Le projet ClamAV

« How I learned to stop worrying and love my mail »

Guillaume Arcas <guillaume.arcas@free.fr>

Plan

- Présentation du projet ClamAV
- Fonctionnalités
- Architecture
- Installation & configuration
- Positionnement
- ClamAV dans la pratique
  - Protection du poste de travail
  - Passerelle SMTP
  - Passerelle HTTP
  - Autres protocoles
- En guise de conclusion
- Liens

Présentation

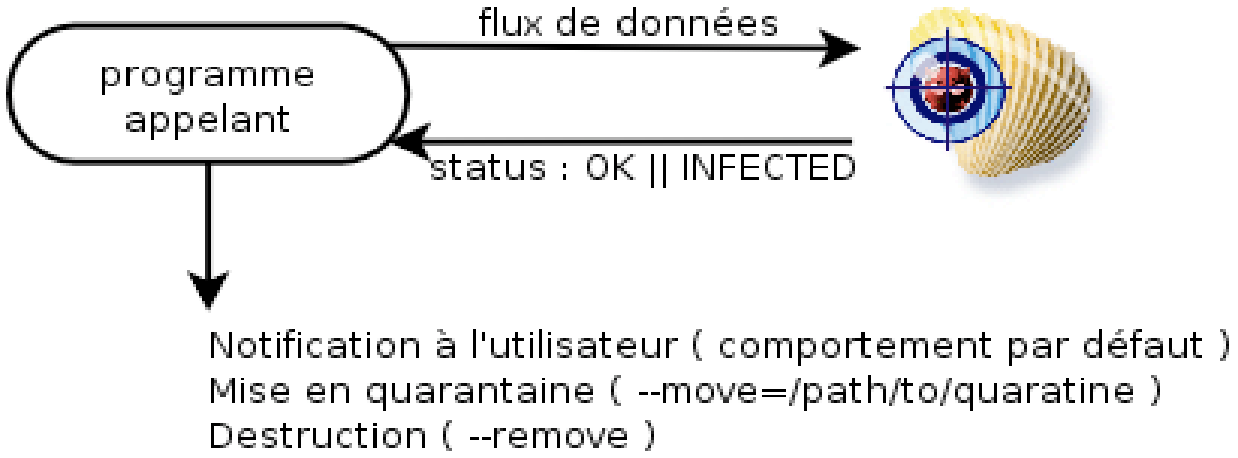
- Le projet ClamAV
  - Antivirus pour Unix distribué sous licence GPL
    - Portage pour plate-formes MS Windows
  - Initialement dédié à l'analyse des flux SMTP, ClamAV fournit un moteur d'analyse qui peut être utilisé en ligne de commande ou sous forme de démon.
  - La librairie libclamav permet l'appel des fonctions d'analyse depuis des applications externes.
  - Un effort important est mis sur la maintenance d'une base de signatures à jour.
  - 30.000 virus reconnus

Fonctionnalités

- Analyse de fichiers par recherche de signatures
- Support des formats d'archive et de compression courants :
  - zip, rar, tar, gzip, bzip2, MS Cabinet/CHM/SZDD
- Support des formats Portable Executable :
  - UPX, FSG, Petite
- Support des formats de BAL mailbox et Maildir
- Base de signatures généralement à jour, parfois la première (SoBig.I)

Architecture

- Principes de fonctionnement :
  - Les fichiers analysés sont passés au crible des signatures de la base locale
  - Le moteur retourne leur status ; OK ou INFECTED
  - Le programme appelant prend la décision.
    - Exemple
      - Clamscan : notification, mise en quarantaine ou destruction



Installation 1/3

- A partir du code source :
  - GNU/Linux
  - FreeBSD
  - OpenBSD
    - ClamAv fera son entrée dans l'arbre des ports de la 3.7
  - HPUX, AIX, Solaris, IRIX, SCO
  - Mac OS X
  - CygWin
- Paquetages précompilés disponibles pour :
  - Debian, Red Hat, Mandrake, FreeBSD/NetBSD/OpenBSD
  - Microsoft Windows
    - clamwin.sourceforge.net, élu Project of the month February 2005

