Serveur proxy

1. Les serveurs proxy

Un serveur proxy est chargé d'effectuer une requête au nom d'un client vers un autre serveur pour un protocole donné. Le terme français pour proxy est d'ailleurs « mandataire », le serveur étant mandaté pour effectuer une action au nom du client. On dit qu'un serveur proxy travaille en rupture de flux. La plupart des proxys travaillent avec le protocole HTTP, et si on parle de proxy sans préciser le protocole applicatif, il s'agit d'un proxy web (HTTP).

a. Protection des clients

Les serveurs proxys étant les seuls à aller sur Internet (en principe, tout client doit passer par le proxy pour obtenir un contenu provenant d'Internet), ils sont en première ligne en cas d'agissement hostile de l'extérieur. Un serveur proxy correctement configuré assurera donc une protection naturelle des navigateurs Internet sur le réseau.

b. Serveurs de cache

Toutes les requêtes passent par le proxy, le proxy récupère les données sur le serveur et les retransmet au client. Dans la plupart des cas, le serveur conserve sur son disque une copie de ces données afin de répondre directement aux clients suivants s'ils font les mêmes requêtes. La navigation des clients est donc accélérée puisqu'il n'est pas nécessaire de systématiquement relayer les demandes vers les serveurs web.

La généralisation du haut débit rend les bénéfices de proxys serveurs de cache moins spectaculaires.

c. Filtrages

Les serveurs proxys ont la possibilité de refuser tout ou partie de leurs requêtes à certains clients. On peut alors refuser en bloc toute navigation, ou filtrer certaines url pour empêcher la navigation sur des sites non professionnels par exemple. Le serveur proxy est supérieur au pare-feu pour cette fonction car le proxy « comprend » ce qui est demandé (une URL), alors que le pare-feu se borne à autoriser ou interdire tout trafic sur un port (80 pour Internet) sans distinguer les sites web visités.

d. Inconvénients

Les serveurs proxy ne sont pas sans inconvénients. Ils supposent une configuration spécifique des clients (on précise alors l'adresse IP du proxy au navigateur), et sont limités à un protocole applicatif, nécessitant alors d'autres mécanismes de protection ou d'optimisation pour chacun des protocoles. Pour chaque déploiement envisagé de proxy, il conviendra donc d'estimer précisément les avantages et inconvénients générés par le proxy.

2. Le serveur proxy squid

a. Configuration de base

Squid est composé d'un service dont le script de lancement normalisé trouve sa configuration dans un fichier unique **squid.conf**, généralement situé dans **/etc/squid**.

La configuration de squid dans un mode de fonctionnement standard (rupture de flux pour les accès clients et quelques listes d'accès pour gérer les autorisations) n'a rien de bien difficile, mais dans la plupart des implémentations, le fichier de configuration par défaut de squid a de quoi impressionner. Sur le paquetage fourni avec debian par exemple, le fichier fait près de 5000 lignes, dont environ un pour cent seulement sont lues au démarrage du service.

Fichier squid.conf d'un paquetage debian sans commentaires

Constatez qu'un certain nombre de liste de contrôle d'accès (acl) ainsi que de règles sont définies par défaut. Ceci ne dispense pas d'une configuration précise du proxy pour assurer la meilleure sécurité.

```
# grep ^[^#] squid.conf
acl all src all
```

```
acl manager proto cache_object
acl localhost src 127.0.0.1/32
acl to_localhost dst 127.0.0.0/8
acl localnet src 10.0.0.0/8  # RFC1918 possible internal network
acl localnet src 172.16.0.0/12   # RFC1918 possible internal network
acl localnet src 192.168.0.0/16  # RFC1918 possible internal network
acl SSL_ports port 443    # https
acl SSL_ports port 563    # snews
acl SSL_ports port 873    # rsync
acl Safe_ports port 80    # http
acl Safe_ports port 21    # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70    # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl Safe_ports port 631         # cups
acl Safe_ports port 873         # rsync
acl Safe_ports port 901         # SWAT
acl purge method PURGE
acl CONNECT method CONNECT
http_access allow manager localhost
http_access deny manager
http_access allow purge localhost
http_access deny purge
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost
http_access deny all
icp_access allow localnet
icp_access deny all
http_port 3128
hierarchy_stoplist cgi-bin ?
access_log /var/log/squid/access.log squid
refresh_pattern ^ftp:        1440    20%    10080
refresh_pattern ^gopher:     1440    0%     1440
refresh_pattern -i (/cgi-bin/|\?)  0 0%     0
refresh_pattern (Release|Package(.gz)*)$    0       20%    2880
refresh_pattern .            0       20%    4320
acl shoutcast rep_header X-HTTP09-First-Line ^ICY\s[0-9]
upgrade_http0.9 deny shoutcast
acl apache rep_header Server ^Apache
broken_vary_encoding allow apache
extension_methods REPORT MERGE MKACTIVITY CHECKOUT
visible_hostname beta
hosts_file /etc/hosts
coredump_dir /var/spool/squid
```

