machines connues
- Surveiller, pendant quelque temps, le fonctionnement du filtre (j-printstats -ttd)
- Définir les limites en fonction des observations
- Si des adresses IP non locaux mais connus dépassent **fréquemment** les limites, les ajouter dans la classe FRIEND

```
martins@paris:~> j-printstats -ttd | more
...
                    -      CONNECT     :       RCPTS      : HOST NAME
   HOST ADDRESS     -  01m   10m   01h :  01m   10m   01h :
 . 81.255.43.92     -    4   187  1173 -    0     0     0 :
 . 193.49.22.101    -    5    38   271 -    5    37   256 : evry
 . 127.0.0.1        -    2    23   126 -    2    23   126 : localhost
 . 10.3.50.2        -    1    17   105 -    2    34   210 : net-adm
 . 83.205.161.72    -    0    13    13 -    0     8     8 : AToulon-151-1-34-72.w83-205.abo.wanadoo.fr
 . 129.199.96.40    -    1     9     9 -    2    18    18 : nef2.ens.fr
 . 193.48.180.100   -    2     9    51 -    3    13    80 : fontainebleau
 . 194.214.158.228  -    0     8    28 -    0    15    55 : w8
 . 194.214.158.75   -    0     6    20 -    0    10    31 : cep
 . 213.154.79.14    -    0     6    12 -    0     1     7 :
 . 195.157.101.65   -    0     4    24 -    0     4    24 : dh070-00.web.dircon.net
 . 193.252.22.25    -    0     4     8 -    0     4     8 : smtp6.wanadoo.fr
 . 81.80.49.99      -    0     4     4 -    0     3     3 : 3eme-meudon.rain.fr
```

Nombre de connexions ouvertes

- Limite dans le nombre de connexions ouvertes par un meme client
- Utile pour détection d'attaques de déni de service
- Configuration dans j-chkmail.cf

```
CHECK_OPEN_CONNECTIONS      YES
OPEN_CONN_FROM_DOMAIN       30
OPEN_CONN_FROM_LOCAL        30
OPEN_CONN_FROM_FRIEND       15
OPEN_CONN_FROM_UNKNOWN      6
```

- Configuration dans j-policy.txt

```
ConnOpen:10.3               30
ConnOpen:ensmp.fr           20
ConnOpen:LOCAL              10
```

Petits checks entre amis...

```
# Pattern matching (ces options seront surement changées ou regroupées dans la version 1.8 finale)
#     VALUES :  NO  YES
CHECK_HEADERS_CONTENT      YES
CHECK_HELO_CONTENT         YES
CHECK_FROM_CONTENT         YES

# Existence de certains en-têtes (pas vraiment effectif)
#     VALUES :  OK  REJECT  TEMPFAIL
NO_TO_HEADERS              OK
NO_FROM_HEADERS            OK
NO_HEADERS                 OK

# Les destinataires accessibles uniquement à partir des réseaux connus
# CHECK_LOCAL_USERS (utilise fichier j-local-users)
#     VALUES :  NO  YES
CHECK_LOCAL_USERS          NO
```

Petits checks entre amis...

- Limitation du nombre de connexions vides par client SMTP

```
## CHECK_EMPTY_CONNECTIONS
#     Check the number of empty connections (YES ou NO)
CHECK_EMPTY_CONNECTIONS    NO
#     Maximum number of empty connections over 4 hours
MAX_EMPTY_CONN             20

# CHECK_BADRCPTS
#     Vérifie le nombre de Bad Recipients (YES ou NO)
CHECK_BADRCPTS             NO
#     Maximum number of Bad Recipients over 4 hours
MAX_BADRCPTS               20

# CHECK_BADEHLO
#     Check EHLO command parameter (YES ou NO)
CHECK_BADEHLO              NO

# CHECK_BAD_NULL_SENDER
#     Check Bad '<>' Sender Address (YES ou NO)
CHECK_BAD_NULL_SENDER      NO
```

-

Petits checks entre amis...

- Limitation du nombre de connexions vides par client SMTP

```
# CHECK_BAD_SENDER_MX
#     Check Bad Sender MX (YES ou NO)
CHECK_BAD_SENDER_MX        NO

# CHECK_DATE_IN_FUTURE
#     Check if message date is in the future (YES ou NO)
CHECK_DATE_IN_FUTURE       NO

# SPAMTRAP_RESULT
#     Result from SPAM TRAP check (OK  REJECT  TEMPFAIL)
SPAMTRAP_RESULT            OK

# CHECK_SPAMTRAP_HISTORY
#     Reject connections from clients sending messages to spam traps (YES ou NO)
CHECK_SPAMTRAP_HISTORY     NO

# CHECK_NB_RCPT
#     Check the number of recipients for each message (YES ou NO)
CHECK_NB_RCPT              NO
MAX_RCPT_FROM_DOMAIN       300
MAX_RCPT_FROM_LOCAL        1000
MAX_RCPT_FROM_FRIEND       200
MAX_RCPT_FROM_UNKNOWN      25
```

Petits checks entre amis...