Installation 2/3

- Pré-requis pour une installation à partir du code source
  - Librairies zlib
    - Si possible une version > 1.2.1
      - Contournement : --disable-zlib-vcheck
  - Librairies GNU MP 3
    - Vérification des bases de signatures
      - Contournement : --disable-dsig
  - Librairies bzip2
  - Utilisateur et groupe clamav
    - Sauf si installation dans un compte Utilisateur
      - ./configure –prefix=/home/joe –disable-clamav

Installation 3/3

- Quelques options de compilation utiles :
  - Compilation du filtre sendmail
    - --enable-milter
  - Support du mode « analyse à la volée »
    - Pour Linux et FreeBSD
    - --enable-clamuko
  - Trilogie configure/make/make install

Configuration 1/3

- Deux fichiers :
  - [/etc/]clamd.conf :
    - Paramètres de configuration du démon clamd et des programmes associés
  - [/etc/]freshclam.conf :
    - Paramètres de configuration de l'utilitaire de mise à jour des bases de signatures.
- Par défaut, les fichiers créés ne sont pas utilisables :
  - Commenter la ligne `Example`

Configuration 2/3

- clamd.conf
  - Journalisation
    - LogFile /path/to/fichier.log
    - LogSyslog
    - LogFileMaxSize (0 : nolimit)
    - LogTime
  - Connexion au démon
    - Socket
      - LocalSocket /path/to/clamav.sock
    - TCP
      - TCPSocket 3310 (valeur par défaut)

Configuration 3/3

- clamd.conf (suite)
  - Gestion des ressources
    - MaxConnectionQueueLength
    - StreamMaxLength
    - MaxThreads
  - Sécurité
    - SelfCheck
    - ExitOnOOM
    - ArchiveMaxRecursion, ArchiveMaxFileSize, etc.
    - ArchiveBlockEncrypted

Mises à jour 1/2

- Tâche essentielle : Pas de signature, pas de détection.
- Risques :
  - Absence de signature
    - Réactivité des *maintaners* ClamAV
      - Premier antivirus à fournir une signature pour le ver SoBig.I
    - Disponibilité des serveurs
      - Plusieurs miroirs (round-robin DNS)
    - Intégrité des bases de signatures
      - Vérification des signatures (librairie GNU MP)

Mises à jour 2/2

- Freshclam
  - Mode démon : freshclam -d
  - Crontab
  - Configuration : [/etc/]freshclam.conf
  - Enregistrement TXT sur current.cvd.clamav.net
  - current.cvd.clamav.net. 275 IN TXT "**0.83:29:752:1110216729**“
    - 0.83 : version de clamav
    - 29 : n° version de la base main.cvd
    - 725 : n° version de la base daily.cvd
    - 1110216729 : horodatage Epoch
  - Rechargement Clamd après mise à jour
    - NotifyClamd

