SquidGuard

(Filtrage web)

RTLs BAO XII à Lomé **Roger Yerbanga**

Janvier 2012

Introduction (1)

- Obligations légales de nos abonnés :
  - « adultes »
  - drogues
  - pari en ligne
  - hacking et phishing
  - racistes, antisémites, inçitant à la haine, ...
  - ...
- Sensibilisations et informations auprès des abonnés
- Filtrage des URLs nécessaires au bon usage des outils informatiques.

Introduction (2)

- SquidGuard se grèffe à Squid comme redirecteur
- Possède une base de données de plusieurs catégories de sites web (listes noires et listes blanches)
- Analyse chaque requêtes squid, et décider d'interdire ou pas (Filtrage)
- Filtrage : souvent fonction de l'URL distant, de la source, et de l'heure.

Installation - Debian

- Simple comme Bonjour
-
- *# aptitude install squidguard*
-

Gestion des listes noires (1)

- On ne va pas créer les listes à la main
- Plusieurs listes listent déjà plusieurs centaines de milliers voire millions de sites :
  - http://www.shallalist.de/
  - http://cri.univ-tlse1.fr/documentations/cache/
  - http://squidguard.mesd.k12.or.us/blacklists.tgz
  - http://urlblacklist.com/?sec=download
  - http://squidguard.mesd.k12.or.us/blacklists.tgz
  - http://www.bn-paf.de/filter/de-blacklists.tar.gz
- Utiliser une liste
- Et la maintenir à jour (à l'aide de script)
- Avoir le moyen de faire des exceptions locales

Gestion des listes noires (2)

- Liste de l'université de toulouse :
- # *cd /tmp*
- # *wget http://cri.univ-tlse1.fr/blacklists/download/blacklists*
- # *tar xvf blacklists.tar.gz*
- # *mv blacklists/* /var/lib/squidguard/db/*
  - Copie des catégories dans la base de données
- # */usr/sbin/update-squidguard*
  - Génération de la base de données

Gestion des listes noires (3)

- Le script : maj_listesnoires
-

```
#!/bin/bash
cd /tmp
rm -Rf blacklist* >/dev/null 2>&1
wget http://cri.univ-tlse1.fr/blacklists/download/blacklists.tar.gz
if [ -f /tmp/blacklists.tar.gz ]; then
    tar xf blacklists.tar.gz
    cp -au blacklists/* /var/lib/squidguard/db/ >/dev/null 2>&1
    /usr/sbin/update-squidguard >/dev/null 2>&1
fi
```

- A faire tourner 1 fois par mois ou par semaine avec 1 cron

Questions ???

Config : gestion des filtrages (1)

- Fichier ***/etc/squid/squidGuard.conf***
- Autorisation ?
- Interdiction ?
- Depuis quelle source ?
- Vers quelle catégorie de site ?
- Pour quelle période de la journée ?

Config : gestion des filtrages (2)

- **Déclarations des temps :**
- *time <nom> {*
  Spécification1
  Spécification2
  …
  }
- *Exemples*
- *time **workhours** {*
  weekly mtwhf 08:00 – 17:30
  }
- *time **jour_an** {*
  *date *.01.01 00:00 - 24:00*
  }
- *time **nuit** {*
  *Weekly * 00:00 – 08:00*
  }

Config : exercice

- Trouver les déclarations de temps pour :
  - Week-end
  - Tous les après-midi
  - Pour le jour de la fête du travail
  - Pour le 31 décembre 2012 à minuit

Config : gestion des filtrages (3)

- **Déclarations des groupes de sources et des groupes de destinations :**
- *src <nomdugroupe> {*
- *Spécification1*
  Spécification2
  …
  }
- *Exemples*
- *src* ***bao*** *{*
  ip 10.196.1.0/24 192.168.7.101 192.168.1.101
  }
- *src* ***admin*** *{*
  ip 10.196.1.197 10.196.1.1
  user root foo bar
  within workhours
  }
- *src* ***wifi*** *{*
  ip 172.19.0.0/24
  outside workhours
  domain refer.sn
  }

Config : gestion des filtrages (4)

- **Déclarations des groupes de destinations :**
- *dest <nomdugroupe> {*
  Spécification1
  Spécification2
  …
  }
- *Exemples*
- *dest **adult** {*
  domainlist adult/domains
  urllist adult/urls
  expressionlist adult/expressions
  }
- *dest **agressif** {*
  urllist agressif/urls
  within workhours
  }
- *dest **malware** {*
  domainlist malware/domains
  }

Questions ???

Config : gestion des filtrages (5)

acl *{*

sourcegroupname *[within|outside timespacename] {*

pass [!]destgroupname [...]

[rew|rewrite rewritegroupname [...]

[redirect [301:|302:]new_url] }

sourcegroupname *within|outside timespacename {*

pass [!]destgroupname [...]

[rew|rewrite rewritegroupname [...]

[redirect [301:|302:]new_url]

} ***else*** *{*

pass [!]destgroupname [...]

[rew|rewrite rewritegroupname [...]

[redirect [301:|302:]new_url] }

...

default *[within|outside timespacename] {*

pass [!]destgroupname [...]

[rew|rewrite rewritegroupname [...]

redirect [301:|302:]new_url } }

Config : gestion des filtrages (6)

Exemple d'ACL :

```
  acl {
      admin {
            pass     any }
      dialup {
            pass    white
            pass    !malware !adult !mixed_adult !hacking !phishing all
            redirect http://cache.refer.sn/cgi-bin/squidGuard.cgi?clientaddr=%a+clientname=%n+srcclass=
%s+targetclass=%t }
 cnfd within workhours {
            pass !adult !agressif !astrology !dangerous_material
            pass !gambling !hacking !malware !mixed_adult !phishing !sect
            pass !drogue !black all
            redirect http://cache.refer.sn/cgi-bin/squidGuard.cgi?clientaddr=%a+clientname=%n+srcclass=
%s+targetclass=%t
      }
      default {
            pass !hacking !malware !phishing all
            redirect http://cache.refer.sn/cgi-bin/squidGuard.cgi?clientaddr=%a+clientname=%n+srcclass=
%s+targetclass=%t
      }
}
```

Config : gestion des filtrages (7)

- Section défaut : exécutée par défaut quand rien ne match
- *any* et *all* = tout
- *none* = *!any* = rien
- *in-addr* = une adresse IP
- *!in-addr* = nom de domaine au lieu d'une IP dans l'URL
- Les redirections :
  - *%a* : adresse IP du client
  - *%n* : domaine du client (sinon « unknown »)
  - *%s* : source group du client (sinon « unknown »)
  - *%t* : target groupe du client
  - *%u* : url demandée

Questions ???

Adaptation de la config de squid

- /etc/squid/squid.conf
- Repérer la section url_rewrite :
- Ajouter les lignes :
  - *url_rewrite_program /usr/bin/squidGuard -c /etc/squid/squidGuard.conf*
  - *url_rewrite_children 10*
  - *redirector_bypass on*
- Relancer squid et c'est bon

Questions ???

Questions ???

Questions ???

Exercice

- *Mettre en pratique sur le squid de Lomé*

Documentations

http://www.sdconsult.no/linux/SquidGuard/config.html
http://www.squidguard.org/about.html
http://www.squidguard.org/blacklists.html
http://cri.univ-tlse1.fr/blacklists/
http://cri.univ-tlse1.fr/documentations/cache/squidguard.html
http://www.squidguard.org/Doc/examples.html