CHAPITRE 7 :
Filtrage par PROXY
— Cas Proxy WEB —

Mohammed SABER

Département Électronique, Informatique et Télécommunications
École Nationale des Sciences Appliquées "ENSA"
Université Mohammed Premier OUJDA

Année Universitaire : 2017-2018

Plan de chapitre

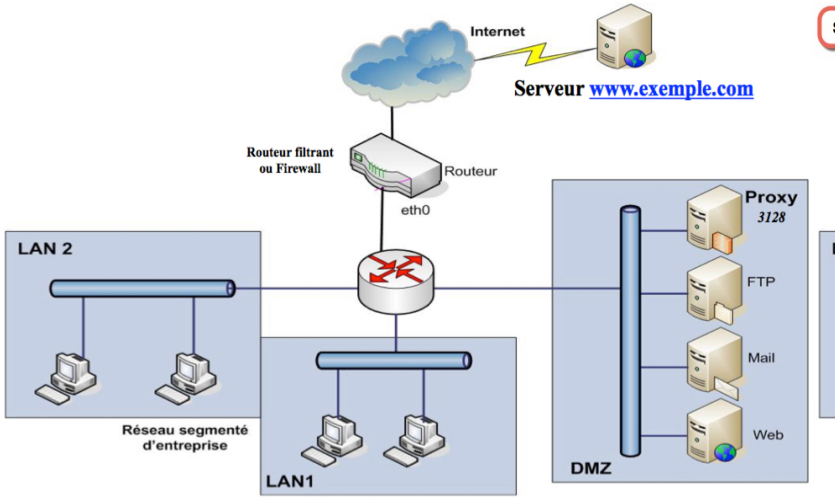
Plan de chapitre

Introduction

- Proxy = mandataire (traduction)
- Un Proxy est un service mandataire pour une application donnée.
- C'est-à-dire qu'il sert d'intermédiaire dans une connexion entre le client et le serveur pour relayer la requête qui est faite.
- Ainsi, le client s'adresse toujours au Proxy, et c'est lui qui s'adresse ensuite au serveur.
- Permet de casser complètement la connectivité directe à l'Internet des machines internes (possibilités de fermer tous les ports entre les machines d'un réseau interne et de l'Internet).
- Ne peuvent être utilisées que des applications supportées par un relais applicatif, par exemple :
  - FTP vers une machine passerelle puis vers l'Internet.
  - Cache Web.
  - Serveur relai de messagerie.
  - etc ...