Sans configuration particulière, un serveur proxy squid fait naturellement office de serveur de cache, et protège les réseaux locaux par une rupture de flux (les requêtes des navigateurs ne vont pas sur Internet, mais s'arrêtent au proxy qui va consulter les serveurs en leur lieu et place).

Avant qu'il puisse fonctionner, un serveur a tout de même besoin d'un minimum de configuration.

Configuration minimum d'un proxy squid dans le fichier squid.conf

```
http_port numero_port
cache_dir ufs repertoire taille rep_niveau_1 rep_niveau_2
visible_hostname nom_serveur
```

Fichier squid.conf : configuration de base	
numero_port	Le numéro de port sur lequel le serveur écoute et qui doit être configuré sur les navigateurs. La valeur par défaut est 3128, et 8080 est une valeur historique courante.

repertoire	Le répertoire dans lequel les données mises en cache sont stockées.
taille	Taille en Mégaoctets maximum pour les données mises en cache. Valeur par défaut : 100 Mo.
rep_niveau_1	Nombre de sous-répertoires de premier niveau maximum du répertoire de cache. Valeur par défaut : 16.
rep_niveau_2	Nombre de sous-répertoires de deuxième niveau maximum du répertoire de cache. Valeur par défaut : 256.
nom_serveur	Nom d'hôte du serveur proxy. Ce nom apparaît notamment dans les journaux d'activité.

b. Gestion des accès clients

Il s'agit ensuite de préciser qui peut ou ne peut pas accéder à Internet par l'Intermédiaire du serveur proxy.

La première étape est de définir des hôtes ou ensembles d'hôtes (groupes, réseaux) auquel on appliquera une autorisation. Ces groupes sont créés sous le nom d'acl (acces control list).

Définition de listes de contrôle d'accès dans le fichier squid.conf

`acl` *`nom_liste type_acl A.B.C.D/M`*

Fichier squid.conf : définition d'acl		
nom_liste		Le nom de la liste créé. Valeur alphanumérique quelconque.
type_acl	src	Définition des adresses d'expéditeurs.
	dst	Définition des adresses de destinataires.
A.B.C.D/M		Adresse de réseau et masque de sous réseau (nombre de bits du masque).
		Adresse d'hôte et masque de sous réseau (nombre de bits du masque).
		Intervalle d'adresses : A.B.C.D-E.F.G.H/M (nombre de bits à 1 du masque).

Exemple de définition d'acl

Notez la définition de l'acl « all » qui désigne tous les réseaux possibles.

```
acl all src all
acl rezo_local src 192.168.1.0/24
acl serveurs_interdits dst 172.11.5.2-172.11.5.5/24
```

Il n'y a plus qu'à faire savoir à squid quoi faire de ces acl.

Autorisation des acl dans le fichier squid.conf

`http_access` *`autorisation nom_acl`*

Fichier squid.conf : autorisation d'acl	
autorisation	Autorisation ou refus de l'acl. Les deux valeurs possibles sont allow et deny.
nom_acl	Le nom de la liste à autoriser ou refuser.

Exemple d'autorisations d'acl

Chaque acl est traitée selon un contrôle d'accès allow ou deny.

```
acl all src all
acl rezo_local src 192.168.1.0/24
acl serveurs_interdits dst 172.11.5.2-172.11.5.5/24
http_access deny serveurs_interdits
http_access allow rezo_local
http_access deny all
```

Il est possible de définir des acl dans un fichier extérieur au fichier de configuration principal.

Intégration d'un fichier d'acl dans le fichier de configuration

```
acl nom_acl "fichier_acl"
```

Où *fichier_acl* représente le chemin absolu du fichier contenant les acls. Ce fichier doit impérativement être entre doubles quotes.