

## PTI #02 : Serveur Proxy Squid et Netfilter

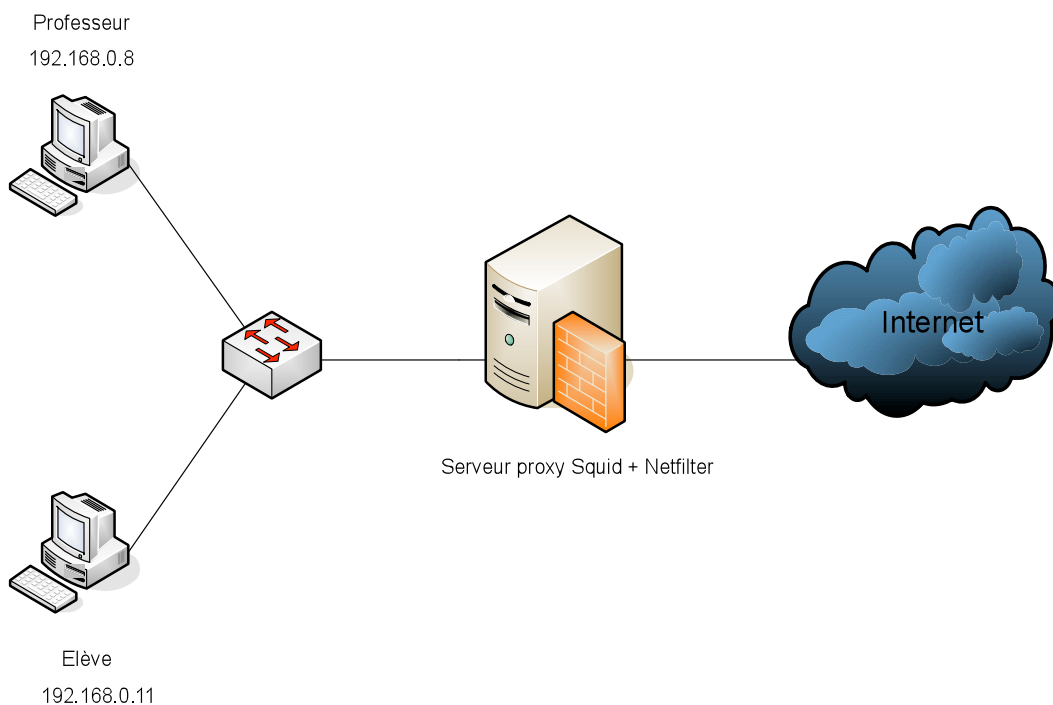
## Compétences abordées

- C21 : Installer et configurer un microordinateur
- C22 : Installer et configurer un réseau
- C23 : Installer et configurer un dispositif de sécurité
- C26 : Installer un périphérique
- C31 : Assurer les fonctions de base de l'administration réseau
- C32 : Assurer les fonctions de l'exploitation

## Objectifs

Un serveur proxy permet dans le milieu scolaire de limiter l'accès au réseau. Si on ne veut pas qu'un utilisateur accède à des sites à caractère illicite, on peut bloquer l'accès à ces sites soit à tous les utilisateurs, soit à certains utilisateurs. Il est aussi possible de bloquer juste certains mots que l'utilisateur pourrait taper lors d'une recherche ou bien si le site comporte ces mots interdits, le site sera bloqué.

## Mise en place



## Etat du réseau

- Système d'exploitation :
  - Linux Fedora Core 5
  - Windows XP Professionnel
- Caractéristiques matérielles :
  - Ethernet 10/100 mbps

## Configuration des interfaces

Serveur Proxy :

eth0 : 192.168.0.254

eth1 : 172.16.6.112

Postes client :

Elève : 192.168.0.9

Professeur : 192.168.0.11

Activation du routage

Sur le serveur, il faut activer le routage grâce à la commande :

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

Modification du fichier de configuration de Squid

On ouvre le fichier :

```
vim /etc/squid/squid.conf
```

Puis on recherche les lignes où se trouvent les informations visible\_name et http\_port :

```
visible_name julien # ligne n'existant pas par défaut (à rajouter dans le fichier)
http_port 8080
```

visible\_name : indique le nom du serveur

http\_port : indique le port utilisé par le serveur proxy

Accélérateur de requêtes

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

httpd\_accel\_host : serveur accéléré

httpd\_accel\_port : port pour lequel les requêtes doivent être accélérées

httpd\_accel\_with\_proxy : utilisation du proxy avec le cache

httpd\_accel\_uses\_host\_header : prise en compte des entêtes de serveur

### Ajout des règles Netfilter

Notre politique par défaut est de bloquer tout. Donc il nous faut laisser passer le trafic Web, DNS afin que les clients puissent surfer sur internet.

#### Chargement des modules

Netfilter nécessite le chargement de certains modules lorsque ces derniers ne sont pas compilés dans le noyau Linux.

```
modprobe ip_tables
modprobe iptable_filter
modprobe iptable_nat
```

ip\_tables : module principal  
iptable\_filter : module de filtrage des paquets  
iptable\_nat : module pour la translation d'adresse

On vide les tables de Netfilter

```
iptables -t nat -F
iptables -F
```

La politique par défaut

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

Autorisation du DNS

```
iptables -A FORWARD -p udp -i eth0 -s 212.180.1.79 --sport 53 -j ACCEPT
iptables -A FORWARD -p udp -o eth0 -d 212.180.1.79 --dport 53 -j ACCEPT
iptables -A FORWARD -p udp -o eth0 -d 212.180.0.137 --dport 53 -j ACCEPT
iptables -A FORWARD -p udp -i eth0 -s 212.180.0.137 --sport 53 -j ACCEPT

iptables -A INPUT -p udp -i eth0 --sport 53 -j ACCEPT
iptables -A OUTPUT -p udp -o eth0 --dport 53 -j ACCEPT
```

Les requêtes HTTP

```
iptables -A INPUT -p tcp -i eth1 --dport 8080 -j ACCEPT
iptables -A OUTPUT -p tcp -o eth1 --sport 8080 -j ACCEPT

iptables -A INPUT -p tcp -i eth0 --sport 80 -j ACCEPT
iptables -A OUTPUT -p tcp -o eth0 --dport 80 -j ACCEPT
```

La translation d'adresse

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Et pour finir on force le passage par le proxy

```
iptables -t nat -A PREROUTING -p tcp -i eth1 --dport 80 -j REDIRECT --to-port 8080
```