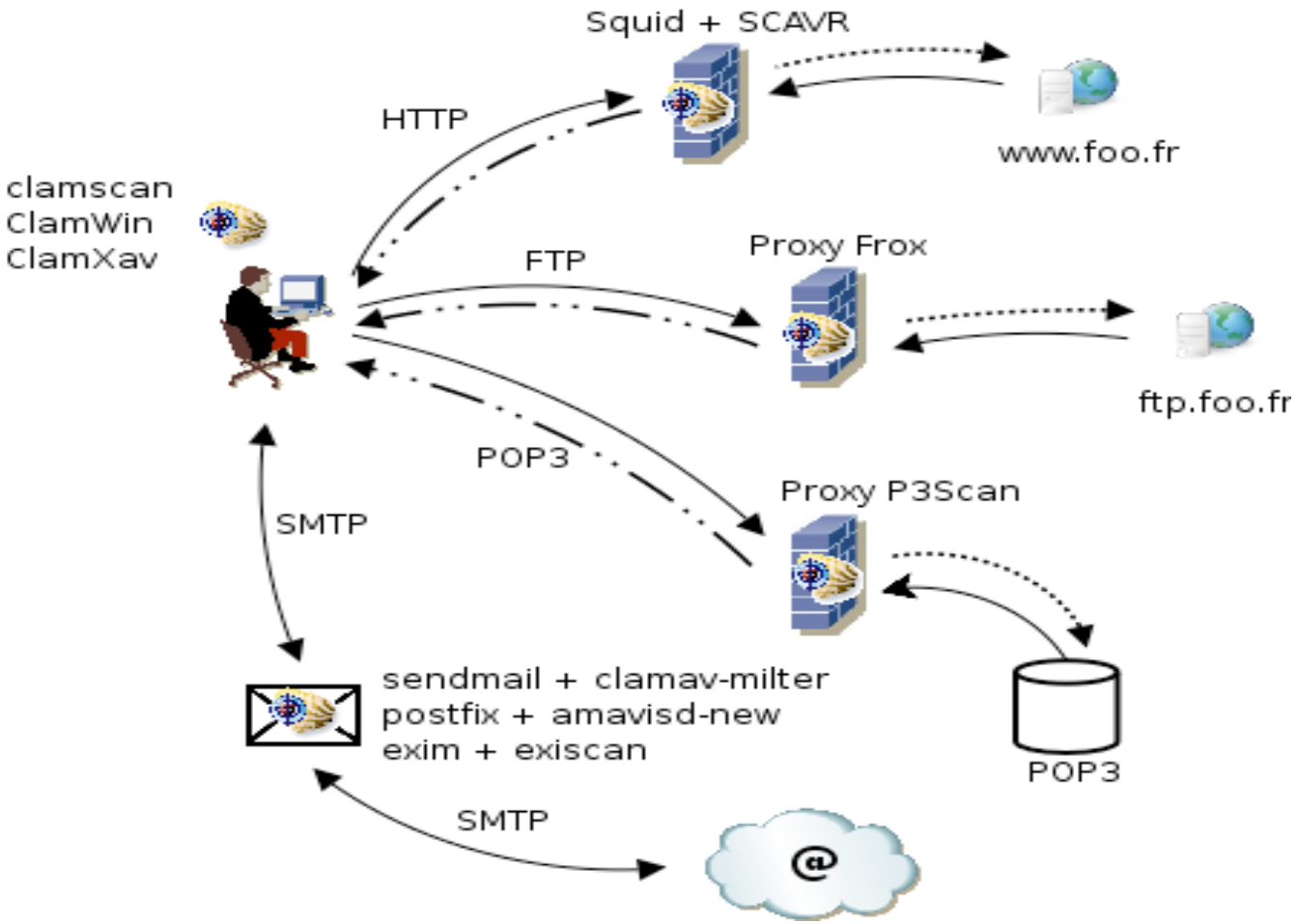
Signatures 1/2

- Les signatures ClamAV sont distribuées dans deux fichiers binaires : main.cvd et daily.cvd.
- L'utilitaire sigtool permet :
  - de lire les attributs d'un fichier CVD
    - $ sigtool -i main.cvd
      Build time: 10 Mar 2005 22-01 +0100
      Version: 761
      # of signatures: 481
      Functionality level: 4
      Builder: ccordes
      MD5: c65a6fd33813ebcb33d3c901669b2c2
      Digital signature:ArCQ3k4W/Ki4R14iohPB5trT <truncated>
      Verification OK.
  - d'afficher les noms des virus reconnus :
    - $ sigtool -l main.cvd
      <snip>
      Gen.1701.1704 Cascade - Version B
      Gen.1701.B
      Gen.1701.Cascade - Version A
      Gen.1704.Cascade - Format
      Gen.1704.Cascade - Version A
      Gen.1706
      _1707_0001_000
      </snip>
- Sigtool est utilisé par les développeurs ClamAV pour construire et signer les fichiers CVD.