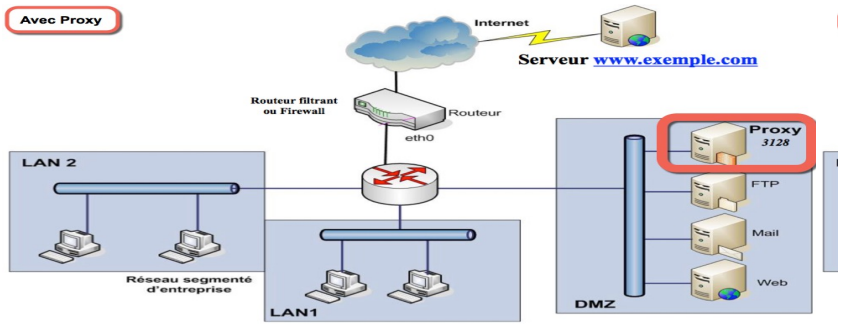
Plan de chapitre

Fonctionnement d'un serveur Proxy
Architecture sans Proxy



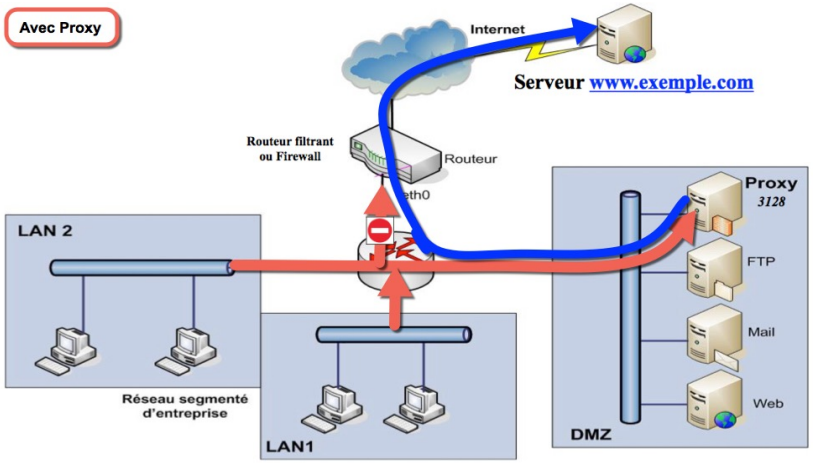
Fonctionnement d'un serveur Proxy
Architecture avec Proxy

- Le principe de fonctionnement basique d'un serveur proxy est assez simple : il s'agit d'un serveur "mandaté" par une application pour effectuer une requête sur Internet à sa place.
- Ainsi, lorsqu'un utilisateur se connecte à Internet à l'aide d'une application cliente configurée pour utiliser un serveur proxy, celle-ci va se connecter en premier lieu au serveur proxy et lui donner sa requête.



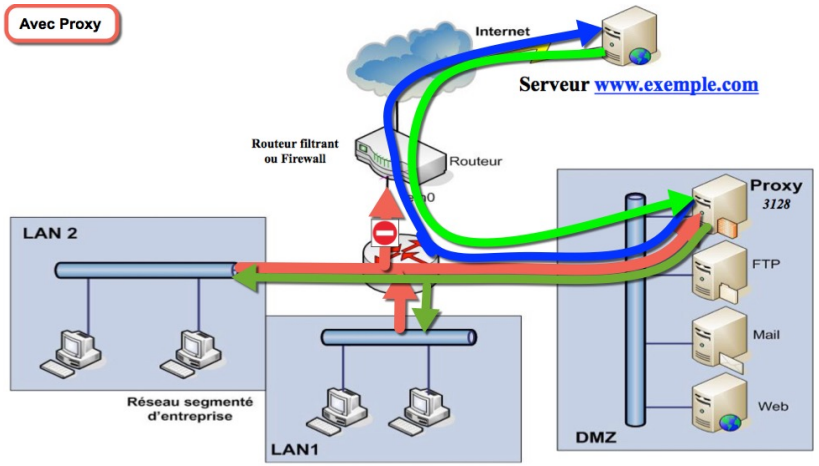
Fonctionnement d'un serveur Proxy
Architecture avec Proxy

Le serveur proxy va alors se connecter au serveur que l'application demandé par le client et lui transmettre la requête.



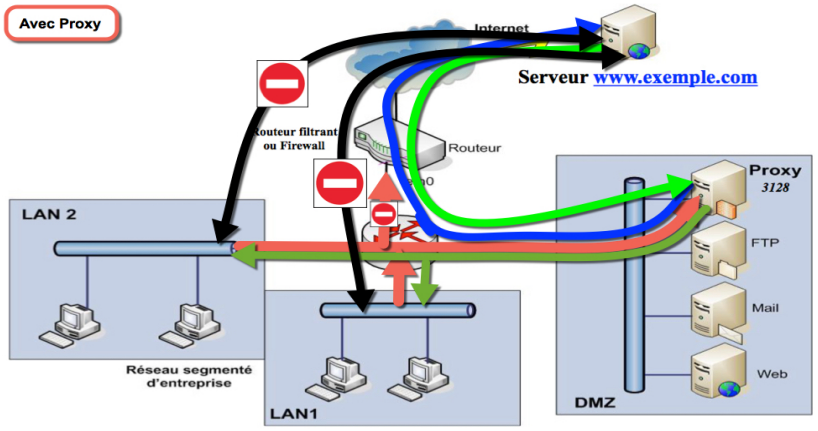
Fonctionnement d'un serveur Proxy
Architecture avec Proxy

Le serveur va ensuite donner sa réponse au proxy, qui va à son tour la transmettre à l'application cliente.