- Limitation du nombre de connexions vides par client SMTP

```
# RESOLVE_FAIL
#     What to do if client DNS resolution fails or is forged (OK REJECT TEMPFAIL)
RESOLVE_FAIL                OK
RESOLVE_FORGED              OK

#     Quotas de connexions acceptées
RESOLVE_ACCEPT_06H          9
RESOLVE_ACCEPT_12H          10
RESOLVE_ACCEPT_18H          11
RESOLVE_ACCEPT_24H          12
```

-

Filtrage de contenu – (anti SPAM)

Configuration Filtrage de contenu

- Textuel
  - Recherche textuelle (Expressions régulières – Pattern Matching)
  - Filtrage de URLs
- Oracle (filtre heuristique)

Configuration

- Pattern Matching SPAM_REGEX
- Filtrage URL SPAM_URLBL (1.8)
- Filtrage Heuristique SPAM_ORACLE
-

```
Activation : CONTENT_CHECK = SPAM_ORACLE et SPAM_URLBL et SPAM_REGEX
CONTENT_CHECK               YES
SPAM_ORACLE                 NO
SPAM_REGEX                  NO
SPAM_URLBL                  NO                      v1.8 *


SPAM_REGEX_SCORE            50
SPAM_REGEX_MAX_MSG_SIZE     40000

# Actions dépendantes du score REGEX et URLBL
#     VALUES :  OK  REJECT  DISCARD  X-HEADER
LO_SCORE_ACTION             X-HEADER

HI_SCORE_ACTION             X-REJECT
```

Expressions régulières - REGEX

```
ANYWHERE  5  viagra
BODY     25  <IMG[^>]{1,160}><BR><IMG[^>]{1,160}><BR><IMG[^>]{1,160}>
SUBJECT  50  SEXUALLY[ -]EXPLICIT
URLEXPR  10  seduction[^ />]*\.(com|biz)
URLEXPR  10  [a-z]+[0-9]{2,5}(biz|drug[s]?|medications|rx|meds|tabs|pill[s]?)\.(biz|us)
URLSTR   50  bigbonus-casino.net
```

- Règles :
  - Pas plus de quelques centaines d'expressions regulières
  - Des expressions spécifiques sont bien plus rapides que des expressions générales
  - *get.{1,40}(doctorate|university).{1,40}diploma* mieux que *get.*(doctorate|university).*diploma*

URLBL – liste noire d'URLs

- Source des données (j-chkmail.cf)
  - DNS_URLBL multi.surbl.org

    Plus facile à mettre en oeuvre – crée des dépendances externes
  - DB_URLBL /etc/mail/jchkmail/j-urlbl.db

    Pas de dépendance externe (seulement pour sa mise à jour) – plus rapide si localisée sur un disque rapide (astuce : mettre dans RAMdisk ou simplement copier dans /tmp sous Solaris)
- Récupération bases URL – deux ou trois fois par jour
  - Scripts /etc/mail/jchkmail/get-urlbl et Makefile

```
RSYNCSERVER="j-chkmail.ensmp.fr:1873"
rsync rsync://$RSYNCSERVER/urlbl/j-urlbl.txt /tmp/
if [ "$?" = "0" ] ;
then
   mv j-urlbl.db j-urlbl.db.old
   j-makemap -b j-urlbl.db < /tmp/j-urlbl.txt
   j-ndc reload databases
fi
```

Filtrage de contenu – Marquage des messages

- Calcul du Score :
  - Score_msg = (Score_regex + Score_URLBL) / 5 + Score_oracle
  - Ex : Score_regex = 5, Score_URLBL = 20, Score_oracle = 2 -> Score_msg = 7
- Ajout d'un en-tête

```
X-j-chkmail-Score: MSGID : 42A420CE.002 on paris : j-chkmail score : XXXXXXXX : 20/50 4
```

- Marquage du Subject

```
SCORE_ON_SUBJECT              YES
SCORE_ON_SUBJECT_THRESHOLD    3
SCORE_ON_SUBJECT_TAG          [JUNK???]
```