Signatures 2/2

- Sigtool permet de « décompiler » (option -u) un fichier CVD et d'en extraire les fichiers texte suivants :
  - main.hdb
    - Contient les empreintes MD5 des fichiers infectés
    - Format : checksum:size:virus_name
    - Exemple :
      e35ee4383d38eef5fbe135dee9598716:451007:Trojan.Banker-21
  - main.db
    - Contient les signatures hexadécimales
    - Format : virus_name:hexa_sig
    - Exemple :
      Trojan.URLspoof.gen\
      (Clam)=6c6f636174696f6e2e687265663d756e6573636170652827*3a2f2f*25303140*2729
  - main.ndb
    - Contient les signatures hexadécimales étendues
    - Format : virus_name:target_type:offset:hexadecimal_sig[:function_level]
    - Exemple :
      Worm.Mydoom.Gen-1:1:*:a3d6d<snip>d4769{-50000}0<snip>f:3
  - main.zmd
    - Règles pour les archives ZIP chiffrées
    - Exemple :
      # virname:encrypted:filename:normal size:csize:crc32:cmethod:fileno:maxdepth
      Worm.Padowor.A-zippwd:1:*:72767:69779:5f6f7a3f:*:1:1

Positionnement



ClamAV dans la pratique

Protection du poste de travail

- Deux modes :
  - A la volée
    - Utilisation du module Dazuko pour Linux/FreeBSD
      - Les fichiers peuvent alors être analysés lors de leur écriture sur disque, lecture ou accès.
      - Fonctionne mais absence parfois de messages clairs pour l'utilisateurs
  - A posteriori
    - Utilisation des utilitaires clamscan et clamdscan
      - En ligne de commande ou par crontab