Fonctionnement d'un serveur Proxy
Architecture avec Proxy

Le serveur jamais connecté directement à l'application cliente.



Plan de chapitre

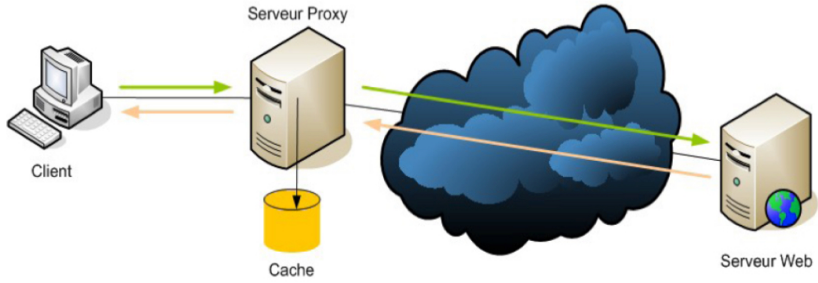
Fonctionnalités d'un serveur Proxy

- Avec l'utilisation de TCP/IP au sein des réseaux locaux, le rôle de relais du serveur proxy est directement assuré par les passerelles et les routeurs.
- Les serveurs proxy un certain nombre de fonctionnalités :
  - Fonctions de cache.
  - Fonction d'enregistrement.
  - Fonction de filtre.
  - Fonction de sécurité.
  - Autres fonctions.

Fonctionnalités d'un serveur Proxy
Fonction de cache

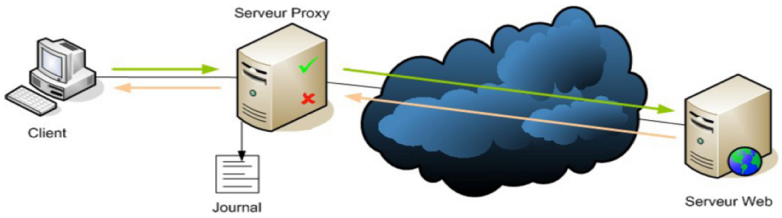
- La plupart des proxys assurent ainsi une fonction de **cache**, c'est-à-dire la capacité à garder en **mémoire (en "cache")** les pages les plus souvent visitées par les utilisateurs du réseau local afin de pouvoir les leur fournir le plus rapidement possible.
- En effet, en informatique, le terme de **"cache"** désigne un espace de stockage temporaire de données (le terme de **"tampon"** est également parfois utilisé).
- Un serveur proxy ayant la possibilité de cacher ("mettre en mémoire cache") les informations est généralement appelé "**serveur proxy-cache**".
- Cette fonctionnalité implémentée dans certains serveurs proxy permet d'une part de réduire l'utilisation de **la bande passante** vers Internet ainsi que de réduire le temps d'accès aux documents pour les utilisateurs.
  - Le cache accélère les consultations des informations déjà demandées.
  - Le trafic réseau en est diminué.
- Toutefois, pour mener à bien cette mission, il est nécessaire que le proxy compare régulièrement les données qu'il stocke en mémoire cache avec les données distantes afin de s'assurer que les données en cache sont toujours valides.

Fonctionnalités d'un serveur Proxy
Fonction de cache



Fonctionnalités d'un serveur Proxy
Fonction d'enregistrement

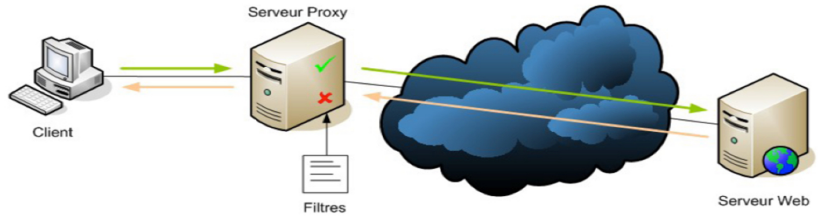
- Le serveur garde une trace détaillée de toutes les informations qui le traversent.
- Par l'utilisation d'un proxy, il est possible d'assurer un suivi des connexions via la constitution de journaux d'activité (**logs**) en enregistrant systématiquement les requêtes des utilisateurs lors de leurs demandes de connexion à Internet.



