Installation d'un serveur proxy

Squid et SquidGard

Aurélien BONNARDON

10/01/2010

Ce document détaille l'installation du serveur proxy Squid et de son plugin SquidGard sous Debian.

Table des matières

Introduction

Un serveur mandataire ou proxy est une machine qui a pour fonction de relayer des requêtes entre un poste client et un serveur. Les serveurs mandataires sont notamment utilisés pour assurer les fonctions de mémoire cache, de logging des requêtes, pour la sécurité du réseau local, pour le filtrage et l'anonymat.

Squid est un proxy capable d'utiliser les protocoles FTP, HTTP, Gopher, et HTTPS. C'est un logiciel libre distribué sous la licence GNU GPL. Squid garde les données les plus fréquemment utilisées en mémoire. Il conserve aussi les requêtes DNS. Il existe un plugin à ce dernier, SquidGard, qui permet de filtrer les informations demandées par les clients.

Les manipulations suivantes ont été faites sous Debian, mais il est possible de l'étendre à d'autres systèmes Unix en adaptant quelques commandes.

1 Squid

1.1 Installation

On installe Squid à partir des paquets Debian :

```
apt-get install squid
```

1.2 Configuration

Le fichier de configuration de Squid est /etc/squid/squid.conf. Voici un exemple complet de configuration, commenté :

```
# Definition du port 3128
http_port 3128

# Nom de la machine
visible_hostname Tryx

# Lignes a mettre
hierarchy_stoplist cgi-bin ?
acl QUERY urlpath_regex cgi-bin \?
cache deny QUERY

#  Fichier de log
access_log /var/log/squid/access.log squid
cache_log /var/log/squid/cache.log

# Fichier du PID (pour un script)
pid_filename /var/run/squid.pid

# Fichier des hosts
hosts_file /etc/hosts

# Taille max du cache
cache_mem 16 MB

# Lignes a mettre
```

```
refresh_pattern ^ftp:           1440    20%     10080
refresh_pattern ^gopher:        1440    0%      1440
refresh_pattern .               0       20%     4320

# Definition des ACL
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl interne src 192.168.4.0/255.255.255.0

acl Safe_ports port 80          # http
acl Safe_ports port 443         # https

acl purge method PURGE
acl CONNECT method CONNECT

# Regles
http_access allow manager localhost
http_access deny manager
http_access allow interne
http_access deny all

# Interdire la connexion à tous les ports exceptés ceux définis par
les acl Safe_ports
http_access deny !Safe_ports

# Autoriser les reponses
http_reply_access allow all

# Group du cache
cache_effective_group proxy

# Adresse de l'administrateur
cache_mgr aurelien.bonnardon@gmail.com

# ?
coredump_dir /var/spool/squid
```

1.3 Authentification et ajout d'utilisateurs

Si l'on souhaite que les utilisateurs s'authentifient auprès du proxy avant de pouvoir l'utiliser, on ajoute la ligne suivante dans le fichier de configuration :

```
auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/passwd
```

Pour ajouter les utilisateurs, on utilise l'outil d'apache htpasswd (il faut qu'Apache soit installé) :

```
htpasswd –c /etc/squid/passwd toto
```

2 SquidGuard

Squidguard est un plugin de Squid. Il permet de filtrer les pages consultées par les utilisateurs. On peut définir des groupes d'utilisateurs à partir de leurs logins (authentification réalisée par Squid) ou

d'adresses IP sources (fixe, réseau, range ou a partir d'un fichier de la base de données). SquidGuard va comparer la destination des requêtes HTTP (URL et domaine) à sa base de données et agir en fonction du comportement configuré grâce à des ACL. Si un utilisateur essaye d'accéder à une page interdite, il se verra redirigé vers une page spécifiée dans la configuration.

2.1 Installation

On l'installe avec la commande :

```
apt-get install squidguard
```

2.2 Intégration à Squid

Dans un premier temps, il faut ajouter la ligne suivante dans le fichier de configuration de Squid pour qu'il prenne en compte SquidGuard :

```
redirect_program /usr/bin/squidGuard -c /etc/squid/squidGuard.conf
```

2.3 Téléchargement d'une liste noire

Nous allons maintenant installer une blacklist référençant un grand nombre de site dont on souhaite interdire l'accès. Nous allons utiliser celle réalisée par l'université de Toulouse, elle est conseillée par le site officiel de SquidGuard :

```
wget http://cri.univ-tlse1.fr/blacklists/download/blacklists.tar.gz

tar zxvf blacklist.tar.gz -C /var/lib/squidGuard/db/

cd /var/lib/squidGuard/db

mv blacklist/* .
```

2.4 Configuration

La configuration de SquidGuard se fait par le fichier spécifié à Squid, /etc/squid/squidGuard.conf. Voici un exemple :

```
# Repertoire de log et de la base de donnees (contenant les
blacklists)
dbhome /var/lib/squidguard/db
logdir /var/log/squidguard

# On definit 2 profils utilisateurs qui doivent être créé dans Squid
src admin {
     user toto
}
src users {
     user tata
}
src clients {
      ip 192.168.4.0/255.255.255.0
}

# Definition des bases de donnees de filtrage utilisees
dest adult {
      domainlist adult/domains
```

```
	urllist adult/urls
}
dest publicite {
	domainlist publicite/domains
	urllist publicite/urls
}
dest warez {
	domainlist warez/domains
	urllist warez/urls
}
dest porn {
	domainlist porn/domains
	urllist porn/urls
}
# ACL
acl {
	admin {
		pass all
	}
	users {
		pass !porn !adult !publicite !warez all
		redirect http://localhost/interdiction.html
	}
	clients {
			pass none
			redirect http://localhost/authentification.html
	}
	default {
		pass none
	}
}
```