Exemple

Clamscan / clamdscan

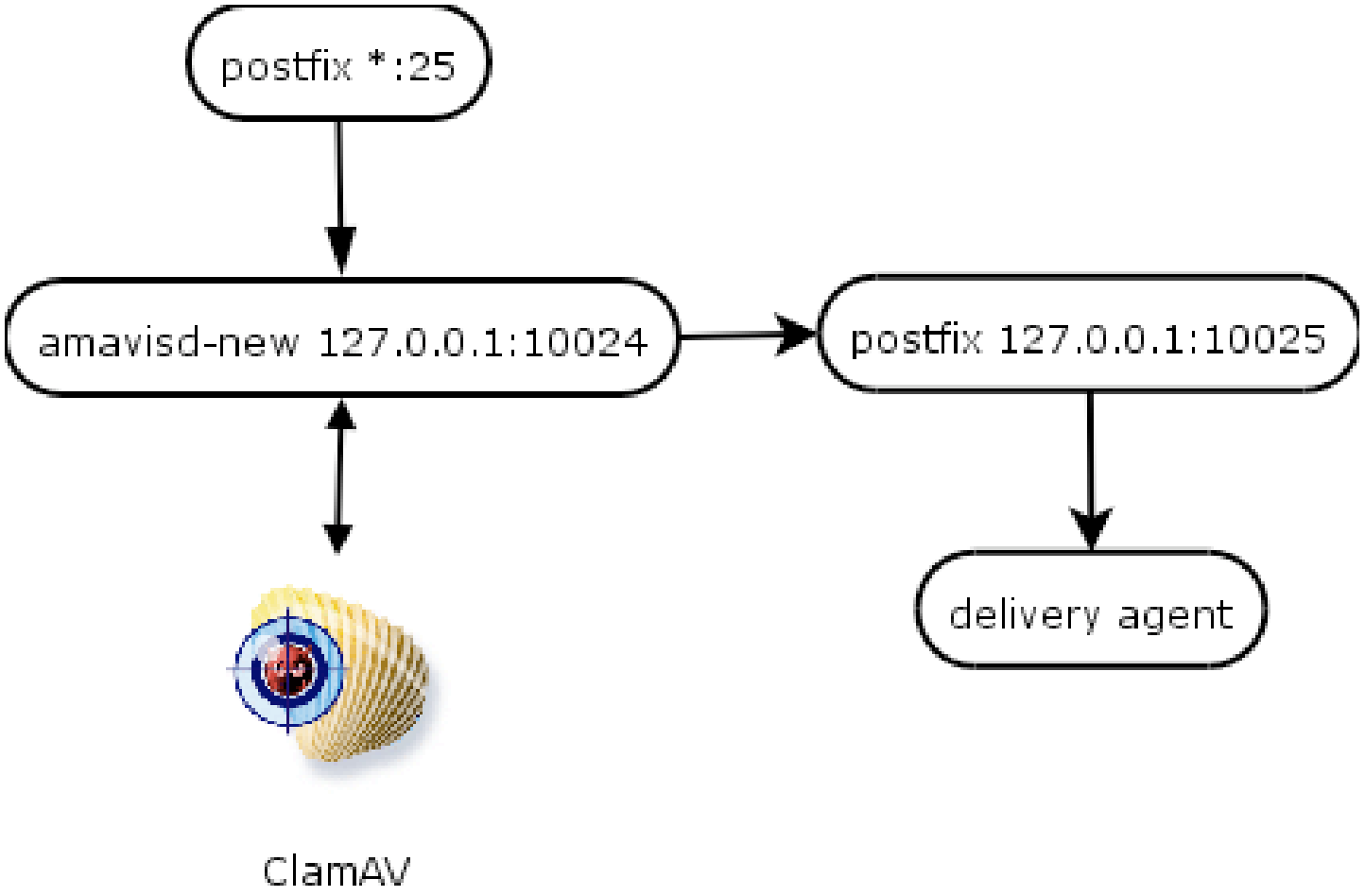
Passerelle SMTP 1/3

- ClamAV / Sendmail
  - Utilisation du milter clamav-milter
    - Il est alors conseillé de désactiver le support de clamuko
      - ./configure –enable-milter –disable-clamuko
    - Configuration Sendmail
    - INPUT_MAIL_FILTER(`clmilter',`S=local:/var/run/clmilter.sock, F=, T=S:4m;R:4m')dnl define(`confINPUT_MAIL_FILTERS', `clmilter')
    - Configuration Clamd
    - /etc/clamd.conf : LocalSocket /var/run/clmilter.sock
    - Configuration clamav-milter
    - /usr/local/sbin/clamav-milter -lo /var/run/clmilter.sock

Passerelle SMTP 2/3

- ClamAV / PostFix / Amavisd-new
  - Configuration PostFix
    - master.cf
      - Déclaration smtp-amavis
    - main.cf
      - `content_filter=smtp-amavis:[127.0.0.1]:10024`
  - Amavisd-new
    - amavis.conf
      - Déclaration de ClamAV comme antivirus
        - » Socket ou port TCP (si chroot)