  - Si *SCORE_ON_SUBJECT_TAG* est vide, le marquage est de la forme *[J-XXX]*

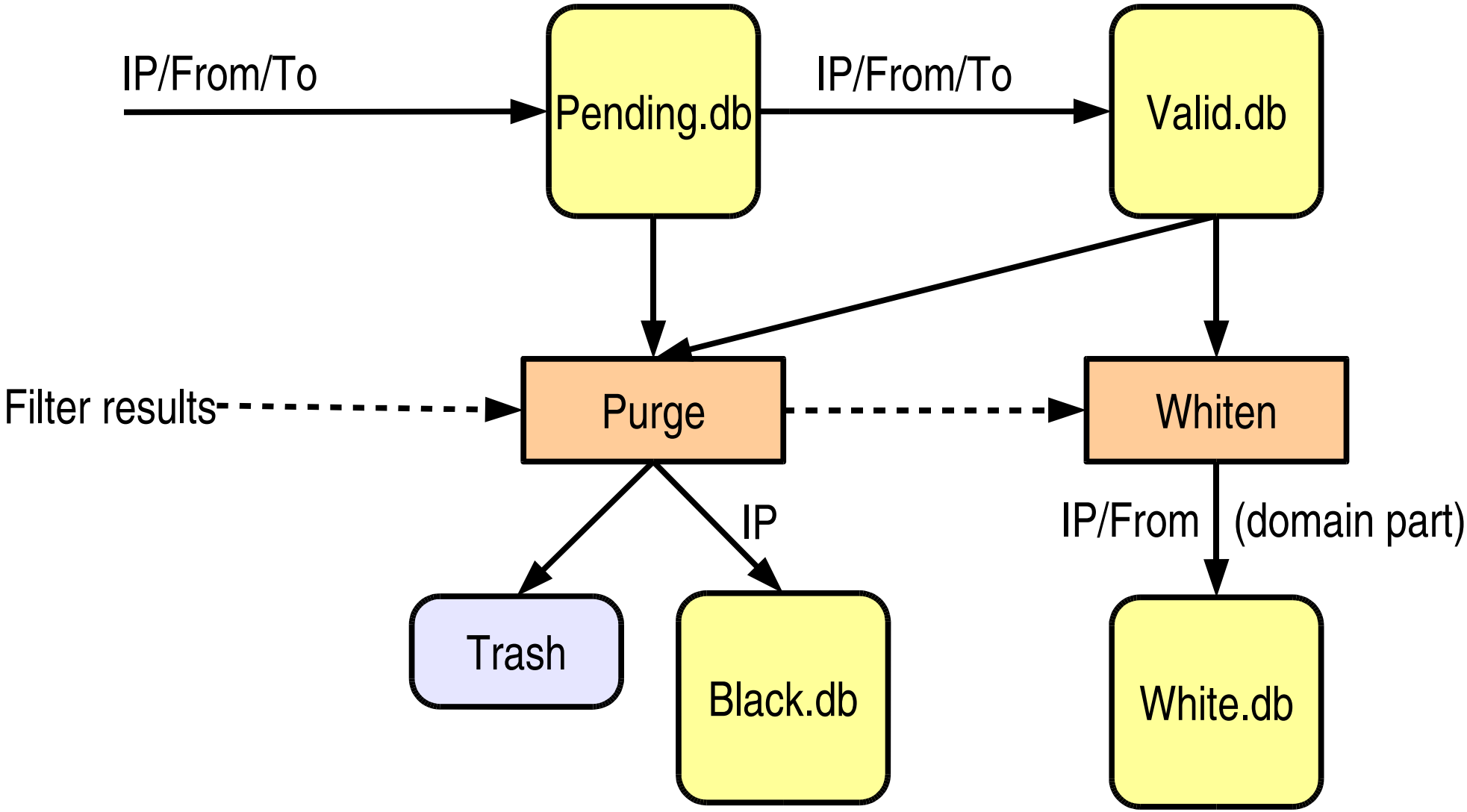
Filtrage sur le poste client

-
  - Si Expediteur connu
    - met message dans *«Inbox»*
  - Si *«List-ID»* contient *«cru.fr»*
    - Met message dans *«Listes-CRU»*
  - ...
  - Si *«X-j-chkmail-score»* contient *«XXXX»*
    - Met dans *«Score-HI»*
  - Si *«X-j-chkmail-score»* contient *«X»*
    - Met dans *«Score-LO»*
  - Sinon
    - Met dans *«Inbox»*

Adaptive Delay Greylisting – en cours...