- Génère un fichier journal (fichier de log) : enregistre la trace des requêtes effectuées par tous les clients utilisant le proxy :
  - L'identification du client,
  - Les dates et heures de connexion,
  - Les URL des ressources consultées,
  - Les tailles et temps de téléchargement, etc.

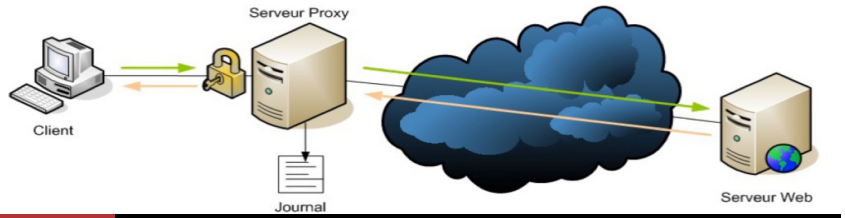
Fonctionnalités d'un serveur Proxy
Fonction de filtrage

- Par l'utilisation d'un proxy, Il est ainsi possible de filtrer les connexions à Internet en analysant d'une part les requêtes des clients, d'autre part les réponses des serveurs.
- Lorsque le filtrage est réalisé en comparant la requête du client avec **la liste de contrôle d'accès (ACL)**.
- C.à.d la requête est comparée avec une liste de requêtes autorisées, on parle de **liste blanche**, lorsqu'il s'agit d'une liste de sites interdits on parle de **liste noire**.
- Enfin l'analyse des réponses des serveurs conformément à une liste de critères (mots-clés, ...) est appelé **filtrage de contenu**.



Fonctionnalités d'un serveur Proxy
Fonction de sécurité (authentification)

- Dans la mesure où le proxy est l'intermédiaire indispensable des utilisateurs du réseau interne pour accéder à des ressources externes, il est parfois possible de l'utiliser pour authentifier les utilisateurs.
- C'est-à-dire de leur demander de s'identifier à l'aide d'un nom d'utilisateur et d'un mot de passe par exemple.
- Il est ainsi aisé de donner l'accès aux ressources externes aux seules personnes autorisées à le faire et de pouvoir enregistrer dans les fichiers journaux des accès identifiés.
- Ce type de mécanisme lorsqu'il est mis en œuvre pose bien évidemment de nombreux problèmes relatifs aux libertés individuelles et aux droits des personnes.



Fonctionnalités d'un serveur Proxy
Les reverse-proxy

- On appelle **reverse-proxy** (en français le terme de relais inverse est parfois employé) un serveur proxy-cache "monté à l'envers", c'est-à-dire un **serveur proxy** permettant non pas **aux utilisateurs d'accéder au réseau Internet**, mais aux utilisateurs d'Internet d'accéder indirectement à certains serveurs internes.
- **Le reverse-proxy** sert ainsi de relais pour les utilisateurs d'Internet souhaitant accéder à un site web interne en lui transmettant indirectement les requêtes.
- Grâce au **reverse-proxy**, le serveur web est protégé des attaques directes de l'extérieur, ce qui renforce la sécurité du réseau interne.
- D'autre part, la fonction de cache du **reverse-proxy** peut permettre de soulager la charge du serveur pour lequel il est prévu, c'est la raison pour laquelle un tel serveur est parfois appelé **"accélérateur" (server accelerator)**.
- Enfin, grâce à des algorithmes perfectionnés, le **reverse-proxy** peut servir à répartir la charge en redirigeant les requêtes vers différents serveurs équivalents ; on parle alors de **"répartition de charge"**, ou en anglais **"load balancing"**.

Plan de chapitre

Avantages et Inconvénient d'un serveur Proxy

Avantages d'un serveur Proxy

- Limiter par exemple l'accès à Internet.
- Cacher les utilisateurs.
- Filtrage applicatif (HTTP, FTP, . . .)
- Optimise la bande passante vers l'Internet en mettant en cache (disque) les informations consultées de l'Internet.
- Filtrage efficace des sites autorisés / interdits.

