

PTI : Proxy Squid

Fonctions de filtrage à l'aide d'un proxy Squid

COMPETENCES ABORDEES

C21.....	Installer et configurer un microordinateur
C22.....	Installer et configurer un réseau
C23.....	Installer et configurer un dispositif de sécurité
C31.....	Assurer les fonctions de base de l'administration d'un réseau
C32.....	Assurer les fonctions de l'exploitation

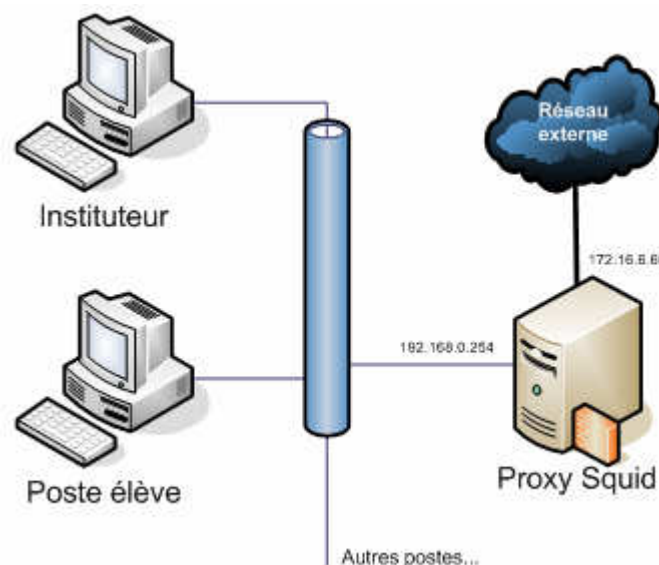
OBJECTIFS

Une école comportant quelques postes avec un accès à Internet à disposition des élèves, nécessitait une solution permettant d'empêcher les élèves d'accéder à des sites au contenu illicite ou à caractère pornographique. Un serveur proxy Squid a donc été mis en place pour réaliser ce filtrage.

MISE EN PLACE

Etat du réseau :

- Systèmes d'exploitation :
 - GNU/Linux Fedora Core 2 ;
 - Windows XP Professionnel.
- Caractéristiques matérielles :
 - Ethernet 10/100Mbps.



CONFIGURATIONS DE BASE

Configuration des interfaces :

▪ Serveur Proxy :

`eth0 (192.168.0.254)`

interface vers le réseau interne ;

`eth1 (172.16.6.66)`

interface vers le réseau externe.

```
ifconfig ethx xxx.xxx.xxx.xxx netmask xxx.xxx.xxx.xxx
```

▪ Postes :

`192.168.0.1`

poste de l'instituteur ;

`192.168.0.2-192.168.0.100`

autres postes.

Activation du routage :

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

On peut ensuite effectuer des tests pour vérifier que le routage fonctionne correctement à l'aide de commandes Ping.

Activation de la translation d'adresse :

Afin de permettre aux postes d'accéder à Internet, il est nécessaire d'activer la translation d'adresse. Ainsi tous les postes seront regroupés derrière de serveur Proxy, tous ayant la même adresse IP vis-à-vis de l'extérieur.

```
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
```

-t NAT	<i>translation d'adresse (Network Address Translation) ;</i>
-A POSTROUTING	<i>règle à effectuer après routage du paquet ;</i>
-o eth1	<i>pour les paquets sortants par l'interface eth1 du serveur ;</i>
-j MASQUERADE	<i>action : translation d'adresse.</i>

Forcer le passage par le proxy :

Après avoir effectué les configurations de base, il faut maintenant faire en sorte que le passage par le proxy soit obligatoire pour toutes les requêtes sortantes HTTP.

Pour cela on utilise les règles de filtrage **Netfilter** (*iptables*).

```
iptables -t nat -A PREROUTING -p tcp -i eth0 --dport 80 -j REDIRECT --to-port 8080
```

-A PREROUTING	<i>règle à effectuer avant le routage du paquet ;</i>
-p tcp	<i>utilisation du protocole TCP ;</i>
-i eth0	<i>paquets entrant via l'interface eth0 ;</i>
--dport 80	<i>toutes les requêtes en direction d'un port 80 ;</i>
-j REDIRECT	<i>action : redirection du paquet ;</i>
--to-port 8080	<i>redirection vers le port 8080 du proxy.</i>

Modification du fichier de configuration :

Quelques modifications et paramétrages sont à effectuer dans le fichier de configuration `"/etc/squid/squid.conf"`.

```
visible_name gengis
http_port 8080
```

visible_name	<i>nom du serveur proxy ;</i>
http_port 8080	<i>port utilisé par le serveur proxy.</i>

▪ Accélération des requêtes :

Il est aussi possible d'accélérer le traitement des requêtes par le serveur, et ce en ajoutant quelques options au fichier de configuration.

```
httpd_accel_host virtual
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
```

httpd_accel_host	<i>serveur à accélérer (virtual si plusieurs) ;</i>
httpd_accel_port	<i>port pour lequel les requêtes doivent être accélérées ;</i>
httpd_accel_with_proxy	<i>utilisation du proxy avec cache ;</i>
httpd_accel_uses_host_header	<i>prise en compte des entêtes de serveur (~ virtual).</i>

Mise en place de règles ACL (Access Control List) :

Une fois le serveur proxy configuré, il ne reste de plus qu'à établir les critères de restriction d'accès à certains contenus Web.

▪ Déclaration des règles et des postes :

```
acl admin src 192.168.0.1
acl postes src 192.168.0.2-192.168.0.100
acl sex url_regex -i porn sex teen xxx
```

- Application des règles:

Les règles doivent être appliquées dans l'ordre allant du moins restrictif au plus restrictif, permettant ainsi d'autoriser certaines actions en fonction de certains paramètres.

```
http_access allow admin
http_access deny sex
http_access allow postes
http_access deny all
```