- Greylisting classique a des problèmes d'échelle pour traitement de gros trafic :
  - Facile à empoisonner la base de triplets en attente
  - Bases trop importants si très gros trafic (compromis entre taille de base acceptable et qualité de son contenu)
- Adaptive Delay Greylisting cherche à diminuer la taille des bases
  - Attribution de durées de vie variables en fonction de la «qualité» du triplet
  - Génération plus «intelligente» de la liste blanche
  - Coopération avec les autres méthodes de filtrage de j-chkmail
- Modes de fonctionnement :
  - STANDALONE : le client gère seul sa base de données greylisting
  - CLIENT/SERVEUR : le client a une base locale qui représente son historique. Le serveur contient le historique de tous les clients. Lorsqu'un client ne trouve pas l'information en local, il consulte le serveur.

Adaptive Delay Greylisting



Configuration (version classique)

```
#     Greylist default activation (NO | YES)
GREY_CHECK                NO

#     Greylist mode ( STANDALONE | CLIENT )
GREY_MODE                 STANDALONE
#     Remote Greylist Server Socket when running in CLIENT mode
GREY_SOCKET               local:/var/jchkmail/j-greyd.sock
#     Timeout to connect go j-grey server when running in CLIENT mode
GREY_CONNECT_TIMEOUT      10s

#     Greylist delay for normal messages
GREY_MIN_DELAY_NORMAL     10m
#     Greylist max age for pending entries (normal messages)
GREY_MAX_DELAY_NORMAL     3d
#     Greylist delay for null sender messages
GREY_MIN_DELAY_NULLSENDER   10m
#     Greylist max age for pending entries (null sender messages)
GREY_MAX_DELAY_NULLSENDER   24h
#     Greylist max age for inactive valid entries (normal messages)
GREY_MAX_AGE_NORMAL       1w
#     Greylist max age for inactive valid entries (null sender messages)
GREY_MAX_AGE_NULLSENDER    4h
```

Configuration (version classique)

```
#     Max normal pending messages
GREY_PENDING_NORMAL        1000
#     Max null sender pending messages
GREY_PENDING_NULLSENDER    1000

#     How to construct IP part of ntuple ( NONE | FULL | NET )
GREY_IP_COMPONENT          NET
#     How to construct FROM part of ntuple ( NONE | FULL | HOST | USER )
GREY_FROM_COMPONENT        FULL
#     How to construct FROM part of ntuple ( NONE | FULL | HOST | USER )
GREY_TO_COMPONENT          USER

# GREY_REPLACE_NULLSENDER
#     Set To value to From value if NULL SENDER
#     VALUES :  NO  YES
GREY_REPLACE_NULLSENDER    NO

#     Greylist database cleanup interval
GREY_CLEANUP_INTERVAL      10m

#  Clean up checks : ( None BadResolve DomainMatch BadRCPT SpamTrap BadMX BadClient Spammer All )
GREY_DEWHITE_FLAGS         None
```

Autres options de configuration

- Communication entre j-chkmail et sendmail

```
#  Syntax : inet:PORT@HOSTNAME | local:SOCKET_PATH
SOCKET                      local:/var/run/jchkmail/j-chkmail.sock
#     Timeout before closing a sendmail connection
SM_TIMEOUT                  7200
```

- Identité sous laquelle tourne le filtre

```
#     Filter USER ID
USER                        smmsp
#     Filter GROUP ID
GROUP                       smmsp
```

- Taille de l'historique long

```
#     Number of entries of history (times 1024)
HISTORY_ENTRIES             128
```

- Gestion de la quarantaine

```
#     Quarantine directory clean-up interval
CLEANUP_INTERVAL            21600
#     Quarantine
QUARANTINE_MAX_AGE          86400
```

```
#     syslog facility
LOG_FACILITY               local5
#     j-chkmail log level
LOG_LEVEL                  10

#     Automatically reload configuration data (time interval)
AUTO_RELOAD_TABLES         3600


# DB_CACHE_SIZE
#     BerkeleyDB database cache size
DB_CACHE_SIZE              512000

#     Number of file descriptors (integer value or MAX)
FILE_DESCRIPTORS           MAX
#     Available file descriptors soft lower bound
FD_FREE_SOFT               100
#     Available file descriptors hard lower bound
FD_FREE_HARD               50
#     Available file descriptors limited by select function  ( NO | YES )
USE_SELECT_LIMIT           YES
```

Conclusions

- Bientôt, une interface web pour configurer j-chkmail – contribution de Eric Le Seac'h
- Merci de votre attention
- Questions ???