Passerelle SMTP 3/3



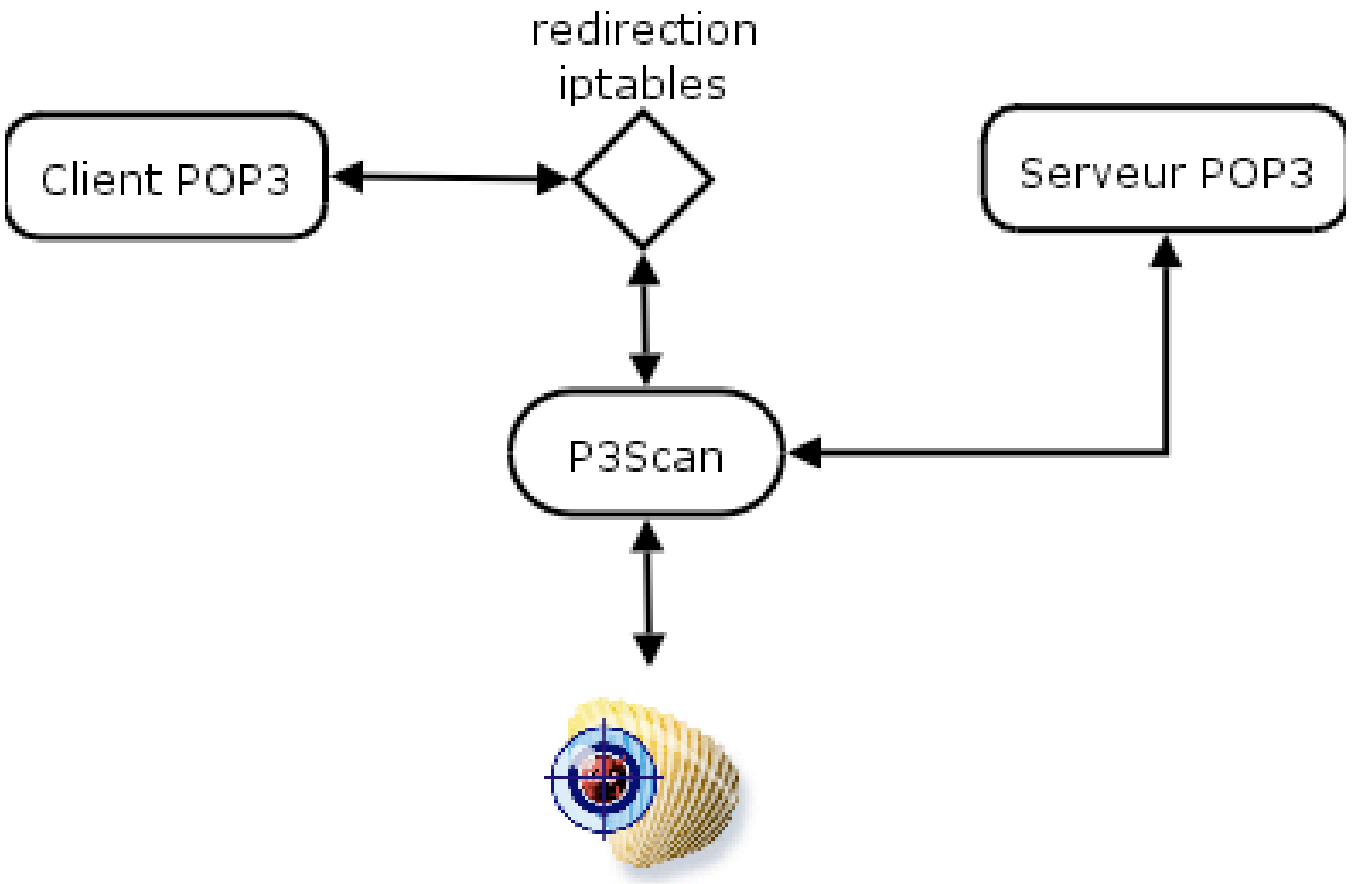
Protection HTTP

- Pourquoi ?
  - Redirecteur de connexions
  - Appliquettes Java mal-intentionnées
  - Virus récupérés via Webmail
- Comment ?
  - Association Squid / ClamAV
    - SafeSquid : gratuit mais pas OpenSource/Libre
    - SCAR : redirecteur Python pour Squid
    - SquidClam : encore en phase de développement, réécriture en C de SCAVR
  - Association Apache/ClamAV
    - Mod_clamav

Autres protocoles

- Principe :
  - Redirection de flux vers un proxy
  - Utilisé pour analyser
    - POP3 : P3scan
    - FTP : Squid ou Frox

Exemple de redirection



En guise de conclusion

- Premier projet d'antivirus OpenSource/Libre qui « tient » la route
- Gestion un peu arbitraire des mises à jour
  - Messages OUT OF DATE
  - Compilation peu souple (jusqu'à récemment)
    - Mais est-ce un défaut ?
  - 3 mises à jour en 15 jours 0.80 > 0.83
- Signatures à jour
- Peu de mécanismes en dehors de l'analyse par signatures
    - Mais est-ce un défaut ?
- Projets à suivre :
    - Snort-inline (2.3.0) et preprocessor clamav
      - Ebauche d'IPS

Liens

- Projet ClamAV : http://www.clamav.net
- Liste « exhaustive » des applications externes : http://www.clamav.net/3rdparty.html