Inconvénient d'un serveur Proxy

Nécessite une connexion utilisateur par type de service difficile si l'application n'est pas supportée par le proxy.

Plan de chapitre

Mise en œuvre de Proxy Web Squid
Installation de Proxy Web Squid

- Installation sous debian :

```
# apt-get install squid
```

- Démarrage de service :

```
# /etc/init.d/squid start OR service squid start
```

- Supprimer le contenu du cache :

```
# squid -z
```

- Le fichier de configuration `/etc/squid/squid.conf` fonctionne de la même manière que les autres fichiers de configuration Linux, on entre des directives et les options qui vont avec.
- Les lignes commençant par # sont des commentaires.
- Il y a plusieurs directives à configurer, pour faire simple, voici seulement quelques directives à connaître : Configuration générale, configuration de cache, configuration de filtrage et configuration d'authentification.

Mise en œuvre de Proxy Web Squid
Configuration générale et configuration de cache

```
########################## # SQUID.CONF # ##########################

# CONFIGURATION GENERALE

# Numéro de port http sur lequel les clients se connectent. Souvent 8080
# On peut aussi préciser sur quelle @IP

http_port 192.168.0.101:3128

# Nom DNS du proxy
visible_hostname proxy.mynetcourse.info
```

```
# CONCERNANT LE CACHE :

# Mémoire vive allouée à Squid
cache_mem 20 MB

# Quand le cache est rempli à 90% il se vide jusqu'à 75% de sa capacité
cache_swap_low 75

cache_swap_high 90

# Interdire de stocker en cache des objets de plus de 8M
maximum_object_size 8192 KB
```


Mise en œuvre de Proxy Web Squid
Configuration de filtrage par les ACLs

- Les **ACLs** sont des listes de machines, de réseaux auxquelles on affecte un certain nombres de droits.
- Elles sont utilisées pour dire que telle machine ou tel réseau à le droit ou pas de faire telles choses.
- Elles se configurent en deux temps :
  - D'abord la déclaration des **ACLs** avec la directive `acl` :

```
acl <nom-acl> src/dest groupe-de-machines
```

  - Ensuite, on donne des droits sur l'`acl` que l'on a déclaré avec par exemple la directive `http_access` qui donne des droits sur les requêtes **http**.

```
http_access allow/deny <nom-acl>
```

Mise en œuvre de Proxy Web Squid
Configuration de filtrage par les ACLs

```
### Déclaration de diverses ACL ###

# Cette liste concerne tous les accès provenant du réseau 192.168.0.0
acl lan1 src 192.168.0.0/255.255.255.0

# Cette liste concerne tous les accès à destination du réseau 10.0.0.0
acl servers dest 10.0.0.0/255.0.0.0

# Cette liste concerne tous les accès à destination du domaine yahoo.fr
acl yahoo dest www.yahoo.fr

# Cette liste concerne des mots-clés
acl interdit url_regex drogue
acl interdit url_regex violence

# Cette liste concerne toutes les machines non listées ci-dessus
acl autres src 0.0.0.0/0.0.0.0
```

Stratégie par défaut

```
### Droits de requêtes http pour les acl déclarées au-dessus ###
http_access deny interdit
http_access allow lan1
http_access deny servers
http_access deny all

# ... Il est possible d'imaginer beaucoup d'autres restrictions
```


Mise en œuvre de Proxy Web Squid
Configuration d'authentification

- Création des utilisateurs avec leurs mots de passe.
  - Par exemple pour créer l'utilisateur **toto** avec le mot de passe **motdepasse**, utiliser la commande :

```
# htpasswd -cb /etc/squid/users toto motdepasse
```

  - Testez votre fichier de mot de passe en tapant la commande :

```
# /usr/lib/squid/ncsa_auth /etc/squid/users
toto motdepasse
OK
```

- Autorisation au niveau de proxy sur le fichier de configuration `squid.conf` :

```
auth_param basic program /usr/lib/squid/ncsa_auth
/etc/squid/users
acl restriction proxy_auth REQUIRED
http_access allow restriction
http_access deny !restriction
```


QUESTIONS ?